Pacific Journal of Mathematics

GENERIC PROPERTIES OF WHITEHEAD'S ALGORITHM AND ISOMORPHISM RIGIDITY OF RANDOM ONE-RELATOR GROUPS

ILYA KAPOVICH, PAUL SCHUPP AND VLADIMIR SHPILRAIN

Volume 223 No. 1 January 2006

PACIFIC JOURNAL OF MATHEMATICS
Vol. 223, No. 1, 2006

GENERIC PROPERTIES OF WHITEHEAD'S ALGORITHM AND ISOMORPHISM RIGIDITY OF RANDOM ONE-RELATOR GROUPS

ILYA KAPOVICH, PAUL SCHUPP AND VLADIMIR SHPILRAIN

We prove that Whitehead's algorithm for solving the automorphism problem in a fixed free group F_k has strongly linear time generic-case complexity. This is done by showing that the "hard" part of the algorithm terminates in linear time on an exponentially generic set of input pairs. We then apply these results to one-relator groups. We obtain a Mostow-type isomorphism rigidity result for random one-relator groups: If two such groups are isomorphic then their Cayley graphs on the *given generating sets* are isometric. Although no nontrivial examples were previously known, we prove that one-relator groups are generically *complete* groups, that is, they have trivial center and trivial outer automorphism group. We also prove that the stabilizers of generic elements of F_k in $\mathrm{Aut}(F_k)$ are cyclic groups generated by inner automorphisms and that $\mathrm{Aut}(F_k)$-orbits are uniformly small in the sense of their growth entropy. We further prove that the number $I_k(n)$ of *isomorphism types* of k-generator one-relator groups with defining relators of length n satisfies

$$\frac{c_1}{n}(2k-1)^n \le I_k(n) \le \frac{c_2}{n}(2k-1)^n,$$

where c_1, c_2 are positive constants depending on k but not on n. Thus $I_k(n)$ grows in essentially the same manner as the number of cyclic words of length n.

1. Introduction

The famous Mostow Rigidity Theorem [1973] says that if M_1 and M_2 are complete connected hyperbolic manifolds of finite volume and dimension $n \ge 3$ then their fundamental groups are isomorphic if and only if the manifolds themselves are isometric. For a finitely generated group G with a finite generating set A the naturally associated geometric object is the Cayley graph $\Gamma(G, A)$. Thus one might say that a class of groups equipped with specified finite generating sets

MSC2000: primary 20P05; secondary 03D15, 20F36, 57M05, 68W40.
Keywords: one-relator groups, Whitehead algorithm, generic-case complexity.

has the *isomorphism rigidity property* if whenever two groups from this class are isomorphic then their Cayley graphs on the *given* generating sets are isometric. Phenomena of this type were known for various classes of Coxeter and Artin groups; see, for example, [Rosas 1988; Prassidis and Spieler 2000; Bahls 2003; Brady et al. 2002; Mühlherr and Weidmann 2002]. In the present paper we obtain the first result of this kind for a class of groups given in terms of "general" finite presentations. We prove that if two "random" one-relator groups $G_u = \langle a_1, \dots, a_k | u = 1 \rangle$ and $G_v = \langle a_1, \dots, a_k | v = 1 \rangle$ are isomorphic then their Cayley graphs $\Gamma(G_u, \{a_1, \dots, a_k\})$ and $\Gamma(G_v, \{a_1, \dots, a_k\})$ are isometric. Indeed, their Cayley graphs are isomorphic as labeled graphs by a graph isomorphism which is only allowed to permute the label set $\{a_1, \dots, a_k\}^{\pm 1}$. This provides a conceptually new source of group-theoretic rigidity given by "random" or "generic" groups. Such rigidity arises not from structural restrictions, such as the structure of flats or of finite subgroups, but rather from the rigidity of "randomness" itself.

The theorems in this paper are based on combining very different probabilistic and algebraic techniques: the generic-case analysis of Whitehead's algorithm in this paper and the results of [Kapovich and Schupp 2005a] on the Nielsen uniqueness property for generic groups that utilized the graph minimization and genericity techniques developed in [Arzhantseva and Ol′shanskiĭ 1996]. Our goal is to obtain new algebraic and geometric applications and the probabilistic tool used in this paper, large deviation theory applied to finite state Markov chains, is quite basic from the point of view of probability theory. Nevertheless, combining it with algebraic and algorithmic considerations as well as with earlier probabilistic results on Nielsen Uniqueness produces surprisingly powerful results.

We adopt the following convention throughout this paper.

Convention 1.1. Let $F_k = F(a_1, \dots, a_k)$ be the free group of rank $k \geq 2$. The *group alphabet* is $\Sigma := \{a_1, \dots, a_k\}^{\pm 1}$. A word $w \in \Sigma^*$ is *reduced* if w does not contain any subwords of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$. The *length*, $|w|$, of a word w is the number of letters in w. Since every element of F_k can be represented by a unique reduced word, we can identify elements of F_k with reduced words. The length $|g|$ of an element $g \in F_k$ is the length of the unique reduced word in Σ^* which represents g.

A word w is *cyclically reduced* if all cyclic permutations of w are reduced. We use C to denote the set of all cyclically reduced words in F_k. Any reduced word w can be uniquely decomposed as a concatenation $w = vuv^{-1}$ where u is a cyclically reduced. The word u is called the *cyclically reduced form of* w and $\|w\| := |u|$ is the *cyclic length* of w.

An element $w \in F_k$ is *minimal* if $|\phi(w)| \geq |w|$ for all $\phi \in \mathrm{Aut}(F_k)$. In other words, w is a shortest element in its orbit $\mathrm{Aut}(F_k)w$.

Recall that the *automorphism problem* (also called the *automorphic conjugacy problem* or the *automorphic equivalence problem*) for a free group F_k is the following decision problem: Given two elements $u, v \in F_k$, is there an automorphism $\phi \in \mathrm{Aut}(F_k)$ such that $\phi(u) = v$? If there is such an automorphism we say that u and v are *automorphically equivalent*. An algorithm for solving this problem was given in the classic paper [Whitehead 1936]. We need to give a brief description of Whitehead's solution, and more details are given in Section 4 below. Whitehead introduced a particular finite set of generators of $\mathrm{Aut}(F_k)$, now called *Whitehead automorphisms*. These automorphisms are divided in two types. The Whitehead automorphisms of the *first kind* are "relabeling automorphisms" induced by permutations of the set $\{a_1, \ldots, a_k\}^{\pm 1}$ and thus do not change the length of an element. The remaining Whitehead automorphisms are of the *second kind* and can change the length of an element. These automorphisms are precisely defined in Definition 4.2 below.

Proposition 1.2 (Whitehead's Theorem [1936]).

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

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

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

This statement immediately gives Whitehead's algorithm for solving the automorphism problem for F_k. First, by length reduction there is a algorithm which, given any element $w \in F_k$, finds a minimal element $w' \in \mathrm{Aut}(F_k)w$. To start, cyclically reduce w. Then repeatedly check if there is a Whitehead automorphism τ decreasing the cyclically reduced length of the current element and if so, apply such a τ and cyclically reduce the result. This process terminates in at most $|w|$ steps with a minimal element and requires at worst quadratic time in the length of w. Each step takes at most linear time since the number of Whitehead automorphisms is fixed. Thus given two elements of F_k we can first replace them by minimal $\mathrm{Aut}(F_k)$-equivalent elements. By peak reduction, if these minimal elements have different lengths then there does not exist an automorphism taking one of original elements to the other. This quadratic time procedure is the so-called "easy part" of Whitehead's algorithm.

