The Linearity of the Conjugacy Problem for Constant Size Lists of Torsion Elements in Word Hyperbolic Groups

David Buckley

January 19, 2007

Abstract

For any hyperbolic group G and natural number n, there is an algorithm which, given $m < n$ and lists $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_m)$ with all a_i and b_i words in the generators of G, will determine whether or not there exists a $g \in G$ such that $a_i^g = b_i$ for all $i \in \{1, \ldots, m\}$ and output such a g if one exists. Further, if one assumes a RAM model of computing (i.e. basic arithmetic operations on integers can be done in constant time), the algorithm will run in time $O(m^2\mu)$ where μ is the total length of all a_i and b_i. If one assumes that at least one of the a_i or b_i is of infinite order, the algorithm is the same for any n, and will run in time $O(m\mu)$.

1 Introduction

In [1], Bridson and Howie demonstrate a solution of the conjugacy problem for lists of elements in a hyperbolic group – in fact, they prove that the problem is solvable in quadratic time for a torsion free group (using the notation of the abstract, their bound on running time is $O(n\mu^2)$).

The aim here is to both improve the bound on running time and to go some way towards fixing the rather limp conclusion in part 2 of Theorem B in their paper, in which their algorithm simply terminates when the lists contain entirely elements of finite order without giving any results on the conjugacy.

The ideas used here closely relate to the ideas in [2], in which Epstein and Holt show that the conjugacy problem for single elements in a hyperbolic group can be solved in linear time if one assumes a RAM model of computing. They do so by showing that infinite order elements tend to be well-behaved when raised to large powers, and finite order elements can be conjugated to elements of short length, whose conjugacy can be precomputed. In fact, we use a number of results from that paper which relate to these facts in order to establish the result here.

Of course, as in the aforementioned paper, we are assuming a RAM model of computing – that is, we are assuming the basic operations such as addition and multiplication of integers takes place in constant time, which is reasonable when

one assumes that one is not dealing with integers greater than some large upper bound, say 2^{31} – that is, those integers which would fit within a standard 32-bit word. For the purposes of this algorithm, we can make some appropriate assumption, like that our input consists of lists of length less than 2^{31}, whose total element length is also less than 2^{31}. We will also assume that every word w in each of the input lists has $|w|_G > 1$ (this is sensible, since words of length 0 must be the identity, which is clearly conjugate only to itself, so if we receive such an element, we can either trivially reject the input lists as not being conjugate, or simply remove the elements from the input without affecting conjugacy).

We will presume for the duration of this paper that the ambient finitely generated group G has been picked along with a finite presentation, and that this group is hyperbolic in the sense of having δ-thin triangles in its Cayley graph Γ as in [3]. We will also assume that an ordering on the generators has been picked, so that the notion of a short-lex least representative word for each element exists.

The technicalities behind the proof in the case where one element has infinite order are largely covered by showing that any infinite order element can be raised to some (bounded) power and then conjugated by some other element (of bounded length) to produce a straight element (that is, $|g^n|_G = |n||g|_G$ for any $n \in \mathbb{Z}$), then noting that the length of any element when conjugated by large powers of some straight element is very predictable. That is, either the length of the resulting elements will grow in a strict linear sense, or every conjugate will be equal to the original element multiplied by a word of bounded length.

We use a number of results from [2]. Firstly, Section 3.1 there which allows us to reduce words to a conjugate of either a quasigeodesic or a short word (paraphrased along with Section 3.2 which allows us to find short-lex straight powers in Proposition 2.6 here), and secondly the remainder of the procedure described there (Sections 3.3 and 3.4) which allows the conjugacy problem for single elements to be solved by finding the centraliser of some positive power of the elements (this part is paraphrased in Proposition 3.1).

The above centraliser is exhibited as a cyclic group $<c>$ and a bounded set of coset representatives. For each representative s, we compute approximations of the expected lengths of $a_i^{c^n}$ and $b_i^{h^{-1}s^{-1}c^n}$ for large n, where h is an element such that $a_1^h = b_1$, as found in [2].

By comparing these approximations we can find, for each representative, a range of possible powers of the cyclic generator such that the two lists would be conjugate if and only if one of these powers yielded a conjugating element $c^n sh$, and check only these powers. The number of possible powers is bounded by a constant which depends only on the presentation, hence the whole algorithm will run in linear time.

Unfortunately, since we can only obtain this form of the centraliser for infinite order elements, we once again run up against problems when we consider lists of torsion elements. It is, however, possible to show the following:

Theorem 1.1. *There is an algorithm, which given any list $A = (a_1, a_2, \ldots)$ of ele-*

ments of G and $n \in \mathbb{N}$, will either find a $c \in G$ for which $|(a_i a_{i+1} \dots a_n)^c| \leq (12L + 4\delta + 2)3^{n-i}$ for any $1 \leq i \leq n$, or find an infinite order element $g := a_i a_{i+1} \dots a_j$ ($i \leq j \leq n$). Further, the algorithm will run in time $O(n^2\mu)$, where μ is the total length of the first n elements in the list.

If, after applying this theorem we do not find an element of infinite order, we can replace our lists A and B with $(a_1 \dots a_n, a_2 \dots a_n, \dots, a_n)^{c_A}$ and $(b_1 \dots b_n, b_2 \dots b_n, \dots, b_n)^{c_B}$ respectively, and all elements in the new lists will have bounded length. Thus it is possible to simply precompute conjugacy of lists of "short" elements and to check our input against this. ([1] also gives an exponential time algorithm for solving conjugacy of lists of elements, which can be used here.) The disadvantage of this approach is that as the list grows longer, so does the amount of pre-computation required (in a worse-than-exponential fashion). This is why we have to specify a maximum list length n in order to get a linear time algorithm for lists of length shorter than n.

It should be noted that by results in [4], any subgroup containing only finite order elements must itself be finite, and by a result in [5], any finite subgroup can be conjugated inside a $2\delta + 1$ ball - thus it is possible to modify the above theorem to be independent of n. However, studying this approach has yet to yield an algorithm which remains linear in input length.

Finally, a brief discussion of the centraliser problem for lists will be given.

2 Preliminaries

The notation $x\hat{y}z$ will be used for a geodesic triangle in the Cayley graph of a given group G connecting the points x, y and z, and the sides of such a triangle will be referred to as $[xy]$, $[xz]$ and $[yz]$. Note it's possible that several geodesics connect each of the points. However, once a triangle has been constructed, we will assume all of the sides have been fixed - and that if p is a point on $[xy]$, the geodesic $[xp]$ is the segment of the side between x and p. Note that the sides with ordered endpoints can be regarded as words in the generators of the group, and hence elements of the group.

The notation $=_G$ will be used to represent equality between two group elements, and a bare $=$ to represent equality in the free group on the generators of G. The length of a word w will be written $|w|$, and the length of the group element it represents (ie. the length of a geodesic connecting its endpoints) will be written $|w|_G$. Vertices in the Cayley graph will be equated with words and elements of the group (though referred to as points rather than elements), so for example $q := pw$ denotes the endpoint of the path defined by the word w, based at the point p. On the other hand, if we need to refer to the path itself, it will be denoted $\vec{pq}$.

