1-1-2011

Remnant inequalities and doubly-twisted conjugacy in free groups

Christopher P. Staecker
Fairfield University, cstaecker@fairfield.edu

Remnant inequalities and doubly-twisted conjugacy in free groups

P. Christopher Staecker*†‡§

April 30, 2011

Abstract

We give two results for computing doubly-twisted conjugacy relations in free groups with respect to homomorphisms φ and ψ such that certain remnant words from φ are longer than the images of generators under ψ.

Our first result is a remnant inequality condition which implies that two words u and v are not doubly-twisted conjugate. Further we show that if ψ is given and φ, u, and v are chosen at random, then the probability that u and v are not doubly-twisted conjugate is 1. In the particular case of singly-twisted conjugacy, this means that if φ, u, and v are chosen at random, then u and v are not in the same singly-twisted conjugacy class with probability 1.

Our second result generalizes Kim's "bounded solution length". We give an algorithm for deciding doubly-twisted conjugacy relations in the case where φ and ψ satisfy a similar remnant inequality. In the particular case of singly-twisted conjugacy, our algorithm suffices to decide any twisted conjugacy relation if φ has remnant words of length at least 2.

As a consequence of our generic properties we give an elementary proof of a recent result of Martino, Turner, and Ventura, that computes the densities of injective and surjective homomorphisms from one free group to another. We further compute the expected value of the density of the image of a homomorphism.

1 Introduction

Let G and H be finitely generated free groups, and $\varphi, \psi : G \to H$ be homomorphisms. The group H is partitioned into the set of *doubly-twisted conjugacy*

*Address: Department of Mathematics and Computer Science, Fairfield University, Fairfield CT

†Email: cstaecker@fairfield.edu

‡Keywords: Nielsen theory, coincidence theory, twisted conjugacy, doubly twisted conjugacy, asymptotic density

§MSC2000: 54H25, 20F10

classes as follows: $u, v \in H$ are in the same class (we write $[u] = [v]$) if and only if there is some $z \in G$ with

$$u = \varphi(z) v \psi(z)^{-1}.$$

Our principal motivation for studying doubly-twisted conjugacy is Nielsen coincidence theory (see [4] for a survey), the study of the coincidence set of a pair of mappings and the minimization of this set while the mappings are changed by homotopies. Our focus on free groups is motivated specifically by the problem of computing *Nielsen classes* of coincidence points for pairs of mappings $f, g : X \to Y$, where X and Y are compact surfaces with boundary.

A necessary condition for two coincidence points to be combined by a homotopy (thus reducing the total number of coincidence points) is that they belong to the same Nielsen class. (Much of this theory is a direct generalization of similar techniques in fixed point theory, see [8].) The number of "essential" Nielsen classes is called the Nielsen number, and is a lower bound for the minimal number of coincidence points when f and g are allowed to vary by homotopies.

On surfaces with boundary, deciding when two coincidence points are in the same Nielsen class is equivalent to solving a natural doubly-twisted conjugacy problem in the fundamental groups, using the induced homomorphisms given by the pair of mappings. Thus the Nielsen classes of coincidence points correspond to twisted conjugacy classes in $\pi_1(Y)$.

The problem of computing doubly-twisted conjugacy classes in free groups is nontrivial, even in the singly-twisted case which arises in fixed point theory, where φ is an endomorphism and ψ is the identity. An algorithm for the singly-twisted conjugacy decision problem where φ is an automorphism is given in [1]. Few techniques for computing doubly-twisted conjugacy in free groups are available. A generally applicable technique using abelian and nilpotent quotients is given in [13], but is it is hard to predict when it will be sucessful. A technique is given in [14] which can often show that two words are in different doubly-twisted conjugacy classes, but the hypotheses on the homomorphisms are quite strong.

Our methods are based on the combinatorial *remnant* condition for homomorphisms. Informally, a homomorphism φ has remnant if the images under φ of generators have limited cancellation when multiplied together. The noncancelling parts are called the remnant subwords.

If $\varphi, \psi : G \to H$ are homomorphisms and $u, v \in H$ are words, we consider the remnant subwords of φ which remain uncancelled even after making products with the words u and v themselves. If, in each generator a, this remnant subword is of length greater than or equal to the length of $\psi(a)$, then u and v are in different doubly-twisted conjugacy classes. This is shown in Section 3.

In Section 4 we present some improvements to recent work of Martino, Turner, and Ventura in [11] concerning the density of injective and surjective homomorphisms of free groups. Their paper shows that, when the rank of H is greater than 1, a homomorphism chosen at random will be injective but not surjective with probability 1. We give a new and more elementary proof of this

theorem, and strengthen the result concerning surjectivity by showing that the expected value of the density of the image subgroup of a random homomorphism is 0. We also treat the case when the rank of H is 1.

In Section 5 we consider only the traditional remnant subword (without making products with u and v). If this subword of $\varphi(a)$ is of length strictly greater than the length of $\psi(a)$ for each generator a, then we give an algorithm to decide whether or not u and v are in different doubly-twisted conjugacy classes. This result is a generalization of Kim's "bounded solution length" technique in [9], and was developed independently for singly-twisted conjugacy by Hart, Heath, and Keppelmann in [5].