Now suppose that starting with elements $u, v \in F_k$ the process above yields corresponding minimal elements u', v' of the same length. Peak reduction implies that if these two minimal elements are automorphically equivalent then there is

a chain of Whitehead automorphisms taking one element to the other so that the *cyclically reduced length is constant throughout the chain*. Since the number of elements of given length is bounded by an exponential function, this provides an algorithm which is at worst exponential time for deciding if two minimal elements of the same length are in the same $\mathrm{Aut}(F_k)$-orbit. This stage is called the "hard part" of Whitehead's algorithm.

Taken together, these two parts provide a complete solution for the automorphism problem for F_k and requires *at most exponential time* in terms of the maximum of the lengths of the input words. Note that Whitehead's algorithm actually solves the *Search Automorphism Problem* as well. If u, v are in the same $\mathrm{Aut}(F_k)$-orbit, the algorithm produces an explicit automorphism taking u to v.

Whether or not Whitehead's algorithm actually requires exponential time is currently an active research question. The only well understood case is $k = 2$, where Myasnikov and Shpilrain [2003] proved that an improved version of Whitehead's algorithm takes at most polynomial time. Substantial further progress for $k = 2$ has been made by Bilal Khan [2004]. Very interesting partial results regarding the complexity of Whitehead's algorithm for $k > 2$ have recently been obtained by Donghi Lee [2003].

Experimental evidence (see, for example, [Booth et al. 2004; Haralick et al. 2005; Miasnikov and Myasnikov 2004]) strongly indicates that even for $k > 2$ Whitehead's algorithm usually runs very quickly. In the present paper we provide a theoretical explanation of this phenomenon and prove that for an "exponentially generic" set of inputs the "easy" first stage of the Whitehead algorithm terminates immediately and the "hard" second part terminates in linear time.

The study of genericity, or "typical behavior", in group theory was initiated by Gromov [1987; 1993], Ol′shanskii [1992] and Champetier [1994]. The importance of these ideas is becoming increasingly clear and manifestations of genericity in many different group-theoretic contexts are the subject of active investigation [Arzhantseva 1997; 1998; 2000; Arzhantseva and Ol′shanskiĭ 1996; Champetier 1994; 1995; 2000; Cherix and Valette 1996; Cherix and Schaeffer 1998; Żuk 2002; Kapovich and Schupp 2005a; Ghys 2004; Gromov 2003; Kapovich et al. 2003; Kapovich et al. 2005; Ollivier 2003]. Intuitively, a subset Q of $S \subseteq F_k$ is generic in S if a "randomly" chosen long element of S belongs to Q with probability tending to 1, or that Q has "measure 1" in S. The precise definitions of genericity used in [Kapovich et al. 2003; Kapovich et al. 2005] are given in Definition 2.1 below.

We need the following crucial definition.

Definition 1.3. A cyclically reduced element $w \in F_k$ is *strictly minimal* if the cyclically reduced length $\|\tau(w)\|$ is strictly greater than $|w|$ for every noninner Whitehead automorphism τ of the second kind. We use SM to denote the set of

all strictly minimal elements of F_k. Also, SM' denotes the set of all $w \in F_k$ such that the cyclically reduced form of w belongs to SM.

The description of Whitehead's algorithm given above shows that every element of SM is already minimal in its $\mathrm{Aut}(F_k)$-orbit. Moreover, if $w \in SM$ then any chain of Whitehead moves that preserves the cyclic length of w must consist entirely of conjugations and of Whitehead automorphisms of the first kind, that is, relabeling automorphisms. Thus if $w \in SM$ and $w' \in F_k$ is another minimal element with $|w| = |w'|$ then Whitehead's algorithm, applied to the pair (w, w'), terminates in time linear in $|w|$. Moreover, for arbitrary $(w_1, w_2) \in F_k^2$ such that at least one of w_1, w_2 is $\mathrm{Aut}(F_k)$-equivalent to a strictly minimal element, Whitehead's algorithm terminates in at most quadratic time on (w_1, w_2).

We give here a short informal summary of our results regarding Whitehead's algorithm and the properties of random one-relator groups. Precise and detailed statements are given in Section 3.

Convention 1.4. For $u \in F_k$ set $G_u = \langle a_1, \ldots, a_k | u \rangle$.

By saying that a certain property holds for a generic element we mean that there is an exponentially generic set such that every element of that set has the property. We prove that:

(a) The cyclically reduced form of a generic element of F_k is strictly minimal and a generic cyclically reduced element is strictly minimal.

(b) The generic-case complexity of Whitehead's algorithm for F_k is strongly linear-time.

(c) For any $u \in F_k$ the orbit $\mathrm{Aut}(F_k)u$ is an exponentially negligible subset of F_k. Moreover, all such orbits are "uniformly small" in F_k. Namely, there is a number $\alpha < 2k - 1$ such that for any $u \in F_k$ the exponential growth rate of $\mathrm{Aut}(F_k)u$ is at most $\alpha < 2k - 1$. (The growth rate of F_k is $2k - 1$.)

(d) For a generic element $u \in F_k$ the stabilizer of u in $\mathrm{Aut}(F_k)$ is infinite cyclic and is generated by the inner automorphism corresponding to conjugation by u.

(e) For a generic $u \in F_k$ the one-relator group G_u is a complete group, that is, it has trivial center and trivial outer automorphism group.

(f) A generic one-relator group G_u is torsion-free, nonelementary and word-hyperbolic, and it has either the Menger curve or the Sierpiński carpet as its boundary. If $k = 2$ the boundary is the Menger curve.

(g) If we *fix* a generic one-relator group G_u then there is a quadratic-time algorithm (in terms of $|v|$) which decides if an *arbitrary* one-relator group $G_v = \langle a_1, \ldots, a_k | v \rangle$ is isomorphic to G_u.

(h) Two generic one-relator groups G_u, G_v are isomorphic if and only if $|u| = |v|$ and there is a relabeling automorphism τ such that $\tau(u)$ is a cyclic permutation of v or v^{-1}.

(i) The number $I_k(n)$ of *isomorphism types* of one-relator groups on k generators with defining relators of length n satisfies

$$\frac{c_1}{n}(2k-1)^n \leq I_k(n) \leq \frac{c_2}{n}(2k-1)^n,$$

where $c_1 = c_1(k) > 0$, $c_2 = c_2(k) > 0$ are constants independent of n.

The structure of Whitehead's algorithm for solving the automorphism problem is similar to that of Garside's algorithm (and its various modifications) for solving the conjugacy problem in braid groups. (See for example [Garside 1969; Birman et al. 1998; Franco and González-Meneses 2003].) In both cases there has been a great deal of experimental evidence that in practice the algorithms almost always work much faster than the worst-case exponential time estimate suggests. Statements (a) and (b) above provide the first proof explaining why this happens for Whitehead's algorithm. It remains an interesting open problem to find and prove similar statements for Garside's algorithm.

