Mathematische Annalen (2026) 395:52
https://doi.org/10.1007/s00208-026-03475-9

**Mathematische Annalen**

# On the conjugacy problem for subdirect products of hyperbolic groups

**Martin R. Bridson**[1]

Received: 14 May 2025 / Revised: 10 April 2026 / Accepted: 11 April 2026



## Abstract

If $G_1$ and $G_2$ are torsion-free hyperbolic groups and $P < G_1 \times G_2$ is a finitely generated subdirect product, then the conjugacy problem in $P$ is solvable if and only if there is a uniform algorithm to decide membership of the cyclic subgroups in the finitely presented group $G_1/(P \cap G_1)$. The proof of this result relies on a new technique for perturbing elements in a hyperbolic group to ensure that they are not proper powers.


**Mathematics Subject Classification** 20F67 · 20F10 · 20F65

## 1 Introduction

A subgroup $P < G_1 \times \cdots \times G_m$ is a *subdirect product* if its projection to each factor $G_i$ is onto. In this article we will be concerned with the conjugacy problem for subdirect products of torsion-free hyperbolic groups. In this setting, Bridson, Howie, Miller and Short [5] proved that if $P$ projects to a subgroup of finite index in each pair of factors $G_i \times G_j$, then $P$ is finitely presented and its conjugacy problem is solvable. If $P$ does not virtually surject to each $G_i \times G_j$, then the situation is much wilder.

In the case $m = 2$, there is a correspondence between subdirect products and *fibre products*: if $P < G_1 \times G_2$ is subdirect then there is an isomorphism $G_1/(P \cap G_1) \cong G_2/(P \cap G_2)$ and $P$ is the fibre product of the maps $p_i : G_i \twoheadrightarrow G_i/(P \cap G_i)$; see [6], where it is proved that $P$ is finitely generated if and only if $Q := G_1/(P \cap G_1)$ is finitely presented.

The case where $G_1 \cong G_2 \cong F$ is a free group was studied by Mihailova [11] and Miller [12]. They proved that if $p_1 = p_2$ and $Q$ has an unsolvable word problem, then neither the membership problem nor the conjugacy problem for $P$ can be solved algorithmically. These fibre products $P < F \times F$ are not finitely presented, and for finitely presented subdirect products of free groups (with any number of factors), the

✉ Martin R. Bridson
bridson@maths.ox.ac.uk

1 Mathematical Institute, University of Oxford, Andrew Wiles Building, Woodstock Road, Oxford OX2 6GG, UK

conjugacy and membership problems can always be solved [6]. But finite presentation does not save us in the hyperbolic setting: Baumslag, Bridson, Miller and Short [1] constructed torsion-free hyperbolic groups $G$ and finitely presented fibre products $P < G \times G$ for which both the membership and conjugacy problems are unsolvable.

Our purpose here is to strengthen these results by establishing criteria for solvability that are both necessary and sufficient. It is not difficult to show that the membership problem for a finitely generated subdirect product of hyperbolic groups $P < G_1 \times G_2$ is solvable if and only if the word problem in $Q = G_1/(G_1 \cap P)$ is solvable or, equivalently, the Dehn function of $Q$ is recursive (see Theorem D in [3] for a quantified version of this). In search of a similar characterisation for the solvability of the conjugacy problem in $P$, we are forced to examine the membership problem for cyclic subgroups in $Q$.

It is traditional to call the uniform membership problem for cyclic subgoups the power problem. Thus a finitely generated group $Q$ has a *solvable power problem* if there is an algorithm that, given two words $u, v$ in the generators, will decide whether or not $u$ lies in the subgroup of $Q$ generated by $v$. When one moves from consideration of the word problem to consideration of the power problem, the appropriate analogue of the Dehn function is the *rel-cyclics Dehn function*, which we introduce in Sect. 2.

**Theorem A** *Let $G_1$ and $G_2$ be torsion-free hyperbolic groups, let $P < G_1 \times G_2$ be a finitely generated subdirect product, and let $Q$ be the finitely presented group $G_1/(G_1 \cap P)$. Then, the following conditions are equivalent:*

(1) *the conjugacy problem in $P$ is solvable;*
(2) *the power problem in $Q$ is solvable;*
(3) *the rel-cyclics Dehn function $\delta^c_Q(n)$ is recursive.*

It is important to note that although the power problem covers membership of both finite and infinite cyclic subgroups, a solution to the power problem does not allow one to determine which elements of the group have finite order. Indeed, Collins [7] proved that the order problem, i.e. the problem of deciding the orders of elements, can be arbitrarily harder. This points to a subtle necessity in the definition of the rel-cyclics Dehn function: it has to control the distortion of cyclic subgroups without determining whether those subgroups are infinite. Collins also proved that the power problem can be arbitrarily harder than the word problem (which is the membership problem for the trivial cyclic subgroup $\{1\}$). In the light of these results, the following corollary is a straightforward consequence of Theorem A.

**Corollary B** *There exist torsion-free hyperbolic groups $G$ and finitely generated subdirect products $P < G \times G$ such that the membership problem for $P$ is solvable but the conjugacy problem for $P$ is not.*

*There also exist examples where the membership and conjugacy problems for $P$ are solvable but there is no algorithm to decide which elements of $G \times G$ have a non-zero power that lies in $P$.*

When trying to understand conjugacy problems, one is inevitably drawn into studying centralisers, because if $\gamma$ conjugates $u$ to $v$ in a group $G$, then the set of all solutions to the equation $x^{-1}ux = v$ is the coset $C_G(u)\gamma$. In torsion-free hyperbolic groups, centralisers of non-trivial elements are cyclic. In our proof of Theorem A, certain arguments only work smoothly when the element of $G$ under consideration generates its own centraliser. The following proposition will be useful in this regard (and I imagine it may be of similar use in other settings). A related (non-algorithmic) result is contained in Minasyan's work on conjugacy separability for subdirect products of hyperbolic groups [13]. We will deduce Proposition C from a more geometric result, Proposition D, which in turn is motivated by the Lyndon–Schützenburger Theorem [10], which states that in a non-abelian free group, if $a, b, c$ do not pairwise commute, then $a^p b^q c^r \neq 1$ for all powers $p, q, r \geq 2$.

**Proposition C** *Given a torsion-free hyperbolic group $G = \langle X \mid R \rangle$, a group $Q$ with a solvable word problem, and a non-injective epimorphism $p : G \twoheadrightarrow Q$, there is a finite set $\mathcal{E} \subset F(X)$ and an algorithm that, given a word $w \in F(X)$, will output a word $w' \in F(X)$ with $p(w) = p(w')$ in $Q$ such that $w' \in \mathcal{E}$ or else the centraliser $C_G(w')$ is $\langle w' \rangle$.*

Throughout this article, it will be helpful to take the formal viewpoint that a choice of generators $X$ for a group $G$ is an epimorphism $F(X) \twoheadrightarrow G$ from the free group on $X$. To prevent a clutter of notation, we avoid giving this epimorphism a name: instead, we use the phrase "in $G$" when there is a need to specify that words in the generators are being considered as products of the generators in $G$ rather than elements of $F(X)$. Similarly, we write "$u = v$ in $G$" if $uv^{-1} \in \ker(F(X) \twoheadrightarrow G)$, and we write $C_G(w)$ to denote the centraliser in $G$ of the image of $w \in F(X)$. An advantage of this convention is that, given an epimorphism $p : G \twoheadrightarrow Q$, one can regard $X$ as a generating set for $Q$ by composing $F(X) \twoheadrightarrow G$ with $p : G \twoheadrightarrow Q$. From a geometric viewpoint, this is useful because it allows us to extend $p : G \twoheadrightarrow Q$ to a label-preserving local isometry of Cayley graphs $\mathrm{Cay}(G, X) \twoheadrightarrow \mathrm{Cay}(Q, X)$. In the associated word metrics, $d_Q(p(h), p(g)) \leq d_G(h, g)$ for all $h, g \in G$.

The elements $h \in G$ in the following proposition are those that are represented by words $w \in F(X)$ that are geodesics in $\mathrm{Cay}(Q_a, X)$.