In Sections 3 and 5 we show that, given a homomorphism ψ, the remnant inequality used in that section will hold with probability 1 when φ is chosen at random. This implies in Section 3 that if ψ is fixed and φ, u, and v are all chosen at random, then $[u] \neq [v]$ with probability 1. In Section 5 we show that if ψ is fixed and φ is chosen at random, then there is an algorithm to decide whether or not $[u] = [v]$ for any words u and v.

The techniques and algorithms described in this paper have been implemented for the computational algebra system GAP [3]. Source code and a user-friendly web based version are available for experimentation at the author's website.

The author would like to thank Robert F. Brown, Marlin Eby, and Philip Heath for helpful comments on this paper, and Armando Martino for bringing the reference [11] to our attention.

2 Generic remnant properties

Wagner, in [15], defined the remnant condition for free group endomorphisms which would become a key tool for several later techniques for computation of the Nielsen number in fixed point theory (the special case where ψ is the identity) for certain mappings on surfaces with boundary. Extensions of Wagner's technique have been made in [7] and [9], and for Nielsen periodic point theory in [6].

Wagner's definition of remnant extends to homomorphisms (not necessarily endomorphisms) of free groups as follows. Throughout, for a word $w \in H$, the reduced word length of w is denoted $|w|$.

Definition 1. Let H be a free group, and $t = (h_1, \ldots, h_n)$ a tuple of words of h. We say that t *has remnant* when, for each i, there is a nontrivial subword of h_i which does not cancel in any product of the form

$$h_j^{\alpha_j} h_i h_k^{\beta_k}$$

where $j, k \in \{1, \ldots, n\}$, with $\alpha_l, \beta_l \in \{-1, 0, 1\}$ for $l \neq i$ and $\alpha_i, \beta_i \in \{0, 1\}$. Each such noncanceling subword is called the remnant of h_i, denoted $\mathrm{Rem}_t\, h_i$.

The statement that a set of elements has remnant is closely related to the statement that it be Nielsen reduced (see e.g. [10]).

If G has generators $a_1, \ldots, a_n$, and $\varphi : G \to H$ is a homomorphism, then we say that φ *has remnant* if the tuple $(\varphi(a_1), \ldots, \varphi(a_n))$ has remnant in the above sense. In this case, the remnant of $\varphi(a_i)$ is denoted $\mathrm{Rem}_\varphi\, a_i$.

If φ has remnant, the *remnant length* of φ is the minimum length of $|\mathrm{Rem}_\varphi\, a_i|$ for any i.

Throughout this paper, the remnant condition is used typically as follows: we will have a homomorphism $\varphi : G \to H$ and some element $z \in G$ with reduced form $z = a_{j_1}^{\eta_1} \ldots a_{j_k}^{\eta_k}$. When φ has remnant, writing $X_i = \varphi(a_{j_i})^{\eta_i}$, we have the reduced product

$$\varphi(z) = X_1 \ldots X_k = R_1 \ldots R_k,$$

where R_i is the subword of X_i which does not cancel in the product $X_1 \ldots X_k$. Since φ has remnant, the right hand side will be fully reduced and $(\mathrm{Rem}_\varphi\, a_i)^{\eta_i}$ will be a subword of R_i for all i.

Use of the asymptotic density in the context of doubly-twisted conjugacy was presented in [14]. We will quote the relevant terms and results here.

For a free group G and a natural number p, let G_p be the subset of all words of length at most p. The *asymptotic density* (or simply *density*) of a subset $S \subset G$ is defined as

$$D(S) = \lim_{p \to \infty} \frac{|S \cap G_p|}{|G_p|},$$

where $|\cdot|$ denotes the cardinality. The set S is said to be *generic* if $D(S) = 1$.

Similarly, if $S \subset G^l$ is a set of l-tuples of elements of G, the asymptotic density of S is defined as

$$D(S) = \lim_{p \to \infty} \frac{|S \cap (G_p)^l|}{|(G_p)^l|},$$

and S is called *generic* if $D(S) = 1$.

A homomorphism on the free groups $G \to H$ with $G = \langle a_1, \ldots, a_n \rangle$ is equivalent combinatorially to an n-tuple of elements of G (the n elements are the words $\varphi(a_1), \ldots, \varphi(a_n)$). Thus the asymptotic density of a set of homorphisms can be defined in the same sense as above, viewing the set of homomorphisms as a collection of n-tuples.