Conjugation will be written with superscripts, that is $g^h := h^{-1}gh$.

In [2], a result by Shapiro is proved:

Lemma 2.1. *Suppose w is a word in the generators of G. Then reduction of w to its short-lex least representative can be done in time linear in $|w|$.*

We will denote use of this lemma (ie. the act of finding short-lex reduced words) by π operating on both elements, words and lists of elements or words in the obvious way. Of course, we will also use it implicitly, since it implies that operations like finding the length of an element, or deciding equality of two elements can be done in time linear in the length of the input elements.

Definition 2.2. *On a δ-thin geodesic triangle $x\hat{y}z$, let c_x be the point on $[yz]$ at distance $\frac{d(y,x)+d(y,z)-d(x,z)}{2}$ from y (similar for c_y, c_z). Then we have that $p \in [c_x y]$ implies $d(p,p') \leq \delta$ where p' is the point on $[yc_z]$ with $d(y,p') = d(y,p)$.*

*The points c_x, c_y and c_z are the **meeting points** of the triangle.*

*A **midpoint** of a geodesic $[xy]$ is a vertex p on $[xy]$ with:*

$$|d(p,x) - d(p,y)| \leq 1$$

That is, if $[xy]$ is of even length, one finds a unique midpoint, but if it's odd, there are two: one on each side of the actual halfway point.

If $w := a_1 a_2 \dots a_k$, where each a_i is a generator, let $w(i) := a_1 a_2 \dots a_i$ ($0 \leq i \leq |w|$). Also, let $w^\infty(i) := w^{\left\lfloor \frac{i}{|w|} \right\rfloor} w(i - |w| \left\lfloor \frac{i}{|w|} \right\rfloor)$ for $i \in \mathbb{Z}$. We can regard w^∞ as a two-way infinite path based at the identity simply by mapping $\mathbb{Z} \to \gamma : z \mapsto w^\infty(z)$.

If $w := [xy]$, let p be the midpoint such that $|[xp]|$ is minimised. We write $w_L := [xp] = w(\left\lfloor \frac{|w|}{2} \right\rfloor)$, $w_R := [py] = w(\left\lfloor \frac{|w|}{2} \right\rfloor)^{-1} w$, and $w_C := w^{w_L} = w_R w_L$.

For example, suppose $w = abcde$ is geodesic. Then $w^\infty(11) = abcdeabcdea$, $w^\infty(-3) = w^{-1}w(2) = e^{-1}d^{-1}c^{-1}$, $w_L = ab$, $w_R = cde$ and $w_C = cdeab$.

Definition 2.3. *A word w is short-lex straight if, for all $i \in \mathbb{N}$, $w^\infty(i)$ is its own short-lex least representative.*

Lemma 2.4. *Suppose $x\hat{y}z$ is a triangle with meeting points c_x, c_y, c_z on sides opposite x, y, and z respectively, and that p is a midpoint on $[xy]$. Then:*

$$d(p,z) \leq \frac{2\max\{d(x,z), d(y,z)\} - d(x,y) + 1}{2} + \delta$$

Proof. Assume that $d(x,z) \geq d(y,z)$, as in Figure 1. Then clearly:

$$\begin{aligned} d(c_z, p) &= d(y,p) - d(y,c_z) \\ &\leq \frac{d(x,y)+1}{2} - \frac{d(x,z)+d(x,y)-d(y,z)}{2} \\ &= \frac{d(y,z)-d(x,z)+1}{2} \end{aligned}$$

If we assume the other side is longer, we can exchange x and y in the above to get a similar equation, hence:

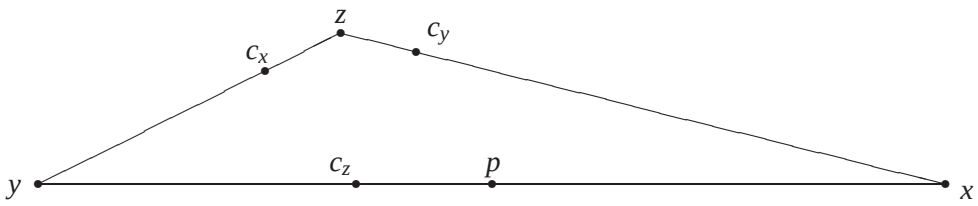

Figure 1: A Triangle in Hyperbolic Space

$$d(c_z,p) \leq \left|\frac{d(x,z)-d(y,z)}{2}\right| + \frac{1}{2}$$

We know $d(c_z,c_x) \leq \delta$ and $d(c_x,z) = \frac{d(x,z)+d(y,z)-d(x,y)}{2}$, so combining the three, we find:

$$\begin{aligned} d(p,z) &\leq d(p,c_z)+d(c_z,c_x)+d(c_x,z) \\ &\leq \left|\frac{d(x,z)-d(y,z)}{2}\right| + \frac{1}{2} + \frac{d(x,z)+d(y,z)-d(x,y)}{2} + \delta \\ &= \frac{\max\{d(x,z),d(y,z)\}-d(x,y)+1}{2} + \delta \end{aligned}$$

Which is the required result. □

Next is an easy lemma that allows us to multiply two elements in our lists.

Lemma 2.5. *Suppose $n \in \mathbb{N}$, and $a_1,\ldots,a_n,b_1,\ldots,b_n \in G$. Then $(a_1,\ldots,a_n)$ is conjugate in G to $(b_1,\ldots,b_n)$ if and only if $(a_1a_2,a_2,\ldots,a_n)$ is conjugate in G to $(b_1b_2,b_2,\ldots,b_n)$.*

Clearly one can extend this to show that we can multiply any elements in the list together, provided we do the same in both lists.

In [2], it's proved that the conjugacy problem for single elements is linear in the total element length. As a step in this proof it is shown that, for $L = 34\delta+1$ (a constant that will be used throughout this paper):

Proposition 2.6. *There exists a constant $Q \in \mathbb{N}$ depending only on the group (and presentation) such that for any short-lex least w for which the word w_C has length strictly greater than $2L$, there exists some integer $0 < k \leq Q$ and some word a whose length is less than 4δ such that $((w_C)^k)^a$ is short-lex straight.*

Moreover, k and a can be computed in time linear in $|w|$.

In particular, if w is of finite order, then $|w_C|_G \leq 2L$.

Finally, for the remainder of the paper, let V be the volume of a 2δ-ball in Γ (that is, the number of geodesic words whose length is less than or equal to 2δ).

We can now move onto results.

3 Conjugacy of finite lists containing at least one infinite order element

In this section, we suppose that we are given lists $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_m)$, and that a_1 is of infinite order.

Our first task is to attempt to get a handle on the centraliser of a_1. We can do this for short-lex straight elements using part of the method for solving the conjugacy problem for individual infinite order elements outlined in [2], which is summarised here:

Proposition 3.1. *For any short-lex straight element w, set $c^l = w$ with $l \in \mathbb{N}$ maximal. Then there exists a set $S \subset G$ with $|S| \leq V$ whose elements are of length at most $|c| + 2\delta$, such that every element of the centraliser of w can be expressed in the form $c^n s$ for some $s \in S$ and $n \in \mathbb{Z}$.*

Moreover, S and c can be computed in time linear in $|w|$.

