DECISION PROBLEMS AND PROFINITE COMPLETIONS OF GROUPS

MARTIN R. BRIDSON

Abstract. We consider pairs of finitely presented, residually finite groups $P \hookrightarrow \Gamma$ for which the induced map of profinite completions $\hat{P} \to \hat{\Gamma}$ is an isomorphism. We prove that there is no algorithm that, given an arbitrary such pair, can determine whether or not P is isomorphic to Γ. We construct pairs for which the conjugacy problem in Γ can be solved in quadratic time but the conjugacy problem in P is unsolvable.

Let $\mathcal{J}$ be the class of super-perfect groups that have a compact classifying space and no proper subgroups of finite index. We prove that there does not exist an algorithm that, given a finite presentation of a group Γ and a guarantee that $\Gamma \in \mathcal{J}$, can determine whether or not $\Gamma \cong \{1\}$.

We construct a finitely presented acyclic group H and an integer k such that there is no algorithm that can determine which k-generator subgroups of H are perfect.

For Karl Gruenberg, in memoriam

Introduction

The profinite completion of a group Γ is the inverse limit of the directed system of finite quotients of Γ; it is denoted $\hat{\Gamma}$. The natural map $\Gamma \to \hat{\Gamma}$ is injective if and only if Γ is residually finite. In [9] Bridson and Grunewald settled a question of Grothendieck [18] by constructing pairs of finitely presented, residually finite groups $u : P \hookrightarrow \Gamma$ such that $\hat{u} : \hat{P} \to \hat{\Gamma}$ is an isomorphism but P is not isomorphic to (or even quasi-isometric to) Γ. Pairs of finitely generated groups with this property had been found earlier by Platonov and Tavkin [23], Bass and Lubotzky [1], and Pyber [24].

In the present article we begin to explore how different a pair of finitely presented residually finite groups $u : P \hookrightarrow \Gamma$ can be if $\hat{u} : \hat{P} \to \hat{\Gamma}$ an isomorphism, and ask how hard it can be to determine if u is an isomorphism. To make precise the distinctions involved, we focus on the basic decision problems of

---

Date: 8 April 2008; 18 September 2008.

2000 *Mathematics Subject Classification.* 20E18, 20F10.

Key words and phrases. Profinite groups, conjugacy problem, isomorphism problem.

This research was supported by a Senior Fellowship from the EPSRC of Great Britain.

group theory. Since all finitely generated, residually finite groups has a solvable word problem, the first serious issue to be addressed is the solvability of the conjugacy problem.

Theorem A. *There exist pairs of finitely presented, residually finite groups* $u : P \hookrightarrow \Gamma$ *such that* $\hat{u} : \hat{P} \to \hat{\Gamma}$ *is an isomorphism but the conjugacy problem in* P *is unsolvable while the conjugacy problem in* Γ *can be solved in quadratic time.*

Refinements of this result are discussed in Section 2. In particular the "quadratic time" assertion is sharpened and made more precise, and the issue of whether Γ can be made conjugacy separable is discussed.

Concerning the isomorphism problem we prove the following result, a more technical statement of which appears as Theorem 4.1.

Theorem B. *There does not exist an algorithm that, given a finitely presented, residually finite group* Γ *and a finitely presentable subgroup* $u : P \hookrightarrow \Gamma$ *with* $\hat{u} : \hat{P} \to \hat{\Gamma}$ *an isomorphism, can determine whether or not* P *is (abstractly) isomorphic to* Γ*, nor does there exist an algorithm that can determine whether or not* u *is an isomorphism.*

As an illustration of the difficulty of deciding which subgroups of a fixed residually finite group are profinitely equivalent to the ambient group we prove:

Theorem C. *There exists a residually finite, finitely presented group* Γ*, an integer* k*, a finitely presented subgroup* $u : P \hookrightarrow \Gamma$ *with* $\hat{u} : \hat{P} \to \hat{\Gamma}$ *an isomorphism, and a recursive sequence of* k*-generator subgroups* $\iota_n : K_n \hookrightarrow \Gamma$ *with* $P \subset K_n \subset \Gamma$ *such that there is no algorithm that can decide for which* n *the map* $\hat{\iota}_n : \hat{K}_n \to \hat{\Gamma}$ *is an isomorphism.*

Our proof of Theorem A is based on the constructions in [2], [13] and [9], together with some observations on the nature of universal central extensions (Propositions 1.3 and 1.6). Theorems B and C further require the construction of new families of finitely presented groups, well adapted for use in the framework of [9] but wild enough to encode undecidable phenomena (see Sections 3 and 5). To this end, in Theorem 5.6 we exhibit a finitely presented acyclic group H and an integer k such there is no algorithm that can determine which k-generator subgroups of H are perfect, while in Theorem 3.1 we prove a sharper version of the following result. Recall that a group G is termed *super-perfect* if $H_1(G;\mathbb{Z}) = H_2(G;\mathbb{Z}) = 0$.

Theorem D. *Let* $\mathcal{J}$ *be the class of super-perfect groups that have a compact classifying space and no proper subgroups of finite index. There does not exist an algorithm that, given a finite presentation of a group* Γ *and a guarantee that* $\Gamma \in \mathcal{J}$*, can determine whether or not* $\Gamma \cong \{1\}$.

The proof of this theorem involves an algorithm that I learnt from C.F. Miller III. Given a finite presentation of a perfect group, this algorithm will output a finite presentation of the universal central extension of the group; see Corollary 3.6.

Karl Gruenberg asked me if Theorem B might be true after a London Algebra Colloquium that I gave in March 2004 on my work with Fritz Grunewald [9]. Conversations with Karl, who died in October 2007, were always stimulating, both mathematically and culturally, and he is sorely missed.

1. Background and Preparation

In this Section we gather five sets of ideas that we will need in the proofs of the theorems stated in the introduction.

1.1. **The Bridson-Grunewald Construction.** Most of the pairs $u : P \hookrightarrow \Gamma$ that we shall consider, with $\hat{u}$ an isomorphism, derive from the main construction in [9]. Thus we begin by recalling the salient points of that article. Recall that a finitely presented group G is said to be of *type* F_3 if there is a CW-complex $K(G,1)$ that has fundamental group G, contractible universal cover, and only finitely many cells in its 3-skeleton.

Theorem 1.1 (Bridson-Grunewald)**.** *If Q is a finitely presented group that is infinite but has no non-trivial finite quotients, and if $H_2(Q,\mathbb{Z}) = 0$, then there is a short exact sequence of groups*

$$1 \to N \to \Gamma \xrightarrow{p} Q \to 1$$

where Γ is finitely presented, torsion-free, hyperbolic and residually finite, N is finitely generated but not finitely presented, the inclusion $u : P \hookrightarrow \Gamma \times \Gamma$ of the fibre product

$$P = \{(\gamma_1, \gamma_2) \mid p(\gamma_1) = p(\gamma_2)\}$$

induces an isomorphism of profinite completions $\hat{P} \to \hat{\Gamma} \times \hat{\Gamma}$, but P is not isomorphic to $\Gamma \times \Gamma$.

If Q is of type F_3, then P is finitely presented.

The assertion in the final sentence of this theorem is a special case of the 1-2-3 Theorem of Baumslag, Bridson, Miller and Short [2]. The short exact sequence in the first sentence comes from Wise's variation on the Rips construction (see [25], [26]), which is proved using small cancellation theory. See Section 7 of [9] for a demonstration of the explicit nature of this construction.

Theorem 1.2 (Rips-Wise)**.** *There is an algorithm that associates to every finite group-presentation $\mathcal{Q} \equiv \langle X \mid R \rangle$ a finite presentation $\mathcal{G} \equiv \langle \check{X} \mid \check{R} \rangle$ with $\check{X} = X \cup \{a_1, a_2, a_3\}$ and $|\check{R}| = |R| + 6|X|$, such that the group Γ with presentation $\mathcal{G}$ is residually finite, torsion-free, hyperbolic (in the sense of Gromov) and* *has a compact 2-dimensional classifying space. The subgroup* $N \subset \Gamma$ *generated by* $\{a_1, a_2, a_3\}$ *is normal and there is a short exact sequence*

$$1 \to N \to \Gamma \xrightarrow{p} Q \to 1$$

defined by $p(x) = x$ *for all* $x \in X$.

