Clusters, Currents, and Whitehead's Algorithm

Ilya Kapovich

CONTENTS

Using geodesic currents, we provide a theoretical justification for some of the experimental results obtained by Haralick, Miasnikov, and Myasnikov via pattern-recognition methods regarding the behavior of Whitehead's algorithm on nonminimal inputs. In particular, we prove that the images of "random" elements of a free group F under the automorphisms of F form "clusters" that share similar normalized Whitehead graphs and similar behavior with respect to Whitehead's algorithm.

1. INTRODUCTION

The *automorphism problem* for a free group $F = F(a_1, \dots, a_k)$, where $k \geq 2$, asks, given two arbitrary elements $u, v \in F$, whether there exists $\phi \in \mathrm{Aut}(F)$ such that $\phi(u) = v$. In a classic 1936 paper [Whitehead 36], Whitehead provided an algorithm that solved the automorphism problem. He introduced a special finite generating set of $\mathrm{Aut}(F)$ consisting of the so-called *Whitehead automorphisms*. He proved that if $u \in F$ is a cyclically reduced word that is not shortest in its $\mathrm{Aut}(F)$-orbit, then there exists a Whitehead automorphism τ such that $\tau(u)$ has smaller cyclically reduced length than τ. This provides a quadratic-time algorithm for finding a *minimal* element in the orbit $\mathrm{Aut}(F)f$ for any $f \in F$, that is, the element of smallest length in $\mathrm{Aut}(F)f$. Namely, first cyclically reduce f to get $f' \in F$, and then check whether there is a Whitehead automorphism τ that decreases the cyclically reduced length of f'. If not, then f' is minimal. If so, replace f' by $\tau(f)$ and then repeat the entire step. Whitehead also proved that if $u, v \in F$ are cyclically reduced minimal elements of the same length, then $v \in \mathrm{Aut}(F)u$ if and only if there exists a chain of Whitehead automorphisms taking u to v and such that the cyclically reduced length is constant throughout the chain. Together with the above procedure for computing minimal representatives, this provides an algorithm for solving the automorphism problem that runs in at most exponential time in terms of $|u| + |v|$. The second,

2000 AMS Subject Classification: Primary 20F36; Secondary 20E36

Keywords: Whitehead's algorithm, geodesic currents, free groups, genericity

© A K Peters, Ltd.
1058-6458/2007 $0.50 per page

"hard," part of Whitehead's algorithm has an a priori exponential upper bound for the running time, although in practice the algorithm appears always to terminate much faster.

Since this 1936 paper of Whitehead there has been a great deal of work on the study of the automorphism problem and of Whitehead's algorithm (see, for example, the recent paper [Lee 06]). However, even now, 70 years later, the precise complexity of Whitehead's algorithm is still unknown; nor is it known whether there exists a polynomial-time algorithm for solving the automorphism problem in a free group. The only well-understood case is $k = 2$, for which it is known that the automorphism problem is indeed solvable in polynomial time [Myasnikov and Shpilrain 03, Khan 04].

A recent paper of Kapovich, Schupp, and Shpilrain [Kapovich et al. 06] proves that for any $k \geq 2$, Whitehead's algorithm has linear-time generic-case complexity. It turns out that "random" cyclically reduced elements of F are already minimal, so that the first (minimization) part of Whitehead's algorithm terminates in a single step. Moreover, the second, "hard," part of the algorithm is also proved in [Kapovich et al. 06] to run in at most linear time in this case.

It is therefore interesting to understand the behavior of Whitehead's algorithm on nonminimal inputs that are also generated via some natural probabilistic process. A. D. Miasnikov, A. G. Myasnikov, and R. Haralick [Haralick et al. 04, Haralick et al. 05a, Haralick et al. 05b], using pattern-recognition methods, experimentally discovered some interesting features of the behavior of Whitehead's algorithm in this setup. Before discussing their observations, we need to fix some notation.

Convention 1.1. For the remainder of the paper let $F = F(A)$ be a free group with a fixed free basis $A = \{a_1, \ldots, a_k\}$, where $k \geq 2$. Let $X = \Gamma(F, A)$ be the Cayley graph of F with respect to A, so that X is a $(2k)$-regular tree. Set $\Sigma = A \cup A^{-1} = \{a_1, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}\}$.

For a word w in Σ^* we will denote the length of w by $|w|$. A word $w \in \Sigma^*$ is said to be *reduced* if w is freely reduced in F, that is, if w does not contain subwords of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$. A word w is *cyclically reduced* if all cyclic permutations of w are reduced. (In particular, w itself is reduced.) We denote by C the set of all nontrivial cyclically reduced words in F.

Since every element of F can be uniquely represented by a freely reduced word, we identify elements of F and freely reduced words. Any freely reduced element w can be uniquely decomposed as a concatenation $w = vuv^{-1}$, where u is a cyclically reduced word. The word u is called the *cyclically reduced form of* w, and $\|w\| := |u|$ is the *cyclic length* of w.

Some of the experimental conclusions of Miasnikov et al., described in detail in [Haralick et al. 05b], can be summarized as follows. First take a large sample of long, random, cyclically reduced words W_1 in F. If there are any nonminimal elements, apply Whitehead's algorithm and replace them by their minimal representatives. The resulting set W_2 consists of only minimal words. By the results of [Kapovich et al. 06], most of elements of W_1 are already minimal, and therefore the difference between W_1 and W_2 will be very small and can be disregarded.

Then some of the elements w of W_2 (again usually chosen at random) are replaced by $\phi_w(w)$, where ϕ_w comes from some finite collection Φ of automorphisms chosen so that $\|w\| < \|\phi_w(w)\|$. The resulting set W_3 thus contains both minimal and nonminimal elements. Some of the experimentally observed results were as follows:

- The nonminimal elements of the set W_3 formed several "clusters."
- For each "cluster" $\mathcal{C}$, all the elements of $\mathcal{C}$ had approximately the same normalized Whitehead graphs.
- Moreover, for each "cluster" $\mathcal{C}$ there was a Whitehead automorphism τ such that for all $w \in \mathcal{C}$,

$$\|\tau(w)\| < \|w\|.$$

  (In fact, often, depending on how Φ is constructed, one can choose τ to be a Nielsen automorphism.)