As in Proposition 2.6, in order to find short-lex straight elements which are conjugates of some power of an input word w, it is useful to be able to guarantee that the length of w_C is strictly greater than $2L$. In fact, we can do this for any infinite order word:

Proposition 3.2. *Let $M := 26000\delta^5 L^3 V^4$. Let w be any infinite order geodesic word in the generators of G with $|w| \leq 2L$. Then $|(\pi(w^M))_C| > 2L$.*

Proof. Note that by [3], we know the following (the explicit values are taken from the proofs):

- (Proposition 3.2) For any infinite order geodesic word w, the two way infinite path in γ defined by w^∞ is a (λ, ε)-quasigeodesic, where $\lambda = |w|V$ and $\varepsilon = 2|w|^2V^2 + 2|w|V$.

- (Theorem 2.19) That $e(0) = \delta$, $e(l) = 2^{\frac{l}{\delta} - 2}$ for $l > 0$ is a divergence function for any δ-hyperbolic space (ie. given geodesics $\gamma = [xy]$ and $\gamma' = [xz]$, $r, R \in \mathbb{N}$ such that $r + R < \min(|\gamma|, |\gamma'|)$ and $d(\gamma(R), \gamma'(R)) > e(0)$, if α is a path from $\gamma(R + r)$ to $\gamma'(R + r)$ lying outside the ball of radius $R + r$ around x, then $|\alpha| > e(r)$.)

- (Proposition 3.3) In a δ-hyperbolic space with divergence function e, given a (λ, ε)-quasigeodesic α between x and y, and a geodesic γ starting and ending at the same points as α, every point on γ is within a distance D of a point on α, for any D that satisfies $e(\frac{D - e(0)}{2}) \geq 4D + 6\lambda D + \varepsilon$.

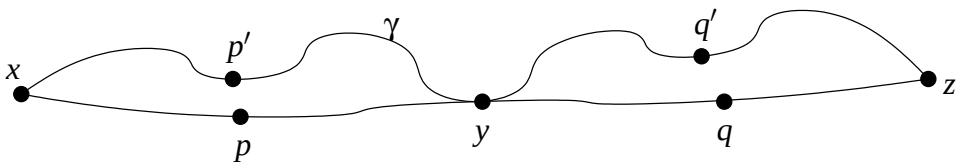

Figure 2: Cutting across a long quasigeodesic

Now, consider the (λ,ε)-quasigeodesic γ given in the first result and pick D from the third result appropriately, and define the points $x := 1$, $y := w^n$ and $z := w^{2n}$ for some n. Let $[xy]$ and $[yz]$ be the short-lex geodesics. Let p be a midpoint of $[xy]$ and q the corresponding midpoint of $[yz]$ (that is, $q = y[xp]$). See figure 2.

Then there exists a point p' on γ within D of p, we can pick the point $q' = y[xp']$ so that q' is clearly within D of q. Then:

$$\begin{aligned} d(p,q) &\geq d(p',q') - 2D \\ &\geq \frac{d_\gamma(p',q')}{\lambda} - \varepsilon - 2D \\ &= \frac{|w|n}{\lambda} - \varepsilon - 2D \end{aligned}$$

Since we need $d(p,q) > 2L$, it is sufficient to ensure $\frac{|w|n}{\lambda} - \varepsilon - 2D > 2L$. So taking $n > \lambda(2L + 2D + \varepsilon)$, it is clear that $d(p,q) = |(\pi(w^N))_C| > 2L$. We can find λ and ε from the first result, and after much manipulation and approximation, we find that it is sufficient to take $D = 6144\delta^5L^2V^4$, hence $\lambda(2L+2D+\varepsilon) \leq (2LV)(13000\delta^5L^2V^4) = 26000\delta^5L^3V^5 = M$, and $n > M$ implies that $|(\pi(w^N))_C| > 2L$ as required. □

Remark 3.3. *The value of M given above is of course by no means optimal - for each particular case, it is likely that a much lower bound can be obtained by solving the equations programmatically. However, the above bound illustrates that there is a definite computable value.*

Combining this result with the previous one, we obtain a more useful proposition:

Proposition 3.4. *There exists a constant $P \in \mathbb{N}$ depending only on the group and presentation such that for any infinite order geodesic word w, there exists a set $S \subset G$ with $|S| \leq V$ whose elements are of length at most $P|w|$, a short-lex straight element $c \in G$ whose length is at most $P|w|$ and an element p of length at most $P|w|$ such that every element of the centraliser of w can be expressed in the form pc^ns for some $s \in S$ and $n \in \mathbb{Z}$.*

Moreover, S, p and c can be computed in time linear in $|w|$.

Proof. Firstly, suppose that $|w_C|_G \leq 2L$. Then, by Proposition 3.2 applied to w_C, $|(\pi((w_C)^M))_C| > 2L$. In this case, let $q' := w_L$ and $m_1 := M$. On the other hand, if $|w_C|_G > 2L$ let $q' := 1$ and $m_1 := 1$. Then either way, letting $w'' := \pi((w^{q'})^{m_1})$, we have $|w''_C|_G > 2L$. Hence, by proposition 2.6, there is a power $m'_2 \leq Q$, and a word a of length less than or equal to 4δ such that $w' := \pi(((w''_C)^{m'_2})^a)$ is short-lex straight. Let $q := q'w''_L a$, and $m_2 := m_1 m'_2$, so that $w' = \pi((w^q)^{m_2})$. Clearly, $|q| \leq (MQ+1)|w| + 4\delta$ and $m_2 \leq MQ$.

Now let us apply Proposition 3.1 to w' to give us a c which is short-lex straight, along with a set S'.

Now, suppose g is some element of the centraliser of w. Then $w'^{q^{-1}gq} =_G w'$, hence $q^{-1}gq$ is in the centraliser of w' and thus $q^{-1}gq =_G c^n s'$ for some $s' \in S'$ and some integer n. Let us set $p := q$ and $S := \{s'q^{-1} : s' \in S'\}$, then clearly every element of the centraliser of w can be expressed in the form $qc^n s'q^{-1} = pc^n s$ for some $s' \in S'$, $s \in S$ and $n \in \mathbb{Z}$ as required.

