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

David Buckley

September 11, 2006

1 Abstract

For any hyperbolic group G and natural number n, there is an algorithm which, given $m < n$ and lists $A = (a_1, \dots, a_m)$ and $B = (b_1, \dots, b_m)$ 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 $i \in \{1, \dots, m\}$ 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 the group is torsion free, or that at least one of the a_i is of infinite order, the algorithm is the same for any n, and will run in time $O(m\mu)$.

2 Introduction

In [**?**], Bridson and Howie demonstrate the solubility 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 $O(nL^2)$).

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 [**?**], 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 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 in the input lists has length of least 1 (this is sensible, since words of length 0 must be the identity, which is clearly conjugate to only the identity, 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 [**?**]. We will also assume that an ordering on the generators has been picked, so that the notion of a short-lex least representative 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 element 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 then use some of the result from [**?**], that is, the method of exhibiting some superset of the centraliser of an infinite order element as a cyclic group and a bounded set of coset representatives, and then for each representative, compute approximations of the length of each element of each list when raised to this representative multiplied by large powers of the cyclic generator.

By comparing these approximations we can find, for each representative, a range of possible powers of the cyclic generator such that the two lists could be conjugate and check only these powers. The number of possible powers is bounded by a constant depending only on the group, 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 2.1. *There is an algorithm, which given any list $A = [a_1, a_2, \ldots]$ of elements of G and $n \in \mathbb{N}$, will either find a $g \in G$ for which $|(a_i a_{i+1} \ldots a_n)^g| \leq (12L + 4\delta + 2)3^{n-i}$ 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 L is the total length of the first n elements in the list.*

Thus it is possible to simply precompute conjugacy of lists of "short" elements and to check our input against this. ([**?**] also gives an exponential time algorithm for solving conjugacy of lists of elements). 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.

3 Preliminaries

The notation $x\hat{y}z$ will be used for a geodesic triangle 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. If the geodesic is ambiguous, we will write $[xy]_\gamma$ to mean the path between x and y that is a sub-path of γ. 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 of words. 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 elements of the group (though referred to as points rather than elements), so for example 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 $\vec{pw}$.

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

In [**?**], a result by Shapiro is proved:

Lemma 3.1. *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 3.2. *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 either:*

$$d(p,x)+1 \geq d(p,y) \geq d(p,x)$$

Or:

$$d(p,y)+1 \geq d(p,x) \geq d(p,y)$$

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

If $w := a_1 a_2 \ldots a_k$, where each a_i is a generator, let $w(i) := a_1 a_2 \ldots a_i$. Also, let $w^\infty(i) := w^{\left\lfloor \frac{i}{|w|} \right\rfloor} w(i - |w| \left\lfloor \frac{i}{|w|} \right\rfloor)$ (defined on negative numbers, too, so if $w = abc$, $w^\infty(-2) = w^{-1}w(1) = c^{-1}b^{-1}$). We can also regard w^∞ as a two-way infinite path based at the identity simply by mapping $\mathbb{Z} \to \gamma : z \mapsto w^\infty(z)$.

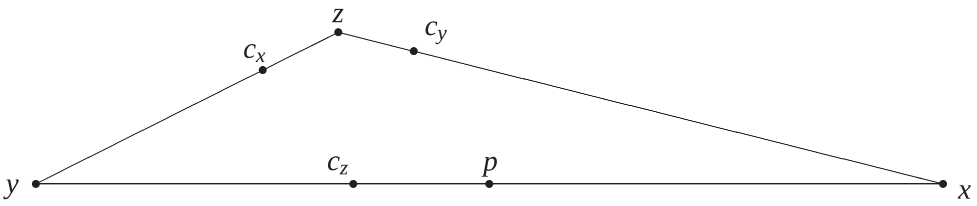
If $w := [xy]$, let p be the midpoint such that $|[xp]|$ is minimised. We write $w_L := [xp] = w(\left\lfloor \frac{|w|}{2} \right\rfloor)$, $w_R := [py] = w(\left\lfloor \frac{|w|}{2} \right\rfloor)^{-1} w$, and $w_C := \pi(w^{w_L}) = \pi(w_R w_L)$.