As discussed earlier, statement (h) above may be regarded as an analogue of Mostow rigidity for random one-relator groups. Indeed, it says that two generic one-relator groups G_u and G_v are isomorphic if and only if their Cayley graphs corresponding to the *given* generating sets $\{a_1, \ldots, a_k\}$ are isomorphic as labeled graphs where the graph isomorphism is only allowed to permute the label set $\{a_1, \ldots, a_k\}^{\pm 1}$. This means that the class of random one-relator groups has the isomorphism rigidity property. We will see that isomorphism rigidity is also responsible for us being able to estimate the number of isomorphism types of one-relator groups in the statement (i) above. In subsequent work Kapovich and Schupp [2005b] combine the results of this paper with methods involving Kolmogorov complexity to prove that a random one-relator presentation G_u is "essentially incompressible". This means that G_u does not admit any finite group presentation of total length much smaller than $|u|$.

2. Generic sets and Generic Complexity

We need to recall the definitions concerning genericity used in [Kapovich et al. 2003]. Note that the length condition on sets of pairs which we consider here is slightly different from that used in [Kapovich et al. 2003].

We say that a sequence $x_n \in \mathbb{R}$, $n \geq 1$ with $\lim_{n\to\infty} x_n = x \in \mathbb{R}$ *converges exponentially fast* if there are $0 < \sigma < 1$ and $K > 0$ such that for all $n \geq 1$

$$|x - x_n| \leq K\sigma^n.$$

Definition 2.1. Let S be a set of words in the group alphabet Σ. Let $\rho(n, S)$ denote the number of words $w \in S$ with $|w| \leq n$. Also, let $\gamma(n, S)$ denote the number of words $w \in S$ with $|w| = n$.

We say that a subset $B \subseteq S$ is *generic in* S if

$$\lim_{n\to\infty} \frac{\rho(n, B)}{\rho(n, S)} = 1.$$

If, in addition, the convergence is exponentially fast, we say that B is *exponentially generic in* S.

The complement of an (exponentially) generic set in S is said to be *(exponentially) negligible in* S.

Similarly, let $D \subset S \times S$ and let $\rho(n, D)$ denote the number of pairs $(u, v) \in D$ such that $|u| \leq n$ and $|v| \leq n$. Note that $\rho(n, S \times S) = \rho(n, S)^2$. We say that D is *generic in* $S \times S$ if

$$\lim_{n\to\infty} \frac{\rho(n, D)}{\rho(n, S \times S)} = 1.$$

Again, if convergence is exponentially fast, we say that D is *exponentially generic in* $S \times S$.

We can now apply this concept to decision problems. The following notion was introduced in [Kapovich et al. 2003].

Definition 2.2 (Generic-case complexity). Let $S \subseteq \Sigma^*$ be an infinite set of words and let $D \subseteq S \times S$. (We regard the set $S \times S$ as the set of all inputs for a decision problem D, so that we are now working relative to S).

Suppose that Ω is a partial algorithm for deciding if an element $(u, v) \in S \times S$ belongs to D. Note that this means that Ω is *correct*. That is, whenever Ω does produce a definite answer, that answer is correct. Let $t(n) \geq 0$ be a nondecreasing function. We say that Ω *solves D with strong generic-case time complexity bounded by t in $S \times S$* if there exists an exponentially $S \times S$-generic subset $A \subset S \times S$ such that for any $(u, v) \in A$ with $|u| \leq n$, $|v| \leq n$ the algorithm Ω terminates on the input (u, v) in at most $t(n)$ steps.

Let S, D be as above and let $\mathcal{B}$ be a deterministic time complexity class such as linear time, quadratic time, polynomial time, etc. We say that D is *decidable with strong S-generic case complexity in $\mathcal{B}$* if there exist a function $t(n)$ satisfying the constraints of the complexity class $\mathcal{B}$ and a correct partial algorithm Ω that solves D with strong generic-case time complexity bounded by t in $S \times S$.

3. Main results

We can now state our main results regarding Whitehead's algorithm in more technical detail.

Theorem A. *Let $F_k = F(a_1, \dots, a_k)$, where $k \geq 2$.*

(1) *The set $SM \subseteq C$ is exponentially C-generic and the set $SM' \subseteq F_k$ is exponentially F_k-generic. Hence the set $SM \times SM \subseteq C \times C$ is exponentially $C \times C$-generic and the set $SM' \times SM' \subseteq F_k \times F_k$ is exponentially $F_k \times F_k$-generic.*

(2) *There is a linear time (in $|w|$) algorithm which, given a freely reduced word w, decides whether or not $w \in SM$ and whether or not $w \in SM'$.*

(3) *Every $w \in SM$ is minimal in its* $\mathrm{Aut}(F_k)$*-orbit; that is, for every $\alpha \in \mathrm{Aut}(F_k)$ we have $|w| \leq |\alpha(w)|$.*

Moreover, if $w \in SM$ and v is a cyclically reduced word with $|w| = |v|$ then w and v are in the same $\mathrm{Aut}(F_k)$*-orbit if and only if there exists a Whitehead automorphism τ of the first kind such that $\tau(w)$ is a cyclic permutation of v.*

(4) *Whitehead's algorithm works in* linear time *on pairs $(u, v) \in SM \times SM$ and so has strongly linear time generic-case complexity on $C \times C$. Similarly, Whitehead's algorithm works in linear time on pairs $(u, v) \in SM' \times SM'$ and so has strongly linear time generic-case complexity on $F_k \times F_k$.*

(5) *Whitehead's algorithm works in at most* quadratic time *on* all *pairs (u, v) such that at least one of u, v is in the same* $\mathrm{Aut}(F_k)$*-orbit as an element of SM.*

The theorem above says that for a "random" pair of cyclically reduced words (u, v) both u and v are strictly minimal. Hence the "easy" first part of Whitehead's algorithm terminates in a single step and the "hard" second part reduces to simply checking if one can get from u to v by applying a relabeling automorphism and then a cyclic permutation.

Recall that for a subset $S \subseteq F_k$ the *exponential growth rate* or *growth entropy* of S is

$$H(S) := \limsup_{n\to\infty} \sqrt[n]{\rho(n, S)}.$$

Then $H(F_k) = 2k - 1$ and $S \subseteq F_k$ is exponentially F_k-negligible if and only if $H(S) < 2k - 1$.

Corollary 3.1. *For any $w \in F_k$ the set* $\mathrm{Aut}(F_k)w$ *is exponentially negligible in F_k and the set $C \cap \mathrm{Aut}(F_k)w$ is exponentially negligible in C. Moreover*

$$H(\mathrm{Aut}(F_k)w) \leq H(F - SM') < 2k - 1.$$

Proof. We may assume that w is minimal. Let L be the set of elements of length $|w|$ in the orbit $\mathrm{Aut}(F_k)w$. Now L is finite and any element in $\mathrm{Aut}(F_k)w - L$ is not minimal and hence not strictly minimal. Therefore $T := C \cap [\mathrm{Aut}(F_k)w - L] \subseteq C - SM$. By part (1) of Theorem A the set $C - SM$ is exponentially C-negligible and therefore so is the set T. We have $C \cap \mathrm{Aut}(F_k)w = T \cup (C \cap L)$ and therefore $C \cap \mathrm{Aut}(F_k)w$ is C-negligible, as claimed.