**Proposition D** (Power-Avoiding Lemma) *Let $G$ be a hyperbolic group with finite generating set $X$ and consider $X$ as a generating set for each of the quotients $Q_a := G/\langle\langle a \rangle\rangle$. Then, for each element of infinite order $a \in G$, there exist constants $K, N$ with the following property: if $d_G(1, h) = d_{Q_a}(\langle\langle a \rangle\rangle, h\langle\langle a \rangle\rangle) > N$, then $ha^K \in G$ is not a proper power.*

The lengthy proof of Proposition D is presented in Sect. 4. I hope that this result may be of independent interest, but the reader who is willing to take Propositions C and D on faith can move directly from the preliminaries in Sects. 2 and 3 to the proof of Theorem A in Sect. 5.

## 2 The rel-cyclics Dehn function

Let $\mathcal{P} \equiv \langle X \mid R \rangle$ be a finite presentation of a group $Q$. By definition, a word $w$ in the free group $F(X)$ represents the identity in $Q$ if and only if there is an equality in $F(X)$

$$w = \prod_{i=1}^{M} \theta_i^{-1} r_i \theta_i \tag{2.1}$$

with $r_i \in R \cup R^{-1}$ and $\theta_i \in F(X)$. The number $M$ of factors in the product on the righthand side is defined to be the *area* of the product. This terminology is motivated by the correspondence with diagrams that comes from van Kampen's Lemma [2].

One defines $\text{Area}(w)$ to be the least area among all products of this form for $w$. The *Dehn function* of $\mathcal{P}$ is the function $\delta : \mathbb{N} \to \mathbb{N}$ defined by

$$\delta(n) = \max\{\text{Area}(w) \mid w =_Q 1 \text{ and } |w| \leq n\}.$$

Up to the standard coarse bi-Lipschitz equivalence relation $\simeq$ of geometric group theory, this function is independent of the chosen presentation and it is common to abuse notation by adding a subscript, viz. $\delta_Q(n)$.

The *noise* of the product on the right of (2.1) is defined to be $\sum_{i=0}^{M} |\theta_i \theta_{i+1}^{-1}|$, with the convention that $\theta_0$ and $\theta_{M+1}$ are the empty word. An analysis of the standard proof of van Kampen's Lemma yields the *Bounded Noise Lemma*, an observation (and terminology) that is due to the authors of [1]; see [8], p.18 for an explicit proof.

**Lemma 2.1** (Bounded Noise Lemma) *If* $\text{Area}(w) = M$*, then there is a product of the form* (2.1) *with area* $M$ *and noise at most* $ML + |w|$*, where* $L$ *is the length of the longest relator in* $R$*.*

***Remark 2.2*** With the Bounded Noise Lemma in hand, it is clear that the word problem is solvable in $Q$ if and only if $\delta_Q(n)$ is a recursive function: on the one hand, knowing that $w = 1$ in $Q$, one can naively search for equalities of the form (2.1) until one is found, giving a bound on $\text{Area}(w)$ that can be sharpened to an exact value by checking the finitely many products with fewer factors that satisfy the Bounded Noise Lemma – thus $\delta_Q(n)$ can be computed; conversely, given a word $w$ of length $n$, if $\delta_Q(n)$ can be computed, then one can determine whether $w = 1$ in $Q$ by testing the validity of (2.1) for each product with $M \leq \delta_Q(n)$ that satisfies the Bounded Noise Lemma, and there are only finitely many such equalities that need to be tested.

We shall employ a similar argument to see that the recursiveness of the following function is equivalent to the solvability of the power problem in $Q$.

**Definition 2.3** The *rel-cyclics* Dehn function of a finitely presented group $Q = \langle X \mid R \rangle$ is

$$\delta^c(n) := \max_{w,u}\{\text{Area}(w\, u^{-p}) + |pn| \colon |w| + |u| \leq n,\ w =_Q u^p,\ |p| \leq o(u)/2\},$$

where $o(u) \in \mathbb{N} \cup \{\infty\}$ is the order of $u$ in $\Gamma$.

***Remarks 2.4*** (1) The condition $|p| \leq o(u)/2$ is equivalent to requiring that $|p|$ is the least non-negative integer such that $w = u^{\pm p}$ in $Q$.

(2) We allow $p = 0$, so $\delta(n) \leq \delta^c(n)$.

(3) The standard proof that the Dehn function of a finitely presented group is independent of the presentation, up to $\simeq$ equivalence, shows that $\delta^c(n)$ is as well.

With this understanding, we write $\delta^c_Q(n)$ when we want to emphasize which group we are considering.

(3) If we replaced the condition $|p| \leq o(u)/2$ with $|p| \leq o(u)$ then the resulting variant of $\delta^c(n)$ would control the orders of $u \in Q$ with $|u| \leq n$; in particular the order problem in $Q$ would be solvable when this function was recursive. The work of Collins [7] and Corollary B tell us that we must avoid this in the context of Theorem A.

The following proposition establishes the equivalence of the second and third conditions in Theorem A.

**Proposition 2.5** *The power problem in a finitely presented group $Q$ is solvable if and only if the rel-cyclics Dehn function $\delta^c_Q(n)$ is recursive.*

***Proof*** First we assume that the power problem in $Q$ is solvable. For each pair of words $u, v$ of length at most $n$ in the generators of $Q$, we use the solution to the power problem to decide if $v$ lies in the cyclic subgroup of $Q$ generated by $u$. If it does not, we discard this pair. If it does, then we use the solution to the word problem in $Q$ (i.e. the membership problem for the cyclic group $\{1\}$) to test the words $vu^i$, with $|i|$ increasing, until we identify the least non-negative integer $|p|$ such that $v = u^p$ or $v = u^{-p}$ in $Q$; replacing $p$ by $-p$ if necessary, we may assume $v = u^p$. Note that if $u$ has finite order then the minimality of $|p|$ implies $|p| \leq o(u)/2$. With $p$ in hand, we can calculate $\mathrm{Area}_Q(vu^{-p})$ by searching for equalities of the form (2.1) with $w = vu^{-p}$, restricting our attention to those that satisfy the Bounded Noise Lemma (Lemma 2.1): first, a naive search will identify one valid equality, giving an upper bound $M$ on $\mathrm{Area}_Q(vu^{-p})$, and the exact value of $\mathrm{Area}_Q(vu^{-p})$ can then be calculated by checking the validity of (2.1) for the finitely many products with at most $M$ factors that satisfy the Bounded Noise Lemma. Having calculated $\mathrm{Area}_Q(vu^{-p})$ for each pair $u, v$ and $|p|$ minimal, we obtain $\delta^c_Q(n)$. Thus $\delta^c_Q(n)$ is a recursive function.

Conversely, if the rel-cyclics Dehn function is recursive, then, given words $u, v$, we take an integer $n$ that is greater than the length of each and compute $\delta^c_Q(n)$. If $v = u^p$ for some $p \in \mathbb{Z}$, then for the minimal $|p|$ we have $|p|n \leq \delta^c_Q(n)$. Moreover, when $|p|$ is minimal, $\mathrm{Area}(vu^{-p}) \leq \delta^c_Q(n)$. Thus, in order to determine whether $v \in \langle u \rangle$, we only need to check for each $p$ with $|p| \leq \delta^c_Q(n)$ whether there is a valid free quality as in (2.1), with $w = vu^{-p}$, running over only products with $M \leq \delta^c_Q(n)$ factors that satisfy the conclusion of the Bounded Noise Lemma. This is a finite check. □

## 3 Some basic hyperbolic facts

The reader is assumed to be familiar with the rudiments of Gromov's theory of hyperbolic groups [9], but it is nevertheless useful to gather the following basic facts and settle on names for various constants. These are mostly standard facts from [4], pp. 402–406, with the exception of Lemma 3.1(3). As is standard, we say that $G$ is $\delta$-hyperbolic if each side of every geodesic triangle in the Cayley graph $\mathrm{Cay}(G, X)$ is contained in the $\delta$-neighbourhood of the union of the other two sides.