In order to make Theorem 1.1 useful, one needs a plentiful supply of groups of type F_3 that are super-perfect and have no finite quotients. As explained in Section 8 of [9], one can obtain such a supply by proceeding as follows. Following the constructions in [4], one can embed any group G of type F_3 in a group G' of type F_3 that has no non-trivial finite quotients; one does this by forming suitable free products and HNN extensions. One then obtains a group Q as needed in Theorem 1.1 by forming the universal central extension of G'. The constructions at the heart of the present article implement this basic procedure in an algorithmic manner, using carefully chosen input groups G.

1.2. **Universal central extensions.** The standard reference for universal central extensions is [22], pp. 43-47.

A central extension of a group G is a group $\tilde{G}$ equipped with a homomorphism $\pi : \tilde{G} \to G$ whose kernel is central in $\tilde{G}$. Such an extension is *universal* if given any other central extension $\pi' : E \to G$ of G, there is a unique homomorphism $f : \tilde{G} \to E$ such that $\pi' \circ f = \pi$.

The following proposition summarizes those properties of universal central extensions that we need.

Proposition 1.3. (1) *G has a universal central extension $\tilde{G} \to G$ if and only if G is perfect. (If it exists, $\tilde{G} \to G$ is unique up to isomorphism over G.)*

(2) *If G is expressed as a quotient of a free group $G = F/R$, then the natural map $[F, F]/[F, R] \to G$ is the universal central extension of G.*
(3) *The kernel of the map $[F, F]/[F, R] \to G$ is $R \cap [F, F]/[F, R]$, which according to Hopf's formula is $H_2(G; \mathbb{Z})$. Thus the universal central extension of a super-perfect group G is $\mathrm{id} : G \to G$.*
(4) *If $\tilde{G} \to G$ is a universal central extension, then $\tilde{G}$ is super-perfect.*
(5) *If G has no non-trivial finite quotients then neither does $\tilde{G}$.*
(6) *If G is finitely presented then so is $\tilde{G}$.*
(7) *If G is of type F_3 then so is $\tilde{G}$.*
(8) *If G has a 2-dimensional classifying space $K(G, 1)$ then $\tilde{G}$ is torsion-free and has a compact classifying space.*

Proof. The first four facts are standard; see [22], pp. 43-47. Point (5) is proved by noting that since $\tilde{G}$ is perfect, a non-trivial finite quotient would have to be non-abelian, and factoring out the centre would give a non-trivial quotient of G.

For items (6) and (7) we consider the short exact sequence furnished by (2) and (3):

$$1 \to H_2(G;\mathbb{Z}) \to \tilde{G} \to G \to 1.$$

If G is finitely presented then $H_2(G;\mathbb{Z})$ is finitely generated. Finitely generated abelian groups have classifying spaces with finitely many cells in each dimension, so in particular they are of type F_3. For any n, if the first and last groups in a short exact sequence are of type F_n then so is the group in the middle (and likewise, if they have compact classifying spaces then so does the group in the middle) — see [16], Section 7.1.

Turning to (8), recall that if a group has a finite-dimensional classifying space, it is torsion-free (Remark 1.4). Thus, by consideration of the short exact sequence above, it suffices to argue that $H_2(G;\mathbb{Z})$ is torsion-free (in which case it has a compact classifying space, namely a torus of the appropriate dimension). Now, $H_2(G;\mathbb{Z})$ is isomorphic to the second homology group of the given $K = K(G,1)$, which is assumed to have no 3-cells. Thus $H_2(G;\mathbb{Z})$ is isomorphic to the kernel of the second boundary map in the cellular chain complex of K; in particular it is a free abelian group. □

Remark 1.4. If a group G has a finite dimensional $K(G,1)$ then G must be torsion-free for otherwise it would contain an element of prime order, g say, and the quotient of $\tilde{K}$ by $\langle g\rangle \cong \mathbb{Z}_p$ would be a finite-dimensional $K(\mathbb{Z}_p,1)$, contradicting the fact that $\mathbb{Z}_p$ has cohomology in infinitely many dimensions.

We shall also need to control the complexity of the word problem when we pass to universal central extensions. This relies on the simple observation:

Lemma 1.5. *If G is a finitely generated, recursively presented group and $H \subset G$ is a finitely generated subgroup with a solvable word problem, then there is an algorithm that, given a word w in the generators of G and a guarantee that $w \in H$, can determine whether or not $w = 1$ in G.*

Proof. Fix finite sets of generators A for H and X for G, and for each $a \in A$ fix a word u_a in $X^{\pm 1}$ such that $a = u_a$ in G. Given a word w in the letters $X^{\pm 1}$ with the promise that it defines an element of H, one runs through products π of the words u_a and their inverses, doing a naïve search on products P of conjugates of the defining relations of G to check if P is equal to $w\pi$ in the free group $F(X)$. Running through all possibilities for π and P along finite diagonals, one will eventually find a valid formula, proving that w is equal in G to a certain word in the letters $A^{\pm 1}$. One can then use the solution to the word problem in H to decide whether or not $w = 1$ in G. □

Proposition 1.6. *If G is a finitely presented perfect group whose centre is finitely generated, then the word problem in G is solvable if and only if the word problem in its universal central extension $\tilde{G}$ is solvable.*

Proof. We fix a finite generating set X for G, choose a preimage $\tilde{x} \in \tilde{G}$ for each $x \in X$, and fix a finite generating set Z for the centre of $\tilde{G}$ that includes a finite generating set Z' for the kernel of $\tilde{G} \to G$. Note that the centre of $\tilde{G}$ is finitely generated because it is an extension of the centre of G by $H_2(G;\mathbb{Z})$. Let $\tilde{X} = \{\tilde{x} : x \in X\}$ and note that $\tilde{X} \cup Z'$ generates $\tilde{G}$.

First suppose that $\tilde{G}$ has a solvable word problem. Given a word w in the letters $X^{\pm 1}$, we replace each occurrence in w of $x \in X$ by $\tilde{x}$ and ask if the resulting word $\tilde{w}$ defines a central element of $\tilde{G}$. The hypothesized solution to the word problem in $\tilde{G}$ allows us to decide this because it is enough to check if $[\tilde{w}, y] = 1$ for all $y \in \tilde{X} \cup Z'$. If $\tilde{w}$ is not central, we stop and declare that $w \neq 1$ in G. If $\tilde{w}$ is central in $\tilde{G}$ then w is central in G, and as in Lemma 1.5 this enables us to decide whether or not $w = 1$ in G.

Now suppose that G has a solvable word problem. Given a word W in the letters $(\tilde{X} \cup Z')^{\pm 1}$, we consider the word w obtained by deleting all occurrences of all letters $z \in Z'$. If $w \neq 1$ in G, then we declare $W \neq 1$ in $\tilde{G}$. If $w = 1$ then we know W is central in $\tilde{G}$ and hence we can use Lemma 1.5 to determine whether or not $W = 1$. □

1.3. **Aspherical presentations.** We remind the reader that a presentation of a group G is termed *aspherical* if the standard 2-complex of the presentation is a $K(G,1)$, that is, the universal covering is contractible. For example, a free presentation of a free group is aspherical.

It is straightforward to prove that if $\Pi_1 \equiv \langle \mathcal{A}_1 \mid \mathcal{R}_1 \rangle$ and $\Pi_2 \equiv \langle \mathcal{A}_2 \mid \mathcal{R}_2 \rangle$ are aspherical presentations of groups G_1 and G_2, then the natural presentations $\langle \mathcal{A}_1 \sqcup \mathcal{A}_2 \mid \mathcal{R}_1 \sqcup \mathcal{R}_2,\, u_i v^{-1}\, (i = 1, \dots, n) \rangle$ of any amalgamated free product of the form $G_1 *_F G_2$ with F free of rank n, is also aspherical. Likewise, the natural presentations of HNN extensions of the form $G_1 *_F$ will be aspherical.