Let u be an arbitrary element of $\mathrm{Aut}(F_k)w$. Since u need not be cyclically reduced let u_0 be the cyclically reduced form of u.

If $u_0 \notin SM$ then u is contained in the set $F_k - SM'$ which is exponentially F_k-negligible by part (1) of Theorem A. Now suppose that u_0 is strictly minimal. Since u_0 is conjugate to u, $u_0 \in \mathrm{Aut}(F_k)w$. Since u_0 is minimal, $|u_0| = |w|$ and $u_0 \in L$. Thus u is contained in the F_k-conjugacy class of an element of L. It is not difficult to see that any conjugacy class in F_k has exponential growth rate $\sqrt{2k-1}$ and is thus exponentially negligible. Therefore the orbit $\mathrm{Aut}(F_k)w$ is contained in the union of finitely many exponentially F_k-negligible sets and is exponentially F_k-negligible, as required.

Moreover, the set $F_k - SM'$ contains the conjugacy class of a_1. Thus

$$H(F_k - SM') \geq \sqrt{2k-1}.$$

The previous argument shows that $\mathrm{Aut}(F_k)w$ is contained in the union of $F - SM'$ and of finitely many F_k-conjugacy classes $K_1, \ldots, K_m$. Hence

$$\begin{aligned} H(\mathrm{Aut}(F_k)w) &\leq \max\{H(F_k - SM'), H(K_1), \ldots, H(K_m)\} = H(F_k - SM') \\ &< 2k-1, \end{aligned}$$

where the last inequality holds since SM' is exponentially F_k-generic and $F_k - SM'$ is exponentially F_k-negligible. □

Corollary 3.1 shows that automorphic orbits in F_k are "uniformly small" in the sense of their growth rate. This can be viewed as a generalization of the results from [Borovik, Myasnikov and Shpilrain 2002] and [Burillo and Ventura 2002], papers that establish (with specific quantitative growth estimates) that the set of primitive elements is exponentially negligible in F_k.

As mentioned before, the worst-case complexity of Whitehead's algorithm is known to be polynomial time for $k = 2$. The results of [Kapovich et al. 2005] and Theorem A imply that the *average-case* complexity (as opposed to generic-case) of Whitehead's algorithm is linear time for $k = 2$.

A deep result of McCool [1975] shows that for any $w \in F_k$ the stabilizer of w in $\mathrm{Aut}(F_k)$ is finitely presentable. Similar arguments as those used in the proof of Theorem A allow us to conclude that $\mathrm{Aut}(F_k)$-stabilizers of generic elements of F_k are very small.

Definition 3.2. The set TS (for "trivial stabilizer") is the set of all words $w \in SM$ (necessarily cyclically reduced) such that w is not a proper power and such that for every nontrivial relabeling automorphism τ of F_k the elements w and $\tau(w)$ are not conjugate in F_k. Also, TS' denotes the set of all elements of F_k whose cyclically reduced form is in TS.

Theorem B. *Let $k \geq 2$. Then*:

(1) *The set TS' is exponentially F_k-generic and the set TS is exponentially C-generic.*

(2) *There is a linear-time (in terms of $|w|$) algorithm which, given a freely reduced word w, decides if $w \in TS'$ or if $w \in TS$.*

(3) *For any nontrivial $w \in TS'$ the stabilizer* $\mathrm{Aut}(F_k)_w$ *of w in* $\mathrm{Aut}(F_k)$ *is the infinite cyclic group generated by the inner automorphism $ad(w)$ of F_k. Here $ad(w) : u \mapsto wuw^{-1}$ for $u \in F_k$.*

(4) *For every $w \in TS'$ the stabilizer* $\mathrm{Out}(F_k)_w$ *of the conjugacy class of w in* $\mathrm{Out}(F_k)$ *is trivial.*

These results, together with the work of Kapovich and Schupp [2005a] on the isomorphism problem for one-relator groups yield strong conclusions about the properties of generic one-relator groups. There are several different notions of genericity in the context of finitely presented groups, namely genericity in the sense of Arzhantseva and Ol′shanskii [1996] and in the sense of Gromov [1987] (see also [Ol′shanskiĭ 1992]). These two notions essentially coincide in the case of one-relator groups. Recall that a group G is *complete* if all automorphisms of G are inner (so that $\mathrm{Out}(G) = \{1\}$) and if G also has trivial center so that the adjoint map $ad : G \to \mathrm{Aut}(G)$ is an isomorphism.

Theorem C. *There exists an exponentially C-generic set Q_k of nontrivial cyclically reduced words in F_k with the following properties*:

(1) *There is an exponential time (in $|w|$) algorithm which, given a cyclically reduced word w, decides whether or not $w \in Q_k$.*

(2) *Let $u \in Q_k$. Then the one-relator group G_u is a complete one-ended torsion-free word-hyperbolic group.*

(3) *If $u \in Q_k$ then the hyperbolic boundary ∂G_u is homeomorphic to either the Menger curve or the Sierpiński carpet. If $k = 2$ then ∂G_u is homeomorphic to the Menger curve.*

(4) *Let $u, v \in Q_k$. Then the groups G_u and G_v are isomorphic if and only if there exists a relabeling automorphism τ of F_k such that $\tau(u)$ is a cyclic permutation of either v or v^{-1}. In particular, $G_u \cong G_v$ implies $|u| = |v|$.*

(5) *Let $u \in Q_k$ be a fixed element. Then there exists a quadratic time algorithm (in terms of $|v|$) which, given an* arbitrary *$v \in F_k$, decides if the groups G_u and G_v are isomorphic.*

A result of Champetier [1995], obtained by completely different methods, states that generic (in the sense of [Gromov 1993; Ol′shanskiĭ 1992]) *two-relator* groups are word-hyperbolic with boundary homeomorphic to the Menger curve.

Prior to Theorem C there were no known nontrivial examples of complete one-relator groups and some experts in the field believed that such groups might not exist. Our proof that such groups do exist is obtained by an indirect probabilistic argument. The set Q_k is obtained as the intersection $Q_k = R_k \cap Z_k$ of two exponentially C-generic sets, R_k and Z_k, and hence Q_k is also exponentially generic. In particular it is certainly nonempty. The genericity of the sets R_k and Z_k is established using two very different methods: namely, the Arzhantseva–Ol′shanskii graph-minimization method in [Kapovich and Schupp 2005a] and large deviation theory in the present paper. This demonstrates the strength of the "probabilistic argument" for producing groups with genuinely new and often unexpected features.

In the definitions of genericity both in the sense of Gromov [Gromov 1993; Ol′shanskiĭ 1992] and in the sense of Ol′shanskii [Arzhantseva and Ol′shanskiĭ 1996] one counts group presentations as opposed to group isomorphism classes. It is very natural to ask, for fixed numbers of generators and defining relators, how many *isomorphism types* there are of groups with particular constraints on the lengths of the relators. As a corollary of Theorem C it turns out that the number of *isomorphism types* of one-relator groups with relators of length n grows in essentially the same way (taking into account the obvious symmetries) as the number of one-relator presentations with relators of length n.

