UNIVERSITY OF SOUTHAMPTON

Infinite permutation groups containing all finitary permutations

by

Charles Garnet Cox

A thesis submitted in partial fulfillment for the degree of Doctor of Philosophy

in the
Faculty of Mathematics
School of Social, Human, and Mathematical Sciences

August 2016

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICS
SCHOOL OF SOCIAL, HUMAN, AND MATHEMATICAL SCIENCES

Doctor of Philosophy

by Charles Garnet Cox

Groups naturally occur as the symmetries of an object. This is why they appear in so many different areas of mathematics. For example we find class groups in number theory, fundamental groups in topology, and amenable groups in analysis. In this thesis we will use techniques and approaches from various fields in order to study groups.

This is a 'three paper' thesis, meaning that the main body of the document is made up of three papers. The first two of these look at permutation groups which contain all permutations with finite support, the first focussing on decision problems and the second on the R_∞ property (which involves counting the number of twisted conjugacy classes in a group). The third works with wreath products $C \wr \mathbb{Z}$ where C is cyclic, and looks to determine the probability of choosing two elements in a group which commute (known as the degree of commutativity, a topic which has been studied for finite groups intensely but at the time of writing this thesis has only two papers involving infinite groups, one of which is in this thesis).

Contents

Academic Thesis: Declaration of Authorship

I, Charles Paul Garnet Cox, declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

Title of thesis: Infinite permutation groups containing all finitary permutations.

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published works of others, this has always been clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself or jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. This thesis consists of material published in:
   [Cox14] C. Cox: Twisted conjugacy in Houghton's groups
   [Cox16a] C. Cox: A note on the R_∞ property for groups $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$
   [Cox16b] C. Cox: The degree of commutativity and lamplighter groups

Signed:

Date:

Acknowledgements

First, I thank my Mum and Dad for always being there for me.

I thank all of the members of staff at the University of Southampton for the interesting and helpful discussions. In particular I thank my supervisor Armando Martino for his time and academic insight, my advisor Graham Niblo, and my examiners Ian Leary and Collin Bleak for their time and their kind comments. Pre-PhD I would like to thank Christopher Voll and Arslan Hojiyew, you were both a great inspiration.

This seems a good point to explicitly mention all of those people whose offices I have been seen in during my PhD. Thank you (in roughly the order that you started or that I met you): Alex Bailey, Raffaele Rainone, Max Fennelly, Elkaïoum Moutuou, Tom Harris, Yu Yen, Chris Cave, Joe Tait, Conor Smyth, Simon St-John Green, Michael West, David Matthews, Michal Ferov, Robin Frankhuizen, Matt Burfitt, Dionisis Syrigos, Ingrid Membrillo-Solis, Doha Kattan, Ana Cláudia Lopes Onório, Hector Durham, Larry So, Semih Piri, Ashley Steward, Tyrone Cutler, Abigail Linton, Lorna Willington, Xin Fu, Fabio Strazzeri, James Strudwick, Kiko Belchí, and Mariam Pirashuili. I have enjoyed your friendship, conversations, and many a fried breakfast: may you keep this tradition going. In particular I thank Alex, Raff, Tom, Joe, Simon, Mike, Michal, Dave, and Matt for being so welcoming and being so very memorable, and again Matt for being the best person to share a desk with, and for being such a kind and thoughtful soul. I thank Dave, Simon, and Peter Jones for the joy of making music and plenty of laughs.

I also thank the people I lived with and met through those I lived with during my PhD: Jess, Silke, Lukas, Sebastian, Timo, Joachim, Joanna, Paul (aka Frank), and Josh. Thank you for all of the comedy, cooking, and tea.

Thank you to all of those I have met in the last three years, it has been very special.

Nomenclature

$\mathbb{Z}$	the integers
$\mathbb{Z}_n$	$\{1, 2, \ldots, n\}$
$\mathbb{N}$	the natural numbers, which we will consider to be the positive integers
Countable	of cardinality equal to a subset of $\mathbb{N}$
Countably infinite	of cardinality equal to $\mathbb{N}$
Uncountable	of greater cardinality than $\mathbb{N}$
$A \times B$	the cartesian product of A and B i.e. $\{(a, b) \mid a \in A, b \in B\}$
C_n	the cyclic group of order n
D_n	the dihedral group of order $2n$
S_n	the symmetric group of order $n!$
	unless stated, we will assume that C_n, D_n, and S_n act on the set $\mathbb{Z}_n$
$\langle A \rangle$	the group generated by elements from the set A
$\langle A \rangle_H$	the normal closure of A
$N_H(G)$	the normaliser of G i.e. $\{\rho \in H \mid \rho^{-1} g \rho \in G\}$
$\mathrm{Sym}(X)$	the group of all permutations of X
$\mathrm{FSym}(X)$	the group of all permutations of X with finite support
$\mathrm{FAlt}(X)$	the group of all even permutations of X with finite support
ϕ_g	the automophism induced by conjugation by g
	i.e. $(h)\phi_g := g^{-1}hg$ for all $h \in G$
$G \cong_\Psi H$	G is isomorphic to H via the isomorphism $\Psi : G \to H$
$\bigoplus_{i \in I} G_i$	the direct sum of the groups G_i
$\prod_{i \in I} G_i$	the direct product of the groups G_i
1	the identity element of a group (unless the group is abelian)
$H \leqslant_f G$	H has finite index in G
$G \wr_X H$	the permutational wreath product with head H acting on X
$[G, H]$	the commutator subgroup of G and H, i.e. $\langle g^{-1}h^{-1}gh \mid g \in G, h \in H \rangle$
	when working with functions that we may compose, we
	will act on the right, so that fg means apply f then g

Background

1 Introduction

The aim of this chapter is to provide background and context for the three papers that follow. We will refer to these as paper 1, paper 2, and paper 3 respectively.

We begin by introducing common ways to produce a new group from two or more groups. This leads us to discuss group extensions and finite index subgroups. We then give background relating to paper 1 on decision problems for groups. Section 3 contains background for paper 2, including a proof (Proposition 3.3.1 on page 31) which was my first result as a PhD student. The final section provides background for paper 3, including introductions to growth of groups and the degree of commutativity of a group.

There is much relevant and interesting mathematics which could have been included in this chapter. In general I have tried to take an efficient path to cover those topics relevant to the three papers. For this reason I have given a more cursory overview of topics for which I am aware of a reference which reflects my view and where the technicalities involved seem disproportionate to the relevance of the topic. Thus, only a cursory glance has been given to: free groups; Turing machines; Tietze transformations; classes of groups e.g. hyperbolic groups; properties of groups e.g. virtually, poly, locally, meta, and when these properties are preserved. References for these topics are provided within the text for the interested reader.

Throughout we shall assume The Axiom of Choice, indeed, it is vital to some of our arguments (for example in paper 2, where we assume that every infinite set contains a countably infinite subset).

1.1 Groups as collections of permutations

This section aims to provide motivation for considering groups as permutations of a set. For many groups this allows for a more hands on approach. I developed this point of view since the Houghton groups, studied in paper 1, are naturally seen as permutations of a countable set $\{1, \ldots, n\} \times \mathbb{N}$ for some $n \in \mathbb{N}$. I also took this approach in paper 2.

Paper 3 involves generalisations of the lamplighter groups, which are wreath products (defined below) and whose elements can be naturally viewed as permutations of a set. In both paper 1 and paper 2 we encounter the following.

Notation. For a non-empty set X, let $\mathrm{Sym}(X)$ denote the group of all permutations of X. Furthermore, let $\mathrm{FSym}(X)$ denote the group of all permutations of X with finite support, and let $\mathrm{FAlt}(X)$ denote the group of all even permutations of X with finite support. We will denote these by Sym, FSym, and FAlt respectively if it is not ambiguous to do so.

For more information on the groups Sym, FSym, and FAlt, see [Cam99, Chap. 6].

Definition 1.1.1. Let G be a group. Then $\mathrm{Aut}(G)$ is the group of all isomorphisms from G to G, known as *automorphisms* of G. Let $\phi \in \mathrm{Aut}(G)$. If there exists a $g \in G$ such that $(h)\phi = g^{-1}hg$ for all $h \in G$, then ϕ is called *inner*. The set of all inner automorphisms form a normal subgroup of $\mathrm{Aut}(G)$, which we denote $\mathrm{Inn}(G)$. Not all automorphisms are inner. For example $\mathbb{Z}$ is abelian and so $\mathrm{Inn}(\mathbb{Z})$ is trivial, yet $\mathbb{Z}$ has an automorphism of order 2 (which sends each element to its inverse). Then $\mathrm{Out}(G) := \mathrm{Aut}(G) \big/ \mathrm{Inn}(G)$ and these elements are known as *outer automorphisms*.

Notation. Let $G \leqslant \mathrm{Sym}(X)$ for some non-empty set X. Then, for any $\rho \in N_{\mathrm{Sym}(X)}(G)$, let $(h)\phi_\rho := \rho^{-1}h\rho$ for all $h \in G$. Note that $\phi_\rho \in \mathrm{Aut}(G)$ (though it is not necessarily in $\mathrm{Inn}(G)$).

Definition 1.1.2. Let A and B be non-empty sets. Then $A \cap B$, the intersection of A and B, is the supremum of sets X such that $X \subseteq A$ and $X \subseteq B$. Moreover, $A \cup B$ (the union of A and B) is the infimum of all sets X such that $A \subseteq X$ and $B \subseteq X$. We will indicate that $A \cap B$ is empty by writing $A \sqcup B$ for the *disjoint union* of A and B.

Some simple observations about $\mathrm{FAlt}(X)$, $\mathrm{FSym}(X)$, and $\mathrm{Sym}(X)$

As with conjugacy in S_n, conjugacy in $\mathrm{Sym}(X)$ preserves cycle type (see Lemma 4.3 in paper 2). Moreover, in $\mathrm{Sym}(X)$, elements are conjugate if and only if they have the same cycle type. Similarly, if X is infinite, elements in $\mathrm{FSym}(X)$ and $\mathrm{FAlt}(X)$ are conjugate if and only if they have the same cycle type (clearly elements in $\mathrm{FAlt}(X)$ with the same cycle type are conjugate in $\mathrm{FSym}(X)$, but we may then introduce a 2-cycle outside of the support of the elements in $\mathrm{FAlt}(X)$ in order to produce a conjugator in $\mathrm{FAlt}(X)$).

Also, $\mathrm{FAlt}(X)$ is centreless for any infinite set X. This follows from the same arguments that (for $n \geqslant 3$) S_n is centreless (for example see the end of the proof of Lemma 3.3.3). From this it also follows that, for any infinite set X, $\mathrm{FAlt}(X)$ is simple i.e. contains no non-trivial proper normal subgroups. We provide quite a hands on proof of this below.

Lemma 1.1.3. *For any infinite set X,* $\mathrm{FAlt}(X)$ *is generated by S, where S is the set of all 3-cycles with support in X.*

Proof. Using S we can produce any element which is a product of two 2-cycles (for example choose $(a_1\ a_2)(a_2\ b_1)$ and $(a_2\ b_1)(b_1\ b_2)$ whose product is $(a_1\ a_2)(b_1\ b_2)$). Now, given an element $\sigma \in \mathrm{FAlt}(X)$, write σ as a product of 2-cycles. By definition this product will consist of an even number of 2-cycles. Now, each pair of 2-cycles will either be: trivial; a 3-cycle; or a product of two 2-cycles. □

Note that, from this lemma, for any infinite set X we have that $|X| = |S| = |\mathrm{FAlt}(X)|$. Moreover $\mathrm{FAlt}(X)$ is an index 2 subgroup of $\mathrm{FSym}(X)$, and so for any infinite set X we also have that $|X| = |\mathrm{FSym}(X)|$.

Lemma 1.1.4. *For any infinite set X,* $\mathrm{FAlt}(X)$ *is simple.*

Proof. Assume that $1 \neq \sigma \in N$, a non-trivial normal subgroup of $\mathrm{FAlt}(X)$. Then $\sigma \in A_n$ where $n \geqslant 5$. But $A_n \cap N \trianglelefteq A_n$, and (since N is non-trivial and A_n is simple for $n \geqslant 5$) we have that $N \cap A_n = A_n$. Thus N contains a 3-cycle and so $N = \mathrm{FAlt}(X)$ by the previous lemma. □

Note that only the cardinality of X determines the structure of $\mathrm{Sym}(X)$, since if there exists a bijection $f : X \to Y$, then this induces an isomorphism between $\mathrm{Sym}(X)$ and $\mathrm{Sym}(Y)$ e.g. $\phi^{(f)} : \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$, $\sigma \mapsto f^{-1}\sigma f$. Moreover $\phi^{(f)}$ induces isomorphisms $\mathrm{FSym}(X) \cong \mathrm{FSym}(Y)$ and $\mathrm{FAlt}(X) \cong \mathrm{FAlt}(Y)$ by restriction.

It is worth remarking on a curiosity which occurs in infinite groups at this stage. Note that $\mathrm{FSym}(\mathbb{N}) \cong \mathrm{FSym}(k\mathbb{N})$ for all $k \in \mathbb{N}$. Thus there is an infinite chain of proper subgroups

$$\mathrm{FSym}(\mathbb{N}) > \mathrm{FSym}(2\mathbb{N}) > \mathrm{FSym}(4\mathbb{N}) > \mathrm{FSym}(8\mathbb{N}) > \dots$$

and each group is isomorphic to $\mathrm{FSym}(\mathbb{N})$. A simpler example of this can be seen using $\mathbb{Z}$ and its subgroups, though this is a torsion free example whilst the FSym example contains only torsion groups. We will see later that these two examples can be combined (see Remark 2.7.2). We now provide two other simple cardinality proofs.

Lemma 1.1.5. *Let X be an infinite set. Then* $\mathrm{Sym}(X)$ *has cardinality* $2^{|X|}$ *(the size of the power set of X).*

Proof. Partition X into X_1 and X_2, so that there is a bijection f between X_1 and X_2. We may then define $\hat{f} \in \mathrm{Sym}(X)$ by $(x)\hat{f} = (x)f$ if $x \in X_1$ and $(x)\hat{f} = (x)f^{-1}$ if $x \in X_2$. Also, since X is infinite, $|X_1| = |X|$. Now, for each subset A of X_1, define $f_A \in \mathrm{Sym}(X)$ to be the element $\hat{f}$ restricted to $A \sqcup (A)f$ so that

$$(x)f_A := \begin{cases} (x)\hat{f} & \text{if } x \in A \sqcup (A)f \\ x & \text{otherwise.} \end{cases}$$

Thus, for each subset of X_1 there is an element of $\mathrm{Sym}(X)$. Hence $\mathrm{Sym}(X)$ has size at least the size of the power set of X_1. For the reverse inclusion, note that

$$|\mathrm{Sym}(X)| \leqslant |X^X| \leqslant |(2^X)^X| = |2^{X\times X}| = |2^X|.$$

In order to see that $|(2^X)^X| = |2^{X\times X}|$, note for any sets A, B, C that $B^{A\times C}$ consists of functions $f(a,c) = b$. By fixing c we may consider these as functions $f_c(a) = b$. We can then think of these as functions from C to B^A. Hence $B^{A\times C}$ is equal to $(B^A)^C$ and they have the same size. □

Lemma 1.1.6. *Let X be an infinite set. Then* $\mathrm{FSym}(X)$ *has* $2^{|X|}$ *subgroups.*

Proof. For any subset A of X, there is a subgroup $\mathrm{FSym}(A)$ of $\mathrm{FSym}(X)$. Now, any group containing λ elements has 2^λ subsets. This therefore bounds the maximum number of subgroups a group may have. □

There has been recent work relating to properties of these groups.

Theorem. [BH15] Let $\kappa < \lambda$ be two infinite cardinals. Then there is no embedding of $\mathrm{FAlt}(\lambda)$ into $\mathrm{Sym}(\kappa)$

Recall that the regular representation of a group G is realised by considering the action of elements of G on the underlying set of G (choosing a right or left action of G provides us with the right or left regular representation of G respectively, but we will always consider right actions). This allows us to see G as a subgroup of $\mathrm{Sym}(G)$. This is the idea for Cayley's Theorem (which applies to infinite groups by using $\mathrm{Sym}(G)$ rather than the finite symmetric groups S_n). Some simple observations are that each non-trivial element $g \in G \leqslant \mathrm{Sym}(G)$ has $\mathrm{supp}(g) = G$ and that if g has order $r \in \mathbb{N}$, then g consists entirely of r-cycles. Such a representation of a group may be much 'larger' than necessary e.g. the regular representation of D_n produces a subgroup of S_{2n} and yet D_n can naturally be seen as a subgroup of S_n.

Proposition. [HO15, 5.13] For every finitely generated infinite group Q, there exists a finitely generated group G such that $\mathrm{FSym}(\mathbb{N}) \lhd G < \mathrm{Sym}(\mathbb{N})$ and $G/\mathrm{FSym}(\mathbb{N}) \cong Q$.

Proof. Let $S_Q := \{q_1, \ldots, q_m\}$ denote a finite generating set for Q and realise Q via its right regular representation Ψ. Let 1 denote the identity element of Q. Computations show that the set $(S_Q)\Psi \cup \{(1\ q_1), (1\ q_2), \ldots, (1\ q_m)\}$ generates a subgroup G of $\mathrm{Sym}(Q)$ containing $(Q)\Psi$ and $\mathrm{FSym}(Q)$. Since conjugation by elements in $\mathrm{Sym}(Q)$ preserves cycle type, $\mathrm{FSym}(Q) \trianglelefteq G$, and since $(Q)\Psi$ only consists of elements with infinite support we have that $(Q)\Psi \cap \mathrm{FSym}(Q) = 1$. The Second Isomorphism Theorem yields the final claim. □

Theorem 1.1.7 ([Sco87] or [DM96])**.** *Let G be equal to* $\mathrm{FSym}(X)$, $\mathrm{FAlt}(X)$, *or* $\mathrm{Sym}(X)$ *where X is an infinite set. Then* $\mathrm{Aut}(G) \cong N_{\mathrm{Sym}(X)}(G) = \mathrm{Sym}(X)$.

In paper 2, Theorem 1.1.7 is generalised to investigate subgroups of $\mathrm{Sym}(X)$ that contain $\mathrm{FAlt}(X)$. A crucial ingredient of this proof can be found in Section 3.3 on page 31.

Proposition. ([Cox16a, Prop. 1]). Let $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$. Then $\mathrm{FAlt}(X)$ is characteristic in G, $\mathrm{Aut}(G) \cong N_{\mathrm{Sym}(X)}(G)$, and G is monolithic.

1.2 Standard group theoretic constructions

We now discuss standard group theoretic constructions to produce a new group from two or more groups. These are the direct product, the semidirect product, and the wreath product. We do this in order to introduce notation and a permutational way of thinking about groups.

Remark. *All group actions will be considered as faithful i.e. if we say that G acts on X, then G can be thought of as a subgroup of* $\mathrm{Sym}(X)$*, or equivalently that there is a monomorphism from G to* $\mathrm{Sym}(X)$*.*

Let A be a non-empty set, and let A^{-1} denote the inverses of A. Then $\langle A \rangle$ is the set consisting of all finite products taking values from A and A^{-1}, or equivalently the smallest subgroup containing the set A. If $\langle A \rangle = G$, then we will say that A *generates* G and that G is *generated by* A. Let $A \subseteq H$. Then the *normal closure* of A, denoted $\langle A \rangle_H$, is the smallest group containing A which is normal in H. Clearly the largest such group is always H. The normaliser of G in H, denoted $N_H(G)$, is the largest subgroup of H in which G is normal. Clearly the smallest subgroup in which G is normal is G itself. The normal closure and normaliser are therefore, in some respect, complimentary notions when considering groups that are normal and lie between G and H.

Direct Products

The first natural way to produce a new group from groups G and H is via the *direct product*. Algebraically this can be seen as the group which takes as its underlying set $G \times H$ and inherits multiplication from G and H separately i.e. if $g, g' \in G$ and $h, h' \in H$, then the multiplication $*$ in $G \times H$ is defined by $(g, h) * (g', h') := (gg', hh')$ where gg' is computed as multiplication in G and hh' is computed as multiplication in H. This construction can also be seen geometrically. Let G act on a set X, H on a set Y, and assume that $X \cap Y$ is empty (this is not restrictive since we may define $X' = X \times \{1\}$ and $Y' := Y \times \{2\}$ so that X' and Y' then have trivial intersection). Then $G \times H$, the direct product of G and H, naturally acts on the set $X \sqcup Y$, where an element $a \in G \times H$ always decomposes into two permutations g, h where $\mathrm{supp}(g) \leqslant X$ and $\mathrm{supp}(h) \leqslant Y$. This allows us to 'see' the permutations g and h as elements of G and H respectively.

Example 1.2.1. Let $n, m \in \mathbb{N}$. We have that S_k naturally acts on k objects, for example the elements of the set $\mathbb{Z}_k$. Then $S_n \times S_m$ can be thought of as a subgroup of S_{n+m}. Let $\sigma \in S_{n+m}$ be written in disjoint cycle notation. Then $\sigma \in S_n \times S_m$ if and only if each cycle of σ has support in either $\{1, \ldots, n\}$ or $\{n+1, \ldots, n+m\}$. We may therefore write σ uniquely as a product of two permutations, one consisting of all of the cycles of σ with support contained in $\{1, \ldots, n\}$ which we will denote by α, and one consisting of all of the cycles of σ with support contained in $\{n+1, \ldots, n+m\}$ which we will denote by β. It is then clear that α and β commute: by construction these permutations have disjoint supports.

We can also combine finitely many groups using the direct product. If $G_1, G_2, \ldots, G_n$ are groups, then $H := G_1 \times G_2 \times \ldots \times G_n$ is the *direct product of the* G_i. When dealing with infinitely many groups, there is a choice to make. Let $\{G_i \mid i \in \mathbb{N}\}$ be an infinite family of non-trivial groups. For example we could set $G_i := C_2$ for all $i \in \mathbb{N}$. For each $i \in \mathbb{N}$, let $S^{(i)}$ denote a generating set for G_i. Now $\bigoplus_{i \in \mathbb{N}} G_i$ is the direct sum of the G_i and is generated by $\bigsqcup_{i \in \mathbb{N}} S^{(i)}$, the union of all of the generating sets of the G_i. The direct product of the G_i, denoted $\prod_{i \in \mathbb{N}} G_i$, consists of elements of the form $\prod_{k \in A} g_k$ where $A \subseteq \mathbb{N}$ and $g_k \in G_k$ for each $k \in A$. One way to therefore visualise elements of the direct product is that each element is a sequence which takes its i^{th} term from G_i. The direct sum can then be seen as the subgroup of the direct product consisting of all elements which can be written using a sequence containing only finitely many non-trivial elements. From this reasoning it can be seen that if G_0 is trivial, then

$$\bigoplus_{i \geqslant 0} G_i \cong \bigoplus_{i \in \mathbb{N}} G_i \text{ and } \prod_{i \geqslant 0} G_i \cong \prod_{i \in \mathbb{N}} G_i.$$

If all of the G_i are countable, then the direct sum of them is countable (we have given a countable generating set above) whilst the direct product will be uncountable. This can be observed since $|G_i| \geqslant 2$ for all $i \in \mathbb{N}$ and so this direct product has size at least equal to a direct product of infinitely many C_2's. Now, each element $g \in \prod_{i \in \mathbb{N}} C_2$ can be thought of as a subset A of $\mathbb{N}$ where $n \in A$ if and only if g has a non-trivial factor in the n^{th} C_2. Hence the elements of this group are in bijection with the power set of $\mathbb{N}$, and hence the product is uncountable. Also note that the proof of Lemma 1.1.5 was essentially showing that $\mathrm{Sym}(X)$ contains an infinite direct product of C_2's.

Note that $\bigoplus_{i \in \mathbb{N}} C_2$ and $\prod_{i \in \mathbb{N}} C_2$ can naturally be seen to be subgroups of $\mathrm{Sym}(X)$ where $X = \{1, 2\} \times \mathbb{N}$ and the n^{th} C_2 moves only the points $(1, n)$ and $(2, n)$.

Semidirect Products

A semidirect product $G \rtimes_\psi H$ can be thought of as a generalisation of a direct product of G and H where the 'interaction' between G and H is given by H acting via automorphisms of G. Moreover, if $h, h' \in H$ induce automorphisms ϕ and ϕ' respectively, we require that

hh' induces the automorphism $\phi \circ \phi'$, i.e. there is a homomorphism ψ from H to $\mathrm{Aut}(G)$. For each generator $h \in H$, let $\psi_{(h)}$ denote the automorphism induced by conjugation by h. In the case where $\psi_{(h)}$ is the identity for all h, we will obtain the direct product. The semidirect product $G \rtimes_\psi H$ can also be thought of as the set $G \times H$ with multiplication $(g, h)(g', h') := (g(g')\psi_{(h^{-1})}, hh')$.

In some cases this automorphism can be realised via a permutation of the underlying set which G acts on. For example in $D_n := C_n \rtimes_\psi C_2$, the dihedral group of order $2n$, where ψ sends the non-trivial element of C_2 to $\phi : C_n \to C_n$, $a \mapsto a^{-1}$. Note that G must be normal in the group $G \rtimes_\psi H$, since conjugation by elements of H sends every element of G to an element in G.

Example 1.2.2. The group D_∞ is defined by extending the definition of D_n to use the infinite cyclic group. We will define it to be the subgroup of $\mathrm{Sym}(\mathbb{Z})$ which is generated by two permutations. The 'translation' in this case is the most natural one to define on $\mathbb{Z}$, the permutation $t : \mathbb{Z} \to \mathbb{Z}$, $z \mapsto z + 1$. The reflection is given by the permutation $s : \mathbb{Z} \to \mathbb{Z}$, $z \mapsto -z$. This produces the group $\mathbb{Z} \rtimes_\psi C_2$, where ψ sends the non-trivial element of C_2 to the non-trivial automorphism of $\mathbb{Z}$. In this case omitting the definition of ψ is not ambiguous: $\mathbb{Z}$ has only one non-trivial automorphism, and so if we wished to use the trivial automorphism we would write $\mathbb{Z} \times C_2$.

With this example the automorphism is in $N_{\mathrm{Sym}(\mathbb{Z})}(\langle t \rangle)$. It may be for a particular action that the automorphism is not realisable in this way, for example by viewing $\mathbb{Z}^2 \leqslant \mathrm{Sym}(\{1, 2\} \times \mathbb{Z})$ with one generator translating only $\{(1, z) : z \in \mathbb{Z}\}$ and the other generator translating only $\{(2, z) : z \in \mathbb{Z}\}$. One of the first aims of paper 2 was to show that if $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$, then $N_{\mathrm{Sym}(X)}(G) \cong_\Psi \mathrm{Aut}(G)$ where $\Psi : g \mapsto \phi_g$.

Example 1.2.3. Let us consider $\mathrm{FSym}(\mathbb{Z})$. Conjugation by any element of $\mathrm{Sym}(\mathbb{Z}) \setminus \mathrm{FSym}(\mathbb{Z})$ induces an outer automorphism of $\mathrm{FSym}(\mathbb{Z})$. Thus, if $H < \mathrm{Sym}(\mathbb{Z})$ with $H \cap \mathrm{FSym}(\mathbb{Z}) = 1$, $\langle \mathrm{FSym}(\mathbb{Z}), H \rangle$ is in fact the semidirect product $\mathrm{FSym}(\mathbb{Z}) \rtimes H$, where the automorphisms are provided by the action of the elements of H on the set $\mathbb{Z}$. The second Houghton group H_2 is given by choosing $H := \langle t \rangle$, where t sends z to $z+1$ for all $z \in \mathbb{Z}$. For any $n \geqslant 3$, the Houghton group H_n is not a semidirect product in this way.

One way to construct a group $H < \mathrm{Sym}(X) \setminus \mathrm{FSym}(X)$ is as follows. Let $\hat{H} \leqslant \mathrm{Sym}(H)$ denote the right regular representation of H i.e. the one obtained by defining $\hat{H}$ to act on the set H via the multiplication defined on H. As with the previous example we may then produce $\langle \hat{H}, \mathrm{FSym}(H) \rangle$ which is equal to the semidirect product $\mathrm{FSym}(H) \rtimes \hat{H}$.

Generalising semidirect products

Just as the semidirect product was a generalisation of the direct product, the constructions of the previous two sections are examples of group extensions. These are naturally described via short exact sequences.

Definition 1.2.4. Let $G_1, \ldots, G_n$ be groups. Then

$$G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \ldots \xrightarrow{\phi_{n-1}} G_n$$

is an *exact sequence of groups* if, for each $i \in \mathbb{Z}_{n-2}$, the image of ϕ_i is equal to the kernel of ϕ_{i+1}. Moreover a *short exact sequence of groups* is an exact sequence of groups of the form

$$1 \xrightarrow{\phi_1} N \xrightarrow{\phi_2} G \xrightarrow{\phi_3} Q \xrightarrow{\phi_4} 1. \tag{1}$$

Immediate consequences of the definition of a short exact sequence are that ϕ_2 must be a monomorphism and that ϕ_3 must be an epimorphism. I thank Ana Khukhro, currently at the University of Neuchâtel, for providing the following clear (non semidirect product) example.

Example. Consider the sequence

$$1 \longrightarrow 2\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

which can be seen to be exact (so that $\mathbb{Z}$ is an extension of $2\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$). This cannot be a semidirect product since $\mathbb{Z}$ does not contain torsion: all of its non-trivial elements have infinite order.

The following helps us to decide which group extensions are semidirect products.

Lemma 1.2.5. *A group G is a semidirect product of Q and N if and only if there is a group extension of the form (1) above where ϕ_3 splits (meaning there is a homomorphism $f : Q \to G$ such that $(q)f\phi_3 = q$ for all $q \in Q$).*

Proof. Consider if ϕ_3 splits. Let $N_G := (N)\phi_2$ and let $Q_G := (Q)f$ so that $N_G \trianglelefteq G$ and $Q_G \leqslant G$. Now, if $n \in N_G$ then $(n)\phi_3 = 1$, and so $n \notin Q_G \setminus \{1\}$ i.e. $N_G \cap Q_G = \{1\}$. If $g \in G$ then $(g)\phi_3 \in Q$ and $(g)\phi_3 f = q \in Q_G$. So take $gq^{-1} \in \ker(\phi_3)$. Then $gq^{-1} = n \in N_G$ and so $g = nq$. This means that $G = N_G Q_G$, and so G is a semidirect product of Q and N as required.

Conversely, let $(N)\phi_2 := N_G$ and consider if ϕ_3 does not split. Then there is no monomorphism Ψ from Q to G such that $(Q)\Psi \cap N_G = \{1\}$, and so the short exact sequence does not provide a semidirect decomposition for G. □

Example. Let X be an infinite set and consider the sequence

$$1 \longrightarrow \mathrm{FAlt}(X) \longrightarrow \mathrm{FSym}(X) \xrightarrow{\phi} C_2 \longrightarrow 1.$$

Here the C_2 can be visualised as a two cycle lying in $\mathrm{FSym}(X)$. This immediately yields a splitting for ϕ, making this a semidirect product.

Example. Consider the sequence

$$1 \longrightarrow \mathbb{Z} \times C_2 \longrightarrow \mathbb{Z} \rtimes C_4 \xrightarrow{\phi} C_2 \longrightarrow 1$$

where $\mathbb{Z} \rtimes C_4$ is not a direct product. If we merely require the maps to be an epimorphism and monomorphism, then the sequence may not be exact. Let $\{a, t\}$ denote a generating set for $\mathbb{Z} \rtimes C_4$ where t generates $\mathbb{Z}$ and a generates C_4 (which acts on $\mathbb{Z}$ via the automorphism $t \mapsto t^{-1}$). In order to be exact we must then have that $\mathbb{Z} \times C_2$ is generated by a^2 and t and that ϕ sends a to x, the non-trivial element of C_2. For this map to be split we would then need there to be a map $f : C_2 \to \mathbb{Z} \rtimes C_4$ such that either $f : x \mapsto a$ or $f : x \mapsto a^3$. But for f to be a homomorphism f must then send $x \cdot x$ to a^2 but also $x \cdot x = 1$ so $(x^2)f = 1$. Thus this is not a split extension.

Example. Let $n \geqslant 3$ and consider H_n, the n^{th} Houghton group. These are defined on page 25 and fit into the short exact sequence

$$1 \longrightarrow \mathrm{FSym}(X_n) \longrightarrow H_n \xrightarrow{\pi} \mathbb{Z}^{n-1} \longrightarrow 1$$

where $\pi : g \mapsto (t_1(g), t_2(g), \ldots, t_{n-1}(g))$. At first glance it may be thought that $e_i \mapsto g_i$ for all $i \in \mathbb{Z}_{n-1}$ is a splitting for this map (where $\{e_i\}_{i=1}^{n-1}$ denote the standard basis for $\mathbb{Z}^{n-1}$). However this cannot be a homomorphism since $g_2g_3 \neq g_3g_2$. There is no splitting of π since $\lfloor n/2 \rfloor$ is the largest possible rank of any free abelian subgroup of H_n. This can be seen since, in order for elements to commute in $\mathrm{Sym}(X_n)$, they must either: have disjoint supports; or where their supports intersect they must induce the same permutation of X_n; or one must induce a permutation of the orbits of the other. This means that, for any $n \geqslant 3$, there cannot be a monomorphism from $\mathbb{Z}^{n-1}$ to H_n.

Wreath Products

A permutational wreath product, as the name suggests, can naturally be seen as a permutation group. We first provide an algebraic definition.

Definition. Let G and H be groups and let H act on a set X. Then the *unrestricted permutational wreath product* of G and H with respect to X has elements which come in pairs. One entry is an element $h \in H$ and the other entry is a function $f : X \to G$. Let B' be the set of all such functions. If $f_1, f_2 \in B'$, then $(f_1 \times f_2)(x) := f_1(x) \cdot f_2(x)$ for all $x \in X$, where $\cdot$ denotes the binary operation of G. Moreover if $h \in H$ then $h^{-1}(f(x))h := f(xh^{-1})$ for all $x \in X$. This is the semidirect product $B' \rtimes H$, where H acts by permuting the entries of functions in B'. The *restricted permutational wreath product*, denoted $G \wr_X H$, is defined analogously as the semidirect product $B \rtimes H$ where

H is the *head* of $G \wr_X H$ and where B, the *base* of $G \wr H$, is the subgroup of B' consisting of functions with finite support i.e. functions $f \in B'$ such that $\{x \in X : f(x) \neq 1\}$ is finite.

Given groups G and H where H acts on a set X, $G \wr_X H$ can also be defined from a permutational perspective. For each $x \in X$, let $G := G_x$ as sets, and make G_x a group by inheriting the same multiplication from G. The base of $G \wr_X H$ is then given by $B := \bigoplus_{x \in X} G_x$. We may also consider an infinite product of G_x to produce the unrestricted permutational wreath product of G and H (so that if G is non-trivial then B' will be uncountable). Note that any permutation of the factors G_x will be an automorphism of B. To be more specific, for any element $g \in G$ and any $x \in X$, let g_x denote the element of G_x within B which produces the same permutation on G_x as g does on G. For any $b \in B$, there exist $g^{(1)}, \ldots, g^{(n)} \in G$ and $x_1, \ldots, x_n \in X$, such that $b := \prod_{i=1}^n g_{x_i}^{(i)}$. For any $\sigma \in \mathrm{Sym}(X)$, we have an automorphism ϕ_σ of B, defined by

$$(b)\phi_\sigma := \prod_{i=1}^{n} g_{(x_i)\sigma}^{(i)}.$$

Now, since $H \leqslant \mathrm{Sym}(X)$, we may impose that H induces these automorphisms of B via conjugation, producing

$$\bigoplus_{x \in X} G_x \rtimes H =: G \wr_X H.$$

A wreath product is the result of this construction using the regular action for H i.e. the group $G \wr_H H$ where H acts on itself by multiplication on the right. Since we will only use permutational wreath products within this work and the set that H acts on should be clear, we will often suppress the set X from the notation and simply write $G \wr H$ to denote the permutational wreath product of G and H over the set X.

Example 1.2.6 (Finite symmetric groups)**.** Let $n, m \in \mathbb{N}$. Just as $S_n \times S_m$ naturally acts on $n + m$ objects, the permutational wreath product $S_n \wr S_m$ naturally acts on nm objects. To be more specific, for each $i \in \mathbb{Z}_m$, let $Y_i := \{(i, 1), \ldots, (i, n)\}$. We will work with with permutations with support contained within

$$\bigsqcup_{s=1}^{m} Y_s.$$

Let us describe four permutations that generate $S_n \wr S_m$. Let $\alpha_1 := ((1, 1)\ (1, 2))$ and $\alpha_2 := ((1, 1)\ (1, 2)\ \ldots\ (1, n))$. Note that α_1 and α_2 generate a copy of S_n as a subgroup of S_{nm} (acting on Y_1). Now, let

$$\beta_1 := \prod_{k=1}^{n} ((1, k)\ (2, k)) \text{ and } \beta_2 := \prod_{k=1}^{n} ((1, k)\ (2, k)\ \ldots\ (m, k))$$

where β_1 and β_2 can be seen to generate a copy of S_m which permutes the m sets $Y_1, \ldots, Y_m$. As was mentioned within the definition of wreath products,

$$S_n \wr S_m \cong \left(\bigoplus_{i=1}^{m} S_n \right) \rtimes S_m$$

where the automorphisms are given by the above action i.e. how S_m permutes the m sets $\{Y_i \mid i \in \mathbb{Z}_m\}$.

We now introduce the groups studied in paper 3, which also happen to be natural examples of infinite groups constructed via the wreath product. Note that for groups of the form $G \wr H$ where H is cyclic, the regular action corresponds to the 'natural' permutation action and so such groups can be thought of as permutational wreath products or as wreath products.

Example 1.2.7 (The Lamplighter group $C_2 \wr \mathbb{Z}$)**.** The base of this group is $\bigoplus_{\mathbb{Z}} C_2 =: B$. One can consider this as a bi-infinite street (the real line) with a streetlamp located at every integer point. When dealing with the restricted wreath product we have that any group element may only 'light' finitely many lamps. If a_k denotes the generator of C_2 which 'turns on' the k^{th} lamp, then $\{a_i \mid i \in \mathbb{Z}\}$ is a generating set for B. We may then introduce an action of $\mathbb{Z} = \langle t \rangle$ on B by imposing that conjugation by t induces the automorphism $a_k \mapsto a_{k+1}$ for all $k \in \mathbb{Z}$. A suitable generating set for $C_2 \wr \mathbb{Z}$ is therefore $\{a_0, t\}$. This generating set is frequently encountered within the literature. The action of $\mathbb{Z}$ is often thought of as a 'lamplighter' who moves to light different lamps. From a permutational viewpoint, the action of $\mathbb{Z}$ can be thought of as a 'shift' or translation of $\mathbb{Z}$ which allows any finite collection of lamps to be lit using only a_0 (or a_k for any $k \in \mathbb{Z}$, since $\{a_k, t\}$ is also a generating set for $C_2 \wr \mathbb{Z}$ for any $k \in \mathbb{Z}$).

This group has been given much attention, for example see [LPP96] and [Par92] where random walks and growth of such groups have been studied. These concepts will be described in Section 4. Also dead end and seesaw elements for these groups have been investigated, see [CT05].

Example 1.2.8 (Lamplighter groups)**.** In a similar way, we can consider $C \wr \mathbb{Z}$ where C is a cyclic group. If C is finite, the base of this group can be thought of as lamps with a discrete number of different settings e.g. for C_4, we could think of the possible 'states' of each lamp to be 'off', 'low', 'medium', and 'high'. In the case where C is infinite, one can think of each lamp as having an associated 'voltage' (which can take any value in $\mathbb{Z}$). A presentation for the group $C \wr \mathbb{Z}$ where $|C| = n$ is therefore

$$\langle a, t \mid a^n = 1; [t^{-i}at^i, t^{-j}at^j] = 1 \text{ for all } i \neq j \rangle.$$

Moreover if G has presentation $\langle S_G \mid R_G \rangle$, then

$$G \wr \mathbb{Z} = \langle S_G, t \mid R_G; [t^{-i}gt^i, t^{-j}ht^j] = 1 \text{ for all } i \neq j \text{ and for all } g, h \in S_G \rangle.$$

Example 1.2.9. Consider $\mathbb{Z} \wr C_n$. This is equal to $\mathbb{Z}^n \rtimes_\psi C_n$, where the automorphisms of $\mathbb{Z}^n$ relate to cyclically permuting the n copies of $\mathbb{Z}$. Similarly, S_n acts on the n point set $\{1, \ldots, n\} =: Y$, and so the permutational wreath product $\mathbb{Z} \wr_Y S_n$ is equal to $\mathbb{Z}^n \rtimes_\psi S_n$, where S_n acts by permuting the n copies of $\mathbb{Z}$.

1.3 Results regarding finite index subgroups

Let H be a subgroup of G. We say that H has *finite index* in G if and only if there exist $a_1, \ldots, a_n \in G$ such that, as sets, $G = Ha_1 \sqcup Ha_2 \sqcup \ldots \sqcup Ha_n$. We may then say that H has index n in G, and denote this by $[G : H] = n$. Note that, by definition, $Ha_i \neq Ha_j$ for all distinct i and j in $\mathbb{Z}_n$. If H is not a finite index subgroup of G, then we say that H has *infinite index* in G.

Notation. Let $H \leqslant_f G$ denote that H is a finite index subgroup of G and let $H \leqslant_n G$ denote that H has index n in G.

Remark. *Although index is often studied as part of an undergraduate course, the concept of finite index can be missed since it has little relevance to finite group theory. It is for this reason that we discuss some elementary results. The structure of these results came about from discussions with Hector Durham, a fellow PhD student at the University of Southampton.*

Lemma 1.3.1. *If $K \leqslant_f G$, then there exists $N \trianglelefteq_f G$ (normal and finite index in G) such that $N \leqslant K$.*

Proof. Let K have index n in G and let $N := \bigcap_{g \in G}(g^{-1}Kg)$. Then G acts on $K \backslash G$ by right multiplication, and so there is a homomorphism $\phi : G \to S_n$. Now $h \in \ker(\phi)$ if,

$$\begin{aligned} Kgh &= Kg \text{ for all } g \in G \\ \Leftrightarrow ghg^{-1} &\in K \text{ for all } g \in G \\ \Leftrightarrow h &\in g^{-1}Kg \text{ for all } g \in G. \end{aligned}$$

Hence $\ker(\phi) = N$ and N is normal. Moreover $G / \ker(\phi) \cong \operatorname{Im}(\phi) \leqslant S_n$, and so N has index m in G where $m \leqslant n!$ and m divides $n!$. □

Lemma 1.3.2. *If G is finitely generated then there exist only finitely many $K \leqslant G$ of any given index.*

Proof. Suppose $H \leqslant_n G$. Right multiplication by G on $H \backslash G$ gives a homomorphism $\phi_H : G \to S_n$. Note that $\operatorname{Stab}(H) = H$ since $g \in \operatorname{Stab}(H) \Leftrightarrow Hg = H$. Thus, by choosing $1 \in \mathbb{Z}_n$ to correspond to the coset H in $H\backslash G$, the preimage of Stab(1) in S_n is H. Hence $H = H' \Leftrightarrow \phi_H = \phi_{H'}$.

$$\text{But } G \text{ finitely generated } \Rightarrow \exists \text{ only finitely many homomorphisms } G \to S_n$$

(there are $(n!)^{|S|}$ maps from S to S_n) and so there can only be finitely many index n subgroups. □

Lemma 1.3.3 (Poincaré)**.** *Let $H \leqslant_f G$ and $K \leqslant_f G$. Then $H \cap K \leqslant_f G$.*

Proof. We use the map (from cosets of $H \cap K$ in G to cosets of $H \times K$ in $G \times G$) defined by $(H \cap K)a \mapsto (Ha, Ka)$. Our aims are to show that this map is well defined and injective. In order to show it is well defined, consider if b were used as a coset representative rather than a. Then $b = ag$ where $g \in H \cap K$. Hence $g \in H$ and $g \in K$. Thus $(Hb, Kb) = (Ha, Ka)$, and so changing the representative does not change the map. In order to show injectivity, consider if $(Ha, Ka) = (Hb, Kb)$. Then $ab^{-1} \in H \cap K$ and so $(H \cap K)a = (H \cap K)b$. Moreover, this means that $[G : H \cap K] \leqslant [G : H][G : K]$. □

Lemma 1.3.4. *If $H \leqslant_n G$ and G is finitely generated, then there exists a $K \leqslant_f H$ which is characteristic in G.*

Proof. Recall that a finite index normal subgroup of G can be constructed by $\bigcap_{g \in G} g^{-1}Hg$ i.e. $\bigcap_{g \in G}(H)\phi_g$. Including all automorphisms will produce a characteristic subgroup. Let

$$K := \bigcap_{\phi \in \mathrm{Aut}(G)} (H)\phi \tag{2}$$

and note that, for any $\phi \in \mathrm{Aut}(G)$, $(H)\phi \leqslant_n G$. By Lemma 1.3.2, there are only finitely many possible images for H in (2), and so, by Lemma 1.3.3, K is finite index in G. Finally, K is characteristic in G since the image of K under $\psi \in \mathrm{Aut}(G)$ is contained within

$$\bigcap_{\phi \in \mathrm{Aut}(G)} ((H)\phi\psi)$$

which is equal to K. □

We now prove a result for interest, which can be found, amongst other places, in [Fen14].

Lemma 1.3.5. *Let $H \leqslant_n G$ and $K \leqslant G$. Then $H \cap K \leqslant_f K$.*

Proof. By definition we have that $G = Ha_1 \sqcup Ha_2 \sqcup \ldots \sqcup Ha_n$. Let us only keep those a_i such that

$$Ha_i \cap K \neq \emptyset. \tag{3}$$

Thus, after a renumbering, we have that $K = (Ha_1 \cap K) \sqcup (Ha_2 \cap K) \sqcup \ldots \sqcup (Ha_m \cap K)$. From (3), we have for each $i \in \mathbb{Z}_m$ that there exists a $b_i \in Ha_i \cap K$ and so we may replace each a_i with some $b_i \in K$ (so that $Ha_i \cap K = Hb_i \cap K$ for each $i \in \mathbb{Z}_m$). Now $Hb_i \cap K = Hb_i \cap Kb_i = (H \cap K)b_i$ and so

$$K = (H \cap K)b_1 \sqcup (H \cap K)b_2 \sqcup \ldots \sqcup (H \cap K)b_m.$$

Thus $H \cap K \leqslant_f K$ and $[K : H \cap K] \leqslant [G : H]$. □

We may also draw a simple conclusion from this lemma.

Lemma 1.3.6. *If $N \trianglelefteq G$ where N is simple and infinite, then any finite index subgroup of G must contain N.*

Proof. Using N as the subgroup K in the previous lemma, we have, for any $H \leqslant_f G$, that $H \cap N$ is of finite index in N. By Lemma 1.3.1 we have that there must be a normal finite index subgroup of N in $H \cap N$. But since N is infinite and simple, the only finite index normal subgroup of N is N itself, and so $H \cap N$ must be equal to N. □

2 Background for Paper 1

This section is about the construction of algorithms to answer questions about groups or classes of groups.

2.1 Free groups

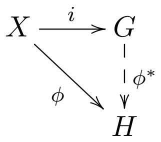
Let X be a non-empty set. Then a *word* in X is an ordered n-tuple $a_1 a_2 \ldots a_n$ where $a_1, \ldots, a_n \in X \cup X^{-1} =: X^{\pm 1}$. A word is then *reduced* if it contains no subword of the form xx^{-1} or $x^{-1}x$ where $x \in X$. Since all of our words are finite, we can always delete such pairs from our word in order to produce a reduced word. We will now define the free group on X, which we denote by $F(X)$. The underlying set of $F(X)$ is the set of all reduced words on X, and the group operation on $F(X)$ is concatenation of words with cancellation i.e. if $a_1 \ldots a_n$ and $b_1 \ldots b_m$ are words on X, then their product is the result of reducing $a_1 \ldots a_n b_1 \ldots b_m$ (where it may be that $a_1 \ldots a_n b_1 \ldots b_m$ is a reduced word). The identity is therefore the empty word and inverses can then be computed. The operation is also associative.

Example. If $|X| = 1$, then $F(X) \cong \mathbb{Z}$.

A common form to present the information of a group G is a *group presentation*. This involves two pieces of information, S and R, where S denotes the set of generators of G and R denotes the set of relations of G. We may then write $G = \langle S \mid R \rangle$ to mean that G is the group generated by S subject to the relations R. Formally, G is the quotient of the free group generated by S and the normal closure of the set R. If R is empty then we say that G is *free on S*. Free groups have the following *universal property*.

Let G be a group with generating set X (so that there is an injective map $i : X \to G$). Then G is free on X if and only if the following universal property holds:

every map ϕ from X into a group H extends into a unique homomorphism ϕ^* from G to H so that the diagram below commutes.