**Lemma 3.1** *For any $\delta$-hyperbolic group $G$ with finite generating set $X$, and for all $\lambda \geq 1$, $\varepsilon \geq 0$, there are positive constants $E, C$ and $\mu$ such that the following statements hold.*

(1) *The Hausdorff distance between any $(\lambda, \varepsilon)$-quasigeodesic in $\mathrm{Cay}(G, X)$ and any geodesic with the same endpoints is at most $E$.*
(2) *Every quadrilateral in $\mathrm{Cay}(G, X)$ with $(\lambda, \varepsilon)$-quasigeodesic sides is $C$-slim, meaning that each side is contained in the $C$-neighbourhood of the union of the other 3 sides.*
(3) *For every $g \in G$ of infinite order, $d(1, g^i) \leq \mu\, d(1, g^p)$ for all integers $0 < i < p$.*

***Proof*** (1) is the standard Morse Lemma for hyperbolic spaces, [4], p. 401. Item (2) follows easily from (1) and the slimness of triangles (after introducing a diagonal). Assertion (3) is proved in [3, Proposition 4.7]. □

**Lemma 3.2** *For any $\delta$-hyperbolic group $G$ with finite generating set $X$, there exist positive constants $\varepsilon_0$ and $\lambda_0 \geq 1$ such that the following statements hold.*

(1) *For each conjugacy class of infinite-order elements in G, if $w \in F(X)$ is a word of minimal length among all representatives of this class, then the lines in $\mathrm{Cay}(G, X)$ labelled $w^*$ are $(\lambda_0, \varepsilon_0)$-quasigeodesics;*
(2) *moreover, if $|w| > 12\delta$ then $d(1, w^p) \geq \frac{p}{2}|w| - 2\delta$ for all $p \geq 0$.*

***Proof*** If $|w| > 8\delta$, then according to Theorem III.H.1.13 of [4], the lines labelled $w^*$ are $(\lambda_0, \varepsilon_0)$-quasigeodesics where the constants $\lambda_0, \varepsilon_0$ depend only on $\delta$. There are only finitely many $w$ to consider with $|w| \leq 8\delta$, so increasing the constants $\lambda_0, \varepsilon_0$ if necessary, we may assume that the lines for these are also $(\lambda_0, \varepsilon_0)$-quasigeodesics. Item (2) is a special case of [4, Theorem III.H.1.13(3)]. □

**Lemma 3.3** *If G is torsion-free and hyperbolic, then there is an algorithm that, given a word $w$ in the generators, will decide if $w$ is non-trivial in G and, if it is, will produce a word $w_0$ such that $C_G(w) = \langle w_0 \rangle$.*

***Proof*** The word problem in $G$ is solvable, so we can determine whether $w \neq 1$. If $w \neq 1$, then $C_G(w)$ is cyclic. Lemma 3.1(3) tells us that $C_G(w)$ is generated by $g \in G$ with $d(1, g) \leq \mu|w|$. For each word $v$ of length at most $\mu|w|$, we use the solution to the word problem to decide if $[v, w] = 1$ in $G$. If $[v, w] = 1$ and $v \neq 1$ in $G$, then, searching in parallel, we use the solution to the word problem to either find coprime integers $q \geq 1$ and $q' \geq 2$ such that $v^q = w^{\pm q'}$, in which case we discard $v$, or else find an integer $p \geq 1$ such that $w = v^{\pm p}$. The largest $p$ that is found identifies the corresponding $v$ as $w_0$. □

### 3.1 Thin triangles and tripod comparison

In the proof of Proposition D, the most convenient definition of hyperbolicity to work with is the one phrased in terms of *$\eta$-thin triangles*. We recall this definition here and refer the reader to [4] pp. 409–411 for details of how it is equivalent to other hyperbolicity conditions. This formulation is particularly useful when one wants to

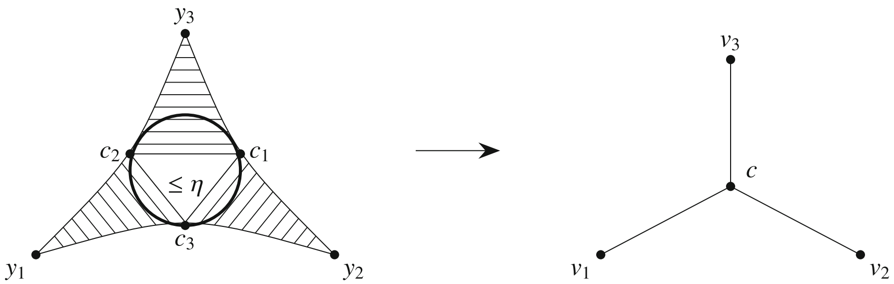



**Fig. 1** Thin triangles

make arguments with several juxtaposed triangles or polygons, following small fibres (point inverses of the maps $f_\Delta$ defined below) around the diagram.

By definition, a triple of positive numbers $l_1, l_2, l_3$ satisfies the triangle inequality if $l_i + j_j \leq l_k$ for all permutations $i, j, k$ of 1, 2, 3. Associated to each such triple there is a unique tripod $T(l_1, l_2, l_3)$ – that is, a metric graph with four vertices $c, v_1, v_2, v_3$ such that $d(v_i, v_{i+1}) = d(c, v_i) + d(c, v_{i+1}) = l_i$, with indices mod 3; there is a permitted degeneracy $c = v_i$ when $l_{i-1} + l_i = l_{i+1}$.

Given a triangle $\Delta = \Delta(y_1, y_2, y_3)$ in any geodesic space $Y$, with $l_i = d(y_i, y_{i+1})$ (indices mod 3) there is a canonical map $f_\Delta : \Delta \to T(l_1, l_2, l_3)$. One says that $X$ has *$\eta$-thin triangles* if $\text{diam}(f_\Delta^{-1}(t)) \leq \eta$ for all $\Delta$ and all $t \in T(l_1, l_2, l_3)$; see Fig. 1. The preimage of the central vertex $c \in T(l_1, l_2, l_3)$ is the discrete analogue of the *inscribed circle* of $\Delta$.

**Lemma 3.4** *A group $G$ with finite generating set $X$ is hyperbolic if and only if there is a constant $\eta > 0$ such that all triangles in the Cayley graph* $\text{Cay}(G, X)$ *are $\eta$-thin.*

## 4 Avoiding proper powers

In this section we prove Proposition D and deduce Proposition C. The proof of Proposition D is surprisingly long and challenging. I regret that I have been unable to find a more elementary proof of Proposition C.

**Proposition D** (Power-Avoiding Lemma) *Let $G$ be a hyperbolic group with finite generating set $X$ and consider $X$ as a generating set for each of the quotients $Q_a := G/\langle\langle a\rangle\rangle$. Then, for each element of infinite order $a \in G$, there exist constants $K, N$ with the following property: if $d_G(1, h) = d_{Q_a}(\langle\langle a\rangle\rangle, h\langle\langle a\rangle\rangle) > N$, then $ha^K \in G$ is not a proper power.*

### 4.1 Set-up and strategy

We assume that $G$ is $\delta$-hyperbolic with respect to a fixed finite generating set $X$ and that geodesic triangles in $\text{Cay}(G, X)$ are $\eta$-thin in the sense of Sect. 3.1. For each $g \in G$ we select a geodesic $\sigma_g \in F(X)$ representing it. To avoid a clutter of notation, we write $d$ instead of $d_G$.

We assume that constants $N$ and $K$ have been chosen with $N \gg k \gg 0$, where $k = d(1, a^K)$. The values of $N$ and $k$ will be specified more precisely at the end of the proof; they will be chosen so that $k$ and $N - k$ dwarf various combinations of the other constants that arise in the proof. Suppose

$$d(1, h) > N \gg k = d(1, a^K).$$

Consider the Cayley graph $\mathfrak{Q}_a := \mathrm{Cay}(G/\langle\langle a \rangle\rangle, X)$. The quotient map $\mathrm{Cay}(G, X) \to \mathfrak{Q}_a$ preserves the lengths of paths and hence does not increase distances. If two paths in $\mathfrak{Q}_a$ are labelled by the same word $w$ in the generators, then these two paths have the same length in $\mathfrak{Q}_a$ and the same diameter, which we denote by

$$\mathrm{diam}_{\mathfrak{Q}}(w).$$

We also write

$$\mathrm{diam}_{\mathfrak{Q}}(S)$$

for the diameter in $\mathfrak{Q}_a$ of subsets $S \subset \mathrm{Cay}(G, X)$.

The constant $\xi := \mathrm{diam}_{\mathfrak{Q}}(\sigma_a)$ will play a role in the proof, as will the constants $E$ and $\mu$ from Lemma 3.1 and the constant $C_0$ obtained by appealing to Lemma 3.1 with the constants $\lambda_0, \varepsilon_0$ from Lemma 3.2 in place of $\lambda, \varepsilon$.

We want to derive a contradiction from the assumption that there exists $g \in G$ with $g^p = ha^K$ and $p \geq 2$. The proof will divide into various cases, each giving rise to a different geometric configuration. In each case the strategy for obtaining a contradiction is the same: we want to identify two long arcs that are close in $\mathrm{Cay}(G, X)$ but are such that the image of one has small diameter in $\mathfrak{Q}_a$ while the image of the other is large.