1.4. **Higman's group.** The following group constructed by Graham Higman [20] will provide useful input to certain of our constructions.

$$J = \langle a, b, c, d \mid aba^{-1} = b^2,\ bcb^{-1} = c^2,\ cdc^{-1} = d^2,\ dad^{-1} = a^2 \rangle.$$

The salient features of J are described in the following proposition, in which D is the group with presentation $D = \langle \alpha, \beta, \gamma \mid \alpha\beta\alpha^{-1} = \beta^2,\ \beta\gamma\beta^{-1} = \gamma^2 \rangle$.

Proposition 1.7. (1) *J has no non-trivial finite quotients.*
(2) *The given presentation of J is aspherical.*
(3) *$J \cong D_1 *_{F_2} D_1$, where $D_1 \cong D_2 \cong D$ and the amalgamation identifies the subgroups $\langle \alpha_i, \gamma_i \rangle \subset D_i$ by $\alpha_1 = \gamma_2$ and $\gamma_1 = \alpha_2$.*
(4) *The abelianization of $\langle a, b, c \rangle \subset J$ is infinite cyclic, generated by the image of a.*
(5) *$H_i(J;\mathbb{Z}) = 0$ for all $i \geq 1$.*

Proof. Higman [20] proved (1) using some elementary number theory.

The first thing that we must prove for (3) is that the subgroup of D generated by α and γ is free of rank 2. But this is clear from Britton's Lemma, once one observes that D is obtained from the infinite cyclic group generated by γ by two HNN extensions along cyclic subgroups: the first extension has stable letter β, the second has stable letter α and amalgamated subgroups in $\langle\beta\rangle$. Following the comments in Section 1.3, this HNN description also shows that the given presentation of D is aspherical, and that the presentation of $D_1 *_{F_2} D_2$ displayed below is too.

The isomorphism in (3) is given by $a \mapsto \alpha_1,\ b \mapsto \beta_1,\ c \mapsto \gamma_1,\ d \mapsto \beta_2$ (which has an obvious inverse). This restricts to an isomorphism from $\langle a, b, c\rangle \subset J$ to D_1, which has abelianisation $\mathbb{Z}$, generated by the image of α_1. This proves (4).

In order to prove (2) we compare the given presentation of J to that associated with the description $J \cong D_1 *_{F_2} D_2$, namely

$$\langle \alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2 \mid \alpha_i\beta_i\alpha_i^{-1} = \beta_i^2,\ \beta_i\gamma_i\beta_i^{-1} = \gamma_i^2\ (i = 1, 2),\ \alpha_1\gamma_2^{-1},\ \alpha_2\gamma_1^{-1}\rangle.$$

The generators α_2 and γ_2 together with the last two relators can be removed by obvious Tietze moves. These relators correspond to bigons (2-cells with boundary cycles of length 2) in the standard 2-complex of the presentation, and the effect of the Tietze moves is to shrink each of these to an edge in the obvious manner. Since this shrinking is a homotopy equivalence, we conclude that the modified presentation is still aspherical. The given presentation of J is obtained from this modified presentation by simply renaming the generators, so (2) is proved.

Turning to (5), note that we already know that $H_1(J; \mathbb{Z})$, the abelianization of J, is trivial. Also, in the light of (1), we know that the groups $H_i(J; \mathbb{Z})$ coincide with the homology groups of the cellular chain complex of the standard 2-complex of the given presentation of J. The group of cellular k-chains C_k is trivial if $k \geq 3$ (as there are no k-cells), so $H_k(J; \mathbb{Z}) = 0$ for $k \geq 3$ and $H_2(J; \mathbb{Z})$ is isomorphic to the kernel of $\partial_2 : C_2 \to C_1$. The final point to note is that ∂_2 is injective because $H_1(J; \mathbb{Z}) = C_1/\text{im}(\partial_2) = 0$ and $C_1 \cong C_2 \cong \mathbb{Z}^4$. □

The final argument in the above proof generalizes immediately to prove the following lemma, which we shall need in Section 5.

Lemma 1.8. *If G has an aspherical presentation with n generators and m relations, and the abelianization of G is finite, then $H_2(G; \mathbb{Z}) \cong \mathbb{Z}^{m-n}$.*

1.5. **Centralizers and conjugacy in hyperbolic groups.** Recall from [17] that a finitely generated group Γ is said to be *hyperbolic* (in the sense of Gromov) if there is a constant $\delta > 0$ such that each side of each triangle in the Cayley graph of Γ is contained in the δ-neighbourhood of the union of the other two sides.

We shall only consider torsion-free hyperbolic groups. The centralizer of every non-trivial element in such a group is cyclic; in particular every element is contained in a maximal cyclic subgroup, and the centralizer of a non-cyclic subgroup is trivial.

Hyperbolic groups admit a rapid and effective solution to the conjugacy problem, both for individual elements and for finite subsets (but not finitely generated subgroups). In particular, Bridson and Howie [7] prove that if a torsion-free group Γ is δ-hyperbolic with respect to a generating set of cardinality k, then there is a constant $C = C(\delta, k)$ and an algorithm that, given two lists of words $[a_1, \dots, a_m]$ and $[b_1, \dots, b_m]$ in the generators of Γ, the longest word having length ℓ, will terminate after at most $Cm\ell^2$ steps having determined whether or not there exists an element $\gamma \in \Gamma$ such that $\gamma a_i \gamma^{-1} = b_i$ for $i = 1, \dots, m$, outputting such a γ if it exists. Applying this to lists of length one, we deduce that the conjugacy problem for individual elements can be solved in quadratic time in Γ, and indeed in the direct product of finitely many copies of Γ. A sharper result was obtained by Epstein and Holt [15]. They prove that the conjugacy problem in Γ is solvable in linear time if one uses a standard RAM model of computation in which basic arithmetical operations on integers are assumed to take place in constant time; this gives an algorithm of Turing complexity $O(n \log n)$. This algorithm extends easily to $\Gamma \times \Gamma$.

To mark the distinction between Turing and RAM models of computation, we shall use the term *RAM-linear* when referring to the Epstein-Holt algorithm.

2. The conjugacy problem

With the preceding discussion in hand, we can state a more precise version of Theorem A.

Theorem 2.1. *There exist pairs of finitely presented, residually finite groups $u : P \hookrightarrow G$ such that $\hat{u} : \hat{P} \to \hat{G}$ is an isomorphism but the conjugacy problem in P is unsolvable while the conjugacy problem in G can be solved in RAM-linear time.*

Proof. In [13] (cf. section 3.1 below) Collins and Miller described a group G that has an unsolvable word problem and a compact 2-dimensional classifying space $K(G, 1)$; in particular G is torsion-free. As in [4] (or Section 3.2 below), by forming suitable free products with amalgamation and HNN extensions along free subgroups, we can embed G in a group G' that again has such a classifying space and has the additional feature that G' has no proper subgroups of finite index. By construction, G' has trivial centre. And since G' contains a copy of G, it has an unsolvable word problem.

Let Q be the universal central extension of G'. We saw in Proposition 1.3 that Q is super-perfect, torsion-free, has no proper subgroups of finite index, and has a compact classifying space. In Proposition 1.6 we proved that the word problem in Q is unsolvable.

Let Γ be the torsion-free hyperbolic group obtained by applying Theorem 1.2 to Q and let $P \subset \Gamma\times\Gamma$ be the fibre product of $\Gamma \to Q$. Theorem 1.1 assures us that P is finitely presented and that $P \to \Gamma \times \Gamma$ induces an isomorphism of profinite completions. We saw in Section 1.5 that the conjugacy problem in $\Gamma \times \Gamma$ can be solved in RAM-linear time, so we will be done if we can argue that the conjugacy problem in P is unsolvable.