For example, suppose $w = abca^{-1}b^2a^{-1}$ is geodesic. Then $w_L = abc$, $w_R = a^{-1}b^2a^{-1}$ and $w_C =_G a^{-1}b^3c$.

Definition 3.3. *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 3.4. *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 $d(x,z) \geq d(y,z)$. Then clearly:

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

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

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

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 to allow us to multiply two elements in our lists.

Lemma 3.5. *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 $[b_1b_2,b_2,\ldots,b_n]$.*

In [**?**], 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 3.6. *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.

4 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 "long" elements using part of the method for solving the conjugacy problem for individual infinite order elements outlined in [**?**], which is summarised here:

Proposition 4.1. *There exist constants $N, P \in \mathbb{N}$ depending only on the group and presentation such that:*

For any short-lex straight element w, there exists a set $S \subset G$ with $|S| < N$ whose elements are of length at most $P|w|$, and an infinite order element $c \in G$ whose length is at most $P|w|$ such that every element of the centraliser of w_C can be expressed in the form sc^m for some $s \in S$ and $m \in \mathbb{Z}$.

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

It will turn out that in order to produce short-lex straight elements as some conjugate of some power of a 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 4.2. *Let $M := 16L^3V^3$. Then given any geodesic word $w \in G$ of infinite order with $|w| \leq 2L$, $|(\pi(w^M))_C| > 2L$.*

Proof. Note that by [**?**], we know the following (the actual 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 $\gamma(R+r)$ $\gamma'(R+r)$ 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 $e(\frac{D-e(0)}{2}) \geq 4D + 6\lambda D + \varepsilon$.

Now, consider the (λ, ε)-quasigeodesic γ given in the first result and pick D from the third result appropriately, and let x be 1, y be 1^{w^n} and z be $1^{w^{2n}}$ 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 1.

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

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

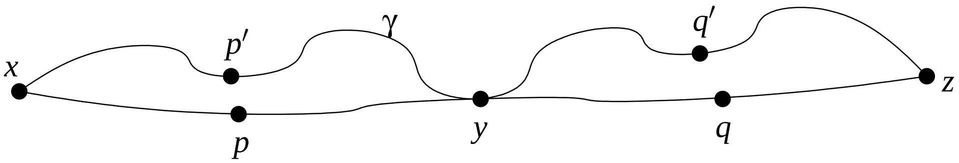


Figure 1: Cutting across a long quasigeodesic

Hence, if we take $n > \frac{\lambda(2L+2D+\varepsilon)}{|w|}$, it is clear that $d(p,q) = |(\pi(w^N))_C| > 2L$. We can get λ and ε from the third result, and a particular solution to the inequality in the third result (using the function from the second) is given by $D = \lceil 10\delta + 4\delta\log_2(4\delta(4+6\lambda)) + \frac{\varepsilon}{4+6\lambda} \rceil$. Now recall that $1 \leq |w| \leq 2L$ and expand the inequation for n:

$$\begin{aligned} n &> \left\lceil 2LN(2L+2(10\delta+4\delta\log_2(4\delta(4+12LN))+\frac{8L^2N^2+4LN}{4+12LN})+8L^2N^2+4LN) \right\rceil \\ &= \left\lceil 4LN(2\delta(13+2\log_2(\delta(1+3LN)))+L+8L^2N^2+4LN+\frac{2L^2N^2+LN}{1+3LN}) \right\rceil =: M' \end{aligned}$$

It is simply a matter of taking a number of approximations to see that $M' \leq 16L^3V^3$, hence we are done. □

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

Proposition 4.3. *There exist constants $N,P \in \mathbb{N}$ depending only on the group and presentation such that for any infinite order geodesic word w, there exists a set $S \subset G$ with $|S| < N$ 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 $sc^n p$ 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 $|w_C| \leq 2L$. Then, by Proposition 4.2 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 $|w_C| > 2L$ let $q' := 1$ and $m_1 := 1$. Then either way, letting $w'' := \pi((w^{q'})^{m_1})$, we have $|w''_C| > 2L$. Hence, by proposition 3.6, 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 $q_1 := q'w''_L a$, and $m_2 := m_1 m'_2$, so that $w' = \pi((w^{q_1})^{m_2})$. Clearly, $|q_1| \leq (MQ+1)|w| + 4\delta$ and $m_2 \leq MQ$.