This means that we may talk about *the* free group on X, since all groups which are free on X are isomorphic (since any two satisfy the universal property and so there are injective homomorphisms between them). This leads to the common terminology that, if $|X| = n$, then $F(X)$ is *the free group of rank n.*

Lemma 2.1.1. *Let X and Y be non-empty sets. Then $F(X) \cong F(Y)$ if and only if $|X| = |Y|$.*

Proof. If $|X| = |Y|$ then this immediately yields the isomorphism. For the other direction we follow [Bog08, Thm. 3.8 & Cor. 3.11]. Let $\mathbb{Z}_2 := \{0, 1\}$ and for any non-empty set Z let H_Z consist of all functions $f : Z \to \mathbb{Z}_2$ such that the preimage of 1 is a finite set. Given $f, g \in H_Z$, let $(f + g)(z) := f(z) + g(z) \pmod 2$ for all $z \in Z$. Note that $H_Z \cong \bigoplus_{z \in Z} C_2$. For any $m \in Z$, let $f_m \in H_Z$ be defined by

$$f_m(z) := \begin{cases} 1 & \text{if } z = m \\ 0 & \text{otherwise} \end{cases}$$

so that $\{f_z : z \in Z\}$ corresponds to our standard generating set for $\bigoplus_{z \in Z} C_2$. Now note that $\{f_z : z \in Z\}$ corresponds to a basis for H_Z when thinking of H_Z as a vector space over $\mathbb{F}_2$. Importantly the rank of a vector space over a field is well defined i.e. the size of the basis completely determines the vector space up to isomorphism. Moreover the map $Z \to H_Z$, $z \mapsto f_z$ can be extended to an epimorphism $\Psi_Z : F(Z) \to H_Z$. Now, if $\phi : F(X) \to F(Y)$ is an isomorphism, then $((X)\phi)\Psi_Y$ generates H_Y. This is because

$$\langle X \rangle = F(X) \Rightarrow \langle (X)\phi \rangle = F(Y) \Rightarrow (\langle (X)\phi \rangle)\Psi_Y = \langle ((X)\phi)\Psi_Y \rangle = H_Y$$

and so $|X| \geqslant |Y|$. Running the argument with ϕ^{-1} then yields that $|Y| \geqslant |X|$. $\square$

One way to think about the universal property is as follows. Consider all groups which can be generated by a set X. We could consider a partial order $\prec$ on all such groups, which is produced by $G = \langle X \mid S \rangle \succ \langle X \mid S' \rangle = G'$ if and only if there is a set T such that $G' = \langle X \mid S \sqcup T \rangle$ (intuitively the size of the set of relators dictates the number of equations which the generators in the presentation satisfy). With this ordering, the free group on X is maximal, whilst the trivial group is minimal. In some sense the universal property captures the free group on X being maximal (since it surjects onto any other group generated by X).

Example. Again we consider $|X| = 1$. In this case all groups generated by X will be cyclic, and there will be a group between C_n and the trivial group if and only if n is composite i.e. not prime. Moreover, from the universal property, $\mathbb{Z}$ is comparable with all other groups generated by X (indeed, it is greater than them all).

For what follows, we usually place restrictions on $G = \langle S \mid R\rangle$ through conditions on S and R. In order to work with Turing machines we require our inputs to be recursive and so will nearly always consider recursively presented groups (see Definition 2.4.4). Often this is achieved by S and R being finite. If there exists a finite set S such that $G = \langle S \mid R\rangle$ we say that G is *finitely generated* and if R is finite then we say that G is *finitely related*. If G is finitely generated and finitely related then we say that G is *finitely presented*.

2.2 Decision Problems

In 1911, Max Dehn (a student of David Hilbert) asked three questions regarding presentations of a group. As with many topics studied within group theory, they have an underlying topological flavour which we will discuss on the next page.

1) The word problem: given a group presentation $\langle S \mid R\rangle$, can one determine whether any two words $a_1 \dots a_n$ and $b_1 \dots b_m$ (where $a_1, \dots, a_n, b_1, \dots b_m \in S^{\pm 1}$) represent the same group element? Equivalently, does $a_1 \dots a_n(b_1 \dots b_m)^{-1}$ represent the identity element in G?

2) The conjugacy problem: given a group presentation $\langle S \mid R\rangle$ and two words $a_1 \dots a_n$ and $b_1 \dots b_m$ (where $a_1, \dots, a_n, b_1, \dots, b_m \in S^{\pm 1}$) can one determine whether, as elements of G, $a_1 \dots a_n$ and $b_1 \dots b_m$ are conjugate in G?

3) The isomorphism problem: given group presentations $G := \langle S \mid R\rangle$ and $\tilde{G} := \langle \tilde{S} \mid \tilde{R}\rangle$, can one determine whether G and $\tilde{G}$ are isomorphic?

Throughout we will denote the word problem for G by $\mathrm{WP}(G)$ and the conjugacy problem for G by $\mathrm{CP}(G)$. Note that if $\mathrm{CP}(G)$ can be solved, a solution for $\mathrm{WP}(G)$ is obtained since $\{1\}$ is its own conjugacy class.

At the time of phrasing the questions, "can one determine" was presumably via human computation and thought. The questions were given more mathematical formalism by Turing's work on decidability. The modern interpretation of Dehn's questions is given by replacing "can one determine" with "is it Turing decidable". To be Turing decidable a question must involve inputs A which must be recursive (and so countable) so that there is a Turing Machine which, for any input A, answers the question correctly by outputting information B (which again must be recursive). Thus by phrasing Dehn's problems in this way they only apply to recursively presented groups. Importantly we then obtain that, if any of these problems has a solution for one finite presentation, then for any other finite presentation there exists a Turing machine to solve the problem (this can be achieved by using Tietze transformations, see, for example, [LS01, Chp. 2]). This means that one can work with one fixed finite presentation in order to solve these problems for a given group. In order for a group to have unsolvable word or conjugacy problem, it is therefore sensible to impose that G is finitely presented: it will then have unsolvable word or conjugacy problem for all finite presentations. Throughout this thesis we will use the modern interpretation of Dehn's questions, though we will not provide an introduction to Turing machines, choosing rather to treat them as a black box. Both [Rot95] and [Coo04] provide details for the interested reader.

Every space has a group associated to it by the π_1 functor. In this topological framework the three questions above can be thought of as asking if one can decide whether:

1) a loop in the space is contractible;
2) two loops in the space are freely homotopic;
3) two spaces have non-isomorphic fundamental group (implying that they are not homotopy equivalent).

These questions seem reasonable both from their group theoretic and topological phrasing; however answering the word problem in the negative for semigroups was achieved in [Mar47] and [Pos47]. It was some time later before the word problem was answered in the negative for a finitely presented group in [Nov55] and [Boo59]. A general solution to the word problem (one which takes any input for S and R) even for finitely presented groups is therefore impossible (and so this means that a general solution to the strictly harder conjugacy problem is also impossible). A general solution to the isomorphism problem is also impossible. This was achieved in [Ady55] and [Rab58] by showing that for any Markov property $\mathcal{P}$, there is no Turing machine which, on input of any finite presentation, decides whether the group produced satisfies $\mathcal{P}$. A property $\mathcal{P}$ is Markov if and only if there is a finitely presented group G_+ satisfying $\mathcal{P}$ and a finitely presented group G_- such that for any finitely presented group H with $G_- \hookrightarrow H$, H does not satisfy $\mathcal{P}$. Since the property of 'being the trivial group' is Markov, there can be no Turing machine which decides whether a group presentation represents the trivial group. This problem is clearly as difficult as the isomorphism problem. But there are groups where these problems can be solved. Therefore much research has been conducted in order to find classes of groups for which these problems are decidable. One such class where all three problems are solvable is hyperbolic groups. This means that there exists an algorithm which, given a group presentation which is known to produce a hyperbolic group, the algorithm can decide whether any two words given with respect to this presentation are equal and whether they are conjugate. Moreover there is an algorithm (see [DG11]) which, given any two presentations which are known to produce hyperbolic groups, decides whether the two groups are isomorphic. Since being posed by Dehn, many more questions regarding presentations of groups have been posed, and these are generally known as *decision problems*. Examples of these can be found at the beginning of the first paper within this thesis (on page 51). For a more detailed introduction to decision problems, see [Mil92].

2.3 A partial solution to the word problem

It is worth noting that one part of the word problem and conjugacy problem can always be solved (for recursively presented groups). Let $G = \langle S \mid R \rangle$ be a recursive presentation.

Now enumerate

$$\mathrm{Id}(S,R) := \left\{ \prod_{k=1}^{s} (w_k^{-1} r_{i_k} w_k) \mid s \in \mathbb{N};\ r_{i_1}, \ldots, r_{i_s} \in R^{\pm 1};\ w_1, \ldots, w_s \text{ words in } S \right\}.$$

We therefore have that $\mathrm{Id}(S,R)$ consists of all words in $\langle S \mid R \rangle$ which represent the identity. Let $a_1 \ldots a_d$ be a word with respect to the presentation $\langle S \mid R \rangle$. We may assume this word is reduced (that $a_i a_{i+1} \neq 1$ for any $i \in \mathbb{Z}_{n-1}$) since the word has finite length. Hence, if $a_1 \ldots a_d$ represents the identity in G, then $a_1 \ldots a_d$ will appear as an element of $\mathrm{Id}(S,R)$. Since we may enumerate the elements of $\mathrm{Id}(S,R)$, we may therefore decide which elements of $\langle S \mid R \rangle$ represent the identity. Note however that this does not mean that we can decide which elements do not represent the identity. We now provide examples where this other 'half' of the word problem is also possible.

Example 2.3.1 (Lamplighter groups have solvable word problem)**.** We will take a combinatorial approach to solving the word problem for $G = C \wr \mathbb{Z}$, where C is a cyclic group. Fix the presentation with generating set $\{a, t\}$, where a generates the cyclic group which moves the point $(0,0)$ and t generates the copy of $\mathbb{Z}$ which moves all points of the set $C \times \mathbb{Z}$ (so that t is a generator of the head of $C \wr \mathbb{Z}$). Given a word g in these generators, one can first check whether g is in the base: simply compute the image of g under the map $G \to \mathbb{Z}$, $a \mapsto 0$ by summing all of the exponents of the t's. Then g is in the base if and only if this sum is 0. Now, the length of g bounds the furthest lamp that can be switched on by g. Let n denote the length of g with respect to our generating set. Deciding whether each point in $\{(0,i) : -n \leqslant i \leqslant n\}$ is fixed therefore decides whether or not g is trivial. This approach also applies to all groups of the form $F \wr \mathbb{Z}$ where $|F|$ is finite (by using the presentation which consists of the elements of F acting on $(0,0)$ and the generator t used for $C \wr \mathbb{Z}$).

Definition 2.3.2. A group G is said to be *residually finite* if, for any $g \in G \setminus \{1\}$, there exists a finite index normal subgroup N such that $g \notin N$.

Example 2.3.3 (Examples of residually finite groups)**.** Every finite group F is residually finite (since the trivial group is both normal and finite index in F). Also $\mathbb{Z}$ is residually finite, since for any $n \in \mathbb{Z}$, $(n+1)\mathbb{Z} = \{a \in \mathbb{Z} \mid a \equiv 0 \bmod |n|+1\}$ is finite index in $\mathbb{Z}$.

Lemma 2.3.4. *If G contains an infinite simple group, then G is not residually finite.*

We prove this in two stages. First, note that any infinite simple group cannot be residually finite.

Lemma 2.3.5. *If H is not residually finite and $H \leqslant G$, then G is not residually finite.*

Proof. Since H is not residually finite, let $g \in H$ be chosen such that for all $N \trianglelefteq_f H$, $g \in N$. Now, by Lemma 1.3.5, if $M \leqslant_f G$, then $M \cap H \leqslant_f H$. Moreover if $M \trianglelefteq_f G$, then $M \cap H \trianglelefteq_f H$. Hence for all $M \trianglelefteq_f G$, $g \in M$ and G is not residually finite. □

Note that, if X is infinite, then $\mathrm{FAlt}(X)$ is an infinite simple group. Thus all of the groups studied in paper 2 are not residually finite. The lamplighter groups however are residually finite.

Lemma 2.3.6. *Let $G = F \wr \mathbb{Z}$ where F is finite. Then G is residually finite if and only if F is abelian.*

Proof. Let $F := \langle S_F \mid R_F \rangle$ be the presentation for F with generating set equal to the non-trivial elements of F and relations given by the entries of the Cayley table for F. Also let

$$G := \langle S_F, t \mid R_F, [t^{-i}et^i, t^{-j}ft^j] = 1 \text{ for all } e, f \in S_F \text{ and } i \neq j \rangle.$$

Consider $G \big/ \langle t^n \rangle_G$. This has presentation

$$\langle S_F, t \mid R_F, \underbrace{[t^{-i}et^i, t^{-j}ft^j] = 1}_{*} \text{ for all } e, f \in S_F \text{ and } i \neq j, t^n = 1 \rangle$$

where $*$ gives us that $[e, t^{-n}ft^n] = 1$ i.e. the derived subgroup of F. Thus

$$G \big/ \langle t^n \rangle \cong \left(F / F' \right) \wr C_n.$$

Now, if Q is a finite quotient of G, then there exists an $n \in \mathbb{N}$ such that

$$G \longrightarrow \left(F / F' \right) \wr C_n \longrightarrow Q \tag{4}$$

i.e. any finite quotient factors through a group formed by taking the quotient of G by $\langle t^n \rangle$. Thus, if F' is non-trivial, then by choosing an element in F' it will not survive in any finite quotient. Hence if F is not abelian then $F \wr \mathbb{Z}$ will not be residually finite. If F is abelian then any non-trivial element will survive in $F \wr C_n$ for some $n \in \mathbb{N}$ and so $F \wr \mathbb{Z}$ is residually finite. □

Note that if we drop the condition that F is finite, (4) still implies that if F is non-abelian, then $F \wr \mathbb{Z}$ is not residually finite.

The following can be found in [LS01, Ch. 4, Thm. 4.6], which lists as its motivation [McK43] and [Dys64]. Note the earlier dates of these papers compared to the usual references ([Mal58] and [Mos66]). This is probably an example of a result proved independently by different mathematical communities.

Example 2.3.7 (The word problem for finitely presented, residually finite groups)**.** Let $G = \langle S \mid R \rangle$ be a finite presentation for G, a residually finite group, and let w be a word in S. From the above, we may enumerate all words in S that represent the identity element of G. If we may also decide if w represents a non-trivial element in G, then we have solved the word problem. One way to do this is as follows. For each $n \in \mathbb{N}$, enumerate all possible homomorphisms from G to S_n. We do this by choosing $|S|$ elements from S_n and checking whether they satisfy the relations R of G. Since G is finitely generated, for each $n \in \mathbb{N}$ there are only finitely many such homomorphisms. If w represents a non-trivial element of G, we therefore have (from our assumption that G is residually finite) that, for some $n \in \mathbb{N}$, there is a homomorphism ϕ_n from G to S_n such that $(w)\phi_n \neq 1$ i.e. $w \notin \ker(\phi_n)$. We may decide whether $(w)\phi = 1$ for any homomorphism $\phi : G \to S_m$ since finite groups have solvable word problem. Thus, in order to decide whether or not w is trivial, we enumerate all words equal to the identity in order to check if w is trivial in G and compute the image of w under each of the homomorphisms enumerated from G to finite symmetric groups. One of these processes will terminate, and so we have an algorithm for deciding whether or not w represents a trivial element in G.

In [MO11], they discuss whether the finitely related assumption is necessary. Thus, despite the lamplighter groups being residually finite, since they are not finitely related this proof cannot be directly applied to them. In [KMM12] it was shown that the word problem for finitely presented, residually finite groups could be arbitrarily difficult.

There is an analogous definition to residually finite, known as conjugacy separable, which means that there is a finite quotient in which non-conjugate elements are also not conjugate. In the same way as the previous example, every finitely presented conjugacy separable group has solvable conjugacy problem (since it is always possible to decide if two words are conjugate, and by enumerating all homomorphisms to S_n for all $n \in \mathbb{N}$ one also has a process which terminates only when the elements are not conjugate). Finding groups and classes of groups which are conjugacy separable is a current area of research, see for example [Min12] and [BB14].

Conjugacy classes in $C_2 \wr \mathbb{Z}$

We will use the generating set from paper 3. Consider $C_2 \wr \mathbb{Z}$ as acting on $\{0,1\} \times \mathbb{Z} =: X$. Let a denote the generator of C_2 such that $a : (0, z) \mapsto (1, z)$ and $(1, z) \mapsto (0, z)$ for one fixed $z \in \mathbb{Z}$. Let t denote the generator of $\mathbb{Z}$ such that $t : (\delta, z) \mapsto (\delta, z + 1)$ for all $\delta \in \{0, 1\}$ and all $z \in \mathbb{Z}$.

Note that, with this action, if $g, h \in C_2 \wr \mathbb{Z}$ are not conjugate in $\mathrm{Sym}(X)$, then g and h cannot be conjugate in $C_2 \wr \mathbb{Z}$. Let us start by assuming that g is in the base of $C_2 \wr \mathbb{Z}$, which we will denote by B. Since g then contains no infinite orbits, neither can h (since conjugacy in Sym preserves cycle type). Thus, if $g \sim h$, then h must also be in B. Again using cycle type, we must have that $|\operatorname{supp}(g)| = |\operatorname{supp}(h)|$. For $g, h \in B$ to be conjugate in $\mathrm{Sym}(X)$, this is also a sufficient condition. However for them to be conjugate in $C_2 \wr \mathbb{Z}$, this is not the case. First, if $b \in B$, then $b^{-1}gb = g$. Thus if $g \sim h$, then there is a conjugator of the form t^k where $k \in \mathbb{Z}$ (see Lemma 4.17 on page 67). Hence g and h must have the same 'structure' in the following sense. Let y_{min} denote the smallest number k such that $(0, k)y = (1, k')$, and let $g' := t^{-g_{\mathrm{min}}} g t^{g_{\mathrm{min}}}$ and $h' := t^{-h_{\mathrm{min}}} h t^{h_{\mathrm{min}}}$. Hence $g'_{\mathrm{min}} = h'_{\mathrm{min}} = 0$. Now $g \sim h$ if and only if $g' = h'$.

We now consider the case where $g \notin B$. Again, g and h must have the same number of infinite orbits in order to be conjugate (since cycle type is preserved by conjugacy in $\mathrm{Sym}(X)$). Thus, if $g = wt^k$ where $w \in B$, then $h = w't^{\pm k}$ where $w' \in B$. One can then check that wt^k and $w't^{-k}$ are not conjugate in $C_2 \wr \mathbb{Z}$ for any $w, w' \in B$ and any $k \in \mathbb{N}$. We now claim that there are $2^{|k|}$ conjugacy classes in $C_2 \wr \mathbb{Z}$ for elements of the form $\{vt^k \mid v \in B\}$.

First we deal with the case where $g = wt$ with $w \in B$. Let $g' := t^{-w_{\mathrm{min}}} g t^{w_{\mathrm{min}}}$ so that $g' = w't$ with $w' \in B$ and $w'_{\mathrm{min}} = 0$. Note that for any $i \in \mathbb{Z}$, we have that $a_i^{-1}(w't)a_i = a_i w' t a_i t^{-1} t = a_i w' a_{i-1} t = a_i a_{i-1} w' t$. Now $|\operatorname{supp}(w')|/2$ is either odd or even. Conjugation by the appropriate a_i's therefore allows us to conjugate g' to either $a_0 t$ or t respectively. This provides the two distinct conjugacy classes.

The case where $g = wt^k$ (with $w \in B$ and $k > 1$) is similar. We partition X into $X_0, \ldots, X_{k-1}$, where for each $i \in \mathbb{Z}_k$, $X_i := \{(\delta, z) : \delta \in \{0, 1\} \text{ and } z \equiv i \bmod k\}$. Now note that $a_i^{-1} w t^k a_i = a_i a_{i-k} w t^k$. The arguments for $k < 0$ follow by symmetry.

We may use that the conjugacy classes are known to show that the conjugacy problem for $C_2 \wr \mathbb{Z}$ is solvable. Let $g, h \in C_2 \wr \mathbb{Z}$. First note that we can compute $w, w' \in B$ such that $g = wt^k$ and $h = w't^j$. If $j \neq k$, then $g \not\sim h$. Moreover the supports of w and w' are computable, and so we can decide whether or not g and h lie in the same conjugacy class.

2.4 A group with unsolvable word problem

We now construct a group with unsolvable word problem. Historically this was done via two different methods first, but we provide Higman's solution since it is less technical. We must still begin by introducing some notation. For a more rigorous treatment of these ideas, see [Rot95] or [Coo04].

Definition 2.4.1. (Recursive and recursively enumerable sets) We say that a subset A of $\mathbb{Z}$ is *recursively enumerable* (or *semi-decidable*) if there is a Turing Machine which outputs A. If there is also a Turing Machine which outputs $\mathbb{Z} \setminus A$ then we say that the set A is *recursive* (or *decidable*).

Example. The set of prime numbers is recursive, since for any integer one can decide (however inefficiently) whether it has any non-trivial factors or not.

Theorem 2.4.2. *[Coo04, Thm. 5.3.1] There exists a recursively enumerable set which is not recursive.*

Definition 2.4.3. Let R be a ring. Then the *polynomial ring* $R[x]$ is the set of all elements of the form $\{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N} \cup \{0\}$ and $a_0, \ldots, a_n \in R\}$ where

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{m} b_i x^i\right) := \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i\right) \times \left(\sum_{i=0}^{m} b_i x^i\right) := \sum_{i=0}^{n+m} c_i x^i \text{ where } c_k := \sum_{j=0}^{k} a_j b_{k-j}$$

with all undefined terms being considered to be equal to 0. Elements of $R[x]$ are known as *polynomials in one variable* over R, or sometimes just *polynomials* over R.

Example. For any $f \in \mathbb{Z}[x]$, the set of solutions of f which lie in $\mathbb{Z}$ is recursive since, via direct computation, one can decide whether or not $f(n) = 0$ for any $n \in \mathbb{Z}$.

Definition 2.4.4. Given a countable generating set S, a Turing machine can enumerate the countable set of elements $F(S)$. We then say that $G = \langle S \mid R \rangle$ is a *recursive presentation* if there is a Turing machine which takes $F(S)$ and outputs the set R i.e. if the set R is recursively enumerable. We then say that G is *recursively presented*. This definition may seem strange (since it may seem to be correct to call this a recursively enumerable presentation) however one can prove that if $G = \langle S \mid R \rangle$ is a presentation such that R is recursively enumerable, then there exists a set S' such that $G = \langle S' \mid R' \rangle$ and R' is recursive.

The aim of the next example is to show how to take a set which is recursively enumerable and show that it is recursive.

Example. A polynomial over $\mathbb{Z}$ can be thought of as an element of $\bigoplus \mathbb{Z}$, and so there exists a bijection from 'the set of polynomials over $\mathbb{Z}$' to the set $\mathbb{Z}$. One can then consider those polynomials which have integer solutions. The set of all such polynomials is recursively enumerable by the previous example. Moreover it is recursive i.e. it is possible to enumerate all $f \in \mathbb{Z}[x]$ which have no solutions in $\mathbb{Z}$. This can be done using the rational root theorem: given a polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$, we have that $f(p/q) = 0$ if and only if q divides a_n and p divides a_0 (where p and q are coprime integers). Thus our algorithm is simply to compute $f(\pm r)$ for each divisor r of a_0.

The picture changes when looking at polynomials over $\mathbb{Z}$ with more than one variable.

Definition 2.4.5. We say that a set $S \subseteq \mathbb{N}$ is *Diophantine* if there is a polynomial $f(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ with $a \in S$ if and only if there exists $y_1, \ldots y_{m-1} \in \mathbb{Z}$ such that $f(y_1, \ldots, y_{m-1}, a) = 0$.

Theorem 2.4.6 (Matiyasevich's)**.** *Let $S \subseteq \mathbb{N}$ be a recursively enumerable set. Then S is a Diophantine set.*

Clearly every Diophantine set is recursively enumerable. The fact that every recursively enumerable set can be realised as a Diophantine set of some polynomial over $\mathbb{Z}$ means that in some way the Diophantine sets 'characterise' recursively enumerable sets.

Recall that in order to show that the word problem is truly unsolvable, we wish to find a finitely presented group with unsolvable word problem. The finitely presented condition is important here since it means that all other finite presentations of the group will also have unsolvable word problem.

Theorem 2.4.7 (Higman's Embedding Theorem)**.** *A finitely generated group H can be embedded in a finitely presented group G if and only if H is recursively presented.*

In the following proof, free products and amalgamated free products are used. For an introduction to these, see [Ser03].

Theorem 2.4.8 ([Nov55], [Boo59], [Hig61])**.** *There exists a finitely generated group with unsolvable word problem.*

Proof. We will explain Higman's approach. We start with a set $S \subseteq \mathbb{N}$ which is recursively enumerable but not recursive. Define

$$\begin{aligned} H_S :=& \langle a, b, c, d \mid a^{-i} b a^i = c^{-i} d c^i \text{ for all } i \in S \rangle \\ \cong& \langle a, b \rangle *_R \langle c, d \rangle \text{ where } R = \langle x^{-i} y x^i \mid i \in S \rangle. \end{aligned}$$

Now, given a word $w_j = a^{-j} b a^j c^{-j} d^{-1} c^j$, where $j \in \mathbb{N}$, we have that if $j \in S$ then w_j represents a trivial element in H_S. By construction, there is no Turing machine that can enumerate the elements of $\mathbb{N} \setminus S$. Hence if $j \notin S$, then we cannot decide whether w_j is non-trivial. Although this group is not finitely presented, by the previous theorem it embeds into a finitely presented group. Such a group has unsolvable word problem since otherwise H_S would have solvable word problem. We now give a brief proof of this based on [Mil92, Lem. 2.1].

Let us assume that G has solvable word problem where G is a finitely presented group containing H_S as a subgroup. Thus there exists $\phi : H_S \hookrightarrow G$ and $w = 1$ in H if and only if $(w)\phi = 1$ in G. We assumed that we may decide whether $(w)\phi = 1$ in G, and so we may decide if $w = 1$ in H. Hence, should G have solvable word problem, then so does H_S. This contradicts the above (that H_S has unsolvable word problem) and so G is a finitely presented group with unsolvable word problem. □

2.5 History relating to the conjugacy problem

The word problem is 'well behaved' regarding finite index subgroups and finite extensions: if G has solvable word problem, then all groups commensurable to G also have solvable word problem (where G is commensurable to H if and only if there exists $N \trianglelefteq_f G, H$). By contrast the conjugacy problem is not well behaved. Moreover, one cannot even say in general that the conjugacy problem is preserved by index two subgroups or degree two extensions, since explicit examples are constructed in both [CM71] and [GK75]. It is therefore sensible to investigate under what conditions the solvability of the conjugacy problem is preserved, which is a principle aim of [BMV10]. This paper generalises the examples produced in [CM71], and its main theorem is used in paper 1 in order to investigate whether the solvability of the conjugacy problem for Houghton's groups is preserved by commensurable groups.

Another natural question is, if a group H has unsolvable conjugacy problem, does it embed into a group G with solvable conjugacy problem? Clearly this is not possible if the word problem for H is unsolvable. After considering this question, I discovered that it had been asked much earlier by Donald Collins, my supervisor's supervisor.

Question. ([KT76, Problem 5.21], Collins) Can every torsion-free group with solvable word problem be embedded in a group with solvable conjugacy problem? An example due to A. Macintyre shows that this question has a negative answer when the condition of torsion-freeness is omitted.

This question is answered by the following theorem. The solution depends on the power problem, which asks whether there is an algorithm taking as inputs a recursively presented group $G = \langle S \mid R \rangle$ and any words u and v in S, and correctly outputs 'yes' or 'no' as to whether there is an $n \in \mathbb{N}$ such that $u^n = v$ in G.

Theorem. [OS05, Thm. 1] Every countable group with solvable power problem is embeddable into a 2-generated finitely presented group with solvable conjugacy and power problems.

2.6 The word problem and conjugacy problem for Houghton's groups

We will essentially review [ABM15], where the following solutions for $\mathrm{WP}(H_n)$ and $\mathrm{CP}(H_n)$ can be found.

Definition 2.6.1. Fix an $n \in \mathbb{N}$, and let $X_n := \{1, \ldots, n\} \times \mathbb{N}$. Then the n^{th} *Houghton group*, denoted H_n, is a subgroup of $\mathrm{Sym}(X_n)$. An element $g \in \mathrm{Sym}(X_n)$ is in H_n if and only if there exist constants $z_1(g), \ldots, z_n(g) \in \mathbb{N}$ and $(t_1(g), \ldots, t_n(g)) \in \mathbb{Z}^n$ such that, for all $i \in \mathbb{Z}_n$,

$$(i, m)g = (i, m + t_i(g)) \text{ for all } m \geqslant z_i(g). \tag{5}$$

Further discussions for these groups can be found on page 53. For the interested reader we provide an alternative definition for the Houghton groups which has a more algebraic flavour.

Definition 2.6.2. The n^{th} Houghton group H_n is the set of all 'almost' order preserving symmetries of the set X_n (in the sense that there is an ordering of X_n such that, for any $g \in H_n$, for all but finitely many pairs $x, y \in X_n$, if $x < y$, then $xg < yg$). Given points $(i, m), (i', m') \in \{1, \ldots, n\} \times \mathbb{N} =: X_n$, the ordering is the lexicographic one:

$$(i, m) < (i', m') \Leftrightarrow \begin{cases} i < i' \text{ or} \\ i = i' \text{ and } m < m' \end{cases}$$

where $<$ denotes the usual ordering of $\mathbb{N}$ inherited from $\mathbb{R}$.

First, let us mention a key result for computations for Houghton's groups.

Lemma 2.6.3. *[ABM15, Lem 2.1] Let $n \geqslant 2$, let w be a word in the standard generating set S of H_n, and suppose that w represents $g \in H_n$. Then $z_i(g) \leqslant |w|_S$ for all $i \in \mathbb{Z}_n$.*

This is proved by induction on the length of w. Since for any $g \in H_n$ and any point $(i, m) \in X_n$ we may compute $(i, m)g$, we may therefore compute $(i, |w|_S)g$ in order to determine $t_i(g)$ for all $i \in \mathbb{Z}_n$. We may then compute the image under g of all points within the set $\{(i, m) \mid i \in \mathbb{Z}_n \text{ and } m < |w|_S\} =: Z(g)$ and so may describe the action of g on X_n (from only the word w). This description will be given by equations describing the action of g on $Z(g)$ and then finitely many statements of the form

$$(i, m)g = (i, m + t_i(g)) \text{ for all } m \geqslant z_i(g). \tag{6}$$

This computable nature of the permutation induced by a word w allows for the hands on approach to the word problem, conjugacy problem, and twisted conjugacy problem for the Houghton groups H_n (where $n \geqslant 2$). For example the word problem can now be solved since given any word w, we may decide if it represents the identity in H_n

(as we can describe how it moves all points of X_n using equations of the form (6) and equations describing xg for all $x \in Z(g)$). Thus, in order for our word to represent the identity, it must fix all points in X_n and it is sufficient to check if a word fixes all points in $\{(i,m) \mid i \in \mathbb{Z}_n \text{ and } m \leqslant |w|_S\}$ to determine if the word fixes all points in X_n.

Our main aim for this section is to describe how the conjugacy problem can be solved for H_n. We consider conjugacy in $\mathrm{Sym}(X_n)$, and note that conjugacy in $H_n < \mathrm{Sym}(X_n)$ has the further restriction that any element of H_n sends, for each $i \in \mathbb{Z}_n$, almost all (all but finitely many) points in the set $\{(i,m) \mid m \in \mathbb{N}\}$ to $\{(i,m) \mid m \in \mathbb{N}\}$. Thus the number of orbits with infinite intersection with each branch is a conjugacy invariant i.e. if $g \sim h$ in H_n, then $t_i(g) = t_i(h)$ for all $i \in \mathbb{Z}_n$. Clearly the converse is false: elements in $\mathrm{FSym}(X_n)$ with different cycle types cannot be conjugate in $\mathrm{Sym}(X_n)$ and so cannot be conjugate in H_n.

The strategy in [ABM15] to show that $\mathrm{CP}(H_n)$ is solvable is as follows:

i) decide, for any $g, h \in H_n$, whether they are conjugate in $\mathrm{FSym}(X_n)$;

ii) show that, should $a, b \in H_n$ be conjugate in H_n, then there exists a conjugator $x \in H_n$ with $\sum_{i=1}^{n} |t_i(x)| < M(a,b)$, where $M(a,b)$ is a number computable from only a and b;

iii) use the algorithm from (i) for the finite number of pairs $\{(a, g_{\underline{\mathbf{v}}}^{-1} b g_{\underline{\mathbf{v}}}) : \underline{\mathbf{v}} \in V\}$ where $g_{\underline{\mathbf{v}}}$ are elements such that $t(g_{\underline{\mathbf{v}}}) = \underline{\mathbf{v}}$ and V consists of all vectors which sum to 0 and whose absolute values sum to less than or equal to $M(a,b)$.

Part (ii) is completed by first showing that the translation lengths of any conjugator are a bounded distance from each other, which depends only on a and b ([ABM15, Prop. 4.3]) and then, using a centraliser argument, showing that there is a conjugator with certain translation lengths being 0. This shows that there is a conjugator whose translation lengths are bounded by a computable number. This method was adapted in paper 1 in order to solve the twisted conjugacy problem for H_n.

2.7 Generalising the algorithms of [ABM15]

In paper 1 we generalise the algorithm of [ABM15] to twisted conjugacy for Houghton's groups. Whilst doing this work, I considered some possible variations. Recall that, for each $n \in \mathbb{N}$,

$$1 \longrightarrow \mathrm{FSym}(X_n) \longrightarrow H_n \xrightarrow{\pi} \mathbb{Z}^{n-1} \longrightarrow 1$$

where $\pi : g \mapsto (t_1(g), t_2(g), \ldots, t_{n-1}(g))$, defines the n^{th} Houghton group.

Question 1. If G is a group which lies in a short exact sequence of the form

$$1 \longrightarrow \mathrm{FSym} \longrightarrow G \longrightarrow \mathbb{Z}^n \longrightarrow 1$$

then does G have solvable conjugacy problem?

Another option is to replace $\mathbb{Z}^n$ with another group where the conjugacy problem is solvable.

Question 2. Consider the short exact sequence

$$1 \longrightarrow \mathrm{FSym} \longrightarrow G \longrightarrow F_n \longrightarrow 1$$

where F_n denotes the free group of rank n. Then does G have solvable conjugacy problem?

The braided Houghton group H_n^{br} is defined by replacing the permutations of X_n with braids. This group was introduced in [Deg00] where questions regarding the finiteness conditions of this group were posed. For any $n \in \mathbb{N}$, let B_n denote the braid group on n strands. Since $\mathrm{CP}(B_n)$ is well understood, the approach outlined in the previous section for $\mathrm{CP}(H_n)$ could potentially be adapted to solve $\mathrm{CP}(H_n^{br})$.

Question 3. Consider permutational wreath products of the form $H_m \wr_{X_n} H_n$ or even finite iterations of this i.e.

$$(\ldots((H_n \wr_{X_n} H_n) \wr_{X_n} \ldots \wr_{X_n} H_n) \wr_{X_n} H_n.$$

Do such groups have solvable conjugacy problem?

The finiteness conditions of such groups were studied in [KM16]. We solve the word problem for such groups below.

After studying the conjugacy problem for finite index subgroups of Houghton groups, another (similar) family of groups were introduced to me by preliminary work carried out by my supervisor (Armando Martino) and Peter Kropholler. They investigated the finiteness conditions of this family of groups. Recall the homomorphism $\pi : H_n \to \mathbb{Z}^{n-1}$ defined by $g \mapsto (t_1(g), t_2(g), \ldots, t_{n-1}(g))$. Now consider a subgroup K of H_n such that $[\mathbb{Z}^{n-1} : (K)\pi]$, the index of $(K)\pi$ in $(H_n)\pi$, is finite. Note that K need not have finite index in H_n in order to satisfy this property.

Definition 2.7.1. Let G and H be finitely presented groups and let $H \leqslant G$. Then the membership problem for G and H, denoted $\mathrm{MP}(G, H)$, asks whether there exists an algorithm which takes as inputs the finite presentations for G and H and a word w in G, and outputs yes or no depending on whether or not w represents an element of H.

Note that $\mathrm{MP}(G, \{1\})$ is $\mathrm{WP}(G)$. Two possible questions present themselves.

Question 4. Let $K \leqslant H_n$ satisfy $[\mathbb{Z}^{n-1} : (K)\pi] < \infty$. Then is $\mathrm{MP}(H_n, K)$ solvable?

Question 5. Let $K \leqslant H_n$ satisfy $[\mathbb{Z}^{n-1} : (K)\pi] < \infty$. Then is $\mathrm{CP}(K)$ solvable?

Question 4 could be extended to all recursively presented subgroups of H_n. This then relates to a question of Collin Bleak, who asked whether the membership problem for Thompson's group V is solvable for all finitely presented subgroups. This is because Thompson's group V contains, as a subgroup, each Houghton group H_n (for all $n \in \mathbb{N}$).

Remark 2.7.2. *We may now extend the curiosity discussed in Section 1.1. We introduce this via an example. Let H_2, the 2^{nd} Houghton group, act on $\mathbb{Z}$ where t corresponds to the element of* $\mathrm{Sym}(\mathbb{Z})$ *which sends z to $z+1$ for all $z \in \mathbb{Z}$ so that $H_2 = \langle t, (0\ 1)\rangle$. Now $\langle t^2, (0\ 1), (0\ 2)(1\ 3)\rangle$ is a subgroup of H_2 which is isomorphic to $C_2 \wr_X H_2$ for some set X. Moreover, for any $n \geqslant 2$ and any finite group F, there exists a subgroup of H_n isomorphic to $F \wr_Y H_n$ for some set Y. Since these groups do not act primitively on X_n, the cannot contain* $\mathrm{FAlt}(X_n)$ *and so cannot be of finite index in H_n.*

We now produce an algorithm to solve the word problem for the groups in Question 3 above. In fact we will solve the word problem for a larger class of groups. Throughout we will work with a fixed $n \geqslant 2$, and so let $H := H_n$. Thus H acts on $X := X_n$. Now, for any recursively presented group G with solvable word problem we will solve the word problem for $G \wr_X H$.

Let us first choose a finite generating set. Let $G = \langle S_G \mid R_G\rangle$ be a recursive presentation for G with solvable word problem and let $\langle S_H \mid R_H\rangle$ be our standard presentation for H (the one used throughout paper 1, see page 53). We will use $S_G \sqcup S_H$ as our generating set for $G \wr_X H$, where the elements of S_G correspond to the copy of G at $(1,1) \in X$. Recall that the base of $G \wr_X H$ is equal to

$$\bigoplus_{(i,m)\in X} G_{(i,m)}.$$

Lemma 2.7.3. *The word problem for $G \wr_X H$ is solvable.*

Sketch Proof. Let $g \in G \wr_X H$. Our aim is to decide whether g is trivial. The three steps of our algorithm are as follows.

i) From above, the word problem for H is solvable. Hence, given a word which represents g, we can decide whether or not this word lies in the base of $G \wr_X H$.

ii) Let this word be written as $u_1v_1u_2v_2\ldots u_mv_m$ where $u_i \in S_H$ and $v_i \in S_G$ for all $i \in \mathbb{Z}_m$. We may rewrite this as $(u_1v_1u_1^{-1})(u_1u_2v_2u_2^{-1}u_1^{-1})(u_1u_2u_3v_3u_3^{-1}u_2^{-1}u_1^{-1})\ldots$ in order to express g as a product of elements in finitely many different $G_{(i,m)}$ (where each (i,m) is in X).

iii) Solving the word problem for G in each of these is therefore sufficient to decide whether or not the given word represents the identity. This is possible by our assumption that G had solvable word problem. □

Note that this proof only relies on H having solvable word problem. For the conjugacy problem, there is the following result for standard wreath products.

Theorem. [Mat66, Thm. B] Let $W = G \wr H$ be a (restricted) wreath product of two nontrivial groups G and H with $\mathrm{CP}(G)$ and $\mathrm{CP}(H)$ solvable. Then $\mathrm{CP}(W)$ is solvable if and only if the group H has a solvable power problem.

2.8 Decision problems and cryptography

I thank Michal Ferov for explaining the following to me whilst he was a PhD student at Southampton.

- The *conjugator search problem* for a recursively presented group G asks for an algorithm which, given any pair $a, b \in G$ of conjugate elements in G, finds a $g \in G$ such that $g^{-1}ag = b$.

We start with two parties, say Alice and Bob. The aim of a key-exchange method is, via a prearranged strategy, to enable Alice and Bob to both gain access to a key using communication which, if intercepted, will not allow a rogue party to have access to the key. An example of such a method is the Diffie-Hellman key exchange method. The following is an example of producing a key-exchange method using a recursively presented group. This method can be found in [AAG99].

Certain information is made public: a group G with presentation $\langle S \mid R \rangle$; a set $A' := \{a_1, a_2, \ldots, a_m\} \subset G$; a subgroup $A := \langle A' \rangle$ of G; a set $B' := \{b_1, b_2, \ldots, b_n\} \subset G$; and a subgroup $B := \langle B' \rangle$ of G.

Alice now chooses some $\alpha \in A$ and Bob chooses some $\beta \in B$. These will be their private keys. Alice then computes $\{\alpha^{-1}b_1\alpha, \alpha^{-1}b_2\alpha, \ldots, \alpha^{-1}b_n\alpha\} =: C_{A'}$ and sends this set, with this given ordering, to Bob. Bob computes the set $\{\beta^{-1}a_1\beta, \beta^{-1}a_2\beta, \ldots, \beta^{-1}a_m\beta\} =: C_{B'}$ and sends this set (again ordered) to Alice.

The key which they both now wish to compute is $[\alpha, \beta] := \alpha^{-1}\beta^{-1}\alpha\beta$. This is achieved as follows. Alice's key α is given as a word in A'. Thus, by replacing each generator a_i in α with $\beta^{-1}a_i\beta$, she may compute $\beta^{-1}\alpha\beta$. This allows her to compute $[\alpha, \beta]$. Similarly, Bob can replace each generator b_i in β with $\alpha^{-1}b_i\alpha$. Hence Bob has computed $\alpha^{-1}\beta\alpha$, allowing him to compute $[\alpha, \beta] = (\alpha^{-1}\beta\alpha)^{-1}\beta$. In order to use such a key, the word problem for G should be solvable (since the word computed for the commutator by each party may be different). It is also useful for elements in G to have some kind of normal form, since this means that the simplifications to the elements $\alpha^{-1}b_i\alpha$ do not provide any information about α.

Now, consider a rogue agent. They will have access to the ordered sets $A', B', C_{A'}$, and $C_{B'}$. In order to compute $[\alpha, \beta]$ however, they must find α and β from these sets. One way to do this would be to solve the conjugator search problem for each pair a_i and $\beta^{-1}a_i\beta$. By choosing a group where this problem is computationally difficult, the rogue agent can be stopped from being able to easily compute the private key $[\alpha, \beta]$. The theorem below shows that there are many possible candidates for such a group.

Theorem 2.8.1 ([Col72]). *Let D_1 and D_2 be recursively enumerable degrees of unsolvability such that $D_1 \leqslant_T D_2$. Then there is a finitely presented group G such that WP(G) has degree D_1 and CP(G) has degree D_2. In particular, there is a finitely presented group with solvable word problem but unsolvable conjugacy problem.*

Thompson's group F has also been investigated as a possible candidate to be used with encryption methods, since certain extensions of it have solvable word problem and unsolvable conjugacy problem (see [SU05]). This was shown to be insecure in [Mat06]. Recent discussions on this can be found in [Abd16].

3 Background for Paper 2

We begin with a topic touched upon in paper 1 and prevalent in paper 2.

3.1 Twisted Conjugacy

The notion of twisted conjugacy generalises that of conjugacy. Let G be a group and let $\phi \in \mathrm{Aut}(G)$. Then $a, b \in G$ are ϕ-twisted conjugate if and only if $(x^{-1})\phi a x = b$. For any automorphism of G this produces an equivalence relation. My interest in this began in my first paper where it occurs as a condition related to the solvability of the conjugacy problem for extensions of a group. It then featured in paper 2 since it is the foundation of the R_∞ property. We say a group has the R_∞ property if, for every automorphism ϕ, the number of ϕ-twisted conjugacy classes is infinite.

3.2 A brief history of the R_∞ property

The property first became of interest when it arose in Nielsen fixed point theory. For more information, see [BFGJ05] or [Jia83]. The property has also been used in other fields, such as algebraic geometry and number theory, but has since become a subject in its own right, with many papers focussing on groups or families of groups which either have or do not have the property.

Example. For an example of a group without the R_∞ property, consider $\mathbb{Z}$. In general it is more difficult to show a group has the property since it involves checking that there are infinitely many ϕ-twisted conjugacy classes for all automorphisms. Any free group of rank n, where $n \in \mathbb{N} \setminus \{1\}$, provides an example of a group with the R_∞ property. See [Fel10] for a list of many families of groups for which this property has been investigated.

A key motivation for the subject was the following conjecture, which sets R_∞ in a more general context. The concept of exponential growth can be found in Section 4.1.

Conjecture ([FH94]). Let G be a finitely generated group of exponential growth and $\phi : G \to G$. If ϕ is injective, then G has infinitely many ϕ-twisted conjugacy classes.

This conjecture was shown to be false in [GW03], with an example where ϕ is an automorphism of G. In fact we have already seen an example of such a group (by [GW06]): given a lamplighter group $G = C \wr \mathbb{Z}$, G has R_∞ if and only if $|C|$ is coprime to 6.

In paper 2 I studied this property for groups $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$, where X is an infinite set. We will see that no such group has polynomial growth, and any group containing an element with an infinite cycle will have exponential growth. This work was possible because the automorphisms of any such group are of a particular form, specifically that $N_{\mathrm{Sym}(X)}(G) \cong_\Psi \mathrm{Aut}(G)$ where $\Psi : \rho \mapsto \phi_\rho$. A proof of this result can be found in the next section.

In group theory it is often natural to ask whether properties are preserved by finite index subgroups or by finite extensions, a question asked about the R_∞ property in, for example, [TW06]. This is also investigated for the groups in paper 2.

3.3 Automorphisms of groups fully containing FAlt

Throughout this section we shall assume that X is an infinite set. We say that a group $G \leqslant \mathrm{Sym}(X)$ *fully contains* $\mathrm{FAlt}(X)$ if $\mathrm{FAlt}(X) \leqslant G$. Paper 2 deals with such groups. Preliminary observations are that if a group fully contains FAlt then it will have FAlt as a normal subgroup (actually it will be a characteristic subgroup, as stated in Proposition 2.2 of paper 2) and cannot be residually finite (as proved in Lemma 2.3.4 on page 19). Although growth of groups will be discussed in the next section, it is also worth mentioning that no group fully containing FAlt can have polynomial growth (by a theorem of Gromov). Below is a statement about the structure of the automorphism group of such groups.A similar proof was contained in Section 2.2 of the first version of paper 1 to appear on the arXiv, and this proof actually applies to any group $\mathrm{FSym}(X) \leqslant G \leqslant \mathrm{Sym}(X)$ where $\mathrm{FSym}(X)$ is characteristic in G. We now outline this proof with the necessary changes for it to apply to such groups. It can be further adapted to work for $\mathrm{FAlt}(X)$ rather than $\mathrm{FSym}(X)$ (by replacing 2-cycles with 3-cycles). In paper 2 we show that any group fully containing $\mathrm{FAlt}(X)$ has $\mathrm{FAlt}(X)$ as a characteristic subgroup.

Proposition 3.3.1. *Let $n \geqslant 2$. Then $N_{\mathrm{Sym}(X_n)}(H_n) \cong_\Psi \mathrm{Aut}(H_n)$, where $\Psi : \rho \mapsto \phi_\rho$ and H_n denotes the n^{th} Houghton group.*

We will show that any automorphism of $\mathrm{FSym}(X) \leqslant G \leqslant \mathrm{Sym}(X)$ can be realised by conjugation by an element of $\mathrm{Sym}(X)$. Similar arguments may be found in [BCMR14] and [GP14].

Lemma 3.3.2. *Let* $\mathrm{FSym}(X) \leqslant G \leqslant \mathrm{Sym}(X)$. *Moreover, let* ψ *be a monomorphism from* G *to* $\mathrm{Sym}(X)$. *If* ψ *is the identity when restricted to* $\mathrm{FSym}(X)$, *then* ψ *is the identity on* G.

Proof. Let $g \in G$ and Ψ be a monomorphism from G to $\mathrm{Sym}(X)$ which restricts to the identity on $\mathrm{FSym}(X)$. Conjugation by any element of $\mathrm{Sym}(X)$ preserves cycle type. Thus, for any $i, j \in X$,

$$\begin{aligned}((i)g\Psi\ (j)g\Psi) &= (g\Psi)^{-1}(i\ j)(g\Psi) = (g^{-1}\Psi)((i\ j)\Psi)(g\Psi)\\ &= (g^{-1}(i\ j)g)\Psi = ((i)g\ (j)g)\Psi = ((i)g\ (j)g)\end{aligned}$$

and so $(i)g\Psi \in \{(i)g,\ (j)g\}$. Running this argument for the transposition $(j\ k)$ where $k \neq i$ shows that $(j)g\Psi \in \{(j)g, (k)g\} \cap \{(i)g, (j)g\}$ and so $(j)g\Psi = (j)g$. Notice that this argument holds for all $i, j \in X$, and so $g\Psi$ and g produce the same bijection on X. □

Lemma 3.3.3. *Let* $G \leqslant \mathrm{Sym}(X)$ *with* $\mathrm{FSym}(X)$ *a characteristic subgroup of* G. *Then* $N_{\mathrm{Sym}(X)}(G) \cong_\Psi \mathrm{Aut}(G)$ *where* $\Psi : \rho \mapsto \phi_\rho$.

Proof. Let $\phi \in \mathrm{Aut}(G)$ and recall that every automorphism of $\mathrm{FSym}(X)$ can be achieved through conjugation by some $\rho \in \mathrm{Sym}(X)$.

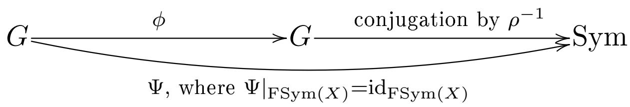


FIGURE 1: The interactions between ϕ, ρ, and Ψ.

Figure 1 and Lemma 3.3.2 together imply, for any $\phi \in \mathrm{Aut}(G)$, that

$$(\phi\phi_{\rho^{-1}})|_{\mathrm{FSym}(X)} = \mathrm{id}_{\mathrm{FSym}(X)} \text{ and so } \phi\phi_{\rho^{-1}} = \mathrm{id}_G\,.$$

Thus every $\phi \in \mathrm{Aut}(G)$ can be achieved through conjugation by some $\rho \in \mathrm{Sym}(X)$ and we have an epimorphism from $N_{\mathrm{Sym}(X)}(G)$ to $\mathrm{Aut}(G)$.