Clearly, the elements of S have a length of at most $(MQ+1)|w| + 4\delta + |w|$, which in particular is less than $(MQ+4\delta+2)|w|$. Similarly, $|c| \leq (MQ+4\delta)|w|$, so it is sufficient to set $P := (MQ+4\delta+2)$. Also, the set S has the same number of elements as S', so clearly $|S| \leq V$. Clearly, we can obtain S and c in time linear in $|w|$, so the proposition is proved. □

Here is a quick lemma which shows that "thin" sections of a geodesic quadrilateral behave in a very specific way:

Lemma 3.5. *Suppose that the points C, D, E and F satisfy $d(C,D) = d(E,F)$. Define a geodesic quadrilateral as in Figure 3, and divide this quadrilateral into two triangles using a geodesic representing $\vec{CE}$. Let p_1 be the meeting point of the triangle $C\hat{D}E$ lying on $u := \vec{CD}$, and let p_2 be the meeting point of the triangle $\triangle CEF$ lying on $v := \vec{FE}$. Let $K := |\vec{CD}| - |\vec{CE}|$. Then for any $i \in \mathbb{Z}$ with $d(F,p_2) \leq i \leq d(C,p_1)$, we have $u(i)\vec{v}(i) =_G h(v(i+K))^{-1}v(i)$ for some word h with $|h| \leq 2\delta$.*

Proof. This is elementary: For any i in the given range, let $w(i)$ be the point on $\vec{CE}$ corresponding to $u(i)$, and $x(i)$ the point on v corresponding to $w(i)$ as in Figure 4. Pick some specific j in the range. It is clear that for any i, $d(u(i),u(j)) = d(x(i),x(j))$, hence we find that $d(x(i),v(i)) = d(x(j),v(j))$. Now we have:

$$\begin{aligned} d(x(j),v(j)) &= |d(E,v(j)) - d(E,x(j))| \\ &= |d(D,u(j)) - d(E,w(j))| \\ &= |d(D,u(j)) - d(C,E) + d(C,w(j))| \\ &= |d(D,u(j)) - d(C,E) + d(C,u(j))| \\ &= |d(C,D) - d(C,E)| \\ &= |K| \end{aligned}$$

It should be clear that if $x(j)$ is closer to E than $v(j)$, the same is true for $x(i)$ and $v(i)$ for all i, hence we can follow the path from $u(i)$ to $w(i)$ to $x(i)$ (of

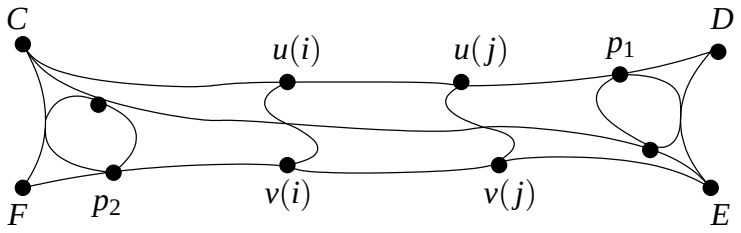

Figure 3: The thin section of a geodesic quadrilateral

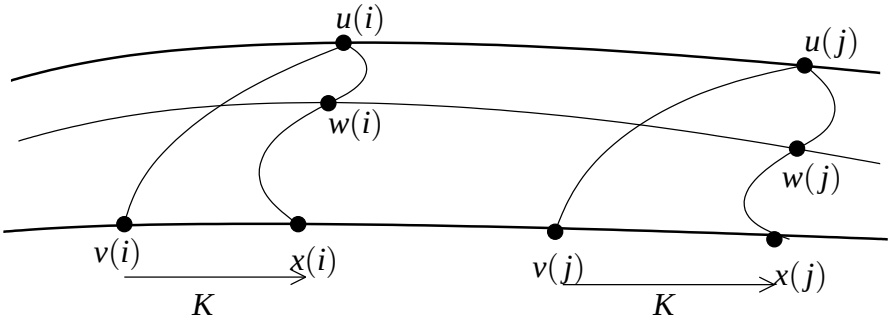

Figure 4: A part of figure 3

length at most 2δ, hence giving us h), then the path from $x(i)$ to $v(i)$ (which is $v(i+K))^{-1}v(i)$) to get the result.

□

We now prove the following useful proposition:

Proposition 3.6. *Suppose that G is a δ-hyperbolic group, that g is a straight word and that a is any geodesic word in the generators of G. Let $N := V + \left\lceil \frac{3|a|+7\delta}{2|g|} \right\rceil + 2$. Then:*

- *If $|a^{g^N}| > |a| + 4\delta$, then letting $K_1 := |a^{g^N}| - |g|N$ and, $K_2 := |a^{g^{-N}}| - |g|N$, for all $i > N$, we have*

$$\left| |a^{g^i}| - K_1 - 2i|g| \right| \leq 3\delta$$

and

$$\left| |a^{g^{-i}}| - K_2 - 2i|g| \right| \leq 3\delta$$

- *Otherwise, letting $K := 2|g|N - |g^N a g^N|$, we have for any $i \in \mathbb{Z}$, there exists a word h of length less than or equal to 2δ such that:*

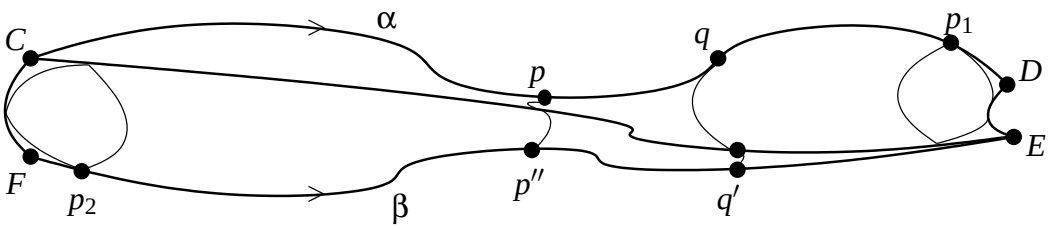

Figure 5: The geodesics α and β lie close.

$$a^{g^i} =_G hg^\infty(-K)$$

Proof. First, suppose that the length of a^{g^i} ($i \in \mathbb{Z}$) is bounded above by some constant R. Our aim in this case is to show that the second case of the proposition applies. Consider the paths $\alpha := g^\infty$, and $\beta := ag^\infty$ (ie. the path following g through each 1^{ag^i}). Let $k > \left\lceil \frac{R}{|g|} \right\rceil$, and let $C := g^{-k}$, $D := g^k$, $E := ag^k$ and $F := ag^{-k}$. Define a geodesic quadrilateral between these points, with $\vec{CD}$ and $\vec{FE}$ being segments of α and β.

Lemma 3.5 can clearly be applied, so that letting $K' := 2|g|k - |g^k a g^k| = d(C,D) - d(C,E)$, we find that for any $i \in \mathbb{Z}$ such that $|i| < k - \left\lceil \frac{R}{|g|} \right\rceil$ (since $d(p_1,D) \leq R$, and $d(p_2,F) \leq R$, this means that $d(F,p_2) \leq |g|i \leq d(C,p_1)$, as required by the lemma), if we take $p := g^i$, $p' := ag^i$ and $p'' := ag^\infty |g|i + K'$, we have:

$$a^{g^i} =_G \vec{pp'} =_G hp''\vec{p'} =_G hg^\infty(-K')$$

Where h is some word such that $|h| \leq 2\delta$. Therefore, we obey the equation in the second case of the proposition for any i in this bounded range. In particular, by taking k to be large, it is clear that there must be at most V distinct conjugates of the form a^{g^i} for $i \in \mathbb{Z}$. Also note if $a =_G h'g^\infty(-K')$, we have $a^{g^i} =_G hg^\infty(-K') =_G hh'^{-1}h'g^\infty(-K') = hh'^{-1}a$ - hence $|a^{g^i}| \leq |a| + 4\delta$, and if the length of conjugates is bounded, $|a| + 4\delta$ will act as a bound. We will thus assume that $R = |a| + 4\delta$.