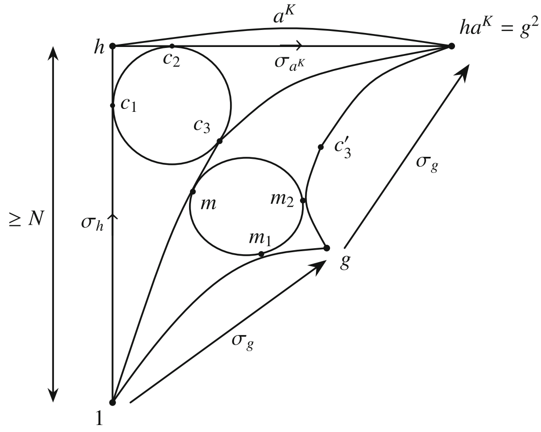
The case where $p$ is odd is more complicated than the case where $p$ is even. We begin with the even case, which immediately reduces to the case $p = 2$.

### 4.2 Excluding the possibility that $g^2 = ha^K$

In order to analyse this possibility, we consider the configuration in Fig. 2. This portrays two geodesic triangles in the Cayley graph of $G$ with their inscribed circles drawn; these triangles are $\Delta(1, h, ha^K)$ and $\Delta(1, g, g^2)$. The vertices are labelled by group elements. The top arc marked $a^K$ connects $h$ to $ha^K$ and is not assumed to be a geodesic, rather it is the path in $\mathrm{Cay}(G, X)$ beginning at $h$ that is labelled $\sigma_a^K$; we write $a^K$ rather than $\sigma_a^K$ to limit the explosion of notation. For some $\lambda \geq 1$ and $\varepsilon \geq 0$, this arc is a $(\lambda, \varepsilon)$-quasigeodesic, so it is a Hausdorff distance at most $E$ from the geodesic $[h, ha^K]$ that is drawn horizontally, where $E$ is the constant of Lemma 3.1(1). Increasing $E$ by $|\sigma_a|/2$ if necessary, we can assume that every point of $[h, ha^K]$ is within a distance $E$ of a vertex $ha^i$ on the top arc.

The side $[1, h] \subset \Delta(1, h, a^K)$ is labelled by the geodesic word $\sigma_h$ and the sides $[1, g]$ and $[g, g^2]$ of $\Delta(1, g, g^2)$ are both labelled by the geodesic word $\sigma_g$, while $[1, g^2] = [1, ha^K]$ is labelled by the geodesic word $\sigma_{g^2}$. The inscribed circle of the isosceles triangle $\Delta(1, g, g^2)$ intersects $[1, g^2]$ at the midpoint $m$.

**Fig. 2** $g^2 = ha^K$




Because $d(1, h)$ is the distance between 1 and the image of $h$ in $\mathfrak{Q}_a$, we have $d(1, h) \leq d(1, ha^i)$ for all $i \in \mathbb{Z}$. The geodesic $[h, g^2]$ is $E$-close to the set of vertices $ha^i$, so the path $[1, c_1, c_2]$ has length at least $d(1, h) - E$ and

$$d(h, c_2) = d(h, c_1) \leq d(c_1, c_2) + E \leq \eta + E. \tag{4.1}$$

From this we obtain a lower bound on $d(c_3, g^2)$,

$$d(c_3, g^2) = d(c_2, g^2) = d(h, g^2) - d(h, c_2) \geq k - (\eta + E). \tag{4.2}$$

For the midpoint $m$ we have, from the triangle inequality,

$$d(m, g^2) = \frac{1}{2}d(1, g^2) \geq \frac{1}{2}(d(1, h) - d(h, g^2)) \geq \frac{1}{2}(N - k) \gg k. \tag{4.3}$$

Comparing this with $d(c_3, g^2) = d(c_2, g^2) = d(h, g^2) - d(h, c_2) \leq k$, we see that $m$ lies between 1 and $c_3$, as drawn. It follows that the point $c_3' \in [g, g^2]$ a distance $d(c_3, g^2)$ from $g^2$ lies on the arc $[m_2, g^2]$. Let $v_\infty$ be the suffix of $\sigma_g$ that labels the arc $\tau_0 := [c_3', g^2]$. From (4.2) we have

$$|v_\infty| = |\tau_0| = d(c_3, g^2) \geq k - (\eta + E). \tag{4.4}$$

This arc $\tau_0$ lies in the $\eta$-neighbourhood of $[c_3, g^2]$, hence in the $2\eta$-neighbourhood of $[c_2, g^2]$ and in the $(2\eta + E)$-neighbourhood of the arc labelled $a^K$ at the top of the picture. The image of this last arc in $\mathfrak{Q}_a$ has diameter $\xi$, therefore

$$\operatorname{diam}_{\mathfrak{Q}}(v_\infty) \leq 2\eta + E + \xi. \tag{4.5}$$

We now focus on a neighbourhood of the vertex $g$ in Fig. 2 as well as the arc $[1, g]$ and the initial segment of $[1, h]$ that has length $d(1, g)$; see Fig. 3

*Case 1: Assume* $d(m_1, g) \geq |v_\infty|/2$

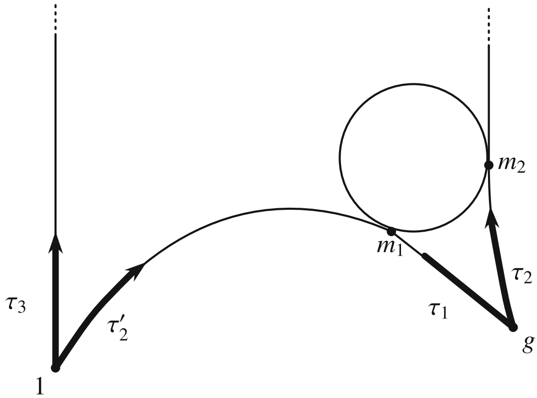



**Fig. 3** The arcs $\tau_i$

In this case, a terminal arc of $[m_1, g]$ is labelled by the suffix of $v_\infty$ that has length $|v_\infty|/2$. This arc, which is labelled $\tau_1$ in Fig. 3, is $\eta$-close to an initial arc $\tau_2 \subset [g, g^2]$ of the same length. Because $[1, g]$ and $[g, g^2]$ are both labelled by the same geodesic word $\sigma_g$, there is an initial arc of $[1, g]$ with the same label as $\tau_2$; in Fig. 3 this arc is called $\tau_2'$. As

$$|\tau_2'| = \frac{1}{2}|v_\infty| \leq \frac{1}{2}k \ll N,$$

the arc $\tau_2'$ is $2\eta$-close to an initial arc of $[1, h]$ of the same length; this arc is called $\tau_3$ in Fig. 3.

Now the desired contradiction emerges, because on the one hand, using (4.4),

$$\mathrm{diam}_{\mathfrak{Q}}(\tau_3) = |\tau_3| = |\tau_2| = |\tau_1| \geq \frac{1}{2}|v_\infty| \geq \frac{1}{2}(k - (\eta + E)), \tag{4.6}$$

while on the other hand, since $\tau_1$ is labelled by a suffix of $v_\infty$, from (4.5) we have

$$\mathrm{diam}_{\mathfrak{Q}}(\tau_1) \leq \mathrm{diam}_{\mathfrak{Q}}(v_\infty) \leq 2\eta + E + \xi. \tag{4.7}$$

Moreover, $\tau_1$ is $\eta$-close to $\tau_2$, which shares a label with $\tau_2'$, which is $2\eta$-close to $\tau_3$, so

$$\mathrm{diam}_{\mathfrak{Q}}(\tau_3) \leq \mathrm{diam}_{\mathfrak{Q}}(\tau_2') + 2\eta = \mathrm{diam}_{\mathfrak{Q}}(\tau_2) + 2\eta \leq \mathrm{diam}_{\mathfrak{Q}}(\tau_1) + 3\eta. \tag{4.8}$$

Together, (4.6), (4.7) and (4.8), imply

$$\frac{1}{2}(k - (\eta + E)) \leq 5\eta + E + \xi, \tag{4.9}$$

which is nonsense if $k$ is large.

*Case 2: Assume* $d(m_1, g) \leq |v_\infty|/2$

In this case the terminal segment of $[1, g]$ labelled $v_\infty$ begins with an arc of length at least $|v_\infty|/2$ on $[1, m_1]$. This arc is $2\eta$-close to an arc of the same length on $[1, h]$, which has diameter at least $|v_\infty|/2$ in $\mathfrak{Q}_a$, so we reach a contradiction as before.