We now show that this epimorphism is injective. We will show that $C_{\mathrm{Sym}(X)}(\mathrm{FSym}(X))$ is trivial which will imply $C_{\mathrm{Sym}(X)}(G)$ is trivial. Assume there is a $\rho \neq 1$ in $\mathrm{Sym}(X)$ such that for all $g \in \mathrm{FSym}(X), \rho g = g\rho$. Let $i \in \mathrm{supp}(\rho)$. Pick $j \notin \{\rho(i), i\}$. Setting $f := (i\ j)$ we have, by our assumption, that $\rho^{-1}(i\ j)\rho = ((i)\rho\ (j)\rho) = (i\ j)$. This is a contradiction as $(i)\rho \neq i$ or j. Since the centraliser is trivial, our epimorphism has trivial kernel and so is injective. □

Remark 3.3.4. *Notice that both Lemma 3.3.2 and Lemma 3.3.3 work with* $\mathrm{FAlt}(X)$ *characteristic in* G *rather than* $\mathrm{FSym}(X)$ *(since* $\mathrm{Aut}(\mathrm{FAlt}(X)) \cong \mathrm{Sym}(X)$, *see [DM96] or [Sco87]). Other conditions on the torsion elements of* G *which form a subgroup may also provide the assumptions used.*

4 Background for Paper 3

In this section we see how questions of a type usually asked in Analysis can be asked about finitely generated groups. Given a group G and a generating set S, there is a natural graph one may associate to G with respect to S. The vertices of this graph are formed from the elements of G, and so are independent of S. We introduce a directed edge from a vertex x_1 to a vertex x_2 if and only if there is an $s \in S$ such that $x_1 s = x_2$. This is called a *Cayley graph* and we will denote it by $\mathrm{Cay}(G, S)$. Note that this will always be a connected graph, and that cycles in this graph provide relationships between elements in G with respect to S. If S is finite, then such a graph will be locally finite. Furthermore, we may produce a metric space from this graph in a canonical way: the distance between two vertices x_1 and x_2 is equal to the shortest path from x_1 to x_2 (where every edge in our graph is defined to have length 1). This distance can depend on S: consider different generating sets for $\mathbb{Z}$. Algebraically we have that $d_S(x_1, x_2) = |x_1^{-1} x_2|_S$, where $|g|_S$ denotes the length of the shortest word representing g using the generating set S. Details on when $\mathrm{Cay}(G, S)$ is a tree can be found in [Ser03]. It may be intuitively clear that $\mathrm{Cay}(G, S)$ is an infinite tree if and only if G is a free group and S is a basis for G. If $\mathrm{Cay}(G, S)$ is a finite tree then G is finite and so G must be trivial.

If S and S' are two finite generating sets of G, then $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S')$ may not be isometric metric spaces. However $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S')$ will be *quasi-isometric* metric spaces. This means that there is a quasi-isometry between them, which really is an 'almost isometry' in that two metric spaces X and Y with metrics d_X and d_Y are quasi-isometric if and only if the following conditions hold.

i) There exists a function $\phi : X \to Y$ and constants $A \in \mathbb{R}_{>0}, B \in \mathbb{R}$ such that for all $x_1, x_2 \in X$: $\frac{1}{A} d_X(x_1, x_2) - B \leqslant d_Y((x_1)\phi, (x_2)\phi) \leqslant A \cdot d_X(x_1, x_2) + B$;

ii) there is a constant $C \in \mathbb{R}$ such that for any $y \in Y$ there exists an $x \in X$ satisfying $d_Y((x)\phi, y) \leqslant C$.

If $S = \{x_1, \ldots, x_n\}$ and $S' = \{y_1, \ldots, y_m\}$, then $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S')$ are quasi-isometric since the generators in S' are elements of G, and so can be written as words in S. Then ϕ may be the identity (the vertex sets of the graphs are the same) and we may set $C := 0$, $B := 0$, and $A := \max\{|x_i|_{S'}, |y_j|_S : i \in \mathbb{Z}_n, j \in \mathbb{Z}_m\}$.

4.1 Growth of groups

In a similar way to when working with metrics in $\mathbb{R}^n$, for a group G with generating set S let $\mathbb{B}_S(n)$ denote the ball of radius n within $\mathrm{Cay}(G, S)$.

$$\mathbb{B}_S(n) := \{\text{vertices } x \in \mathrm{Cay}(G, S) \mid d_S(1, x) \leqslant n\}$$

It may be that more can be said of the form of elements in $\mathbb{B}_S(n)$ for any given n, for example when working with $\mathbb{Z}$ with the standard (single element) generating set. We may then look at how the size of $\mathbb{B}_S(n)$ varies with respect to n. For a group G with finite generating set S, let

$$f_{G,S}(n) := |\mathbb{B}_S(n)| \text{ for all } n \in \mathbb{N}.$$

We therefore have, for all $n \in \mathbb{N}$, that $f_{\mathbb{Z},\{1\}}(n) = 2n + 1$. Using a different finite generating set for $\mathbb{Z}$ also gives a polynomial function, and in fact one can prove that these functions will always be linear i.e. be of the form $a_1 n + a_2$ for some $a_1, a_2 \in \mathbb{R}$. By sketching the Cayley graph for $\mathbb{Z}^2$ with the standard generating set $S = \{(1,0)^T, (0,1)^T\}$ one can see, for $n \geqslant 1$, that $|\mathbb{B}_S(n) \backslash \mathbb{B}_S(n-1)| = 2(n+1)+2(n-1)$. Simple computations then show that $f_{\mathbb{Z}^2,S}(n) = 2n^2 + 2n + 1$. Note that this could also be seen geometrically as $(n+1)^2 + n^2$ by separately considering those points which are an even or odd distance from the identity.

It is now less obvious that there could be a similar formula if a different generating set S' were used i.e. can we determine the form of $f_{\mathbb{Z}^2,S'}(n)$?

Definition 4.1.1. Given functions $f, g : \mathbb{R} \to \mathbb{R}$, we say that f and g have the same growth type if there exists a $C \in \mathbb{R}\backslash\{0\}$ such that, for all $n \in \mathbb{R}$, $g(n/C) \leqslant f(n) \leqslant g(Cn)$.

From the fact that different finite generating sets produce quasi-isometric Cayley graphs, we have for any finite generating sets S and S' that $f_{G,S}$ and $f_{G,S'}$ will be functions with the same growth type. Hence, despite it being possible to use different finite generating sets to produce different growth functions, the *growth* i.e. the growth type of the growth function of a group, is well defined. One could then ask whether there is a 'minimal' growth function in some respect i.e. whether, for a given group, there is a generating set which produces a function which grows slower (asymptotically) than any other growth function for the group. This can be very complex, since all generating sets need to be considered. It may also be that the infimum of all growth rates of the growth functions of a group is not realised by any generating set of a group, for example see [Wil04].

Not all groups have polynomial growth, with the simplest example probably being free groups. Let G be a free group of rank 2 and let $S = \{a, b\}$ generate G. Given a vertex x in $\mathrm{Cay}(G, S) \setminus \{1\}$, there is an $n \in \mathbb{N}$ such that $x \in \mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)$. Now, exactly 3 of xa, xa^{-1}, xb, xb^{-1}, lie in $\mathbb{B}_S(n+1) \setminus \mathbb{B}_S(n)$. Hence, for all $n \in \mathbb{N}$, $|\mathbb{B}_S(n+1) \setminus \mathbb{B}_S(n)| = 3|\mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)|$. It is then straightforward to see that

$$
\begin{aligned}
|\mathbb{B}_S(n+1)| &= |\mathbb{B}_S(0)| + |\mathbb{B}_S(1) \setminus \mathbb{B}_S(0)| + \sum_{k=1}^{n} |\mathbb{B}_S(k+1) \setminus \mathbb{B}_S(k)| \\
&= |\mathbb{B}_S(0)| + |\mathbb{B}_S(1) \setminus \mathbb{B}_S(0)| + 3\sum_{k=0}^{n-1} |\mathbb{B}_S(k+1) \setminus \mathbb{B}_S(k)| \\
&= \dots \\
&= |\mathbb{B}_S(0)| + \sum_{i=0}^{n-1} (3^i |\mathbb{B}_S(1) \setminus \mathbb{B}_S(0)|) + 3^n \sum_{k=0}^{0} |\mathbb{B}_S(k+1) \setminus \mathbb{B}_S(k)| \\
&= -1 + 2 \cdot 3^{n+1}
\end{aligned}
$$

From this computation we make two elementary observations.

Lemma 4.1.2. *Let S be a finite generating set for a group G. Then $\hat{f}_{G,S}(n) := \mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)$ has exponential growth if and only if $f_{G,S}$ does. Moreover, f and $\hat{f}$ have the same growth rate (i.e. $f_{G,S}(n)/\hat{f}_{G,S}(n)$ is of subexponential growth).*

Lemma 4.1.3. *Let S be a finite generating set for G. Then $f_{G,S}(n)$ has at most exponential growth with growth rate less than or equal to $|S^{\pm 1}| - 1$.*

In [Gro81b, Exam. 5.13], Gromov remarked that this growth rate has the smallest exponent amongst all finite generating sets for a free group. Also, in [AGG05], it is shown that there is a set of amenable groups whose growth functions tend to this bound (despite the fact that no amenable group can contain a non-abelian free group).

A natural aim is to classify those groups with polynomial growth. Its elegant and well known answer is given below. We require two definitions.

Definition 4.1.4. Let $\mathcal{P}$ be a property of groups, for example abelian. Then a group G is virtually $\mathcal{P}$ if and only if there exists a finite index subgroup of G that satisfies $\mathcal{P}$.

There are several equivalent definitions of the following.

Definition 4.1.5. Let G be a group. We first define the *lower central series* of G. Let $G^{(0)} := G$ and, for each $k \in \mathbb{N}$, let $G^{(k)} := [G, G^{(k-1)}]$, the group generated by all commutators $[g, g']$ where $g \in G$ and $g' \in G^{(k-1)}$. Then a group is *nilpotent* if and only if there is an $n \in \mathbb{N}$ such that $G^{(n)}$ is the trivial group.

Theorem 4.1.6 ([Gro81a])**.** *Let G be a finitely generated group. Then G has polynomial growth if, and only if, G is virtually nilpotent.*

Another natural question is whether there is a group which has neither polynomial nor exponential growth. From Lemma 4.1.3, no finitely generated group can have growth rate faster than exponential. There is a class of functions between polynomial and exponential however. We shall say *subexponential growth* to identify any function which grows slower than any exponential.

Example. Let a be a real number greater than 1. Then $a^{\sqrt{n}}$ is a function (of n) with subexponential growth but not of polynomial growth.

Question. Is there a finitely generated group of subexponential growth that does not have polynomial growth?

The Grigorchuk group, which was introduced in [Gri84], answers this question in the affirmative, though this group (and the many generalisations) have been found to not be finitely related.

Question. Is there a finitely presented group of subexponential growth?

Perhaps surprisingly, this question is open at the time of writing this thesis.

Paper 2 deals with groups containing $\mathrm{FAlt}(X)$ for some infinite set X. Such groups are not virtually nilpotent (and so finitely generated examples of such groups cannot have polynomial growth by Theorem 4.1.6).

Lemma 4.1.7. *If $G \geqslant \mathrm{FAlt}(X)$ for some infinite set X, then G is not virtually nilpotent.*

Proof. From Lemma 1.3.6 on page 14, if $H \leqslant_f G$, then $\mathrm{FAlt}(X) \leqslant H$. Now we note that any group containing $\mathrm{FAlt}(Y)$ where Y is infinite cannot be nilpotent, since

$$[\mathrm{FAlt}(Y), \mathrm{FAlt}(Y)] = \mathrm{FAlt}(Y) \tag{7}$$

and so $[H, H] \geqslant [H, \mathrm{FAlt}(X)] \geqslant \mathrm{FAlt}(X)$. We now show that (7) holds. By direct computation, for any distinct $a_1, \ldots, a_6 \in Y$, $[(a_1\ a_2\ a_3), (a_1\ a_4)(a_5\ a_6)] = (a_1\ a_4\ a_2)$. Now note that we are free to choose $a_1, \ldots a_6$ and that $\mathrm{FAlt}(Y)$ can be generated by 3-cycles (from Lemma 1.1.3). □

An alternative proof of the following can be found in [BCMR14]. It also follows from [GS10, Exam. 2.3.], which shows that the conjugacy growth function of H_2 is exponential (since for any finitely generated group the growth function is bounded below by the conjugacy growth function).

Lemma 4.1.8. *Let $n \geqslant 2$. Then H_n, the n^{th} Houghton group, has exponential growth.*

Proof. Let $F \leqslant G$ be finitely generated groups. Then G has growth at least that of F, since we may choose a generating set of G which contains the generating set of F. Importantly, if F has exponential growth, then so will G. Thus we need only show that H_2 has exponential growth. We consider H_2 acting on the set $\mathbb{Z}$. Also, let t denote the element of $\mathrm{Sym}(\mathbb{Z})$ which sends z to $z+1$ for all $z \in \mathbb{Z}$. Now, $\{t, (0\ 1)\}$ is a generating set for H_2. But $\langle t^2, (0\ 1)\rangle$ is the lamplighter group $C_2 \wr \mathbb{Z}$, which has exponential growth (see, for example, [BT15]). □

Random Walks on a Cayley graph

A random walk on a Cayley graph can probably only have one interpretation. Let $G = \langle S \mid R \rangle$. We start at 1, the identity element of G. A *random walk* of length n on $\mathrm{Cay}(G, S)$ is then given by a group element $a_1 a_2 \dots a_n$ where, for each $i \in \mathbb{Z}_n$, $a_i \in S^{\pm 1}$. Choosing each a_i from $S^{\pm 1}$ with equal probability provides a finite process for picking elements of G. One could then study, for example, the probability that a random walk ends at the vertex 1. By varying n, asymptomatic behaviour of random walks on $\mathrm{Cay}(G, S)$ can be studied.

4.2 Degree of Commutativity

The degree of commutativity for a finite group is the probability of choosing two elements in the group which commute i.e. for a finite group G, the degree of commutativity of G, denoted $\mathrm{dc}(G)$, is given by

$$\mathrm{dc}(G) := \frac{|\{(a, b) \in G^2 : ab = ba\}|}{|G|^2}. \tag{8}$$

There has been much work towards computing which values between 0 and 1 can be taken by a group and computing (8) for families of groups. The third paper in this thesis extends the work of [AMV] where the definition for the degree of commutativity of a group is extended to finitely generated infinite groups. We will start by looking at well known results from the literature for finite groups.

Computing the degree of commutativity for D_4

We will compute $\mathrm{dc}(D_4)$ by brute force. Let

$$D_4 := \langle r, s \mid r^4 = s^2 = 1, srs = r^{-1} \rangle$$

where each element of D_4 can be written uniquely as $t^j s^k$ for some $j \in \{0, 1, 2, 3\}$ and $k \in \{0, 1\}$. Thus, as sets,

$$D_4 = \{1, r, r^2, r^3, s, rs, r^2 s, r^3 s\}.$$

Simple computation shows that each reflection $r^k s$ commutes with $1, r^2, r^k s$, and $r^{-k} s$. Similarly if a rotation and reflection commute then we have $r^i(r^j s) = (r^j s) r^i = r^j r^{-i}$ from which we obtain that i must be 0 or 2. To summarise: $|C_{D_4}(1)| = 8$; $|C_{D_4}(r)| = 8$; $|C_{D_4}(r^3)| = 8$; $|C_{D_4}(r^2)| = 8$; and $|C_{D_4}(r^k s)| = 4$.

Thus 40 of the 64 possible pairs in D_4 commute, and so $\mathrm{dc}(D_4) = \frac{5}{8}$.

Results for finite groups

A result which may seem surprising is that, if $\mathrm{dc}(G) > \frac{5}{8}$, then $\mathrm{dc}(G) = 1$. The proof does not require sophistigated tools, and can be found in [Gus73]. Note that this bound is sharp, since we have just computed that $\mathrm{dc}(D_4) = \frac{5}{8}$. The definition labelled (8) above can also be used for finite semigroups, since all that it requires is a set G equipped with a binary operation. In this case the degree of commutativity can take any value in $(0,1] \cap \mathbb{Q}$ (see [PS12]). The following result is helpful to shorten the computations for $\mathrm{dc}(G)$, and has seen much use in the literature. It is proved in [Gus73] (where degree of commutativity was first introduced) but with reference to [ET68, Thm. IV], since all of the ingredients of the proof can be found there.

Lemma 4.2.1. *Let G be a finite group. Then*

$$\mathrm{dc}(G) = \frac{\#\ \textit{conjugacy classes of}\ G}{|G|}.$$

Proof. By definition,

$$\mathrm{dc}(G) = \frac{1}{|G|^2} \sum_{x \in G} |C_G(x)|.$$

Now, if $x \sim y$, then $|C_G(x)| = |C_G(y)|$ since $(x)\phi_g = y$ for some $g \in G$. Let $C_1, \ldots, C_m$ be distinct conjugacy classes of G with representatives $x_1, \ldots x_m$ respectively. Then

$$\mathrm{dc}(G) = \frac{1}{|G|^2} \sum_{i=1}^{m} |C_i||C_G(x_i)|. \tag{9}$$

We may now use the orbit stabiliser theorem since G acts, by conjugation, on itself. Thus, for each $i \in \mathbb{Z}_m$,

$$|C_i| = |G| \big/ |C_G(x_i)|$$

and so (9) becomes

$$\frac{m|G|}{|G|^2} = \frac{m}{|G|}.$$

□

It may also interest the reader whether information about the degree of commutativity of normal subgroups of G is related to the degree of commutativity of G.

Lemma 4.2.2 ([Gal71])**.** *Let G be a finite group and N a normal subgroup of G. Then*

$$\mathrm{dc}(G) \leqslant \mathrm{dc}(N) \cdot \mathrm{dc}(G/N).$$

Generalising the definition to infinite groups

In [AMV], the degree of commutativity of infinite groups was investigated. The main challenge is deciding how to choose two 'random' elements in the group. Two possibilities present themselves if G is finitely generated: to either use random walks on the Cayley graph, or to use the balls of radius n on the Cayley graph. In [AMV] they use the second option and so we will give more detail on this. Fix a generating set S. Let $\mathbb{B}_S(n) := \{g \in G : |g|_S \leqslant n\}$. Now define

$$\mathrm{dc}_S(G, n) := \frac{|\{(a, b) \in \mathbb{B}_S(n)^2 : ab = ba\}|}{|\mathbb{B}_S(n)|^2}.$$

Notice the similarity to (8) on page 37. If the numbers $\mathrm{dc}_S(G, n)$ converge as n tends to infinity, we could then say that this is the degree of commutativity of G with respect to S. In order to guarantee this, let

$$\mathrm{dc}_S(G) := \limsup_{n\to\infty}(\mathrm{dc}_S(G, n)). \tag{10}$$

Similarly one could take the lim inf of this sequence. They also pose the following conjecture.

Conjecture. [AMV, Conj. 1.6] Let G be a finitely generated group, and let S be a finite generating set for G. Then: (i) $\mathrm{dc}_S(G) > 0$ if and only if G is virtually abelian; and (ii) $\mathrm{dc}_S(G) > 5/8$ if and only if G is abelian.

Note that any finitely generated and virtually abelian group is virtually $\mathbb{Z}^n$ for some $n \geqslant 0$. Hence, if the conjecture is correct, then all groups G with $\mathrm{dc}_S(G) > 0$ are amenable. From this it therefore seems reasonable that the value of $\mathrm{dc}_S(G)$ is independent of S i.e. if $\tilde{S}$ is another finite generating set for G, then $\mathrm{dc}_S(G) = \mathrm{dc}_{\tilde{S}}(G)$. However it is currently unknown as to whether the value of (10) depends on the finite generating set used. Note that if $\mathrm{dc}_S(G)$ is 0, then $\liminf_{n\to\infty}(\mathrm{dc}_S(G, n))$ is also 0, and so this alternative definition for $\mathrm{dc}_S(G)$ produces a weaker conjecture.

Within the paper they verify their conjecture for groups of polynomial growth.

Theorem. [AMV, Cor. 1.5] Let G be a finitely generated group of polynomial growth, and let S be a finite generating set for G. Then:

i) $\mathrm{dc}_S(G) > 0$ if and only if G is virtually abelian; and

ii) $dc_S(G) > 5/8$ if and only if G is abelian.

One of the key ingredients of their proof is a generalisation of Lemma 4.2.2 above.

Proposition 4.2.3. *[AMV, Prop. 2.3] Let G be a finitely generated subexponentially growing group, and let S be a finite generating system for G. Then, for any finite quotient G/N, we have*

$$\mathrm{dc}_S(G) \leqslant \mathrm{dc}(G/N).$$

They also produce a lower bound for $\mathrm{dc}_S(G)$, which is independent from the choice of S. Note that if $G = \langle S \rangle$ and $H \leqslant G$, then

$$\mathrm{dc}_S(H) := \limsup_{n\to\infty} \frac{|\{(a,b) \in (\mathbb{B}_S(n) \cap H)^2 : ab = ba\}|}{|\mathbb{B}_S(n) \cap H|^2}.$$

Lemma 4.2.4. *[AMV, proof of Thm. 1.3] Let G be a finitely generated polynomially growing group, $H \leqslant G$ a finite index subgroup, and take finite generating sets $G = \langle X \rangle$ and $H = \langle Y \rangle$. Then,*

$$\mathrm{dc}_X(G) \geqslant \frac{dc_X(H)}{[G:H]^2}.$$

In particular, $\mathrm{dc}_Y(H) > 0$ *implies* $\mathrm{dc}_X(G) > 0$.

They also verify their conjecture for hyperbolic groups.

An example: $\mathrm{dc}_S(D_\infty)$

Much of this section came about from a short meeting with my supervisor: many of the ideas are his. We will compute the degree of commutativity for D_∞, the infinite dihedral group, and show that the value we obtain is independent from the choice of finite generating set.

We first use Lemma 4.2.4 to produce a lower bound on $\mathrm{dc}_S(D_\infty)$ which does not depend on our choice of finite generating set. We note that $D_\infty \cong \mathbb{Z} \rtimes C_2$, and so it is virtually $\mathbb{Z}$. Thus

$$\mathrm{dc}_S(D_\infty) \geqslant \frac{1}{[D_\infty : \mathbb{Z}]^2} = \frac{1}{4}.$$

Note that, for every $n \in \mathbb{N}$, there exists a normal finite index subgroup U_n of D_∞ such that ${D_\infty}/{U_n} \cong D_n$. We will now compute $\mathrm{dc}(D_{2k})$ for all $k \in \mathbb{N}$ since Proposition 4.2.3 states, for all $k \in \mathbb{N}$, that

$$\mathrm{dc}_S(D_\infty) \leqslant \mathrm{dc}(D_\infty/U_{2k}) = \mathrm{dc}(D_{2k}).$$

Lemma 4.2.1 can now be used.

$$\mathrm{dc}(D_{2k}) = \frac{\#\text{ conjugacy classes of } G}{|G|}.$$

Computing the number of conjugacy classes for D_n is a common undergraduate exercise (with the main point being that the form of the answer depends on whether n is odd or even: this is why we restricted ourselves to the case where n is even). By direct computation, there will be a conjugacy class for the identity, k conjugacy classes of rotations, and 2 conjugacy classes for the reflections. Geometrically this occurs since each line of reflection either intersects two vertices or two edges of the n-gon. We can also see this algebraically. Let D_n be generated by a reflection b and a rotation a. Then

$$[b] = \{a^i b a^{-i} \mid i \in \mathbb{N}\} = \{a^i b a^{-i} b b \mid i \in \mathbb{N}\} = \{a^{2i} b \mid i \in \mathbb{N}\}$$

which is disjoint from the conjugacy class of $[ab]$, and so $[ab]$ can be the only other conjugacy class containing a reflection.

Thus D_{2k} has $k+3$ conjugacy classes. Hence, for all $k \in \mathbb{N}$,

$$\mathrm{dc}(D_{2k}) = \frac{k+3}{4k}.$$

This provides us with an upper bound of 1/4 for $\mathrm{dc}_S(D_\infty)$, which does not depend on the choice of finite generating set. Hence, for any finite generating set S,

$$\mathrm{dc}_S(D_\infty) = 1/4.$$

From this example, if G is virtually abelian, then the abelianization of G can be identified witha finite index subgroup of G. If we denote this by H then, for any finite set S which generates G, we have that

$$\mathrm{dc}_S(G) \geqslant \frac{1}{[G:H]^2}. \tag{11}$$

If [AMV, Conj. 1.6] is true, then only polynomial growing groups have non-zero degree of commutativity (since such groups are virtually $\mathbb{Z}^n$ for some $n \geqslant 0$). Thus (11) provides some evidence that the value of $\mathrm{dc}_S(G)$ does not depend on the choice for S. Note that the definition could be changed if it depends on the generating set to be the supremum or infimum over all finite generating sets, and that from the example above, Proposition 4.2.3 is sharp. There are a few other implications that follow from the conjecture being true. First, if $\mathrm{dc}(G) = 0$, then any finite extension or finite index subgroup of G also has degree of commutativity zero. Moreover, if $\mathrm{dc}(G) = 0$ and $G \leqslant H$, then $\mathrm{dc}(H) = 0$. If this last statement and the independence of $\mathrm{dc}_S(G)$ on S could be proved, then paper 3 would mean that any group of the form $G \wr H$ where G is non-trivial and H is not torsion would have degree of commutativity 0.

Other possible questions

We discuss the first two questions posed in paper 3. These relate to another possible formulation for defining the degree of commutativity for an infinite group. Let G be a finitely generated group and S be a finite generating set for G. Then

$$\hat{\mathrm{dc}}_S(G) := \limsup_{n\to\infty} \left(\frac{\text{the number of conjugacy classes meeting } \mathbb{B}_S(n)}{|\mathbb{B}_S(n)|} \right) \tag{12}$$

where the numerator is known as the *conjugacy growth function* of G with respect to S. It was first studied by Efremovich in [Efr53]. The definition can also be extended to groups which are not finitely generated, with [BdlH16] recently investigating the conjugacy growth series for FSym. Lemma 4.2.1 motivated the definition (12), since it stated a relationship between the degree of commutativity of a finite group and the number of conjugacy classes the finite group has. Natural questions are then whether the conjecture of [AMV, Conj. 1.6] holds and whether, for every finitely generated group G with finite generating set S, we have $\mathrm{dc}_S(G) = \hat{\mathrm{dc}}_S(G)$. We now compute $\hat{\mathrm{dc}}_{\{r,s\}}(D_\infty)$.

Example 4.2.5 (The Conjugacy Growth Function for D_∞)**.** We will work with a fixed presentation (unlike our work for $\mathrm{dc}_S(D_\infty)$ above). Let

$$D_\infty := \langle r, s \mid s^2, srs = r^{-1} \rangle$$

and let us write the elements of D_∞ using the standard normal form so that, as sets,

$$D_\infty = \{sr^k, r^k \mid k \in \mathbb{Z}\}.$$

Computing conjugate elements in this group is again an undergraduate level exercise. We note that $[s] = \{sr^{2i} \mid i \in \mathbb{Z}\}$, that $[sr] = \{sr^{2i+1} \mid i \in \mathbb{Z}\}$, and for all $k \in \mathbb{Z}$ that $[r^k] = [r^{-k}]$.

Using that $|\mathbb{B}_{\{r,s\}}(n) \cap \langle r \rangle| = 2n + 1$ and $|\mathbb{B}_{\{r,s\}}(n) \cap ([s] \cup [sr])| = 2n - 1$ we see that $f_{D_\infty,\{r,s\}}(n) = 4n$. The conjugacy growth function (when $n \geqslant 2$) is $n + 3$ by similar logic. Now the quotient of these functions is

$$\frac{n+3}{4n}$$

which approaches $\frac{1}{4}$ asymptomatically. Note that the same answer was found above when computing $\mathrm{dc}_S(D_\infty)$ using the definition of [AMV].

Translation Lengths

These are used in paper 3. Let G be a finitely generated group with finite generating set S and let $g \in G$. Then

$$\tau_S(g) := \limsup_{n \to \infty} \frac{|g^n|_S}{n} \tag{13}$$

are the *translation lengths* of G with respect to S.

We first recall Fekete's Lemma, which is of great use in this field. A sequence $\{a_i\}_{i \in \mathbb{N}}$ is *subadditive* if, for all $m, n \in \mathbb{N}$, $a_{n+m} \leqslant a_n + a_m$. Note that (13) provides a subadditive sequence by setting $a_i := |g^i|_S$ for each $i \in \mathbb{N}$.

Lemma 4.2.6 ([Fek23]). *Let $\{a_i\}_{i\in\mathbb{N}}$ be a subadditive sequence. Then $\lim_{n\to\infty}\frac{a_n}{n}$ exists and is equal to $\inf\frac{a_n}{n}$.*

Thus (13) is a real limit and we need only consider the infimum of the sequence. Obvious questions are whether the set $\{\tau_S(g) \mid g \in G\}$ contains points in $\mathbb{R}\setminus\mathbb{Q}$, whether the non-zero points are uniformly bounded away from 0, and the structure of such a set for a particular group or families of groups. These questions have been investigated by Conner (for example in [Con97] and [Con98]). We now prove a result which is remarked upon in paper 3.

Lemma 4.2.7. *Let S' be a finite generating set for a group H such that $\tau_{S'}(H) \subseteq \mathbb{N}\cup\{0\}$. If S is a generating set for $H\wr\mathbb{Z}$ consisting of the generating set S' for H_0 and a generator of the head of $H\wr\mathbb{Z}$, then $\tau_S(H\wr\mathbb{Z}) \subseteq \mathbb{N}$.*

Proof. Let B denote the base of $H\wr\mathbb{Z}$. If $h \in B$, then

$$h \in \bigoplus_{i\in I} H_i$$

where $|I|$ is finite and so $\tau_S(h) \in \mathbb{N}\cup\{0\}$. Now consider $g \in (H\wr\mathbb{Z})\setminus B$, and let $g = wt^k$ where $k \in \mathbb{N}$ (the case where k is negative follows since we always have that $\tau_S(g) = \tau_S(g^{-1})$). Thus

$$w = \prod_{i\in I} a_i \tag{14}$$

where $|I|$ finite and, for each $i \in I$, we have that $a_i \in H_i$. Without loss of generality we may assume that $\min\{I\} = 0$ since

$$\lim_{n\to\infty}\frac{|g|_S}{n} = \lim_{n\to\infty}\frac{|t^{-d}g^n t^d|_S}{n}$$

for any $d \in \mathbb{Z}$.

We first deal with the case where $I \subseteq \{0,1,\ldots,k-1\}$. In this case, from (14), we have that I and It^k are disjoint. Hence

$$nk + n\left(\sum_{i\in I}|a_i|_{S'}\right) \leqslant |g^n|_S \leqslant nk + n\left(\sum_{i\in I}|a_i|_{S'}\right) + 2k$$

meaning that $\tau_S(g) = k + \sum_{i\in I}|a_i|_{S'}$, which is in $\mathbb{N}$ from our hypotheses.

Now let $g = wt^k$ with

$$w = \prod_{i\in I} a_i$$

where, for each $i \in I$, $a_i \in H_i$ and $\max\{I\} \geqslant k$. Let $I' := \{0, 1, \ldots, k-1\}$ and let $j \in I \setminus I'$. Then $j = j' + dk$ for some $j' \in I'$ and $d \in \mathbb{N}$. Consider

$$w' := \left(\prod_{i \in I \setminus \{j\}} a_i \right) a_{j'}.$$

Our claim is that $\tau_S(w't^k) = \tau_S(wt^k)$. This can be seen, for example, by the fact that

$$\lim_{n\to\infty} \frac{|(w't^k)^n|_S}{n} \leqslant \lim_{n\to\infty} \frac{|(wt^k)^n|_S}{n} \leqslant \lim_{n\to\infty} \frac{|(w't^k)^n|_S + 2dk}{n}. \qquad \square$$

Example. We consider the group $C_2 \wr \mathbb{Z}$ with generating set S consisting of a generator of the C_2 located at the vertex 0 and a generator of the head of $C_2 \wr \mathbb{Z}$. Let $g = wt^2$ where $\mathrm{supp}(w) = \{(0, i), (1, i) \mid i = 0, 2, 3\}$. Computing powers of g one sees that there is much cancellation. This corresponds to the fact that, for all $n \in \mathbb{N}$, g^n is close (in the sense of the metric from $\mathrm{Cay}(G, S)$) to the element $(g')^n$, where $g' := w't^2$ and $\mathrm{supp}(w') = \{(0, 1), (1, 1)\}$.

The previous lemma can in fact be extended. Without any hypotheses on the translation lengths of H we have that $\tau_{S'}(H \wr \mathbb{Z} \setminus B) = \mathbb{N}$, where B denotes the base of $H \wr \mathbb{Z}$. If $\tau_{S'}(H \setminus \{1\})$ is uniformly bounded away from 0, then so is $\tau_S(H \wr \mathbb{Z} \setminus \{1\})$. Finally, if $\tau_{S'}(H) \subseteq \mathbb{Q}$ for some finite generating set S' of H, then, using the generating set S from the lemma above, $\tau_S(H \wr \mathbb{Z}) \subseteq \mathbb{Q}$.

4.2.1 Author's note

In paper 1 and paper 2, it is useful to consider permutations restricted to a particular set. This can be achieved in two different ways. Given $g \in \mathrm{Sym}(X)$ and a subset Y of X such that $Yg = Y$, we could interpret $g|Y$ as either: the element of $\mathrm{Sym}(X)$ which fixes all points in $X \setminus Y$; or the element of $\mathrm{Sym}(Y)$ which acts as g on the set Y. The notation $g|Y$ is given the first meaning in paper 1 and the second meaning in paper 2.

Bibliography

[AAG99] Iris Anshel, Michael Anshel, and Dorian Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), no. 3-4, 287–291. MR 1713130

[Abd16] Ali Abdallah, *Public key cryptography based on some extensions of group*, arXiv:1604.04474 (2016).

[ABM15] Y. Antolín, J. Burillo, and A. Martino, *Conjugacy in Houghton's groups*, Publ. Mat. **59** (2015), no. 1, 3–16. MR 3302573

[Ady55] S. I. Adyan, *Algorithmic unsolvability of problems of recognition of certain properties of groups*, Dokl. Akad. Nauk SSSR (N.S.) **103** (1955), 533–535. MR 0081851

[AGG05] G. N. Arzhantseva, V. S. Guba, and L. Guyot, *Growth rates of amenable groups*, J. Group Theory **8** (2005), no. 3, 389–394. MR 2137976

[AMV] Y. Antolín, A. Martino, and E. Ventura, *Degree of commutativity of infinite groups*, Proceedings of the American Mathematical Society (to appear).

[Bau93] Gilbert Baumslag, *Topics in combinatorial group theory*, Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 1993. MR 1243634

[BB14] Oleg Bogopolski and Kai-Uwe Bux, *Subgroup conjugacy separability for surface groups*, arXiv:1401.6203 (2014).

[BCMR14] J. Burillo, S. Cleary, A. Martino, and C. E. Röver, *Commensurations and Metric Properties of Houghton's Groups*, arXiv:1403.0026 (2014).

[BdlH16] Roland Bacher and Pierre de la Harpe, *Conjugacy growth series of some infinitely generated groups*, arXiv:1603.07943 (2016).

[BFGJ05] R. F. Brown, M. Furi, L. Górniewicz, and B. Jiang (eds.), *Handbook of topological fixed point theory*, Springer, Dordrecht, 2005. MR 2170491

[BH15] T. Banakh and M. Heike, *Cardinal invariants distinguishing permutation groups*, arXiv:1506.08969 (2015).

[BMV10] O. Bogopolski, A. Martino, and E. Ventura, *Orbit decidability and the conjugacy problem for some extensions of groups*, Trans. Amer. Math. Soc. **362** (2010), no. 4, 2003–2036. MR 2574885 (2011e:20045)

[Bog08] Oleg Bogopolski, *Introduction to group theory*, EMS Textbooks in Mathematics, European Mathematical Society (EMS), Zürich, 2008, Translated, revised and expanded from the 2002 Russian original. MR 2396717

[Boo59] William W. Boone, *The word problem*, Ann. of Math. (2) **70** (1959), 207–265. MR 0179237 (31 #3485)

[BT15] Michelle Bucher and Alexey Talambutsa, *Minimal exponential growth rates of metabelian Baumslag-Solitar groups and lamplighter groups*, arXiv:1506.03569 (2015).

[Cam99] Peter J. Cameron, *Permutation groups*, LMS Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999. MR 1721031 (2001c:20008)

[CM71] Donald J. Collins and Charles F. Miller, III, *On group-theoretic decision problems and their classification*, 1971, Annals of Mathematics Studies, No. 68. MR 0310044 (46 #9147)

[Col72] Donald J. Collins, *Representation of Turing reducibility by word and conjugacy problems in finitely presented groups*, Acta Math. **128** (1972), no. 1-2, 73–90. MR 0392539

[Con97] Gregory R. Conner, *A class of finitely generated groups with irrational translation numbers*, Arch. Math. (Basel) **69** (1997), no. 4, 265–274. MR 1466819

[Con98] ———, *Properties of translation numbers in nilpotent groups*, Comm. Algebra **26** (1998), no. 4, 1069–1080. MR 1612184

[Coo04] S. Barry Cooper, *Computability theory*, Chapman & Hall/CRC, Boca Raton, FL, 2004. MR 2017461

[Cox14] C. Cox, *Twisted Conjugacy in Houghton's groups*, arXiv:1410.7051 (2014).

[Cox16a] ———, *A note on the R_∞ property for groups* $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$, arXiv:1602.02688 (Feb. 2016).

[Cox16b] ———, *The degree of commutativity and lamplighter groups*, arXiv:1605.04829 (May 2016).

[CT05] Sean Cleary and Jennifer Taback, *Dead end words in lamplighter groups and other wreath products*, Q. J. Math. **56** (2005), no. 2, 165–178. MR 2143495

[Deg00] F. Degenhardt., *Endlichkeitseigenschaften gewisser Gruppen zon Zöpfen unendlicher Ordnung*, PhD Thesis, Frankfurt (2000).

[DG11] François Dahmani and Vincent Guirardel, *The isomorphism problem for all hyperbolic groups*, Geom. Funct. Anal. **21** (2011), no. 2, 223–300. MR 2795509

[DM96] John D. Dixon and Brian Mortimer, *Permutation groups*, Grad. Texts in Math., vol. 163, Springer-Verlag, New York, 1996. MR 1409812 (98m:20003)

[Dys64] V.H. Dyson, *The word problem and residually finite groups*, Notices Amer. Math. Soc 11 **743** (1964).

[Efr53] V.A. Efremovich, *The proximity geometry of Riemannian manifolds (Russian)*, Uspekhi Mat. Nauk **8** (1953), 189.

[ET68] P. Erdős and P. Turán, *On some problems of a statistical group-theory. IV*, Acta Math. Acad. Sci. Hungar **19** (1968), 413–435. MR 0232833

[Fek23] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. **17** (1923), no. 1, 228–249. MR 1544613

[Fel10] Alexander Fel'shtyn, *New directions in Nielsen-Reidemeister theory*, Topology Appl. **157** (2010), no. 10-11, 1724–1735. MR 2639839

[Fen14] Tony Feng, *Topics in infinite groups*, 2014, (Lectures by Jack Button).

[FH94] Alexander Fel′shtyn and Richard Hill, *The Reidemeister zeta function with applications to Nielsen theory and a connection with Reidemeister torsion*, K-Theory **8** (1994), no. 4, 367–393. MR 1300546

[Gal71] P. X. Gallagher, *The number of conjugacy classes in a finite group*, Representation theory of finite groups and related topics (Proc. Sympos. Pure Math., Vol. XXI, Univ. Wisconsin, Madison, Wis., 1970), Amer. Math. Soc., Providence, R.I., 1971, pp. 51–52. MR 0314955

[GK75] A. V. Gorjaga and A. S. Kirkinskiĭ, *The decidability of the conjugacy problem cannot be transferred to finite extensions of groups*, Algebra i Logika **14** (1975), no. 4, 393–406. MR 0414718 (54 #2813)

[GP14] D. Gonçalves and S. Parameswaran, *Sigma theory and twisted conjugacy-II: Houghton groups and pure symmetric automorphism groups*, arXiv:1412.8048 (2014).

[Gri84] R. I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), no. 5, 939–985. MR 764305

[Gro81a] Mikhael Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 53, 53–73. MR 623534

[Gro81b] ______, *Structures métriques pour les variétés riemanniennes*, Textes Mathématiques [Mathematical Texts], vol. 1, CEDIC, Paris, 1981, Edited by J. Lafontaine and P. Pansu. MR 682063

[GS10] Victor Guba and Mark Sapir, *On the conjugacy growth functions of groups*, Illinois J. Math. **54** (2010), no. 1, 301–313. MR 2776997

[Gus73] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034. MR 0327901

[GW03] D. Gonçalves and P. Wong, *Twisted conjugacy classes in exponential growth groups*, Bull. London Math. Soc. **35** (2003), no. 2, 261–268. MR 1952405

[GW06] Daciberg Gonçalves and Peter Wong, *Twisted conjugacy classes in wreath products*, Internat. J. Algebra Comput. **16** (2006), no. 5, 875–886. MR 2274719

[Hig61] G. Higman, *Subgroups of finitely presented groups*, Proc. Roy. Soc. Ser. A **262** (1961), 455–475. MR 0130286

[HO15] M. Hull and D. Osin, *Transitivity degrees of countable groups and acylindrical hyperbolicity*, arXiv:1501.04182 (2015).

[Jia83] Bo Ju Jiang, *Lectures on Nielsen fixed point theory*, Contemporary Mathematics, vol. 14, American Mathematical Society, Providence, R.I., 1983. MR 685755

[KM16] P. H. Kropholler and A. Martino, *Graph-wreath products and finiteness conditions*, J. Pure Appl. Algebra **220** (2016), no. 1, 422–434. MR 3393469

[KMM12] O. Kharlampovich, A. Myasnikov, and Sapir M., *Algorithmically complex residually finite groups*, arXiv:1204.6506 (2012).

[KT76] KT, *Kourovka notebook. unsolved problems in group theory.*, 5th ed., 1976, Novosibirsk.

[LPP96] Russell Lyons, Robin Pemantle, and Yuval Peres, *Random walks on the lamplighter group*, Ann. Probab. **24** (1996), no. 4, 1993–2006. MR 1415237

[LS01] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2001, Reprint of the 1977 edition.

[Mal58] A. I. Mal'cev, *On homomorphisms onto finite groups (Russian)*, Uchen. Zap. Ivanovskogo Gos. Ped. Inst. **18** (1958), 49–60.

[Mar47] A. Markoff, *On the impossibility of certain algorithms in the theory of associative systems*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **55** (1947), 583–586. MR 0020528

[Mat66] Jane Matthews, *The conjugacy problem in wreath products and free metabelian groups*, Trans. Amer. Math. Soc. **121** (1966), 329–339. MR 0193130

[Mat06] Francesco Matucci, *Cryptanalysis of the Shpilrain-Ushakov Protocol in Thompson's Group*, arXiv:math/0607184 (2006).

[McK43] J. C. C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, J. Symbolic Logic **8** (1943), 61–76. MR 0008991

[Mil92] Charles F. Miller, III, *Decision problems for groups—survey and reflections*, Alg. and class. in comb. group theory (Berkeley, CA, 1989), Math. Sci. Res. Inst. Publ., vol. 23, Springer, New York, 1992, pp. 1–59. MR 1230627

[Min12] Ashot Minasyan, *Hereditary conjugacy separability of right-angled Artin groups and its applications*, Groups Geom. Dyn. **6** (2012), no. 2, 335–388. MR 2914863

[MO11] Alexei Miasnikov and Denis Osin, *Algorithmically finite groups*, J. Pure Appl. Algebra **215** (2011), no. 11, 2789–2796. MR 2802165

[Mos66] A. Włodzimierz Mostowski, *On the decidability of some problems in special classes of groups*, Fund. Math. **59** (1966), 123–135. MR 0224693

[Nov55] P. S. Novikov, *Ob algoritmičeskoĭ nerazrešimosti problemy toždestva slov v teorii grupp*, Trudy Mat. Inst. im. Steklov. no. 44, Izdat. Akad. Nauk SSSR, Moscow, 1955. MR 0075197 (17,706b)

[OS05] Alexander Yu. Olshanskii and Mark V. Sapir, *Subgroups of finitely presented groups with solvable conjugacy problem*, Internat. J. Algebra Comput. **15** (2005), no. 5-6, 1075–1084. MR 2197822

[Par92] Walter Parry, *Growth series of some wreath products*, Trans. Amer. Math. Soc. **331** (1992), no. 2, 751–759. MR 1062874

[Pos47] Emil L. Post, *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic **12** (1947), 1–11. MR 0020527

[PS12] V. Ponomarenko and N. Selinski, *Two semigroup elements can commute with any positive rational probability*, College Mathematics Journal **43(4)** (2012).

[Rab58] Michael O. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. of Math. (2) **67** (1958), 172–194. MR 0110743

[Rot95] J. J. Rotman, *An introduction to the theory of groups*, 4th ed., Grad. Texts in Math., Springer-Verlag, New York, 1995. MR 1307623 (95m:20001)

[Sco87] W. R. Scott, *Group theory*, second ed., Dover Publications, Inc., New York, 1987. MR 896269 (88d:20001)

[Ser03] Jean-Pierre Serre, *Trees*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, Translated from the French original by John Stillwell. MR 1954121 (2003m:20032)

[SU05] V. Shpilrain and A. Ushakov., *Thompson's group and public key cryptography*, ACNS 2005 **3531** (2005), 151–163.

[TW06] Jennifer Taback and Peter Wong, *A note on twisted conjugacy and generalized baumslag-solitar groups*, arXiv:math/0606284 (2006).

[Wil04] John S. Wilson, *On exponential growth and uniformly exponential growth for groups*, Invent. Math. **155** (2004), no. 2, 287–303. MR 2031429

TWISTED CONJUGACY IN HOUGHTON'S GROUPS

CHARLES GARNET COX

Abstract. For a fixed $n \geqslant 2$, the Houghton group H_n consists of bijections of $X_n = \{1, \ldots, n\} \times \mathbb{N}$ that are 'eventually translations' of each copy of $\mathbb{N}$. The Houghton groups have been shown to have solvable conjugacy problem. In general, solvable conjugacy problem does not imply that all finite extensions and finite index subgroups have solvable conjugacy problem. Our main theorem is that a stronger result holds: for any $n \geqslant 2$ and any group G commensurable to H_n, G has solvable conjugacy problem.

1. Introduction

Given a presentation $\langle S \mid R \rangle = G$, a 'word' in G is an ordered f-tuple $a_1 \ldots a_f$ with $f \in \mathbb{N}$ and each $a_i \in S \cup S^{-1}$. Dehn's problems and their generalisations (known as decision problems) ask seemingly straightforward questions about finite presentations. The problems that we shall consider include:

- the *word problem* for G, denoted WP(G): show there exists an algorithm which given two words $a, b \in G$, decides whether $a =_G b$ or $a \neq_G b$ i.e. whether these words represent the same element of the group. This is equivalent to asking whether or not $ab^{-1} =_G 1$. There exist finitely presented groups where this problem is undecidable (see [Nov58] or [Boo59]).
- the *conjugacy problem* for G, denoted CP(G): show there exists an algorithm which given two words $a, b \in G$, decides whether or not there exists an $x \in G$ such that $x^{-1}ax = b$. As 1_G has its own conjugacy class, if CP(G) is solvable then so is WP(G). CP(G) is strictly weaker than WP(G) since there exist groups where WP(G) is solvable but CP(G) is not (e.g. see [Mil71]).
- the *ϕ-twisted conjugacy problem* for G, denoted $\mathrm{TCP}_\phi(G)$: show there exists an algorithm which for a fixed $\phi \in \mathrm{Aut}(G)$ and any two words $a, b \in G$, decides whether or not there exists an $x \in G$ such that $(x^{-1})\phi a x = b$ (meaning that a is ϕ-twisted conjugate to b). Note that $\mathrm{TCP}_{Id}(G)$ is CP(G).
- the *(uniform) twisted conjugacy problem* for G, denoted TCP(G): show there exists an algorithm which given a $\phi \in \mathrm{Aut}(G)$ and two words $a, b \in G$, decides whether or not they are ϕ-twisted conjugate. There exist groups G such that CP(G) is solvable but TCP(G) is not (e.g. see [BMV10]).

Should any of these problems be solved for one finite presentation, then they may be solved for any other finite presentation of that group. We therefore say

Date: July 9, 2016.

2010 *Mathematics Subject Classification.* Primary: 20F10, 20B99.

Key words and phrases. uniform twisted conjugacy problem, Houghton group, permutation group, orbit decidability, conjugacy problem for commensurable groups.

that such problems are solvable if an algorithm exists for one such presentation. Many decision problems may also be considered for any group that is recursively presented.

We say that G is a finite extension of H if $H \trianglelefteq G$ and H is finite index in G. If $\mathrm{CP}(G)$ is solvable, then we do not have that finite index subgroups of G or finite extensions of G have solvable conjugacy problem, even if these are of degree 2. Explicit examples can be found for both cases (see [CM77] or [GK75]). Thus it is natural to ask, if $\mathrm{CP}(G)$ is solvable, whether the conjugacy problem holds for finite extensions and finite index subgroups of G. The groups we investigate in this paper are Houghton groups (denoted H_n with $n \in \mathbb{N}$).

Theorem 1. *Let $n \geqslant 2$. Then TCP(H_n) is solvable.*

We say that two groups A and B are commensurable if there exists $N_A \cong N_B$ where N_A is normal and finite index in A and N_B is normal and finite index in B.