In the notation of Theorem 1.1, we have $p : \Gamma \to Q$ with kernel N. We fix a finite generating set X for Q, choose a set of lifts $\tilde{X} = \{\tilde{x} \mid x \in X\}$ with $p(\tilde{x}) = x$ and consider a generating set $\hat{X} \cup \{a_1, \dots, a_l\}$ for Γ, where each a_i is in N and the cyclic subgroups $C_i := \langle a_i\rangle \subset N$ are maximal with respect to inclusion. Note that since Q is torsion free, $\langle a_i\rangle$ will be maximal in Γ not just in N, and hence the centralizer $Z(a_i)$ of (a_i, a_i) in $\Gamma \times \Gamma$ is $C_i \times C_i$. In particular $Z(a_i) \subset P$.

We claim that there is no algorithm that, given a word w in the letters $\tilde{X}^{\pm 1}$, can determine whether or not $(w^{-1}a_1w, a_1)$ is conjugate to (a_1, a_1) in P.

First note that $(w^{-1}a_1w, a_1)$ does indeed belong to P since $p(w^{-1}a_1w) = p(a_1) = 1$. Also observe that $(w, 1)$ conjugates (a_1, a_1) to $(w^{-1}a_1w, a_1)$ in $\Gamma \times \Gamma$. Hence there exists $\pi \in P$ with $\pi(a_1, a_1)\pi^{-1} = (w^{-1}a_1w, a_1)$ if and only if $\pi(w, 1) \in Z(a_1) \subset P$, which is equivalent to $(w, 1) \in P$. But $(w, 1)$ belongs to P if and only if w (viewed now as a word in the letters X) is equal to 1 in Q. And since Q has an unsolvable word problem, there is no algorithm that can determine whether or not $(w, 1) \in P$. □

Remark 2.2. In the course of the above proof we established that the membership problem for P is unsolvable; cf. [2], p.468.

Each of the non-trivial groups Q_n constructed in the proof of Theorem 3.1 can play the role of Q in the above proof. Thus we have:

Addendum 2.3. *There does not exist an algorithm that, given a finitely presented, residually finite group G with a conjugacy word problem and a finitely presentable subgroup $u : P \hookrightarrow G$ with $\hat{u} : \hat{P} \to \hat{G}$ an isomorphism, can determine whether or not P has a solvable conjugacy problem.*

2.1. **Conjugacy separability.** A group G is said to be *conjugacy separable* if, for each pair of non-conjugate elements $x, y \in G$ there exists a finite quotient $p : G \to Q$ such that $p(x)$ is not conjugate to $p(y)$ in Q. Conjugacy separability leads to a solution to the conjugacy problem in a group in much the same way as residual finiteness leads to a solution to the word problem. Conjugacy separability is relevant in the context of the present article because it can be expressed as a property of the pair $(G, \hat{G})$: it is equivalent to the statement that $G \hookrightarrow \hat{G}$ is an embedding and $x, y \in G$ are conjugate in $\hat{G}$ if and only if they are conjugate in G.

One would like to refine Theorem 1.2 so as to ensure that the hyperbolic group Γ is conjugacy separable. It is not yet clear if such a refinement exists[1]. If it did, then one could arrange for the group G in Theorem 2.1 to be conjugacy separable. For the moment, I can only arrange this by weakening the finiteness condition on P.

Proposition 2.4. *There exist residually finite groups $u : P \hookrightarrow \Gamma$, with P finitely generated and Γ finitely presented, so that $\hat{u} : \hat{P} \to \hat{\Gamma}$ is an isomorphism but Γ is conjugacy separable while the conjugacy problem in P is unsolvable.*

Proof. Let $Q = \langle X \mid R \rangle$ be as in the proof of Theorem 2.1 and let $p : F \to Q$ be the implied surjection from the free group on the set X. Let $P \subset F \times F$ be the corresponding fibre product and note that P is generated by the finite set $\{(x, x) \mid x \in X\} \cup \{(r, 1) \mid r \in R\}$.

Arguing exactly as in the proof of Theorem 2.1, we see that P has an unsolvable conjugacy problem and that $P \hookrightarrow F \times F$ induces an isomorphism of profinite completions. Baumslag [3] proved that free groups are conjugacy separable, from which it follows easily that $F \times F$ is. □

Remark 2.5. Finitely presented subgroups of direct products of free groups have solvable conjugacy problem [10]. What is more, using results from [8] and [11], Chagas and Zalesskii [14] recently proved that all finitely presented residually free groups are conjugacy separable. Thus one cannot perturb the proof of Proposition 2.4 in a trivial way so as to make P finitely presented.

3. On the triviality problem for super-perfect groups

In Section 4 we shall prove Theorem B by exploiting the existence of sequences of finite presentations with the following properties.

Theorem 3.1. *There exists a finite set $\mathcal{X}$ and a recursive sequence $(\mathcal{R}_n)$ of finite sets of words in the letters $\mathcal{X}^{\pm 1}$, of fixed cardinality, so that there is no algorithm to determine which of the groups $Q_n = \langle \mathcal{X} \mid \mathcal{R}_n \rangle$ are trivial, and each of the groups has the following properties:*

(1) *$H_1(Q_n; \mathbb{Z}) = H_2(Q_n; \mathbb{Z}) = 0$;*
(2) *Q_n has a compact classifying space $K(Q_n, 1)$;*
(3) *Q_n has no non-trivial finite quotients.*

Moreover, if $Q_n \neq 1$ then Q_n has an unsolvable word problem.

3.1. The origin of the undecidability.

Theorem 3.2 (Collins and Miller)**.** *There is an integer k, a finite set X and a recursive sequence (R_n) of finite sets of words in the letters $X^{\pm 1}$ so that:*

(1) *$|R_n| = k$ for all n, and $|X| < k$;*

[1]Update September 2008: Owen Cotton-Barratt and Henry Wilton have now proved that it does exist.

(2) *each of the groups* $\Lambda_n = \langle X \mid R_n \rangle$ *is torsion-free;*
(3) *there is no algorithm that can determine which of these groups are trivial;*
(4) *if* Λ_n *is non- trivial, then the presentation* $\Pi_n \equiv \langle X \mid R_n \rangle$ *is aspherical and each* $x \in X$ *is non-trivial in* Λ_n.

We sketch the proof. In [13], Collins and Miller explain in detail how Boone's classical example of a finitely presented group B with an unsolvable word problem can be obtained from a finitely generated free group in a finite number of steps, where each step consists of taking a free product with amalgamation or an HNN extension in which the associated subgroups are free of finite rank; in particular B is torsion-free and has an aspherical presentation Π_0.

Collins and Miller go on to observe that in Miller's interpretation of Rabin's construction ([21], p.88), the finite presentations Π^w that are constructed, indexed by words w in the generators of Π_0, either define the trivial group (the case where $w = 1$ in B) or else (when $w \neq 1$ in B) they are the natural presentations associated to passing from B to a group Λ_w by a finite chain of free products with free groups and HNN extensions along finitely generated free groups; in particular Λ_w is torsion-free if $w \neq 1$ in B, and Π^w is aspherical. In Miller's construction the presentations Π^w share a common set of generators (i.e. are defined as quotients of a fixed free group) and have the same number of relators. Moreover the number of relators is greater than the number of generators. If Λ_w is non-trivial then each of the given generators has infinite order.

Thus the proof is complete, modulo a switch of indexing set to $\mathbb{N}$, which can be achieved by replacing each word w by its index in the lex-least ordering, for example.

3.2. **Excluding finite quotients.** Let the presentations $\Pi_n \equiv \langle X \mid R_n \rangle$ be as in Theorem 3.2. We shall describe an algorithm that modifies these presentations so as to ensure that the groups they present have no proper subgroups of finite index.

Suppose $X = \{x_1, \dots, x_l\}$.

Let $\langle Y \mid T \rangle$ be a finite aspherical presentation of a group J that has no finite quotients, and let $y \in Y$ be an element whose normal closure in J is the whole group; that is, $J/\langle\langle y \rangle\rangle = 1$. For example, we can take J to be one of the finitely presented infinite simple groups constructed by Burger and Mozes [12], in which case any $y \neq 1$ will do, or we can take the standard presentation of Higman's group $\langle a, b, c, d \mid aba^{-1} = b^2,\ bcb^{-1} = c^2,\ cdc^{-1} = d^2,\ dad^{-1} = a^2 \rangle$ and let y be any of a, b, c, d.