### 4.3 Excluding the possibility that $g^p = ha^K$ with $p$ odd

In this case we will reach a contradiction by finding a long subword of $\sigma_{g^p}$ that labels two paths in $\mathrm{Cay}(G, X)$, one of which has small diameter in $\mathfrak{Q}_a$ and one of which has large diameter. The reader may find it helpful at each stage of the proof to reflect on what happens in the case where $G$ is a free group.

Given $g \in G$, we consider those words $\theta$ in the generators of $G$ that are shortest among all words representing elements in the conjugacy class of $g$; suppose $\theta = x_\theta^{-1} g x_\theta$ in $G$. Among these, we fix a particular $\theta$ so that $d(1, x_\theta)$ is minimal, and we fix a shortest word $x$ representing $x_\theta$. If $G$ were a free group, $x\theta^p x^{-1}$ would be the geodesic representative of $g^p$ for all $p > 0$, but in the general case a non-trivial argument is needed to bound $|x|$ in terms of $d(1, g^p)$.

There is a line in the Cayley graph labelled $\theta^*$ through the vertex $x_\theta$; this line is a $|\theta|$-local geodesic but might not be a geodesic. A shortest path from the vertex 1 to this line is labelled $x$. The following argument shows that $x$ is also the label on a shortest path from the vertex $g^p$ to this line for all $p > 0$.

Let $x_1$ be any word that conjugates $g^p$ to an element represented by a cyclic permutation of $\theta^p$, where $p > 0$; say $x_1^{-1} g^p x_1 = \theta_0^{-1}\theta^p\theta_0$, with $\theta_0$ a prefix of $\theta$. Then, because roots are unique in torsion-free hyperbolic groups, $x_1$ conjugates $g$ to $\theta_0^{-1}\theta\theta_0$, which being a cyclic permutation of $\theta$ has reduced length $|\theta|$. Therefore,

$$|x_1| \geq |x| = d(1, x_\theta), \tag{4.10}$$

as $|x|$ was chosen to be minimal.

We now fix $x$ (which is a geodesic word), define $g_0 \in G$ by

$$\boxed{g_0 = x^{-1} g x}$$

and work with the geodesic representative $\theta$ for $g_0$. Lemma 3.2(1) provides constants $\lambda_0, \varepsilon_0$ such that the lines in $\mathrm{Cay}(G, X)$ labelled $\theta^*$ are $(\lambda_0, \varepsilon_0)$-quasi-geodesic for all $\theta$ under consideration. We fix a constant $C_0 > 0$ such that every $(\lambda_0, \varepsilon_0)$-quasigeodesic quadrilateral in $H$ is $C_0$-slim (Lemma 3.1(2)).

Recalling our notation that $\sigma_{g^p}$ is a geodesic word for $g^p$, we consider the quadrilateral in the Cayley graph of $G$ with vertices $y_1, y_2, y_3, y_4$ and sides (read in cyclic order) labelled $x^{-1}, \sigma_{g^p}, x, \theta^{-p}$ (see Fig. 4). An important point to observe is that there is no path in the Cayley graph of length less than $|x|$ that connects either $y_2$ or $y_3$ to the fourth side (the arc labelled $\theta^p$), for if there were then the label $x_1$ on this path would contradict the minimality of $|x|$, as in the argument leading to (4.10).

*Case 1: When* $|x|$ *is significant* ($|x| \geq k/100$ *will suffice).*

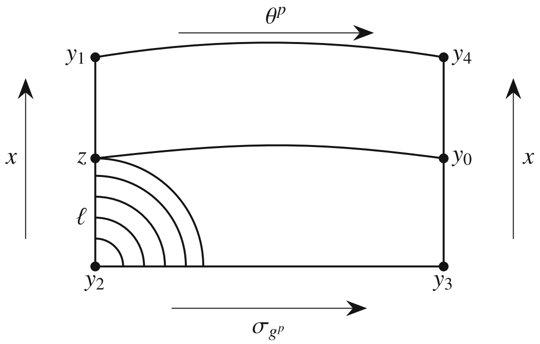



**Fig. 4** When $|x|$ is significant

The key point to prove is that if $x$ is long, then a long initial arc of $[y_2, y_1]$ is in the $C_0$-neighbourhood of $[y_2, y_3]$. To this end, consider the first vertex $z \in [y_2, y_1]$ that is not in this neighbourhood and let $\ell = d(y_2, z)$. We shall prove that

$$\ell \geq \min\left\{\frac{1}{2}d(1, g^p) - C_0,\ |x|/2\right\}. \tag{4.11}$$

If $d(y_2, z) \geq d(y_1, z)$ then we are done, so suppose $d(y_1, z) \geq |x|/2 > C_0$. This supposition precludes $z$ from being within $C_0$ of $[y_1, y_4]$, by the minimality of $|x|$, so $z$ is a distance at most $C_0$ from a point $y_0 \in [y_3, y_4]$. Note that $d(y_4, y_0) \geq |x| - \ell - C_0$, for if not then $d(y_2, y_4) \leq d(y_2, z) + d(z, y_0) + d(y_0, y_4) < |x|$, contradicting the minimality of $|x|$. It follows that $d(y_0, y_3) \leq \ell + C_0$, and measuring the path $(y_2, z, y_0, y_3)$ we conclude that

$$d(1, g^p) = |\sigma_{g^p}| = d(y_2, y_3) \leq 2(\ell + C_0),$$

which completes the proof of (4.11).

An entirely symmetric argument provides the same lower bound on the length of an initial segment of $[y_3, y_4]$ that lies in the $C_0$-neighbourhood of a terminal segment of $\sigma_{g^p}$.

In the setting that concerns us (Fig. 5), $d(1, g^p) = d(1, ha^K) \gg k$, so if $|x| \geq k/100$ then $x$ has a prefix $x'$ of length at least $k/200$ that labels two geodesic arcs in the Cayley graph, the first of which is $C_0$-close to an initial segment of $\sigma_{g^p}$ and the second of which is $C_0$-close to a terminal segment of $\sigma_{g^p}$. In Fig. 5, this puts the first arc $(C_0 + \eta)$-close to a segment of the same length on $[1, h]$ and the second arc $(C_0 + \eta)$-close to a segment of $[h, ha^K]$ and hence $(C_0 + \eta + E)$-close to a segment of the arc labelled $a^K$.

These proximities give contradictory bounds when $k$ is large:

$$\operatorname{diam}_{\mathfrak{Q}}(x') \geq |x'| - (C_0 + \eta) \geq (k/200) - (C_0 + \eta) \tag{4.12}$$

versus

$$\operatorname{diam}_{\mathfrak{Q}}(x') \leq C_0 + \eta + E + \xi.$$

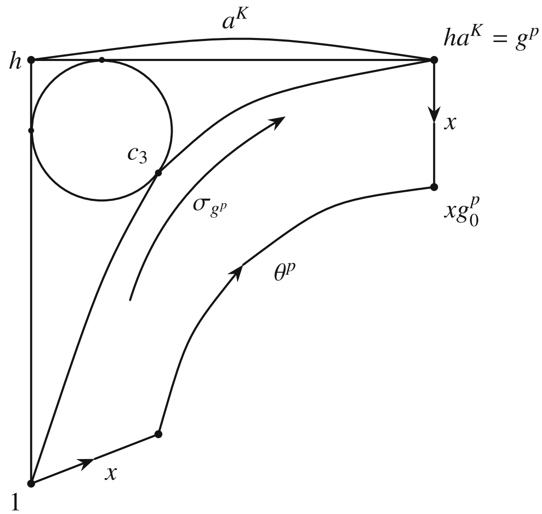



**Fig. 5** $g^p = ha^K$, general case

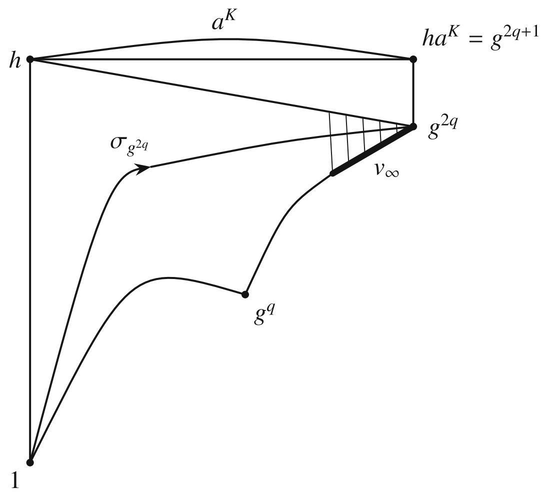



**Fig. 6** When $g$ is small

Thus we have proved that if $|x| \geq k/100$ and $k$ is large, then $g = xg_0x^{-1}$ cannot be a proper root of $ha^K$.