Let $k := N$ as in the statement of this proposition. Since the meeting point, p_1, must be within R of g^k and, p_2 within R of ag^{-k}, it is clear that there must be at least $2N - \left\lceil \frac{2R}{|g|} \right\rceil > V$ distinct $i \in \mathbb{Z}$ such that $|i| \leq k - \left\lceil \frac{R}{|g|} \right\rceil$. The a^{g^i} cannot all be distinct for this range of i, since we know that there are only V possible distinct values, so there must be at least one repeated conjugate, say $a^{g^i} =_G a^{g^{i+l}}$ so that $a^{g^j} =_G a^{g^{j+tl}}$ for any $i,t \in \mathbb{Z}$. (Of course, this is the same as saying that $g^l \in C_G(a)$.) In particular, every possible a^{g^j} for $j \in \mathbb{Z}$ must be equal in G to some a^{g^t} where $|t| \leq k - \left\lceil \frac{|a|+4\delta}{|g|} \right\rceil$ - and hence is equal in G to $h(g^\infty(-K))^{-1}$ for some word h with $|h| \leq 2\delta$ as required by the statement. Thus if the length of conjugates is bounded, we must be in the second case.

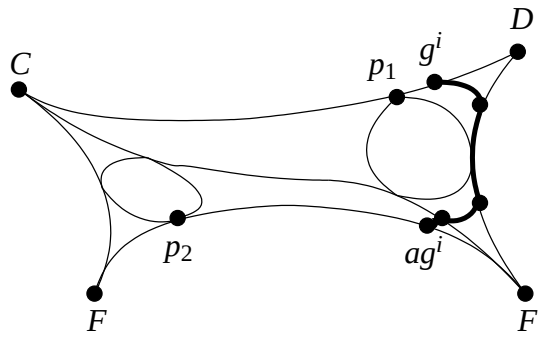

Figure 6: Linear growth after the meeting point

Now suppose that the length of conjugates a^{g^i} for $i \in \mathbb{Z}$ is not bounded above. We will first show that this is equivalent to $|a^{g^N}| > |a| + 4\delta$ (thus demonstrating that the cases as given in the theorem statement indeed correspond to the cases where the length of conjugates are unbounded and bounded respectively).

Let us consider the geodesic quadrilateral with corners $C := 1$, $D := g^N$, $E := ag^N$ and $F := a$, as in Figure 6 and the obvious geodesics connecting them (pick any geodesic to connect D and E). Now let us split this quadrilateral into two triangles using a geodesic connecting C and E (note this is equal in G to ag^N). Let p_1 be the meeting point between 1 and g^N, let p_2 be the meeting point between a and ag^N (see Figure 6 for a diagram of this arrangement), and let k_1 and k_2 be their respective distances from 1 and a (so $k_1 = d(C, p_1) = \frac{|g|N+|ag^N|-|a^{g^N}|}{2}$ and $k_2 = d(F, p_2) = \frac{|g|N+|a|-|ag^N|}{2}$).

The key observation here is that by following the path illustrated in Figure 6, we see that $|a^{g^N}| - 2|g|(N-i) - 3\delta \leq |a^{g^i}| \leq |a^{g^N}| - 2|g|(N-i) + 3\delta$ for any $i \in \mathbb{Z}$ such that $|g|N \geq |g|i \geq \max\{k_1, k_2\}$. Hence, in particular, if we let $k := \left\lceil \frac{\max\{k_1,k_2\}}{|g|} \right\rceil$ (ie. the first k such that $|g|k$ lies after both meeting points), we have $|a^{g^N}| \geq |a^{g^k}| + 2|g|(N-k) - 3\delta \geq 2|g|(N-k) - 3\delta$. If we show that $k < N - \frac{|a|+7\delta}{2|g|} < V + \frac{3|a|}{2|g|} + 2$, we have $|a^{g^N}| > |a| + 4\delta$ as required.

First suppose that $k_1 \leq |a|$ (note $k_2 \leq |a|$ is always true). Then it's clear that $k \leq \left\lceil \frac{|a|}{|g|} \right\rceil < V + \frac{3|a|}{2|g|} + 2$.

So let's consider $|a| \leq k_1$. Once again, we can apply Lemma 3.5 and we find that once again there exists some word w such that the conjugates lying between the meeting points (that is, the a^{g^i} where $k' \leq i < k$ with $k' := \left\lceil \frac{k_2}{|g|} \right\rceil$, the power of the first conjugate after the meeting point p_2) have the form hw with $|h| \leq 2\delta$. In particular we have at most V distinct elements a^{g^i} with $k' \leq i < k$. If we ever get a repeated element, say $a^{g^i} = a^{g^j}$, then $g^{i-j} \in C_G(a)$ and we are in the bounded case, so we must have $k - k' \leq V$. Now since $k' \leq \left\lceil \frac{|a|}{|g|} \right\rceil$, we must have $k < V + \left\lceil \frac{3|a|}{2|g|} \right\rceil +$

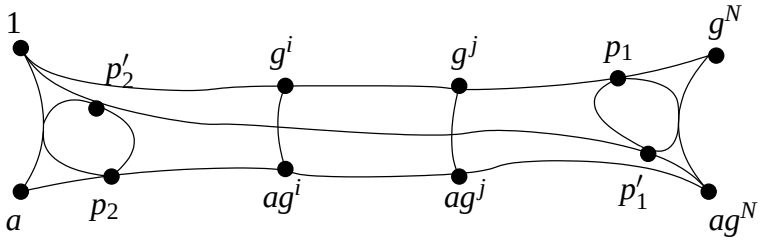

Figure 7: The midsection of the unbounded case, case 2

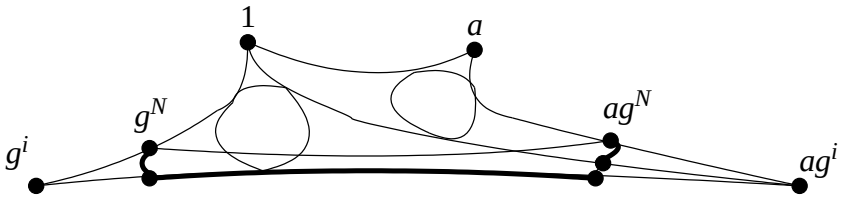

Figure 8: After the first section

$1 \leq V + \frac{3|a|}{2|g|} + 2$, which is what we required above. Thus we have established that $|a^{g^N}| > |a| + 4\delta$ if and only if the set of conjugates $\{a^{g^j} : j \in \mathbb{Z}\}$ is infinite.

Now we prove that all higher powers, g^i for $i \geq N$, will result in conjugates whose length is within 3δ of $|a^{g^N}| + 2(i-N)|g|$. This can easily be seen by following the path marked on figure 8. (We have, as before, $|a^{g^i}| - |g|(i-N) - 3\delta \leq |a^{g^N}| \leq |a^{g^i}| - |g|(i-N) + 3\delta$.)