Theorem 2. *Let $n \geqslant 2$. Then, for any group G commensurable to H_n, CP(G) is solvable.*

We structure the paper as follows. In Section 2 we introduce the Houghton groups, make some simple observations for them, and reduce $\mathrm{TCP}(H_n)$ to a problem similar to $\mathrm{CP}(H_n \rtimes S_n)$, the difference being that, given $a, b \in H_n \rtimes S_n$, we are searching for a conjugator $x \in H_n$. This occurs since, for all $n \geqslant 2$, $H_n \rtimes S_n \cong \mathrm{Aut}(H_n)$. In Section 3 we describe the orbits of elements of $H_n \rtimes S_n$ and produce identities that a conjugator of elements in $H_n \rtimes S_n$ must satisfy. These are then used in Section 4 to reduce our problem of finding a conjugator in H_n to finding a conjugator in the subgroup of H_n consisting of all finite permutations (which we denote by FSym, see Notation 2.1 below). Constructing such an algorithm provides us with Theorem 1. In Section 5 we use Theorem 1 and [BMV10, Thm. 3.1] to prove our main result, Theorem 2.

Acknowledgements. I thank the authors of [ABM13] whose work is drawn upon extensively. I especially thank the author Armando Martino, my supervisor, for his encouragement and the many helpful discussions which have made this work possible. I thank Peter Kropholler for his suggested extension which developed into Theorem 2. Finally, I thank the referee for their many helpful comments.

2. Background

As with the authors of [ABM13], the author does not know of a class that contains the Houghton groups and for which the conjugacy problem has been solved.

2.1. **Houghton's groups.** Throughout we shall consider $\mathbb{N} := \{1, 2, 3, \ldots\}$. For convenience, let $\mathbb{Z}_n := \{1, \ldots, n\}$. For a fixed $n \in \mathbb{N}$, let $X_n := \mathbb{Z}_n \times \mathbb{N}$. Arrange these n copies of $\mathbb{N}$ as in Figure 1 below (so that the k^{th} point from each copy of $\mathbb{N}$ form the vertices of a regular n-gon). For any $i \in \mathbb{Z}_n$, we will refer to the set $i \times \mathbb{N}$ as a *branch* or *ray* and will let (i, m) denote the m^{th} point on the i^{th} branch.

Notation 2.1. *For a non-empty set X, the set of all permutations of X form a group which we denote* $\mathrm{Sym}(X)$*. Those permutations which have finite support (i.e. move finitely many points) form a normal subgroup which we will denote* $\mathrm{FSym}(X)$*. If there is no ambiguity for X, then we will write just* Sym *or* FSym *respectively.*

Note that, if X is countably infinite, then $\mathrm{FSym}(X)$ is countably infinite but is not finitely generated, and $\mathrm{Sym}(X)$ is uncountable and so uncountably generated.

Definition 2.2. Let $n \in \mathbb{N}$. The n^{th} *Houghton group*, denoted H_n, is a subgroup of $\mathrm{Sym}(X_n)$. An element $g \in \mathrm{Sym}(X_n)$ is in H_n if and only if there exist constants $z_1(g), \ldots, z_n(g) \in \mathbb{N}$ and $(t_1(g), \ldots, t_n(g)) \in \mathbb{Z}^n$ such that, for all $i \in \mathbb{Z}_n$,

$$(i, m)g = (i, m + t_i(g)) \text{ for all } m \geqslant z_i(g). \tag{1}$$

For simplicity, the numbers $z_1(g), \ldots, z_n(g)$ are assumed to be minimal i.e. for any $m' < z_i(g)$, $(i, m')g \neq (i, m' + t_i(g))$. The vector $t(g) := (t_1(g), \ldots, t_n(g))$ represents the 'eventual translation length' for each g in H_n since $t_i(g)$ specifies how far g moves the points $\{(i, m) \mid m \geqslant z_i(g)\}$. We shall say that these points are those which are 'far out', since they are the points where g acts in the regular way described in (1). As g induces a bijection from X_n to X_n, we have that

$$\sum_{i=1}^{n} t_i(g) = 0. \tag{2}$$

Given $g \in H_n$, the numbers $z_i(g)$ may be arbitrarily large. Thus $\mathrm{FSym}(X_n) \leqslant H_n$. Also, for any $n \geqslant 2$, we have (as proved in [Wie77]) the short exact sequence

$$1 \longrightarrow \mathrm{FSym}(X_n) \longrightarrow H_n \longrightarrow \mathbb{Z}^{n-1} \longrightarrow 1 \tag{3}$$

where the homomorphism $H_n \to \mathbb{Z}^{n-1}$ is given by $g \mapsto (t_1(g), \ldots, t_{n-1}(g))$.

These groups were introduced in [Hou78] for $n \geqslant 3$. The standard generating set that we will use when $n \geqslant 3$ is $\{g_2, g_3, \ldots, g_n\}$ where for each i,

$$(j, m)g_i = \begin{cases} (1, m+1) & \text{if } j = 1 \\ (1, 1) & \text{if } j = i, m = 1 \\ (i, m-1) & \text{if } j = i, m > 1 \\ (j, m) & \text{otherwise.} \end{cases} \tag{4}$$

Notice that for each i, we have $t_1(g_i) = 1$ and $t_j(g_i) = -\delta_{i,j}$ for $j \in \{2, \ldots, n\}$. Figure 1 shows a geometric visualisation of $g_2, g_4 \in H_5$. Throughout we shall take the vertical ray as the 'first ray' (the set of points $\{(1, m) \mid m \in \mathbb{N}\}$) and order the other rays clockwise.

We shall now see that, for any $n \geqslant 3$, the set $\{g_i \mid i = 2, \ldots, n\}$ generates H_n. First, any valid eventual translation lengths (those satisfying (2)) can be obtained by these generators. Secondly, the commutator (which we define as $[g, h] := g^{-1}h^{-1}gh$ for every g, h in G) of any two distinct elements $g_i, g_j \in H_n$ is a 2-cycle, and so conjugation of this 2-cycle by some combination of g_k's will produce a 2-cycle with support equal to any two points of X_n. This is enough to produce any element that is 'eventually a translation' i.e. one that satisfies condition (1), and so is enough to generate all of H_n. An explicit finite presentation for H_3 can be found in [Joh99], and this was generalised in [Lee12] by providing finite presentations for H_n for all $n > 3$.

We now describe H_1 and H_2. If $g \in H_1$, then $t_1(g) = 0$ (since the eventual translation lengths of g must sum to 0 by condition (2)) and so $H_1 = \mathrm{FSym}(\mathbb{N})$. For H_2 we have $\langle g_2 \rangle \cong \mathbb{Z}$. Using a conjugation argument similar to the one above, it can be seen that a suitable generating set for H_2 is $\{g_2, ((1, 1)\ (2, 1))\}$. These definitions of H_1 and H_2 agree with the result for H_n in [Bro87], that (for $n \geqslant 3$) each H_n is FP_{n-1} but not FP_n i.e. H_1 is not finitely generated and H_2 is finitely generated

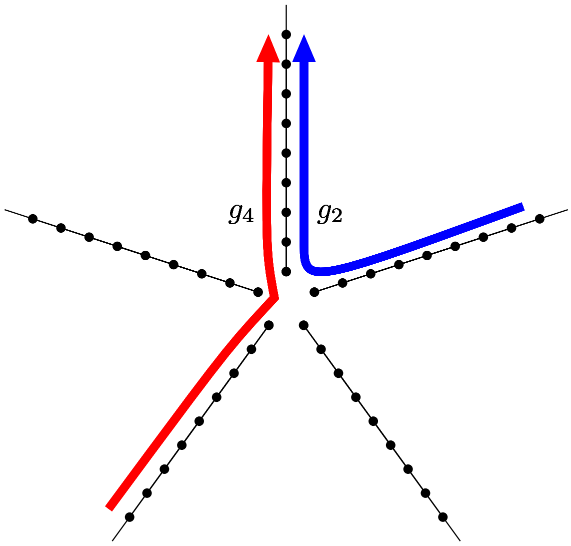


FIGURE 1. Part of the set X_5 and a geometrical representation of the action of the standard generators $g_2, g_4 \in H_5$.

but not finitely presented. Since $H_1 = \mathrm{FSym}(\mathbb{N})$ and $\mathrm{Aut}(\mathrm{FSym}(\mathbb{N})) \cong \mathrm{Sym}(\mathbb{N})$ (see, for example, [DM96] or [Sco87]) we will work with H_n where $n \geqslant 2$.

2.2. **A reformulation of TCP(H_n).** We require knowledge of $\mathrm{Aut}(H_n)$. We noted above that $\mathrm{Aut}(H_1) \cong \mathrm{Sym}(\mathbb{N})$, and so will work with $n \geqslant 2$.

Notation. *Let $g \in \mathrm{Sym}(X)$. Then $(h)\phi_g := g^{-1}hg$ for all $h \in G$.*

From [BCMR14], we have for all $n \geqslant 2$ that $N_{\mathrm{Sym}(X_n)}(H_n) \cong \mathrm{Aut}(H_n)$ via the map $\rho \mapsto \phi_\rho$ and that $N_{\mathrm{Sym}(X_n)}(H_n) \cong H_n \rtimes S_n$. We will make an abuse of notation and consider $H_n \rtimes S_n$ as acting on X_n via the natural isomorphism $N_{\mathrm{Sym}(X_n)}(H_n) \leqslant \mathrm{Sym}(X_n)$. Here $\mathrm{Inn}(H_n) \cong H_n$ because H_n is centreless, and S_n acts on X_n by isometrically permuting the rays, where $g \in H_n \rtimes S_n$ is an isometric permutation of the rays if and only if there exists a $\sigma \in S_n$ such that $(i,m)g = (i\sigma, m)$ for all $m \in \mathbb{N}$ and all $i \in \mathbb{Z}_n$.

Notation. *For any given $g \in H_n \rtimes S_n$, let $\Psi : H_n \rtimes S_n \to S_n$, $g \mapsto \sigma_g$ where σ_g denotes the isometric permutation of the rays induced by g. Furthermore, let $\omega_g := g\sigma_g^{-1}$. Thus, for any $g \in H_n \rtimes S_n$, we have $g = \omega_g\sigma_g$ and will consider $\omega_g \in H_n$ and $\sigma_g \in S_n$. We shall therefore consider any element g of $H_n \rtimes S_n$ as a permutation of X_n which is eventually a translation (denoted ω_g) followed by an isometric permutation of the rays σ_g.*

Definition 2.3. Let $G \leqslant H_n \rtimes S_n$ and $g, h \in H_n \rtimes S_n$. Then we shall say g and h are G-conjugated if there is an $x \in G$ such that $x^{-1}gx = h$.

We now relate twisted conjugacy in H_n to conjugacy in $H_n \rtimes S_n$. Let $c \in H_n \rtimes S_n$. Then the equation for ϕ_c-twisted conjugacy becomes:

$$(x^{-1})\phi_c gx = h \Rightarrow c^{-1}x^{-1}cgx = h \Rightarrow x^{-1}(\omega_c\sigma_c g)x = \omega_c\sigma_c h.$$

Thus, for any $n \geqslant 2$, two elements $g, h \in H_n$ are ϕ_c-twisted conjugate if and only if $\omega_c\sigma_c g$ and $\omega_c\sigma_c h \in H_n \rtimes S_n$ are H_n-conjugated. Note that, if $g, h \in H_n \rtimes S_n$

are H_n-conjugated, then $\sigma_g = \sigma_h$. Thus for the remainder of this note a and b will refer to the elements in $H_n \rtimes S_n$ that we wish to decide are H_n-conjugated, where $\sigma_a = \sigma_b$. In order to solve TCP(H_n), we will therefore produce an algorithm to search for an $x \in H_n$ which conjugates a to b.

3. Computations in $H_n \rtimes S_n$

Our first lemma provides the generating set that we will use for $H_n \rtimes S_n$.

Lemma 3.1. *Let $n \geqslant 2$. Then $H_n \rtimes S_n$ can be generated by 3 elements.*

Proof. If $n \geqslant 3$, two elements can be used to generate all of the isometric permutations of the rays. Our third generator will be g_2, the standard generator for H_n. Conjugating g_2 by the appropriate isometric permutations of the rays produces the set $\{g_i \mid i = 2, \dots, n\}$, which can then be used to generate all permutations in H_n. For $H_2 \rtimes S_2$ we note that H_2 is 2-generated and that S_2 is cyclic. □

3.1. **The orbits of elements in $H_n \rtimes S_n$.** Our main aim for this section is to describe the orbits of any element $g \in H_n \rtimes S_n$ 'far out'. For elements of H_n, any element eventually acted like a translation. In a similar way, any element of $H_n \rtimes S_n$ eventually moves points in a uniform manner. More specifically, $g \in \mathrm{Sym}(X_n)$ is in $H_n \rtimes S_n$ if and only if there exist constants $z_1(g), \dots, z_n(g) \in \mathbb{N}$, $(t_1(g), \dots, t_n(g)) \in \mathbb{Z}^n$, and a permutation $\sigma \in S_n$ such that for all $i \in \mathbb{Z}_n$

$$(i, m)g = (i\sigma, m + t_i(g)) \text{ for all } m \geqslant z_i(g). \tag{5}$$

If $g \in H_n \rtimes S_n$, then $g = \omega_g \sigma_g$. Therefore for any $g \in H_n \rtimes S_n$, σ_g (the isometric permutation of the rays induced by g) will induce the permutation denoted σ in (5), we have that $t_i(\omega_g) = t_i(g)$ for all $i \in \mathbb{Z}_n$, and $z_1(\omega_g), \dots, z_n(\omega_g)$ are suitable values for the constants $z_1(g), \dots, z_n(g)$.

Definition 3.2. Let $g \in H_n \rtimes S_n$ and $i \in \mathbb{Z}_n$. Then a *class* of σ_g, denoted $[i]_g$, is the support of the disjoint cycle of σ_g which contains i i.e. $[i]_g = \{i\sigma_g^d \mid d \in \mathbb{Z}\}$. Additionally, we define the *size* of a class $[i]_g$ to be the length of the cycle of σ_g containing i, i.e. the cardinality of the set $[i]_g$, and denote this by $|[i]_g|$.

We shall choose $z_1(g), \dots, z_n(g) \in \mathbb{N}$ to be the smallest numbers such that

$$(i, m)g^d = (i\sigma_g^d, m + \sum_{s=0}^{d-1} t_{i\sigma_g^s}(g)) \text{ for all } m \geqslant z_i(g) \text{ and all } 1 \leqslant d \leqslant |[i]_g|. \tag{6}$$

Note that, for any $g \in H_n \rtimes S_n$ and all $i \in \mathbb{Z}_n$, we have $z_i(g) \geqslant z_i(\omega_g)$. We now justify the introduction of condition (6). Consider a $g \in H_n \rtimes S_n$, $i \in \mathbb{Z}_n$, and $m \in \mathbb{N}$ such that

$$z_i(\omega_g) \leqslant m < z_i(g) \text{ and } m + t_i(\omega_g) < z_{i\sigma_g}(\omega_g).$$

This would mean $(i, m)g = (i\sigma_g, m + t_i(\omega_g))$, but it may also be that

$$(i, m)g^2 = (i\sigma_g, m + t_i(g))g \neq (i\sigma_g^2, m + t_i(g) + t_{i\sigma_g}(g)).$$

Thus the condition (6) above means that, for any $g \in H_n \rtimes S_n$, the numbers $z_1(g), \dots, z_n(g)$ capture the 'eventual' way that g permutes the points of a ray.

Let us fix some $g \in H_n \rtimes S_n$. Consider if σ_g acts trivially on a particular branch i'. This will mean that this branch has orbits like those occurring for elements of

H_n. If $t_{i'}(g) = 0$, then g leaves all but a finite number of points on this branch fixed. If $t_{i'}(g) \neq 0$, then for any given $m' > z_{i'}(g)$,

$$\{(i', m')g^d \mid d \in \mathbb{Z}\} \supset \{(i', m) \mid m \geqslant m' \text{ and } m \equiv m' \bmod |t_{i'}(g)|\}.$$

Notice that, for any $g \in H_n \rtimes S_n$, the σ_g-classes form a partition of $\mathbb{Z}_n$, relating to the branches of X_n. We now consider the case $|[k]_g| > 1$. We first note, for any $i \in [k]_g$ and $m_1 \geqslant z_i(g)$, that

$$(i, m_1)g^{|[k]_g|} \in \{(i, m) \mid m \in \mathbb{N}\} \tag{7}$$

and that for any $1 \leqslant p < |[k]_g|$, $i \in [k]_g$, and $m_1 \geqslant z_i(g)$,

$$(i, m_1)g^p \notin \{(i, m) \mid m \in \mathbb{N}\}.$$

In fact we may compute $(i, m)g^{|[k]_g|}$ for any $i \in [k]_g$ and $m \geqslant z_i(g)$,

$$(i, m)g^{|[k]_g|} = (i, m + \sum_{s=0}^{|[k]_g|-1} t_{i\sigma_g^s}(g)). \tag{8}$$

In light of this, we introduce the following.

Definition 3.3. For any $g \in H_n \rtimes S_n$, class $[i]_g$, and $k \in [i]_g = \{i_1, i_2, \dots, i_q\}$, let

$$t_{[k]}(g) := \sum_{s=1}^{q} t_{i_s}(g).$$

Hence, if $t_{[k]}(g) = 0$, then for all $i' \in [k]_g$ and $m' \geqslant z_{i'}(g)$, the point (i', m') will lie on an orbit of length $|[k]_g|$. If $t_{[k]}(g) \neq 0$, then (8) states that for all $i' \in [k]_g$ and all $m' \geqslant z_{i'}(g)$, that $(i', m')g^{|[k]_g|} \neq (i', m')$. Hence when $t_{[k]}(g) = 0$, almost all points of the k^{th} ray will lie on an orbit of g of length $|[k]_g|$, and when $t_{[k]}(g) \neq 0$ almost all points of the k^{th} ray will lie in an infinite orbit of g. Since different arguments will be required for finite orbits and infinite orbits, we introduce the following notation.

Notation. *Let $g \in H_n \rtimes S_n$. Then $I(g) := \{i \in \mathbb{Z}_n \mid t_{[i]}(g) \neq 0\}$ consists of all $i \in \mathbb{Z}_n$ corresponding to rays of X_n which have infinite intersection with some infinite orbit of g. Let $I^c(g) := \mathbb{Z}_n \setminus I(g)$, the compliment of $I(g)$.*

Definition 3.4. Two sets are *almost equal* if their symmetric difference is finite.

For any $g \in H_n \rtimes S_n$ and any infinite orbit Ω of g, our aim is now to describe a set almost equal to Ω, so to have a suitable description of the infinite orbits of elements of $H_n \rtimes S_n$. We work with $t_{[k]}(g) > 0$, since if $t_{[k]}(g)$ is negative, we will be able to apply our arguments to g^{-1}. For any $i_1 \in [k]_g$ and $m_1 \geqslant z_{i_1}(g)$, we shall compute the orbit of (i_1, m_1) under g. First,

$$\{(i_1, m_1)g^{d|[k]_g|} \mid d \in \mathbb{N}\} = \{(i_1, m) \mid m > m_1, m \equiv m_1 \bmod |t_{[k]}(g)|\}.$$

Similarly, $\{(i_1, m_1)g^{d|[k]_g|+1} \mid d \in \mathbb{N}\}$ is equal to

$$\{(i_1\sigma_g, m) \mid m > m_1 + t_{i_1}(g), m \equiv m_1 + t_{i_1}(g) \bmod |t_{[k]}(g)|\}. \tag{9}$$

For every $2 \leqslant s \leqslant |[k]_g|$, setting $i_s := i_1\sigma_g^{s-1}$ and $m_s := m_1 + \sum_{d=1}^{s-1} t_{i_d}(g)$ we have, for any $0 \leqslant r < |[k]_g|$, that

$$\{(i_1, m_1)g^{d|[k]|_g+r} \mid d \in \mathbb{N}\} = \{(i_{r+1}, m) \mid m > m_{r+1}, m \equiv m_{r+1} \bmod |t_{[k]}(g)|\}$$

and hence $\{(i_1, m_1)g^d \mid d \in \mathbb{N}\}$ is equal to

$$\bigsqcup_{q=1}^{|[k]_g|} \{(i_q, m) \mid m > m_q, m \equiv m_q \bmod |t_{[k]}(g)|\}. \tag{10}$$

In the case where $t_{[k]}(g) < 0$, we can use similar arguments to those above to compute, for $i_1' \in I(g)$ and $m_1' \geqslant z_i(g)$, the set $\{(i_1', m_1')g^{-d} \mid d \in \mathbb{N}\}$. It is therefore natural to introduce the following.

Definition 3.5. Let $g \in H_n \rtimes S_n$, $i_1 \in I(g)$, and $m_1 \in \mathbb{N}$. Then

$$X_{i_1,m_1}(g) := \{(i_1, m) \in X_n \mid m \equiv m_1 \bmod |t_{[i_1]}(g)|\}.$$

Furthermore, for every $2 \leqslant s < |[k]_g|$ let $i_s := i_1\sigma_g^{s-1}$, $m_s := m_1 + \sum_{d=1}^{s-1} t_{i_d}(g)$, and

$$X_{[i_1],m_1}(g) := \bigsqcup_{q=1}^{|[i_1]_g|} X_{i_q,m_q}(g).$$

Note that suppressing $m_2, \ldots, m_{|[k]_g|}$ from the notation is not ambiguous since these are uniquely determined from i_1, m_1, and g.

Let us summarise what we have shown.

Lemma 3.6. *Let $g \in H_n \rtimes S_n$ and $i \in I(g)$. Then, for any infinite orbit Ω of g intersecting $\{(i, m) \in X_n \mid m \geqslant z_i(g)\}$, there exists $i' \in I(g)$ and constants $d_1, e_1 \in \mathbb{N}$ such that the set*

$$X_{[i],d_1}(g) \sqcup X_{[i'],e_1}(g)$$

is almost equal to Ω.

We may now show that the action of elements of $H_n \rtimes S_n$ is computable.

Lemma 3.7. *Let $G = \langle S \mid R\rangle$ be the presentation for $H_n \rtimes S_n$ as described in Lemma 3.1. Then there is an algorithm which, given a word w over $S^{\pm 1}$ representing $g \in H_n \rtimes S_n$, outputs finitely many equations which describe the image of (i, m) under g for every point $(i, m) \in X_n$.*

Proof. From [ABM13, Lem 2.1], the numbers $t_1(\omega_g), \ldots, t_n(\omega_g), z_1(\omega_g), \ldots, z_n(\omega_g)$ are computable. Hence the action of σ_g is computable, as are the classes $[i]_g$ and the numbers $t_{[i]}(g)$. This means that the action of g on the set

$$\{(i, m) \mid i \in \mathbb{Z}_n \text{ and } m \geqslant z_i(\omega_g)\} =: Y$$

is defined by finitely many computable equations. For each $i \in \mathbb{Z}_n$, we have the equation

$$(i, m)g := (i\sigma_g, m + t_i(\omega_g)) \text{ for all } m \geqslant z_i(\omega_g).$$

Since $X_n \setminus Y$ is finite, one can compute the action of g on each point in this set and then describe this action with finitely many equations. □

It is possible to solve $\mathrm{WP}(H_n \rtimes S_n)$ in quadratic time. From [ABM13, Lem 2.1], the size of $\{(i, m) \mid i \in \mathbb{Z}_n \text{ and } m \leqslant z_i(\omega_g)\}$ is bounded by a linear function in terms of $|g|_S$ (the word length of g with respect to S). Then, for each point in this set one may compute the action of g which involves $|g|_S$ computations. We then have that g is the identity if and only if g acts trivially on this set. Moreover, for any $g \in H_n \rtimes S_n$, the numbers $z_1(g), \dots, z_n(g)$ are computable (using, for example, the previous lemma).

3.2. **Identities arising from the equation for conjugacy.** In Section 2.2 we showed that $\mathrm{TCP}(H_n)$ was equivalent to producing an algorithm which, given any $a, b \in H_n \rtimes S_n$, decides whether or not a and b are H_n-conjugated. In this section we shall show some necessary conditions which any $x \in H_n$ must satisfy in order to conjugate a to b. First, some simple computations to rewrite $t_i(\sigma_a x \sigma_a^{-1})$ are needed. Note that, since $\sigma_a = \sigma_b$ is a necessary condition for a and b to be H_n-conjugated (and σ_a, σ_b are computable), the following will not be ambiguous.

Notation. *We will write $[i]$ to denote $[i]_a$ (which is also a class of σ_b).*

Lemma 3.8. *For any isometric permutation of the rays σ and any $y \in H_n$, we have that*

$$t_i(\sigma^{-1} y \sigma) = t_{i\sigma^{-1}}(y) \text{ for all } i \in \mathbb{Z}_n.$$

Proof. Let $\sigma = \sigma_1 \sigma_2 \dots \sigma_s$ be written in disjoint cycle notation, and let $\sigma_1 = (i_1\ i_2\ \dots\ i_q)$. Since $\sigma \in N_{\mathrm{Sym}(X_n)}(H_n)$, we have that $\sigma^{-1} y \sigma \in H_n$. We may now compute $t_{i_1}(\sigma^{-1} y \sigma)$ by considering the image of (i_1, m) where $m \geqslant \max(z_i(y))$.

$$(i_1, m)\sigma^{-1} y \sigma = (i_q, m) y \sigma = (i_q, m + t_{i_q}(y))\sigma = (i_1, m + t_{i_q}(y))$$

Similarly, for $1 < s \leqslant q$,

$$(i_s, m)\sigma^{-1} y \sigma = (i_{s-1}, m) y \sigma = (i_{s-1}, m + t_{i_{s-1}}(y))\sigma = (i_s, m + t_{i_{s-1}}(y)).$$

Thus $t_i(\sigma^{-1} y \sigma) = t_{i\sigma^{-1}}(y)$ for any $i \in \mathbb{Z}_n$. □

From this lemma, we may rewrite $t_i(\sigma_a x \sigma_a^{-1})$ as $t_{i\sigma_a}(x)$.

Lemma 3.9. *Let $a, b \in H_n \rtimes S_n$. Then a necessary condition a and b to be H_n-conjugated is that, for all $[i]$ classes, $t_{[i]}(a) = t_{[i]}(b)$.*

Proof. From our hypotheses, we have that

$$\begin{aligned} \omega_b \sigma_a &= x^{-1} \omega_a \sigma_a x \\ \Rightarrow \omega_b &= x^{-1} \omega_a (\sigma_a x \sigma_a^{-1}) \end{aligned}$$

and so, since ω_a, ω_b, x, and $\sigma_a x \sigma_a^{-1}$ can all be considered as elements of H_n, we have for all $i \in \mathbb{Z}_n$ that

$$t_i(\omega_b) = t_i(x^{-1}) + t_i(\omega_a) + t_i(\sigma_a x \sigma_a^{-1})$$

which from the previous lemma can be rewritten as

$$t_i(\omega_b) = -t_i(x) + t_i(\omega_a) + t_{i\sigma_a}(x). \tag{11}$$

Now, for any branch i', we sum over all k in $[i']$

$$\begin{aligned} \sum_{k \in [i']} t_k(\omega_b) &= -\sum_{k \in [i']} t_k(x) + \sum_{k \in [i']} t_k(\omega_a) + \sum_{k \in [i']} t_k(x) \\ \Rightarrow \sum_{k \in [i']} t_k(\omega_b) &= \sum_{k \in [i']} t_k(\omega_a) \\ \Rightarrow t_{[i']}(b) &= t_{[i']}(a) \end{aligned}$$

as required. □

Thus, if $a, b \in H_n \rtimes S_n$ are H_n-conjugated, then $I(a) = I(b)$. For any $g \in H_n \rtimes S_n$ the set $I(g)$ is computable, and so the first step of our algorithm can be to check that $I(a) = I(b)$. Hence the following is not ambiguous.

Notation. *We shall use I to denote $I(a)$ and $I(b)$.*

Intuitively, choosing a value for $t_k(x)$ for one $k \in [i']$ should define $t_{k'}(x)$ for all $k' \in [i']$. A proof of this follows naturally from the computations within the proof of the previous lemma.

Lemma 3.10. *Let $a, b \in H_n \rtimes S_n$ be conjugate by $x \in H_n$. Then, for each class $[k]$, choosing a value for $t_{i'}(x)$ for some $i' \in [k]$ determines values for $\{t_i(x) \mid i \in [k]\}$. Moreover, let $i_1 \in [k]$ and, for $2 \leqslant s \leqslant |[k]|$, let $i_s := i_1\sigma_a^{s-1}$. Then the following formula determines $t_{i_s}(x)$ for all $s \in \mathbb{Z}_{|[k]|}$*

$$t_{i_s}(x) = t_{i_1}(x) + \sum_{d=1}^{s-1}(t_{i_d}(\omega_b) - t_{i_d}(\omega_a)).$$

Proof. If $|[k]| = 1$, then there is nothing to prove. From (11) within the proof of Lemma 3.9, we have for all $i \in \mathbb{Z}_n$ that

$$t_i(\omega_b) = -t_i(x) + t_i(\omega_a) + t_{i\sigma_a}(x). \tag{12}$$

Within (12), set i to be equal to $i_s \in [k]$ (so that $s \in \mathbb{Z}_q$) to obtain

$$\begin{aligned} t_{i_s}(\omega_b) &= -t_{i_s}(x) + t_{i_s}(\omega_a) + t_{i_s\sigma_a}(x) \\ \Rightarrow t_{i_s\sigma_a}(x) &= t_{i_s}(x) + t_{i_s}(\omega_b) - t_{i_s}(\omega_a). \end{aligned}$$

Setting $s = 1$ provides a formula for $t_{i_2}(x)$. If $2 \leqslant s < q$, then

$$\begin{aligned} t_{i_s\sigma_a}(x) &= t_{i_s}(x) + t_{i_s}(\omega_b) - t_{i_s}(\omega_a) \\ &= t_{i_{s-1}}(x) + t_{i_{s-1}}(\omega_b) - t_{i_{s-1}}(\omega_a) + t_{i_s}(\omega_b) - t_{i_s}(\omega_a) \\ &= \dots \\ &= t_{i_1}(x) + \sum_{d=1}^{s}(t_{i_d}(\omega_b) - t_{i_d}(\omega_a)). \end{aligned}$$

Thus, for all $s \in \mathbb{Z}_q$, we have a formula for $t_{i_s}(x)$ which depends on the computable values $\{t_i(a), t_i(b) \mid i \in [k]\}$ and the value of $t_{i_1}(x)$. □

4. An algorithm for finding a conjugator in H_n

In this section we will construct an algorithm which, given $a, b \in H_n \rtimes S_n$ with $\sigma_a = \sigma_b$, either outputs an $x \in H_n$ such that $x^{-1}ax = b$, or halts without outputting such an x if one does not exist.

We will often need to make a choice of some $i \in [k]_g$. For each class $[k]_g$ we shall do this by introducing an ordering on $[k]_g$. We shall choose this ordering to be the one defined by $i_1 := \inf[k]_g$ (under the usual ordering of $\mathbb{N}$) and $i_s := i_1\sigma_g^{s-1}$ for all $2 \leqslant s \leqslant |[k]_g|$. Hence $[k]_g = \{i_1, \dots, i_{|[k]_g|}\}$.

4.1. **An algorithm for finding a conjugator in** FSym**.** Many of the arguments of this section draw their ideas from [ABM13, Section 3]. By definition, any element which conjugates a to b will send the support of a to the support of b. If we wish to find a conjugator in FSym, this means that the symmetric difference of these sets must be finite, whilst $\mathrm{supp}(a) \cap \mathrm{supp}(b)$ can be infinite.

Notation. *For any $g, h \in \mathrm{Sym}$, let $N(g,h) := \mathrm{supp}(g) \cap \mathrm{supp}(h)$, the intersection of the supports of g and h.*

Notation. *Let $g \in H_n \rtimes S_n$. Then $Z(g) := \{(i,m) \in X_n \mid i \in \mathbb{Z}_n$ and $m < z_i(g)\}$ which is analogous to the Z region which has been used by some authors when dealing with the Houghton groups.*

Definition 4.1. Let $g \in H_n \rtimes S_n$. Then, for a fixed $r \in \mathbb{N}$, let g_r denote the element of $\mathrm{Sym}(X_n)$ which consists of the product of all of the r-cycles of g. Furthermore, let g_∞ denote the element of $\mathrm{Sym}(X_n)$ which consists of the product of all of the infinite cycles of g.

Our strategy for deciding whether $a, b \in H_n \rtimes S_n$ are FSym-conjugated is as follows. We will show that, for any $r \in \mathbb{N}$, if a_r and b_r are FSym-conjugated, then a_r and b_r are FSym-conjugated by some x where $\mathrm{supp}(x)$ is contained in a computable finite set. Similarly we will show that if a_∞ and b_∞ are FSym-conjugated, then there is a computable finite set such that there is a conjugator of a_∞ and b_∞ with support contained within this set. In order to decide if $a, b \in H_n \rtimes S_n$ are FSym-conjugated we may then decide if a_∞ and b_∞ are FSym-conjugated, produce such a conjugator y_1 if one exists, and then decide if $y_1^{-1} a y_1$ and b are FSym-conjugated by deciding whether $(y_1^{-1} a y_1)_r$ and b_r are FSym-conjugated for every $r \in \mathbb{N}$ (which is possible since b_r is non-trivial for only finitely many $r \in \mathbb{N}$).

Lemma 4.2. *If $g, h \in \mathrm{Sym}$ are FSym-conjugated, then*

$$|\,\mathrm{supp}\,(g) \setminus N(g,h)| = |\,\mathrm{supp}\,(h) \setminus N(g,h)| < \infty.$$

Proof. The proof [ABM13, Lem 3.2] applies to our more general hypotheses. □

Lemma 4.3. *Let $g \in H_n \rtimes S_n$ and $r \in \mathbb{N}$. Then $g_r \in H_n \rtimes S_n$. Note this means that g_r restricts to a bijection on $Z(g_r)$ and $X_n \setminus Z(g_r)$.*

Proof. It is clear that $g_r \in \mathrm{Sym}(X_n)$. From our description of orbits in Section 3.1, for all $(i,m) \in X_n \setminus Z(g)$ we have that (i,m) lies either on: an infinite orbit of g; an orbit of g of length $s \neq r$; or on an orbit of g of length r. In the first two cases, we will have that $(i,m)g_r = (i,m)$ for all $(i,m) \in X_n \setminus Z(g)$. In the final case, we have that $(i,m)g_r = (i,m)g$ for all $X_n \setminus Z(g)$. Hence, g_r is an element for which there exists an isometric permutation of the rays σ, and constants $t_1(g_r), \ldots, t_n(g_r) \in \mathbb{Z}$ and $z_1(g_r), \ldots, z_n(g_r) \in \mathbb{N}$ such that for all $i \in \mathbb{Z}_n$

$$(i,m)g_r = (i\sigma, m + t_i(g_r)) \text{ for all } m \geqslant z_i(g_r)$$

which was labelled (5) in Section 3.1. Thus, $g_r \in H_n \rtimes S_n$. □

Lemma 4.4. *Let $G = \langle S \mid R \rangle$ be the presentation for $H_n \rtimes S_n$ as described in Lemma 3.1. Then there is an algorithm which, given any $r \in \mathbb{N}$ and a word w over $S^{\pm 1}$ representing $g \in H_n \rtimes S_n$, outputs finitely many equations which describe the image of (i,m) under g_r for every point $(i,m) \in X_n$.*

Proof. First, compute the numbers $z_1(g), \dots, z_n(g)$ and $t_1(g), \dots, t_n(g)$ and classes $\{[k]_g \mid k = 1 \dots, n\}$. Then produce equations of the form

$$(i,m)g = (i\sigma_g, m + t_i(g)) \text{ for all } (i,m) \in X_n \setminus Z(g).$$

We now wish to write similar equations for g_r. In order to define g_r, we keep any equation relating to the point (i_1, m_1) if and only if

$$|\mathcal{O}_g(i_1, m_1)| := |\{(i_1, m_1)g^d \mid d \in \mathbb{Z}\}| = r.$$

We note that for all $(i', m') \in X_n$, the number $|\mathcal{O}_g(i', m')|$ is computable. First, let $(i', m') \in X_n \setminus Z(g)$. Then $|\mathcal{O}_g(i', m')|$ is infinite if $t_{[i']}(g) \neq 0$ and is equal to $|[i']_g|$ otherwise. If $(i', m') \in Z(g)$, either $|\mathcal{O}_g(i', m')|$ is finite and so $(i', m')g^d = (i', m')$ for some $d \in \mathbb{N}$, or $(i', m')g^d \in X_n \setminus Z(g)$ for some $d \in \mathbb{N}$ and so (i', m') lies in an infinite orbit of g. □

Notation. *Let $g \in \mathrm{Sym}(X)$. Given any set $Y \subseteq X$ for which $Yg = Y$ (so that g restricts to a bijection on Y), let $g\big|Y$ denote the element of* $\mathrm{Sym}(X)$ *which acts as g on the set Y and leaves all points in $X \setminus Y$ invariant i.e. for every $x \in X$*

$$x(g\big|Y) := \begin{cases} xg & \text{if } x \in Y \\ x & \text{otherwise.} \end{cases}$$

Lemma 4.5. *Fix an $r \in \mathbb{N}$ and let $g, h \in H_n \rtimes S_n$. If g_r and h_r are* FSym-*conjugated, then there exists an $x \in$* FSym *which conjugates g_r to h_r such that* $\mathrm{supp}(x) \subseteq Z(g_r) \cup Z(h_r)$.

Proof. Since we are working with a fixed $g_r, h_r \in H_n \rtimes S_n$, let $N := N(g_r, h_r)$, $Z := Z(g_r) \cup Z(h_r)$, and $Z^c := X_n \setminus Z$. If g_r and h_r are FSym-conjugated, then

$$(i,m)g_r = (i,m)h_r \text{ for all } (i,m) \in Z^c. \tag{13}$$

By Lemma 4.3 and (13), g_r and h_r restrict to a bijection of Z^c. Thus, g_r and h_r must also restrict to a bijection of Z.

Applying Lemma 4.2 to g_r and h_r we have that

$$|\,\mathrm{supp}\,(g_r) \setminus N| = |\,\mathrm{supp}\,(h_r) \setminus N| < \infty$$

where, from (13), $Z^c \cap \mathrm{supp}(g_r) = Z^c \cap \mathrm{supp}(h_r) \subseteq N$. Thus $\mathrm{supp}(g_r) \setminus N$ and $\mathrm{supp}(h_r) \setminus N$ are both subsets of Z. Now, for any finite subset $D \subseteq N$,

$$|D \cup (\mathrm{supp}\,(g_r) \setminus N)| = |D \cup (\mathrm{supp}\,(h_r) \setminus N)| < \infty.$$

Setting $D := Z \cap N$ we have that

$$|\,\mathrm{supp}(g_r\big|Z)| = |\,\mathrm{supp}(h_r\big|Z)| < \infty. \tag{14}$$

Since g_r and h_r consist of only r-cycles, $g_r\big|Z$ and $h_r\big|Z$ are elements of FSym with the same cycle type, and so are FSym-conjugated. Thus there is a conjugator $x \in$ FSym with $\mathrm{supp}(x) \subseteq \mathrm{supp}(g_r\big|Z) \cup \mathrm{supp}(h_r\big|Z)$. Therefore $\mathrm{supp}(x) \subseteq Z$, as required. □

Lemma 4.6. *If $g_\infty = h_\infty$ and $g, h \in H_n \rtimes S_n$ are* FSym-*conjugated, then there is an $x \in$* FSym *which conjugates g to h and has support contained within a computable set.*

Proof. We use the previous lemma. For each $r \in \mathbb{N}$ let $Z_r := Z(g_r) \cup Z(h_r)$. Moreover, let $Y := (\bigcup_{r\in\mathbb{N}} Z_r)\setminus\mathrm{supp}(g_\infty)$ and $Y^c := X_n\setminus Y$. If $x \in \mathrm{FSym}$ conjugates g to h, then for all $r \in \mathbb{N}$, x conjugates g_r to h_r. Note that Y is computable. First, compute which g_r are non-trivial by computing $I^c(g)$ (so that for each $j \in I^c(g)$, $g_{|[j]_g|}$ is non-trivial) and then, from the proof of Lemma 4.4, compute the length of all orbits of points $(i, m) \in Z(g)$. This means that, apart from finitely many $r \in \mathbb{N}$, g_r is trivial, and so Y is finite. This means that the finite number of $r \in \mathbb{N}$ such that $Z_r \neq \emptyset$ are known. Finally, $\mathrm{supp}(g_\infty) \cap Z(g)$ is computable (by Lemma 3.7). As noted in (13) above, $(i, m)g = (i, m)h$ for all $(i, m) \in Y^c$ and (again from the previous proof) $g\big|Y$ and $h\big|Y$ have the same cycle type. Thus there is an $x \in \mathrm{FSym}$ which conjugates $g\big|Y$ to $h\big|Y$ and, since $g\big|Y^c = h\big|Y^c$, we may choose x so that $\mathrm{supp}(x) \subseteq Y$. Notice that, from our choice of Y, this means that $\mathrm{supp}(x) \cap \mathrm{supp}(g_\infty) = \emptyset$. □

We now reduce finding an FSym-conjugator of a and b to the case of Lemma 4.6. In order to do this we require a well known lemma.

Lemma 4.7. *Let $x \in G$ conjugate $a, b \in G$. Then, $x' \in G$ also conjugates a to b if, and only if, $x' = cx$ for some $c \in C_G(a)$.*

Lemma 4.8. *Let $g, h \in H_n \rtimes S_n$. If g_∞ and h_∞ are* FSym*-conjugated, then there exists an $x \in$* FSym *which conjugates g_∞ to h_∞ with* $\mathrm{supp}(x) \subseteq Z(g_\infty) \cup Z(h_\infty)$.

Proof. Let $Z := Z(g_\infty)\cup Z(h_\infty)$. We start by using a similar argument to the proof of [ABM13, Prop 3.1] to show that there is a computable bound for $z_i(x)$. We will assume that $t_{[i]}(g) > 0$, since replacing g and h with $\omega_g^{-1}\sigma_g$ and $\omega_h^{-1}\sigma_g$ respectively will provide an argument for $t_{[i]}(g) < 0$. Note that $I(g_\infty) = I(g) = I(h) = I(h_\infty)$. For all $i \in I(g_\infty)$ and all $m \geqslant z_i(g_\infty)$, we have that $(i, m)(g_\infty)^{|[i]_g|} = (i, m+t_{[i]}(g))$. Let $x \in \mathrm{FSym}$ conjugate g_∞ to h_∞. We will show for all $i \in \mathbb{Z}_n$ that

$$(i, m)x = (i, m) \text{ for all } m \geqslant z_i(x).$$

We first produce a computable bound for $z_j(x)$ for all $j \in I^c(g)$. Let $j \in I^c(g)$, $(j, m) \in X_n \setminus Z$, and assume that $(j, m) \in \mathrm{supp}(x)$. Then $(j, m)h_\infty = (j, m)$ and so $(j, m)x^{-1}g_\infty x = (j, m)$. If $(j, m)x^{-1} \notin \mathrm{supp}(g_\infty)$, then the 2-cycle $\gamma := ((j, m)\ (j, m)x^{-1})$ is in $C_{\mathrm{FSym}}(g_\infty)$ and so (by Lemma 4.7) $x' := \gamma x$ also conjugates g to h. Now, by construction, $(j, m) \notin \mathrm{supp}(x')$. If $(j, m)x^{-1} = (j', m') \in \mathrm{supp}(g_\infty)$, then x sends (j', m') to (j, m). But, from the fact that $(j, m)x^{-1}g_\infty x = (j, m)$, x must send $(j', m')g_\infty$ to (j, m), and so x sends both (j', m') and $(j', m')g_\infty$ to (j, m), a contradiction. Therefore we may assume that

$$\{(j, m) \mid j \in I^c(g)\} \cap \mathrm{supp}(x) \subseteq Z(g_\infty) \cup Z(h_\infty).$$

We now show that there is a computable bound for $z_i(x)$ for all $i \in I(g_\infty)$. Assume, for a contradiction, that for some $i \in I(g_\infty)$ we have that

$$z_i(x) > \max(z_i(g_\infty), z_i(h_\infty)).$$

For all $m \geqslant 0$, we then have that $z_i(x)+m \geqslant z_i(x) > \max(z_i(g_\infty), z_i(h_\infty))$. Hence, for all $m \geqslant 0$

$$\begin{aligned}&(i, z_i(x) + m)(x^{-1}g_\infty x)^{-|[i]_g|} = (i, z_i(x) + m)(h_\infty)^{-|[i]_g|}\\ =&(i, z_i(x) + m - t_{[i]}(h_\infty)) = (i, z_i(x) + m - t_{[i]}(g_\infty)).\end{aligned}$$

Similarly,

$$(i, z_i(x) + m)(x^{-1}g_\infty x)^{-|[i]_g|} = (i, z_i(x) + m)x^{-1}(g_\infty)^{-|[i]_g|}x$$
$$=(i, z_i(x) + m)(g_\infty)^{-|[i]_g|}x = (i, z_i(x) + m - t_{[i]}(g_\infty))x$$

and so $(i, z_i(x) + m - t_{[i]}(g_\infty))x = (i, z_i(x) + m - t_{[i]}(g_\infty))$, which contradicts the minimality of $z_i(x)$. We may therefore enumerate all possible bijections of the set $Z(g_\infty) \cup Z(h_\infty)$ to decide whether or not g_∞ and h_∞ are FSym-conjugated. □

We will now produce an element which conjugates a to b using the conjugators computed in Lemma 4.5 and Lemma 4.8.

Proposition 4.9. *Given $a, b \in H_n \rtimes S_n$, there is an algorithm which decides whether or not a and b are* FSym*-conjugated, and produces a conjugator in* FSym *if one exists.*

Proof. First, we may compute a_∞ and b_∞ and so use Lemma 4.8 to decide whether or not they are FSym-conjugated. If a_∞ and b_∞ are not FSym-conjugated, then a and b are not FSym-conjugated since such a conjugator would also conjugate a_∞ to b_∞. Thus, let $y_1 \in$ FSym conjugate a_∞ to b_∞.

Now, a necessary condition for elements $a, b \in H_n \rtimes S_n$ to be conjugate in $\mathrm{Sym}(X_n)$ is that they have the same cycle type. Let $M := \{r \in \mathbb{N} \mid g_r \neq \mathrm{id}\}$. Then $a := a_\infty \prod_{d \in M} a_d$ and $b := b_\infty \prod_{d\in M} b_d$. Note that $|M|$ is finite and that M is computable by the process described for computing Y in Lemma 4.6. From Lemma 4.8 we may produce an element $y_1 \in$ FSym such that

$$y_1^{-1}ay_1 = \big(y_1^{-1}a_\infty y_1\big)\big(y_1^{-1}(\prod_{d\in M} a_d)y_1\big) =: a'.$$

Importantly this means that $a'_\infty = b_\infty$. We now describe how to compute finitely many equations to describe the action of a' on X_n. Note that y_1 was computed by enumerating bijections of a computable finite set. Hence the bijection induced by y_1 is known. Now, compute $(i, m)y_1^{-1}ay_1$ for each point $(i, m) \in \mathrm{supp}(y_1) \cup \mathrm{supp}(y_1)a^{-1} =: Y_1$. Finally, note that $(i, m)a = (i, m)a'$ for all $(i, m) \in X_n \setminus Y_1$ since

$$(i, m)y_1^{-1}ay_1 = (i, m)ay_1 = (i, m)a \text{ for all } (i, m) \notin Y_1.$$

Now, from Lemma 4.6, it is decidable whether there exists $y_2 \in$ FSym which conjugates a' to b with $\mathrm{supp}(y_2) \cap \mathrm{supp}(b_\infty) = \emptyset$. Note that, if there is an element y_2, then it also conjugates $a'(b_\infty)^{-1}$ to $b(b_\infty)^{-1}$. Hence

$$\begin{aligned}(y_1y_2)^{-1}a(y_1y_2) &= y_2^{-1}a'y_2\\ &= y_2^{-1}a'(b_\infty)^{-1}b_\infty y_2\\ &= y_2^{-1}a'(b_\infty)^{-1}y_2 b_\infty\\ &= b(b_\infty)^{-1}b_\infty\\ &= b.\end{aligned}$$

□

4.2. **Reducing the problem to finding a conjugator in** FSym**.** The previous section provided us with an algorithm for deciding whether $a, b \in H_n \rtimes S_n$ are FSym-conjugated. Our problem is to decide if a and b are H_n-conjugated. We start with a simple observation.

Definition 4.10. Given $g, h \in H_n \rtimes S_n$ and a group G such that $\mathrm{FSym}(X_n) \leqslant G \leqslant H_n$, a *witness set of G-conjugation* is a subset $V(g,h,G)$ of $\mathbb{Z}^n$ satisfying that if g, h are G-conjugated, then there is an $x \in G$ such that $g = x^{-1}hx$ and $t(x) \in V(g,h,G)$.

Lemma 4.11. *Let* $\mathrm{FSym}(X_n) \leqslant G \leqslant H_n$. *If, for any* $g, h \in H_n \rtimes S_n$ *it is possible to compute a witness set of G-conjugation $V(g,h,G)$, then there is an algorithm which, given any* $a, b \in H_n \rtimes S_n$, *decides whether they are G-conjugated.*

Proof. We use, from the previous section, that there exists an algorithm for deciding if $g, h \in H_n \rtimes S_n$ are FSym-conjugated. For any $\underline{\mathbf{v}} \in \mathbb{Z}^n$ with $\sum_{i=1}^n \underline{\mathbf{v}}_i = 0$ let

$$x_{\underline{\mathbf{v}}} := \prod_{i=2}^{n} g_i^{-\underline{\mathbf{v}}_i} \tag{15}$$

so that $t(x_{\underline{\mathbf{v}}}) = \underline{\mathbf{v}}$. Thus, if g and h are G-conjugated, then there exists $\underline{\mathbf{v}} \in V(g,h,G)$ and $x \in \mathrm{FSym}$ such that $x_{\underline{\mathbf{v}}}x$ conjugates g to h. Now, to decide if g and h are G-conjugated, it is sufficient to check whether any of the pairs $\{(x_{\underline{\mathbf{v}}}^{-1} g x_{\underline{\mathbf{v}}}, h) \mid \underline{\mathbf{v}} \in V(g,h,G)\}$ are FSym-conjugated. This is because

$$x^{-1}(x_{\underline{\mathbf{v}}}^{-1} g x_{\underline{\mathbf{v}}})x = h \Leftrightarrow (x_{\underline{\mathbf{v}}}x)^{-1} g (x_{\underline{\mathbf{v}}}x) = h$$

and so a pair is FSym-conjugated if and only if g and h are G-conjugated. □

From this lemma, if, for any $g, h \in H_n \rtimes S_n$, the set $V(g,h,H_n)$ was computable (from only g and h), then $\mathrm{TCP}(H_n)$ would be solvable. We shall show that solving our problem can be achieved by producing an algorithm to decide if elements are G-conjugated where G is a particular subgroup of H_n. We restrict our attention to searching for a conjugator x such that $t_i(x) \equiv 0 \bmod |t_{[i]}(g)|$ for all $i \in I(g)$, since this will mean that any infinite orbit $\mathcal{O}_g$ of g will be almost equal to $(\mathcal{O}_g)x$. Let $|\sigma_g|$ denote the order of σ_g (the isometric permutation of the rays induced by g). We will impose the condition that $t_i(x) \equiv 0 \bmod |t_i(g^{|\sigma_g|})|$ for all $i \in I(g)$ to use in the next section. This is a stronger condition since, for any $i \in I(g)$, $|t_{[i]}(g)| = |t_i(g^{|[i]_g|})|$.