Corollary 3.3. *Let $k \geq 2$ be an integer. For $n \geq 1$ define $I_k(n)$ to be the number of* isomorphism types *among the groups given by presentations $\langle a_1, \ldots, a_k | u = 1\rangle$ where u varies of the set of all cyclically reduced words of length n. Then there exist constants $A = A(k) > 0$, $B = B(k) > 0$ such that for any $n \geq 1$*

$$\frac{B}{n}(2k-1)^n \leq I_k(n) \leq \frac{A}{n}(2k-1)^n.$$

Proof. Let Q_k be the exponentially generic set of cyclically reduced words given by Theorem C and recall that C denotes the set of all cyclically reduced words.

It follows from Lemma 6.1 below that the number $\gamma(n, C)$ of cyclically reduced words of length n satisfies

$$c_2(2k-1)^n \geq \gamma(n, C) \geq c_1(2k-1)^n$$

for some constants $c_1, c_2 > 0$ independent of n.

Since Q_k is exponentially C-generic, Lemma 6.1 below implies that

$$\lim_{n\to\infty} \frac{\gamma(n, Q_k)}{\gamma(n, C)} = 1.$$

Thus there is $n_0 > 1$ such that for any $n \geq n_0$ we have

$$\gamma(n, Q_k) \geq \tfrac{1}{2}\gamma(n, C) \geq \tfrac{1}{2}c_1(2k-1)^n.$$

Let M be the number of all Whitehead automorphisms of the first kind (that is, relabeling automorphisms). Let $n \geq n_0$ and let $u \in Q_k$ with $|u| = n$. Part 4 of Theorem C implies that the number of $v \in Q_k$ with $G_v \cong G_u$ is at most $2nM$. Here the factor of $2n$ corresponds to the number of cyclic permutations of $u^{\pm 1}$.

Therefore for $n \geq n_0$:

$$I_k(n) \geq \frac{\gamma(n, Q_k)}{2Mn} \geq \frac{c_1}{4Mn}(2k-1)^n.$$

The set PP of cyclically reduced proper powers is exponentially negligible in C; see [Arzhantseva and Ol′shanskiĭ 1996]. Thus there exist $K > 0$ and $0 < \sigma < 1$ such that for any $n \geq 1$ we have

$$\gamma(n, PP) \leq K\sigma^n \gamma(n, C) \leq Kc_2\sigma^n(2k-1)^n.$$

It is easy to see that if u is cyclically reduced of length n and is not a proper power, then all n cyclic permutations of u are distinct words. Clearly, if v is a cyclic permutation of u then $G_u \cong G_v$.

Therefore

$$I_k(n) \leq \frac{\gamma(n, C - PP)}{n} + \gamma(n, PP) \leq \frac{c_2}{n}(2k-1)^n + \gamma(n, PP) \leq \frac{2c_2}{n}(2k-1)^n,$$

where the last inequality holds for all sufficiently large n. □

Via an additional technical argument, Kapovich and Schupp [2005b] improve the estimate for $I_k(n)$ and establish that

$$\lim_{n\to\infty} \frac{nI_k(n)}{(2k-1)^n} = \frac{1}{k!2^{k+1}}.$$

4. Whitehead automorphisms

We follow [Lyndon and Schupp 1977, Chapter I] in recalling the basic definitions and results about Whitehead automorphisms.

Convention 4.1. If u and w are words in the alphabet Σ, then w_u will denote the number of occurrences of u as a subword of w. In particular, if $a \in \Sigma$ is a letter, then w_a is the number of occurrences of the letter a in w and if $x, y \in \Sigma$ with $y \neq x^{-1}$ then w_{xy} is the number of occurrences of xy in w.

Definition 4.2 (Whitehead automorphisms). A *Whitehead automorphism* of F_k is an automorphism τ of F_k 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 $a \in \Sigma$, called 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_k, we always have $\tau(a) = a$ in this case). To every such τ we associate a pair (A, a) where a is as above and A consists of all those elements of Σ, including a but excluding a^{-1}, such that $\tau(x) \in \{xa, a^{-1}xa\}$. We say that (A, a) is the *characteristic pair* of τ.

Note that for any $a \in \Sigma$ the inner automorphism $ad(a)$ is a Whitehead automorphism of the second kind. Observe also that the set SM of strictly minimal words is closed under applying relabeling Whitehead automorphisms, cyclic permutations and taking inverses.

Here is an immediate corollary of Proposition 1.2.

Proposition 4.3. *Let w be a cyclically reduced word of length $n > 0$ such that $w \in SM$. Let w' be a cyclically reduced word of length n.*

Then $w' \in \mathrm{Aut}(F_k)w$ if and only if there is a relabeling Whitehead automorphism τ such that w' is a cyclic permutation of $\tau(w)$.

Remark 4.4. It is easy to see that primitive elements of F_k are never strictly minimal.

If $u \in F_k$ is primitive and $|u| > 1$ then u is not minimal and hence not strictly minimal. Suppose now that $|u| = 1$, so that u is a_i^{ϵ} (where $\epsilon \in \{1, -1\}$). Pick an index $j \neq i$, $1 \leq i \leq j$. Consider the Whitehead automorphism τ of the second kind which sends a_j to $a_j a_i$ and fixes all a_t for $t \neq j$. Then $\tau(u) = u$, and hence u is not strictly minimal.

Definition 4.5 (Weighted Whitehead graph). Let w be a nontrivial cyclically reduced word in Σ^*. Let c be the first letter of w. Thus the word wc is freely reduced. (We use the word wc so that we need only consider linear words as opposed to cyclic words.)

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 $x \neq y^{-1}$ there is an undirected edge in Γ_w from x^{-1} to y labeled by the sum $\hat{w}_{xy} := (wc)_{xy} + (wc)_{y^{-1}x^{-1}}$. where $(wc)_{xy}$ is the number of occurrences of xy in wc and $(wc)_{y^{-1}x^{-1}}$ is the number of occurrences of $y^{-1}x^{-1}$ in wc.

One can think of $\hat{w}_{xy}$ as the number of occurrences of xy and $y^{-1}x^{-1}$ in the "cyclic" word defined by w. There are $k(2k-1)$ undirected edges in Γ_w. Edges may have label zero, but there are no edges from a to a for $a \in \Sigma$. It is easy to see that for any cyclic permutation v of w or of w^{-1} we have $\Gamma_w = \Gamma_v$.

Convention 4.6. Let w be a fixed nontrivial cyclically reduced word. For two subsets $X, Y \subseteq \Sigma$ we denote by $X.Y$ the sum of all edge-labels in the weighted Whitehead graph Γ_w of w of edges from elements of X to elements of Y. Thus for

$x \in \Sigma$ the number $x.\Sigma$ is equal to $w_x + w_{x^{-1}}$, the total number of occurrences of $x^{\pm 1}$ in w.

The next lemma gives an explicit formula for the difference of the lengths of w and $\tau(w)$, where τ is a Whitehead automorphism.

Lemma 4.7 [Lyndon and Schupp 1977, Chapter I, Proposition 4.16]. *Let w be a nontrivial cyclically reduced word and let τ be a Whitehead automorphism of the second kind with the characteristic pair (A, a). Let $A' = \Sigma - A$. Then*

$$\|\tau(w)\| - \|w\| = A.A' - a.\Sigma.$$

Proposition 4.3 guarantees fast performance of Whitehead's algorithm on strictly minimal words. It turns out that a cyclically reduced word w is strictly minimal if the distribution of the numbers on the edges of the weighted Whitehead graph of w, divided by $|w|$, is close to the uniform distribution as are the frequencies with which individual letters occur in w.