Now let us apply Proposition 4.1 to w' to give us a c' which is not necessarily short-lex straight, along with a set S'. We can apply the method above to obtain a power m_3 and a word q_2 with similar bounds such that $c := \pi((c'^{q_2})^{m_3})$ is short-lex straight.

Now, suppose g is some element of the centraliser of w. Then $w'^{q_1^{-1}gq_1} =_G w'$, hence $q_1^{-1}gq_1$ is in the centraliser of w', thus $q_1^{-1}gq_1 =_G s'c'^k$ for some $s' \in S'$ and some integer k. Let $k = im_3 + j$ with i, j integers and $0 \leq j < m_3$. Now $g =_G q_1 s' c'^j c'^{im_3} q_1^{-1} =_G q_1 s' c'^j (c^{q_2^{-1}})^{m_3} q_1^{-1} =_G q_1 s' c'^j q_2 c^{m_3} q_2^{-1} q_1^{-1}$ so we can simply create a new set $S := \{q_1 s' c'^j q_2 : s \in S', 0 \leq j < m_3\}$ with $p := q_2^{-1} q_1^{-1}$.

Clearly, the elements of S have a length of at most $(MQ+1)|w| + 4\delta + P|w| + MQ((MQ+1)P|w| + 4\delta) + (MQ+1)P|w| + 4\delta$, which in particular is less than some $P'|w|$, where P' depends only on the group, and similarly $|c| \leq P'|w|$. Also, the set S has at most MQN elements. Hence we have the required bounds. Clearly, obtaining S and c can be done in time linear in $|w|$. □

Remark 4.4. *Note that as in [**?**] one can reduce the lengths of words produced by the above result by noting that (in the first paragraph) there might be power lower than m_2 of w, which when conjugated by q_1, is also short-lex straight. If this is the case, we can detect it by searching for w' as a substring of $(w')^2$. For instance, if $w' = a_1 a_2 \ldots a_i$ (for $i \in \mathbb{N}$ and a_j generators of G for $1 \leq j \leq i$) and there exists a $j \in \mathbb{N}$ such that $(w')^2 = a_1 a_2 \ldots a_j a_1 a_2 \ldots a_i a_{j+1} a_{j+2} \ldots a_i$ then $a_1 a_2 \ldots a_j$ is also short-lex straight. Also, it should be clear that $a_r = a_{r+j}$ for $1 \leq r \leq i - j$, hence j divides i and $w' = (w'(j))^{\frac{i}{j}}$. Let $h = \mathrm{hcf}\{\frac{i}{j}, m_2\}$, and we can replace w' with $w'(\frac{i}{h})$ and m_2 with $\frac{m_2}{h}$. (We must take the highest common factor to avoid getting fractional powers of a word, which is poorly defined - and regarless, the centraliser of $a^{\frac{1}{i}}$ is not generally a superset of a.) We can apply this in a similar way to c.*

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

Lemma 4.5. *Suppose that the points C, D, E and F have $d(C,D) = d(E,F)$. Define C geodesic quadrilateral as in Figure 2, and divide this quadrilateral into two triangles using a geodesic representing $\vec{CE}$, and that p_1 is the meeting point of the triangle $C\hat{D}E$ lying on $u := \vec{CD}$, and p_2 is the meeting point of the triangle $\triangle CEF$ lying on $v := \vec{FE}$. Let $K := |\vec{CD}| - |\vec{CE}|$, then any for $i \in \mathbb{Z}$ with $d(F, p_2) \leq i \leq d(p_1, D)$, we have $u(i\overrightarrow{)v}(i) =_G hv(i + \vec{K})v(i)$ 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 3. 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:

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

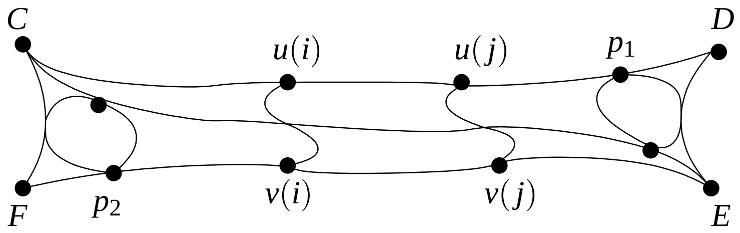


Figure 2: The thin section of C geodesic quadrilateral

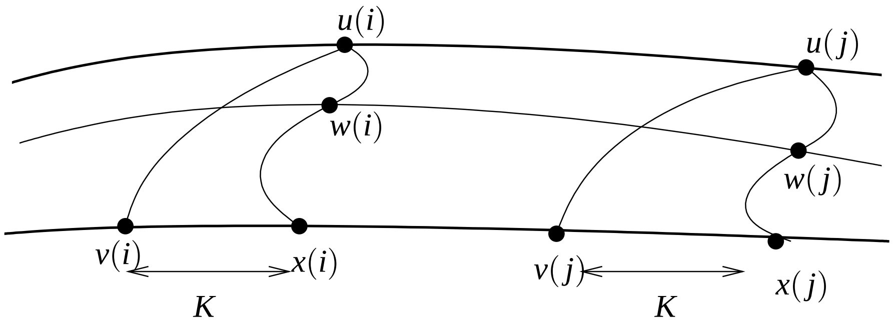


Figure 3: C part of figure 2

It should be clear that if $x(j)$ is closer to D 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 length at most 2δ, hence giving us h), then the path from $x(i)$ to $v(i)$ (which is $v(i-\vec{K})v(i)$) to get the result.

□

We now prove the following useful proposition:

Proposition 4.6. *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 $N := V + \left\lceil \frac{3|a|+8\delta}{2|g|} \right\rceil + 1$. 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

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

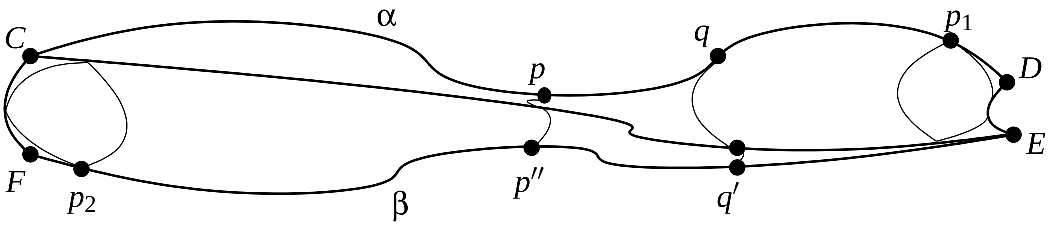


Figure 4: The geodesics α and β lie close.

- *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:*

$$a^{g^i} =_G h(g^{\infty}(K))^{-1}$$

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 $\vec{EF}$ being segments of α and β.