Definition 4.12. Let $g \in H_n \rtimes S_n$, $|\sigma_g|$ denote the order of $\sigma_g \in S_n$, and

$$H_n^*(g) := \{x \in H_n \mid t_i(x) \equiv 0 \bmod \left|t_i(g^{|\sigma_g|})\right| \text{ for all } i \in I(g)\}.$$

Recall that if $a, b \in H_n \rtimes S_n$ are H_n-conjugated, then $\sigma_a = \sigma_b$. Also, from Lemma 3.9, $t_{[i]}(a) = t_{[i]}(b)$ for all $i \in \mathbb{Z}_n$. Hence, if a and b are H_n-conjugated, then $H_n^*(a) = H_n^*(b)$.

Lemma 4.13. *Assume there exists an algorithm which, given any* $g, h \in H_n \rtimes S_n$, *decides whether g and h are $H_n^*(g)$-conjugated. Then there exists an algorithm which, given any* $g, h \in H_n \rtimes S_n$, *decides whether g and h are H_n-conjugated.*

Proof. Given $g \in H_n \rtimes S_n$, construct the set

$$P_g := \{(\underline{\mathbf{v}}_1, \dots, \underline{\mathbf{v}}_n) \in \mathbb{Z}^n : 0 \leqslant \underline{\mathbf{v}}_i < \left|t_i(g^{|\sigma_g|})\right| \text{ for all } i \in I(g) \text{ and } \underline{\mathbf{v}}_k = 0 \text{ otherwise}\}.$$

Note that, for any $y \in H_n \rtimes S_n$, P_y will be finite. Define $x_{\underline{\mathbf{v}}}$ as in (15) above. Note that $H_n = \bigsqcup_{\underline{\mathbf{v}} \in P_g} x_{\underline{\mathbf{v}}} H_n^*(g)$ and so any element of H_n is expressible as a product of $x_{\underline{\mathbf{v}}}$ for some $\underline{\mathbf{v}} \in P_g$ and an element in $H_n^*(g)$. Thus, deciding whether any of the finite number of pairs $\{(x_{\underline{\mathbf{v}}}^{-1} g x_{\underline{\mathbf{v}}}, h) \mid \underline{\mathbf{v}} \in P_g\}$ are $H_n^*(g)$-conjugated is sufficient to decide whether g and h are H_n-conjugated. □

Remark 4.14. *From Lemma 4.11, if for any $g, h \in H_n \rtimes S_n$ a set $V(g, h, H_n^*(g))$ is computable, then it is possible to decide whether any $g, h \in H_n \rtimes S_n$ are $H_n^*(g)$-conjugated. By Lemma 4.13, it will then be possible to decide whether any $g, h \in H_n \rtimes S_n$ are H_n-conjugated. From Section 2.2, this will mean that TCP(H_n) is solvable.*

In the following two sections we will show that for any $g, h \in H_n \rtimes S_n$ a witness set of $H_n^*(g)$-conjugation is computable from only g and h. In Section 4.3 we show that the following is computable.

Notation. *Let $g, h \in H_n \rtimes S_n$ and $n \geqslant 2$. Let $M_I(g, h)$ denote a number such that, if g and h are $H_n^*(g)$-conjugated, then there is a conjugator $x \in H_n^*(g)$ with*

$$\sum_{i \in I(g)} |t_i(x)| < M_I(g, h).$$

In Section 4.4 we show that for any $g, h \in H_n \rtimes S_n$, numbers $\{y_j(g, h) \mid j \in I^c(g)\}$ are computable (using only g and h) such that if there exists an $x \in H_n^*(g)$ which conjugates g to h, then there is an $x' \in H_n^*(g)$ which conjugates g to h such that $t_i(x') = t_i(x)$ for all $i \in I(g)$ and $t_j(x') = y_j(g, h)$ for all $j \in I^c(g)$.

Remark 4.15. *Note that if the numbers $M_I(g, h)$ and $\{y_j(g, h) \mid j \in I^c(g)\}$ are computable using only g and h then the set $V(g, h, H_n^*(g))$ is computable from only g and h. This is because defining $V(g, h, H_n^*(g))$ to consist of all vectors $\underline{\mathbf{v}}$ satisfying:*

i) $\sum_{i \in I} |\underline{\mathbf{v}}_i| < M_I(g, h)$;
ii) $\underline{\mathbf{v}}_i = y_i$ *for all* $i \in I^c(g)$;
iii) $\sum_{i=1}^{n} \underline{\mathbf{v}}_i = 0$.

provides us with a finite set such that if g and h are $H_n^*(g)$-conjugated, then they are conjugate by an $x \in H_n^*(g)$ with $t(x) \in V(g, h, H_n^*(g))$.

4.3. **Showing that $M_I(g, h)$ is computable.** Let $g, h \in H_n \rtimes S_n$ and $x \in H_n^*(g)$ conjugate g to h. In this section we will show that a number $M_I(g, h)$ is computable from only the elements g and h.

Notation. *Let $x \in H_n^*(a)$ conjugate $a, b \in H_n \rtimes S_n$. Then, for each $i \in I$, let $l_i(x)$ be chosen so that $t_i(x) = l_i(x)|t_{[i]}(a)|$. Note, since $t_i(x) \equiv 0 \bmod \left|t_{[i]}(a)\right|$ for all $i \in I$, that $l_i(x) \in \mathbb{Z}$ for each $i \in I$.*

Recall that $\sigma_a = \sigma_b$ and that Lemma 3.9 tells us that, if a and b are H_n-conjugated, then $t_{[i]}(a) = t_{[i]}(b)$ for every $[i]$ class of σ_a. Thus, for every $i \in I$ and $d_1 \in \mathbb{N}$, we have that $X_{i_1,d_1}(a) = X_{i_1,d_1}(b)$ (the sets from Definition 3.5). Also, $(X_{i_1,d_1}(a))x$ is almost equal to $X_{i_1,d_1}(a)$ since the set $X_{i_1,d_1}(a)$ consists of all points $(i_1, m) \in X_n$ where $m \equiv d_1 \bmod |t_{[i_1]}(a)|$. Moreover $(X_{[i_1],d_1}(a))x$ is almost equal to $X_{[i_1],d_1}(a)$ since $X_{[i_1],d_1}(a)$ is the union of sets $X_{i_s,d_s}(a)$ where for each $i_s \in [i_1]$ we have that $(X_{i_s,d_s}(a))x$ is almost equal to $X_{i_s,d_s}(a)$.

Remark 4.16. *From (11) in the proof of Lemma 3.9, we have for any H_n-conjugated $g, h \in H_n \rtimes S_n$ and any $i \in I(g)$ that $t_{i\sigma_g}(x) - t_i(x) = t_i(\omega_h) - t_i(\omega_g)$. If we assume that $x \in H_n^*(g)$, we then have that $t_i(\omega_g) \equiv t_i(\omega_h) \bmod |t_{[i]}(g)|$. Hence if g and h are $H_n^*(g)$ conjugate, then for any infinite orbit $\mathcal{O}_g$ of g, there must be an infinite orbit of h which is almost equal to $\mathcal{O}_g$. It will therefore not be ambiguous to omit a and b and simply write X_{i_1,d_1} and $X_{[i],d_1}$.*

Definition 4.17. Given $g \in H_n \rtimes S_n$, we define an equivalence relation $\sim_g$ on $\{[k]_g \mid k \in I(g)\}$ as the one generated by setting $[i]_g \sim_g [j]_g$ if and only if there is an orbit of g almost equal to $X_{[i],d_1}(g) \sqcup X_{[j],e_1}(g)$ for some $d_1, e_1 \in \mathbb{N}$. Writing $[i] \sim_g [j]$ will not be ambiguous since the relation $\sim_g$ will always be used with respect to the σ_g-classes of g. Note that if $a, b \in H_n \rtimes S_n$ are H_n-conjugated, then $\sigma_a = \sigma_b$ and a and b produce the same equivalence relation.

Proposition 4.18. *Let $a, b \in H_n \rtimes S_n$ be $H_n^*(a)$-conjugated. Then there exists a computable constant $K(a,b)$ (computable from only on a and b) such that for any $x \in H_n^*(a)$ which conjugates a to b and any given i, j where $[i] \sim_a [j]$, we have that $\big||[i]||l_i(x)| - |[j]||l_j(x)|\big| < K(a,b)$.*

Proof. We follow in spirit the proof of [ABM13, Prop 4.3]. For convenience, we introduce notation to describe a set almost equal to $X_{[i],d_1}$.

Notation. *For any set $Y \subseteq X_n$, and any $\underline{\mathbf{q}} := (\underline{\mathbf{q}}(1), \underline{\mathbf{q}}(2), \ldots, \underline{\mathbf{q}}(n)) \in \mathbb{N}^n$, let $Y\big|_{\underline{\mathbf{q}}} := Y \setminus \{(i,m) \mid i \in \mathbb{Z}_n \text{ and } m < \underline{\mathbf{q}}(i)\}$.*

We will assume that $a, b \in H_n \rtimes S_n$ and $x \in H_n^*(a)$ are known. Let $i, j \in I$ satisfy $[i] \sim_a [j]$. Then there exist $d_1, e_1 \in \mathbb{N}$ such that $X_{[i],d_1} \sqcup X_{[j],e_1}$ is almost equal to an infinite orbit of a and hence, by Remark 4.16, is almost equal to an infinite orbit of b. Denote these infinite orbits by $\mathcal{O}_a$ and $\mathcal{O}_b$ respectively.

Let ϵ_k be the smallest integers such that

i) for all $k \in [i] \cup [j]$, $\epsilon_k \geqslant \max(z_k(a), z_k(b))$;
ii) for all $k \in [i]$, $\epsilon_k \equiv d_k \bmod |t_{[i]}(a)|$;
iii) for all $k \in [j]$, $\epsilon_k \equiv e_k \bmod |t_{[j]}(a)|$

and define $v \in \mathbb{Z}^n$ by $v_k = \begin{cases} \epsilon_k & \text{if } k \in [i] \cup [j] \\ 1 & \text{otherwise.} \end{cases}$

We now have that

$$X_{[i],d_1}\big|_v \subseteq X_{[i],d_1} \cap \mathcal{O}_a;\; X_{[i],d_1}\big|_v \subseteq X_{[i],d_1} \cap \mathcal{O}_b;$$
$$X_{[i],d_1}\big|_v \subseteq X_{[j],e_1} \cap \mathcal{O}_a;\text{ and } X_{[i],d_1}\big|_v \subseteq X_{[j],e_1} \cap \mathcal{O}_b.$$

This allows us to decompose $\mathcal{O}_a$ and $\mathcal{O}_b$:

$$\mathcal{O}_a = X_{[i],d_1}\big|_v \sqcup X_{[j],e_1}\big|_v \sqcup S_{i,j}$$
$$\mathcal{O}_b = X_{[i],d_1}\big|_v \sqcup X_{[j],e_1}\big|_v \sqcup T_{i,j}$$

where $S_{i,j}$ and $T_{i,j}$ are finite sets. Define ϵ'_k to be the smallest integers such that for all $k \in [i] \cup [j]$

i) $\epsilon'_k \geqslant z_k(x)$;
ii) $\epsilon'_k \geqslant \epsilon_k + |t_k(x)|$;
iii) $\epsilon'_k \equiv \epsilon_k \bmod |t_{[k]}(a)|$

and define $v' \in \mathbb{Z}^n$ by $v'_k = \begin{cases} \epsilon'_k & \text{if } k \in [i] \cup [j] \\ 1 & \text{otherwise.} \end{cases}$

These conditions for ϵ'_k imply that x restricts to a bijection from

$$X_{[i],d_1}\big|_{v'} \text{ to } X_{[i],d_1}\big|_{v'+t(x)}$$
$$\text{and } X_{[j],e_1}\big|_{v'} \text{ to } X_{[j],e_1}\big|_{v'+t(x)}.$$

Hence x restricts to a bijection between the following finite sets

$$\big(X_{[i],d_1}\big|_v \setminus X_{[i],d_1}\big|_{v'}\big) \sqcup \big(X_{[j],e_1}\big|_v \setminus X_{[j],e_1}\big|_{v'}\big) \sqcup S_{i,j} \tag{16}$$

$$\text{(17)} \qquad \text{and } \big(X_{[i],d_1}\big|_v \setminus X_{[i],d_1}\big|_{v'+t(x)}\big) \sqcup \big(X_{[j],e_1}\big|_v \setminus X_{[j],e_1}\big|_{v'+t(x)}\big) \sqcup T_{i,j}.$$

By definition, x eventually translates with amplitude $t_k(x) = l_k(x) \cdot |t_{[k]}(a)|$ for each $k \in [i] \sqcup [j]$. Thus

$$\Big|\Big(X_{[i],d_1}|_v \setminus X_{[i],d_1}|_{v'+t(x)}\Big)\Big| = \Big|\big(X_{[i],d_1}|_v \setminus X_{[i],d_1}|_{v'}\big)\Big| + \sum_{k\in[i]} l_k(x)$$

$$\text{and } \Big|\Big(X_{[j],e_1}|_v \setminus X_{[j],e_1}|_{v'+t(x)}\Big)\Big| = \Big|\big(X_{[j],e_1}|_v \setminus X_{[j],e_1}|_{v'}\big)\Big| + \sum_{k'\in[j]} l_{k'}(x).$$

Now, since (16) and (17) have the same cardinality, we have

$$\text{(18)} \qquad \sum_{k\in[i]} l_k(x) + \sum_{k'\in[j]} l_{k'}(x) + |T_{i,j}| = |S_{i,j}|.$$

Using Lemma 3.10 we may rewrite each element of $\{l_k(x) \mid k \in [i]\}$ as a computable constant plus $l_i(x)$ and each element of $\{l_{k'}(x) \mid k \in [j]\}$ as a computable constant plus $l_j(x)$. Let $A_{i,j}$ denote the sum of all of these constants (which 'adjust' the values of the translation lengths of x amongst each σ_a class). Now (18) becomes

$$|[i]|l_i(x) + |[j]|l_j(x) + A_{i,j} + |T_{i,j}| = |S_{i,j}|.$$

By the generalised triangle inequality we have

$$|[i]||l_i(x)| \leqslant |[j]||l_j(x)| + |A_{i,j}| + |S_{i,j}| + |T_{i,j}|$$
$$\text{and } |[j]||l_j(x)| \leqslant |[i]||l_i(x)| + |A_{i,j}| + |S_{i,j}| + |T_{i,j}|.$$

Thus

$$|[i]||l_i(x)| - |[j]||l_j(x)| \leqslant |A_{i,j}| + |S_{i,j}| + |T_{i,j}| =: C(i,j)$$
$$|[j]||l_j(x)| - |[i]||l_i(x)| \leqslant |A_{i,j}| + |S_{i,j}| + |T_{i,j}| = C(j,i)$$
$$\Rightarrow \big||[i]||l_i(x)| - |[j]||l_j(x)|\big| \leqslant C(i,j).$$

We may then complete this process for all pairs of rays $i', j' \in I$ such that there exist $d_1', e_1' \in \mathbb{N}$ such that $X_{[i'],d_1'} \sqcup X_{[j'],e_1'}$ is almost equal to an infinite orbit of a. Let $\hat{C}(a,b)$ denote the maximum of all of the $C(i',j')$.

Now, consider if $k, k' \in I$ satisfy $[k] \sim_a [k']$. This means that there exist $k^{(1)}, k^{(2)}, \ldots, k^{(f)} \in I$ and $d_1^{(0)}, d_1^{(1)}, \ldots, d_1^{(f)}, e_1^{(1)}, \ldots, e_1^{(f)}, e_1^{(f+1)} \in \mathbb{N}$ such that for all $p \in \mathbb{Z}_{f-1}$

$$X_{[k],d_1^{(0)}} \sqcup X_{[k^{(1)}],e_1^{(1)}}, X_{[k^{(p)}],d_1^{(p)}} \sqcup X_{[k^{(p+1)}],e_1^{(p+1)}}, \text{ and } X_{[k^{(f)}],d_1^{(f)}} \sqcup X_{[k'],e_1^{(f+1)}}$$

are almost equal to orbits of a. We wish to bound $\big||[k]||l_k(x)| - |[k']||l_{k'}(x)|\big|$, and will do this by producing bounds for

$$|[k]||l_k(x)| - |[k']||l_{k'}(x)| \text{ and } |[k']||l_{k'}(x)| - |[k]||l_k(x)|.$$

We start by rewriting $|[k]||l_k(x)| - |[k']||l_{k'}(x)|$ as

$$\big(|[k]||l_k(x)| - |[k^{(1)}]||l_{k^{(1)}}(x)|\big) + \big(|[k^{(1)}]||l_{k^{(1)}}(x)| - |[k^{(2)}]||l_{k^{(2)}}(x)|\big) + \ldots$$
$$\ldots + \big(|[k^{(f-1)}]||l_{k^{(f-1)}}(x)| - |[k^{(f)}]||l_{k^{(f)}}(x)|\big) + \big(|[k^{(f)}]||l_{k^{(f)}}(x)| - |[k']||l_{k'}(x)|\big)$$

which by definition is bounded by

$$C(k, k^{(1)}) + \sum_{q=1}^{f-1} C(k^{(q)}, k^{(q+1)}) + C(k^{(f)}, k')$$

and so

$$\begin{aligned}|[k]||l_k(x)| - |[k']||l_{k'}(x)| &\leqslant C(k,k^{(1)}) + \sum_{q=1}^{f-1} C(k^{(q)},k^{(q+1)}) + C(k^{(f)},k') \\ &\leqslant (f+1)\hat{C}(a,b) \\ &\leqslant n\cdot \hat{C}(a,b)\end{aligned}$$

Similarly, $|[k']||l_{k'}(x)|-|[k]||l_k(x)| \leqslant (f+1)\hat{C}(a,b) \leqslant n\cdot\hat{C}(a,b)$. Thus $n\cdot\hat{C}(a,b)+1$ is a suitable value for $K(a,b)$.

Now we note that, without knowledge of the conjugator x, for all k,k' such that $X_{[k],d_1} \sqcup X_{[k'],e_1}$ is almost equal to an infinite orbit of a, the sets $S_{k,k'}$ and $T_{k,k'}$ are computable, and so the constants $C(k,k')$ are also computable. Hence $\hat{C}(a,b)$ and so $K(a,b)$ are computable using only the elements a and b. □

We shall now show that, if a is conjugate to b in $H_n^*(a)$, then there is a conjugator $x \in H_n^*(a)$ such that for all $i \in I$ there exists a $j \in I$ such that $[j] \sim_a [i]$ and $t_j(x) = 0$. This will allow us to use the previous proposition to bound $|t_k(x)|$ for all $[k] \sim_a [j]$. We will produce such a conjugator using an adaptation of the element defined in [ABM13, Lem 4.6]. As with their argument, we again use Lemma 4.7, which stated that if $x \in G$ conjugates a to b then $y \in G$ also conjugates a to b if and only if there exists a $c \in C_G(a)$ such that $cx = y$.

Notation. *Let $g \in H_n \rtimes S_n$ and $i \in I(g)$. Then $\mathfrak{C}_g([i]) := \{k \mid [k] \sim_g [i]\} \subseteq I(g)$. This is the set of all $k \in \mathbb{Z}_n$ corresponding to rays of X_n whose σ_g-class is related to $[i]_g$.*

Definition 4.19. Let $g \in H_n \rtimes S_n$ and fix an $i \in I(g)$. Then $g_{[i]}$ is defined to be equal to the product of all cycles of g_∞ which have support almost equal to $X_{[j'],d_1}(g) \sqcup X_{[j''],e_1}(g)$ where $j', j'' \in \mathfrak{C}_g([i])$ and $d_1, e_1 \in \mathbb{N}$.

An element $g \in \mathrm{Sym}(X_n)$ is in $H_n \rtimes S_n$ if and only if there exists an isometric permutation of the rays σ and an element $h \in H_n$ such that $g = h\sigma$. Also, since $(H_n)\pi \cong \mathbb{Z}^{n-1}$ (where $\pi : g \mapsto (t_1(g), t_2(g), \ldots, t_n(g))$), we have for any choice of $a_1, \ldots, a_{n-1} \in \mathbb{Z}$ that there exists an $h \in H_n$ with $t_i(h) = a_i$ for all $i \in \mathbb{Z}_{n-1}$ and $t_n(h) = -\sum_{s=1}^{n-1} t_s(h)$.

Lemma 4.20. *Let $g \in H_n \rtimes S_n$. For every $i \in I, g_{[i]}$ lies in $C_{H_n \rtimes S_n}(g)$.*

Proof. Fix an $i \in I(g)$. By considering $g_{[i]}$ and g in $\mathrm{Sym}(X_n)$, the commutativity follows since we are choosing disjoint cycles from g_∞. Notice that we will only choose finitely many disjoint cycles from g since it only has finitely many infinite orbits. Thus $\mathrm{supp}(g_{[i]})$ and $\{(k,m) \mid k \in I^c(g), m \in \mathbb{N}\}$ have finite intersection. Let $[j] \sim_g [i]$. Then any infinite orbit of g containing a subset almost equal to $X_{[j],d}$ (for any $d \in \mathbb{N}$) will be an infinite orbit of $g_{[i]}$. Thus if $g_{[i]}$ has an orbit almost equal to $X_{[i'],d_1'} \sqcup X_{[j'],e_1'}$ for any $i', j' \in I(g)$ and some $d_1', e_1' \in \mathbb{N}$, then for every $d \in \mathbb{N}$ there is an orbit of $g_{[i]}$ containing a subset almost equal to $X_{[i'],d}$ and an orbit of $g_{[i]}$ containing a subset almost equal to $X_{[j'],d}$. Let $(k,m) \in X_n$ with $m \geqslant z_k(g)$. Then

$$(k,m)g_{[i]} = \begin{cases} (k,m)g & \text{if } [k] \sim_g [i] \text{ and } m \geqslant z_k(g) \\ (k,m) & \text{otherwise.} \end{cases}$$

Now let h and σ satisfy

$$t_k(h) := \begin{cases} t_k(g) & \text{if } [k] \sim_g [i] \\ 0 & \text{otherwise} \end{cases} \quad \text{and } (k,m)\sigma := \begin{cases} (k,m)\sigma_g & \text{if } [k] \sim_g [i] \\ (k,m) & \text{otherwise.} \end{cases}$$

Now, since h restricts to a bijection on X_n, we have that $\sum_{i=1}^{n} t_i(h) = 0$. Hence we may choose h such that $g_{[i]} = h\sigma$ with $h \in H_n$ and σ an isometric permutation of the rays. □

An immediate consequence of this lemma is that for any $g \in H_n \rtimes S_n$, the element $(g_{[i]})^{|\sigma_g|}$ is in $C_{H_n}(g)$.

Lemma 4.21. *Let $a, b \in H_n \rtimes S_n$ be conjugate by some $x \in H_n^*(a)$. Then there exists a conjugator $x' \in H_n^*(a)$ which, for each $i \in I$, there is a j such that $[j] \sim_a [i]$ and $t_j(x') = 0$.*

Proof. Let $x \in H_n^*(a)$ conjugate a to b. From the definition of $H_n^*(a)$, we have for all $i \in I$ that $t_i(x) \equiv 0 \bmod |t_i(a^{|\sigma_a|})|$. Thus there exist constants $m_1, \dots, m_n \in \mathbb{Z}$ such that, for all $i \in I$,

$$t_i(x) = m_i |t_i(a^{|\sigma_a|})|.$$

Also recall that, for any $i \in I$, $\mathfrak{C}_a([i]) := \{k \mid [k] \sim_a [i]\}$. The sets $\mathfrak{C}_a([i])$ partition I. Let $R(a) := \{j^1, \dots j^u\} \subseteq I$ be representatives of $\sim_a$-classes (so that $a_\infty = \prod_{s=1}^{u} a_{[j^s]}$). Thus, for any given $i \in I$, there is a unique $d \in \{1, \dots, u\}$ such that $[j^d] \sim_a [i]$. Choose some $j \in R(a)$ and consider

$$(a_{[j]})^{-|\sigma_a| m_j} x.$$

First, by Lemma 4.20, $(a_{[j]})^{|\sigma_a|} \in C_{H_n}(a)$. Moreover, $(a_{[j]})^{|\sigma_a|} \in H_n^*(a)$. Hence, for any $d \in \mathbb{Z}$, $(a_{[j]})^{|\sigma_a| d} \in C_{H_n^*(a)}(a)$. We now note that

$$t_j(a_{[j]}^{-|\sigma_a| m_j} x) = 0$$

and that $a_{[j]}^{-|\sigma_a| m_j} x$ conjugates a to b by Lemma 4.7. Thus a suitable candidate for x' is

$$\prod_{j \in R(a)} a_{[j]}^{-|\sigma_a| m_j} x.$$

□

Recall that $M_I(a,b)$ was a number such that, if $a, b \in H_n \rtimes S_n$ are $H_n^*(a)$-conjugated, there exists an $x \in H_n^*(a)$ which conjugates a to b and $\sum_{i \in I} |t_i(x)| < M_I(a,b)$.

Proposition 4.22. *Let $a, b \in H_n \rtimes S_n$ be $H_n^*(a)$-conjugated. Then a number $M_I(a,b)$ is computable.*

Proof. Let $S(a) := \{i^1, \dots, i^v\} \subseteq I$ be representatives of I, so that $\bigsqcup_{i \in S(a)} [i] = I$ and, for any distinct $d, e \in \mathbb{Z}_v$, we have $[i^d] \neq [i^e]$. We work for a computable bound for $\{|l_i(x)| \mid i \in S(a)\}$ since $t_i(x) = l_i(x)|t_{[i]}(a)|$ and the numbers $|t_{[i]}(a)|$ and $|\sigma_a|$ are computable. Lemma 3.10 from Section 3.2 will then provide a bound for $|l_i(x)|$ for all $i \in I$. Proposition 4.18 says that there is a computable number $K(a,b) =: K$ such that for every $i, j \in I$ where $[i] \sim_a [j]$, we have

$$\big| |[i]| |l_i(x)| - |[j]| |l_j(x)| \big| < K.$$

By Lemma 4.21, we can assume that for any given $i \in S(a)$, either $t_i(x) = 0$ or there exists a $j \in I$ such that $[j] \sim_a [i]$ and $t_j(x) = 0$. If $t_i(x) = 0$, then we are done. Otherwise,

$$\big||[i]||l_i(x)| - |[j]||l_j(x)|\big| < K \Rightarrow \big||[i]||l_i(x)|\big| < K \Rightarrow |l_i(x)| < \frac{K}{|[i]|} < K.$$

Continuing this process for each $i \in S(a)$ (of which there are at most n) implies that

$$\sum_{i \in S(a)} |l_i(x)| < nK.$$

We may then compute, using Lemma 3.10 from Section 3.2, a number K' such that

$$\sum_{i \in I} |l_i(x)| < K'.$$

A suitable value for $M_I(a,b)$ is therefore $K' \cdot \max\{|t_{[i]}(a)| : i \in I\}$. □

4.4. **Showing that the numbers $\{y_j(g,h) \mid j \in I^c\}$ are computable.** In this section we will show, given any $g, h \in H_n \rtimes S_n$, numbers $\{y_j(g,h) \mid j \in I^c(g)\}$ are computable such that if there exists an $x \in H_n^*(g)$ which conjugates g to h, then there is an $x' \in H_n^*(g)$ which conjugates g to h such that $t_i(x') = t_i(x)$ for all $i \in I(g)$ and $t_j(x') = y_j(g,h)$ for all $j \in I^c(g)$. From the previous section, the number $M_I(g,h)$ is computable. From the arguments of Section 4.2, it is now sufficient to show that such numbers $\{y_j(g,h) \mid j \in I^c\}$ are computable for any $g, h \in H_n \rtimes S_n$ in order to solve TCP(H_n) for any $n \geqslant 2$.

Note that the condition on elements to be in $H_n^*(g)$ provides no restriction on the translation lengths for the rays in $I^c(g)$. This means that the arguments in this section work as though our conjugator is in H_n.

From Section 3.1 we have that for any $g \in H_n \rtimes S_n$, any point (j,m) such that $j \in I^c(g)$ and $m \geqslant z_j(g)$ lies in an orbit of g of size $|[j]|$.

Notation. *Let $g \in H_n \rtimes S_n$ and $r \in \mathbb{N}$. Then $I^c_r(g) := \{j \in I^c(g) \mid |[j]| = r\}$. Also, we may choose $j_r^1, \dots, j_r^u$ such that $[j_r^1] \cup [j_r^2] \cup \dots \cup [j_r^u] = I^c_r(g)$ and $[j_r^k] \cap [j_r^{k'}] = \emptyset$ for every distinct $k, k' \in \mathbb{Z}_u$. We shall say that $j_r^1, \dots, j_r^u$ are representatives of $I^c_r(g)$.*

Lemma 4.23. *Let $g, h \in H_n \rtimes S_n$ and $r \in \mathbb{N}$. If $x_1, x_2 \in H_n$ both conjugate g to h and $j_r^1, \dots, j_r^u$ are representatives of $I^c_r(g)$, then*

$$\sum_{s=1}^{u} t_{j_r^s}(x_1) = \sum_{s=1}^{u} t_{j_r^s}(x_2).$$

Proof. Fix an $r \in \mathbb{N}$ and let $j_r^1, \dots, j_r^u$ be representatives of $I^c_r(g)$. Let d, d' be distinct numbers in $\mathbb{Z}_u$, $[j_r^d] := \{k_1, \dots, k_r\}$, $[j_r^{d'}] := \{k'_1, \dots, k'_r\}$, and let $c_{j_r^d, j_r^{d'}} \in \mathrm{Sym}(X_n)$ be defined by

$$(i,m)c_{j_r^d, j_r^{d'}} := \begin{cases} (i, m+1) & \text{if } i \in [j_r^d] \text{ and } m \geqslant z_i(g) \\ (i, m-1) & \text{if } i \in [j_r^{d'}] \text{ and } m \geqslant z_i(g) + 1 \\ (k_e, z_{k_e}(g)) & \text{if } i = k'_e \text{ and } m = z_{k_{e'}}(g) \\ (i,m) & \text{otherwise.} \end{cases}$$

Note that $c_{j_r^d, j_r^{d'}} \in C_{H_n}(g)$. Thus, given $x_1, x_2 \in H_n$ which both conjugate g to h, it is possible to produce, by multiplying by an element of the centraliser which is a product of elements $c_{j_r^1,k}$ (with $k \in \{j_r^2, \dots, j_r^u\}$), elements $x_1', x_2' \in H_n$ which both conjugate g to h and for which $t_{j_r^s}(x_1') = 0 = t_{j_r^s}(x_2')$ for all $s \in \{2, \dots, u\}$ and so by Lemma 3.10, $t_j(x_1') = t_j(x_2')$ for all $j \in I_r^c(g) \setminus [j_r^1]$. By construction we then have that

$$t_{j_r^1}(x_1') = \sum_{s=1}^{u} t_{j_r^s}(x_1) \text{ and } t_{j_r^1}(x_2') = \sum_{s=1}^{u} t_{j_r^s}(x_2).$$

Now consider $y := x_1'(x_2')^{-1}$. By construction $t_j(y) = 0$ for all $j \in I_r^c(g) \setminus [j_r^1]$ since $t_j(x_1') = t_j(x_2')$ for all $j \in I_r^c(g) \setminus [j_r^1]$. Also $t_j(y) = t_{j_r^1}(y)$ for all $j \in [j_r^1]$ since y conjugates g to g (and so we also have that $y \in C_{H_n}(g)$). If $t_{j_r^1}(y) \neq 0$, then y contains an infinite cycle with support intersecting the branch j_r^1 and a branch $j_p \in I^c(g) \setminus I_r^c(g)$ so that $|[j_p]| = p \neq r$ i.e. the infinite cycle contains $(j_r^1, m_1), (j_p, m_2) \in X_n$. This means there exists an $e \in \mathbb{Z}$ such that $(j_r^1, m_1)y^e = (j_p, m_2)$. But then $y^e \in C_{H_n}(g)$ and y^e sends an r-cycle to an p-cycle where $r \neq p$, a contradiction. Hence for any $x, x' \in H_n$ which both conjugate g to h,

$$\sum_{s=1}^{u} t_{j_r^s}(x) = \sum_{s=1}^{u} t_{j_r^s}(x').$$

□

From this proof, the following is well defined.

Notation. *Let $g, h \in H_n \rtimes S_n$, $r \in \mathbb{N}$ and $j_r^1, \dots, j_r^u$ be representatives of $I_r^c(g)$. Then $M_{\{j_r^1,\dots,j_r^u\}}(g, h)$ denotes the number such that, for any $x \in H_n^*(g)$ which conjugates g to h, $\sum_{d=1}^{u} t_{j_r^d}(x) = M_{\{j_r^1,\dots,j_r^u\}}(g, h)$. Since we will fix a set of representatives, we will often denote $M_{\{j_r^1,\dots,j_r^u\}}(g, h)$ by $M_r(g, h)$.*

Also from this proof, if g and h are H_n-conjugated, then for any values $y_1, \dots, y_u \in \mathbb{Z}$ such that $\sum_{d=1}^{u} y_d = M_{\{j_r^1,\dots,j_r^u\}}(g, h)$, there exists an $x \in H_n^*(a)$ which conjugates g to h with $t_{j_r^d}(x) = y_d$ for all $d \in \mathbb{Z}_u$. We will show that one combination $\{y_d \in \mathbb{Z} \mid d \in \mathbb{Z}_u\}$ is computable in order to show, for any $g, h \in H_n \rtimes S_n$ and any $r \in \mathbb{N}$, that $M_r(g, h)$ is computable. The following will be useful for this. Recall that for any $g \in H_n \rtimes S_n$, $Z(g) := \{(i, m) \in X_n \mid i \in \mathbb{Z}_n \text{ and } m < z_i(g)\}$.

Notation. *Let $g \in H_n \rtimes S_n$ and $r \geqslant 2$. Then $\eta_r(g) := |\operatorname{supp}(g_r|Z(g_r))|/r$ denotes the number of orbits of $g_r\big|Z(g_r)$ of length r. This is well defined since Lemma 4.3 states that g_r restricts to a bijection on $Z(g_r)$. Also, let $\eta_1(g) := Z(g) \setminus (\operatorname{supp}(g\big|Z(g))$. Since $Z(g_r)$ is finite for all $r \in \mathbb{N}$, we have that $\eta_r(g)$ is finite for all $r \in \mathbb{N}$.*

We now prove that, for any $r \in \mathbb{N}$ and any $g, h \in H_n \rtimes S_n$, the numbers $M_r(g, h)$ are computable. Within the proof we also choose the values for $\{y_j(g, h) \mid j \in I^c(g)\}$ which we shall use, but note that any combination of values which sum to $M_r(g, h)$ would be suitable.

Lemma 4.24. *Let $g, h \in H_n \rtimes S_n$, $r \in \mathbb{N}$ and $j_r^1, \dots, j_r^u$ be representatives of $I_r^c(g)$. Then $M_{\{j_r^1,\dots,j_r^u\}}(g, h)$ is computable (using only the elements g and h).*

Proof. For each $r \in \mathbb{N}$, x must send the r-cycles of g to the r-cycles of h. First, we fix an $r \in \mathbb{N}$ and let $j_r^1, \dots, j_r^u$ be representatives of $I_r^c(g)$. Consider the case where $\eta_r(g) = \eta_r(h) = 0$ and g and h are conjugate by some $x \in H_n^*(a)$. This means that all of the r-cycles of g and h lie outside of $Z(g)$ and $Z(h)$ respectively. One way for a potential conjugator to therefore act is to restrict to a bijection between the

r-cycles of g on the ray j_r^d and the r-cycles of h on the ray j_r^d for each $d \in \mathbb{Z}_n$. Thus suitable values for $\{y_d(g,h) \mid d \in \mathbb{Z}_u\}$ such that $x \in H_n$ conjugates g to h and $t_{j_r^d}(x) = y_d(g,h)$ for all $d \in \mathbb{Z}_u$ are given by:

$$y_k(g,h) = z_k(h) - z_k(g) \text{ for all } k \in \{j_r^1, \dots, j_r^u\}. \tag{19}$$

We now wish to generalise this. Given any $g, h \in H_n \rtimes S_n$ which are H_n-conjugated, let

$$y_k(g,h) = z_k(h) - z_k(g) \text{ for all } k \in \{j_r^2, \dots, j_r^u\}. \tag{20}$$

For each cycle in $Z(g_r)$, increase $t_{j_r^1}(x)$ by 1. Similarly, for each cycle in $Z(h_r)$, decrease $t_{j_r^1}(x)$ by 1. This means that

$$y_{j_r^1}(g,h) = z_k(h) - z_k(g) + \eta_r(g) - \eta_r(h). \tag{21}$$

We work towards proving that the values for $y_k(g,h)$ defined in (20) and (21) are suitable in 3 steps. First, consider if $\eta_r(g) = \eta_r(h)$. This means that there is a conjugator in FSym which conjugates $g_r\big|Z(g_r)$ to $h_r\big|Z(h_r)$ i.e. the eventual translation lengths defined in (19) are sufficient. Second, consider if $\eta_r(g) = \eta_r(h) + d$ for some $d \in \mathbb{N}$. In this case, first send $\eta_r(g) - \eta_r(h)$ r-cycles in $Z(g_r)$ to those in $Z(h_r)$. Then send the d remaining cycles in $Z(g_r)$ to the first d r-cycles on the branches $[j_r^1]$ by increasing $y_{j_r^1}(g,h)$ by d. Finally, if $\eta_r(g) = \eta_r(h) - e$ for some $e \in \mathbb{N}$, then send the $\eta_r(g)$ r-cycles in $Z(g_r)$ to r-cycles in $Z(h_r)$ and then send the first e r-cycles of g on the branches $[j_r^1]$ to the remaining r-cycles in $Z(h_r)$ by decreasing $y_{j_r^1}(g,h)$ by e. With all of these cases, the values defined in (20) and (21) are suitable. □

Proof of Theorem 1. From Remark 4.14 and Remark 4.15 of Section 4.2, $\mathrm{TCP}(H_n)$ is solvable if, given $a, b \in H_n \rtimes S_n$, the numbers $M_I(a,b)$ and $\{y_j(a,b) \mid j \in I^c\}$ are computable from only a and b. Thus, from the work of this section and the previous section, $\mathrm{TCP}(H_n)$ is solvable. □

5. Applications of Theorem 1

Our strategy is to use [BMV10, Thm. 3.1]. We first set up the necessary notation.

Definition 5.1. Let H be a group and $G \trianglelefteq H$. Then $A_{G \trianglelefteq H}$ denotes the subgroup of $\mathrm{Aut}(G)$ consisting of those automorphisms induced by conjugation by elements of H i.e. $A_{G \trianglelefteq H} := \{\phi_h \mid h \in H\}$.

Definition 5.2. Let G be a finitely presented group. Then $A \leqslant \mathrm{Aut}(G)$ is *orbit decidable* if, given any $a, b \in G$, there is an algorithm which decides whether there is a $\phi \in A$ such that $a\phi = b$. If $\mathrm{Inn}(G) \leqslant A$, then this is equivalent to finding a $\phi \in A$ and $x \in G$ such that x conjugates $a\phi$ to b.

The algorithmic condition in the following theorem means that certain computations for D, E, and F are possible. This is satisfied by our groups being given by recursive presentations, and the maps between them being defined by the images of the generators.

Theorem 5.3. (*Bogopolski, Martino, Ventura* [BMV10, Thm. 3.1]). *Let*

$$1 \longrightarrow D \longrightarrow E \longrightarrow F \longrightarrow 1$$

be an algorithmic short exact sequence of groups such that

(i) *D has solvable twisted conjugacy problem,*

(ii) *F has solvable conjugacy problem, and*
(iii) *for every $1 \neq f \in F$, the subgroup $\langle f \rangle$ has finite index in its centralizer $C_F(f)$, and there is an algorithm which computes a finite set of coset representatives, $z_{f,1}, \ldots, z_{f,t_f} \in F$,*

$$C_F(f) = \langle f \rangle z_{f,1} \sqcup \cdots \sqcup \langle f \rangle z_{f,t_f}.$$

Then, the conjugacy problem for E is solvable if and only if the action subgroup $A_{D \trianglelefteq E} = \{\phi_g \mid g \in E\} \leqslant Aut(D)$ is orbit decidable.

Remark. *For all that follows, the action subgroup $A_{D \trianglelefteq E}$ is provided as a recursive presentation where the generators are words from* Aut(D).

5.1. **Conjugacy for finite extensions of H_n.** Note that when we say that B is a finite extension of A we mean that $A \trianglelefteq B$ and that A is finite index in B. The following is well known.

Lemma 5.4. *If G is finitely generated and H is a finite extension of G, then H is finitely generated.*

Proposition 5.5. *Let $n \geqslant 2$. If E is a finite extension of H_n, then CP(E) is solvable.*

Proof. Within the notation of Theorem 5.3, set $D := H_n$ and F to be a finite group so to realise E as a finite extension of H_n. Since F is finite, it is well known that conditions (ii) and (iii) of Theorem 5.3 are satisfied (see, for example, [TC36]). The main theorem of the previous section (Theorem 1) states that condition (i) is satisfied. Thus CP(E) is solvable if and only if $A_{H_n \trianglelefteq E} = \{\phi_e \mid e \in E\}$ is orbit decidable. We note that $A_{H_n \trianglelefteq E}$ contains a copy of H_n (since H_n is centreless). Moreover, it can be considered as a group lying between H_n and $H_n \rtimes S_n$. Hence $A_{H_n \trianglelefteq E}$ is isomorphic to a finite extension of H_n, and so by Lemma 5.4 is finitely generated. Thus $A_{H_n \trianglelefteq E} = \langle \phi_{e_1}, \phi_{e_2}, \ldots, \phi_{e_k} \rangle$ where $\{e_1, \ldots, e_k\}$ is a finite generating set of E. From Lemma 3.7, given any $g \in N_{\mathrm{Sym}(X_n)}(H_n) \cong \mathrm{Aut}(H_n)$, we may compute σ_g: the isometric permutation of the rays induced by g. Thus we may compute $\langle \sigma_{e_i} \mid i \in \mathbb{Z}_k \rangle =: E_\sigma$. Now, given $a, b \in H_n$, our aim is to decide whether there exists $\phi_e \in A_{H_n \trianglelefteq E}$ such that $(a)\phi_e = b$. Since $\mathrm{Inn}(H_n) \leqslant A_{H_n \trianglelefteq E}$, this is equivalent to finding a $\tau \in E_\sigma$ and $x \in H_n$ such that $(x\tau)^{-1} a (x\tau) = b$, which holds if and only if $x^{-1} a x = \tau b \tau^{-1}$.

Finally, since E_σ is finite (there are at most $n!$ permutations of the rays), searching for an $x \in H_n$ which conjugates a to $\sigma_e b \sigma_e^{-1}$ for all $\sigma_e \in E_\sigma$ provides us with a suitable algorithm. Searching for such a conjugator can be achieved by Theorem 1 or [ABM13, Thm. 1.2]. □

5.2. **Conjugacy for finite index subgroups of H_n.** Recall that $g_2, \ldots, g_n$ were elements of H_n such that g_i: translates the first branch of X_n by 1; translates the i^{th} branch by -1; sends $(i, 1)$ to $(1, 1)$; and does not move any points of the other branches (which meant that, if $n \geqslant 3$, then $H_n = \langle g_i \mid i = 2, \ldots, n \rangle$). For any given $n \geqslant 2$, the family of finite index subgroups $U_p \leqslant H_n$ were defined (for $p \in \mathbb{N}$) in [BCMR14] as follows. Note that FAlt(X) denotes the index 2 subgroup of FSym(X) consisting of all even permutations on X.

$$U_p := \langle\ \mathrm{FAlt}(X_n), g_i^p \mid i \in \{1, ..., n\}\ \rangle$$

Notation. *Let $A \leqslant_f B$ denote that A has finite index in B.*

Let $n \geqslant 3$. If p is odd, then U_p consists of all elements of H_n whose eventual translation lengths are all multiples of p. If p is even, then U_p consists of all elements u of H_n whose eventual translations are all multiples of p and

$$u \prod_{i=2}^{n} g_i^{t_i(u)} \in \mathrm{FAlt}(X_n) \tag{22}$$

i.e. $\mathrm{FSym}(X_n) \leqslant U_p$ if and only if p is odd. This can be seen by considering, for some $i, j \in \mathbb{Z}_n$, the commutator of g_i^p and g_j^p. This will produce p 2-cycles which will produce an odd permutation if and only if p is odd. If $n = 2$, then for all $p \in \mathbb{N}$ all $u \in U_p \leqslant H_2$ will satisfy (22).

Lemma 5.6 (Burillo, Cleary, Martino, Röver [BCMR14])**.** *Let $n \geqslant 2$. For every finite index subgroup U of H_n, there exists a $p \geqslant 2$ with*

$$\mathrm{FAlt}(X_n) = U_p' < U_p \leqslant_f U \leqslant_f H_n.$$

where U_p' denotes the commutator subgroup of U_p.

Alternative proof. Let $n \geqslant 2$ and let $U \leqslant_f H_n$. Thus $\mathrm{FAlt} \cap U \leqslant_f \mathrm{FAlt}$. Since FAlt is both infinite and simple, $\mathrm{FAlt} \leqslant U$. Let $\pi_n : H_n \to \mathbb{Z}^{n-1}$, $g \mapsto (t_2(g), \ldots, t_n(g))$. Thus $(U)\pi_n \leqslant_f \mathbb{Z}^{n-1}$ and so there is a number $d \in \mathbb{N}$ such that $(d\mathbb{Z})^{n-1} \leqslant (U)\pi_n$ ($[(U)\pi_n : \mathbb{Z}^{n-1}]$ is one such value for d). Choose this d to be minimal (so that if $d' < d$ then $(d'\mathbb{Z})^{n-1} \nleqslant (U)\pi_n$). This means that for any $k \in \mathbb{Z}_n \setminus \{1\}$ there exists a $u \in U$ such that $t_k(u) = -d$, $t_1(u) = d$, and $t_i(u) = 0$ otherwise. Moreover, for each $k \in \mathbb{Z}_n \setminus \{1\}$ there is a $\sigma \in \mathrm{FSym}$ such that $g_k^d \sigma \in U$. First, let $n \geqslant 3$. Since $\mathrm{FAlt} \leqslant U$, we may assume that either σ is trivial or is a 2-cycle with disjoint support from $\mathrm{supp}(g_i)$. Thus $(g_k^d\sigma)^2 = g_k^{2d} \in U$. If $n = 2$, we may assume that σ is either trivial or equal to $((1, s)\ (1, s+1))$ for any $s \in \mathbb{N}$. Now, by direct computation, $g_2^d((1,1)\ (1,2))g_2^d((1, d+1)\ (1, d+2)) = g_2^{2d}$. Thus, for any $n \geqslant 2$,

$$\langle g_2^{2d}, \ldots, g_n^{2d}, \mathrm{FAlt}(X_n)\rangle \leqslant U$$

Hence, if $p := 2d$, then $U_p \leqslant U$. □

Remark. $\{(U_p)\pi_n \mid p \in \mathbb{N}\}$ *are the congruence subgroups of* $\mathbb{Z}^{n-1}$.

Now, given $U \leqslant_f H_n$, our strategy for showing that $\mathrm{CP}(U)$ is solvable is as follows. First, we show for all $p \in \mathbb{N}$ that $\mathrm{TCP}(U_p)$ is solvable. Using Theorem 5.3, we then obtain that all finite extensions of U_p have solvable conjugacy problem. By the previous lemma, we have that any finite index subgroup U of H_n is a finite extension of some U_p (note that $U_p \trianglelefteq U$ since $U_p \trianglelefteq H_n$). This will show that $\mathrm{CP}(U)$ is solvable.

$\mathrm{TCP}(U_p)$ requires knowledge of $\mathrm{Aut}(U_p)$. From [Cox16, Prop. 1], we have that any group G for which there exists an infinite set X where $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$ has $N_{\mathrm{Sym}(X)}(G) \cong \mathrm{Aut}(G)$ by the map $\rho \mapsto \phi_\rho$. From the proof of Lemma 5.6, we have that any finite index subgroup of H_n contains $\mathrm{FAlt}(X_n)$. Thus, if $U \leqslant_f H_n$, then $N_{\mathrm{Sym}(X_n)}(U) \cong \mathrm{Aut}(U)$ by the map $\rho \mapsto \phi_\rho$. In fact we may show that a stronger condition holds.

Lemma 5.7. *If $1 \neq N \trianglelefteq H_n$, then* $\mathrm{FAlt}(X_n) \leqslant N$.