In the present paper we provide a theoretical justification of these experimental results. It turns out that the explanation comes from exploring the action of $\mathrm{Out}(F)$ on the space of geodesic currents on F, analyzed by the author in [Kapovich 05, Kapovich 06]. Recall that C denotes the set of all nontrivial cyclically reduced words in F.

Our main result is the following theorem.

Theorem 1.2. *Let $F = F(A)$ be a free group, where $A = \{a_1, \ldots, a_k\}$ and $k \geq 2$. Let $\phi \in \mathrm{Aut}(F)$ be an arbitrary automorphism that is not a composition of a relabeling and an inner automorphism.*

Then there exist a Whitehead automorphism τ of F and a cyclic word w with the following properties:

(1) *For an m_A-a.e. point $\omega \in \partial F$ we have*

$$\|\tau\phi(\omega_n)\| < \|\phi(\omega_n)\|$$

as $n \to \infty$ and

$$\lim_{n\to\infty} [\Gamma_{\phi(\omega_n)}] = [\Gamma_{\phi(w)}],$$

where $[\Gamma_g]$ is the normalized Whitehead graph corresponding to the conjugacy class of $g \in F$.

(2) *For every $\epsilon > 0$ there is a C-exponentially generic subset $U \subseteq C$ such that for each $f \in C$,*

$$\|\tau\phi(f)\| < \|\phi(f)\|$$

and

$$d\big([\Gamma_{\phi(f)}], [\Gamma_{\phi(w)}]\big) \le \epsilon.$$

(3) *For every $\epsilon > 0$ there is an F-exponentially generic subset $W \subseteq F$ such that for every $f \in W$,*

$$\|\tau\phi(f)\| < \|\phi(f)\|$$

and

$$d\big([\Gamma_{\phi(f)}], [\Gamma_{\phi(w)}]\big) \le \epsilon.$$

The definitions of genericity, Whitehead graphs, and the uniform measure m_A are given in the subsequent sections. Informally, if $\omega \in \partial F$ is an m_A-random point, the element $\omega(n) \in F$ is a "random" freely reduced element of length n, which is also close to being cyclically reduced. Normalized Whitehead graphs of a cyclically reduced word w, roughly speaking, record the frequencies with which the two-letter freely reduced words occur in w.

Thus Theorem 1.2 shows that in terms of the experiments described above, there will be one "cluster" for each $\phi \in \Phi$ consisting of all $\phi_w(w)$ such that $\phi_w = \phi$, $w \in W_2$.

Note that the Whitehead automorphism τ in the statement of Theorem 1.2 is algorithmically computable in terms of $\phi \in \mathrm{Aut}(F)$, although the complexity of such an algorithm is a priori exponential in terms of the word length of the outer automorphism $[\phi]$ in $\mathrm{Out}(F)$. The main tool used in the proof of Theorem 1.2 is the machinery of *geodesic currents* on free groups, discussed in more detail in Section 2 below.

Together with a recent result of S. Francaviglia [Francaviglia 06], the proof of Theorem 1.2 turns out to imply the existence of the following "universal" length-reducing factorization for automorphisms of free groups (when applied to "random" elements of F):

Corollary 1.3. *Let $\phi \in \mathrm{Aut}(F)$ be an arbitrary automorphism that is not a composition of a relabeling automorphism and an inner automorphism. Then there exists a factorization*

$$\phi = \sigma_m \sigma_{m-1} \cdots \sigma_1 \alpha,$$

where $m \ge 1$, the automorphism α is a composition of a relabeling automorphism and an inner automorphism, σ_i are Whitehead automorphisms of the second kind, and the following holds: Set $\psi_0 = \alpha$, $\psi_i = \sigma_i \sigma_{i-1} \cdots \sigma_1 \alpha$ for $i = 1, \dots, m$. Thus $\psi_m = \phi$. Then for an m_A-a.e. point $\omega \in \partial F$ as $n \to \infty$ we have

$$\|\psi_i \omega_n\| < \|\psi_{i+1}\omega_n\|, \quad i = 1, \dots, m-1,$$

so that

$$\|\omega_n\| = \|\psi_0\omega_n\| < \|\psi_1\omega_n\| < \cdots < \|\psi_m\omega_n\| = \|\phi\omega_n\|.$$

2. GEODESIC CURRENTS

We recall some basic notions related to geodesic currents on free groups. We refer the reader to [Kapovich 05, Kapovich 06, Martin 95] for a more comprehensive discussion.

Convention 2.1. We identify the hyperbolic boundary ∂F with the set of all geodesic rays from 1 in X, or equivalently, with the set of all semi-infinite freely reduced words

$$\omega = a_1 a_2 \cdots a_n \cdots,$$

where $a_i \in A^{\pm 1}$. The boundary ∂F is endowed with the Cantor-set topology and with the homeomorphic left F-action by left translations, as usual. We also define

$$\partial^2 F := \{(\zeta, \xi) : \zeta, \xi \in \partial F \text{ and } \zeta \ne \xi\}.$$

Note that $\partial^2 F$ comes equipped with the diagonal left F-action by homeomorphisms.

For a directed geodesic segment $\gamma = [x, y]$ in X with $x, y \in F$, $x \ne y$, we denote by $\mathrm{Cyl}_X(\gamma)$ the set of all $(\zeta, \xi) \in \partial^2 F$ such that the geodesic $[\zeta, \xi]$ in X passes through γ in the correct direction. Note that $\mathrm{Cyl}_X(\gamma) \subseteq \partial^2 F$ is an open–closed compact subset of $\partial^2 F$.