Definition 3.3. Let E_n' be the group with presentation

$$\Pi_n' \equiv \langle X \cup Y_1 \cup \dots Y_l \mid R_n,\ T_1, \dots, T_l,\ x_i^{-1} y_i\ (i = 1, \dots, l) \rangle,$$

where the $\langle Y_i \mid T_i\rangle$ are disjoint duplicates of $\langle Y \mid T\rangle$ (our fixed presentation of J) with $y_i \in Y_i$ corresponding to $y \in Y$.

If the group Λ_n presented by Π_n is non-trivial, then each x_i has infinite order in Λ_n. In this case Π_n' is the natural presentation for the group obtained from Λ_n in l stages by forming amalgamated free products

$$\Lambda_{n,1} = \Lambda_n *_{\mathbb{Z}} J_1 \ \text{ then } \ \Lambda_{n,i} = \Lambda_{n,i-1} *_{\mathbb{Z}} J_i \ \text{ until } \Lambda_n' := \Lambda_{n,l-1} *_{\mathbb{Z}} J_l,$$

where the J_i are isomorphic copies of J and the amalgamation defining $\Lambda_{n,i}$ identifies $x_i \in \Lambda_n \subset \Lambda_{n,i-1}$ with $y \in Y$ in the copy of J that is being attached.

On the other hand, if $\Lambda_n = 1$ then $\Lambda_n' = 1$, as one sees by making iterated use of the observation that the pushout of the diagram $\{1\} \leftarrow \mathbb{Z} \to J$ is trivial if the generator of $\mathbb{Z}$ is mapped to $y \in J$, since $J/\langle\langle y\rangle\rangle = 1$.

Notation: Let $\mathcal{X}$ and Σ_n be, respectively, the generators and relators of Π_n' as given in Definition 3.3.

Lemma 3.4. *Let the groups Λ_n and Λ_n' and the presentation $\Pi_n' \equiv \langle \mathcal{X} \mid \Sigma_n\rangle$ be as above.*

(1) *Λ_n' is trivial if and only if Λ_n is trivial.*
(2) *For all $n \in \mathbb{N}$, the group Λ_n' has no non-trivial finite quotients.*
(3) *The cardinality of Σ_n is independent of n, and $|\Sigma_n| > |\mathcal{X}|$.*
(4) *If Λ_n' is non-trivial then the presentation Π_n' is aspherical.*

Proof. Item (1) is covered by the preceding discussion while (3) is manifest in the definition of Π_n'. In the light of the observations in Section 1.3, item (4) follows immediately from the above description of Π_n' as the presentation of an iterated free product with cyclic amalgamation, together with the fact that $\langle Y \mid T\rangle$ and Π_n are aspherical.

Suppose Λ_n' is non-trivial and consider the copies J_i of J visible in the repeated amalgamations formed in passing from Λ_n to Λ_n'. The relations $x_i = y_i$ show that the union of the J_i generates Λ_n'. Since J has no non-trivial finite quotients, neither does Λ_n'. □

3.3. **Presenting universal central extensions.** I learnt the following result from C.F. Miller III, and I am grateful to him for letting me reproduce his proof here.

Given a group Γ, we shall use the standard notation $[A, B]$ to denote the subgroup of Γ generated by the set of commutators $\{[a, b] : a \in A, b \in B\}$.

Proposition 3.5. *Let $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m\rangle$ be a finitely presented group, let F be the free group on $\{x_1, \dots, x_n\}$ and let $R \subset F$ be the normal closure of $\{r_1, \dots, r_m\}$. Suppose that Γ is perfect and choose $c_i \in [F, F]$ such that $x_i c_i \in R$. Then the following is a finite presentation for the universal central extension of G:*

$$\langle x_1, \dots, x_n \mid x_i c_i,\ [x_i, r_j]\ (i = 1, \dots, n;\ j = 1, \dots, m)\rangle.$$

Proof. Let $K \subset F$ be the subgroup that is the normal closure of the relators in the above presentation. We must prove that F/K is isomorphic to $[F,F]/[F,R]$, the universal central extension of G.

Note that $[F,R] \subset K$.

Let $\tilde{X} := \{x_1c_1, \ldots, x_nc_n\}$. Since $x_ic_i \in R$, the image of $\tilde{X}$ in $F/[F,R]$ is central. In particular $K/[F,R]$ is abelian, generated by the image of $\tilde{X}$.

Since the image of $\tilde{X}$ generates $F/[F,F]$, the natural map $K/[F,R] \to F/[F,F]$ is onto. Moreover, as the image of $\tilde{X}$ is a basis for $F/[F,F] \cong \mathbb{Z}^n$, it must also be a basis for $K/[F,R]$. Hence the natural map $K/[F,R] \to F/[F,F]$ is an isomorphism. In particular the kernel of this map is trivial, so $K \cap [F,F] \subset [F,R]$. But $[F,R] \subset K$, so $K \cap [F,F] \subset [F,R]$.

Now consider the map $[F,F] \to F/K$. As $x_ic_i \in K$ and $c_i \in [F,F]$, the image of this map contains x_iK for $i = 1, \ldots, n$. Thus the map is onto. Its kernel is $[F,F] \cap K$, which we just proved is $[F,R]$. Therefore F/K is isomorphic to $[F,F]/[F,R]$. □

Corollary 3.6. *There exists an algorithm that, given a finite presentation $\langle X \mid \Sigma \rangle$ of a perfect group G, will output a finite presentation $\langle X \mid \tilde{\Sigma} \rangle$ for the universal central extension of G.*

Proof. Let F be the free group on X. The algorithm generates an enumeration $d_0, d_1, \ldots$ of words representing the elements of $[F,F]$ and an enumeration $\rho_0, \rho_1, \ldots$ of the normal closure of Σ; it runs through the list of all pairs (d_i, ρ_j), proceeding along finite diagonals. It works as follows: for each $x \in X$ in turn, it runs through the products $xd_i\rho_j$ checking to see if any of them is equal to the identity in F (that is, freely equal to the empty word). Since the given group G is perfect, the algorithm will eventually find indices $i(x)$ and $j(x)$ such that $xd_{i(x)}\rho_{j(x)}$ is equal to the identity in F. The algorithm outputs

$$\tilde{\Sigma} = \{xd_{i(x)} : x \in X\} \cup \{[\sigma,\, x_k] : \sigma \in \Sigma, x \in X\}.$$

□

3.4. **The proof of Theorem 3.1.** In Subsection 3.2 we constructed a recursive sequence of finite presentations $\Pi'_n \equiv \langle \mathcal{X} \mid \Sigma_n \rangle$ defining quotients Λ'_n of a fixed free group $F = F(\mathcal{X})$, such that none of the Λ'_n have any non-trivial finite quotients but there was no algorithm to determine which of the Λ'_n are trivial; if $\Lambda'_n \neq 1$ then Π'_n is aspherical. Furthermore, if $\Lambda'_n \neq 1$ then it has an unsolvable word problem, because it contains a copy of the group B with which the proof of Theorem 3.2 began.

To complete the proof of Theorem 3.1 we apply the algorithm of Corollary 3.6 to transform each of the presentations Π'_n into a presentation $\tilde{\Pi}_n \equiv \langle \mathcal{X} \mid \tilde{\Sigma}_n \rangle$ for the universal central extension $\tilde{\Lambda}'_n$ of Λ'_n. Note that the presentations $\tilde{\Pi}_n$ still define the groups $\tilde{\Lambda}'_n$ as quotients of the fixed free group $F(\mathcal{X})$, and that $|\tilde{\Sigma}_n|$ is independent of n.

If we define $Q_n := \tilde{\Lambda}'_n$ and $\mathcal{R}_n := \tilde{\Sigma}_n$, then Proposition 1.3 assures us that the groups $Q_n = \langle \mathcal{X} \mid \mathcal{R}_n \rangle$ have the properties stated in Theorem 3.1. □

4. The isomorphism problem

The following is a more precise formulation of Theorem B.