Proof. We have that $N \cap \mathrm{FAlt}(X_n) \trianglelefteq H_n$. Since $\mathrm{FAlt}(X_n)$ is simple, the only way for our claim to be false is if $N \cap \mathrm{FAlt}(X_n)$ were trivial. Now, $N \leqslant H_n$, and so $[N, N] \leqslant \mathrm{FSym}(X_n)$. Thus $[N, N]$ must be trivial, and so N must be abelian. But the condition for elements $\alpha, \beta \in \mathrm{Sym}(X_n)$ to commute (that, when written in disjoint cycle notation, either a power of a cycle in α is a power of a cycle in β or the cycle in α has support outside of $\mathrm{supp}(\beta)$) is not preserved under conjugation by $\mathrm{FAlt}(X_n)$, and so cannot be preserved under conjugation by H_n i.e. N is not normal in H_n, a contradiction. $\square$

Remark. *It follows that all Houghton groups are monolithic: each has a unique minimal normal subgroup which is contained in every non-trivial normal subgroup. The unique minimal normal subgroup in each case will be* $\mathrm{FAlt}(X_n)$.

For any $U \leqslant_f H_n$ we now describe $N_{\mathrm{Sym}(X_n)}(U)$ in order to describe $\mathrm{Aut}(U)$. For each $U \leqslant_f H_n$, we will show that there exists an $m \in \mathbb{N}$ such that $U_m \leqslant U$ and $N_{\mathrm{Sym}(X_n)}(U) \leqslant N_{\mathrm{Sym}(X_n)}(U_m)$. This will mean that U_m is characteristic in U.

Proposition 5.8. *Let $n \geqslant 2$ and $U \leqslant_f H_n$. Then there exists an $m \in \mathbb{N}$ such that $U_m \leqslant U$ and $N_{\mathrm{Sym}(X_n)}(U) \leqslant N_{\mathrm{Sym}(X_n)}(U_m)$.*

Proof. Let $n \geqslant 2$ and $U \leqslant_f H_n$. We first introduce notation to describe U.

Notation. *For each $i \in \mathbb{Z}_n$, let $T_i(U) := \min\{t_i(u) \mid u \in U \text{ and } t_i(u) > 0\}$. Furthermore for all $k \in \mathbb{Z}_n$, let $T^k(U) := \sum_{i=1}^{k} T_i(U)$ and let $T^0(U) := 0$.*

We will now introduce a bijection $\phi_U : X_n \to X_{T^n(U)}$ which will induce a monomorphism $\hat{\phi}_U : U \to \mathrm{Sym}(X_{T^n(U)})$. Our bijection ϕ_U will send the i^{th} branch of X_n to $T_i(U)$ branches in $X_{T^n(U)}$. For simplicity let $g_1 := g_2^{-1}$. Now, for any $i \in \mathbb{Z}_n$ and $d \in \mathbb{N}$,

$$X_{i,d}(g_i^{T_i(U)}) := \{(i,m) \mid m \equiv d \bmod |t_i(g_i^{T_i(U)})|\}$$

where $|t_i(g_i^{T_i(U)})| = T_i(U)$ by the definition of g_i.

Thus the i^{th} branch of X_n may be partitioned into $T_i(U)$ parts:

$$X_{i,1}(g_i^{T_i(U)}) \sqcup X_{i,2}(g_i^{T_i(U)}) \sqcup \ldots \sqcup X_{i,T_i(U)}(g_i^{T_i(U)}).$$

We will now define the bijection ϕ_U by describing the image under ϕ_U of all points in each set $X_{i,d}(g_i^{T_i(U)})$ where $i \in \mathbb{Z}_n$ and $d \in \mathbb{Z}_{T_i(U)}$. Let $(i,m) \in X_{i,d}(g_i^{T_i(U)})$. Then

$$((i,m))\phi_U := \left(T^{i-1}(U) + d,\ \frac{m-d}{T_i(U)} + d\right)$$

i.e. ϕ_U sends, for all $i \in \mathbb{Z}_n$ and $d \in \mathbb{Z}_{T_i(U)}$, the ordered points of $X_{i,d}(g_i^{T_i(U)})$ to the ordered points of the $(T^{i-1}(U) + d)^{\text{th}}$ branch of $X_{T^n(U)}$. An example of this bijection with $n = T_1(U) = T_2(U) = T_3(U) = 3$ is given below.

We now describe the image of U under $\hat{\phi}_U$. First, $\hat{\phi}_U$ preserves cycle type. Thus $\mathrm{FAlt}(X_{T^n(U)}) \leqslant (U)\hat{\phi}_U$. Moreover $\mathrm{FSym}(X_{T^n(U)}) \leqslant (U)\hat{\phi}_U$ if and only if $\mathrm{FSym}(X_n) \leqslant U$. Secondly, by construction, for each $i \in \mathbb{Z}_{T^n(U)}$ there exists a $g \in (U)\hat{\phi}_U$ such that $t_i(g) = 1$.

Notation. *For any $n \in \mathbb{N}$ and any $i \in \mathbb{Z}_n$, let $R_i := i \times \mathbb{N}$, the i^{th} branch of X_n or $X_{T^n(U)}$, and $Q_i := (R_i)\phi_U$, so that Q_i consists of $T_i(U)$ branches of $X_{T^n(U)}$.*

Using this notation we have that, for any $g \in (U)\hat{\phi}_U$,

(23) if $t_i(g) = k$, then $t_j(g) = k$ for all j such that $R_j \subseteq Q_i$

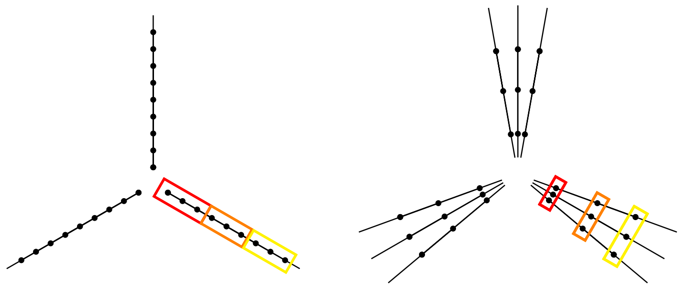


FIGURE 2. Our bijection between X_n and $X_{T^n(U)}$, which can be visualised by rotating the rectangles 90 degrees clockwise.

i.e. for any $u \in U$ and any $i \in \mathbb{Z}_n$, the eventual translation lengths of $(u)\hat{\phi}$ for the branches in Q_i must be the same.

We now describe $N_{\mathrm{Sym}(X_{T^n(U)})}((U)\hat{\phi}_U) =: G$ in order to describe $N_{\mathrm{Sym}(X_n)}(U)$. Consider if $\rho \in G$ sent an infinite subset of $R_i \subseteq X_{T^n(U)}$ to infinite subsets of $R_j, R_{j'} \subseteq X_{T^n(U)}$ with $j \neq j'$. Let $g \in (U)\hat{\phi}_U$ be chosen so that $t_i(g) = 1$. Thus g has an infinite cycle containing $\{(i, m) \mid m \geqslant z_i(g)\}$. Conjugation by an element $\tau \in \mathrm{Sym}$ changes the support of a permutation exactly by τ i.e.

$$\tau^{-1}(1\ \dots\ d)\tau = ((1)\tau\ \dots\ (d)\tau).$$

Thus $\rho^{-1}g\rho$ has an infinite cycle containing the set $\{(i, m)\rho \mid m \geqslant z_i(g)\}$. Let $(i', m') = (i, z_i(g))\rho$. Then $\{(i', m')(\rho^{-1}g\rho)^d \mid d \in \mathbb{N}\}$ has infinite intersection with R_j and $R_{j'}$. But from the description of orbits of H_n in [ABM13], $\rho^{-1}g\rho \notin H_{T^n(U)}$ and so $(\rho^{-1}g\rho)\hat{\phi}_U^{-1} \notin U$ i.e. $\rho \notin G$. Now imagine if $(R_i)\rho$ and R_j had infinite intersection but were not almost equal. Then there must be a $k \neq i$ such that $(R_k)\rho$ has infinite intersection with R_j. This is a contradiction since $(R_j)\rho^{-1}$ would then have infinite intersection with R_i and R_k. Hence if $(R_i)\rho$ and R_j have infinite intersection (where $i, j \in \mathbb{Z}_{T^n(U)}$), then $(R_i)\rho$ and R_j are almost equal.

We now consider necessary and sufficient conditions on the branches of $X_{T^n(U)}$ for there to be a $\sigma \in G$ which produces an isometric permutation of those branches. Let us assume that σ is an isometric permutation of the rays and sends $R_j \subseteq Q_k$ to $R_{j'} \subseteq Q_{k'}$. If $k = k'$ then for all $g \in (U)\hat{\phi}_U$, $t_j(g) = t_{j'}(g)$; hence all isometric permutations of the branches in Q_k will lie in G. If $k \neq k'$ then let $g \in U$ be such that $t_j(g) > 0$, $t_{j'}(g) < 0$, and $t_i(g) = 0$ for all branches i in $X_{T^n(U)} \setminus (Q_k \cup Q_{k'})$. Such an element exists by Lemma 5.6: there is a $p \in \mathbb{N}$ such that $U_p \leqslant U$. Thus $t_{j'}(\sigma^{-1}g\sigma) > 0$ and so, by (23), if $\sigma^{-1}g\sigma \in (U)\hat{\phi}_U$ then we must have for all branches i' in $Q_{k'}$ that $t_{i'}(\sigma^{-1}g\sigma) > 0$. From our choice of g, we may conclude that Q_k cannot contain fewer branches than $Q_{k'}$. Similarly $t_j(\sigma g\sigma^{-1}) < 0$ and so for all rays i in Q_k, $t_i(\sigma g\sigma^{-1}) < 0$ meaning that $Q_{k'}$ cannot contain fewer branches than Q_k. Hence Q_k and $Q_{k'}$ are of the same size and so we must have that $T_k(U) = T_{k'}(U)$.

Since the above arguments hold for any element of G which may permute the branches of $X_{T^n(U)}$, we may assume without loss of generality that $\rho \in G$ sends almost all of each branch to itself (by replacing ρ with $\rho\sigma_\rho^{-1}$ if necessary). Since, for each branch, ρ preserves the number of infinite orbits induced by g, we have for all $i \in \mathbb{Z}_{T^n(U)}$ and all $g \in (U)\hat{\phi}_U$ that $t_i(\rho^{-1}g\rho) = t_i(g)$. Fix a $k \in \mathbb{Z}_{T^n(U)}$ and choose $g \in H_n$ so that $t_k(g) = 1$. Note that $g^{-1}\rho g\rho^{-1} \in \mathrm{FSym}$. Thus there is a $d \in \mathbb{N}$ such that, for all $m > d$, $(k,m)g^{-1}\rho g\rho^{-1} = (k,m)$. For some $m' > d$, consider if $(m')\rho = m' + s$. There must be such an m' since ρ sends only finitely many points of R_i to another branch. Without loss of generality we may assume that s is positive (since we may replace ρ with ρ^{-1}). Hence

$$(k, m'+1)g^{-1}\rho g\rho^{-1} = (k,m')\rho g\rho^{-1} = (k, m'+s)g\rho^{-1} = (k, m'+s+1)\rho^{-1}.$$

But, from our assumptions, $(k, m'+1)g^{-1}\rho g\rho^{-1} = (k, m'+1)$. Hence

$$\rho : (k, m'+1) \mapsto (k, m'+s+1)$$

i.e. $\rho : (k,m) \mapsto (k, m+s)$ for all $m \geqslant m'$. Running this argument for each $i \in \mathbb{Z}_{T^n(U)}$ we have for any $\rho \in G$ that $\rho\sigma_\rho^{-1} \in H_{T^n(U)}$. Note that $H_{T^n(U)} \leqslant G$, since conjugation by elements of $H_{T^n(U)}$ preserves cycle type and the eventual translation lengths. Hence $G \leqslant H_{T^n(U)} \rtimes S_{T^n(U)}$.

To summarise, given $U \leqslant_f H_n$, we first compute $T(U) := (T_1(U), \dots T_n(U))$. We have that

$$H_{T^n(U)} \leqslant (N_{\mathrm{Sym}(X_n)}(U))\hat{\phi}_U \leqslant H_{T^n(U)} \rtimes S_{T^n(U)}.$$

Moreover, we may produce a finite a generating set for the isometric permutations of the rays of $(N_{\mathrm{Sym}(X_n)}(U))\hat{\phi}_U$ by the following process.

i) Let $i, j \in \mathbb{Z}_n$ so that

$$Q_i = \bigcup_{s=1}^{T_i(U)} R_{i_s} \text{ and } Q_j = \bigcup_{s=1}^{T_j(U)} R_{j_s}$$

for some branches $\{i_1, i_2, \dots, i_{T_i(U)}, j_1, j_2, \dots, j_{T_j(U)}\}$ of $X_{T^n(U)}$. If $T_i(U) = T_j(U)$ (i.e. Q_i and Q_j contain the same number of branches of $X_{T^n(U)}$), then define $\sigma(Q_i, Q_j)$ to have support equal to $Q_i \cup Q_j$ and to swap the branches i_s and j_s for all $s \in \mathbb{Z}_{T_i(U)}$ i.e. as a permutation of $S_{T^n(U)}$, $\sigma(Q_i, Q_j)$ can be thought of as

$$(i_1\ j_1)(i_2\ j_2)\dots(i_{T_i(U)}\ j_{T_i(U)}).$$

ii) Let $i \in \mathbb{Z}_n$ so that

$$Q_i = \bigcup_{s=1}^{T_i(U)} R_{i_s}.$$

Then for any distinct $d, e \in \mathbb{Z}_{T_i(U)}$, define $\sigma(R_{i_d}, R_{i_e})$ to have support equal to $R_{i_d} \cup R_{i_e}$ so that $\sigma(R_{i_d}, R_{i_e})$ swaps the branches R_{i_d} and R_{i_e} of Q_i. Thus $\sigma(R_{i_d}, R_{i_e})$ can be thought of as a transposition in $S_{T^n(U)}$ and by choosing the appropriate generators of type (ii) one can produce, for any $s \in \mathbb{Z}_n$, any permutation of the branches $T^s(U)+1, \dots, T^{s+1}(U)$.

Now consider the image of these elements under $\hat{\phi}_U^{-1}$. For those of type (i) described above, if $T_i(U) = T_j(U)$ we have that there is an isometric permutation of the rays of X_n which swaps the branches R_i and R_j and fixes all other branches. In order to describe the action of elements of type (ii) under $\hat{\phi}_U^{-1}$, we introduce some notation.

Notation. *Let* $Y_{i,0}(U) := \{(i,m) \mid 1 \leqslant m \leqslant T_i(U)\}$ *and, for any* $s \in \mathbb{N}$, *let* $Y_{i,s}(U) := \{(i,m) \mid sT_i(U)+1 \leqslant m \leqslant (s+1)T_i(U)\} = Y_{i,0}(U)g_i^{-sT_i(U)}$.

Thus $R_i = \bigsqcup_{s=0}^{\infty} Y_{i,s}(U) = \bigsqcup_{s=0}^{\infty} Y_{i,0}(U) g_i^{-sT_i(U)}$. We then have that, for any $i \in \mathbb{Z}_n$ and permutation $\sigma \in \mathrm{FSym}(X_n)$ with support contained within $Y_{i,0}(U)$, there exists an element u_σ in $N_{\mathrm{Sym}(X_n)}(U)$ such that for every $s \in \mathbb{N} \cup \{0\}$,

$$u_\sigma \big| Y_{i,s}(U) = g_i^{sT_i(U)} \sigma g_i^{-sT_i(U)}$$

i.e. u_σ consists of the permutation σ on every set $Y_{i,s}(U)$.

Finally, note that for any standard generator $g_i \in H_{T^n(U)}$, $\mathrm{supp}((g_i)\hat{\phi}_U^{-1}) = X_{1,1}(g_j^{T_i(U)}) \sqcup X_{j,d}(g_j^{T_i(U)}) \subseteq X_n$ for some $j \in \mathbb{Z}_n$ and $d \in \mathbb{N}$.

Notation. *Let G and H be groups and H act on a set X. Then $G \wr_X H$ denotes the permutational wreath product with base $B := \bigoplus_{x \in X} G_x$ and head H.*

For any $m \in \mathbb{N}$ and $U_m \leqslant H_n$, we have that $T(U_m) = (m, m, \ldots, m)$. Thus the sets $\{Q_i \mid i \in \mathbb{Z}_n\}$ are all of the same size and so

$$N_{\mathrm{Sym}(X_{nm})}((U_m)\hat{\phi}_{U_m}) = H_{nm} \rtimes (S_m \wr S_n).$$

Note that, for any $s \in \mathbb{N}$, $N_{\mathrm{Sym}(X_n)}(U_m) \leqslant N_{\mathrm{Sym}(X_n)}(U_{ms})$. Now, given $U \leqslant_f H_n$, choose $p \in \mathbb{N}$ such that $U_p \leqslant U$ (this is possible by Lemma 5.6). We end by showing that the generators of $N_{\mathrm{Sym}(X_n)}(U)$ all lie within $N_{\mathrm{Sym}(X_n)}(U_p)$. First, note that any isometric permutation of the rays of X_n lies in $N_{\mathrm{Sym}(X_n)}(U_p)$. Second, the permutations u_σ introduced above lie in $N_{\mathrm{Sym}(X_n)}(U_p)$ since for every $i \in \mathbb{Z}_n$ $T_i(U)$ divides $T_i(U_p)$ and so for any $i \in \mathbb{Z}_n$ there is an $f \in \mathbb{N}$ such that $Y_{i,0}(U_p) = \bigsqcup_{s=0}^{f} Y_{i,s}(U)$. Finally, for any standard generator $g_i \in H_{T^n(U)}$, we have that $(g_i)\hat{\phi}_U^{-1} \in N_{\mathrm{Sym}(X_n)}(U_p)$, since $T_i(U)$ divides $T_i(U_p)$ implies that there is a $j \in \mathbb{Z}_{T^n(U_p)}$ and an $e \in \mathbb{N}$ such that $(g_i)\hat{\phi}_U^{-1} = (g_j^e)\hat{\phi}_{U_p}^{-1}$. □

In our final section we will show that there exists an algorithm which, for any $n \geqslant 2$, $p \in \mathbb{N}$, and H_{np}-conjugated $a, b \in H_{np} \rtimes S_{np}$, decides whether a and b are $(U_p)\hat{\phi}_{U_p}$-conjugated.

Proposition 5.9. *Let $n \geqslant 2, p \in \mathbb{N}$ and $U_p \leqslant H_n$. Then TCP(U_p) is solvable.*

Proof. Our aim is to produce an algorithm which, given $a, b \in U_p$ and $\phi_\rho \in \mathrm{Aut}(U_p)$, decides whether there exists an $u \in U_p$ such that $(u^{-1})\phi_\rho a u = b$ i.e. $u^{-1}\rho a u = \rho b$. Let $\hat{\phi} := \hat{\phi}_{U_p}$. Let us rephrase our question in $(U_p)\hat{\phi}$:

$$\begin{aligned} u^{-1}\rho a u &= \rho b \\ \Leftrightarrow (u^{-1}\rho a u)\hat{\phi} &= (\rho b)\hat{\phi} \\ \Leftrightarrow (u^{-1})\hat{\phi}(\rho a)\hat{\phi}(u)\hat{\phi} &= (\rho b)\hat{\phi} \end{aligned}$$

where $(\rho a)\hat{\phi}, (\rho b)\hat{\phi} \in H_{np} \rtimes S_{np}$ and $(u)\hat{\phi} \in (U_p)\hat{\phi} \leqslant H_{np}$ from the proof of Proposition 5.8. The algorithm for TCP(H_{np}) in Section 4 may be used to produce a conjugator $x \in H_{np}$ if one exists. Given such a x, Proposition 6.1 decides whether there exists a $y \in (U_p)\hat{\phi}$ which conjugates $(\rho a)\hat{\phi}$ to $(\rho b)\hat{\phi}$. □

Proposition 5.10. *Let $n \geqslant 2$, $p \in \mathbb{N}$, and $U_p \leqslant H_n$. If E is a finite extension of U_p, then $A_{U_p \trianglelefteq E}$ is orbit decidable.*

Proof. Recall that for $A_{U_p \trianglelefteq E} = \{\phi_e \mid e \in E\}$ to be orbit decidable, there must exist an algorithm which decides, given any $a', b' \in U_p$, whether there exists a $\psi \in A_{U_p \trianglelefteq E}$ such that

$$(a')\psi = b'. \tag{24}$$

Since $\mathrm{Aut}(U_p) \cong N_{\mathrm{Sym}(X_n)}(U_p)$, we may rewrite (24) as searching for an element $\phi_\rho \in \mathrm{Aut}(U_p)$ such that

$$(a')\phi_\rho = b' \text{ and } \phi_\rho \in A_{U_p \trianglelefteq E}$$

i.e. searching for a $\rho \in E$ such that $\rho^{-1}a'\rho = b'$.

Now we rephrase this question using the map $\hat{\phi} := \hat{\phi}_{U_p}$:

$$(\rho^{-1})\hat{\phi}(a')\hat{\phi}(\rho)\hat{\phi} = (b')\hat{\phi}.$$

Let $a := (a')\hat{\phi}$, $b := (b')\hat{\phi}$, and $y := (\rho)\hat{\phi}$. Thus $a, b \in (U_p)\hat{\phi} \leqslant H_{np}$ are known, and y must be chosen to be any element in $(E)\hat{\phi}$ so that $y^{-1}ay = b$. Recall that

$$H_{np} \leqslant (E)\hat{\phi} \leqslant H_{np} \rtimes S_{np}.$$

As with the proof of Proposition 5.5, let $E_\sigma := \langle \sigma_e \mid e \in (E)\hat{\phi} \rangle$. For each isometric permutation of the rays $\tau \in E_\sigma$, we may then decide whether there is an $x \in H_{np}$ such that $x^{-1}ax = \tau b \tau^{-1}$ by Theorem 1 or [ABM13, Thm. 1.2]. □

Proposition 5.11. *Let $n \geqslant 2$ and $U_p \trianglelefteq_f G$. Then CP(G) is solvable.*

Proof. We again use [BMV10, Thm. 3.1]. G is a finite extension of U_p by F, some finite group. TCP(U_p) is solvable by Proposition 5.9. $A_{U_p \trianglelefteq G}$ is orbit decidable by Proposition 5.10. Hence CP(G) is solvable. □

5.3. **Conjugacy for groups commensurable to H_n.** Recall that A and B are commensurable if and only if there exist $N_A \cong N_B$ with N_A finite index and normal in A and N_B finite index and normal in B. Our aim is to prove Theorem 2, that, for any $n \geqslant 2$ and any group G commensurable to H_n, CP(G) is solvable.

Proof of Theorem 2. Fix an $n \geqslant 2$ and let G and H_n be commensurable. Then there is a $U \trianglelefteq_f G, H_n$. Let $p \in \mathbb{N}$ be chosen as in our proof of Lemma 5.6, so that $U_p \leqslant_f U$. We therefore wish to show that $U_p \trianglelefteq G$ so that we may apply Proposition 5.11 to obtain that CP(G) is solvable. It is a well know result that if A is characteristic in B and B is normal in C, then A is normal in C.

In the proof of Proposition 5.8 it is shown that $N_{\mathrm{Sym}(X_n)}(U) \leqslant N_{\mathrm{Sym}(X_n)}(U_p)$. Hence every automorphism of U is an automorphism of U_p (since if $\phi_\rho \in \mathrm{Aut}(U)$ then $\phi_\rho \in \mathrm{Aut}(U_p)$). Thus U_p is characteristic in U and so $U_p \trianglelefteq G$ and G is a finite extension of U_p. □

6. Computational results about centralisers in H_{np}

Our main aim for this section is to prove the following. Recall, from Section 5.2, that $(U_p)\hat{\phi}_{U_p} \leqslant H_{np}$. For any $U \leqslant H_{np}$, let $t(U) := \{t(u) \mid u \in U\}$.

Proposition 6.1. *Let $n \geqslant 2$, $p \in \mathbb{N}$, and $a, b \in H_{np} \rtimes S_{np}$ be H_{np}-conjugated. Then there is an algorithm which, given $a, b \in H_{np} \rtimes S_{np}$ and an $x \in H_{np}$ which conjugates a to b, decides whether a and b are $(U_p)\hat{\phi}_{U_p}$-conjugated.*

Our main tool will be Lemma 4.7, which stated that if $x \in H_{np}$ conjugates a to b then $y \in H_{np}$ also conjugates a to b if and only if there exists a $c \in C_{H_{np}}(a)$ such that $cx = y$. From this lemma, if a and b are conjugate by $x \in H_{np}$, then a and b are $(U_p)\hat{\phi}_{U_p}$-conjugated if and only if there is a $c \in C_{H_{np}}(a)$ such that $cx \in (U_p)\hat{\phi}_{U_p}$. When p is odd, $\mathrm{FSym}(X_{np}) \leqslant (U_p)\hat{\phi}_{U_p}$, and so $cx \in C_{H_{np}}(a)$ if and only if $t(cx) \in t((U_p)\hat{\phi}_{U_p})$. Our first aim is to reduce to this case. More specifically to prove, when p is even, that one can decide whether $x(\prod_{i=2}^{np} g_i^{-t_i(x)}) \in \mathrm{FAlt}(X_{np})$ and moreover one can decide whether $C_{H_{np}}(a)$ contains an odd permutation.

Remark 6.2. *If $t(x) \in (2\mathbb{Z})^n$, then the condition $x(\prod_{i=2}^{np} g_i^{-t_i(x)}) \in \mathrm{FAlt}(X_{np})$ implies that $x \in U_2 = \langle g_2^2, \ldots, g_{np}^2, \mathrm{FAlt}(X_{np})\rangle$. This condition exactly captures when an element, with suitable eventual translation lengths, lies in a subgroup U_{2d}.*

We will then work to decide whether there exists a $c \in C_{H_{np}}(a)$ such that $t(cx) \in t((U_p)\hat{\phi}_{U_p})$. We will do this by proving that there is an algorithm which, given $a \in H_{np} \rtimes S_{np}$, outputs a finite generating set for $t(C_{H_{np}}(a))$. To set the scene we begin by briefly describing the structure of such centralisers.

6.1. A description of the structure of $C_{H_{np}}(a)$ where $a \in H_{np} \rtimes S_{np}$.

It is possible to develop structure theorems for $C_{H_{np}}(a)$ for $a \in H_{np} \rtimes S_{np}$ using the arguments from [JG15]. We will take more of a 'local' view since we wish to describe a generating set for $t(C_{H_{np}}(a))$. In order to do this, the key observation is that elements of $C_{H_{np}}(a)$ conjugate a to a. Therefore, for each $r \in \mathbb{N}$, they send the r-cycles of a to the r-cycles of a. This means that any element of $C_{H_{np}}(a)$ decomposes are a product $\alpha^{(\infty)} \prod_{i \in \mathbb{N}} \alpha^{(r)}$ where

i) $\mathrm{supp}(\alpha^{(\infty)}) \subseteq \mathrm{supp}(a_\infty)$;
ii) $\mathrm{supp}(\alpha^{(1)}) \subseteq X_{np} \setminus \mathrm{supp}(a)$; and
iii) $\mathrm{supp}(\alpha^{(r)}) \subseteq \mathrm{supp}(a_r)$ for each $r \in \mathbb{N} \setminus \{1\}$.

Importantly, we always have that $\alpha^{(\infty)}$ and $\{\alpha^{(r)} \mid r \in \mathbb{N}\}$ are all elements of H_{np}. This means that a suitable generating set for $t(C_{H_{np}}(a))$ consists of elements whose support lies in exactly one of (i), (ii), or (iii) above. It may be immediately clear that the elements $c_{j_1^r, j_2^r}$ defined in Lemma 4.23 are suitable generators of $t(C_{H_{np}}(a))$ which have zero entries for each coordinate in I. We will give details in Section 6.3 below. The generators for $t(C_{H_{np}}(a))$ which have zero entries for each coordinate in I^c will be similar to the elements $\{a_{[i]} \mid i \in I\}$ (see Definition 4.19, Section 4.3). An idea of what is meant by 'similar' is best given by an example. Consider if $a = g_2^5 \in H_2$. Then $a_{[1]} = a_{[2]} = g_2^5$. But $C_{H_2}(a) = \langle g_2 \rangle$, so that g_2 may be considered as a 'root' of g_2^5. The main aim of Section 6.3 will be to prove that such 'roots' are suitable to provide our generating set and are computable from only the element a.

6.2. **Reducing the problem to showing that $t(C_{H_{np}}(a))$ is computable.** Let p be even and let $a, b \in H_{np} \rtimes S_{np}$ be conjugate by $x \in H_{np}$. Our first aim is to decide whether or not $x(\prod_{i=2}^{np} g_i^{-t_i(x)}) \in \mathrm{FAlt}(X_{np})$. This follows immediately from the solution to $\mathrm{WP}(H_n)$ in [ABM13, Lem 2.1], since this states that for any $g \in H_{np}$, a finite set is computable such that each point outside of this set is either fixed by g, or lies in an infinite orbit of g. Since $x(\prod_{i=2}^{np} g_i^{-t_i(x)}) \in \mathrm{FSym}(X_{np})$ by construction, we may use their lemma to determine the cycle type of this element. We now need to be able to decide whether there exists a $c' \in C_{H_{np}}(a)$ such that $c' \in \mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})$.

In order to decide whether such a c' exists consider, for our given $a \in H_{np} \rtimes S_{np}$, whether there are any branches $j \in I^c$. If so, either $|[j]|$ is odd or even. If $|[j]|$ is even, then we have that the first $|[j]|$-cycle on this branch is a finite order element of the centraliser which lies in $\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})$. Alternatively if $|[j]|$ is odd, then the element that permutes only the first two $|[j]|$-cycles of the branches $[j]$ provides an element of the centraliser which lies in $\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})$. If there are no such branches (i.e. if $I = \mathbb{Z}_{np}$), then from Section 3.1, all of the finite permutations of a lie inside a finite subset of X_{np}. This set is also computable (by again using [ABM13, Lem 2.1] or by computing the numbers $z_1(a), \ldots, z_{np}(a)$ using Lemma 3.7). We may therefore search for an odd permutation within this set to decide whether there is a $c' \in C_{H_{np}}(a) \cap \big(\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})\big)$. An even length cycle in $Z(a)$ will be a suitable candidate for c', and if there are two m-cycles in $Z(a)$, then the element which permutes these two cycles is also a possible candidate. Since, for every $r \in \mathbb{N}$, centralisers must restrict to a bijection on r-cycles, it is exactly in these specific circumstances that $C_{H_{np}}(a) \cap \big(\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})\big)$ is empty i.e. the case where p is even, $I = \mathbb{Z}_{np}$, there are no even length cycles in $Z(a)$, and for each odd number $m \geqslant 1$ there is at most one cycle of length m in $Z(a)$.

We now prove that producing a finite generating set for $t(C_{H_{np}}(a))$ is sufficient to produce an algorithm for Proposition 6.1. Let $\{\delta_1, \ldots, \delta_e\}$ denote a finite generating set of $t(C_{H_{np}}(a))$, and let $\hat{\delta_1}, \ldots, \hat{\delta_e} \in C_{H_{np}}(a)$ be chosen such that $t(\hat{\delta_j}) = \delta_j$ for each $j \in \mathbb{Z}_e$. We will show that such elements are computable from only a. Let $x \in H_{np}$ conjugate a to b. For now let us also assume that there is a $c' \in C_{H_{np}}(a) \cap \big(\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})\big)$. Deciding whether there is a $c \in C_{H_{np}}(a)$ such that $t(cx) \in t((U_p)\hat{\phi}_{U_p})$ is equivalent to finding powers α_i of the generators $\delta_i \in \mathbb{Z}^n$ such that

$$t(x) + \sum_{i=1}^{e} \alpha_i \delta_i \in t((U_p)\hat{\phi}_{U_p}). \tag{25}$$

Hence we must decide whether there are constants $\{a_1, \ldots, a_{n-1}\}$ and $\{\alpha_1, \ldots, \alpha_e\}$ such that

$$t(x) + \sum_{i=1}^{e} \alpha_i \delta_i = (a_1 \ldots a_1\ a_2 \ldots a_2 \ldots \ldots a_n \ldots a_n)^T, \text{ where } a_n := -\sum_{i=1}^{n-1} a_i. \tag{26}$$

Viewing this as np linear equations, if this system of equations has a solution, then an element c of $C_{H_{np}}(a)$ exists such that $cx = y \in H_{np}$ where y conjugates a to b and $t(y) \in t((U_p)\hat{\phi}_{U_p})$ (so that $y \in (U_p)\hat{\phi}_{U_p}$). If this system of equations has no solution, then no such c exists and so there is no conjugator y of a and b such that $t(y) \in$

$t((U_p)\hat{\phi}_{U_p})$ (so that there also cannot be a conjugator of a and b in $(U_p)\hat{\phi}_{U_p}$). We now deal with the case where there is no $c' \in C_{H_{np}}(a) \cap \big(\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})\big)$. Note that, from above it is decidable whether or not such a c' exists.

Notation. *Let sgn:* FSym $\to \{0,1\}$ *be the sign function for* FSym*, so that the preimage of* 0 *is* FAlt*. Also, let* $\xi : H_{np} \to \{0,1\}$, $h \mapsto sgn(h(\prod_{i=2}^{np} g_i^{-t_i(h)}))$.

We must then include the equation

$$\xi(x) + \sum_{j=1}^{e} \alpha_j \xi(\hat{\delta_j}) \equiv 0 \bmod 2 \tag{27}$$

which ensures that for the chosen $c \in C_{H_{np}}(a)$ we have $\xi(cx) = 0$ i.e. $cx \in (U_p)\hat{\phi}_{U_p}$. From these assumptions, our choice of generating set is arbitrary: if $h, h' \in C_{H_{np}(a)}$ satisfy $t(h) = t(h')$, then we must have that $h^{-1}h' \in \mathrm{FAlt}(X_{np})$, since otherwise $C_{H_{np}}(a) \cap \big(\mathrm{FSym}(X_{np}) \setminus \mathrm{FAlt}(X_{np})\big)$ would be non-empty.

By writing these equations as a matrix equation we may compute the Smith normal form and so decide whether or not the equations have an integer solution (see, for example, [Laz96]).

6.3. **Producing a finite generating set for $t(C_{H_{np}}(a))$.** Recall that, for any $i \in \mathbb{Z}_n$, the set Q_i was defined to be the image of the i^{th} branch of X_{np} under the bijection ϕ_{U_p} (which induced the homomorphism $\hat{\phi}_{U_p}$). If $u \in (U_p)\hat{\phi}_{U_p}$, then for all $i \in \mathbb{Z}_n$ and for all $k, k' \in Q_i$ we have that $t_k(u) = t_{k'}(u)$. We first describe the possible eventual translation lengths of $C_{H_{np}}(a)$. Note, for any $p \in \mathbb{N}$, that

$$t((U_p)\hat{\phi}_{U_p}) = \left\{ (\underbrace{a_1 \dots a_1}_{p} \underbrace{a_2 \dots a_2}_{p} \dots \underbrace{a_n \dots a_n}_{p})^T \;\middle|\; a_1, \dots, a_{n-1} \in \mathbb{Z}, a_n = -\sum_{i=1}^{n-1} a_i \right\}.$$

Our aim for this section is now to show that a finite generating set for $t(C_{H_{np}}(a))$ is computable from only a. Our generators of $C_{H_{np}}(a)$ will either act on rays in I or in I^c. We will first prove the elements defined in Lemma 4.23 are suitable generators of $t(C_{H_{np}}(a))$ which have zero entries for each coordinate in I. We will then show that the other generators are computable from only a.

For all $r \in \mathbb{N}$, any $g \in C_{H_{np}}(a)$ restricts to a permutation of the r-cycles of a. Thus if $|[k]_a| = 1$ and $t_k(a) = 0$, let $X := \{(k,m) \mid m \geqslant z_k(a)\}$. We then have that

$$\mathrm{FSym}(X) \leqslant C_{H_{np}}(a).$$

If $k' \neq k$ also has $|[k']| = 1$ and $t_{k'}(a) = 0$, let $X' := \{(k', m) \mid m \geqslant z_{k'}(a)\}$. Note that $c_{k,k'}$ (defined within the proof of Lemma 4.23 in Section 4.4) and the transposition μ with support $\{(k, z_k(a)), (k', z_{k'}(a)\}$ lie within $C_{H_{np}}(a)$. Moreover $\langle c_{k,k'}, \mu \rangle$ is a group isomorphic to H_2. In general, if $|\{j : |[j]| = 1 \text{ and } j \in I^c\}| = p$, then there are elements of $C_{H_{np}}(a)$ which generate a group isomorphic to H_p and each element has support contained within the fixed points of a. Similar arguments work (for any $r \in \mathbb{N}$) for the r-cycles of a. Recall that $I^c_r(g) := \{j \in I^c(g) \mid |[j]| = r\}$. If $|I^c_r(g)| = p$, then there are elements of $C_{H_{np}}(a)$ which generate a group isomorphic to H_q where $q = p/r$. The factor $1/r$ occurs since elements of $C_{H_{np}}(a)$ must restrict to a bijection of the r-cycles of a and so if $|[j]| = r$ and $t_{[j]}(a) = 0$ then, for any $m \geqslant z_j(a)$, where (j,m) is sent by a defines where $(j,m)a^d$ must be sent for all $d \in \mathbb{Z}_{|[j]|}$.

Let $\Lambda_j(a) := \{(k,m) \mid k \in [j] \text{ and } m \geqslant z_j(a)\}$. For each $r \in \mathbb{N}$, if there are $j, j' \in I_r^c(a)$ with $[j] \neq [j']$, then we shall have generators of $t(C_{H_{np}}(a))$ with support almost equal to

$$\Lambda_j(a) \sqcup \Lambda_{j'}(a).$$

The element $c_{j,j'}$ is a suitable candidate for such a generator. Recall that $c_{j,j'}$ has $t_k(x)$ non-zero for exactly $2|[j]|$ entries, corresponding to the branches $[j] \sqcup [j']$. Choosing representatives $j_r^1, \ldots, j_r^u$ for the classes of I_r^c, we note that all of the elements of

$$\{c_{j_r^d, j_r^{d'}} \mid d, d' \in \mathbb{Z}_u \text{ where } d \text{ and } d' \text{ are distinct}\} =: \Theta_r$$

lie in $C_{H_{np}}(a)$ and that no two elements of this set have the same image under t.

Finally we note that, if $j \in I_r^c(a)$ and $j' \in I_{r'}^c(a)$ with $r \neq r'$, then for all $m \geqslant z_j(a)$ and $m' \geqslant z_{j'}(a)$, no element of $C_{H_{np}}(a)$ may have an infinite cycle with support containing (j,m) and (j',m') as centralisers in Sym must send r-cycles to r-cycles. Thus generators of $t(C_{H_{np}}(a))$ with zero entries in I are given by

$$t(\bigsqcup_{r\in\mathbb{N}} \Theta_r) \tag{28}$$

which is computable since for almost all $r \in \mathbb{N}$, we have that $I_r^c(a) = \emptyset$.

We now work towards showing that our generators of $t(C_{H_{np}}(a))$ with zero entries in I^c are computable. We start by showing that they have a 'similar' form to the elements $\{a_{[i]} \mid i \in I\}$.

Lemma 6.3. *Let $g \in C_{H_{np}}(a)$ and $i \in I$. If $t_i(g) \neq 0$, then $t_j(g) \neq 0$ for all $[j] \sim_a [i]$.*

Proof. The proof is similar to that of Lemma 4.20. Fix an $i \in I$. Recall $[i] \sim_a [j]$ if and only if there exist $i^{(1)}, i^{(2)}, \ldots, i^{(q)} \in I$ and $d_1^{(0)}, d_1^{(1)}, \ldots, d_1^{(q)}, e_1^{(1)}, \ldots, e_1^{(q)}, e_1^{(q+1)}$ such that for all $p \in \mathbb{Z}_{q-1}$ each one of the sets

$$X_{[i],d_1^{(0)}} \cup X_{[i^{(1)}],e_1^{(1)}}, X_{[i^{(p)}],d_1^{(p)}} \cup X_{[i^{(p+1)}],e_1^{(p+1)}}, \text{ and } X_{[i^{(q)}],d_1^{(q)}} \cup X_{[j],e_1^{(q+1)}} \tag{29}$$

is almost equal to some infinite orbit of a. Also, if $g \in C_{\mathrm{Sym}(X_{np})}(a)$ then where g sends a point $(i,m) \in X_{np}$ defines where g must send the points $\{(i,m)a^d \mid d \in \mathbb{Z}\}$. Hence if $g \in C_{H_{np}}(a)$ and $t_i(g) \neq 0$, then g must act non-trivially on all of the orbits with infinite intersection with the i^{th} branch of X_{np}, and hence must act non-trivially on the orbit of a almost equal to $X_{[i],d_1^{(0)}} \cup X_{[i^{(1)}],e_1^{(1)}}$. This means that $t_{i^{(1)}}(g)$ must be non-zero and so g must act non-trivially on all orbits of a with infinite intersection with the branch $i^{(1)}$. Thus g must also act non-trivially on the orbit $X_{[i^{(1)}],d_1^{(1)}} \cup X_{[i^{(2)}],e_1^{(2)}}$. Continuing in this way we have that g must act non-trivially on any orbit of a which is almost equal to one of those in (29). Thus $t_j(g) \neq 0$, as required. ☐

Remark 6.4. *Let $i \in I$. Consider if $g, h \in C_{H_{np}}(a)$ are such that $t_i(g), t_i(h) \neq 0$. The previous lemma states that for all $[j] \sim_a [i]$, $t_j(g)$ and $t_j(h)$ are non-zero. Let $\tilde{g} := t(g_{[i]})$ and $\tilde{h} := t(h_{[i]})$. Note that $\tilde{g}, \tilde{h} \in t(C_{H_{np}}(a))$. We then have that $\tilde{g}, \tilde{h}$ are linearly dependent. For assume they were not. Then there exist $d, e \in \mathbb{Z} \setminus \{0\}$ such that the i^{th} coordinate of $d\tilde{g} + e\tilde{h}$ is zero, but for some $[k] \sim_a [i]$ we would have that the k^{th} coordinate of $d\tilde{g} + e\tilde{h}$ is non-zero, contradicting the previous lemma.*

Recall that, for any $i \in I(g)$, $\mathfrak{C}_g([i]) := \{k \mid [k] \sim_g [i]\}$. We may impose an ordering on these sets by saying that $\mathfrak{C}_g([i])$ is less than $\mathfrak{C}_g([j])$ if and only if

$$\min(\mathfrak{C}_g([i])) < \min(\mathfrak{C}_g([j])).$$

Denote this ordering by $\hat{<}$. Let $\mathfrak{C}_g([i^1])$ be the smallest set under $\hat{<}$, and then choose $i^2, \ldots, i^e$ such that

$$\mathfrak{C}_g([i^1]) \hat{<} \mathfrak{C}_g([i^2]) \hat{<} \ldots \hat{<} \mathfrak{C}_g([i^e]) \text{ and } \bigsqcup_{d=1}^{e} \mathfrak{C}_g([i^d]) = I(g). \tag{30}$$

In the following lemma we will show that particular generators of $t(C_{H_{np}}(a))$ are computable. We will denote these by γ_f, with $f \in \mathbb{Z}_e$. Each $\gamma_f \in C_{H_{np}}(a)$ will satisfy

i) $t_{i^f}(\gamma_f) \in \mathbb{N}$;
ii) $t_{i^f}(\gamma_f)$ is minimal i.e. for any $g \in C_{H_{np}}(a)$, $t_{i^f}(\gamma_f)$ divides $|t_{i^f}(g)|$;
iii) for all $k \notin \mathfrak{C}_g([i^f])$, $t_k(\gamma_f) = 0$;
iv) γ_f only consists of infinite cycles i.e. $\gamma_f = (\gamma_f)_\infty$.

Note that, from Remark 6.4, if $g \in C_{H_{np}}(a)$, then $t(g_{[i^f]}) = d \cdot t(\gamma_f)$ for some $d \in \mathbb{Z}$ (since they are linearly dependent and $t_{i^f}(\gamma_f)$ is minimal). We shall now show, for all $f \in \mathbb{Z}_e$ and for all $k \in \mathfrak{C}_g([i^f])$, that the numbers $t_k(\gamma_f)$ are computable, which will mean that $\{t(\gamma_f) \mid f \in \mathbb{Z}_e\}$ is computable.

Lemma 6.5. *Let $a \in H_{np} \rtimes S_{np}$ be given as a word in the standard generating set described in Lemma 3.1 and $i^1, \ldots, i^e$ be chosen as in (30) above. Then there is an algorithm which takes this word and outputs a set of elements $\{\gamma_f \mid f \in \mathbb{Z}_e\}$ satisfying the properties above.*

Proof. Fix an $f \in \mathbb{Z}_e$. We first note, for all $k \in \mathfrak{C}_a([i^f])$, that $|t_k(\gamma_f)| \leqslant |t_k(a_{[i^f]}^{|\sigma_a|})|$. This is because $(a_{[i^f]})^{|\sigma_a|} \in C_{H_{np}}(a)$ by Lemma 4.20 and that $t_{i^f}(\gamma_f)$ must be minimal (condition (ii) above). Thus, for all $k \in \mathfrak{C}_a([i^f])$,

$$|t_k(\gamma_f)| \leqslant |t_k(a_{[i^f]}^{|\sigma_a|})| = |t_k(a^{|\sigma_a|})| = \frac{|\sigma_a|}{|[k]|} \cdot |t_{[k]}(a)| \leqslant |\sigma_a| \cdot |t_{[k]}(a)| \tag{31}$$

where $|\sigma_a| \cdot |t_{[k]}(a)|$ is computable by Lemma 3.7. Secondly, for all $k \in I^c$, we have that $t_k(\gamma_f) = 0$. Thus for all $j \in I^c$ we have that $z_j(\gamma_f)$ is bounded by $z_j(a)$.

We shall now show that, for each $k \in I$, $z_k(\gamma_f) \leqslant z_k(a) + |t_k(\gamma_f)|$. Since we showed above that $|t_k(\gamma_f)|$ is bounded above by $|\sigma_a| \cdot |t_{[k]}(a)|$, we will then have that $z_k(a) + |\sigma_a| \cdot |t_{[k]}(a)|$ is a computable upper bound for $z_k(\gamma_f)$.

Recall that Lemma 3.10 states that if $a, b \in H_{np} \rtimes S_{np}$ are conjugate by some $x \in H_{np}$, then for each class $[i] = \{i_1, \ldots, i_q\}$ there is a formula for $t_{i_s}(x)$ for all $s \in \mathbb{Z}_q$ given by

$$t_{i_s}(x) = t_{i_1}(x) + \sum_{r=1}^{s-1} (t_{i_r}(\omega_b) - t_{i_r}(\omega_a)).$$

Thus, since elements of $C_{H_{np}}(a)$ conjugate a to a, if $g \in C_{H_{np}}(a)$ and $i \in I$, then for all $i', i'' \in [i]$, we have that $t_{i'}(g) = t_{i''}(g)$.

Let $k \in I$. We shall now assume, for a contradiction, that $z_k(\gamma_f)$ is minimal and that $z_k(\gamma_f) > z_k(a) + |t_k(\gamma_f)|$. Since $\gamma_f \in C_{H_{np}}(a)$, we have

$$(i, m)a\gamma_f = (i, m)\gamma_f a \text{ for all } (i, m) \in X_{np}. \tag{32}$$

We may assume that $t_{[k]}(a) > 0$, since replacing a with a^{-1} yields a proof for when $t_{[k]}(a) < 0$. Let $m > z_k(a) + |t_k(\gamma_f)|$. Note that

$$(k,m)a^{-|[k]|}\gamma_f = (k, m - t_{[k]}(a))\gamma_f$$

and also that

$$(k,m)a^{-|[k]|}\gamma_f = (k,m)\gamma_f a^{-|[k]|} = (k, m + t_k(\gamma_f))a^{-|[k]|} = (k, m - t_{[k]}(a) + t_k(\gamma_f)).$$

Thus $(k, m - t_{[k]}(a))\gamma_f = (k, m - t_{[k]}(a) + t_k(\gamma_f))$, which contradicts the minimality of $z_k(\gamma_f)$.

We now show that $t(\gamma_f)$ is computable. From (31) above, $t_{i^f}(\gamma_f) \leqslant |\sigma_a| \cdot |t_{[i^f]}(a)|$. Therefore we must decide whether there is a $g \in C_{H_{np}}(a)$ with

$$t_{i^f}(g) = s \text{ for some } s \in \{1, \ldots, |\sigma_a| \cdot |t_{[k]}(a)| - 1\}.$$

Starting with $s = 1$ (since we want to find a $g \in C_{H_{np}}(a)$ with $t_{i^f}(g)$ minimal) define $\gamma_f^{(s)}$ to be the partial bijection

$$(i^f, m)\gamma_f^{(s)} := (i^f, m + s) \text{ for all } m \geqslant z_k(a) + |\sigma_a| \cdot |t_{[k]}(a)| \tag{33}$$

which defines the action of $\gamma_f^{(s)}$ on almost all points in the ray i^f (using our bound for $z_k(\gamma_f)$). This is so that $\gamma_f^{(s)}$ will satisfy condition (ii) above. We also want $\gamma_f^{(s)}$ to be in the centraliser of a. Hence, for all $(i, m) \in X_{np}$, $\gamma_f^{(s)}$ must satisfy,

$$(i,m)a\gamma_f^{(s)} = (i,m)\gamma_f^{(s)}a \text{ and } (i,m)a^{-1}\gamma_f^{(s)} = (i,m)\gamma_f^{(s)}a^{-1}. \tag{34}$$

Deciding if there exists a $g \in C_{H_{np}}(a)$ with $t_{i^f}(g) = s$ is therefore achieved if one can decide whether there is an element $\gamma_f^{(s)} \in H_{np}$ satisfying (33) and (34).