We denote by $\mathcal{P}(X)$ the set of all directed geodesic segments of positive length in X with endpoints in $VX = F$. We also set $F_* := F - \{1\}$.

Definition 2.2. (Uniform measure.) For $v \in F_*$ denote by $\mathrm{Cyl}_A(v)$ the set of all geodesic rays $\omega \in \partial F$ that begin with v. The *uniform measure* m_A on ∂F is the Borel probability measure on ∂F defined by

$$m_A(\mathrm{Cyl}_A(v)) = \frac{1}{2k(2k-1)^{|v|-1}} \quad \text{for every } v \in F_*.$$

Definition 2.3. (Geodesic currents.) A *geodesic current* on F is a locally finite (that is, finite on compact subsets) positive Radon measure ν on $\partial^2 F$ such that ν is F-invariant. The set of all geodesic currents on F is denoted by $\mathrm{Curr}(F)$. The space $\mathrm{Curr}(F)$ comes equipped with the natural weak topology, which can be described as follows: For $\nu_n, \nu \in \mathrm{Curr}(F)$ we have

$$\lim \nu_n = \nu$$

if and only if

$$\lim_{n\to\infty} \nu_n(\mathrm{Cyl}_X(\gamma)) = \nu(\mathrm{Cyl}_X(\gamma)) \quad \text{for every } \gamma \in \mathcal{P}(X).$$

Definition 2.4. (The coordinates on $\mathrm{Curr}(F)$.) If $\nu \in \mathrm{Curr}(F)$ and $\gamma = [x, y] \in \mathcal{P}(X)$, then by F-invariance of ν the value $\nu(\mathrm{Cyl}_X(\gamma))$ depends only on ν and the *label* $v := x^{-1}y \in F$ of γ. For a nontrivial $v \in F$ we define

$$\langle v, \nu\rangle := \nu(\mathrm{Cyl}_X(\gamma)),$$

where $\gamma \in \mathcal{P}(X)$ is any geodesic segment labeled by v. We call $\langle v, \nu\rangle$ the *number of occurrences of v in ν*.

The following lemma [Kapovich 06] summarizes some basic invariance properties satisfied by the coordinates of a geodesic current.

Lemma 2.5. *Let $\nu \in \mathrm{Curr}(F)$. Then for every $v \in F_*$,*

$$\langle v, \nu\rangle = \sum_{a\in A^{\pm 1}, |va|=|v|+1} \langle va, \nu\rangle = \sum_{a\in A^{\pm 1}, |av|=1+|v|} \langle av, \nu\rangle.$$

A current $\nu \in \mathrm{Curr}(F)$ is uniquely determined by the family $(\langle v, \nu\rangle)_{v\in F_*}$. Moreover, as shown in [Kapovich 05, Kapovich 06], every nonnegative family $(\langle v, \nu\rangle)_{v\in F_*}$ satisfying the invariance conditions from Lemma 2.5 defines a current $\nu \in \mathrm{Curr}(F)$.

Definition 2.6. (Uniform current.) The *uniform current* $n_A \in \mathrm{Curr}(F)$ corresponding to the free basis A of F is the geodesic current defined by

$$n_A(\mathrm{Cyl}_X(\gamma)) = \frac{1}{2k(2k-1)^{|\gamma|-1}} \quad \text{for every } \gamma \in \mathcal{P}(X).$$

Thus $\langle v, n_A\rangle = \frac{1}{2k(2k-1)^{|v|-1}}$ for every $v \in F_*$.

Definition 2.7. (Rational currents.) Let $g \in F_*$. If g is not a proper power, define

$$\eta_g := \sum_{h\in[g]} \delta_{(h^{-\infty}, h^{\infty})},$$

where $[g]$ is the conjugacy class of g in F. If $g = g_0^s$, where $s \geq 2$ and $g_0 \in F_*$ is not a proper power, define

$$\eta_g := s\eta_{g_0}.$$

It is easy to see that η_g depends only on the conjugacy class $[g]$ of g in F.

Nonnegative multiples of the currents η_g, $g \in F_*$, are called *rational currents*.

An important basic fact (see [Kapovich 06]) is given in the following proposition:

Proposition 2.8. *The set of rational currents is dense in* $\mathrm{Curr}(F)$.

Convention 2.9. (Cyclic words.) We will often think about conjugacy classes of nontrivial elements of F as *cyclic words*. A *cyclic word* w over A is a nontrivial cyclically reduced word in $F(A)$ written clockwise on a circle without specifying an initial point. The length of that cyclically reduced word is called the *cyclic length* of w and is denoted by $\|w\|$. The circle is thought of as a labeled graph subdivided into $\|w\|$ directed edges, each labeled by a letter of A.

If $v \in F$, we call a vertex on this circle an *occurrence of v in w* if v can be read in the circle starting at that vertex and going clockwise (we are allowed to stop at a different vertex from the one where we started). The number of occurrences of v in w is denoted by $\langle v, w\rangle$.

Also, if $v, g \in F$ are nontrivial elements, we put $\langle v, g\rangle := \langle v, w\rangle$, where w is the cyclic word representing the conjugacy class of g.

The following basic fact gives a useful alternative description of rational currents.

Lemma 2.10. *Let $g \in F_*$ and let w be the cyclic word determined by the conjugacy class of g. Then for every $v \in F_*$ we have*

$$\langle v, w\rangle = \langle v, \eta_g\rangle.$$

There is a natural continuous left action of $\mathrm{Aut}(F)$ on $\mathrm{Curr}(F)$ that factors to the action of $\mathrm{Out}(F)$ on $\mathrm{Curr}(F)$.