Theorem 4.1. *There exists a finitely generated free group $F = F(\mathcal{Y})$ and two recursive sequences of finite subsets (T_n) and (U_n), with cardinalities independent of n, such that:*

(1) *for all n, the group $G_n := \langle \mathcal{Y} \mid T_n \rangle$ is finitely presented, residually finite, and has a compact classifying space;*
(2) *for all n, the subgroup $P_n \subset G_n$ generated by the image of U_n is finitely presentable;*
(3) *for all n, the inclusion $P_n \hookrightarrow G_n$ induces an isomorphism of profinite completions $\hat{P}_n \to \hat{G}_n$;*
(4) *there is no algorithm that can determine for which n the inclusion $P_n \hookrightarrow G_n$ is an isomorphism;*
(5) *there is no algorithm that can determine for which n the groups P_n and G_n are abstractly isomorphic.*

Proof. Let the presentations $\langle \mathcal{X} \mid \mathcal{R}_n \rangle$ for the groups Q_n be as in Theorem 3.1. The proof of the present theorem may be summarized as follows: we take the presentation of $G_n := \Gamma_n \times \Gamma_n$ obtained by applying the algorithm of Theorem 1.2 to $\langle \mathcal{X} \mid \mathcal{R}_n \rangle$, and we define U_n to be the natural generating set for the fibre product $P_n \subset G_n$ of $p_n : \Gamma_n \to Q_n$. What follows is merely a careful exposition of this construction.

Theorem 1.2 associates to $\langle \mathcal{X} \mid \mathcal{R}_n \rangle$ a group Γ_n with presentation $\mathcal{G}_n \equiv \langle \mathcal{X}, a_1, a_2, a_3 \mid \check{\mathcal{R}}_n \rangle$. We define $\mathcal{Y}$ to be the disjoint union of two copies of $\check{\mathcal{X}} = \mathcal{X} \cup \{a_1, a_2, a_3\}$ and denote words w in the letters of the first (resp. second) copy $(w, 1)$ (resp. $(1, w)$).

Let $T_n = \{(1, r), (r, 1) \mid r \in \check{\mathcal{R}}_n\} \cup \{[(x, 1),\, (1, z)] \mid x, z \in \check{\mathcal{X}}\}$ and note that $\langle \mathcal{Y} \mid T_n \rangle$ is a presentation of $G_n := \Gamma_n \times \Gamma_n$.

Let $U_n = \{(a_i, 1),\, (1, a_i) \mid i = 1, 2, 3\} \cup \{(x, 1)(1, x) \mid x \in \check{\mathcal{X}}\}$ and note that the image of U_n in G_n generates the fibre product P_n of the map $p_n : \Gamma_n \to Q_n$, which is defined by $p_n(x, 1) = p_n(1, x) = p(x)$ for $x \in \mathcal{X}$ and $p(a_i) = 1$ for $i = 1, 2, 3$.

Because the derivation of T_n and U_n from $\mathcal{R}_n$ is entirely algorithmic, the sequences (T_n) and (U_n) are recursive.

The Bridson-Grunewald Theorem (1.1) tells us that $P_n \hookrightarrow G_n$ induces an isomorphism $\hat{P}_n \to \hat{G}_n$, and P_n is finitely presentable because Q_n has type F_3. (Recall that Q_n was constructed so as to have a finite classifying space.)

If $Q_n = 1$, then $P_n = G_n$. But if Q_n is infinite then the fact that certain centralizers in P_n are not finitely presented shows that it is not isomorphic to G_n ([9], Section 6). Theorem 3.1 tells us that there is no algorithm that can determine whether or not $Q_n \neq 1$. Hence there is no algorithm that can determine whether or not P_n is isomorphic to G_n, and no algorithm that can determine whether or not $P_n \hookrightarrow G_n$ is an isomorphism. □

5. Super-Perfect Group with Unsolvable Generation Problem

In this Section we prove two theorems, each of which implies that there exist finitely presented super-perfect groups with no finite quotients in which there is no algorithm to determine which finite subsets generate.

5.1. An inability to distinguish super-perfect subgroups from those with free quotients.

Theorem 5.1. *There exists a finitely presented super-perfect group Λ, an integer $r > 0$, and a recursive sequence of r-element subsets $\mathcal{S}_n \subset \Lambda$, given by words in the generators, so that each $\mathcal{S}_n$* **either** *generates Λ or* **else** *generates a subgroup that maps onto a non-abelian free group, and there is no algorithm that can determine which alternative holds. Moreover, Λ has a compact classifying space and no proper subgroups of finite index.*

Remark 5.2. An additional feature of the sets $\mathcal{S}_n$ is that if $\langle \mathcal{S}_n \rangle$ is not equal to Λ then it is not finitely presentable, but this will play no role in the present article.

Theorem 3.2 provides us with an example of a sequence of finitely presented groups $\Lambda_n = \langle X \mid R_n \rangle$, with $k = |R_n|$ fixed, for which there is no algorithm to determine which of the Λ_n are trivial, but where one knows that each $x \in X$ has infinite order in Λ_n if $\Lambda_n \neq 1$.

Let F denote the free group on X and recall once again that the fibre product $P_n \subset F \times F$ of the natural projection $F \to \Lambda_n$ is generated by

$$S_n = \{(x, x) \mid x \in X\} \cup \{(r, 1) \mid r \in R_n\}.$$

Each S_n has $k + l$ elements, where l is the cardinality of $X = \{x_1, \dots, x_l\}$. Moreover since the sequence (R_n) is recursive, so is (S_n).

Let Δ be the amalgamated free product of $F \times F$ with $2l$ copies of Higman's group,

$$J_i = \langle a_i, b_i, c_i, d_i \mid a_i b_i a_i^{-1} = b_i^2,\ b_i c_i b_i^{-1} = c_i^2,\ c_i d_i c_i^{-1} = d_i^2,\ d_i a_i d_i^{-1} = d_i^2 \rangle,$$

where each J_i is attached to $F \times F$ along a cyclic subgroup: for $i \leq l$ the amalgamation identifies $d_i \in J_i$ with $(x_i, 1)$ and for $i > l$ the amalgamation identifies $d_i \in J_i$ with $(1, x_{i-l})$.

Let $\mathcal{C} = \bigcup_{i=1}^{2l} \{a_i, b_i, c_i\}$, let $S_n^+ = S_n \cup \mathcal{C}$ and let $M_n \subset \Delta$ be the subgroup generated by S_n^+.

Lemma 5.3. (1) *Δ has no non-trivial finite quotients.*

(2) *If* $\Lambda_n = 1$ *then* $M_n = \Delta$.
(3) *If* $\Lambda_n \neq 1$ *then* M_n *maps onto a free group of rank* $2l$.

Proof. We saw in Proposition 1.7 that J has no non-trivial finite quotients, and the union of the subgroups $J_i \cong J$ generate Δ, so (1) is proved.

If $\Lambda_n = 1$ then S_n generates $F \times F$, and it is clear that $F \times F$ and $\mathcal{C}$ together generate Δ. This proves (2).

If $\Lambda_n \neq 1$ then the subgroup of $F \times F$ generated by S_n has trivial intersection with each of the cyclic subgroups $\langle (x_i, 1)\rangle$ and $\langle (1, x_i)\rangle$. Furthermore, in Proposition 1.7 we proved that the subgroup $D_i \subset J_i$ generated by $\{a_i, b_i, c_i\}$ (which is isomorphic to $D = \langle a, b, c \mid aba^{-1} = b^2,\, bcb^{-1} = c^2\rangle$) intersects $\langle d_i \rangle$ trivially. It follows (by the standard theory of amalgamated free products) that $\langle S_n \rangle$ and $\langle \mathcal{C} \rangle$ generate their free product in Δ. Thus M_n is isomorphic to the free product of P_n with $2l$ copies of D. We also proved in Proposition 1.7 that D maps onto $\mathbb{Z}$, and therefore M_n maps onto a free group of rank $2l$. □

Proof of Theorem 5.1. Let $\tilde{\Delta}$ be the universal central extension of Δ. From Lemma 5.3(1) and Proposition 1.3(5), we know that $\tilde{\Delta}$ has no proper subgroups of finite index.