From (34), if the image of $(i', m')\gamma_f^{(s)}$ is known, we may compute $(i', m')\gamma_f^{(s)}a$ to determine where $\gamma_f^{(s)}$ sends $(i', m')a$. This is because $\gamma_f^{(s)}$ must send $(i', m')a$ to $(i', m')\gamma_f^{(s)}a$. Similarly we may compute $(i', m')\gamma_f^{(s)}a^{-1}$ to determine where $\gamma_f^{(s)}$ sends $(i', m')a^{-1}$. Iterating this process, we obtain how $\gamma_f^{(s)}$ permutes all points $\{(i', m')a^d \mid d \in \mathbb{Z}\}$. Recall that we have bounded $z_k(\gamma_f)$ for all $k \in \mathbb{Z}_{np}$, and so it is enough to define $\gamma_f^{(s)}$ on a finite subset of X_{np} i.e. on all points (i, m) where $m \leqslant z_i(\gamma_f) + t_i(\gamma_f)$. From (33), the image of almost all points $\{(i^f, m) \mid m \in \mathbb{N}\}$ under $\gamma_f^{(s)}$ have been defined. Also, for all $i \in [i^f]$ we have that $t_i(\gamma_f^{(s)}) = t_{i^f}(\gamma_f^{(s)})$, and so the image of almost all points $\{(i, m) \mid i \in [i^f] \text{ and } m \in \mathbb{N}\}$ under $\gamma_f^{(s)}$ has been defined. From Lemma 6.3, we have that $t_k(\gamma_f) \neq 0$ for all k such that $[k] \sim_a [i^f]$. Using (34) we may determine how $\gamma_f^{(s)}$ permutes points on every orbit of $a_{[i^f]}$ with subset almost equal to $X_{[i^f],d_1}$ for each $d_1 \in \mathbb{N}$. Each of these orbits of a will be almost equal to $X_{[i^f],d_1} \sqcup X_{[j],e_1}$ for some $[j] \sim_a [i^f]$ and $e_1 \in \mathbb{N}$. For each j we have therefore defined $t_j(\gamma_f^{(s)})$ and so by using (34) again, we may define $\gamma_f^{(s)}$ on any orbit of $a_{[i^f]}$ with subset almost equal to $X_{[j],d'_1}$ for all $d'_1 \in \mathbb{N}$. Continuing in this way (as we did within the proof of Lemma 6.3) will define $\gamma_f^{(s)}$ for almost all points of every branch j such that $[j] \sim_a [i^f]$. For each choice of s, we may decide if there exist constants $t_k(\gamma_f^{(s)})$ such that for all $k \in \mathbb{Z}_{np}$ and m in

$$\{z_k(a) + |\sigma_a| \cdot |t_{[k]}(a)|, \ldots, z_k(a) + |\sigma_a| \cdot |t_{[k]}(a)| + t_k(\gamma_f^{(s)}) - 1\},$$

$\gamma_f^{(s)}$ satisfies $(k,m)\gamma_f^{(s)} = (k, m + t_k(\gamma_f^{(s)}))$. From the way that $\gamma_f^{(s)}$ has been constructed, we must have that $t_j(\gamma_f^{(s)}) = 0$ for all $[j] \not\sim_a [i^f]$ meaning that $\gamma_f^{(s)}$ will satisfy condition (iii) above. It will also satisfy $t_k(\gamma_f^{(s)}) < |\sigma_a| \cdot |t_{[k]}(a)|$ for all $[k] \sim_a [i^f]$. It is then decidable whether the finite number of equations defining the action of $\gamma_f^{(s)}$ produce a bijection from

$$\{(i,m) \mid i \in \mathbb{Z}_{np} \text{ and } m < z_i(a) + |\sigma_a| \cdot |t_{[i]}(a)|\}$$
$$\text{to } \{(i,m) \mid i \in \mathbb{Z}_{np} \text{ and } m < z_i(a) + |\sigma_a| \cdot |t_{[i]}(a)| + t_i(\gamma_f^{(s)})\}$$

and so it is decidable whether the equations defining $\gamma_f^{(s)}$ produce a bijection on X_{np} i.e. whether $\gamma_f^{(s)} \in \mathrm{Sym}(X_{np})$. If so, $\gamma_f^{(s)} \in H_{np}$ since we have constructed the equations which an element of $\mathrm{Sym}(X_{np})$ satisfies if and only if it is an element in H_{np}. Note that, when the process can be completed, the element $\gamma_f^{(s)} \in C_{H_{np}}(a)$ satisfies $\mathrm{supp}(\gamma_f^{(s)}) = \mathrm{supp}(a_{[i^f]})$, meaning that $\gamma_f^{(s)}$ satisfies condition (iv) above. The smallest s for which this process produces an element in H_{np} will be the element γ_f. Hence the vectors $\{t(\gamma_p) \mid p \in \mathbb{Z}_e\}$ are computable. ☐

Proof of Proposition 6.1. Given $a \in H_{np} \rtimes S_{np}$, we may compute a finite generating set for $t(C_{H_{np}}(a))$ by computing the sets $\{t(\gamma_p) \mid p \in \mathbb{Z}_e\}$ (using the previous lemma) and $t(\bigsqcup_{r\in\mathbb{N}} \Theta_r)$ (which was labelled (28) above).

From Section 6.2, we may use these values to decide if there is a conjugator in $(U_p)\hat{\phi}_{U_p}$ by the solvability of equation (26) and, under certain computable circumstances, equation (27). ☐

References

[ABM13] Y. Antolín, J. Burillo, and A. Martino, *Conjugacy in Houghton's groups*, arXiv:1305.2044 (2013).

[BCMR14] J. Burillo, S. Cleary, A. Martino, and C. E. Röver, *Commensurations and Metric Properties of Houghton's Groups*, arXiv:1403.0026 (2014).

[BMV10] O. Bogopolski, A. Martino, and E. Ventura, *Orbit decidability and the conjugacy problem for some extensions of groups*, Trans. Amer. Math. Soc. **362** (2010), no. 4, 2003–2036. MR 2574885 (2011e:20045)

[Boo59] W.W. Boone, *The word problem*, Annals of mathematics **70**(2) (1959), 207–265.

[Bro87] K. S. Brown, *Finiteness properties of groups*, Proceedings of the Northwestern conference on cohomology of groups (Evanston, Ill., 1985), vol. 44, 1987, pp. 45–75. MR 885095 (88m:20110)

[CM77] D. J. Collins and C. F. Miller, III, *The conjugacy problem and subgroups of finite index*, Proc. London Math. Soc. (3) **34** (1977), no. 3, 535–556. MR 0435227 (55 #8187)

[Cox16] C. Cox, *A note on the R_∞ property for groups* $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$, arXiv:1602.02688 (2016)

[DM96] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR 1409812 (98m:20003)

[GS14] D. Gonçalves and S. Parameswaran, *Sigma theory and twisted conjugacy-II: Houghton groups and pure symmetric automorphism groups*, arXiv:1412.8048 (2014)

[GK75] A. V. Gorjaga and A. S. Kirkinskiĭ, *The decidability of the conjugacy problem cannot be transferred to finite extensions of groups*, Algebra i Logika **14** (1975), no. 4, 393–406. MR 0414718 (54 #2813)

[Hou78] C. H. Houghton, *The first cohomology of a group with permutation module coefficients*, Archiv der Mathematik **31** (1978), 254–258.

[Joh99] D. L. Johnson, *Embedding some recursively presented groups*, Groups St. Andrews 1997 in Bath, II, London Math. Soc. Lecture Note Ser., vol. 261, Cambridge Univ. Press, Cambridge, 1999, pp. 410–416. MR 1676637 (2000h:20057)

[Laz96] F. Lazebnik, *On Systems of Linear Diophantine Equations*, Math. Mag. Vol. 69, 1996, pp. 261–266

[Lee12] S. R. Lee, *Geometry of Houghton's Groups*, arXiv:1212.0257v1 (2012).

[Mil71] C.F. Miller III, *On group-theoretic decision problems and their classification*, Annals of Math. Studies **68**, (1971).

[Nov58] P.S. Novikov *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov. **44** (1955), 143 pages. Translation in *Amer. Math. Soc. Transl.* **9**(2) (1958), 1–122.

[Sco87] W. R. Scott, *Group theory*, second ed., Dover Publications, Inc., New York, 1987. MR 896269 (88d:20001)

[JG15] S. St. John-Green, *Centralizers in Houghton's groups*, Proceedings of the Edinburgh Mathematical Society (Series 2) **58** (2015), 769–785.

[TC36] J. A. Todd and H. S. M. Coxeter, *A practical method for enumerating cosets of a finite abstract group*, Proceedings of the Edinburgh Mathematical Society (Series 2) **5** (1936), 26–34.

[Wie77] J. Wiegold, *Transitive groups with fixed-point-free permutations*, II. Arch. Math. (Basel) 29 (1977), no. 6, 571–573.

Mathematical Sciences, University of Southampton, SO17 1BJ, UK
E-mail address: `charles.cox@soton.ac.uk`
URL: `http://www.southampton.ac.uk/~cc14v07/`

A NOTE ON THE R_∞ PROPERTY FOR GROUPS $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$

CHARLES GARNET COX

Abstract. For any group G, let $\hat{G} \leqslant \mathrm{Sym}(G)$ be obtained by the regular action of G on itself. In this note we show, for any infinite group G (of any cardinality) that $H := \langle \hat{G}, \mathrm{FAlt}(G)\rangle$ has the R_∞ property. Also, if G is finitely generated, then we show that all groups commensurable to H have the R_∞ property. As a corollary, we obtain that any countable group G embeds into a group H such that all groups commensurable to H have the R_∞ property. We also have a result for the Houghton groups, which are a family of groups we denote H_n, where $n \in \mathbb{N}$. We show that, given any $n \in \mathbb{N}$, any group commensurable to H_n has the R_∞ property.

Contents

1. Introduction

The notion of twisted conjugacy and its relationship to fixed point theory has attracted significant attention. For any group G and any $\phi \in \mathrm{Aut}(G)$, we say that two elements $a, b \in G$ are ϕ-twisted conjugate (denoted $a \sim_\phi b$) if there exists an $x \in G$ such that

$$(x^{-1})\phi a x = b. \tag{1}$$

Notice that when $\phi = \mathrm{id}_G$ this becomes the equation for conjugacy. Now, given any $\phi \in \mathrm{Aut}(G)$, define the Reidemeister number of ϕ, denoted $R(\phi)$, to be the number of ϕ-twisted conjugacy classes in G. Thus $R(\mathrm{id}_G)$ records the number of conjugacy classes of G and deciding whether this is infinite has been studied for some time (e.g. [HNN49] where an infinite group with $R(\mathrm{id}_G)$ finite was constructed). We say that G has the R_∞ property if $R(\phi) = \infty$ for every $\phi \in \mathrm{Aut}(G)$.

Date: March, 2016.

2010 *Mathematics Subject Classification.* Primary: 20E45, 20E36.

Key words and phrases. R infinity property, twisted conjugacy, twisted conjugacy classes, highly transitive groups, commensurable groups.

Notation. *For a non-empty set X, let* $\mathrm{Sym}(X)$ *denote the group of all permutations of X. Furthermore, let* $\mathrm{FSym}(X)$ *denote the group of all permutations of X with finite support, and let* $\mathrm{FAlt}(X)$ *denote the group of all even permutations of X with finite support.*

A first example one may consider for the R_∞ property is $\mathbb{Z}$. Although this has infinitely many conjugacy classes, the only non-trivial automorphism has Reidemeister number 2. Similarly, for any $m \in \mathbb{N} := \{1, 2, \ldots\}$, the automorphism ψ of $\mathbb{Z}^m$ which sends a to a^{-1} for all $a \in \mathbb{Z}^m$ has Reidemeister number 2^m. In [JLS14] and [GP14] however, the family of Houghton groups, which (for any $n \in \mathbb{N}$) are denoted H_n, act on $\{1, \ldots, n\} \times \mathbb{N} =: X_n$, and which lie in the short exact sequence

$$1 \longrightarrow \mathrm{FSym}(X_n) \longrightarrow H_n \longrightarrow \mathbb{Z}^{n-1} \longrightarrow 1$$

were shown to have the R_∞ property. In this note we start with a simpler, more general proof of their theorem, and then develop this to a large family of groups.

Definition. A group G *fully contains* FAlt if there is an infinite set X and monomorphism $\Theta : G \mapsto \mathrm{Sym}(X)$ such that $\mathrm{FAlt}(X) \leqslant (G)\Theta$. If $\mathrm{FAlt}(X) \leqslant G \leqslant \mathrm{Sym}(X)$, then we shall say that G fully contains $\mathrm{FAlt}(X)$.

Note that any Houghton group H_n fully contains $\mathrm{FAlt}(X_n)$, but let us justify that this is a large class of groups. For any infinite group G, we have that $G \leqslant \mathrm{Sym}(X)$ for some X (with the possibility that $X = G$ since G can always be embedded into $\mathrm{Sym}(G)$ using a regular representation of G). Then $\langle G, \mathrm{FAlt}(X)\rangle$ fully contains $\mathrm{FAlt}(X)$. A natural question is then whether $\langle G, \mathrm{FAlt}(X)\rangle$ has the R_∞ property. We are able to make some progress with this question. We first answer it positively for the case when G is torsion i.e. we show that $\langle G, \mathrm{FAlt}(X)\rangle$ has the R_∞ property for any torsion group G. We then show a surprisingly general result. For any infinite group G (of arbitrary cardinality) we show that $\langle \hat{G}, \mathrm{FAlt}(G)\rangle$, where $\hat{G} \leqslant \mathrm{Sym}(G)$ is the regular representation of G, has the R_∞ property. Let us now summarise the route which this note takes and the results we obtain.

Note that if G fully contains $\mathrm{FAlt}(X)$, then G is centreless and is not residually finite (since for any infinite set X, $\mathrm{FAlt}(X)$ is not residually finite). Also, given any infinite set X, any group G fully containing $\mathrm{FAlt}(X)$ will have $\mathrm{FAlt}(X)$ as a normal subgroup. Thus, unless $G = \mathrm{FAlt}(X)$, G will not be simple. We first investigate such groups, with an emphasis on describing their automorphism group so to approach twisted conjugacy.

Definition. A group G is monolithic if it has a non-trivial normal subgroup that is contained in every non-trivial normal subgroup of G i.e. if it has a minimal non-trivial normal subgroup.

Let $N_{\mathrm{Sym}(X)}(G)$ denote the normaliser of G in $\mathrm{Sym}(X)$.

Proposition 1. *(Lem. 2.1, Prop. 2.2). Let G fully contain* $\mathrm{FAlt}(X)$. *Then* $\mathrm{FAlt}(X)$ *is characteristic in G,* $\mathrm{Aut}(G) \cong N_{\mathrm{Sym}(X)}(G)$*, and G is monolithic.*

We then work with arguments using cycle type (using that the conjugacy classes of $\mathrm{Sym}(X)$ are well know: each consists of all elements of the same cycle type).

Definition. Let $g \in \mathrm{Sym}(X)$. Then an orbit of g is $\{xg^d \mid d \in \mathbb{Z}\}$ where $x \in X$. Also, g has an infinite orbit if there is a $y \in X$ such that $\{yg^d \mid d \in \mathbb{Z}\}$ is infinite.

Proposition 3.2. *Let G fully contain* $\mathrm{FAlt}(X)$*. If for every $\rho \in N_{\mathrm{Sym}(X)}(G)$, there is an $s \in \mathbb{N}$ such that ρ has finitely many orbits of size s, then G has the R_∞ property.*

From the structure of $\mathrm{Aut}(H_n)$, where H_n denotes the n^{th} Houghton group, Proposition 3.2 immediately yields that, for any $n \geq 2$, H_n has the R_∞ property.

Corollary 3.4. *Let G fully contain* $\mathrm{FAlt}(X)$*. If for every $g \in G$, g does not have an infinite orbit, then G has the R_∞ property.*

Clearly torsion groups satisfy Corollary 3.4.

Corollary 3.5. *Let G be an infinite torsion group which fully contains* FAlt*. Then G has the R_∞ property.*

This means that any torsion group T can be embedded into an infinite torsion group (of any cardinality greater than or equal to $|T|$) which has the R_∞ property. It is in fact easy to construct an uncountable family of such groups.

Corollary 3.7. *There exist uncountably many countable torsion groups which have the R_∞ property.*

Focusing our attention towards actions satisfying (2) provides a stronger result. Note that this condition applies to the regular representation of any group.

(2) For all $g \in G \leqslant \mathrm{Sym}(X)$, if g has an infinite orbit, then all but finitely many points in X lie in an infinite orbit of g.

Theorem 5.2. *Let G satisfy condition (2) and fully contain* $\mathrm{FAlt}(X)$*. Then G has the R_∞ property.*

In the final section we focus on results relating to commensurable groups.

Lemma. *Let G be a finitely generated group. If G and all finite index subgroups of G have the R_∞ property, then all groups commensurable to G have the R_∞ property.*

Condition (2) is preserved under taking subgroups. We therefore obtain.

Corollary 6.5. *Let G satisfy condition (2) and fully contain* $\mathrm{FAlt}(X)$*. Then all groups commensurable to G have the R_∞ property.*

We show that if $G \leqslant \mathrm{Sym}(X)$ satisfies condition (2), then so does $\langle G, \mathrm{FAlt}(X)\rangle$, and so obtain Corollary 5.3 using the following proposition. Note that, from [Fel10, Thm 3.3], a similar result to Corollary 5.3 can be obtained.

Proposition. [HO15, Prop 5.13] *For every finitely generated infinite group Q, there exists a finitely generated group G such that* $\mathrm{FSym}(\mathbb{N}) \lhd G \leqslant \mathrm{Sym}(\mathbb{N})$ *and* $G/\mathrm{FSym}(\mathbb{N}) \cong Q$.

Corollary 5.3. *Let G be any countably infinite group. Then there exists a group H which*

i) contains an isomorphic copy of G;
ii) is finitely generated;
iii) has the R_∞ property, and all groups commensurable to H also have the R_∞ property.

In [GK10], sigma theory is used to prove (for certain groups G) the existence of a finite index subgroup of $\mathrm{Aut}(G)$ which has the R_∞ property. Our final result is that, for the Houghton groups, in fact all commensurable groups have the R_∞ property. We do this by using Proposition 3.2.

Theorem 6.6. *Let $n \in \mathbb{N}$. If G is any group commensurable to H_n, the n^{th} Houghton group, then G has the R_∞ property.*

A few conventions will be used throughout this note:

i) we shall always work with right actions;
ii) unless specified, X will refer to an infinite set;
iii) we shall always consider elements to be written in disjoint cycle notation;
iv) for all of the results in this note, the same proofs can be used if FAlt is replaced with FSym.

Remark. *Let $g \in \mathrm{Sym}(X)$. We shall say 'a cycle of g' to refer, for some $x \in X$, to an orbit $\{xg^d \mid d \in \mathbb{Z}\}$. If there is an $x \in X$ such that this set is infinite, then this is an infinite cycle of g and g contains an infinite cycle. If there is an $x \in X$ such that this set has cardinality r, then this is an r-cycle of g and g contains an r-cycle. If, for some $s \in \mathbb{N}$, there are only finitely many $x \in X$ such that $|\{xg^d \mid d \in \mathbb{Z}\}| = s$, then we shall say that g has finitely many s-cycles. Similarly g may have finitely many infinite cycles.*

Acknowledgements. I thank the authors of [JLS14] and [GP14], whose papers drew my attention to the R_∞ property. I thank my supervisor Armando Martino for his continued guidance and encouragement. Finally I thank Hector Durham, also of the University of Southampton, for the numerous interesting discussions, especially those regarding monolithic groups.

2. Preliminary observations

The groups $\mathrm{FAlt}(X)$, $\mathrm{FSym}(X)$, and $\mathrm{Sym}(X)$ often arise when considering permutation groups (see, for example, [Cam99] and [DM96]). Note that any countable group can be considered as a subgroup of $\mathrm{Sym}(X)$ where X is countable (for example set $X := G$ and use the regular representation of G).

Notation. *Let $G \leqslant \mathrm{Sym}(X)$. For any given $\rho \in N_{\mathrm{Sym}(X)}(G)$, let ϕ_ρ denote the automorphism of G induced by conjugation by ρ i.e. $\phi_\rho(g) := \rho^{-1}g\rho$ for all $g \in G$.*

The three groups $\mathrm{FAlt}(X), \mathrm{FSym}(X), \mathrm{Sym}(X)$ have the property that

$$N_{\mathrm{Sym}(X)}(G) \to \mathrm{Aut}(G), \rho \mapsto \phi_\rho \text{ is an isomorphism.} \tag{3}$$

This means that $\mathrm{Aut}(\mathrm{FAlt}(X)) \cong N_{\mathrm{Sym}(X)}(\mathrm{FAlt}(X)) = \mathrm{Sym}(X) \cong \mathrm{Aut}(\mathrm{FSym}(X))$ and that $\mathrm{FAlt}(X)$ is characteristic in $\mathrm{FSym}(X)$ which is characteristic in $\mathrm{Sym}(X)$. Our first aim is to show that any group G fully containing $\mathrm{FAlt}(X)$ satisfies (3). We do this by showing that $\mathrm{FAlt}(X)$ is characteristic in such a G and then apply the following lemma.

Lemma 2.1. *Let $G \leqslant \mathrm{Sym}(X)$ and $\mathrm{FAlt}(X)$ be a characteristic subgroup of G. Then $N_{\mathrm{Sym}(X)}(G) \cong_\Psi \mathrm{Aut}(G)$ where $\Psi : \rho \mapsto \phi_\rho$.*

Proof. Running the proof of [GP14, Cor. 3.3] using 3-cycles rather than 2-cycles yields the result. □

For any group G satisfying (3), we may use the following reformulation of twisted conjugacy, which has been used extensively by many authors working with the R_∞ property. Recall that ϕ_ρ denotes the automorphism induced by conjugation by $\rho \in \mathrm{Sym}(X)$. Thus,

$$(x^{-1})\phi_\rho a x = b \Rightarrow \rho^{-1}(x^{-1})\rho a x = b \Rightarrow x^{-1}\rho a x = \rho b. \tag{4}$$

We may then show that $R(\phi_\rho) = \infty$ by finding a set of elements $\{a_k \mid k \in \mathbb{N}\}$ such that

$$\rho a_i \sim \rho a_j \Leftrightarrow i = j. \tag{5}$$

This is because, if such a set of elements exist, then each a_k lies in a distinct ϕ_ρ-twisted conjugacy class, and so $R(\phi_\rho) = \infty$. Thus in our case, showing that a set of elements $\{a_k \mid k \in \mathbb{N}\}$ where (5) holds for each $\rho \in N_{\mathrm{Sym}(X)}(G)$ will show that G has the R_∞ property.

Proposition 2.2. *If G fully contains* $\mathrm{FAlt}(X)$*, then* $\mathrm{FAlt}(X)$ *is a characteristic subgroup of G.*

Proof. We first show that $\mathrm{FAlt}(X)$ is a unique minimal normal subgroup of G, known as the monolithic property. Clearly $\mathrm{FAlt}(X)$ is normal in G, since it is normal in $\mathrm{Sym}(X)$ (conjugation in $\mathrm{Sym}(X)$ preserves cycle type).

Consider $N \trianglelefteq G$. We have $N \cap \mathrm{FAlt}(X) \trianglelefteq \mathrm{FAlt}(X)$, and since $\mathrm{FAlt}(X)$ is simple, $N \cap \mathrm{FAlt}(X)$ must either be trivial or $\mathrm{FAlt}(X)$. Consider an element $g \in N$. This must either: be in $\mathrm{FSym}(X)$; contain infinitely many finite cycles; or contain an infinite cycle. We now show that there exists a $\sigma \in \mathrm{FAlt}(X)$ such that $\sigma^{-1}g\sigma g^{-1} \in \mathrm{FAlt}(X) \setminus \{1\}$. Since N is normal, g and $\sigma^{-1}g\sigma$ are in N and so this will prove the claim. For the case where $g \in \mathrm{FSym}(X)$, choose σ so that $\sigma^{-1}g\sigma$ and g have disjoint supports. For the case where g contains infinitely many finite cycles, pick 4 distinct cycles (each of length greater than 1) of g and points b_1, b_2, b_3, b_4: one from each cycle. A suitable σ is then $(b_1\ b_2)(b_3\ b_4)$. Finally, assume that g contains an infinite cycle. Let x be a point within this cycle and define the homomorphism

$$f : \{xg^d \mid d \in \mathbb{Z}\} \to \mathbb{Z},\ xg^k \mapsto k \text{ for all } k \in \mathbb{Z}. \tag{6}$$

Thus the image of f is

$$(\ldots -3\ \ -2\ \ -1\ 0\ 1\ 2\ 3 \ldots) =: a.$$

Let $\mu := (-1\ 0\ 1)$ so that $\mu^{-1}a\mu a^{-1}$ equals $(-2\ \ -1\ 1)$. Thus $(\mu)f^{-1}$ is a suitable candidate for σ in this case.

Now, let $\phi \in \mathrm{Aut}(G)$ and consider $\mathrm{FAlt}(X) \cap (\mathrm{FAlt}(X))\phi$. As above, this must be trivial or $\mathrm{FAlt}(X)$. If it were trivial, this would contradict the uniqueness of $\mathrm{FAlt}(X)$ as a minimal, non-trivial, normal subgroup in G, and hence $\mathrm{FAlt}(X)$ is characteristic in G. □

We may use Lemma 2.1 and Proposition 2.2 to prove that all automorphisms of $\mathrm{Sym}(X)$ are inner. Also, consider if $\mathrm{FSym}(X) \leqslant G \leqslant \mathrm{Sym}(X)$. Then, for all $\rho \in N_{\mathrm{Sym}(X)}(G)$ and all $g \in \mathrm{FSym}(X)$, we have that $(g)\phi_\rho$ has the same cycle type as g. Thus $\mathrm{FSym}(X)$ is characteristic in G.

We are now ready to produce conditions on the cycle type of elements in G and in $N_{\mathrm{Sym}(X)}(G)$ for automorphisms to have infinite Reidemeister number. In order to do this we will use the condition equivalent to showing that $R(\phi_\rho) = \infty$ (labelled (5) above) and well known facts about $\mathrm{Sym}(X)$ regarding cycle type.

3. Results using facts about conjugacy in Sym

Lemma 3.1. *Let G fully contain $\mathrm{FAlt}(X)$. Then $R(\mathrm{id}_G) = \infty$.*

Proof. All that needs to be done is to produce an infinite family of elements which all lie in distinct conjugacy classes. We have the equation $x^{-1}ax = b$. Conjugation by elements of G cannot change the cycle type of elements of $\mathrm{Sym}(X)$. Thus choosing a_k to be a cycle of length $2k+1$ (or any infinite family of elements of $\mathrm{FAlt}(X)$ with distinct cycle types) proves the claim. □

Notation. *For any $g \in \mathrm{Sym}(X)$ and $x \in X$, let $\mathcal{O}_x(g) := \{xg^d : d \in \mathbb{Z}\}$. Also, let $\eta_r(g) := |\{x \in X : |\mathcal{O}_x(g)| = r\}|/_r$, the number of r-cycles in g. We shall use $\eta_1(g)$ to denote the number of fixed points of g and $\eta_\infty(g)$ to denote the number of distinct infinite orbits induced by g. If any of these values is infinite then, since our arguments will be unaffected by the size of this infinity, we shall write $\eta_r(g) = \infty$.*

From the previous section, for any group fully containing $\mathrm{FAlt}(X)$ we have that the map $\Psi : \mathrm{Aut}(G) \to N_{\mathrm{Sym}(X)}(G), \phi_\rho \mapsto \rho$ is an isomorphism. We may therefore consider elements of $\mathrm{Aut}(G)$ as elements of $\mathrm{Sym}(X)$.

Proposition 3.2. *Let G fully contain $\mathrm{FAlt}(X)$ and $\rho \in N_{\mathrm{Sym}(X)}(G)$. If $\eta_r(\rho)$ is finite for some $r \in \mathbb{N}$, then $R(\phi_\rho) = \infty$.*

Proof. We shall work with the reformulation of twisted conjugacy in (5) above and argue for any $\rho \in N_{\mathrm{Sym}(X)}(G)$ using three cases. Let $s \in \mathbb{N}$ be the smallest number such that $\eta_s(\rho)$ is finite.

Case A: $s = 1$ and $\eta_\infty(\rho) > 0$. As in (6) in the proof of Proposition 2.2, let f be a homomorphism from an infinite cycle of ρ to the element of $\mathrm{Sym}(\mathbb{Z})$ which sends z to $z+1$ for all $z \in \mathbb{Z}$. For each $k \in \mathbb{N}$ let

$$\prod_{i=0}^{k-1} (2i \;\; 2i+1) =: a_k{}' \in \mathrm{FSym}(\mathbb{Z}).$$

Now, for each $k \in \mathbb{N}$, let $(a_k')f^{-1} =: a_k \in \mathrm{FSym}(X)$. The set of elements lying in disjoint ϕ_ρ-twisted conjugacy classes is then given by $\{a_{2k} \mid k \in \mathbb{N}\} \subset \mathrm{FAlt}(X)$. This is because $\eta_1(\rho a_k)$ is finite for all $k \in \mathbb{N}$, and is strictly increasing as a function of k. Thus, if $i \neq j$, the elements ρa_i and ρa_j have a different number of fixed points and hence are not conjugate in $G \leqslant \mathrm{Sym}(X)$.

Case B: $s = 1$ and $\eta_\infty(\rho) = 0$. Since ρ has finitely many fixed points and no infinite cycles, ρ contains infinitely many finite cycles. Thus ρ has infinitely many odd length cycles or infinitely many even length cycles. First assume that ρ has infinitely many odd length cycles and index a countably infinite subset of these by the natural numbers. Let $\rho = \rho' \prod_{i \in \mathbb{N}} \rho_i$, where each ρ_i is a finite cycle of odd length and $\rho' \in \mathrm{Sym}(X)$ has cycles with disjoint support from all of the ρ_i's. Now, for any $m \in \mathbb{N}$, $\rho(\rho_m)^{-1}$ has more fixed points than ρ. Defining

$$\prod_{i=1}^{k} \rho_i^{-1} =: a_k \in \mathrm{FAlt}(X)$$

means that $i < j \Rightarrow \eta_1(\rho a_i) < \eta_1(\rho a_j)$ and so $\{a_k \mid k \in \mathbb{N}\}$ provides our infinite family of elements which are pairwise not ϕ_ρ-twisted conjugate. Similarly, if ρ has infinitely many even length cycles, complete the same construction with $\rho =$

$\rho' \prod_{i\in\mathbb{N}} \rho_i$ where each ρ_i is a finite cycle of even length and $\rho' \in \mathrm{Sym}(X)$ has cycles with disjoint support from all of the ρ_i's.

Case C: $s > 1$. All we shall use is that ρ has infinitely many fixed points. For any $k \in \mathbb{N}$, let a_k consist of $2k$ s-cycles such that $\mathrm{supp}(a_k) \subset X \setminus \mathrm{supp}(\rho)$. We then have, for all $k \in \mathbb{N}$: that $a_k \in \mathrm{FAlt}(X)$; that $\eta_s(\rho a_k)$ is finite; and that $\eta_s(\rho a_k)$ is strictly increasing as a function of k. □

Proposition 3.3. *Let* $a, b \in \mathrm{Sym}(X)$, $\mathrm{supp}(b) \subsetneq \mathrm{supp}(a)$, *and* $x \in \mathrm{Sym}(X)$ *satisfy* $x^{-1}ax = b$. *Then* $\eta_\infty(x) > 0$.

Proof. We assume, for a contradiction, that $\eta_\infty(x) = 0$. Since $x^{-1}ax = b$, x must restrict to a bijection from $\mathrm{supp}(a)$ to $\mathrm{supp}(b)$ i.e.

$$(\mathrm{supp}(a) \cup \mathrm{supp}(b)) \setminus (\mathrm{supp}(a) \cap \mathrm{supp}(b)) \subseteq \mathrm{supp}(x)$$

which from our hypotheses is equivalent to

$$\mathrm{supp}(a) \setminus \mathrm{supp}(b) \subseteq \mathrm{supp}(x).$$

Thus x sends some $n \in \mathrm{supp}(a) \setminus \mathrm{supp}(b)$ to some $m \in \mathrm{supp}(b)$. Now, since all of the cycles in x are finite, there is a $k \in \mathbb{N}$ such that $(m)x^k$ is in $\mathrm{supp}(b)$ but $(m)x^{k+1}$ is in $X \setminus \mathrm{supp}(b)$ i.e. x sends a point in $\mathrm{supp}(b)$ to a point in $X \setminus \mathrm{supp}(b)$. Hence $x^{-1}ax$ and b have different supports, a contradiction. □

Corollary 3.4. *Let G be a group fully containing* $\mathrm{FAlt}(X)$. *If* $\eta_\infty(g) = 0$ *for all* $g \in G$, *then G has the R_∞ property.*

Proof. By Proposition 3.2, if $\phi_\rho \in \mathrm{Aut}(G)$ has $\eta_s(\rho) < \infty$ for any $s \in \mathbb{N}$, then $R(\phi_\rho) = \infty$. We may therefore assume that $\eta_r(\rho) = \infty$ for all $r \in \mathbb{N}$. This means that $X \setminus \mathrm{supp}(\rho)$ is an infinite set.

Our aim is to show that there is an infinite set of elements in G which are not ϕ_ρ-twisted conjugate. Let $b_0 := 1$, the identity element of G. For each $k \in \mathbb{N}$, let $b_k := b'_k b_{k-1}$ where $\eta_2(b'_k) = 2$, $|\mathrm{supp}(b'_k)| = 4$, $\mathrm{supp}(b'_k) \subset X \setminus \mathrm{supp}(\rho)$, and $\mathrm{supp}(b'_k) \cap \mathrm{supp}(b_{k-1}) = \emptyset$. Thus, for each $k \in \mathbb{N}$, $b_k \in \mathrm{FAlt}(X)$ and $\eta_2(b_k) = 2k$. For $i < j$ we have that $\mathrm{supp}(\rho b_i) \subsetneq \mathrm{supp}(\rho b_j)$. Since $\eta_\infty(g) = 0$ for all $g \in G$, Proposition 3.3 implies that $\rho b_i \not\sim \rho b_j$ i.e. $R(\phi_\rho) = \infty$. □

Notice that this provides an alternative proof to [JLS14] and [GP14] that $\mathrm{FSym}(X)$ has the R_∞ property. We also have the following.

Corollary 3.5. *Let G be an infinite torsion group which fully contains* FAlt. *Then G has the R_∞ property.*

Corollary 3.6. *Let G be a torsion group. For every $\alpha \geq |G|$, there exists a torsion group H_α of cardinality α which has the R_∞ property and contains an isomorphic copy of G.*

Of course, there are also groups which are not torsion and have no infinite cycles. This is because an element $\rho \in \mathrm{Sym}(X)$ with $\eta_r(\rho)$ non-zero for infinitely many $r \in \mathbb{N}$ will have infinite order but need not contain an infinite cycle.

Corollary 3.7. *There exist uncountably many countable torsion groups which have the R_∞ property.*

Proof. We will work within $\mathrm{Sym}(\mathbb{N}\times\mathbb{N})$. For each $n \geq 2$, define

$$\phi^{(n)} : C_n \hookrightarrow \mathrm{Sym}(\mathbb{N}\times\mathbb{N}), (1\ \dots\ n) \mapsto \rho$$

where $\mathrm{supp}(\rho) = \{(m,n) \mid m \in \mathbb{N}\}$ and

$$(m,n)\rho := \begin{cases} (m-n+1,n) & \text{if } m \equiv 0 \bmod n \\ (m+1,n) & \text{otherwise} \end{cases}$$

i.e. ρ consists of n-cycles 'all the way down' the n^{th} copy of $\mathbb{N}$.

Let $\mathbb{P}$ denote the set of all prime numbers. Then, for any subset $S \subseteq \mathbb{P}$, let $G_S := \bigoplus_{p\in S} C_p$. Note that there are uncountably many choices for S. Also,

$$\bigoplus_{p\in S} C_p \hookrightarrow \mathrm{Sym}(\mathbb{N}\times\mathbb{N})$$

by using the maps $\phi^{(n)}$ defined above. For any $S \subseteq \mathbb{P}$, let $\tilde{G}_S := \langle G_S, \mathrm{FAlt}(\mathbb{N}\times\mathbb{N})\rangle$. Note that $\tilde{G}_S$ is torsion and fully contains FAlt and so, by Corollary 3.5, $\tilde{G}_S$ has the R_∞ property. Our final aim is therefore to show that if $S \neq S'$, then $\tilde{G}_S$ and $\tilde{G}_{S'}$ are not isomorphic. By Proposition 2.2, $\tilde{G}_S$ and $\tilde{G}_{S'}$ each have $\mathrm{FAlt}(\mathbb{N}\times\mathbb{N})$ as a unique minimal normal subgroup. Since G_S and $G_{S'}$ contain no non-trivial elements of finite support,

$$\tilde{G}_S \big/ \mathrm{FAlt}(\mathbb{N}\times\mathbb{N}) \cong G_S \text{ and } \tilde{G}_{S'} \big/ \mathrm{FAlt}(\mathbb{N}\times\mathbb{N}) \cong G_{S'}.$$

Hence if $\tilde{G}_S$ and $\tilde{G}_{S'}$ are isomorphic, then G_S and $G_{S'}$ are isomorphic. But since $S \neq S'$, there is a $p \in \mathbb{P}$ in one set that is not in the other. Without loss of generality let $p \in S \setminus S'$. By construction, G_S has p-torsion but $G_{S'}$ does not. Hence $\tilde{G}_S \ncong \tilde{G}_{S'}$. ☐

4. Results regarding centralisers in Sym

Before working with actions satisfying condition (2) (on page 91) we require some well known results about centralisers. This is because of the following lemma. Throughout this section we shall say that g conjugates a to b if $g^{-1}ag = b$.

Lemma 4.1. *Let $a, b, g, g' \in G$ and g conjugate a to b. Now, g' conjugates a to b if, and only if, $g' = cg$ for some $c \in C_G(a)$.*

We start with a simple observation. It applies to centralisers since $C_G(a)$ consist of all elements of G which conjugate a to a.

Lemma 4.2. *Let $a, b \in \mathrm{Sym}(X)$ be conjugate in $\mathrm{Sym}(X)$ and let $x \in X$. If $g \in \mathrm{Sym}(X)$ conjugates a to b and $g : x \mapsto x'$, then $g : xa^k \mapsto x'b^k$ for all $k \in \mathbb{Z}$.*

Proof. Let $g : x \mapsto x'$ and $g^{-1}ag = b$. For all $k \in \mathbb{Z}$,

$$(x')(g^{-1}ag)^k = (x')g^{-1}a^kg = (xa^k)g.$$

But $g^{-1}ag = b$, and so $(xa^k)g$ must be equal to $(x')b^k$. ☐

We must first describe centralisers in $\mathrm{Sym}(X)$. Throughout we shall work with a fixed $\rho \in \mathrm{Sym}(X)$.

Notation. *Let $\alpha_{r,i}(\rho)$ denote the i^{th} r-cycle of ρ, and for every valid r and i let $\alpha_{r,i}(\rho) := (\alpha_{r,i}^{(1)}\ \alpha_{r,i}^{(2)} \dots \alpha_{r,i}^{(r)})$ where $\alpha_{r,i}^{(k)} \in \mathrm{supp}(\alpha_{r,i}(\rho))$ for all $1 \leqslant k \leqslant r$. Note that 1-cycles denote fixed points. Also, for each $r \in \mathbb{N}$, let $I_\rho(r)$ be the indexing set for the r-cycles of ρ. Similarly let $z_i(\rho) := (\dots z_i^{(-1)}\ z_i^{(0)}\ z_i^{(1)}\ z_i^{(2)} \dots)$ denote the i^{th} infinite cycle of ρ where, for all $k \in \mathbb{Z}$, $z_i^{(k)} \in \mathrm{supp}(z_i(\rho))$. Finally, let I_ρ denote the indexing set for the infinite cycles of ρ.*

Lemma 4.3. *Let $g \in \mathrm{Sym}(X)$ consist of a single r-cycle i.e. be defined so that $\alpha_{r,1}(g) = (a_1 \dots a_r)$, and $\alpha_{r,k+1}(g), \alpha_{s,k}(g)$, and $z_k(g)$ are not defined for any $k \geq 1$. Then $C_{\mathrm{Sym}(X)}(g) = \mathrm{Sym}(X \setminus \{a_1, \dots, a_r\}) \times \langle g \rangle$.*

Sketch proof. We note that, for any $x \in \mathrm{Sym}(X)$,

$$x^{-1}gx = x^{-1}(a_1 \dots a_r)x = ((a_1)x\ (a_2)x \dots (a_r)x). \tag{7}$$

Thus all elements of $\mathrm{Sym}(X)$ with disjoint support from g lie in $C_{\mathrm{Sym}(X)}(g)$. Furthermore, if $x : a_1 \mapsto a_{1+k}$, then, by the previous lemma, this uniquely determines where x sends $a_2, \dots, a_r$. Using the proof of Lemma 4.2 we see that, mod r, $x : a_i \mapsto a_{i+k}$ for all $i \in \{1, \dots, r\}$. □

If $g = \prod_{i \in I} g_i$ where the g_i are disjoint cycles, then $x^{-1}gx = \prod_{i\in I} x^{-1}g_i x$ and we may apply (7) to see that conjugation by any $x \in \mathrm{Sym}(X)$ again changes the support exactly by the action of x. This allows us to generalise the previous lemma.

Lemma 4.4. *Let $\rho \in \mathrm{Sym}(X)$. Then $C_{\mathrm{Sym}(X)}(\rho)$ is generated by elements*

i) of the form $\prod_{\substack{r\in\mathbb{N}\\ i\in I_\rho(r)}} \alpha_{r,i}(\rho)^{d_{r,i}} \prod_{j \in I_\rho} z_j(\rho)^{e_j}$ for some constants $d_{r,i}, e_j \in \mathbb{Z}$;

ii) which permute the cycles of the same length within ρ, i.e. are elements of $\mathrm{Sym}(X)$ containing cycles of the form

(a) $\prod_{j=1}^{r} (\alpha_{r,i_1}^{(j)}\ \alpha_{r,i_2}^{(j)} \dots \alpha_{r,i_k}^{(j)})$ for some distinct $\{i_1, \dots, i_k\} \subseteq I_\rho(r)$;

(b) $\prod_{j\in\mathbb{Z}} (z_{i_1}^{(j)}\ z_{i_2}^{(j)} \dots z_{i_k}^{(j)})$ for some distinct $\{i_1, \dots, i_k\} \subseteq I_\rho$;

(c) $\prod_{j=1}^{r} (\dots \alpha_{r,i_{-1}}^{(j)}\ \alpha_{r,i_0}^{(j)}\ \alpha_{r,i_1}^{(j)} \dots)$ for some distinct $\{i_m \mid m \in \mathbb{Z}\} \subseteq I_\rho(r)$;

(d) $\prod_{j\in\mathbb{Z}} (\dots z_{i_{-1}}^{(j)}\ z_{i_0}^{(j)}\ z_{i_1}^{(j)} \dots)$ for some distinct $\{i_m \mid m \in \mathbb{Z}\} \subseteq I_\rho$.

Thus, $C_{\mathrm{Sym}(X)}(\rho)$ is an unrestricted wreath product with base consisting of all elements of type (i) and head consisting of all elements of type (ii).

Proof. The only reference the author is aware of is [anon], but the result follows from the ideas of the previous lemma. □

Notation. *Let $g \in \mathrm{Sym}(X)$. Given any set $Y \subseteq X$ for which $Yg = Y$ (so that g restricts to a bijection on Y), let $g\big|Y$ denote the element of $\mathrm{Sym}(Y)$ which acts as g on the set Y i.e. for every $y \in Y$, $y(g\big|Y) := yg$.*

The following lemma is included for interest, and will not be used in this note.

Lemma 4.5. *Let $g \in \mathrm{Sym}(X)$. Then $C_{\mathrm{Sym}(X)}(g)$ is either uncountable or virtually free abelian of finite rank.*

Proof. Since X is infinite, g must either have

i) $\eta_\infty(g)$ non-zero;
ii) $\eta_r(g)$ infinite for at least one $r \in \mathbb{N}$;
iii) $\eta_r(g)$ non-zero for infinitely many $r \in \mathbb{N}$.

If either (ii) or (iii) occurs, then from the previous lemma we have that $C_{\mathrm{Sym}(X)}(g)$ is uncountable. In case (i), if $\eta_\infty(g)$ is infinite, again $C_{\mathrm{Sym}(X)}(g)$ is uncountable. If $\eta_\infty(g) = n$ and cases (ii) and (iii) do not apply, then the centraliser contains a wreath product with base including $\mathbb{Z}^n$ (corresponding to the n infinite cycles of g) and head corresponding to a copy of S_n permuting these n infinite cycles. Denote this virtually $\mathbb{Z}^n$ group by G. Since (ii) and (iii) do not occur, there are only finitely many points outside of the support of the infinite cycles of g. Denote these points by Y. Now let $g' := g\big|Y$. Thus $C_{\mathrm{Sym}(Y)}(g')$ is finite and so $C_{\mathrm{Sym}(X)}(g) \cong G \times C_{\mathrm{Sym}(Y)}(g')$, a virtually $\mathbb{Z}^n$ group. □

Notation. *Let $g \in \mathrm{Sym}(X)$. Then, for a fixed $r \in \mathbb{N}$, let $g\big|_r$ denote the element of* $\mathrm{Sym}(X)$ *which consists of the product of all of the r-cycles of g, so that $\eta_r(g(g\big|_r)^{-1}) = 0$, and for all $s \neq r$, $\mathrm{supp}(g\big|_r) \cap \mathrm{supp}(g\big|_s) = \emptyset$. Similarly let $g\big|_\infty$ denote the element of* $\mathrm{Sym}(X)$ *which consists of the product of all of the infinite cycles of g.*

The last results of this section will be needed in the next section, where we will work with groups satisfying the following condition.

(8) Let $G \leqslant \mathrm{Sym}(X)$. For all $g \in G$, if $\eta_\infty(g) > 0$, then $X \setminus \mathrm{supp}(g\big|_\infty)$ is finite.

Lemma 4.6. *Let $G \leqslant \mathrm{Sym}(X)$, $g \in G$, and $\sigma \in \mathrm{FSym}(X)$. Also, fix some $s \in \mathbb{N}$.*
i) if $\eta_\infty(g) > 0$ and $\eta_r(g) = 0$ for all $r \in \mathbb{N}$, then $\sum_{r\in\mathbb{N}} \eta_r(g\sigma)$ is finite.
ii) if $\eta_s(g) = \infty$ and $\eta_r(g) = 0$ for all $r \in \mathbb{N} \setminus \{s\}$, then $\eta_s(g\sigma) = \infty$, $\sum_{r\in\mathbb{N}\setminus\{s\}} \eta_r(g\sigma)$ is finite, and $\eta_\infty(g\sigma) = 0$.

Thus, if G satisfies condition (8), then $\langle G, \mathrm{FSym}(X)\rangle$ also satisfies condition (8).

Proof. We first deal with case (ii). Let

$$F := \bigsqcup_{1\leqslant k\leqslant s} \mathrm{supp}(g^{-k}\sigma g^k).$$

Outside of F, the element $g\sigma$ consists of s-cycles. Notice that F is finite (it has size at most $s \times |\mathrm{supp}(\sigma)|$). Hence $\eta_s(g\sigma) = \infty$, $\sum_{r\in\mathbb{N}\setminus\{s\}} \eta_r(g\sigma)$ is finite, and $\eta_\infty(g\sigma) = 0$, as claimed.

We now deal with case (i). For any $k \in I_g$, recall that $z_k(g)$ is the k^{th} infinite cycle of g, and that $z_k(g) = (\dots z_k^{(-1)}\ z_k^{(0)}\ z_k^{(1)}\ z_k^{(2)} \dots)$.

Record those $i \in I_g$ such that $\mathrm{supp}(z_i(g)) \cap \mathrm{supp}(\sigma) \neq \emptyset$. Since σ has finite support, there will be only finitely many such i. Label these $i_1, \dots, i_d$. Note that

$$mg = mg\sigma \text{ for all } m \in X \setminus \left(\bigsqcup_{j=1}^{d} \mathrm{supp}(z_{i_j}(g))\right).$$

Now, for each $j \in \{1, \dots, d\}$, record numbers $\min(i_j)$ and $\max(i_j)$ such that:

i) $z_{i_j}^{(\min(i_j))}, z_{i_j}^{(\max(i_j))} \in \mathrm{supp}(\sigma)$;
ii) for all $d < \min(i_j)$, $z_{i_j}^{(d)} \notin \mathrm{supp}(\sigma)$; and
iii) for all $d > \max(i_j)$, $z_{i_j}^{(d)} \notin \mathrm{supp}(\sigma)$.

Finally, define

$$F := \bigsqcup_{j=1}^{d} \{m \in \mathrm{supp}(z_{i_j}(g)) \mid \min(i_j) - 1 \leqslant m \leqslant \max(i_j)\}.$$

Now, for all $m \in X \setminus F$, $mg = mg\sigma$. Hence, for all $m \in X \setminus F$, we must have that $m \in \mathrm{supp}((g\sigma)\big|_\infty)$ i.e. that m lies within an infinite cycle of $g\sigma$. Thus, all of the finite cycles of $g\sigma$ lie within F, a finite set. This proves the claim. □

Lemma 4.7. *Let $\rho \in \mathrm{Sym}(X)$. If $g \in C_{\mathrm{Sym}(X)}(\rho)$ is an element which, apart from on a finite set consists of infinite cycles, then $\rho g((\rho g)\big|_\infty)^{-1} \in \mathrm{FSym}(X)$.*

Proof. We note that, by definition, $\rho \in C_{\mathrm{Sym}(X)}(g)$. Hence, ρ restricts to a bijection of the r-cycles of g (for all $r \in \mathbb{N}$) and the infinite cycles of g. For each $r \geq 2$, let $Y_r := \mathrm{supp}(g\big|_r)$. Also, let $Y_1 := X \setminus \mathrm{supp}(g)$ and $Y_\infty := \mathrm{supp}(g\big|_\infty)$. From our hypotheses, we have that the set $\bigsqcup_{r\in\mathbb{N}} Y_r$ is finite. Hence, so is

$$\sum_{r\in\mathbb{N}} \sum_{s\in\mathbb{N}} \eta_s\big((\rho g)\big|Y_r\big).$$

Let $g\big|Y_\infty = \prod_{i\in I} g_i$ where $|I| = \eta_\infty(g)$ and the g_i are the disjoint infinite cycles of g. Lemma 4.4 describes the structure for the cycles that $\rho\big|Y_\infty$ contains. We consider each possibility (i), (ii)(b), and (ii)(d) from Lemma 4.4.