Lemma 4.5 clearly can be applied, so that letting $K' := 2|g|k - |g^k a g^k| = d(C,E) - d(C,D)$, we find that for any $i \in \mathbb{Z}$ such that $|i| < k - \left\lceil \frac{R}{|g|} \right\rceil$ (this means that g^i is definately between the meeting points, hence in the range given in Lemma 4.5), if we take $p := g^i$, $p' := ag^i$ and $p'' := ag^{\infty}|g|i - K'$, we have $a^{g^i} =_G \vec{pp'} =_G h\vec{p''p'} =_G h((g^{\infty}(K'))^{-}1$ for some word h such that $|h| \leq 2\delta$, hence we obey the inequation in the second case of the proposition for this (and hence any) bounded range. In particular, this means that there must be at most V distinct conjugates of the form a^{g^i} for $i \in \mathbb{Z}$. Also note if $a =_G h'(g^{\infty}(K'))^{-1}$, we have $a^{g^i} =_G h(g^{\infty}(-K'))^{-1} =_G hh'^{-1}h'(g^{\infty}(-K'))^{-1} = hh'^{-1}a$ - hence $|a^{g^i}| \leq |a| + 4\delta$ (we can thus take $R = 4\delta + |a| + 4\delta$).

Let $k := N$ as in the statement of this proposition. We must prove that the value of K given works for any power $i \in \mathbb{Z}$. Since the meeting point, p_1, must be within $|a| + 4\delta$ (ie. the longest possible value of a^{g^i} for any i) of g^k and, p_2, within $|a| + 4\delta$ of ag^{-k}, it is clear that there must be at least $2N - \left\lceil \frac{2|a|+8\delta}{|g|} \right\rceil \geq 2V + \frac{|a|}{|g|} + 1$ distinct $i \in \mathbb{Z}$ such that $|i| \leq k - \left\lceil \frac{|a|+4\delta}{|g|} \right\rceil$. The a^{g^i} cannot all be distinct 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

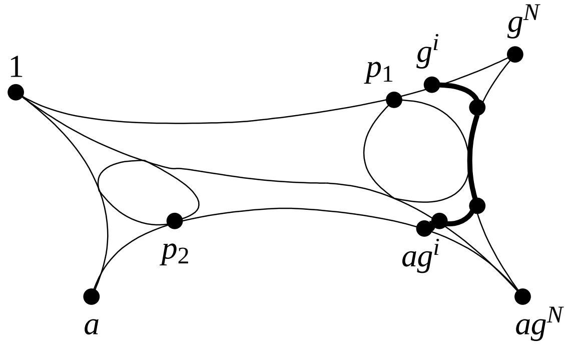


Figure 5: The end of the unbounded case

the length of conjugates is bounded, we must be in the second case.

Now suppose that the length of conjugates a^{g^i} for $i \in \mathbb{Z}$ is not bounded above. We'd like to show that this is equivalent to $|a^{g^N}| > |a| + 4\delta$ (thus putting us in the first case of the statement), and prove the inequalities which approximate the length of a conjugate for high powers.

Let us consider the geodesic quadrilateral with corners $C := 1$, $D := g^N$, $E := ag^N$ and $F := a$, 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). We will first prove that $|a^{g^N}| > |a| + 4\delta$. 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 5 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 5, 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 $|a^{g^N}| \geq |a^{g^k}| + 2|g|(N-k) - 3\delta \geq 2|g|(N-k) - 3\delta$, so our aim will be to show that $k < N - \frac{|a|+7\delta}{2|g|} \leq V + \frac{3|a|}{2|g|} + 1$. If this is true, then we have shown that $|a^{g^N}| > |a| + 4\delta$ - so that our means of distinguishing cases given in the statement is correct.

First suppose that $k_1 \leq |a|$ (note $k_2 \leq |a|$ is always true). Then it's clear that $k \leq \left\lceil \frac{|a|}{|g|} \right\rceil < V + \frac{3|a|}{2|g|} + 1$ as required.