Clearly, then, we are in the first case in the theorem and it is trivial to compute the constants: $K_1 = |ag^N| - |g|N$, $K_2 = |ag^{-N}| - |g|N$ (to see this, simply replace g with g^{-1} - which is clearly also a straight word) - and we have proved the theorem. □

Now we can approach the problem of solving the conjugacy of the two lists.

Recall that we have two lists $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_m)$, and that a_1 is of infinite order. Recall also that we have both an element $h \in G$ such that $a_1^h = b_1$ (we can get this using the method in [2]) and from Proposition 3.4, elements $c, p \in G$ such that c is straight along with a set S of size bounded by V so that every element in the centraliser of a_1 can be expressed in the form $pc^n s$ for some $n \in \mathbb{Z}$ and $s \in S$.

Any element that conjugates A to B must conjugate a_1 to b_1, and hence is of the form $pc^n sh$. Hence, we need only search for elements of this form. For simplicity, let us replace B with $\pi(B^{h^{-1}})$ and A with $\pi(A^p)$. Since the size of S is bounded by V, depends only on the group and presentation, we can iterate through its elements in constant time.

Now, suppose we are given some element $s \in S$. We will proceed through

$i \in \{1,\dots,m\}$ to find a bounded range of possible $g \in G$ which could be considered as candidates for conjugating elements. That is, for each $i \in \{1,\dots,m\}$, we need to find a range of $k \in \mathbb{Z}$ which contains any k such that $a_i^{c^k s} = b_i$. By iterating over every $s \in S$, we aim to either eliminate or check every possible element of the centraliser. Let us apply Proposition 3.6 with $a = a_i$ and $g = c$, and with $a = b_i^{s^{-1}}$ and $g = c$. Note that one only needs to apply Proposition 3.6 once for each a_i.

Clearly if the two elements result in different cases in the proposition then no k can exist such that $a_i^{c^k s} = b_i$, since if it did, for any $l \in \mathbb{Z}$ we have $a_i^{c^{k+l}} = b_i^{s^{-1}c^l}$, and for large l, we would get a contradiction on the length of this element. Thus, we can move onto the next element of S.

If both elements are in the first case, let $K_{1a} := K_1(a_i, c)$ and $K_{1b} := K_1(b_i^{s^{-1}}, c)$ with K_{2a} and K_{2b} defined similarly. Comparing lengths of elements, we find that if we assume that there exists some $k \in \mathbb{Z}$ such that $a_i^{c^k s} =_G b_i$, then for all $l \in \mathbb{N}$, $a_i^{c^{k+l}} = b_i^{s^{-1}c^l}$, and we have:

$$\begin{aligned} & |K_{1a} + 2(k+l)|c| - K_{1b} - 2l|c|| \\ = \;& |K_{1a} + 2k|c| - K_{1b}| \\ \leq \;& 6\delta \end{aligned}$$

Hence we have:

$$\left| k - \frac{K_{1b} + K_{1a}}{2|c|} \right| \leq \frac{6\delta}{2|c|}$$

Applying the same reasoning to the other side gives:

$$\left| k - \frac{K_{2a} + K_{2b}}{2|c|} \right| \leq \frac{6\delta}{2|c|}$$

So we can restrict k to within the intersection of each of these clearly bounded ranges, and we need to check at most 6δ elements $a_i^{c^k s}$ for equality to b_i in order to find any k which exists. This can be done in time $O(m\mu)$ (since the lengths of said elements must be linear in the input length).

Now suppose both elements lie in the second case. This does not immediately allow us to eliminate any elements, however we can use the bounds for the previous case unless all elements in the list have this property. Suppose that they do indeed all have this property. We know that conjugates will repeat after at most V powers, and we can, for each i, in time $O(\mu)$, work out exactly how long the repeating sequence is by simply evaluating each conjugate $a_i^{c^k}$ until one of them is equal to simply a_i. While we are doing this, we can also make a list M_i of each k such that $a_i^{c^k s} = b_i$. Let l_i be the length of the repeating sequence for a_i for each i, then we simply need to find a number between 0 and $\operatorname{lcm}\{l_1,\dots,l_m\} \leq V!$ which, for each i, is in $M_i + n_i\mathbb{Z}$. This can be solved in time linear in m by simply checking every number $0 \leq j \leq \operatorname{lcm}\{l_1,\dots,l_m\}$ to see if it satisfies $j \in M_i + l_i\mathbb{Z}$ for all $1 \leq i \leq m$.

Thus in all cases, we can, in time $O(m\mu)$ as required, solve the conjugacy problem for lists containing at least one infinite order element.

4 Conjugacy of Lists

Suppose $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, \ldots, b_n)$ with a_i and b_i geodesic words in the generators of G for all i.

We will describe an algorithm to determine whether $A^g = B$ for some $g \in G$ which will reduce to the case where the $|a_i|$ and $|b_i|$ all have length less than or equal to some fixed bound $K_{i,n}$. We can then determine conjugacy simply by pre-computing conjugacy of all such lists of "short" elements and looking up the particular problem. Suppose $A = (a_1, a_2, \ldots)$ is a list of geodesic words in G and $n \in \mathbb{N}$. Then consider the following algorithm:

Algorithm 4.1. *1. Let $c \leftarrow 1, k \leftarrow 1$.*

2. If $|(\pi((a_j \ldots a_k)^c)_C| > 2L$ for any $1 \leq j \leq k$, let $g \leftarrow a_j \ldots a_k$, stop and return g.

3. Let $c \leftarrow c(\pi(a_k^c))_L$.

4. Let $k \leftarrow k+1$.

5. If $k = n+1$, then stop and return c, else go to step 2.

Proposition 4.2. *The above algorithm will either find a $c \in G$ for which $|(a_i a_{i+1} \ldots a_n)^c| \leq (12L + 4\delta + 2)3^{n-i}$ for any $1 \leq i \leq n$, or find an infinite order element $g = a_i a_{i+1} \ldots a_j$ $(i \leq j \leq n)$. Further, the algorithm will run in time $O(n^2\mu)$, where μ is the total length of the first n elements in the list.*

Proof. First let us suppose $n = 1$. It should be clear that the algorithm will produce either a g (which must be infinite order by Proposition 2.6) or a c as required, and run in linear time. Let $K_{1,1} = 2L$. Define μ_k to be the total length of the first k words in A, plus k (that is, $\mu_k := \sum_{i=1}^{k} |a_i|$). Note that since $|a_i|_G > 0$, we have $\mu_k \geq k$.

Let us briefly consider the change in length of c at step 3. Using Lemma 2.4 we can see that if we consider the triangle with corners $C := 1$, $D := a_k^c$ and $E := c^{-1}$ as illustrated in Figure 9 ($p = (\pi(a_k^c))_L$ is the midpoint of $\vec{CD} = \pi(a_k^c)$ closest to C), we must have $d(E, p) \leq \frac{2\max\{|c|, |a_k c|\} - |c^{-1} a_k c| + 1}{2} + \delta \leq |a_k| + |c| + \delta + \frac{1}{2}$. Hence $|c(\pi(a_k^c))_L| \leq k(\delta + \frac{1}{2}) + \sum_{i=1}^{k} |a_i| = \mu_k + k(\delta - \frac{1}{2})$, so at step 2, $|c| \in O(\mu_k)$.