A theorem of Robert F. Brown in [15] established that "most" endomorphisms have remnant. This is strengthened and made more specific in [14] as the following:

Lemma 2. *Let G and H be free groups with the rank of H greater than 1. Then for any natural number l, the set of homomorphisms $\varphi : G \to H$ with remnant length at least l is generic.*

3 The density of non-conjugate pairs

Given a homomorphism $\varphi : G \to H$ and two elements $u, v \in H$, there is a natural homomorphism $\varphi * u * v : G * \mathbb{Z} * \mathbb{Z} \to H$, (where $*$ denotes the free

product) defined as follows: let $G = \langle a_1, \ldots, a_n \rangle$, write b_1 as the generator of the first $\mathbb{Z}$ factor, and b_2 as the generator of the second $\mathbb{Z}$ factor. We then define $\varphi * u * v$ on each factor by

$$\varphi * g * h : \begin{array}{ccc} a_i & \mapsto & \varphi(a_i) \\ b_1 & \mapsto & u \\ b_2 & \mapsto & v \end{array}$$

The basic idea of the present theorem is inspired by the nice proof of Wagner's theorem given in [9].

Theorem 3. *Let the rank of H be greater than 1, let $\varphi, \psi : G \to H$ be homomorphisms, and let $u, v \in H$. Let $\overline{\varphi} = \varphi * u * v$. If $\overline{\varphi}$ has remnant with*

$$|\operatorname{Rem}_{\overline{\varphi}} a| \geq |\psi(a)|$$

for all generators $a \in G$, then $[u] \neq [v]$.

Proof. For the sake of a contradiction we assume that $[u] = [v]$, and so there is some $z \in G$ with

$$\psi(z) = u^{-1}\varphi(z)v. \tag{1}$$

Express z as the reduced word

$$z = a_{j_i}^{\eta_i} \ldots a_{j_k}^{\eta_k},$$

where a_{j_i} are generators of G and $\eta_i \in \{-1, 1\}$, and write the images of the generators as the reduced words $X_i = \varphi(a_{j_i}^{\eta_i})$ and $Y_i = \psi(a_{j_i}^{\eta_i})$.

We first write

$$u^{-1}\varphi(z)v = u^{-1}X_1 \ldots X_k v = R_u R_1 \ldots R_k R_v,$$

where the right hand side is reduced, R_i is the subword of X_i which does not cancel in the above, and R_u and R_v are the subwords of u^{-1} and v which do not cancel in the above. Because $\overline{\varphi}$ has remnant, we know that R_u and R_v are nontrivial, and R_i contains $(\operatorname{Rem}_{\overline{\varphi}} a_{j_i})^{\eta_i}$ as a subword.

Then we have

$$\begin{aligned} |u^{-1}\varphi(z)v| &= |R_u| + |R_v| + \sum_{i=1}^{k} |R_i| \\ &\geq |R_u| + |R_v| + \sum_{i=1}^{k} |\operatorname{Rem}_{\overline{\varphi}} a_{j_i}| \\ &> \sum_{i=1}^{k} |\operatorname{Rem}_{\overline{\varphi}} a_{j_i}| \geq \sum_{i=1}^{k} |Y_i| \geq |\psi(z)|, \end{aligned}$$

and the strict inequality contradicts (1). ∎

The above theorem is similar to the result of [14] that $[u] \neq [v]$ when $\varphi * \psi * (uv^{-1})$ has remnant. The fact that we require no remnant condition of ψ allows our result, unlike that of [14], to be specialized to the case of singly-twisted conjugacy:

Corollary 4. *For an endomorphism $\varphi : G \to G$, let $[u]$ denote the singly-twisted conjugacy class of u.*

If $\varphi * u * v$ has remnant, then $[u] \neq [v]$.

We now note that Theorem 3 will generically apply for a particular ψ when φ, u, and v are chosen at random. This result is a strengthening of the final Theorem of [14] using different methods.

Theorem 5. *Let the rank of H be greater than 1, and let $\psi : G \to H$ be any homomorphism. Then (again letting $[u]$ denote the doubly-twisted conjugacy class with respect to φ and ψ) the set*

$$S = \{(\varphi, u, v) \mid [u] \neq [v]\}$$

is generic.

Proof. Letting n be the number of generators of G, we may view a triple (φ, u, v) as a $(n+2)$-tuple of elments of H (since a choice of φ is combinatorially equivalent to a choice of the n image words in H). Thus we view S as a subset of the cartesian product H^{n+2}.

Let k be the maximum length of any $|\psi(a_i)|$. Then by Theorem 3 we have

$$\begin{aligned} S &= \{t = (\varphi(a_1), \ldots, \varphi(a_n), u, v) \mid [u] \neq [v]\} \supset \{t \in H^{n+2} \mid t \text{ has remnant length at least } k\} \\ &= \{\rho : F_{n+2} \to H \mid \rho \text{ has remnant length at least } k\} \end{aligned}$$

and by Lemma 2 this set is generic. □

Since ψ above is allowed to be any homomorphism, the special cases where ψ is the identity homomorphism and the trivial homomorphism give:

Corollary 6. *Let G and H be free groups with the rank of H greater than 1.*

- *If $G = H$ and $[u]$ denotes the singly-twisted conjugacy class of $u \in G$ with respect to an endomorphism $\varphi : G \to G$, then the set*

  $$\{(\varphi, u, v) \mid [u] \neq [v]\}$$

  is generic.

- *For homomorphisms $\varphi : G \to H$, the set*

  $$\{(\varphi, u, v) \mid uv^{-1} \notin \varphi(G)\}$$

  is generic.