We have generators $\mathcal{A} = X_\lambda \cup X_\rho \cup \mathcal{C}$ for Δ, where $X_\lambda = \{(x, 1) \mid x \in X\}$ generates the subgroup $F \times \{1\}$ and $X_\rho = \{(1, x) \mid x \in X\}$ generates the subgroup $\{1\} \times F$. We may regard S_n (and hence S_n^+) as a set of words in these generators by replacing (x, x) in the definition of S_n by $(x, 1)(1, x)$ and by identifying $(r, 1)$ with the corresponding reduced word in the letters $X_\lambda^{\pm 1}$.

We choose a lift $\tilde{a} \in \tilde{\Delta}$ of each $a \in \mathcal{A}$ and define $\tilde{\mathcal{A}} = \{\tilde{a} \mid a \in \mathcal{A}\}$. We then choose a finite generating set Z for the kernel of $\tilde{\Delta} \to \Delta$ and work with the generating set $\mathcal{B} = \tilde{\mathcal{A}} \cup Z$ for $\tilde{\Delta}$.

We define $\tilde{S}_n^+$ to be the set of words in the letters $\mathcal{A}^{\pm 1}$ obtained by replacing each $a \in \mathcal{A}$ by $\tilde{a}$, and we define $\mathcal{S}_n = \tilde{S}_n^+ \cup Z$.

By construction, the subgroup of $\tilde{\Delta}$ generated by $\mathcal{S}_n$ maps onto $M_n \subset \Delta$ and contains the kernel of $\tilde{\Delta} \to \Delta$. Thus $\mathcal{S}_n$ generates $\tilde{\Delta}$ if $M_n = \Delta$ (equivalently, $\Lambda_n = 1$) and $\langle \mathcal{S}_n \rangle$ maps onto a free group of rank $2l$ if $\Lambda_n \neq 1$. And the sequence Λ_n was chosen deliberately so that there is no algorithm that can determine which of these alternatives holds.

Since the standard presentations of $F \times F$ and J are aspherical and Δ is obtained from these groups by a sequence of amalgamations along cyclic subgroups, Δ has an aspherical presentation (see Section 1.3). It follows from Proposition 1.3(8) that $\tilde{\Delta}$ also has a compact classifying space. □

Remark 5.4. Returning to Remark 5.2, note that since M_n is obtained from $\langle \mathcal{S}_n \rangle \subset \tilde{\Delta}$ by factoring out the finitely generated subgroup $\langle Z \rangle$, if $\langle \mathcal{S}_n \rangle$ were finitely presentable then M_n would be too. But M_n is not finitely presentable if $\Lambda_n \neq 1$, because it contains $P_n \subset F \times F$ as a free factor, and this is not finitely presentable [19].

5.2. **An inability to distinguish between subdirect products in an acyclic group.** A subgroup H of a direct product $G_1 \times G_2$ is termed a *subdirect product* if the restriction to H of the coordinate projection $G_1 \times G_2 \to G_i$ is onto for $i = 1, 2$. An important example of a subdirect product is the fibre product $P \subset G \times G$ of a surjection $p : G \to Q$. Such fibre products can be characterised as those subdirect products of $G \times G$ that contain the diagonal.

We need the following variation on Theorem 3.1 of [10].

Lemma 5.5. *Let A and B be super-perfect groups, let $P \subset A \times B$ be a subdirect product, and let $L = A \cap P$. Then $H_1(P; \mathbb{Z}) \cong H_2(A/L; \mathbb{Z})$.*

Proof. Note that $L := A \cap P$ is normal in both A and P. The actions of P and A by conjugation on L define the same subgroup of $\mathrm{Aut}(L)$ and hence the coinvariants $H_0(P/L; H_1(L, \mathbb{Z}))$ and $H_0(A/L; H_1(L, \mathbb{Z}))$ coincide. We will prove that the first of these groups is isomorphic to $H_1(P, \mathbb{Z})$ and the second is isomorphic to $H_2(A/L; \mathbb{Z})$.

The five term exact sequence for $Q = A/L$ gives the exactness of

$$\cdots H_2(A; \mathbb{Z}) \to H_2(A/L; \mathbb{Z}) \to H_0(A/L; H_1(L; \mathbb{Z})) \to H_1(A; \mathbb{Z}) \cdots .$$

Thus, since A is super-perfect, $H_2(A/L; \mathbb{Z}) \cong H_0(A/L; H_1(L; \mathbb{Z}))$.

Similarly, the five term exact sequence for P/L gives the exactness of

$$\cdots H_2(P/L; \mathbb{Z}) \to H_0(P/L; H_1(L; \mathbb{Z})) \to H_1(P; \mathbb{Z}) \to H_1(P/L; \mathbb{Z}) \to 0.$$

Thus, since $B \cong P/L$ is super-perfect, $H_1(P; \mathbb{Z}) \cong H_0(P/L; H_1(L; \mathbb{Z}))$. □

A discrete group G is said to be *acyclic* if $H_i(G; \mathbb{Z}) = 0$ for all $i \geq 1$. It follows from the Mayer-Vietoris theorem that a free product of acyclic groups is acyclic and from the Künneth formula that a direct product of acyclic groups is acyclic. We proved in Proposition 1.7(5) that Higman's group J is acyclic.

Theorem 5.6. *There exists a finitely presented acyclic group* H*, with no non-trivial finite quotients, an integer m, and a recursive sequence of m-element subsets $\theta_n \subset \mathrm{H} \times \mathrm{H}$, given as words in the generators of* $\mathrm{H} \times \mathrm{H}$*, with the following properties:*

1. *For all n, the subgroup Θ_n generated by θ_n is a subdirect product that contains the diagonal subgroup $\mathrm{H}^{\Delta} := \{(h, h) \mid h \in \mathrm{H}\}$.*
2. *For all n, the finite quotients of Θ_n are all abelian.*
3. *If $\Theta_n \neq \mathrm{H} \times \mathrm{H}$ then $H_1(\Theta_n; \mathbb{Z})$ is infinite and torsion free.*
4. *There is no algorithm that, with input θ_n, can determine whether or not Θ_n is equal (or isomorphic) to* $\mathrm{H} \times \mathrm{H}$.

Proof. Let $\langle Y \mid T \rangle$ be the standard presentation for Higman's group J and consider the recursive sequence of presentations (Π'_n) for Λ'_n given in definition 3.3. The presence of the relations $x_i^{-1} y_i$ in Π'_n shows that the union $\mathbb{Y}$ of the sets Y_i generates Λ'_n.

Let V_n be the set of words in the letters $\mathbb{Y}^{\pm 1}$ obtained from R_n (a subset of the relations of Π'_n) by replacing each occurrence of x_i with y_i. Note that (V_n) is a recursive sequence since (R_n) was. We make the Tietze moves on (Π'_n) that delete the x_i and the relations $x_i^{-1}y_i$, thus obtaining the presentation $\langle \mathbb{Y} \mid V_n, T_1, \dots, T_l\rangle$ for Λ'_n.

Let H be the free product of l copies $J_i = \langle Y_i \mid T_i\rangle$ of J and let $q_n : \mathrm{H} \to \Lambda'_n$ be the epimorphism implicit in the labelling of generators. The fibre product $\Theta_n := \{(h_1, h_2) \mid q_n(h_1) = q_n(h_2)\} \subset \mathrm{H} \times \mathrm{H}$ of q_n is generated by $\theta_n = \{(y, 1)(1, y) \mid y \in \mathbb{Y}\} \cup \{(v, 1) \mid v \in V_n\}$. When the elements of θ_n are expressed in the obvious manner as words in the generators $\{(y, 1),\, (1, y) \mid y \in \mathbb{Y}\}$ of $\mathrm{H} \times \mathrm{H}$, the sets (θ_n) form a recursive sequence of sets of a fixed cardinality, since (V_n) is such a sequence.