Lemma 4.8 (Strict minimality criterion). *Let*

$$0 < \epsilon < \frac{2k-3}{k(2k-1)(4k-3)}.$$

Suppose w is a cyclically reduced word of length n such that

(a) *for every letter $x \in \Sigma$ we have*

$$\frac{w_x}{n} \in \Big(\frac{1}{2k} - \frac{\epsilon}{2}, \frac{1}{2k} + \frac{\epsilon}{2}\Big);$$

(b) *for every edge in the weighted Whitehead graph of w the label of this edge, divided by n, belongs to*

$$\Big(\frac{1}{k(2k-1)} - \epsilon, \frac{1}{k(2k-1)} + \epsilon\Big).$$

Then for any noninner Whitehead automorphism τ of $F(a_1, \ldots, a_k)$ of second kind we have $\|\tau(w)\| > \|w\| = |w|$, so that $w \in SM$.

Proof. Let (A, a) be the characteristic pair of τ and let $A' = \Sigma - A$. Since τ is assumed to be noninner, we have both $|A| \geq 2$, and $|A'| \geq 2$. Hence $|A|\ |A'| \geq 2(2k-2)$ and there are at least $2(2k-2)$ edges between A and A' in the weighted Whitehead graph of w. Recall that $a.\Sigma$ is the total number of occurrences of $a^{\pm 1}$ in w.

By Lemma 4.7, $\|\tau(w)\| - \|w\| = A.A' - a.\Sigma$. By assumption on w we have $a.\Sigma \leq n(\frac{1}{k} + \epsilon)$ and

$$\|\tau(w)\| - \|w\| = A.A' - a.\Sigma \geq 2n(2k-2)\Big(\frac{1}{k(2k-1)} - \epsilon\Big) - n\Big(\frac{1}{k} + \epsilon\Big) > 0,$$

where the last inequality holds by the choice of ϵ. □

We will see later that the strict minimality criterion holds for an exponentially generic set of cyclically reduced words.

5. A little probability theory

Fortunately, probability theory provides us with a good way of estimating the relative frequencies with which particular one- and two-letter words occur as subwords in freely reduced words of length n in a free group F_k. This tool is called "large deviation theory". Since we are only interested in applications of large deviation theory, we refer the reader to Chapter 3 of the excellent and comprehensive book [Dembo and Zeitouni 1998] and give only a brief overview of how this theory works. The statements most relevant to our discussion are Theorems 3.1.2, 3.1.6 and 3.1.13 of that reference.

Convention 5.1. Let Σ be as in Convention 1.1. Suppose $\Pi = (\Pi_{ij})_{i,j\in\Sigma}$ is the transition matrix of a Markov process with a finite set of states Σ. Suppose Π is *irreducible*, that is, for every position (i, j) there is $m > 0$ such that $(\Pi^m)_{i,j} > 0$. Assume also that Π is *aperiodic*, that is, for each $i \in \Sigma$ the gcd of all $m > 0$ such that $(\Pi^m)_{i,i} > 0$ is equal to 1. Suppose also that the Markov process starts with some probability distribution on Σ. Let $f : \Sigma \to \mathbb{R}$ be a fixed function. Let $Y_1, \ldots, Y_n, \ldots$ be a Markov chain for this process. We are interested in estimating the probability that $\frac{1}{n}\sum_{i=1}^{n} f(Y_i)$ belongs to a particular interval $J \subseteq \mathbb{R}$, or, more generally, to a particular Borel subset of $\mathbb{R}$. This probability defines what is referred to as an *empirical measure* on $\mathbb{R}$. A similarly defined *pair empirical measure* counts $\frac{1}{n}\sum_{i=1}^{n} g(Y_i, Y_{i+1})$, where $g : \Sigma \times \Sigma \to \mathbb{R}$ is some function (in the summation one takes $Y_{n+1} = Y_1$).

Example 5.2. In a typical application to free groups, a freely reduced word $w = Y_1 \ldots Y_n$ in a free group $F(a_1, \ldots, a_k)$, $k > 1$, can be viewed as such a Markov chain for a Markov process with the set of states $\Sigma = \{a_1 \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}\}$ and with transition probabilities $\Pi_{x,y} = P(x|y) = 1/(2k-1)$ if $y \neq x^{-1}$ and $\Pi_{x,y} = P(x|y) = 0$ if $y = x^{-1}$, where $x, y \in \Sigma$. The initial distribution on Σ is uniform, so that for any $x \in \Sigma$ the probability for a Markov chain to start at x is $1/(2k)$. The sample space for the Markov process of length n consists of *all* words of length n in Σ. However, a word which is not freely reduced will occur as a trajectory with zero probability because of the definition of $\Pi_{x,y}$. It is easy to see that this Markov process induces precisely the uniform distribution on the set of all freely reduced words of length n and the probability assigned to a freely reduced word of length $n \geq 1$ is

$$\frac{1}{2k(2k-1)^{(n-1)}}.$$

If we want to count the number w_a of occurrences of $a \in \Sigma$ in such a freely reduced word, we should take f to be the characteristic function of a, meaning that $f(a) = 1$ and $f(y) = 0$ for all $y \neq a$, $y \in \Sigma$. Then $(1/n) \sum_{i=1}^{n} f(Y_i)$ is precisely w_a/n. Similarly, if $g(a, b) = 1$ and $g(x, y) = 0$ for $(x, y) \neq (a, b)$ then the pair empirical measure essentially counts w_{ab}/n.

Going back to the general case, large deviation theory guarantees the existence of a *rate function* $I(x) \geq 0$ (with some additional good convexity properties) such that for any closed subset C of $\mathbb{R}$:

$$\limsup_{n\to\infty} \frac{1}{n} \log P\left(\frac{1}{n}\sum_{i=1}^{n} f(Y_i) \in C\right) \leq -\inf_{x\in C} I(x). \tag{1}$$

Therefore, if $\inf_{x\in C} I(x) = s > 0$ then for all but finitely many n we have

$$P\left(\frac{1}{n}\sum_{i=1}^{n} f(Y_i) \in C\right) \leq \exp(-sn/2)$$

and thus the above probability converges to zero exponentially fast when n tends to ∞.

Similarly, for any open subset $U \subseteq \mathbb{R}$ we have

$$\liminf_{n\to\infty} \frac{1}{n} \log P\left(\frac{1}{n}\sum_{i=1}^{n} f(Y_i) \in U\right) \geq -\inf_{x\in U} I(x),$$

so that for $s' = \inf_{x\in U} I(x) \geq 0$ we have

$$P\left(\frac{1}{n}\sum_{i=1}^{n} f(Y_i) \in U\right) \geq \exp(-2s'n) \tag{†}$$

for all sufficiently large n.