Proof. The first statement follows directly from Theorem 5 letting ψ be the identity. For the second statement, let ψ be the trivial homomorphism. Then $[u] = [v]$ if and only if $u = \varphi(z)v$, which is to say that $uv^{-1} \in \varphi(G)$. □

4 The densities of injections and surjections

From the second statement of Corollary 6, together with Lemma 2, we obtain an alternative (and easier) proof of a recent result by Martino, Turner, and Ventura in [11] concerning the densities of injective and surjective homomorphisms of free groups. The preprint [11] addresses only the second statement below:

Theorem 7. *Given free groups G and H, let* $\mathrm{Epi}(G,H)$ *and* $\mathrm{Mono}(G,H)$ *be the sets of all surjective and injective homomorphisms $G \to H$, respectively.*

1. *If the rank of H is 1 and the rank of G is $n > 1$, then*

$$D(\mathrm{Epi}(G,H)) = \frac{1}{\zeta(n)}, \quad D(\mathrm{Mono}(G,H)) = 0,$$

   where $\zeta(n)$ is the Reimann zeta function. (Note that $\zeta(n) \to 1$ as $n \to \infty$.)

2. *If the ranks of G and H are both 1, or the rank of H is greater than 1, then*

$$D(\mathrm{Epi}(G,H)) = 0, \quad D(\mathrm{Mono}(G,H)) = 1.$$

Proof. Let G have generators $a_1, \ldots, a_n$.

Statement 1 concerns homomorphisms $G \to \mathbb{Z}$, each of which is equivalent to a choice of n integers (where $n > 1$). Let a homomorphism φ be given by integers $m_1, \ldots, m_n$. Then φ is never injective: if $\varphi(a_1) = m_1$ and $\varphi(a_2) = m_2$, then $\varphi(a_1^{m_2}) = m_1 m_2 = \varphi(a_2^{m_1})$. Thus $\mathrm{Mono}(G,H)$ is empty, and so $D(\mathrm{Mono}(G,H)) = 0$.

The homomorphism φ is surjective if and only if there are integers $k_1, \ldots, k_n$ with

$$k_1 m_1 + \cdots + k_n m_n = 1.$$

This in turn is equivalent to requiring that $\gcd(m_1, \ldots, m_n) = 1$, since the gcd is the smallest positive integer which is an integral linear combination of $m_1, \ldots, m_n$. It is known that the probability (in the appropriate asymptotic sense) of n randomly chosen integers being coprime is $1/\zeta(n)$, see [12]. Thus $D(\mathrm{Epi}(G,H)) = 1/\zeta(n)$.

Now we prove statement 2, first in the case where the ranks of G and H are both 1. We may consider both G and H to be the integers $\mathbb{Z}$. In this case, a homomorphism is equivalent to a choice of a single integer (the degree of the homomorphism). The homomorphism will be surjective if and only if the degree is ± 1, and will be injective if and only if the degree is nonzero. The desired densities follow.

Now we prove the case where the rank of H is greater than 1. We first note that any homomorphism $\varphi : G \to H$ with remnant is injective: If some φ with remnant were not injective, then there would be words $x, y \in G$ with

$$\varphi(x)\varphi(y)^{-1} = 1.$$

But writing the above in terms of generators will show that the above product cannot cancel, since the remnants will remain. Since the homomorphisms with remnant have density 1 by Lemma 2, we have $D(\mathrm{Mono}(G,H)) = 1$.

The statement concerning $\mathrm{Epi}(G,H)$ is implied by the second statement of Corollary 6. Let S be the set of triples (φ, u, v) with $uv^{-1} \notin \varphi(G)$, and Corollary 6 says that $D(S) = 1$. Let T be the set of non-surjective homomorphisms $G \to H$. Certainly S is a subset of $T \times H \times H$, and it is easy to check that $D(A \times H) = D(A)$ for any set A. Thus we have

$$D(\mathrm{Epi}(G,H)) = 1 - D(T) = 1 - D(T \times H \times H) \leq 1 - D(S) = 0.$$

□

The second statement of Corollary 6 suggests that a much stronger statement concerning surjective homomorphisms may be possible. In the case where H has rank greater than 1, we have shown that the image set $\varphi(G)$ is a proper subset of H with probability 1. We wish to give a more specific measure of the generic size of the subset $\varphi(G) \subset H$.

Let $\mathrm{ED}(G,H)$ be the *expected value* of $D(\varphi(G))$, which we define as follows:

$$\mathrm{ED}(G,H) = \lim_{p\to\infty} \frac{1}{|H_p|^n} \sum_{\varphi \in (H_p)^n} D(\varphi(G)),$$

where n is the number of generators of G, so we regard a homomorphism $\varphi : G \to H$ as an element of H^n.