If $\phi \in \mathrm{Aut}(F)$, then ϕ is a quasi-isometry of the Cayley graph X of F. Therefore, ϕ induces a canonical boundary homeomorphism $\partial\phi : \partial F \to \partial F$ that diagonally extends to a homeomorphism $\partial^2\phi : \partial^2 F \to \partial^2 F$. If $\nu \in \mathrm{Curr}(F)$ and $\phi \in \mathrm{Aut}(F)$, the current $\phi\nu \in \mathrm{Curr}(F)$ is defined by setting

$$\phi\nu(S) := \nu((\partial^2\phi)^{-1}(S))$$

for every Borel subset $S \subseteq \partial^2 F$. It is not hard to show (see [Kapovich 06]) that for every $g \in F_*$ and every $\phi \in \mathrm{Aut}(F)$ we have $\phi\eta_g = \eta_{\phi(g)}$.

The following useful statement, established in [Kapovich 06], gives a "coordinate" description of the action of $\mathrm{Aut}(F)$ on $\mathrm{Curr}(F)$.

Proposition 2.11. *Let $\phi \in \mathrm{Aut}(F)$. Then there exists an integer $K = K(\phi) > 0$ with the following property: For every $v \in F_*$ there exists a collection of nonnegative integers $\{c(u, v, \phi) : u \in F, |u| = K|v|\}$ such that for every $\nu \in \mathrm{Curr}(F)$,*

$$\langle v, \phi\nu\rangle = \sum_{u \in F, |u| = K|v|} c(u, v, \phi)\langle u, \nu\rangle.$$

If $a_n, a \in \mathbb{R}$ and $\lim_{n\to\infty} = a$, we say that the convergence in this limit is *exponentially fast* if there exist $0 < \sigma < 1$, $b > 0$ such that $|a_n - a| \le b\sigma^n$ for all $n \ge 1$.

Definition 2.12. (Generic sets.) Let $S \subseteq F$ be an infinite subset. Let $T \subseteq S$. We say that T is *generic* in S, or *S-generic*, if

$$\lim_{n\to\infty} \frac{\#\{g \in T : |g| \le n\}}{\#\{g \in S : |g| \le n\}} = 1.$$

If, in addition, the convergence in this limit is exponentially fast, we say that T is *exponentially S-generic*.

In practice, we will be interested only in the cases in which $S = F$ or $S = C$ (recall that C is the set of all nontrivial cyclically reduced words in F). We refer the reader to [Kapovich et al. 03, Kapovich et al. 06] for more details regarding genericity and generic-case complexity.

3. THE LENGTH FUNCTIONAL

It turns out that the notion of "cyclic length" with respect to the free basis A extends naturally to a continuous linear function on $\mathrm{Curr}(F)$.

Definition 3.1. (Length of a current.) Let $\nu \in \mathrm{Curr}(F)$. We define the *length $L(\nu)$ of ν with respect to A* as

$$L(\nu) := \sum_{a \in A^{\pm 1}} \langle a, \nu\rangle.$$

In the language of [Kapovich 06] we have $L(\nu) = I(\ell_A, \nu)$, where I is the "intersection form" and where $\ell_A : F \to \mathbb{R}$ is the length function defined as $\ell_A(w) = \|w\|$ for $w \in F$. Note that for any automorphism $\phi \in \mathrm{Aut}(F)$ the number $L(\phi n_A)$ is exactly what in [Kaimanovich et al. 05] is called the *generic stretching factor* $\lambda_A(\phi)$ of ϕ with respect to A.

The following basic properties of length follow directly from the results about the intersection form established in [Kapovich 06].

Proposition 3.2. *The following hold:*

(i) *The function $L : \mathrm{Curr}(F) \to \mathbb{R}$ is continuous and linear.*

(ii) *For any integer $m \ge 1$ and for every $\nu \in \mathrm{Curr}(F)$ we have*

$$L(\nu) = \sum_{v \in F, |v| = m} \langle v, \nu\rangle.$$

(iii) *For every $w \in F_*$ we have*

$$\|w\| = L(\eta_w).$$

(iv) *We have $L(n_A) = 1$.*

In view of Propositions 2.11 and 3.2 we obtain the following result:

Proposition 3.3. *Let $\phi \in \mathrm{Aut}(F)$.*

(i) *There exist $m \ge 2$ and a collection of integers $\{d(u) : u \in F, |u| = m\}$ such that for every $\nu \in \mathrm{Curr}(F)$ we have*

$$L(\phi\nu) = \sum_{|u| = m} d(u)\langle u, \nu\rangle.$$

(ii) *Suppose $m \ge 1$ is an integer and $\{d(u) \in \mathbb{Z} : u \in F, |u| = m\}$ are such that for every cyclic word w we have*

$$\|\phi(w)\| = \sum_{|u| = m} d(u)\langle u, w\rangle.$$

Then for every $\nu \in \mathrm{Curr}(F)$ we have

$$L(\phi\nu) = \sum_{|u| = m} d(u)\langle u, \nu\rangle.$$

Proof: Assertion (i) follows directly from Propositions 2.11 and 3.2. Suppose the assumptions of assertion (ii) hold. Then the conclusion of assertion (ii) holds for every current of the form η_g, $g \in F_*$. Therefore, in view of Lemma 2.10, the conclusion of assertion (ii) holds for every $\nu \in \mathrm{Curr}(F)$, since rational currents are dense in $\mathrm{Curr}(F)$. □

4. WHITEHEAD AUTOMORPHISMS

Recall that $\Sigma = A \cup A^{-1} = \{a_1, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}\}$. We follow [Lyndon and Schupp 77, Chapter 1] in our discussion of Whitehead automorphisms. We recall the basic definitions and results.

Definition 4.1. (Whitehead automorphisms.) A *Whitehead automorphism* of F is an automorphism τ of F of one of the following two types:

(1) There is a permutation t of Σ such that $\tau|_\Sigma = t$. In this case τ is called a *relabeling automorphism* or a *Whitehead automorphism of the first kind*.