Large deviation theory also provides an explicit formula for computing the rate function $I(x)$ above and assures that in reasonably good cases, like Example 5.2 above, the function $I(x)$ is a strictly convex nonnegative function achieving its unique minimum at a point x_0 corresponding to the expected value of f (or the "equilibrium"). For instance, in the case of the Markov process for F_k considered in Example 5.2, the symmetry considerations imply that x_0 is the expected value of the number of occurrences of $a \in \Sigma = \{a_1, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}\}$, divided by n, in a freely reduced word w of length n in F_k — namely, $x_0 = \frac{1}{2k}$. Then the equality $I(x_0) = 0$ and large deviation theory [Dembo and Zeitouni 1998, Theorems 3.1.2 and 3.1.6] implies that for any $\epsilon > 0$ we have

$$\inf\left\{I(x) \mid x \in \left[0, \tfrac{1}{2k} - \epsilon\right] \cup \left[\tfrac{1}{2k} + \epsilon, 1\right]\right\} = s_\epsilon > 0.$$

The preceding computation means that for any fixed $\epsilon > 0$ we have

$$P\Big(\frac{w_a}{n} \in \big[0, \tfrac{1}{2k} - \epsilon\big] \cup \big[\tfrac{1}{2k} + \epsilon, 1\big] \;\Big|\; w \in F_k \text{ with } |w| = n\Big) \underset{n\to\infty}{\leq} \exp(-s_\epsilon n/2);$$

that is, this probability tends to zero exponentially fast when n tends to infinity.

Accordingly,

$$P\Big(\frac{w_a}{n} \in \big(\tfrac{1}{2k} - \epsilon, \tfrac{1}{2k} + \epsilon\big) \;\Big|\; w \in F_k \text{ with } |w| = n\Big) \to_{n\to\infty} 1$$

and the convergence is exponentially fast.

We present a formula for computing $I(x)$ for reference purposes. Let Π, Σ, f be as in Convention 5.1. Then formula (1) holds with

$$I(x) = \sup_{\theta\in R} \theta x - \log \rho(\Pi_\theta).$$

Here Π_θ is a $\Sigma \times \Sigma$-matrix, where the entry in the position (i, j) is $\Pi_{ij} \exp(\theta f(j))$ and where $\rho(\Pi_\theta)$ is the Perron–Frobenius eigenvalue of Π_θ. The convexity of $I(x)$ follows from the fact that in the above formula $I(x)$ is obtained via a Legendre–Fenchel transform (also known as "convex conjugation") of a smooth function. A different explicit formula for $I(x)$ is given in [Dembo and Zeitouni 1998, Theorem 3.1.6].

Theorem 3.1.13 of the same reference also provides an analogue of (1) for the pair empirical measure corresponding to a finite state Markov process, which, in the context of Example 5.2 allows one to estimate the expected relative frequencies with which a fixed two-letter word occurs as a subword of a freely reduced word.

Recall that $\gamma(n, F_k) = 2k(2k-1)^{n-1}$ is the number of all freely reduced words of length n in F_k. When applied to the Markov process corresponding to freely reduced words in a free group F_k, as in Example 5.2 above, Theorems 3.1.2, 3.1.6 and 3.1.13 of [Dembo and Zeitouni 1998] imply:

Proposition 5.3. *Let $F_k = F(a_1, \ldots, a_k)$ be a free group of rank $k > 1$.*

(1) *For any $\epsilon > 0$ and for any $a \in \Sigma$ we have*

$$\lim_{n\to\infty} \frac{\#\Big\{w \in F_k \;\Big|\; |w| = n \text{ and } \frac{w_a}{n} \in \big(\frac{1}{2k} - \epsilon, \frac{1}{2k} + \epsilon\big)\Big\}}{\gamma(n, F_k)} = 1,$$

and the convergence is exponentially fast.

(2) *For any $a, b \in \Sigma$ such that $b \neq a^{-1}$ and for any $\epsilon > 0$ we have*

$$\lim_{n\to\infty} \frac{\#\Big\{w \in F_k \;\Big|\; |w| = n \text{ and } \frac{w_{ab}}{n} \in \Big(\frac{1}{2k(2k-1)} - \epsilon, \frac{1}{2k(2k-1)} + \epsilon\Big)\Big\}}{\gamma(n, F_k)} = 1,$$

and the convergence is exponentially fast.

It is worth noting, as pointed out to us by Steve Lalley, that one can also obtain the conclusion of Proposition 5.3 without using large deviation theory and relying instead on generating functions methods but such an approach would be longer and require considerably more computation.

6. Whitehead graphs of generic words

The next two preliminary statements are straightforward and we omit the proofs.

Lemma 6.1. *The following hold in* F_k:

(1) *For every* $n > 0$ *we have* $\gamma(n, C) \le \gamma(n, F_k) \le 2k\gamma(n, C)$ *and* $\rho(n, C) \le \rho(n, F_k) \le 2k\rho(n, C)$. *Moreover,*

$$\gamma(n, F_k) = 2k(2k-1)^{n-1} \quad \text{and} \quad \rho(n, F_k) = 1 + \frac{k}{k-1}((2k-1)^n - 1).$$

(2) *A set* $D \subseteq F_k$ *is exponentially* F_k*-negligible if and only if* $\dfrac{\gamma(n, D)}{(2k-1)^n} \to 0$ *exponentially fast when* $n \to \infty$.

(3) *A set* $D \subseteq C$ *is exponentially* C*-negligible if and only if* $\dfrac{\gamma(n, D)}{(2k-1)^n} \to 0$ *exponentially fast when* $n \to \infty$.

(4) *A subset* $D \subseteq F_k$ *is exponentially* F_k*-generic if and only if* $\dfrac{\gamma(n, D)}{\gamma(n, F_k)} \to 1$ *exponentially fast when* $n \to \infty$.

(5) *A subset* $D \subseteq C$ *is exponentially* C*-generic if and only if* $\dfrac{\gamma(n, D)}{\gamma(n, C)} \to 1$ *exponentially fast when* $n \to \infty$.

Proposition 6.2. *Let* $A \subseteq C$. *Let* A' *be the set of all freely reduced words in* F_k *whose cyclically reduced form belongs to* A. *Then*:

(1) *If* A *is exponentially* C*-negligible then* A' *is exponentially* F_k*-negligible*.

(2) *If* A *is exponentially* C*-generic then* A' *is exponentially* F_k*-generic*.

The above proposition shows that the notions of being exponentially F_k-generic and exponentially C-generic (same for negligible) essentially coincide.

The results of large deviation theory stated in Section 5 now allow us to describe the weighted Whitehead graph of a "random" cyclically reduced word of length n of F_k.

Proposition 6.3. *Let* $\epsilon > 0$ *be an arbitrary number. Let* $Q(n, \epsilon)$ *be the number of all cyclically reduced words* w *of length* n *such that for every edge of the weighted Whitehead graph of* w *the label of this edge, divided by* n, *belongs to the interval*

$$\Big(\frac{1}{k(2k-1)} - \epsilon, \frac{1}{k(2k-1)} + \epsilon\Big).$$

Similarly, for $a \in \Sigma$ let $T(n, a, \epsilon)$ be the number of all cyclically reduced words w of length n such that

$$\frac{w_a}{n} \in \Big(\frac{1}{2k} - \frac{\epsilon}{2}, \frac{1}{2k} + \frac{\epsilon}{2}\Big).$$

Then:

(1) *We have*

$$\lim_{n\to\infty} \frac{Q(n,\epsilon)}{\gamma(n,C)} = 1,$$

and the convergence is exponentially fast.