By construction, $\Theta_n = \mathrm{H} \times \mathrm{H}$ if and only if Λ'_n is trivial, and the Λ'_n were chosen so that there is no algorithm that can determine when $\Lambda'_n = 1$.

Since it is a fibre product, $\Theta_n \subset \mathrm{H} \times \mathrm{H}$ is subdirect product and contains the diagonal subgroup $\mathrm{H}^\Delta = \mathrm{H} \times \mathrm{H}$. Since $\mathrm{H}^\Delta \cong \mathrm{H}$ is a free product of copies of Higman's group, it has no non-trivial finite quotients, so any finite quotient G of Θ_n is generated by the images of the non-diagonal generators $(v, 1)$. Moreover, these are forced to commute in G, because given $(v_1, 1)$ and $(v_2, 1)$ we have $(v_i, 1)(1, v_i) = 1$ in G and $(v_i, 1)$ commutes with $(1, v_j^{-1})$ in Θ_n. Thus G is abelian.

It only remains to prove that $H_1(\Theta_n; \mathbb{Z})$ is infinite and torsion free if $\Lambda'_n \neq 1$. But this follows immediately from Lemmas 5.5 and 1.8 because Λ'_n has an aspherical presentation with more relations than generators, namely Π'_n. $\square$

6. The proof of Theorem C

We maintain the notation of the preceding proof. We fix a finite presenation $\mathrm{H} = \langle \mathbb{Y} \mid \mathbb{T}\rangle$, where $\mathbb{Y}$ is the disjoint union of the Y_i, as above. By applying the algorithm of Theorem 1.2 to this presentation we obtain a short exact sequence $1 \to N \to \Gamma \xrightarrow{p} \mathrm{H} \to 1$ and a presentation for Γ with generators $\mathbb{Y} \cup \{a_1, a_2, a_3\}$, where $\{a_1, a_2, a_3\}$ generates N.

As generators for $\Gamma \times \Gamma$ we take two disjoint copies of this generating set, writing $(u, 1)$ for words in the first and $(1, u)$ for words in the second.

Theorem 1.1 assures us that the fibre product $P \subset \mathrm{H}\times\mathrm{H}$ is finitely presented and that $\hat{P} \to \hat{\mathrm{H}} \times \hat{\mathrm{H}}$ is an isomorphism.

Let $\pi : \Gamma \times \Gamma \to \mathrm{H} \times \mathrm{H}$ denote the map induced by p. By definition, $P = \pi^{-1}(\mathrm{H}^\Delta)$ where H^Δ is the diagonal subgroup. Let $K_n = \pi^{-1}(\Theta_n)$. Note that $P \subset K_n$, by Theorem 5.6(1), and that K_n is generated by $\tilde{\theta}_n := \theta_n \cup \mathcal{A}$, where $\mathcal{A} = \{(a_i, 1),\, (1, a_i) \mid i = 1, 2, 3\}$. Since (θ_n) is a recursive sequence, so is $(\tilde{\theta}_n)$.

If $\Theta_n = \mathrm{H} \times \mathrm{H}_n$ then $K_n = \Gamma \times \Gamma$. If $\Theta_n \neq 1$ then Theorem 5.6(3) tells us that that there is a map, q say, from Θ_n onto an infinite abelian group Z.

The composition $q \circ \pi$ maps K_n onto Z but $q \circ \pi(P) = 1$ because $\pi(P) \cong \mathrm{H}$ is perfect. Thus if $\Theta_n \neq 1$ we obtain infinitely many finite quotients of K_n in which the image of P is trivial; in particular $\hat{P} \to \hat{K_n}$ is not surjective. Since $\hat{P} \to \hat{\Gamma} \times \hat{\Gamma}$ is an isomorphism, it follows that $\hat{K_n} \to \hat{\Gamma} \times \hat{\Gamma}$ is not injective.

We proved in Theorem 5.6 that there is no algorithm that can determine when $\Theta_n \neq 1$, so the proof of Theorem C is complete. □

References

[1] H. Bass and A. Lubotzky, *Nonarithmetic superrigid groups: counterexamples to Platonov's conjecture*, Annals of Math. **151** (2000), 1151–1173.

[2] G. Baumslag, M.R. Bridson, C.F. Miller III, H. Short, *Fibre products, non-positive curvature, and decision problems*, Comm. Math. Helv. **75** (2000), 457–477.

[3] G. Baumslag, *Residual nilpotence and relations in free groups*, J. Algebra **2** (1965), 271–282.

[4] M.R. Bridson, *Controlled embeddings into groups that have no non-trivial finite quotients*, Geom. Topol. Monogr. **1** (1998), 99–116.

[5] M.R. Bridson, *Direct factors of profinite completions and decidability*, J. Group Theory, to appear.

[6] M.R. Bridson, *The Schur multiplier, profinite completions and decidability*, preprint, University of Oxford, April 2008.

[7] M.R. Bridson and J. Howie, *Conjugacy of finite subsets in hyperbolic groups*, Internat. J. Algebra Comput. **15** (2005), 725–756.

[8] M.R. Bridson, J. Howie, C.F. Miller III and H. Short, *Subgroups of direct products of limit groups*, Annals of Math., to appear. arXiv:0704.3935

[9] M.R. Bridson and F.J. Grunewald, *Grothendieck's problems concerning profinite completions and representations of groups*, Annals of Math. **160** (2004), 359–373.

[10] M.R. Bridson and C.F. Miller III, *Structure and finiteness properties of subdirect products of groups*, Proc. London Math. Soc., to appear. arXiv:0708.4331.

[11] M.R. Bridson and H. Wilton, *Subgroup separability in residually free groups*, Math. Z., Math. Z. **260** (2008), 25–30.

[12] M. Burger and S. Mozes, *Lattices in product of trees*, Inst. Hautes Études Sci. Publ. Math. **92** (2000), 151–194.

[13] D. J. Collins and C. F. Miller III, *The word problem in groups of cohomological dimension 2*, in "Groups St. Andrews in Bath", LMS Lecture Notes 270 (1998), (eds. Campbell, Robertson, Smith), pp. 211–218.

[14] S.C. Chagas and P.A. Zalesskii, *Finite Index Subgroups of Conjugacy Separable Groups*, preprint, February 2008.

[15] D.B.A. Epstein and D.F. Holt, *The linearity of the conjugacy problem in word-hyperbolic groups*, Internat. J. Algebra Comput **16** (2006), 287–305.

[16] R. Geoghegan, "Topological Methods in Group Theory", Graduate Texts in Mathematics **243**, Springer Verlag, New York, 2007.

[17] M. Gromov, *Hyperbolic groups*, in 'Essays in group theory' (S.M. Gersten, ed Math. Sci. Res. Inst. Publ., 8, Springer, New York, 1987, pp. 75-263.

[18] A. Grothendieck, *Représentations linéaires et compactification profinie des groupes discrets*, Manuscripta Math. **2** (1970), 375–396.

[19] F.J. Grunewald, *On some groups which cannot be finitely presented*, J. London Math Soc. **17** (1978), 427–436.

[20] G. Higman, *A finitely generated infinite simple group*, J. London Math Soc. **26** (1951), 61–64.

[21] C.F. Miller III, "On group-theoretic decision problems and their classification", Annals of Mathematics Studies, No. 68, Princeton University Press (1971).

[22] J. Milnor, *'Introduction to Algebraic K-Theory'*, Ann. Math. Studies 72, Princeton University Press, Princeton 1971.

[23] V. Platonov and O.I. Tavgen, *Grothendieck's problem on profinite completions of groups*, Soviet Math. Doklady **33** (1986), 822-825.

[24] L.Pyber, *Groups of intermediate subgroup growth and a problem of Grothendieck*, Duke Math. J. **121** (2004), 169–188.

[25] E. Rips, *Subgroups of small cancellation groups*, Bull. London Math Soc., **14** (1982), 45-47.

[26] D. Wise, *A residually finite version of Rips's construction*, Bull. London Math. Soc. 35 (2003), 23-29.

Mathematical Institute, 24-29 St Giles', Oxford OX1 3LB, UK
E-mail address: bridson@maths.ox.ac.uk