(2) There is an element $a \in \Sigma$, the *multiplier*, such that for any $x \in \Sigma$,

$$\tau(x) \in \{x, xa, a^{-1}x, a^{-1}xa\}.$$

In this case we say that τ is a *Whitehead automorphism of the second kind*. (Note that since τ is an automorphism of F, we always have $\tau(a) = a$ in this case.) With every such τ we associate a pair (T, a), where a is as above and T consists of all those elements of Σ, including a but excluding a^{-1}, such that $\tau(x) \in \{xa, a^{-1}xa\}$. We will say that (T, a) is the *characteristic pair* of τ.

Note that for any $a \in \Sigma$ the inner automorphism corresponding to the conjugation by a is a Whitehead automorphism of the second kind.

Definition 4.2. (Minimal elements.) An element $w \in F$ is said to be *automorphically minimal*, or just *minimal*, if for *every* $\alpha \in \mathrm{Aut}(F)$ we have $|w| \le |\alpha(w)|$.

Proposition 4.3. (Whitehead's algorithm.)

(1) *If $u \in F$ is cyclically reduced and not minimal, then there is a Whitehead automorphism τ such that $\|\tau(u)\| < \|u\|$.*

(2) *Let $u, v \in F$ be minimal (and hence cyclically reduced) elements with $|u| = |v| = n > 0$. Then $\mathrm{Aut}(F)u = \mathrm{Aut}(F)v$ if and only if there exists a finite sequence of Whitehead automorphisms $\tau_s, \ldots, \tau_1$ such that $\tau_s \cdots \tau_1(u) = v$ and such that for each $i = 1, \ldots, s$ we have*

$$\|\tau_i \cdots \tau_1(u)\| = n.$$

Definition 4.4. (Strict minimality.) A nontrivial cyclically reduced word w in F is *strictly minimal* if for every non-inner Whitehead automorphism τ of F of the second kind we have

$$\|\tau(w)\| > \|w\|.$$

Definition 4.5. (Simple automorphisms.) An automorphism $\phi \in \mathrm{Aut}(F)$ is called *simple* if it is the composition of an inner and a relabeling automorphism.

Clearly, if ϕ is simple, then for every $w \in F_*$ we have $\|\phi(w)\| = \|w\|$. Proposition 4.3 immediately implies that every strictly minimal element is minimal, and moreover, if u is strictly minimal and $\phi \in \mathrm{Aut}(F)$ is such that $\|u\| = \|\phi(u)\|$, then ϕ is simple.

Definition 4.6. (Weighted Whitehead graph.) Let w be a nontrivial cyclic word in $F(A)$. The *weighted Whitehead graph* Γ_w *of* w is defined as follows. The vertex set of Γ_w is Σ. For every $x, y \in \Sigma$ such that $x \ne y^{-1}$ there is an undirected edge in Γ_w from x^{-1} to y labeled by the sum

$$\langle xy, w\rangle + \langle y^{-1}x^{-1}, w\rangle,$$

the number of occurrences of the words xy and $y^{-1}x^{-1}$ in w.

The *normalized Whitehead graph* $[\Gamma_w]$ of w is the labeled graph obtained from Γ_w by dividing every edge label by $\|w\|$.

Definition 4.7. An *abstract Whitehead graph* is a labeled graph Γ whose vertex and edge sets are the same as those for a weighted Whitehead graph of a cyclic word and such that each edge e of Γ is labeled by a real number $r(e)$. If Γ, Γ' are two abstract Whitehead graphs, we define

$$d(\Gamma, \Gamma') = \max_{e \in E\Gamma} |r(e) - r(e')|.$$

This turns the set of all abstract Whitehead graphs into a metric space homeomorphic to $\mathbb{R}^{k(2k-1)}$.

Note that if w is a cyclic word, then both Γ_w and $[\Gamma_w]$ are abstract Whitehead graphs. Note also that for $[\Gamma_w]$ the sum of all edge labels is equal to 1.

Convention 4.8. Let w be a fixed nontrivial cyclic word. For two subsets $P, Q \subseteq \Sigma$ we denote by $P \underset{w}{.} Q$ the sum of all edge labels in the weighted Whitehead graph Γ_w of w of edges from elements of P to elements of Q. Thus for $x \in \Sigma$ the number $x \underset{w}{.} \Sigma$ is equal to the total number of occurrences of $x^{\pm 1}$ in w.

The next lemma, which is from [Lyndon and Schupp 77, Proposition 4.16], gives an explicit formula for the difference of the lengths of w and $\tau(w)$, where τ is a Whitehead automorphism.

Lemma 4.9. *Let w be a nontrivial cyclically reduced word and let τ be a Whitehead automorphism of the second kind with the characteristic pair (T, a). Let $T' = \Sigma - T$. Then*

$$\|\tau(w)\| - \|w\| = T \underset{w}{.} T' - a \underset{w}{.} \Sigma.$$

Now Lemma 4.9 and Proposition 3.3 immediately imply the following:

Corollary 4.10. *Let τ be a Whitehead automorphism of the second kind. Then there exists a collection of integers $\{b(z) : z \in F, |z| = 2\}$ such that for every $\nu \in \mathrm{Curr}(F)$ we have*

$$L(\tau\nu) = \sum_{|z|=2} b(z)\langle z, \nu\rangle.$$

Remark 4.11. Note that in view of Lemma 4.9 and Corollary 4.10, if w is a cyclic word and τ is a Whitehead automorphism of the second kind, then the quantity

$$\frac{\|\tau(w)\|}{\|w\|}$$

is completely determined by τ and the normalized Whitehead graph $[\Gamma_w]$ of w.

5. PROOF OF THE MAIN RESULT

We begin with the following proposition.

Proposition 5.1. *For every integer $m \geq 2$ there exists a cyclic word w such that*

$$\langle v, w\rangle = 1 \text{ for every } v \in F \text{ with } |v| = m$$

and such that $\|w\| = 2k(2k-1)^{m-1}$.

Proof: This follows from a more general result in [Kapovich 05]. We present an argument here for completeness.

If $v \in F$ is a freely reduced word with $|v| \geq 2$, we denote by v_- the initial segment of v of length $|v| - 1$ and we denote by v_+ the terminal segment of v of length $|v| - 1$.