This expected value is related to $D(\mathrm{Epi}(G,H))$ as follows: a surjection φ has $D(\varphi(G)) = 1$, and so, letting $E_p = \mathrm{Epi}(G,H) \cap (H_p)^n$, we have

$$\mathrm{ED}(G,H) \geq \lim_{p\to\infty} \frac{1}{|H_p|^n} \sum_{\varphi \in E_p} 1 = \lim_{p\to\infty} \frac{|E_p|}{|H_p|^n} = D(\mathrm{Epi}(G,H)).$$

Thus Theorem 7 shows that if H has rank 1 and the rank of G is $n > 1$, then $\mathrm{ED}(G,H) \geq 1/\zeta(n)$. Theorem 7 gives no information in the case where H has rank greater than 1, since it would only imply that $\mathrm{ED}(G,H) \geq 0$, which is already clear. Our goal for the remainder of the section is to compute the precise value of $\mathrm{ED}(G,H)$. We rely on a lemma which estimates $D(\varphi(G))$ when φ has remnant.

Lemma 8. *Let $\varphi : G \to H$ be a homomorphism with remnant length l, and let $n > 1$ be the number of generators of H. Then*

$$D(\varphi(G)) \leq 16n(2n-1)^{\lceil l/2 \rceil}.$$

Proof. If φ does not have remnant, then $l = 0$ and the statement to be proved is $D(\varphi(G)) \leq 16n$, which is always the case. Thus we assume that φ has remnant, and so $l > 0$.

If $w \in \varphi(G)$, then there is some z with $w\varphi(z) = 1$. Thus if $w \in \varphi(G)$, then $\varphi * w$ does not have remnant. Letting

$$S = \{w \mid \varphi * w \text{ does not have remnant}\},$$

we have $\varphi(G) \subset S$. We will give an upper bound on $D(S)$, which will imply an upper bound on $D(\varphi(G))$.

Let G have generators $a_1, \ldots, a_n$, and let u_i and v_i be the subwords of $\varphi(a_i)$ respectively "before" and "after" the remnant subword. That is, we can write $\varphi(a_i)$ as

$$\varphi(a_i) = u_i r_i v_i,$$

where $r_i = \mathrm{Rem}_\varphi\, a_i$, and the product $u_i r_i v_i$ is reduced (allowing perhaps u_i and v_i to be trivial). Write $r_i = s_i t_i$, where $|s_i|$ and $|t_i|$ are at most $\lceil |r_i|/2 \rceil \geq \lceil l/2 \rceil$. For brevity below, write $k = \lceil l/2 \rceil$.

In order for $\varphi * w$ to have no remnant, some initial subword of w or w^{-1} must equal one of the words $u_i s_i$ or $(t_i v_i)^{-1}$, or some terminal subword of w or w^{-1} must equal $(u_i s_i)^{-1}$ or $t_i v_i$. (Note that all of these words have length greater than k.)

If x is a word of length $m < p$, the number of words w of length p having x as the initial subword is $(2n-1)^{p-m}$, since the first m letters of w are fixed, and the remaining $p - m$ letters can be any letter of H except the inverse of the previous. Thus the number of words w having $u_i s_i$ as the initial subword is $(2n-1)^{p-|u_i s_i|} \leq (2n-1)^{p-k}$. Similarly the number of words w of length p having $(t_i v_i)^{-1}$ as the initial subword is at most $(2n-1)^{p-k}$, and the number of words w having $(u_i s_i)^{-1}$ as the terminal subword and the number of words w having $t_i v_i$ as the terminal subword are at most $(2n-1)^{p-k}$. Since there are n possible values for i, and we must allow for words w^{-1} with each of the above 4 constraints, we have

$$|S \cap H_p| \leq 8n(2n-1)^{p-k},$$

and thus

$$D(S) \leq \lim_{p\to\infty} 8n \frac{(2n-1)^{p-k}}{|H_p|} \tag{2}$$

For $i > 0$, the number of words of length exactly i is $2n(2n-1)^{i-1}$, since the first letter can be any letter of H, while each subsequent letter can be anything but the inverse of the previous. Summing gives the formula

$$|H_p| = 1 + \sum_{i=1}^{p} 2n(2n-1)^{i-1} = \frac{n(2n-1)^p - 1}{n-1}$$

and thus we have

$$\frac{(2n-1)^{p-k}}{|H_p|} = \frac{(n-1)(2n-1)^{p-k}}{n(2n-1)^p - 1} \leq 2\frac{(n-1)(2n-1)^{p-k}}{n(2n-1)^p} \leq 2(2n-1)^{-k}.$$

Then (2) becomes

$$D(S) \leq 16n(2n-1)^{-k},$$

and the fact that $\varphi(G) \subset S$ gives the desired result. □

We now make the computation of the expected value.