So let's consider $|a| \leq k_1$. Once again, we can apply Lemma 4.5 and we find 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) once again have the form hw with w constant (as in the bounded case) and $|h| \leq 2\delta$. Hence in particular we have at most V distinct elements a^{g^i} with $k' \leq i < k$. Since if we ever get a repeated element we must have the whole sequence repeat (and

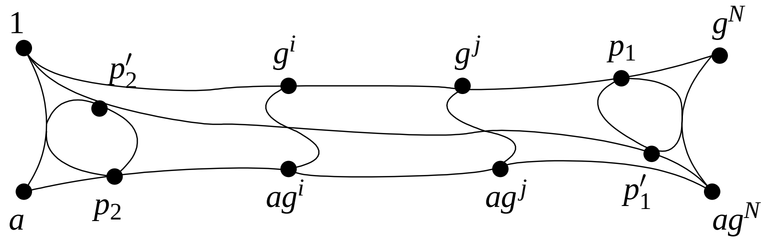


Figure 6: The midsection of the unbounded case, case 2

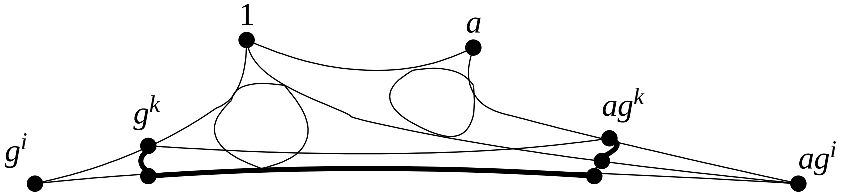


Figure 7: After the first section

thus, the length of conjugates a^{g^j} will be bounded), we must have $k-k' \leq V$. Now since $k' \leq \left\lceil \frac{|a|}{|g|} \right\rceil$, we must have $k < V + \frac{3|a|}{2|g|} + 1$, 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 7. (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: $K_1 = |ag^k| - |g|k$, $K_2 = |ag^{-k}| - |g|k$ (to see this, simply replace g with g^{-1} - which is clearly also a straight iword) - 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 [**?**]) and from Proposition 4.3, elements $c, p \in G$ such that c is straight along with a set S of size bounded by a constant depending only on the group and presentation so that every element in the centraliser of a_1 can be expressed in the form $sc^n p$ 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 $sc^n ph$. Hence, we need only search for elements of this form. For simplicity, let us replace B with $\pi(B^{(ph)^{-1}})$. Since the size of S is bounded by a constant that depends only on the group, we can iterate through its elements in constant time.

Now, suppose we are given some element $s \in S$. We will proceed through $i \in \{1,\ldots,m\}$ to find a bounded range of possible $g \in G$ which could be considered as candidates for conjugating elements. That is, for each $i \in \{1,\ldots,m\}$, we need to find a range of $k \in \mathbb{Z}$ which contains any k such that $a_i^{sc^k} = b_i$. By iterating over every $s \in S$, we aim to either eliminate or check every possible element of the centraliser. Let us apply Proposition 4.6 with $a = a_i^s$ and $g = c$ and with $a = b_i$ with $g = c$. Note that one only needs to apply Proposition 4.6 once for each b_i.

Clearly if the two elements result in different cases in the proposition then no k can exist such that $a_i^{sc^k} = b_i$, since if it did, for any $l \in \mathbb{Z}$ we have $a_i^{sc^{k+l}} = b_i^{c^l}$, 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 $K_{1a} := K_1(a_i^s, c)$ and $K_{1b} := K_1(b_i, c)$ 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 $a_i^{sc^k} =_G b_i$, then for all $l \in \mathbb{N}$, $a_i^{sc^{k+l}} = b_i^{c^l}$ so 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 these clearly bounded ranges, and we need to check at most 6δ elements $a_i^{sc^k}$ 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 under this power until one of them is equal to simply a_i^s. While we are doing this, we can also make a list M_i of each k such that $a_i^{sc^k} = b_i$. 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 $\operatorname{lcm}\{l_1,\ldots,l_m\} \leq V!$ 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 $0 \leq j \leq \mathrm{lcm}\{l_1, \ldots, l_m\}$ 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.

5 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 5.1.

```
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 $g \leftarrow a_j \ldots a_k$ and 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 5.
```

Proposition 5.2. *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 3.6) 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, $\mu_k := k + \sum_{i=1}^k |a_i|$). We add k to ensure $\mu_k \geq k$.