Let $n \geq 2$. Form a finite directed labeled graph Γ as follows: The vertex set of Γ is

$$V\Gamma := \{u \in F : |u| = m - 1\}.$$

The set of directed edges of Γ is

$$E\Gamma := \{v \in F : |v| = m\}.$$

For each $v \in E\Gamma$ the initial vertex of v in Γ is v_- and the terminal vertex of v in Γ is v_+. Also, the edge $v \in E\Gamma$ is labeled by the *label* $a(v) \in A^{\pm 1}$, which is the last letter of the word v.

Note that for every vertex $u \in V\Gamma$ both the out-degree of u and the in-degree of u in Γ are equal to $2k-1$. Thus Γ is a strongly connected directed graph each vertex of which has in-degree equal to out-degree. Therefore there exists an Euler circuit c in Γ, that is, a cyclic path passing through each directed edge of Γ exactly once. Let c be represented by the edge-path

$$v_1 v_2 \cdots v_t, \text{ where } t = |E\Gamma| = 2k(2k-1)^{m-1}.$$

Let w be the cyclic word defined by the word

$$a(v_1)a(v_2)\cdots a(v_t).$$

Then it is not hard to see that

$$\|w\| = t = 2k(2k-1)^{m-1}$$

and that for every $v \in F$ with $|v| = m$ we have

$$\langle v, w\rangle = 1,$$

as required. □

Recall that n_A is the uniform current on F defined in Definition 2.6.

Proposition 5.2. (Ideal Whitehead algorithm.) *Let $\phi \in \mathrm{Aut}(F)$ be an automorphism such that ϕ is not simple. Then there exists a Whitehead automorphism τ of the second kind such that*

$$1 = L(n_A) \leq L(\tau\phi n_A) < L(\phi n_A).$$

Proof: By Proposition 2.11 there exist an integer $m \geq 2$ and a collection of nonnegative integers

$$\{c(v,z) : v, z \in F, |v| = m, |z| = 2\}$$

such that for every $\nu \in \mathrm{Curr}(F)$ we have

$$\langle z, \phi\nu\rangle = \sum_{|v|=m} c(v,z)\langle v, \nu\rangle.$$

Let w be a cyclic word provided by Proposition 5.1. Recall that we have $\|w\| = 2k(2k-1)^{m-1}$. Let $\theta = \frac{\eta_w}{2k(2k-1)^{m-1}}$. Thus for every $v \in F$ with $|v| = m$ we have

$$\langle v, \theta\rangle = \frac{1}{2k(2k-1)^{m-1}}.$$

Then for every $z \in F$ with $|z| = 2$ we have

$$\langle z, \phi\theta\rangle = \langle z, \phi n_A\rangle. \tag{5–1}$$

Moreover, we have

$$L(\phi\theta) = \sum_{|z|=2} \langle z, \phi\theta\rangle = \sum_{|z|=2} \langle z, \phi n_A\rangle = L(\phi n_A).$$

By [Kapovich et al. 06, Lemma 4.8], the word w is strictly minimal, which implies, in particular, that $\|w\| < \|\phi(w)\|$, since ϕ is not simple. Therefore, by Whitehead's theorem, part (1) of Proposition 4.3, there exists a Whitehead automorphism τ of the second kind such that

$$\|w\| \leq \|\tau\phi(w)\| < \|\phi(w)\|.$$

Therefore

$$1 = L(\theta) \leq L(\tau\phi\theta) < L(\phi\theta).$$

Then by the above formulas and Corollary 4.10 we see that

$$1 = L(n_A) \leq L(\tau\phi n_A) = L(\tau\theta) < L(\theta) = L(\phi n_A),$$

as required. □

Note that Proposition 5.2 means that $n_A \in \mathrm{Curr}(F)$ is "minimal" and even "strictly minimal" in the sense that for every $\phi \in \mathrm{Aut}(F)$,

$$L(n_A) \leq L(\phi n_A),$$

with equality achieved if and only if ϕ is simple.

Corollary 5.3. *Let $\phi \in \mathrm{Aut}(F)$ be a nonsimple automorphism. Then there exists a factorization*

$$\phi = \sigma_m\sigma_{m-1}\cdots\sigma_1\alpha,$$

where $m \geq 1$, the automorphism α is simple, σ_i are Whitehead automorphisms of the second kind, and

$$L(\sigma_{i-1}\cdots\sigma_1\alpha n_A) < L(\sigma_i\sigma_{i-1}\cdots\sigma_1\alpha n_A),$$

$i = 1, \ldots, m-1$.

Proof: Define

$$\Lambda := \{L(\psi n_A) : \psi \in \mathrm{Aut}(F)\}.$$

A recent theorem of S. Francaviglia [Francaviglia 06] shows that Λ is a discrete subset of $\mathbb{R}$. Also, as proved in [Kapovich et al. 06], for every $\psi \in \mathrm{Aut}(F)$ we have $L(\psi n_A) \geq 1$, and moreover, $L(\psi n_A) = 1$ if and only if ψ is simple.

Let $\phi \in \mathrm{Aut}(F)$ be a nonsimple automorphism. Thus $L(\phi n_A) > 1$. Repeatedly applying Proposition 5.2, we conclude that there exists a sequence of Whitehead automorphisms $\tau_1, \tau_2, \ldots$ such that $L(\phi n_A) > L(\tau_1\phi n_A) > L(\tau_2\tau_1\phi n_A) > \cdots$. Since Λ is a discrete subset of $[1, \infty)$, the sequence $\tau_1, \tau_2, \ldots$ must terminate in a finite number of steps with some τ_m. Hence the automorphism $\alpha := \tau_m\cdots\tau_2\tau_1\phi$ must be simple, since otherwise, by Proposition 5.2, the sequence of τ_i could be extended. Then the factorization

$$\phi = \tau_1^{-1}\cdots\tau_m^{-1}\alpha$$

has the required properties, and the corollary is proved. □

Proof of Theorem 1.2.: Let $\phi \in \mathrm{Aut}(F)$ be an automorphism such that ϕ is not simple. By Proposition 5.2 there exists a Whitehead automorphism τ such that

$$L(\tau\phi n_A) < L(\phi n_A).$$

Also, as in the proof of Proposition 5.2, let w be the cyclic word provided by Proposition 5.1.