Denote the product of all cycles of $\rho\big|Y_\infty$ of type (i) by $h^{(1)}$. Any $h \in C_{\mathrm{Sym}(X)}(g)$ which (when written in disjoint cycle notation) contains g_j^{-1} for some $j \in I$, satisfies $\eta_1(hg) = \infty$. Similarly, if $h = \prod_{j\in J} g_j^{d_j}$ where $J \subseteq I$ and $d_j \in \mathbb{Z}\setminus\{-1\}$, then clearly hg consists only of infinite cycles. Next, denote the product of all cycles of $\rho\big|Y_\infty$ of type (ii)(b) by $h^{(2)}$. Then $h^{(2)}\big|_s$ consists of those cycles of $\rho\big|Y_\infty$ of type (ii)(b) of length $s \in \mathbb{N}$, and $h^{(2)}\big|_s \in C_{\mathrm{Sym}(X)}(g)$. Hence, for any $m \in \mathrm{supp}(h^{(2)}\big|_s)$,

$$\{(m)(h^{(2)}\big|_s g)^d \mid d \in \mathbb{Z}\} = \{(m)g^d(h^{(2)}\big|_s)^d \mid d \in \mathbb{Z}\} \supseteq \{(m)g^{es} \mid e \in \mathbb{Z}\}$$

and so m lies in an infinite orbit of $g(h\big|_s)$. Finally, denote the product of all cycles of $\rho\big|Y_\infty$ of type (ii)(d) by $h^{(3)}$. Let us assume that there is a $d \in \mathbb{Z}$ and $m \in \mathrm{supp}(h^{(3)})$ such that $(m)(h^{(3)}g)^d = (m)$. Now, $h^{(3)} \in C_{\mathrm{Sym}(X)}(G)$, and so $(m)(h^{(3)}g)^d = (m)(h^{(3)})^d g^d$. Thus $(h^{(3)})^d : m \mapsto m'$ and $g^d : m' \mapsto m$. But then there are infinite cycles of g and $h^{(3)}$ whose intersection contains at least 2 points, which contradicts that $h^{(3)}$ is of type (ii)(d). Hence $\sum_{r\geq 2} \eta_r((\rho g)\big|Y_\infty)$ is finite. Together with our observations of the possible cycles of ρg within each set Y_r, we have that $\sum_{r\geq 2} \eta_r(\rho g)$ is finite i.e. $\rho g((\rho g)\big|_\infty)^{-1} \in \mathrm{FSym}(X)$. □

We end this section by describing more specifically how any element which conjugates ρb_i and ρb_j (as defined in Corollary 3.4) may act.

Proposition 4.8. *Let:*

i) G fully contain $\mathrm{FAlt}(X)$ *and satisfy condition (8);*
ii) $\rho \in N_{\mathrm{Sym}(X)}(G)$ satisfy $\eta_r(\rho) = \infty$ for all $r \in \mathbb{N}$;
iii) $\{b_k \mid k \in \mathbb{N}\}$ be the elements defined in the proof of Corollary 3.4;
iv) and $g \in G$ conjugate ρb_i to ρb_j for some $j < i$.

Then $\eta_\infty(\rho g) > 0$ and $\sum_{r\geq 2} \eta(\rho g) < \infty$.

Proof. Let $l_{ij} := \mathrm{supp}(b_i) \setminus \mathrm{supp}(b_j)$. If x conjugates ρb_i to ρb_j, then $\eta_\infty(x) \geq |l_{ij}|$. This is because each point of l_{ij} must lie on an infinite cycle of x (from the proof of Corollary 3.4) and no two of these points may lie within the support of the same infinite cycle of x (since x must send these points to within $\mathrm{supp}(\rho b_j)$ in order to conjugate ρb_i to ρb_j). Furthermore, for each infinite cycle $(\ldots a_{-2}\ a_{-1}\ a_0\ a_1 \ldots)$ of x which intersects l_{ij}, there must exist a $d \in \mathbb{Z}$ such that

i) $a_d \in l_{ij}$;
ii) for all $k > d, a_k \in \mathrm{supp}(\rho b_j)$;
iii) and for all $k' < d, a_{k'} \in X \setminus \mathrm{supp}(\rho b_i)$.

Let $g \in G$ conjugate ρb_i to ρb_j, and let y consist of all infinite cycles of g which have non-trivial intersection with l_{ij}. Since y^{-1} conjugates ρb_j to ρb_i, Lemma 4.1 states that $gy^{-1} \in C_{\mathrm{Sym}(X)}(\rho b_i)$. Lemma 4.7 states that $\sum_{r\geq 2} \eta_r(\rho g y^{-1})$ is finite.

We end by making some observations about how y may act. Recall that y consists of $|l_{ij}|$ infinite cycles. Let

$$y_1 := (\ldots m_1^{(-2)}\ m_1^{(-1)}\ m_1^{(0)}\ m_1^{(1)}\ m_1^{(2)} \ldots)$$

be one such infinite cycle of y. Thus $\mathrm{supp}(y_1) = \{m_1^{(k)} \mid k \in \mathbb{Z}\}$ and, for all $k \in \mathbb{Z}$, $(m_1^{(k)})y_1 = m_1^{(k+1)}$. For simplicity let $m_1^{(0)} \in l_{ij}$. Lemma 4.2 can be used to determine where y sends $(\mathrm{supp}(y_1))\rho b_i$. Recall that y conjugates ρb_i to ρb_j, and so for all $k \in \mathbb{Z}$,

$$(m_1^{(k)})(y^{-1}\rho b_i y) = (m_1^{(k)})\rho b_j.$$

Simplifying the left hand side of this expression we see that $(m_1^{(k-1)}\rho b_i)y = (m_1^{(k)}\rho b_j)$. Thus y contains an infinite cycle y_2 such that

$$\{m_1^{(k-1)}\rho b_i \mid k \in \mathbb{N}\} \subset \mathrm{supp}(y_2)$$

and for all $k \geq 1$, $(m_1^{(k-1)}\rho b_i)y = (m_1^{(k)}\rho b_i)$. Let

$$y_2 := (\ldots m_2^{(-2)}\ m_2^{(-1)}\ m_2^{(0)}\ m_2^{(1)}\ m_2^{(2)} \ldots)$$

where, for all $k \geq 0$, $m_2^{(k)} := m_1^{(k)}\rho b_i$. Importantly $m_2^{(0)} = m_1^{(0)}\rho b_i \in l_{ij}$. Thus, from the structure of the infinite cycles of x which intersect l_{ij} non-trivially, we have for all $d \in \mathbb{N}$ that $m_2^{(-d)} \in X \setminus \mathrm{supp}(\rho b_i)$. Note that $y_1 \neq y_2$. One way to see this is that

$$\mathrm{supp}(y_1) \cap l_{ij} = \{m_1^{(0)}\} \text{ and } \mathrm{supp}(y_2) \cap l_{ij} = \{m_1^{(0)}\rho b_i\} = \{m_1^{(0)} b_i\} \neq \{m_1^{(0)}\}$$

meaning that $\mathrm{supp}(y_1) \neq \mathrm{supp}(y_2)$.

We may now compute that the orbit of $m_1^{(0)}$ under ρy is equal to the set

$$\{m_1^{(2k)} \mid k \in \mathbb{Z}\} \cup \{m_2^{(2k+1)} \mid k \in \mathbb{Z}\}$$

where, for all $k \in \mathbb{Z}$, $(m_1^{(2k)})\rho y = m_2^{(2k+1)}$ and $(m_2^{(2k-1)})\rho y = m_1^{(2k)}$. Similarly, the orbit of $m_1^{(1)}$ under ρy is equal to the set

$$\{m_1^{(2k+1)} \mid k \in \mathbb{Z}\} \cup \{m_2^{(2k)} \mid k \in \mathbb{Z}\}$$

where, for all $k \in \mathbb{Z}$, $(m_1^{(2k-1)})\rho y = m_2^{(2k)}$ and $(m_2^{(2k)})\rho y = m_1^{(2k+1)}$. Hence ρy contains infinite cycles $\hat{y}_1$ and $\hat{y}_2$ such that $\mathrm{supp}(\hat{y}_1) \cup \mathrm{supp}(\hat{y}_2) = \mathrm{supp}(y_1) \cup \mathrm{supp}(y_2)$. Thus, given a point $m \in \mathrm{supp}(y) \setminus \mathrm{supp}(\rho b_i)$, we have $(m)\rho y = (m)y$ and so m lies on an infinite cycle of ρy. Given a point $n \in \mathrm{supp}(\rho b_i) \cap \mathrm{supp}(y)$ we have that $n \in \mathrm{supp}(y_k)$ for some infinite cycle of y and that there exists an infinite cycle of

ρy containing n. Hence all points of $\mathrm{supp}(y)$ lie in an infinite cycle of $\rho y_{k'}$ (where $y_{k'}$ is some infinite cycle of y) and so $\eta_r(\rho y \mid \mathrm{supp}(y)) = 0$ for all $r \in \mathbb{N}$. Together with the discussions above of how gy^{-1} must act we obtain the result. □

5. Results for actions satisfying condition (2)

In this section we will consider groups satisfying condition (9) below, which was labelled (2) on page 91 and (8) on page 98.

(9) Let $G \leqslant \mathrm{Sym}(X)$. For all $g \in G$, if $\eta_\infty(g) > 0$, then $X \setminus \mathrm{supp}(g\big|_\infty)$ is finite.

The following is well known.

Lemma 5.1. *Let G be any group. Then, for any $\psi \in \mathrm{Aut}(G)$ and $\phi \in \mathrm{Inn}(G)$, we have that $R(\psi) = R(\psi\phi)$.*

We may now prove the main result of this note.

Theorem 5.2. *Let G fully contain* $\mathrm{FAlt}(X)$ *and satisfy condition (9). Then G has the R_∞ property.*

Proof. Much of the work is in Proposition 4.8. Let $\rho \in N_{\mathrm{Sym}(X)}(G)$. From Proposition 3.2, if $\eta_s(\tau)$ is finite for some $s \in \mathbb{N}$, then $R(\phi_\tau) = \infty$. We may therefore assume that $\eta_r(\rho)$ is infinite for all $r \in \mathbb{N}$. As stated within the proof of Corollary 3.4, there exist an infinite family of elements $\{b_k \mid k \in \mathbb{N}\}$ whose support is contained within the fixed points of our chosen ρ i.e. for all $k \in \mathbb{N}$, $\mathrm{supp}(b_k) \subseteq X \setminus \mathrm{supp}(\rho)$. Let $i, j \in \mathbb{N}$ be such that $\mathrm{supp}(\rho b_j) \subsetneq \mathrm{supp}(\rho b_i)$ and ρb_i, ρb_j are conjugate in G. Note that if no pair is conjugate, then $R(\phi_\rho) = \infty$ since $\{\rho b_k \mid k \in \mathbb{N}\}$ is an infinite family of non-conjugate elements. Thus there exists a $g \in G$ which conjugates ρb_i to ρb_j. In Proposition 4.8 it was shown that $\sum_{r \geq 2} \eta_r(\rho g)$ is finite. Thus $\eta_2(\rho g)$ is finite and Proposition 3.2 states that $R(\phi_{\rho g}) = \infty$. By Lemma 5.1, $R(\phi_\rho) = R(\phi_{\rho g}) = \infty$. □

We obtain the following corollary. This result can also be obtained using [Fel10, Thm. 3.3].

Corollary 5.3. *Let G be any countably infinite group. Then there exists a group H which*

i) contains an isomorphic copy of G;
ii) is finitely generated;
iii) has the R_∞ property, and all groups commensurable to H also have the R_∞ property.

Proof. Embed G into a finitely generated group F. Let $\hat{F} \leqslant \mathrm{Sym}(F)$ denote the regular representation of F. Thus $\hat{F}$ satisfies condition (9). From [HO15, Prop 5.13], $\langle \hat{F}, \mathrm{FSym}(F)\rangle =: H$ is finitely generated. By Lemma 4.6, H satisfies condition (9). By Theorem 5.2, H has the R_∞ property. Corollary 6.5 of the next section then states that all groups commensurable to H have the R_∞ property. □

6. The R_∞ property and commensurable groups

This final section involves results for commensurable groups.

Notation. *Let $N \trianglelefteq_f G$ denote that N is normal and finite index in G.*

Definition 6.1. Let G and H be groups. We say that G is commensurable to H if and only if there exist $N_G \cong N_H$ with $N_G \trianglelefteq_f G$ and $N_H \trianglelefteq_f H$.

We will work towards two results. The first deals with the R_∞ property for groups commensurable to those appearing in Theorem 5.2 (which are those which fully contain FAlt and satisfy condition (9) on page 101). The second result applies to the Houghton groups, a family of groups H_n indexed over $\mathbb{N}$ where, for each $n \in \mathbb{N}$, H_n acts on a set X_n and $\mathrm{FSym}(X_n) \leqslant H_n \leqslant \mathrm{Sym}(X_n)$. Each group H_n therefore fully contains $\mathrm{FAlt}(X_n)$. These were first introduced in [Hou78], but we rely heavily on [Cox14] where an introduction to these groups can be found and a description, for all $n \geq 2$, of the structure of the automorphism group for all finite index subgroups of H_n is given. We start with two well known results.

Lemma 6.2. *If $H \leqslant_f G$ and G is finitely generated, then $\exists\ K \leqslant_f G$ which is characteristic in G.*

Lemma 6.3. [MS14, Lem 2.2(ii)] *Let D be a group with the R_∞ property and*

$$1 \longrightarrow D \longrightarrow E \longrightarrow F \longrightarrow 1$$

be a short exact sequence of groups. If D is characteristic in E and F is any finite group, then E has the R_∞ property.

Combining the previous two results provides an easier condition to check in order to show that all commensurable groups have the R_∞ property.

Lemma 6.4. *Let G be a finitely generated group. If G and all finite index subgroups of G have the R_∞ property, then all groups commensurable to G have the R_∞ property.*

Proof. Let H be commensurable to G. Then $\exists\ N \trianglelefteq_f G, H$. By Lemma 6.2, there exists a group U which is characteristic in H and such that $U \leqslant_f G, H$. From our assumption that all finite index subgroups of G have the R_∞ property, U has the R_∞ property. Hence, by Lemma 6.3, H has the R_∞ property. □

From this lemma we need only investigate finite index subgroups. This leads to our first aim for this section.

Corollary 6.5. *Let G be finitely generated, fully contain* $\mathrm{FAlt}(X)$, *and satisfy condition (9). Then all groups commensurable to G have the R_∞ property.*

Proof. Note that condition (9) is preserved by subgroups. Let $F \leqslant_f G$. It is well known that if $A \leqslant C$ and $B \leqslant_f C$ then $B \cap A \leqslant_f A$. Hence $F \cap \mathrm{FAlt}(X) \leqslant_f \mathrm{FAlt}(X)$. Moreover there is a finite index subgroup of $F \cap \mathrm{FAlt}(X)$ which is normal in $\mathrm{FAlt}(X)$. But since $\mathrm{FAlt}(X)$ is both infinite and simple, $\mathrm{FAlt}(X) \leqslant F$. Thus F satisfies condition (9) and fully contains $\mathrm{FAlt}(X)$. Theorem 5.2 therefore states that F has the R_∞ property, and so Lemma 6.4 yields the result. □

Our final aim is the following.

Theorem 6.6. *Let $n \in \mathbb{N}$. If G is any group commensurable to H_n, the n^{th} Houghton group, then G has the R_∞ property.*

Proof. We first work with FAlt. If G is commensurable to $\mathrm{FAlt}(X)$, then there exists $N \trianglelefteq_f \mathrm{FAlt}(X), G$. Now, since $\mathrm{FAlt}(X)$ is simple and infinite, $N = \mathrm{FAlt}(X)$. Hence we have the short exact sequence

$$1 \longrightarrow \mathrm{FAlt}(X) \longrightarrow G \longrightarrow F \longrightarrow 1$$

where F is some finite group. Let $\phi \in \mathrm{Aut}(G)$ and consider $\mathrm{FAlt}(X) \cap (\mathrm{FAlt}(X))\phi$. This has finite index in $\mathrm{FAlt}(X)$. Since $\mathrm{FAlt}(X)$ is simple, we have $(\mathrm{FAlt}(X))\phi = \mathrm{FAlt}(X)$ i.e. that $\mathrm{FAlt}(X)$ is characteristic in G. Lemma 6.3 states that G has the R_∞ property.

We now work with $n \geq 2$. From Lemma 6.4, it is sufficient to show that, for any $n \geq 2$, all finite index subgroups of H_n have the R_∞ property.

Fix an $n \geq 2$. There are a family of finite index, characteristic subgroups of H_n defined in [BCMR14] and denoted U_p where $p \in \mathbb{N}$. In [Cox14, Prop. 5.8] it was shown that, for any $U \leqslant_f H_n$, there exists an $m \in \mathbb{N}$ such that

$$\mathrm{Aut}(U) \;_\Psi\!\cong N_{\mathrm{Sym}(X_n)}(U) \leqslant N_{\mathrm{Sym}(X_n)}(U_m) \cong_\Psi \mathrm{Aut}(U_m)$$

where $\Psi : N_{\mathrm{Sym}(X_n)}(G) \mapsto \mathrm{Aut}(G)$ is defined by $(g)\Psi = \phi_g$. Furthermore, there is an isomorphism $\mu : N_{\mathrm{Sym}(X_n)}(U_m) \to S \leqslant N_{\mathrm{Sym}(H_{nm})}(H_{nm})$ where, for all $k \geq 2$, $N_{\mathrm{Sym}(X_k)}(H_k) = H_k \rtimes S_k$. Importantly, this isomorphism preserves cycle type. We shall apply Proposition 3.2 to show that any group with automorphism group contained within $N_{\mathrm{Sym}(H_k)}(H_k)$ for some $k \geq 2$ has the R_∞ property.

Fix a $k \geq 2$. Notice that for all $r \in \mathbb{N} \setminus \{1\}$ and for all $g \in H_k$, $\eta_r(g)$ is finite. Given a $\rho \in H_k \rtimes S_k$, which is isomorphic to $\mathrm{Aut}(H_k)$ via the map $\rho \mapsto \phi_\rho$, we have that $\eta_r(\rho)$ is infinite if and only if ρ induces a cyclic permutation of r branches of X_k. Thus, for all $\rho \in N_{\mathrm{Sym}(X_k)}(H_k)$ and all $r > k$ we have that $\eta_r(\rho)$ is finite. Now, for any $U \leqslant_f H_n$, there exists an $m \in \mathbb{N}$ such that $N_{\mathrm{Sym}(X_n)}(U) \leqslant N_{\mathrm{Sym}(X_n)}(U_m)$. Consider if $\rho \in N_{\mathrm{Sym}(X_n)}(U_m)$. Using the above homomorphism $\mu : N_{\mathrm{Sym}(X_n)}(U_m) \to N_{\mathrm{Sym}(X_{nm})}(H_{nm})$, we have that $\eta_r((\rho)\mu)$ is finite for all $r > nm$. Since μ preserves cycle type, $\eta_r(\rho)$ is also finite for all $r > nm$. Hence, by Proposition 3.2, $R(\phi_\rho) = \infty$ and so all automorphisms of U have infinite Reidemeister number. Thus all finite index subgroups of H_n have the R_∞ property and so Lemma 6.4 yields the result. □

References

[anon] anon (http://math.stackexchange.com/users/11763/anon), *Centralizer of a given element in S_n?*, Mathematics Stack Exchange, URL:http://math.stackexchange.com/q/208821 (version: 2013-09-10).

[BCMR14] J. Burillo, S. Cleary, A. Martino, and C. E. Röver, *Commensurations and Metric Properties of Houghton's Groups*, arXiv:1403.0026 (2014).

[Cam99] Peter J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999. MR 1721031 (2001c:20008)

[Cox14] C. Cox, *Twisted Conjugacy in Houghton's groups*, arXiv:1410.7051 (2014).

[DM96] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR 1409812 (98m:20003)

[Fel10] Alexander Fel'shtyn, *New directions in Nielsen-Reidemeister theory*, Topology Appl. 157 (2010), no. 10-11, 1724–1735.

[GK10] Daciberg Gonçalves and Dessislava Hristova Kochloukova, *Sigma theory and twisted conjugacy classes*, Pacific J. Math. **247** (2010), no. 2, 335–352. MR 2734152 (2011m:20099)

[GP14] D. Gonçalves and S. Parameswaran, *Sigma theory and twisted conjugacy-II: Houghton groups and pure symmetric automorphism groups*, arXiv:1412.8048 (2014).

[Hou78] C. H. Houghton, *The first cohomology of a group with permutation module coefficients*, Archiv der Mathematik **31** (1978), 254–258.

[HNN49] Graham Higman, B. H. Neumann, and Hanna Neumann, *Embedding theorems for groups*, J. London Math. Soc. **24** (1949), 247–254. MR 0032641 (11,322d)

[HO15] M. Hull and D. Osin, *Transitivity degrees of countable groups and acylindrical hyperbolicity*, arXiv:1501.04182 (2015).

[JLS14] J. H. Jo, J. B. Lee, and R. L. Sang, *The R_∞ property for Houghton's groups*, arXiv:1412.8767 (2014).

[MS14] T. Mubeena and P. Sankaran, *Twisted conjugacy classes in abelian extensions of certain linear groups*, Canad. Math. Bull. **57** (2014), no. 1, 132–140. MR 3150726

Mathematical Sciences, University of Southampton, SO17 1BJ, UK
E-mail address: `charles.cox@soton.ac.uk`
URL: `http://www.southampton.ac.uk/~cc14v07/`

THE DEGREE OF COMMUTATIVITY AND LAMPLIGHTER GROUPS

CHARLES GARNET COX

Abstract. The degree of commutativity of a group G measures the probability of choosing two elements in G which commute. There are many results studying this for finite groups. In [AMV], this was generalised to infinite groups. In this note, we compute the degree of commutativity for wreath products of the form $\mathbb{Z} \wr \mathbb{Z}$ and $F \wr \mathbb{Z}$ where F is any finite group.

1. Introduction

Let F be a finite group. Then the degree of commutativity of F, denoted $\mathrm{dc}(F)$, is the probability of choosing two elements in F which commute i.e.

$$\mathrm{dc}(F) := \frac{|\{(a,b) \in F^2 : ab = ba\}|}{|F|^2}.$$

This definition was generalised to infinite groups in [AMV] in the following way. Let G be a finitely generated group and S a finite generating set for G. Let $|g|_S$ denote the length of g with respect to the generating set S i.e. the infimum of all word lengths of words in S which represent g. For any $n \in \mathbb{N}$, let the ball of radius n in the Cayley graph of G with respect to the generating set S be denoted by $\mathbb{B}_S(n)$. Thus $\mathbb{B}_S(n) = \{g \in G : |g|_S \leqslant n\}$. Then the degree of commutativity of G with respect to S, as defined in [AMV], is

$$\limsup_{n\to\infty} \frac{|\{(a,b) \in \mathbb{B}_S(n)^2 : ab = ba\}|}{|\mathbb{B}_S(n)|^2} \tag{1}$$

and is denote by $\mathrm{dc}_S(G)$. They also pose an intriguing conjecture.

Conjecture. [AMV, Conj. 1.6] *Let G be a finitely generated group, and let S be a finite generating set for G. Then: (i) $\mathrm{dc}_S(G) > 0$ if and only if G is virtually abelian; and (ii) $\mathrm{dc}_S(G) > 5/8$ if and only if G is abelian.*

They verify this conjecture for hyperbolic groups and groups of polynomial growth (see [Gri91] for an introduction to the growth of groups). In this note we will investigate the conjecture for groups which are wreath products.

Perhaps the best known examples of infinite wreath products are the lamplighter groups $C \wr \mathbb{Z}$ where C is cyclic. Such groups are sensible to investigate with respect to the conjecture since they have exponential growth and yet all elements in the base of $C \wr \mathbb{Z}$ commute. We obtain the following.

Date: June 17, 2016.

2010 *Mathematics Subject Classification.* 20P05.

Key words and phrases. Wreath products, lamplighter group, degree of commutativity, exponential growth.

Theorem 1. *Let $G = C \wr \mathbb{Z}$ where C is a non-trivial cyclic group. Then there is a generating set S of G such that* $\mathrm{dc}_S(G) = 0$.

This work generalises to allow us to replace 'cyclic' with 'finite'.

Theorem 2. *Let $G := F \wr \mathbb{Z}$ where F is a non-trivial finite group. Then there is a generating set S of G such that* $\mathrm{dc}_S(G) = 0$.

Note that the groups of Theorem 2 include the first known examples of non-residually finite groups with degree of commutativity 0, since it is currently open as to whether there exists a non-residually finite hyperbolic group.

Remark. *In the case where G is finite, it is well known that*

$$\mathrm{dc}(G) = \frac{\#\ \textit{conjugacy classes of}\ G}{|G|}.$$

One could therefore define the degree of commutativity for any finitely generated infinite group with respect to a finite generating set S to be

$$\limsup_{n\to\infty} \frac{\#\ \textit{conjugacy classes intersecting}\ \mathbb{B}_S(n)}{|\mathbb{B}_S(n)|}.$$

Such a limit may not be a real limit. Note that this definition includes the conjugacy growth function of G, which was introduced in [Bab88] *and studied, for example, in* [GS10] *and* [HO13].

Two questions then present themselves.

Question 1. *With this definition for degree of commutativity, does the conjecture above (from* [AMV]*) hold?*

Question 2. *Does this definition for the degree of commutativity coincide with (1) above?*

The author is unaware of such questions having been posed before, and these questions are not discussed further in this note.

Acknowledgements. This work would not have been completed without the guidance of my PhD supervisor, Armando Martino. I also thank the other authors of [AMV] for a paper filled with so many ideas.

We now introduce wreath products from an algebraic viewpoint, but will provide intuition (using permutations) below.

Definition. Given groups G and H, the *unrestricted wreath product* of G and H has elements consisting of an element $h \in H$ and a function $f : H \to G$. Let B' be the set of all such functions. If $f_1, f_2 \in B'$, then $(f_1 \times f_2)(h) := f_1(h) \cdot f_2(h)$ for all $h \in H$, where $\cdot$ denotes the binary operation of G. Moreover if $k \in H$ then $k^{-1}(f(h))k := f(hk^{-1})$ for all $h \in H$. This is equal to the semidirect product $B' \rtimes H$. The *restricted wreath product*, denoted $G \wr H$, is defined analogously as the semidirect product $B \rtimes H$ where H is the *head* of $G \wr H$ and B, the *base* of $G \wr H$, is the subgroup of B' consisting of functions with finite support i.e. functions $f \in B'$ such that $f(h) \neq 1$ for only finitely many h. Since the base is a direct sum of $|H|$ copies of G, for any $h \in H$ let G_h denote the copy of G corresponding to h.

It may be useful to provide some of the intuition used when thinking about lamplighter groups i.e. groups of the form $C \wr \mathbb{Z}$ where C is cyclic. Each of these groups acts naturally on the corresponding set $C \times \mathbb{Z}$. We shall picture C as addition modulo n if $|C| = n$ and as $\mathbb{Z}$ otherwise. Hence $C = \{0, 1, \ldots, n-1\}$ or $C = \mathbb{Z}$. A well used generating set is $\{a_0, t\}$ where $\mathrm{supp}(a_0) = \{(0,0), (1,0), \ldots, (n-1, 0)\}$ and $\mathrm{supp}(t) = C \times \mathbb{Z}$ with $t : (m, n) \to (m, n+1)$ for all $m \in C$ and $n \in \mathbb{Z}$. In the case where $|C| = 2$, the base of $C \wr \mathbb{Z}$ can be thought of as a countable collection of street lamps, with each lamp having an 'off' or 'on' setting. If $2 < |C| < \infty$, then we can consider each 'lamp' to have a finite number of settings (possibly corresponding to different levels of brightness). In the case of $\mathbb{Z} \wr \mathbb{Z}$, the base can be thought of as lamps, where each lamp has an associated 'voltage' which takes a value in $\mathbb{Z}$. Although this intuition will not be taken any further, it can also be seen to apply to subgroups of $\mathbb{R} \wr \mathbb{R}$.

2. Proving Theorem 1

The key result we shall draw upon is the following. For the group $G = H \wr \mathbb{Z}$ we shall use the base of $H \wr \mathbb{Z}$ as the set N.

Lemma 2.1. [AMV, Lem. 3.1] *Let G be a finitely generated group, and let S be a finite generating system for G. Suppose that there exists a subset $N \subseteq G$ satisfying the following conditions:*

i) N is S-negligible, i.e. $\lim_{n\to\infty} \frac{|N \cap \mathbb{B}_S(n)|}{|\mathbb{B}_S(n)|} = 0$;

ii) $\lim_{n\to\infty} \frac{|C_G(g) \cap \mathbb{B}_S(n)|}{|\mathbb{B}_S(n)|} = 0$ *uniformly in $g \in G \setminus N$.*

Then, $\mathrm{dc}_S(G) = 0$.

Remark. *Throughout we will restrict ourselves to generating sets which are the union of a generator of $\mathbb{Z}$ and a generating set for G_i for some fixed $i \in \mathbb{Z}$.*

2.1. **Proving that groups $C \wr \mathbb{Z}$ satisfy (ii) of Lemma 2.1.** This is the simpler of the two conditions to prove for such groups. We first introduce the translation lengths of a group. For more discussions on these, see [Con97] and the references therein.

Definition 2.2. Let G be a finitely generated group with finite generating set S and let $g \in G$. Then $\tau_S(g) := \limsup_{n\to\infty} \frac{|g^n|_S}{n}$, the *translation length* of g. Let $F(G)$ denote the set of non-torsion elements in G. If there is a finite generating set S' of G such that $\{\tau_{S'}(g) : g \in F(G)\}$ is uniformly bounded away from 0, then we say that G is *translation discrete.* If a group is translation discrete with respect to one finite generating set, it is translation discrete with respect to all generating sets (see [Con98, Lem. 2.6.1])

We shall use the following.

Lemma 2.3. *Let G be finitely generated, S a finite generating set for G, and $|\mathbb{B}_S(n)| \geqslant f(n)$ for all $n \in \mathbb{N}$, where f is a polynomial of degree 2. Let $N \subseteq G$. If (i) $C_G(g)$ is cyclic for all $g \in G \setminus N$; and (ii) the translation lengths of G are uniformly bounded away from 0, then* $\lim_{n\to\infty} \frac{|C_G(g) \cap \mathbb{B}_S(n)|}{|\mathbb{B}_S(n)|} = 0$ *uniformly in $g \in G \setminus N$.*

Proof. This argument can be found within the proof of [AMV, Thm. 1.7]. From (ii), there exists a constant $\lambda \in \mathbb{R}$ such that $\tau_S(g) \geqslant 1/\lambda$ for all $g \in G$.

Let $h \in G \setminus N$. By (i), $C_G(h) = \langle g \rangle$ for some $g \in G$. We now consider how $C_G(h) \cap \mathbb{B}_S(n)$ grows with respect to n. If $g^k \in C_G(h) \cap \mathbb{B}_S(n)$, then $|g^k|_S \leqslant n$ and $|g^k|_S \geqslant |k|\tau_S(g) \geqslant |k|/\lambda$. Thus $|k| \leqslant \lambda n$ and

$$|C_G(h) \cap \mathbb{B}_S(n)| \leqslant 2\lambda n + 1.$$

Hence, since $\mathbb{B}_S(n)$ grows faster than any linear function, the claim follows. □

We must therefore show the two conditions in this lemma are satisfied. Note that they are independent of the choice of finite generating set used.

Definition 2.4. Let A denote the base of $G = H \wr \mathbb{Z}$ where H is a finitely generated group. If $g \in A$, then $g = \prod_{i \in I} g_i$ where I is a finite subset of $\mathbb{Z}$ and $g_i \in H_i$ for each $i \in I$. Now $g_{\min} := \inf\{I\}$ and $g_{\max} := \sup\{I\}$, the infimum and supremum of I, respectively.

Lemma 2.5. *Let $G := H \wr \mathbb{Z}$ and let A denote the base of G. If $g \in A$, then $C_G(g) \leqslant A$ (and if H is abelian, then $C_G(g) = A$). If $g \in G \setminus A$, then $C_G(g)$ is cyclic.*

Proof. The first claim is clear. For the second, let $g \in G \setminus A$, so that $g = wt^k$ for some $w \in A$ and $k \in \mathbb{Z} \setminus \{0\}$. Now, for any $v \in A$,

$$\begin{aligned} v^{-1}wt^k v &= wt^k \\ \Leftrightarrow v^{-1}wt^k vt^{-k} &= w \\ \Leftrightarrow t^k vt^{-k} &= w^{-1}vw \end{aligned} \tag{2}$$

and so, if v is non-trivial, then $(w^{-1}vw)_{\min} > (t^k vt^{-k})_{\min}$ and so $v \notin C_G(wt^k)$. Now assume that $vt^\alpha \in C_G(wt^k)$. If $v't^\alpha \in C_G(wt^k)$, then $v't^\alpha(vt^\alpha)^{-1} = v'v^{-1}$ and so by (2), $v'v^{-1} = 1$ i.e. $v' = v$. Thus for each $s \in \mathbb{Z}$ such that $vt^s \in C_G(wt^k)$ there is no $v' \neq v$ such that $v't^s \in C_G(wt^k)$. Now assume that α is the smallest positive integer such that there exists a $v \in A$ with $vt^\alpha \in C_G(wt^k)$. If, for some $\beta \in \mathbb{Z}$ there is a $u \in A$ such that $ut^\beta \in C_G(wt^k)$, then, by the division algorithm, $\beta = n\alpha$ for some $n \in \mathbb{Z}$. Thus $ut^\beta = (vt^\alpha)^n$ since for each $s \in \mathbb{Z}$ there is at most one $\nu \in A$ such that $\nu t^s \in C_G(wt^k)$. □

Lemma 2.6. *Let $G = H \wr \mathbb{Z}$ where H is a finitely generated group and let A denote the base of G. Then $\{\tau_S(g) : g \in G \setminus A\}$ is uniformly bounded away from 0 i.e. G is translation discrete.*

Proof. Let S_H denote a finite generating set for H_0. We work with the generating set $S := S_H \cup \{t\}$ of G.

If $g \in G \setminus A$, then $g = wt^k$ where $w \in A$ and $t \in \mathbb{Z} \setminus \{0\}$. Thus for any $n \in \mathbb{N}$, $|g^n|_S \geqslant |k|n \geqslant n$ and so $\tau_S(g) \geqslant 1$. □

Let H be finitely generated with $\tau_S(H) \subseteq \mathbb{N} \cup \{0\}$ for some finite generating set S. Then one can prove, with S' as a finite generating set consisting of the generating set S for H_0 and a generator of the head of $H \wr \mathbb{Z}$, that $\tau_{S'}(H \wr \mathbb{Z}) = \mathbb{N} \cup \{0\}$ and that $\tau_{S'}^{-1}(0)$ is equal to $\{w \in \bigoplus_{i \in I} H_i \mid I \text{ is a finite subset of } \mathbb{Z} \text{ and } w \text{ is torsion}\}$. Moreover, if we drop the condition on the translation lengths of H and let A denote the base of $H \wr \mathbb{Z}$, then $\tau_{S'}(H \wr \mathbb{Z} \setminus A) = \mathbb{N}$.

2.2. **Proving that groups $C \wr \mathbb{Z}$ satisfy (i) of Lemma 2.1.** The author is unaware of how to show that the negligibility of a set is independent of the generating set used. When working with groups of exponential growth, it seems that the 'density' of a set $A \subset G$ may depend on the choice of generating set. Here, density of a subset A of $G = \langle S \rangle$ is thought of as the number

$$\limsup_{n\to\infty} \frac{|A \cap \mathbb{B}_S(n)|}{|\mathbb{B}_S(n)|}$$

(so that a set is negligible if and only if it has density 0). Note that if the negligibility of a set is independent of the finite generating set used, then the results that follow would apply to any finite generating set.

Remark. *We shall work with the generating set $\langle a_0, t\rangle$ where a_0 is a generator of C_0 and t is a generator of $\mathbb{Z}$. The arguments also work for C_i for any $i \in \mathbb{Z}$.*

Essentially we reduce counting the number of elements in the base in $\mathbb{B}_S(n)$ to known results regarding the number of possible compositions of a number.

Definition 2.7. A multiset, denoted $[\ldots]$, is a collection of objects where repeats are allowed e.g. $[1, 2, 2, 3, 5]$. An ordered multiset, denoted $[\ldots]_{\mathrm{ord}}$, is a multiset with a given ordering. Thus $[1, 2, 2, 3, 5]_{\mathrm{ord}} \neq [1, 2, 3, 2, 5]_{\mathrm{ord}}$.

Definition 2.8. Let $n \in \mathbb{N}$. Then a composition of n is an ordered collection of natural numbers that sum to n. Thus there is a natural correspondence between compositions of n and ordered multisets whose elements lie in $\mathbb{N}$ and sum to n. A weak composition of n is a collection of non-negative integers that sum to n. There is a natural correspondence between weak compositions of n and ordered multisets whose elements lie in $\mathbb{N} \cup \{0\}$ and sum to n.

The following are well known.

Lemma 2.9. *Let $n \in \mathbb{N}$. Then the number of compositions of n is 2^{n-1}.*

Proof. We consider a multiset with elements in $\mathbb{N}$, which sum to n, and where each box either represents a plus or a comma.

$$[1\Box 1\Box 1 \ldots 1\Box 1]_{\mathrm{ord}}$$

Now, for each box a choice of a comma or a plus provides a unique ordered multiset consisting of elements in $\mathbb{N}$. ☐

Lemma 2.10. *Let $n \in \mathbb{N}$. Then the number of weak compositions of n into exactly k parts is give by the binomial coefficient*

$$\binom{n+k-1}{k-1}.$$

Proof. From the previous proof the number of compositions of n into exactly k parts is given by the number of ways of placing exactly $k-1$ commas into $n-1$ boxes i.e.

$$\binom{n-1}{k-1}.$$

Now, each composition of $n+k$ into k parts can be thought of as a weak composition of n into k parts by mapping k element multisets which sum to $n+k$ and consist of natural numbers to k element multisets which sum to n and consist of non-negative integers i.e. the map $[m_1, m_2, \ldots, m_k]_{\mathrm{ord}} \mapsto [m_1 - 1, m_2 - 1 \ldots, m_k - 1]_{\mathrm{ord}}$. ☐

We are now ready to prove our first theorem.

Theorem 1. *Let $G = C \wr \mathbb{Z}$ where C is a non-trivial cyclic group. Let $S := \langle a, t\rangle$ be a generating set for G with $a \in C_i$ (for some $i \in \mathbb{Z}$) and $t \in \mathbb{Z}$, the head of G. Then $\mathrm{dc}_S(G) = 0$.*

Proof. From Lemma 2.1 and our work above, all that remains to be done is to show that the base A of G is negligible in G.

Fix an $n \in \mathbb{N}$. Our aim is to produce a bound for $|\mathbb{B}_S(n) \cap A|$. For discussions on normal forms for elements of $C \wr \mathbb{Z}$, see [CT05]. Let $k \leqslant n/2$. If $|g| = n$ and $g_{\min} \geqslant 0$, then there is a word of length n of the form below which represents g

$$w^{(0)}t^{-1}w^{(1)}t^{-1}\dots w^{(k-1)}t^{-1}w^{(k)}tw^{(k+1)}t\dots w^{(2k)} \tag{3}$$

where, for each $i \in \{0, 1, \dots, 2l\}$, $w^{(i)} = a^{d_i}$ for some $d_i \in \mathbb{Z}$. Now, any word $g \in |\mathbb{B}_S(n) \cap A|$ with $g_{\min} \geqslant 0$ can be expressed in the form (3) and must satisfy

$$\sum_{i=0}^{2k} |w^{(i)}|_{\{a\}} \leqslant n - 2k.$$

We now justify why it is sufficient to look at only those $g \in A$ with $g_{\min} \geqslant 0$. Let $A_s := \{g \in A : g_{\min} \geqslant s\}$. By conjugating a word of the form (3) by t^{-s}, we have, for any $s \in \mathbb{Z} \setminus \mathbb{N}$, that

$$|\mathbb{B}_S(n) \cap (A_s \setminus A_{s+1})| \leqslant |\mathbb{B}_S(n) \cap A_0|.$$

Also, for any $s \leqslant -n$, $|\mathbb{B}_S(n) \cap (A_s \setminus A_{s+1})| = 0$. Thus

$$\begin{aligned} |\mathbb{B}_S(n) \cap A| &\leqslant \left(\bigcup_{-n \leqslant s \leqslant -1} |\mathbb{B}_S(n) \cap (A_s \setminus A_{s+1})| \right) \cup |\mathbb{B}_S(n) \cap A_0| \\ &\leqslant (n+1)|\mathbb{B}_S(n) \cap A_0|. \end{aligned}$$

Since groups of the form $C \wr \mathbb{Z}$ (where C is a non-trivial cyclic group) are of exponential growth, producing a bound for $|\mathbb{B}_S(n) \cap A_0|$ will be sufficient to bound $|\mathbb{B}_S(n) \cap A_0|$.

In (3), the words $\{w^{(j)} : j = k+1, k+2, \dots, 2k\}$ are redundant since

$$\begin{aligned} &w^{(0)}t^{-1}w^{(1)}t^{-1}\dots w^{(k-1)}t^{-1}w^{(k)}tw^{(k+1)}t\dots w^{(2k)} \\ =&w^{(0)}w^{(2k)}t^{-1}w^{(1)}w^{(2k-1)}t^{-1}\dots w^{(k-1)}w^{(k+1)}t^{-1}w^{(k)}t^k. \end{aligned}$$

Thus any word $g \in |\mathbb{B}_S(n) \cap A|$ with $g_{\min} \geqslant 0$ can be expressed in the form

$$w^{(0)}t^{-1}w^{(1)}t^{-1}\dots w^{(k-1)}t^{-1}w^{(k)}t^k \tag{4}$$

where, for each $i \in \{0, 1, \dots, k\}$, $w^{(i)} = a^{d_i}$ for some $d_i \in \mathbb{Z}$.

From [BT15], the growth of $C \wr \mathbb{Z}$ with our generating set is greater than 2^n if $|C| \geqslant 3$ and is $\frac{1+\sqrt{5}}{2}$ if $|C| = 2$.

We first work with $|C| = 2$. In this case each $w^{(i)}$ has length 0 or 1. Thus, for each k, there are at most 2^{k+1} choices for the values of $\{w^{(i)} : i = 0, 1, \dots, k\}$. Hence the size of $|\mathbb{B}_S(n) \cap A_0|$ is bounded by

$$\sum_{j=0}^{\lfloor n/2 \rfloor} 2^{j+1} \leqslant 4 \cdot (\sqrt{2})^n \leqslant 4 \cdot \left(\frac{1+\sqrt{5}}{2} \right)^n$$

and so the base of $C_2 \wr \mathbb{Z}$ is negligible.

For the case where $|C| > 2$, we shall use Lemma 2.10. Our aim is to show that $|(\mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)) \cap A_0|$ is bounded by a function which has growth rate 2^n (since this will mean that $|\mathbb{B}_S(n) \cap A_0|$ is also bounded by a function which has growth rate 2^n). Fix an $k \in \{0, 1, \dots, \lfloor \frac{n}{2} \rfloor\}$. We note that all such elements can be represented by a word of the form (4), where $|w^{(i)}| < n - 2k$ for all $i \in \{0, \dots, k\}$. Each word is in bijection with a multiset

$$[u^{(0)}, v^{(0)}, u^{(1)}, v^{(1)}, \dots, u^{(k-1)}, v^{(k-1)}, u^{(k)}, v^{(k)}]_{\mathrm{ord}} \tag{5}$$

where for each $i \in \{0, \dots, k\}$ we have that $u^{(i)}, v^{(i)} \in \mathbb{N} \cup \{0\}$ and that $u^{(i)} v^{(i)} = 0$. This is therefore bounded by the number of weak compositions of $n - 2k$ into $2k + 2$ parts. From Lemma 2.10 this is equal to

$$\binom{n - 2k + 2k + 2 - 1}{2k + 2 - 1} = \binom{n+1}{2k+1}.$$

Now we sum over all viable k:

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n+1}{2k+1} \leqslant \sum_{j=0}^{n+1} \binom{n+1}{j} = 2^n.$$

Hence $|(\mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)) \cap A| \leqslant (n+1)|(\mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)) \cap A_0| \leqslant (n+1) \cdot 2^n$, and so is negligible in $C \wr \mathbb{Z}$. □

Note that from this proof it immediately follows that $(C_2 \times C_2) \wr \mathbb{Z}$, with the generating set consisting of two generators of $(C_2 \times C_2)_0$ and a generator of the head, has degree of commutativity 0.

Theorem 2. *Let $G := F \wr \mathbb{Z}$ where F is a non-trivial finite group. Then there is a generating set S of G such that* $\mathrm{dc}_S(G) = 0$.

Proof. Let $|F| = m > 1$ and let A denote the base of G. Then $A := \bigoplus_{i \in \mathbb{Z}} F_i$ where $F_i = F$ for each $i \in \mathbb{Z}$. Let S denote the generating set consisting of the non-trivial elements of F_0 and a generator t of the head of G. From Section 2.1 we need only show that the base of G is negligible in G.

First we produce a lower bound on the growth of G. Consider words of the form

$$w_1 t w_2 t w_3 \dots t w_k t^{\epsilon}$$

where, for each i, $w_i \in S$ and $\epsilon \in \{0, 1\}$. There are m^k such words (since $|S| = m$) and so $|\mathbb{B}_S(n)| \geqslant |\mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1)| \geqslant m^{\lceil n/2 \rceil}$.

We now produce an upper bound on the growth of A, the base of G. As with the previous proof, we produce an upper bound for words $g \in A \cap (\mathbb{B}_S(n) \setminus \mathbb{B}_S(n-1))$ with $g_{\min} \geqslant 0$. Such words are of the form

$$w_0 t^{-1} w_1 t^{-1} w_2 t^{-1} \dots w_{k-1} t^{-1} w_k t^k$$

where each w_i is either trivial or in $S \setminus \{t\}$ and $\lfloor \frac{n-1}{3} \rfloor \leqslant k \leqslant n - 1$ since there must be at least 1 non-trivial w_i and at most $\lfloor \frac{n-1}{3} \rfloor$ non-trivial w_i. This produces the bound

$$\sum_{k=\lfloor \frac{n-1}{3} \rfloor}^{n-1} \binom{k+1}{n-2k} (m-1)^{n-2k}$$

since, for each k, $n-2k$ of the $\{w_i \mid i = 0, \ldots, k\}$ may be chosen from $S \setminus \{t\}$ and the other w_i are trivial. Now

$$\begin{aligned}\sum_{k=\lfloor \frac{n-1}{3} \rfloor}^{n-1} \binom{k+1}{n-2k} (m-1)^{n-2k} &\leqslant \sum_{k=\lfloor \frac{n-1}{3} \rfloor}^{n-1} \binom{n}{n-2k} (m-1)^{n-2k} \\ &\leqslant (m-1)^2 \cdot \sum_{j=0}^{\lfloor n/3 \rfloor} \binom{n}{j} (m-1)^j \\ &\leqslant (m-1)^2 \cdot (m-1+1)^{\lfloor n/3 \rfloor}\end{aligned}$$

and so the base of G is negligible in G. □

We end by posing two questions, both of which could represent future work. These seem natural in the context of Theorem 1 and Theorem 2.

Question 3. *To what extent can the approach used above apply to more groups? For example, taking a group $G := F \wr T$ where $|F| < \infty$ and T is torsion free (possibly $\mathbb{Z}^n$ for some $n \in \mathbb{N}$) can one state that the base of G is negligible in G?*

Question 4. *Given a finitely generated group H, is the base of $G := H \wr \mathbb{Z}$ negligible in G? Moreover, what if $\mathbb{Z}$ is replaced with another finitely generated infinite group?*

References

[AMV] Y. Antolín, A. Martino, and E. Ventura, *Degree of commutativity of infinite groups*, Proceedings of the American Mathematical Society (to appear).

[Bab88] I. K. Babenko, *Closed geodesics, asymptotic volume and the characteristics of growth of groups*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 4, 675–711, 895. MR 966980

[BT15] Michelle Bucher and Alexey Talambutsa, *Minimal exponential growth rates of metabelian Baumslag-Solitar groups and lamplighter groups*, arXiv:1506.03569 (2015).

[Con97] Gregory R. Conner, *A class of finitely generated groups with irrational translation numbers*, Arch. Math. (Basel) **69** (1997), no. 4, 265–274. MR 1466819

[Con98] ———, *Properties of translation numbers in nilpotent groups*, Comm. Algebra **26** (1998), no. 4, 1069–1080. MR 1612184

[CT05] Sean Cleary and Jennifer Taback, *Metric properties of the lamplighter group as an automata group*, Geometric methods in group theory, Contemp. Math., vol. 372, Amer. Math. Soc., Providence, RI, 2005, pp. 207–218. MR 2140090

[Gri91] Rostislav I. Grigorchuk, *On growth in group theory*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 325–338. MR 1159221

[GS10] Victor Guba and Mark Sapir, *On the conjugacy growth functions of groups*, Illinois J. Math. **54** (2010), no. 1, 301–313. MR 2776997

[HO13] Michael Hull and Denis Osin, *Conjugacy growth of finitely generated groups*, Adv. Math. **235** (2013), 361–389. MR 3010062

Mathematical Sciences, University of Southampton, SO17 1BJ, UK
E-mail address: charles.cox@soton.ac.uk
URL: http://www.southampton.ac.uk/~cc14v07/