Theorem 9. *Let G and H be free groups.*

1. *If the rank of H is 1 and the rank of G is $n > 1$, then*

$$\mathrm{ED}(G, H) = \frac{\zeta(n+1)}{\zeta(n)}$$

2. *If the ranks of G and H are both 1, or if the rank of H is greater than 1, then*

$$\mathrm{ED}(G, H) = 0.$$

Proof. We begin with the first statement, which concerns homomorphisms $G \to \mathbb{Z}$, each of which is equivalent to a choice of n integers (with $n > 1$). If φ is given by the tuple of integers $\mathbf{t} = (m_1, \ldots, m_n)$, then $\varphi(G)$ is equal to the set $d\mathbb{Z}$, the integer multiples of d, where $d = \gcd(\mathbf{t})$. This set has density $1/\gcd(\mathbf{t})$. Thus we have:

$$\mathrm{ED}(G, \mathbb{Z}) = \lim_{p\to\infty} \frac{1}{|H_p|^n} \sum_{\mathbf{t}\in(H_p)^n} \frac{1}{\gcd(\mathbf{t})}$$

Thus $\mathrm{ED}(G, \mathbb{Z})$ is equal to the expected value of the reciprocal of the gcd function when applied to n arguments. A standard rearrangement expresses this expected value as a series:

$$\begin{aligned}
\mathrm{ED}(G, \mathbb{Z}) &= \lim_{p\to\infty} \frac{1}{|H_p|^n} \sum_{\mathbf{t}\in(H_p)^n} \frac{1}{\gcd(\mathbf{t})} \\
&= \lim_{p\to\infty} \frac{1}{|H_p|^n} \sum_{d=1}^{p} \frac{1}{d} |\{\mathbf{t} \in (H_p)^n \mid \gcd(\mathbf{t}) = d\}| \\
&= \sum_{d=1}^{\infty} \frac{1}{d} \lim_{p\to\infty} \frac{1}{|H_p|^n} |\{\mathbf{t} \in (H_p)^n \mid \gcd(\mathbf{t}) = d\}|,
\end{aligned}$$

where the exchanging of the limit and the sum is valid provided that the inner limit exists and is finite. The inner limit can be interpreted as the probability (in the appropriate asymptotic sense) that a random n-tuple has gcd equal to d. This probability is known to be equal to $d^{-n}/\zeta(n)$ (see equation 5.1 of [2]). This gives

$$\mathrm{ED}(G, \mathbb{Z}) = \sum_{d=1}^{\infty} \frac{d^{-1-n}}{\zeta(n)} = \frac{1}{\zeta(n)} \sum_{d=1}^{\infty} \frac{1}{d^{n+1}} = \frac{\zeta(n+1)}{\zeta(n)}$$

where the last equality is the definition of $\zeta(n+1)$.

Now we prove the second statement. First we treat the case where G and H are rank 1. Then we will write $G = H = \mathbb{Z}$, and a homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ is

equivalent to a single integer (the degree of φ). Writing $\varphi \in \mathbb{Z}$ as this integer, we have

$$\mathrm{ED}(\mathbb{Z}, \mathbb{Z}) = \lim_{p\to\infty} \frac{1}{2p+1} \sum_{\varphi=-p}^{p} D(\varphi(\mathbb{Z})).$$

If φ is the homomorphism given by multiplication by k, then the image $\varphi(\mathbb{Z})$ is the set $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$, which has density $1/|k|$. Thus the above becomes

$$\mathrm{ED}(\mathbb{Z}, \mathbb{Z}) = \lim_{p\to\infty} \frac{1}{2p+1} 2 \sum_{k=1}^{p} \frac{1}{k}.$$

(We have dropped the $k = 0$ term, since the image of the trivial homomorphism has density 0.) It is routine to verify that the above limit exists and equals 0.

Now we prove the case where the rank of H is greater than 1. Let R_l be the set of all homomorphisms $\varphi : G \to H$ with remnant length at least l. By Lemma 2 this set is generic.

Let n be the rank of G, and let l be any natural number. Then, using Lemma 8, we have

$$\begin{aligned}
\mathrm{ED}(G, H) &= \lim_{p\to\infty} \frac{1}{|H_p|^n} \left(\sum_{\varphi \in R_l \cap (H_p)^n} D(\varphi(G)) + \sum_{\varphi \in (H_p)^n - R_l} D(\varphi(G)) \right) \\
&\leq \lim_{p\to\infty} \frac{1}{|H_p|^n} \left(\sum_{\varphi \in R_l \cap (H_p)^n} 16n(2n-1)^{-\lceil l/2 \rceil} + \sum_{\varphi \in (H_p)^n - R_l} 1 \right) \\
&= \lim_{p\to\infty} 16n(2n-1)^{-\lceil l/2 \rceil} \frac{|R_l \cap (H_p)^n|}{|H_p|^n} + \frac{|(H_p)^n - R_l|}{|H_p|^n}
\end{aligned}$$

In the limit as $p \to \infty$, the first fraction converges to the density of R_l, which is 1, and the second converges to the density of its complement, which is 0. Thus we have

$$\mathrm{ED}(G, H) \leq 16n(2n-1)^{-\lceil l/2 \rceil},$$

and since l is any natural number, we have $\mathrm{ED}(G, H) = 0$. □

5 Bounded solution length

In this section we show that a remnant inequality similar to the one in Theorem 3 implies an algorithm for deciding doubly-twisted conjugacy relations.