Recall that by Proposition 2.11 there exist an integer $m \geq 2$ and a collection of nonnegative integers

$$\{c(v,z) : v, z \in F, |v| = m, |z| = 2\}$$

such that for every $\nu \in \mathrm{Curr}(F)$ we have

$$\langle z, \phi\nu\rangle = \sum_{|v|=m} c(v,z)\langle v, \nu\rangle.$$

Let $\omega \in \partial F$ be an m_A-random point. Then, as observed in [Kapovich 06],

$$\lim_{n\to\infty} \frac{\eta_{\omega_n}}{n} = \lim_{n\to\infty} \frac{\eta_{\omega_n}}{\|\omega_n\|} = n_A \text{ in } \mathrm{Curr}(F).$$

Hence

$$\lim_{n\to\infty} \phi\frac{\eta_{\omega_n}}{n} = \phi n_A$$

and

$$\lim_{n\to\infty} \tau\phi\frac{\eta_{\omega_n}}{n} = \tau\phi n_A.$$

Since $L : \mathrm{Curr}(F) \to \mathbb{R}$ is continuous and $L(\tau\phi n_A) < L(\phi n_A)$, it follows that for $n \to \infty$,

$$L\left(\tau\phi\frac{\eta_{\omega_n}}{n}\right) < L\left(\phi\frac{\eta_{\omega_n}}{n}\right).$$

Then for $n \to \infty$,

$$\frac{\|\tau\phi(\omega_n)\|}{n} < \frac{\|\phi(\omega_n)\|}{n},$$

and therefore

$$\|\tau\phi(\omega_n)\| < \|\phi(\omega_n)\|,$$

as required.

We have seen in (5–1) that

$$\langle z, \phi\theta\rangle = \langle z, \phi n_A\rangle \text{ for each } z \in F \text{ with } |z| = 2,$$

where $\theta = \frac{\eta_w}{2k(2k-1)^{m-1}}$ and $\|w\| = 2k(2k-1)^{m-1}$. Since

$$\lim_{n\to\infty} \phi\frac{\eta_{\omega_n}}{n} = \phi n_A,$$

this implies that for each $z \in F$ with $|z| = 2$ we have

$$\lim_{n\to\infty} \frac{\langle z, \phi(\omega_n)\rangle}{n} = \langle z, \phi n_A\rangle = \langle z, \phi\theta\rangle = \frac{\langle z, \phi(w)\rangle}{2k(2k-1)^{m-1}}.$$

We also have

$$\|\phi(w)\| = \sum_{|z|=2} \langle z, \phi(w)\rangle = \sum_{|z|=2}\sum_{|v|=m} c(v,z)\langle v, w\rangle$$
$$= \sum_{|z|=2}\sum_{|v|=m} c(v,z)$$

and

$$\|\phi(\omega_n)\| = \sum_{|z|=2} \langle z, \phi(\omega_n)\rangle = \sum_{|z|=2}\sum_{|v|=m} c(v,z)\langle v, \omega_n\rangle.$$

Therefore for any $z' \in F$ with $|z'| = 2$ we have

$$\frac{\langle z', \phi(w)\rangle}{\|\phi(w)\|} = \frac{\sum_{|v|=m} c(v,z')}{\sum_{|z|=2}\sum_{|v|=m} c(v,z)}$$

and

$$\frac{\langle z', \phi(\omega_n)\rangle}{\|\phi(\omega_n)\|} = \frac{\sum_{|v|=m} c(v,z')\langle v, \omega_n\rangle}{\sum_{|z|=2}\sum_{|v|=m} c(v,z)\langle v, \omega_n\rangle}$$
$$= \frac{\sum_{|v|=m} c(v,z')\frac{\langle v, \omega_n\rangle}{n}}{\sum_{|z|=2}\sum_{|v|=m} c(v,z)\frac{\langle v, \omega_n\rangle}{n}}.$$

Since $\lim_{n\to\infty} \frac{\eta_{\omega_n}}{n} = n_A$, it follows that

$$\lim_{n\to\infty} \frac{\langle v, \omega_n\rangle}{n} = \frac{1}{2k(2k-1)^{m-1}}$$

for every $v \in F$ with $|v| = m$. Therefore for every $z' \in F$ with $|z'| = 2$ we have

$$\lim_{n\to\infty} \frac{\langle z', \phi(\omega_n)\rangle}{\|\phi(\omega_n)\|} = \frac{\sum_{|v|=m} c(v,z')}{\sum_{|z|=2}\sum_{|v|=m} c(v,z)} = \frac{\langle z', \phi(w)\rangle}{\|\phi(w)\|}.$$

It follows that $\lim_{n\to\infty}[\Gamma_{\phi(\omega_n)}] = [\Gamma_{\phi(w)}]$, as required.

This establishes part (1) of Theorem 1.2.

Recall that by [Kapovich et al. 06, Proposition 6.2], if $U \subseteq C$ is an exponentially C-generic subset, then the set W consisting of all $w \in F$ whose cyclically reduced forms are in U is exponentially F-generic. Therefore, part (2) of Theorem 1.2 implies part (3). Thus it remains to prove part (2) of Theorem 1.2.