There are two cases left to consider: either $d(1, g)$ is small (and hence $|x|$ is small), or $d(1, g)$ is large but $|x|$ is small.

*Case 2: When $d(1, g)$ is small*

This case is portrayed in Fig. 6. We write $p = 2q + 1$, so $g^{2q+1} = ha^K$. Suppose $d(1, g) = D < k/10$, say. Consider the juxtaposition of geodesic triangles $\Delta(h, g^{2q}, ha^K)$, $\Delta(1, h, g^{2q})$ and $\Delta(1, g^q, g^{2q})$, with the latter having the sides $[1, g^q]$ and $[g^q, g^{2q}]$ both labelled $\sigma_{g^q}$.

As $D$ is significantly smaller than $k$, there is a terminal arc of length $k/2$ on $[g^q, g^{2q}]$ that is $2\eta$-close to a terminal arc of the same length on $[h, g^{2q}]$; let $v_\infty$ be the label on this arc of $[g^q, g^{2q}]$. The thinness of $\Delta(h, g^{2q}, ha^K)$ tells us that $[h, g^{2q}]$ is contained in the $(\eta + D)$-neighbourhood of $[h, ha^K]$ and hence the $(\eta + D + E)$-neighbourhood of the arc labelled $a^K$. Therefore

$$\mathrm{diam}_{\mathfrak{Q}}(v_\infty) \leq 3\eta + D + E + \xi < 3\eta + \frac{1}{10}k + E + \xi. \tag{4.13}$$

With $v_\infty$ in hand, we concentrate on $[1, h] \cup \Delta(1, g^q, g^{2q})$ and reach a contradiction by identify arcs

$$\tau_1 \subset [1, g^q],\ \tau_2 \subset [g^q, g^{2q}],\ \tau_2' \subset [1, g^q] \text{ and } \tau_3 \subset [1, h]$$

exactly as we did in Sect. 4.2 (with constants that have been changed by at most $D$).

*Case 3: When $d(1, g)$ is large but $|x|$ is small.*

We are working with the decomposition $g = x^{-1}g_0x$, where $x$ is a geodesic and $g_0$ is represented by a shortest word representing any conjugate of $g$; let $\theta$ be this word. To cover the remaining cases, it suffices to assume that $|x| \leq \iota = k/100$ and $|\theta| \geq (k/10) - 2\iota$, which we approximate by $k/20$ for convenience. In this case, we consider the juxtaposition of the geodesic triangle $\Delta(1, h, ha^K)$ (with $[1, ha^K]$ labelled $\sigma_{g^p}$) and the quadrilateral that has sides labelled $\sigma_{g^p}$, $\theta^p$ and, on the remaining two sides, $x$. From Lemmas 3.1 and 3.2, we know that this quadrilateral is $C_0$-thin. Figure 4 portrays this situation. Consider the terminal arc of length $k/50$ on the side of the quadrilateral labelled $\theta^p$. This arc (which is labelled by a suffix $\zeta$ of $\theta$, since $|\theta| \geq k/20$) is contained in the $(\iota + C_0)$-neighbourhood of a terminal arc of $[c_3, ha^K] \subset [1, ha^K]$ and hence lies in the $(\iota + C_0 + \eta + E)$-neighbourhood of the arc labelled $a^K$ joining $h$ to $ha^K$. Therefore

$$\mathrm{diam}_{\mathfrak{Q}}(\zeta) \leq \iota + C_0 + \eta + E + \xi = \frac{1}{100}k + C_0 + \eta + E + \xi. \tag{4.14}$$

Now consider the segment labelled $\theta$ at the beginning on the $\theta^p$-side of the quadrilateral, remembering that $\theta$ is a geodesic word. Let $\omega$ be the terminal part of this segment that is labelled $\zeta$ (see Fig. 7).

The thinness of the quadrilateral (Lemma 3.2), tells us that $\omega$ is $C_0$-close to a geodesic segment of length at least $|\omega| - 2C_0 \geq (k/50) - 2C_0$ on $[1, ha^K]$. If we can argue that this last segment, which we call $\beta$, is contained in $[1, c_3]$, then by the thinness of $\Delta(1, h, ha^K)$ it will be $\eta$-close to a segment $\gamma$ of the same length on $[1, h]$, and we know that $\mathrm{diam}_{\mathfrak{Q}}(\gamma) = |\gamma|$. As $\gamma$ lies in the $C_0 + \eta$ neighbourhood of the arc labelled $\zeta$, we could then conclude that

$$\mathrm{diam}_{\mathfrak{Q}}(\zeta) \geq \mathrm{diam}_{\mathfrak{Q}}(\gamma) - C_0 - \eta \geq (k/50) - 3C_0 - \eta, \tag{4.15}$$

which contradicts (4.14) if $k$ is large enough; and this contradiction will finish the proof.

Thus it only remains to prove that $\beta$ is indeed contained in $[1, c_3]$ (and hence is $\eta$-close to $[1, h]$). Since $\beta$ is $C_0$-close to $\omega$, it suffices to prove that the latter is contained

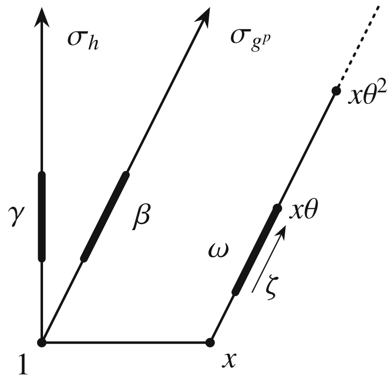



**Fig. 7** The final set of contradictory arcs

in a ball of radius less than $N - k - C_0$ about 1. And since $\omega$ lies at the end of an arc labelled $\theta$ that begins at $x$, it suffices to prove that

$$|\theta| < N - k - \iota - C_0 = N - \frac{101}{100}k - C_0. \tag{4.16}$$

We are in the case where $|\theta| \geq k/20 > 12\delta$, so from Lemma 3.2(2) we know that

$$d(1, g_0^p) \geq \frac{p}{2}|\theta| - 2\delta. \tag{4.17}$$

By the triangle inequality,

$$N + k \geq d(1, ha^K) = d(1, x^{-1}g_0^p x) \geq d(1, g_0^p) - 2|x|. \tag{4.18}$$

As $|x| \leq \iota$, we deduce

$$\frac{p}{2}|\theta| \leq N + k + 2\iota + 2\delta. \tag{4.19}$$

And since $p \geq 3$,

$$|\theta| \leq \frac{2}{3}(N + k + 2\iota + 2\delta\ ) = \frac{2}{3}\left(N + \frac{51}{50}k + 2\delta\right). \tag{4.20}$$

We choose constants $N \gg k$ to ensure that this last quantity is less than $N - k - \iota - C_0$, so the estimate (4.16) is established and the proof is complete. □

**Values of** $N$, $K$ **and** $k$**.** The reader who has successfully followed the above proof will be content that a choice of $N \gg k > 0$ can be made to ensure that all of the desired contradictions are reached. For example, $k$ has to be greater than $11\eta + 3E + 2\xi$ to ensure that (4.9) is false, it has to be greater than $200(2C_0 + 2\eta + E + \xi)$ to obtain a contradiction from (4.12), and it has to be greater than $50(4C_0 + 2\eta + E + \xi)$ in order for (4.15) to contradict (4.14). When we have settled on what a sufficiently large value of $k$ is, we choose $K$ to be the least positive integer such that $d(1, a^K) > k$ and then we increase $k$ to get $d(1, a^K) = k$. After this, $N$ has to be chosen so that the estimate in (4.20) implies the one in (4.16); it is sufficient to let $N = 3k + 3C_0 + 4\delta$. (Psychologically speaking, it can be helpful to imagine that $N/k$ is much bigger.)