Now suppose that $k \in \mathbb{N}$ such that $k > 1$, and we have constants $K_{i,k-1}$ such that at step 5 in the algorithm, we have $|(a_i \ldots a_{k-1})^c| \leq K_{i,k-1}$ for any $1 \leq i \leq k-1$. We will show there exist constants $K_{i,k}$ $(1 \leq i \leq k)$ such that upon reaching step 4 we have, in time $O(k\mu_k)$ either found an element $c \in G$ for which $|(a_i \ldots a_k)^c| \leq K_{i,k}$ for any $1 \leq i \leq k$ or found an infinite order element $g := a_i \ldots a_k$ (for some $1 \leq i \leq k$). (Note that the hypothesis of this paragraph is definitely true for $k = 2$, since we will have $|a_1^c| = |(a_1)_C| \leq 2L$.)

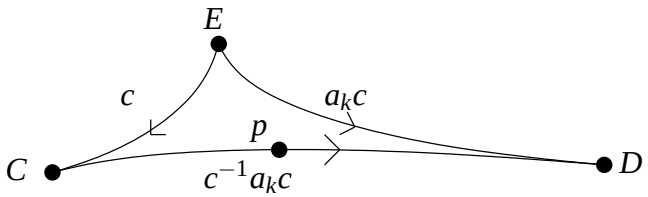

Figure 9: Extending c.

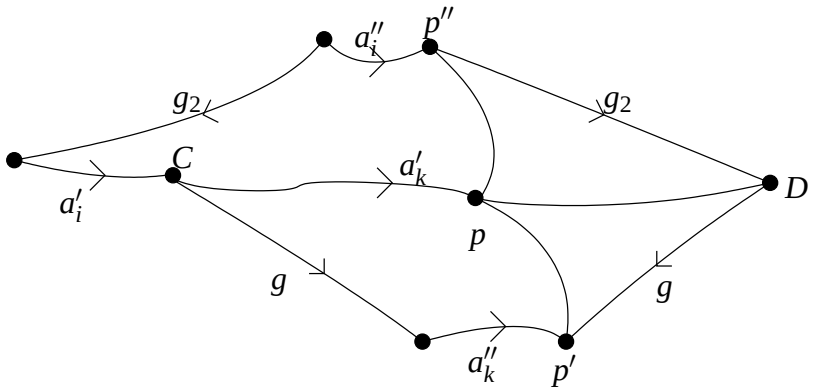

Figure 10: The conjugates of the a_i' are all short.

First, for simplicity of notation, convert A to the list $A' = (a_1', a_2', \ldots, a_k')$ with $a_i' := \pi((a_i \ldots a_{k-1})^c)$ for $1 \leq i \leq k-1$, and $a_k' := \pi(a_k^c)$. Let $g := (a_k')_L$.

Now we use Proposition 2.6 and let $a_i'' := (\pi(a_i' a_k'))_C$ for each $1 \leq i \leq k-1$ and $a_k'' := (a_k')_C$. If for any i, a_i'' has length strictly greater than $2L$ then clearly a_i' is of infinite order by Proposition 2.6, so we are done (as in step 2), otherwise we continue as in the algorithm. The operation of checking the length of each a_i'' can clearly be done in time $O(k\mu_k)$, since the elements a_i' are of length at most $\mu_k + 2|c| \in O(\mu_k)$.

Now define the points $C := 1$ and $D := a_k'$. Let p be a midpoint of $\vec{CD}$. Consider Figure 10 for any $i < k$.

Using Lemma 2.4, it should be clear using the triangle with corners C, D and p', (hence sides a_k', g and ga_k'') along with the fact that $2|g| \leq |a_k'|$ that:

$$\begin{aligned} d(p,p') &\leq \frac{2(|g| + |a_k''|) - |a_k'| + 1}{2} + \delta \\ &\leq |a_k''| + \delta + \frac{1}{2} \\ &\leq 2L + \delta + \frac{1}{2} \end{aligned}$$

Similarly, with the triangle with corners C, D and p'' (hence sides a_k', $g_2 :=$

$(a'_i a'_k)_L$ and $a'^{-1}_i g_2 a''_i$) and using $2|g_2| \leq |a'_k| + |a'_i|$ we know:

$$\begin{aligned} d(p,p'') &\leq \frac{2(|g_2| + |a''_i| + |a'_i|) - |a'_k| + 1}{2} + \delta \\ &\leq |a''_i| + \frac{3}{2}|a'_i| + \delta + \frac{1}{2} \\ &\leq 2L + \delta + \frac{1 + 3K_{i,k-1}}{2} \end{aligned}$$

So:

$$d(p'',p') \leq 4L + 2\delta + 1 + \frac{3}{2}K_{i,k-1}$$

Now it's clear that we have $(a_i \dots a_k)^{cg} = (a'_i a'_k)^g = ((a'_i a'_k)^{g_2})^{g_2^{-1}g} = a_i''^{g_2^{-1}g}$. This has short lex length less than or equal to:

$$\begin{aligned} & 2|g_2^{-1}g| + |a''_i| \\ = \; & 2d(p'',p') + |a''_i| \\ \leq \; & 2(4L + 2\delta + 1 + \frac{3}{2}K_{i,k-1}) + |a''_i| \\ \leq \; & 10L + 4\delta + 2 + 3K_{i,k-1} \end{aligned}$$

Since exactly the same argument works for any $i \leq k-1$, defining this as $K_{i,k}$ and letting $K_{k,k} := 2L$, we have the required constants.

Therefore, since step 3 clearly takes time $O(\mu_k)$, the $k = i$ loop is completed in time $O(i\mu_i)$, and we take time $O(i^2\mu_i)$ to reach step 4 with $k = i$. Hence the algorithm terminates in time $O(n^2\mu_n)$.

We can easily get a bound on the constants $K_{i,k}$ as in the proposition statement using some simple combinatorics and noting that $K_{i,i} = 2L$ for any i:

$$\begin{aligned} K_{i,n} &= 10L + 4\delta + 2 + 3K_{i,k-1} \\ &= \sum_{j=0}^{n-i-1} 3^j(10L + 4\delta + 2) + 3^{k-i-1}.2L \\ &= (10L + 4\delta + 2)(3^{k-i} - 1) + 3^{k-i-1}.2L \\ &\leq (12L + 4\delta + 2)3^{k-i} \end{aligned}$$

□

By Lemma 2.5, the conjugacy problem remains unchanged between studying the lists $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$, and the lists $(a_1 \dots a_n, a_2 \dots a_n, \dots, a_n)$ and $(b_1 \dots b_n, b_2 \dots b_n, \dots, b_n)$. Hence by precomputing the conjugacy problem between all short lists (in the sense that the kth element has length less than or equal

to $(12L+4\delta+2)3^{n-k}$), we can solve the conjugacy problem for lists by applying the above result and then either using the algorithm which requires one infinite order element, or our precomputed results for short lists.