For any $\epsilon' > 0$ define

$$U(\epsilon') = \Big\{u \in C : \left|\frac{\langle v, u\rangle}{\|u\|} - \frac{1}{2k(2k-1)^{m-1}}\right| \le \epsilon' \text{ for every } v \in F, |v| = m\Big\}.$$

Recall also that there exists a collection of integers $\{d(z) : z \in F, |z| = 2\}$ such that

$$L(\tau\nu) - L(\nu) = \sum_{|z|=2} d(z)\langle z, \nu\rangle \quad \text{for every } \nu \in \mathrm{Curr}(F).$$

Since $L(\tau\phi n_A) < L(\phi n_A)$, there is $\epsilon'' > 0$ such that for every $\nu \in \mathrm{Curr}(F)$ satisfying

$$|\langle z, \nu\rangle - \langle z, \phi n_A\rangle| \le \epsilon''$$

for every $z \in F$ with $|z| = 2$, we have $L(\tau\nu) - L(\nu) < 0$.

The properties of $c(v,z)$ listed above imply that there is $\epsilon' > 0$ such that for every $u \in U(\epsilon')$ and for every $z \in F, |z| = 2$ we have

$$\left|\left\langle z, \phi\frac{\eta_u}{\|u\|}\right\rangle - \langle z, \phi n_A\rangle\right| \le \epsilon''.$$

Hence for every $u \in U(\epsilon')$,

$$L\left(\tau\phi\frac{\eta_u}{\|u\|}\right) - L\left(\phi\frac{\eta_u}{\|u\|}\right) < 0,$$

that is,

$$\frac{\|\tau\phi(u)\|}{\|u\|} < \frac{\|\phi(u)\|}{\|u\|} \quad \Rightarrow \quad \|\tau\phi(u)\| < \|\phi(u)\|.$$

The set $U(\epsilon') \subseteq C$ is exponentially C-generic, as was observed in [Kaimanovich et al. 05]. The proof of the

Whitehead graph assertion of part (2) of Theorem 1.2 is similar to that used in part (1). One shows that if $\epsilon > 0$ is arbitrary, then for $\epsilon' > 0$ small enough,

$$d([\Gamma_{\phi(u)}], [\Gamma_{\phi w}]) \leq \epsilon \quad \text{for all } u \in U(\epsilon').$$

We leave the details to the reader. This completes the proof of Theorem 1.2. □

Corollary 5.3 implies Corollary 1.3 from Section 1 in a way similar to the proof of part (1) of Theorem 1.2, and we leave the details to the reader.

ACKNOWLEDGMENTS

The author is grateful to Alexey G. Myasnikov for suggesting that he consider the question addressed by Theorem 1.2. The author especially thanks Paul Schupp for useful conversations and for help with computer experimentation. The author was supported by NSF grant DMS-0404991.

REFERENCES

[Francaviglia 06] S. Francaviglia. "Geodesic Currents and Length Compactness for Automorphisms of Free Groups." arXiv:math.GR/0602555, 2006.

[Haralick et al. 04] R. Haralick, A. D. Miasnikov, and A. G. Myasnikov. "Pattern Recognition Approaches to Solving Combinatorial Problems in Free groups." In *Computational and Experimental Group Theory*, pp. 197–213, Contemp. Math. 349. Providence: Amer. Math. Soc., 2004.

[Haralick et al. 05a] R. Haralick, A. D. Miasnikov, and A. G. Myasnikov. "Pattern Recognition and Minimal Words in Free Groups of Rank 2." *J. Group Theory* 8:4 (2005), 523–538.

[Haralick et al. 05b] R. Haralick, A. D. Miasnikov, and A. G. Myasnikov. "Heuristics for the Whitehead Minimization Problem." *Experiment. Math.* 14:1 (2005), 7–14.

[Kaimanovich et al. 05] V. Kaimanovich, I. Kapovich, and P. Schupp. "The Subadditive Ergodic Theorem and Generic Stretching Factors for Free Group Automorphisms." To appear in *Israel J. Math.*, arXiv:math.GR/0504105, 2005.

[Kapovich 05] I. Kapovich, "The Frequency Space of a Free Group." *Internat. J. Alg. Comput.* (special Gaeta Grigorchuk 50th birthday issue) 15:5–6 (2005), 939–969.

[Kapovich 06] I. Kapovich, "Currents on Free Groups." In *Topological and Asymptotic Aspects of Group Theory*, edited by R. Grigorchuk, M. Mihalik, M. Sapir, and Z. Sunik, pp. 149–176, AMS Contemporary Mathematics Series 394. Providence: Amer. Math. Soc., 2006.

[Kapovich et al. 03] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain. "Generic-Case Complexity, Decision Problems in Group Theory and Random Walks." *J. Algebra* 264:2 (2003), 665–694.

[Kapovich et al. 06] I. Kapovich, P. Schupp, and V. Shpilrain. "Generic Properties of Whitehead's Algorithm and Isomorphism Rigidity of Random One-Relator Groups." *Pacific J. Math.* 223:1 (2006), 113–140.

[Khan 04] B. Khan. "The Structure of Automorphic Conjugacy in the Free Group of Rank Two." In *Computational and Experimental Group Theory*, pp. 115–196, Contemp. Math. 349. Providence: Amer. Math. Soc., 2004.

[Lee 06] D. Lee. "Counting Words of Minimum Length in an Automorphic Orbit." *J. Algebra* 301:1 (2006), 35–38.

[Lyndon and Schupp 77] R. Lyndon and P. Schupp. *Combinatorial Group Theory*. New York: Springer-Verlag, 1977.

[Martin 95] R. Martin. "Non-Uniquely Ergodic Foliations of Thin Type, Measured Currents and Automorphisms of Free Groups." PhD diss., UCLA, 1995.

[Myasnikov and Shpilrain 03] A. G. Myasnikov and V. Shpilrain. "Automorphic Orbits in Free Groups." *J. Algebra* 269:1 (2003), 18–27.

[Whitehead 36] J. H. C. Whitehead. "On Equivalent Sets of Elements in Free Groups." *Annals of Mathematics* 37 (1936), 782–800.

Ilya Kapovich, Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801 (kapovich@math.uiuc.edu)

Received November 18, 2005; accepted June 7, 2006.