### 4.4 Proof of Proposition C

**Proposition C** *Given a torsion-free hyperbolic group $G = \langle X \mid R\rangle$, a group $Q$ with a solvable word problem, and a non-injective epimorphism $p : G \twoheadrightarrow Q$, there is a finite set $\mathcal{E} \subset F(X)$ and an algorithm that, given a word $w \in F(X)$, will output a word $w' \in F(X)$ with $p(w) = p(w')$ in $Q$ such that $w' \in \mathcal{E}$ or else the centraliser $C_G(w')$ is $\langle w'\rangle$.*

***Proof*** By composing $F(X) \to G$ with $p : G \to Q$ we can regard $X$ as a finite generating set for $Q$ as well as $G$, and $p$ extends to a length-preserving map $\mathrm{Cay}(G, X) \to \mathrm{Cay}(Q, X)$. If $a \in \ker(G \to Q)$, then $\mathrm{Cay}(G, X) \to \mathrm{Cay}(Q, X)$ factors through $\mathrm{Cay}(G, X) \to \mathfrak{Q}_a$, so if $w_0 \in F(X)$ arises as the label on a geodesic path in $\mathrm{Cay}(Q, X)$, then the paths in $\mathfrak{Q}_a$ labelled $w_0$ are also geodesics.

We fix a non-trivial element $a \in \ker(G \to Q)$, choose a word $\tilde{a} \in F(X)$ representing $a$, and fix constants $N$ and $K$ satisfying the statement of Proposition D. We define $\mathcal{E} \subset F(X)$ to be the set of words labelling geodesics of length less than $N$ in $\mathrm{Cay}(Q, X)$. The algorithm that we seek proceeds as follows: given $w \in F(X)$, it first uses the solution to the word problem in $Q$ to find a word $w_0 \in F(X)$ of minimal length such that $p(w) = p(w_0)$ in $Q$. We have just observed that the paths in $\mathfrak{Q}_a$ labelled $w_0$ are geodesics, so the element $h \in G$ defined by $w_0$ satisfies the hypotheses of Proposition D unless $|w_0| < N$. If $|w_0| < N$, the algorithm stops and outputs $w' := w_0 \in \mathcal{E}$. If $|w_0| \geq N$, then $ha^K \in G$ is not a proper power and the algorithm outputs $w' := w_0\tilde{a}^K$. By construction, $p(w) = p(w')$, and $C_G(w') = \langle w'\rangle$ if $w' \notin \mathcal{E}$. □

## 5 Proof of Theorem A

We restate the theorem, for the reader's convenience.

**Theorem A** *Let $G_1$ and $G_2$ be torsion-free hyperbolic groups, let $P < G_1 \times G_2$ be a finitely generated subdirect product, and let $Q$ be the finitely presented group $G_1/(G_1 \cap P)$. Then, the following conditions are equivalent:*

(1) *the conjugacy problem in $P$ is solvable;*
(2) *the power problem in $Q$ is solvable;*
(3) *the rel-cyclics Dehn function $\delta^c_Q(n)$ is recursive.*

### 5.1 Choice of generators and notation

We fix epimorphisms $\pi_1 : G_1 \twoheadrightarrow Q$ and $\pi_2 : G_2 \twoheadrightarrow Q$ so that

$$P = \{(g_1, g_2) \mid \pi_1(g_1) = \pi_2(g_2)\} < G_1 \times G_2.$$

All of the groups that we are dealing with are finitely generated, so we are free to work with whatever generating set we choose when establishing (un)decidability. We begin by choosing a finite generating set $X_0$ for $Q$, which defines an epimorphism from the free group $\mu_0 : F(X_0) \twoheadrightarrow Q$. For $i = 1, 2$, we can factor $F(X_0) \twoheadrightarrow Q$ through $\pi_i : G_i \twoheadrightarrow Q$; let $\mu_i : F(X_0) \to G_i$ be this lift of $\mu_0$. We choose a finite set $A_i \subseteq \ker \pi_i$ that generates $\ker \pi_i$ as a normal subgroup and is such that $A_1 \cup \mu_i(X_0)$ generates $G_i$. We then define $X = X_0 \sqcup A_1 \sqcup A_2$ and for $i = 1, 2$ we extend $\mu_i$ by defining $\mu_i|_{A_i}$ to be the inclusion $A_i \hookrightarrow G_i$ while $\mu_1(A_2) = 1$ and $\mu_2(A_1) = 1$. We extend $\mu_0$ by defining $\mu_0(A_1 \sqcup A_2) = 1$. Thus we obtain compatible sets of generators $\mu_i : F(X) \twoheadrightarrow G_i$ for $G_i$ and $\mu_0 : F(X) \twoheadrightarrow Q$ for $Q$. This compatibility will aid the transparency of the proof.

We suppress mention of the maps $\mu_i$, writing expressions such as "$w = 1$ in $Q$" and "$u = v$ in $G_1$", for words $u, v, w \in F(X)$, when what we really mean is $\mu_0(w) = 1$ and $\mu_1(u) = \mu_1(v)$.

We identify $G_1$ with $G_1 \times 1 < G_1 \times G_2$ and $G_2$ with $1 \times G_2$. Correspondingly,[1] we have generators $(x, 1)$ and $(1, x)$ for $G_1 \times G_2$, with $x \in X$, but rather than working with formal words in these symbols, we work with ordered pairs of words $(u, v)$ with $u, v \in F(X)$.

Noting that $(a, 1) = (a, a)$ and $(1, b) = (b, b)$ in $G_1 \times G_2$ for each $a \in A_1 \subset X$ and $b \in A_2 \subset X$, it is easily verified that $P$ is generated by $\{(x, x) \mid x \in X\}$.

### 5.2 The Proof of Theorem A

We first prove (2) $\implies$ (1). Given elements $U = (u_1, u_2)$ and $V = (v_1, v_2)$ of $P$, we use the solution to the conjugacy problem in $G_i$ to decide if there exist words $w_1, w_2 \in F(X)$ conjugating $u_1$ to $v_1$ in $G_1$ and $u_2$ to $v_2$ in $G_2$, respectively. If there is no such pair, then $U$ is not conjugate to $V$. If such a pair does exist, then we replace $V$ by $(w_2, w_2)V(w_2, w_2)^{-1}$. Thus we may assume, without loss of generality, that $v_2 = u_2$ and that $w^{-1}u_1w = v_1$ in $G_1$ for some word $w \in F(X)$.

With this reduction, the set of elements of $G_1 \times G_2$ conjugating $U$ to $V$ is

$$I = \{(z_1^p w, z_2^q) \mid \langle z_1 \rangle = C_{G_1}(u_1),\ \langle z_2 \rangle = C_{G_2}(u_2)\}.$$

There is an algorithm to calculate the maximal roots of elements in a torsion-free hyperbolic group (Lemma 3.3), so we may assume that we have explicit words in the generators giving us $z_1$ and $z_2$ and positive integers $e_i > 0$ such that $z_i^{e_i} = u_i$.

To determine if $U$ is conjugate to $V$ in $P$, we must decide whether $I \cap P$ is non-empty. Since $(u_1, u_2)$ is in $P$, by multiplying on the left by a power of $(u_1, u_2)$, we can transform any $\zeta \in P \cap I$ into $(z_1^{p_1}w, 1)(1, \varepsilon) \in I \cap P$ with $\varepsilon = z_2^j$ for some $0 \le j < e_2$. And $(z_1^{p_1}w, 1)(1, \varepsilon) \in P$ if and only if $\varepsilon w^{-1} \in \langle z_1 \rangle$ in $Q$. Thus, to determine whether $I \cap P$ is non-empty, it suffices to check whether one of the finitely many elements $\varepsilon w^{-1}$ lies in the cyclic subgroup of $Q$ generated by $z_1$, which we can do using the solution to the power problem.

[1] Caution: with this notation, if $G_1 = G_2$ but $\pi_1 \neq \pi_2$ then $(x, x)$ is in $P$ but it might not be in the diagonal subgroup of $G \times G$.