Definition 10. Given homomorphisms $\varphi, \psi : G \to H$ and a pair of group elements $u, v \in H$, we say that the pair (u, v) has *bounded solution length* (or *BSL*) if there is some $k > 0$ such that the equation $u = \varphi(z) v \psi(z)^{-1}$ is satisfied (if at all) only if $|z| \leq k$. The smallest such k is called the *solution bound* (or *SB*) for (u, v).

Our casting of the *BSL* condition generalizes the concept for singly-twisted conjugacy of the same name in [9], where $G = H$ and ψ is assumed to be the identity homomorphism. (Kim works in the setting where the words u and v are always taken to be "Wagner tails" of φ which are not indirectly related in Wagner's algorithm. We omit this distinction so that the *BSL* condition can be defined without any reference to the set of Wagner tails.)

Our main theorem in this section is that if φ and ψ satisfy a remnant condition similar to the condition in Theorem 3 then any pair (u, v) will have *BSL* with a predictable solution bound. This implies an algorithm for deciding doubly-twisted conjugacy relations between any elements.

The following theorem was independently proved in the setting of singly-twisted conjugacy by Hart, Heath, and Keppelmann in [5] using essentially the same argument. Their solution bound was better than the one initially discovered by this author, and has been incorporated into the proof below.

Theorem 11. *Let $\varphi, \psi : G \to H$ be homomorphisms, such that*

$$|\operatorname{Rem}_\varphi a_i| > |\psi(a_i)|$$

for each generator $a_i \in G$. Let $l = \min_i(|\operatorname{Rem}_\varphi a_i| - |\psi(a_i)|)$. Then any pair (u, v) has BSL*, with solution bound*

$$\mathrm{SB} \leq \frac{|u| + |v|}{l}.$$

Proof. Let $u, v \in H$, and let $z \in G$ be a word of length k. To show that (u, v) has *BSL*, we will show that for k sufficiently large, we have $\psi(z) \neq u^{-1}\varphi(z)v$.

As in the proof of Theorem 3, write z as the reduced word $z = a_{j_1}^{\eta_1} \dots a_{j_k}^{\eta_k}$, where each a_j is a generator of G and each $\eta_i = \pm 1$. Let $X_i = \varphi(a_{j_i}^{\eta_i})$ and $Y_i = \psi(a_{j_i}^{\eta_i})$, then we have

$$u^{-1}\varphi(z)v = u^{-1}X_1 \dots X_k v.$$

Since φ has remnant, we can use notation as in the proof of Theorem 3 (though this time not worrying about u^{-1} and v) to write this product as

$$u^{-1}\varphi(z)v = u^{-1}R_1 \dots R_k v,$$

where each R_i is a subword of X_i with $|R_i| \geq |\operatorname{Rem}_\varphi a_{j_i}|$, and no cancellation occurs in any $R_i R_{i+1}$.

Now we will show that $\psi(z) \neq u^{-1}\varphi(z)v$ by showing that these two words

are of different lengths for sufficiently large k. We have

$$\begin{aligned}
|u^{-1}\varphi(z)v| - |\psi(z)| &= |u^{-1}R_1 \dots R_k v| - |Y_1 \dots Y_k| \\
&\geq |R_1 \dots R_k| - |u| - |v| - |Y_1 \dots Y_k| \\
&= -|u| - |v| + \left(\sum_{i=1}^{k} |R_i| \right) - |Y_1 \dots Y_k| \\
&\geq -|u| - |v| + \sum_{i=1}^{k} (|R_i| - |Y_i|) \\
&\geq -|u| - |v| + \sum_{i=1}^{k} (|\operatorname{Rem}_\varphi a_{j_i}| - |Y_i|) .
\end{aligned}$$

By the hypothesis to our theorem, we know that $|\operatorname{Rem}_\varphi a| - |\psi(a)| \geq l$ for every generator $a \in G$. Therefore the above inequalies give

$$|u^{-1}\varphi(z)v| - |\psi(z)| \geq kl - |u| - |v|,$$

and we can choose k sufficiently large so that $|u^{-1}\varphi(z)v| - |\psi(z)|$ is greater than zero. In particular it suffices to choose

$$k > \frac{|u| + |v|}{l}$$

which is the desired solution bound. □

Theorem 11 implies (subject to the remnant hypotheses) that, given any elements $u, v \in H$, we can algorithmically determine whether or not $[u] = [v]$: check for equality of $u = \varphi(z)v\psi(z)^{-1}$ where z ranges over all elements of G with $|z| \leq \frac{|u|+|v|}{l}$.

Example 12. Let us consider the pair of homomorphisms on the free group with two generators:

$$\varphi : \begin{array}{ccc} a & \mapsto & baba^2 \\ b & \mapsto & a^2b^{-1}ab^3 \end{array} \qquad \psi : \begin{array}{ccc} a & \mapsto & b^{-2} \\ b & \mapsto & a \end{array}$$

We will compare the two classes $[bab]$ and $[b^4a^2]$. (Neither Theorem 3 nor the result of [14] will suffice to make the comparison.) It is easy to verify that the hypotheses of Theorem 11 are satisfied with $l = 3$. Thus, if there is some z with

$$\psi(z) = bab\varphi(z)(b^4a^2)^{-1},$$

then it must be the case that $|z| \leq \frac{|bab|+|b^4a^2|}{3} = 3$.