Here is a complete description of the algorithm, given the input of two lists A and B of words in the generators of G, assuming both lists have $m \leq n$ elements, and all conjugacy of all lists of words $(a_1,\ldots,a_n)$ for which $|a_i| \leq (12L+4\delta+2)3^{n-i}$ has been computed using the exponential algorithm given in [1]. Note that if $m < n$ in step 7, we can extend the lists A and B to length n without increasing μ by simply adding several copies of the identity element onto the ends of both lists.

1. Reduce all words in both lists to geodesics using π.
2. Apply Algorithm 4.1 to A to get a conjugating element c or inifinite order element g.
3. If the above step gave an infinite order element $g = a_i \ldots a_j$, then replace A with $[a_i \ldots a_j, a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_m]$ and similar for B, then go to 8. Note that if all the elements are short there may still be an infinite order element.
4. Apply Algorithm 4.1 to B to get a conjugating element c' or infinite order element g.
5. If the above step gave an infinite order element $g = b_i \ldots b_j$, then replace A with $[b_i \ldots b_j, b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_m]$ and similar for B (ie. the lists should now be swapped), then go to 8.
6. Otherwise, replace A with $[a_1 \ldots a_m, a_2 \ldots a_m, \ldots, a_m]^c$ and replace B with $[b_1 \ldots b_m, b_2 \ldots b_m, \ldots, b_m]^{c'}$.
7. Now test conjugacy of A and B using the precomputed list. If a conjugating element g is found, return cgc'^{-1} as a conjugating element. Otherwise the lists are not conjugate. Either way, we can stop.
8. Test conjugacy of a_1 and b_1 using the method in [2] to find a conjugating element h. If this does not exist, the lists are not conjugate, so stop.
9. Use Proposition 3.4 to express some superset of the centraliser of a_1 using a set S, a straight word c and some element p.
10. Apply Proposition 3.6 to a_i^p and c for each $1 \leq i \leq m$.
11. For each $s \in S$, apply Proposition 3.6 to $b_i^{h^{-1}s^{-1}}$ and c.
12. If any i results in different cases for $b_i^{h^{-1}s^{-1}}$ and a_i^p, move onto the next s.
13. If any i results in case 1 for both $b_i^{h^{-1}s^{-1}}$ and a_i^p, use the bounds as given after Proposition 3.6 to test a bounded range of conjugates for equality.

14. Otherwise, test the conjugacy using the bounded length search, as outlined after Proposition 3.6.

15. If any of the previous two steps result in a conjugating element $pc^k sh$, return it and stop. If there is no conjugating element found for any s, the lists are not conjugate, so stop.

Clearly this algorithm runs in time $O(m^2\mu)$. If we know a_1 is of infinite order, we can start at step 8 to get an algorithm that runs in time $O(m\mu)$ and does not require any precomputation dependent on n.

5 Computation of Centralisers

Because of the potentially exhaustive nature of the algorithm above, it already provides enough information to give generators for the centraliser of any input list whose first element is of infinite order: If one sets $A = B$, the algorithm will find conjugating elements only when that element is in the centraliser of A.

On the other hand, since the generators of centralisers of lists are certainly computable by the algorithm discussed in [6], we can add to the precomputation stage the centralisers of all lists of short elements as before.

Here is a complete description of the centraliser algorithm with input list A, assuming A has $m \leq n$ elements, and the above precomputation has been performed:

1. Reduce all words in A to geodesics using π.

2. Apply Algorithm 4.1 to A to get a conjugating element c or inifinite order element g.

3. If the above step gave an infinite order element $g = a_i \dots a_j$, then replace A with $[a_i \dots a_j, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_m]$ and go to 5.

4. Otherwise, replace A with $[a_1 \dots a_m, a_2 \dots a_m, \dots, a_m]^c$, return the generators of the precomputed centraliser for A conjugated by c^{-1}, then stop.

5. Use Proposition 3.4 to express some superset of the centraliser of a_1 using a set S, a straight word c and some element p.

6. Apply Proposition 3.6 to a_i^p and c for each $1 \leq i \leq m$.

7. For each $s \in S$, apply Proposition 3.6 to $a_i^{s^{-1}}$ and c.

8. If any i results in different cases for $a_i^{s^{-1}}$ and a_i^p, move onto the next s.

9. If any i results in case 1 for both $a_i^{s^{-1}}$ and a_i^p, use the bounds as given after Proposition 3.6 to test a bounded range of conjugating elements. Add any element found to be in the centraliser to C.

10. Otherwise, check if a_i^p in the bounded length search, as outlined after Proposition 3.6. Add $pc^k s$ to C whenever $a_i^{pc^k s} = a_i$ for all $1 \leq i \leq m$. Also, if this case ever occurs, add $pc^{\mathrm{lcm}\{l_1,\ldots,l_m\}} p^{-1}$ to C.

11. Once all elements of S have been tested, return C and stop.

C must now be a complete generating set for the centraliser of A. To see this, suppose $g \in C_G(A)$. Then $g = pc^k s$ for some $k \in \mathbb{Z}$ and $s \in S$. If s would result in case 1 for any a_i, it would have been added to C in step 9. Otherwise, let $L := \mathrm{lcm}\{l_1, \ldots, l_m\}$, and let $k = sL + r$ for some $s, r \in \mathbb{Z}$ such that $0 \leq r < L$. Then $pc^L p^{-1}$ is in C, as is $pc^r s$ since both are added in step 10 - hence g is a multiple of elements of C.

Again, if one knows a_1 is of infinite order, one can start from 5; the algorithm will run in time $O(m\mu)$ and requires no precomputation dependent on n. If not, the running time will be in $O(m^2\mu)$.

References

[1] M. R. Bridson and J. Howie, "Conjugacy of finite subsets in hyperbolic groups," 2003.

[2] D. B. E. Epstein and D. F. Holt, "The linearity of the conjugacy problem in word hyperbolic groups," 2005.

[3] J. M. Alonso, T. Brady, D. Cooper, V. Ferlini, M. Lustig, M. Mihalik, M. Shapiro, and H. Short, "Notes on word hyperbolic groups," in *Group theory from a geometric viewpoint*, World Scientific, Singapore, 1991. Proceedings of the ICTP conference in summer 1990.

[4] W. Ballmann, W. Ghys, A. Haefliger, P. de la Harpe, E. Salem, R. Strebel, and M. Troyanov, "Sur les Groups Hyperboliques d'aprés Mikhael Gromov," Notes of a seminar held at Berne, edited by E. Ghys and P. de la Harpe, Birkhäuser, *Progress in Mathematics Series*, 1990

[5] M. R. Bridson and A. Haefliger, "Metric Spaces of Non-Positive Curvature," Springer-Verlag, 1999.

[6] S. M. Gersten and H. B. Short, "Rational subgroups of biautomatic groups," Ann. of Math. (2), 134(1):125-158, 1991