Let us briefly consider the change in length of c at step 3. Using Lemma 3.4 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 8 ($p = (\pi(a_k^c))_L$ 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

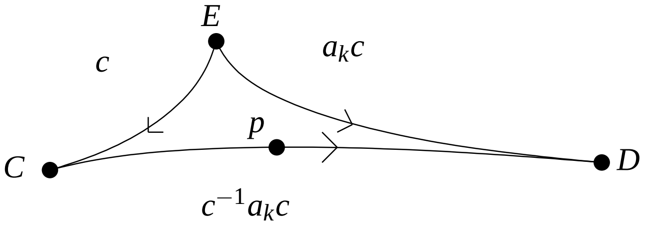


Figure 8: Extending c.

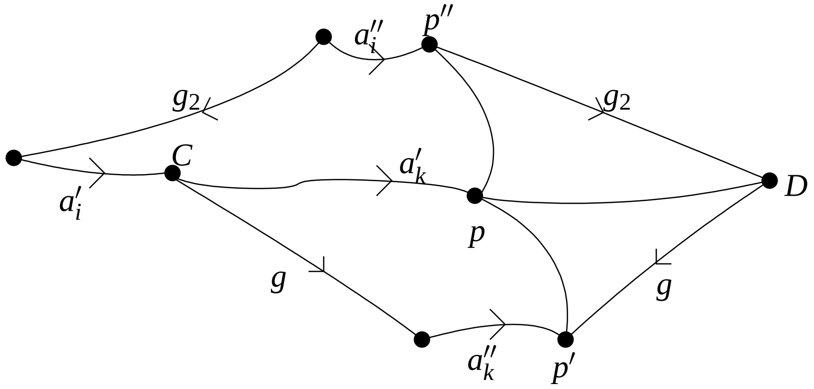


Figure 9: The conjugates of the a_i' are all short.

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 definately true for $k = 2$, since we will have $|a_1^c| = |(a_1)_C| \leq 2L$.)

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 3.6 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 3.6, 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 9 for any $i < k$.

Using Lemma 3.4, 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 $a_i'^{-1} g_2 a''_i$) 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 $(a_i \ldots a_k)^{cg} = (a'_i a'_k)^g = ((a'_i a'_k)^{g_2})^{g_2^{-1}g} = a_i''^{g_2^{-1}g}$. 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 $k=i$. 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 3.5, 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 $(a_1,\dots,a_n)$ for which $|a_i| \leq (12L+4\delta+2)3^{n-i}$ has been computed using the exponential algorithm given in [**?**]. 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 5.1 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 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 5.1 to B to get a conjugating element c' or infinite order element g.

5. If the above step gave an infinite order element $g = b_i\dots b_j$, then replace A with $[b_i\dots b_j, b_1,\dots,b_{i-1},b_{i+1},\dots,b_m]$ and similar for B (ie. the lists should now be swapped), then go to 8.

6. Otherwise, replace A with $[a_1\dots a_m, a_2\dots a_m,\dots,a_m]^c$ and replace B with $[b_1\dots b_m, b_2\dots b_m,\dots,b_m]^{c'}$.

7. Now test conjugacy of A and B using the precomputed list. If a conjugating element c is found, return gcg'^{-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 [**?**] to find a conjugating element h. If this does not exist, the lists are not conjugate, so stop.

9. Use Proposition 4.3 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 4.6 to $b_i^{(ph)^{-1}}$ and c for each $1 \leq i \leq m$.

11. For each $s \in S$, apply Proposition 4.6 to a_i^s and c.

12. If any i results in different cases for $b_i^{(ph)^{-1}}$ and a_i, move onto the next s.

13. If any i results in case 1 for both $b_i^{(ph)^{-1}}$ and a_i, use the bounds as given after Proposition 4.6 to search a bounded range of conjugates.

14. Otherwise, test the conjugacy using the bounded length search, as outlined after Proposition 4.6.

15. If any of the previous two steps result in a conjugating element, 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 $O(m^2\mu)$ and does not require our precomputation.