It suffices to check all elements z of length at most 3 in the above equation. Such a check is performed easily by computer, and reveals that no element z of length at most 3 satisfies the equation. Thus $[bab] \neq [b^4a^2]$.

This gives new and useful algebraic decision algorithms, even in the cases where ψ is taken to be the identity or the trivial homomorphism:

Corollary 13. *Let G and H be finitely generated free groups.*

1. *(Doubly-twisted version) If $\varphi, \psi : G \to H$ are homomorphisms with $|\operatorname{Rem}_\varphi a| > |\psi(a)|$ for every generator $a \in G$, then there is an algorithm to decide whether or not there is some z with*

$$u = \varphi(z) v \psi(z)^{-1}$$

   for any $u, v \in H$.

2. *(Singly-twisted version) If $\varphi : G \to G$ is a homomorphism with $|\operatorname{Rem}_\varphi a| > 1$ for every generator $a \in G$, then there is an algorithm to decide whether or not there is some z with*

$$v = \varphi(z) u z^{-1}$$

   for any $u, v \in H$. (This same algorithm is obtained independently by Hart, Heath, and Keppelmann in [5].)

3. *($\psi = 1$ version) If $\varphi : G \to H$ is a homomorphism with remnant, then there is an algorithm to decide whether or not*

$$w \in \varphi(G)$$

   for any $w \in H$.

The third statement is obtained from the first by letting ψ be the trivial homomorphism, v the trivial element, and $u = w$.

We note that in Theorem 11, the statement that (u, v) has *BSL* over any finite set is a direct generalization of Kim's Theorem 4.7 of [9]. If we let ψ be the identity homomorphism, then our hypothesis is that, for all generators $a \in G$, we have $|\operatorname{Rem}_\varphi(a)| > |a| = 1$, which is to say that $|\operatorname{Rem}_\varphi(a)| \geq 2$. This is precisely the hypothesis used in Kim's Theorem 4.7 to show that any pair of Wagner tails has *BSL*. Kim's focus on the set of Wagner tails allows his solution bound to be more specific than ours (Kim shows that $SB \leq 4$ in all cases).

We conclude by noting that for a particular choice of homomorphism ψ, the remnant hypothesis for Theorem 11 is satisfied for generic φ. Letting l be the maximum length of $\psi(a)$ for any generator $a \in G$, Lemma 2 shows that

$$\{\varphi \mid |\operatorname{Rem}_\varphi a| > |\psi(a)| \text{ for any generator } a \in G\}$$

is generic.

References

[1] O. Bogopolski, A. Martino, O. Maslakova, and E. Ventura. Free-by-cyclic groups have solvable conjugacy problem. *Bulletin of the London Mathematical Society*, 38:787–794, 2006.

[2] J. Chidambaraswamy and R. Sitarmachandrarao. On the probability that the values of m polynomials have a given g.c.d. *Journal of Number Theory*, 26:237–245, 1987.

[3] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[4] D. L. Gonçalves. Coincidence theory. In R.F. Brown, editor, *The Handbook of Topological Fixed Point Theory*, pages 3–42. Springer, 2005.

[5] E. Hart, P. Heath, and E. Keppelmann. An algorithm for Nielsen type periodic numbers of maps with remnant on surfaces with boundary and on bouquets of circles II. In preparation.

[6] E. Hart, P. Heath, and E. Keppelmann. Algorithms for Nielsen type periodic numbers of maps with remnant on surfaces with boundary and on bouquets of circles I. *Fundamenta Mathematicae*, 200:101–132, 2008.

[7] E. Hart and S. Kim. The Nielsen number for free fundamental groups and maps without remnant. *Journal of Fixed Point Theory and Applications*, 2:261–275, 2007.

[8] B. Jiang. *Lectures on Nielsen fixed point theory*. Contemporary Mathematics 14, American Mathematical Society, 1983.

[9] S. Kim. Computation of Nielsen numbers for maps of compact surfaces with boundary. *Journal of Pure and Applied Algebra*, 208:467–479, 2007.

[10] R. Lyndon and P. Schupp. *Combinatorial Group Theory*. Springer, 1977.

[11] A. Martino, E. C. Turner, and E. Ventura. The density of injective endomorphisms of a free group. Preprint, 2008.

[12] J. E. Nymann. On the probability that k positive integers are relatively prime. *Journal of Number Theory*, 4:469–473, 1972.

[13] P. C. Staecker. Computing twisted conjugacy classes in free groups using nilpotent quotients. 2007. arxiv eprint 0709.4407.

[14] P. C. Staecker. Typical elements in free groups are in different doubly-twisted conjugacy classes. 2009. arxiv eprint 0808.0277.

[15] J. Wagner. An algorithm for calculating the Nielsen number on surfaces with boundary. *Transactions of the American Mathematical Society*, 351:41–62, 1999.