Next we prove (1) $\Longrightarrow$ (2). Suppose that the conjugacy problem in $P$ is solvable. First we claim that this hypothesis implies that the word problem in $Q$ is solvable. To help us see this, we first want to find $g_i \in \ker(G_i \twoheadrightarrow Q)$ with $C_{G_i}(g_i) = \langle g_i \rangle$, for $i = 1, 2$. To this end, we fix a non-trivial element $b_i \in \ker(G_i \twoheadrightarrow Q)$. For sufficiently large $p > 0$, the quotient $H_i := G_i/\langle\langle b_i^p \rangle\rangle$ is hyperbolic (see [14], for example). If the kernel of the map $H_i \twoheadrightarrow Q$ induced by $G_i \twoheadrightarrow Q$ is finite, then $Q$ is hyperbolic and therefore has a solvable word problem. If $\ker(H_i \twoheadrightarrow Q)$ is infinite, then for each $N_i > 0$ we can find an element $c_i \in \ker(H_i \twoheadrightarrow Q)$ with $d_{H_i}(1, c_i) > N_i$, where $d_{H_i}$ is the word metric obtained by taking the image of $X$ as generators. We want to apply Proposition D with $a_i = b_i^p$. Let $K_i$ and $N_i$ be the constants of that proposition (with subscripts to indicate which $G_i$ we are working with), choose $c_i$ as above and, following the proof of Proposition C, take a geodesic representative $v_i \in F(X)$ of $c_i$. Then $g_i := v_i a_i^K \in G_i$ is an element of $\ker(G_i \twoheadrightarrow Q)$ that is not a proper power, therefore $C_{G_i}(g_i) = \langle g_i \rangle$.

With $g_i$ in hand, given $w \in F(X)$ we ask whether $(w^{-1}g_1w, g_2) \in P$ is conjugate to $(g_1, g_2)$ in $P$. The elements of $G_1 \times G_2$ conjugating $(g_1, g_2)$ to $(w^{-1}g_1w, g_2)$ are $J = \{(g_1^p w, g_2^q) \mid p, q \in \mathbb{Z}\}$, because $C_{G_i}(g_i) = \langle g_i \rangle$. And since $\langle g_i \rangle \subseteq \ker(G_i \twoheadrightarrow Q)$, the intersection $J \cap P$ will be non-empty if and only if $w \in \ker(G \twoheadrightarrow Q)$. Thus deciding whether $(w^{-1}g_1w, g_2)$ is conjugate to $(g_1, g_2)$ in $P$ tells us whether $w = 1$ in $Q$.

In order to prove that the power problem is solvable in $Q$, we must exhibit an algorithm that, given words $w, u \in F(X)$, will determine whether of not $w \in \langle u \rangle$ in $Q$. Using the solution to the word problem in $Q$, we first decide whether or not $[w, u] = 1$ in $Q$. If $[w, u]$ is non-trivial in $Q$, then $w \notin \langle u \rangle$. If $[w, u] = 1$, then we proceed as follows.

First we use the solution to the word problem in $Q$ to decide if $u \in Q$ is in the image of the exceptional set $\mathcal{E}$ of Proposition C. If $u$ is not in the image of $\mathcal{E}$, then use the algorithm from Proposition C to replace $(u, u) \in P$ with $(u_1, u_2) \in P$ where $u_i \in F(X)$ is such that $u = u_i$ in $Q$ and $C_{G_i}(u_i) = \langle u_i \rangle$. For any $g \in G_1$, the set of elements conjugating $(u_1, u_2)$ to $(g^{-1}u_1g, u_2)$ in $G_1 \times G_2$ is then $\{(u_1^p g, u_2^q) \mid p, q \in \mathbb{Z}\}$. Crucially, we know $(w^{-1}u_1w, u_2)$ is in $P$ because $[w, u] = 1$ in $Q$. And deciding if $(u_1, u_2)$ is conjugate to $(w^{-1}u_1w, u_2)$ in $P$ is equivalent to deciding if $(u_1^p w, u_2^q) \in P$ for some $p, q \in \mathbb{Z}$, which is equivalent to deciding if $w \in \langle u \rangle$ in $Q$. Thus, since the conjugacy problem in $P$ is solvable, we can decide whether or not $w \in \langle u \rangle$ in $Q$.

It remains to consider what happens when $u \in Q$ is in the image of the finite set $\mathcal{E} \subset F(X)$. In this case, we use the solution to the word problem in $Q$ to test which of the powers $u^2, u^3, \ldots$ are in the image of $\mathcal{E}$. We can assume that the empty word is in $\mathcal{E}$, so we are simultaneously checking if $u^p = 1$ in $Q$. Eventually, we will either determine that $u$ has finite order, $m$ say, or else we will find $p > 0$ such that $u^p \notin \mathcal{E}$. If we find $m = o(u)$, we use the solution to the word problem again to decide if $w = u^i$ in $Q$ for some $i \in \{0, \ldots, m-1\}$. If we find $u^p \notin \mathcal{E}$, then we use the algorithm of the previous paragraph to decide whether $w \in \langle u^p \rangle$ in $Q$. If $w \in \langle u^p \rangle$ then we have proved $w \in \langle u \rangle$. If $w \notin \langle u^p \rangle$, then for $i = 1, \ldots, p-1$ we apply the same algorithm with $wu^i$ in place of $w$ to decide if $wu^i \in \langle u^p \rangle$, noting that $w \in \langle u \rangle$ if and only if the answer is yes in one case.

The implications (2) ⇔ (3) were proved in Proposition 2.5, so the proof is complete. □

**Acknowledgements** I am grateful to the University of Oxford for the sabbatical leave that enabled me to finish this article, and to Stanford University for hosting me during this sabbatical. I am also grateful to Tim Riley for extensive and fruitful conversations about the complexity of conjugacy problems, to Ashot Minasyan and Denis Osin for helpful correspondence regarding analogues of the Lyndon–Schützenburger Theorem in hyperbolic groups, and to the anonymous referee for their careful reading and helpful comments. My special thanks go to Chuck Miller for the many insights that I gained from him during our long collaboration on fibre products and decision problems.

**Funding** The author was not supported by any grants during the preparation of this manuscript.

**Data availability** Data sharing is not applicable to this article, as no datasets were generated or analyzed during the current study.

## Declarations

**Conflict of interest** The author has no relevant financial or non-financial interests to disclose.



## References

1. Baumslag, G., Bridson, M.R., Miller, C.F., III., Short, H.: Fibre products, non-positive curvature, and decision problems. Comment. Math. Helv. **75**, 457–477 (2000)
2. Bridson, M.R.: The geometry of the word problem. In: Bridson, M.R., Salamon, S.M. (eds.) Invitations to Geometry and Topology, pp. 29–91. OUP, Oxford (2002)
3. Bridson, M.R.: Conjugacy in fibre products, distortion, and the geometry of cyclic subgroups. Preprint at arXiv:2507.17598
4. Bridson, M.R., Haefliger, A.: Metric Spaces of Non-positive Curvature, Grundlehren der Mathematischen Wissenschaften, vol. 319. Springer, Heidelberg (1999)
5. Bridson, M.R., Howie, J., Miller, C.F., III., Short, H.: On the finite presentation of subdirect products and the nature of residually free groups. Am. J. Math. **135**, 891–933 (2013)
6. Bridson, M.R., Miller, C.F., III.: Structure and finiteness properties of subdirect products of groups. Proc. Lond. Math. Soc. (3) **98**, 631–651 (2009)
7. Collins, D.J.: The word, power and order problems in finitely presented groups. In: Boone, W.W., Cannonito, F.B., Lyndon, R.C. (eds.) Word Problems, Decision Problems and the Burnside Problem in Group Theory. Studies in Logic and Foundations of Mathematics, vol. 71. North Holland, Amsterdam (1973)
8. Dison, W.: Isoperimetric functions for subdirect products and Bestvina–Brady groups. Ph.D. thesis, Imperial College London. Preprint at arXiv:0810.4060 (2008)
9. Gromov, M.: Hyperbolic groups. In: Gersten, S.M. (eds.) Essays in Group Theory, Mathematical Sciences Research Institute Publications, vol. 8, pp. 75–263. Springer, New York (1987)
10. Lyndon, R.C., Schützenberger, M.P.: The equation $a^M b^N = c^P$ in a free group. Mich. Math. J. **9**, 289–298 (1962)

11. Mihailova, K.A.: The occurrence problem for direct products of groups. Dokl. Akad. Nauk SSSR **119**, 1103–1105 (1958)
12. Miller, C.F., III.: On Group-Theoretic Decision Problems and Their Classification. Annals of Mathematical Studies, vol. 68. Princeton University Press, Princeton (1971)
13. Minasyan, A.: On conjugacy separability of fibre products. Proc. Lond. Math. Soc. (3) **115**, 1170–1206 (2017)
14. Ol'shanskii, A.Y.: On residualing homomorphisms and G-subgroups of hyperbolic groups. Int. J. Algebra Comput. **3**, 365–409 (1993)