(2) *For any $a \in \Sigma$ we have*

$$\lim_{n\to\infty} \frac{T(n,a,\epsilon)}{\gamma(n,C)} = 1,$$

and the convergence is exponentially fast.

Proof. Denote $N_n = \gamma(n, F_k)$ and $C_n = \gamma(n, C)$. For a two-letter word xy in Σ^* denote by $E_{xy}(n,\epsilon)$ (correspondingly by $E'_{xy}(n,\epsilon)$) the number of all cyclically reduced (correspondingly freely reduced) words w of length n such that

$$\frac{w_{xy}}{n} \in \Big[0, \frac{1}{k(2k-1)} - \epsilon\Big] \cup \Big[\frac{1}{k(2k-1)} + \epsilon, 1\Big].$$

Similarly, for $a \in \Sigma$ let $E_a(n,\epsilon)$ (correspondingly $E'_a(n,\epsilon)$) denote the number of all cyclically reduced (correspondingly freely reduced) words w of length n such that

$$\frac{w_a}{n} \in \Big[0, \frac{1}{2k} - \epsilon\Big] \cup \Big[\frac{1}{2k} + \epsilon, 1\Big].$$

Fix a letter $a \in \Sigma$ and a two-letter word xy such that $y \neq x^{-1}$.

By Lemma 6.1 we know that $C_n \leq N_n \leq 2kC_n$. Also, since every cyclically reduced word is freely reduced, we have $E_a(n,\epsilon) \leq E'_a(n,\epsilon)$ and $E_{xy}(n,\epsilon) \leq E'_{xy}(n,\epsilon)$.

Therefore

$$\frac{E_a(n,\epsilon)}{C_n} \leq 2k\frac{E_a(n,\epsilon)}{N_n} \leq 2k\frac{E'_a(n,\epsilon)}{N_n} \to_{n\to\infty} 0$$

and

$$\frac{E_{xy}(n,\epsilon)}{C_n} \leq 2k\frac{E_{xy}(n,\epsilon)}{N_n} \leq 2k\frac{E'_{xy}(n,\epsilon)}{N_n} \to_{n\to\infty} 0$$

and the convergence in both cases is exponentially fast by Proposition 5.3.

Note that the label, which we denote $\hat{w}_{xy}$, on the edge $[x^{-1}, y]$ in the weighted Whitehead graph of a cyclically reduced word w differs at most by one from $w_{xy} + w_{y^{-1}x^{-1}}$ (since it is possible that w begins with y and ends with x or that w begins with x^{-1} and ends with x^{-1}).

Therefore for all sufficiently large n the condition

$$\left| \frac{\hat{w}_{xy}}{n} - \frac{1}{k(2k-1)} \right| < \frac{\epsilon}{2}$$

implies that

$$\left| \frac{w_{xy} + w_{y^{-1}x^{-1}}}{n} - \frac{1}{k(2k-1)} \right| < \epsilon.$$

Let $\hat{E}_{xy}(n, \epsilon)$ denote the number of all cyclically reduced words of length n such that

$$\left| \frac{\hat{w}_{xy}}{n} - \frac{1}{k(2k-1)} \right| \geq \epsilon.$$

Then

$$\frac{\hat{E}_{xy}(n, \epsilon)}{C_n} \leq 2k \frac{\hat{E}_{xy}(n, \epsilon)}{N_n} \leq 2k \frac{E'_{xy}(n, \epsilon/8) + E'_{y^{-1}x^{-1}}(n, \epsilon/8)}{N_n} \to_{n\to\infty} 0,$$

where the convergence is exponentially fast by Proposition 5.3. This implies the statement of Proposition 6.3. □

7. The generic complexity of Whitehead's algorithm

Remark 7.1. Before proving the main result, we need to discuss the complexity of the conjugacy problem in the free group F_k. Given freely reduced words u', v', we can find their cyclically reduced forms u and v in time linear in $\max\{|u'|, |v'|\}$) by successively canceling inverse pairs of letters from the two ends of each word. If $|u| \neq |v|$ then clearly u' is not conjugate to v' in F_k.

Suppose now that $|u| = |v| = n$. Then u' is conjugate to v' if and only if u is a cyclic permutation of v. The naive algorithm of comparing all cyclic permutations of u with v takes quadratic time. However, u is a cyclic permutation of v if and only if u is a subword of vv. There is a well-known pattern matching algorithm in computer science, called the Knuth–Morris–Pratt algorithm, which decides if a word u is a subword of a word z in time linear in $|u| + |z|$. See, for example, [Gusfield 1997] for details. Applied to the words u, vv, this algorithm allows us to decide if u is a cyclic permutation of v in linear time in n. Thus the conjugacy problem in F_k is actually solvable in time linear in terms of the maximum of the lengths of the two input words.

We can now prove Theorem A as stated in Section 3:

Proof of Theorem A. Choose

$$0 < \epsilon < \frac{2k-3}{k(2k-1)(4k-3)}.$$

Let $L(\epsilon)$ be the set of all cyclically reduced words w in Σ^* such that

(a) for every letter $a \in \Sigma$ we have

$$\frac{w_a}{n} \in \left(\frac{1}{2k} - \frac{\epsilon}{2}, \frac{1}{2k} + \frac{\epsilon}{2}\right)$$

(where $n = |w|$), and

(b) for every edge in the weighted Whitehead graph of w the label of this edge, divided by n, belongs to

$$\left(\frac{1}{k(2k-1)} - \epsilon, \frac{1}{k(2k-1)} + \epsilon\right).$$

By the strict minimality criterion (Lemma 4.8) we have $L(\epsilon) \subseteq SM$. Proposition 6.3 and Lemma 6.1 imply that $L(\epsilon)$ is exponentially C-generic. Therefore the bigger set SM is also exponentially C-generic. Hence by Proposition 6.2 the set SM' is exponentially F_k-generic and part (1) of the theorem is established.

For a fixed Whitehead automorphism τ and a freely reduced word $w \in F_k$ one can compute the freely reduced word $\tau(w)$ in time linear in $|w|$. Since the set of Whitehead automorphisms is a fixed finite set, one can thus decide in time linear in $|w|$ if a cyclically reduced word w belongs to SM. Thus part (2) of the theorem holds. Now Proposition 1.2 together with Remark 7.1 imply part (3), since there are only finitely many relabeling Whitehead automorphisms of the first kind.

In turn part (3) together with Proposition 1.2 implies parts (4) and (5). □

Remark 7.2. As stated in Theorem A, we can indeed decide if a cyclically reduced word w is strictly minimal, that is, $w \in SM$, in time linear in $|w|$ since the number of Whitehead automorphisms is fixed and finite. A priori however, this requires applying every Whitehead automorphism of the second kind to w and then computing the freely reduced form of the result. This may be undesirable if the rank k of F_k is large since the number of Whitehead automorphisms of the second kind grows exponentially with k.

On the other hand, the subset $L(\epsilon)$ of SM, defined as in the proof of Theorem A with $\epsilon = \frac{2k-3}{2k(2k-1)(4k-3)}$, is still exponentially generic according to the Strict Minimality Criterion. The membership problem in $L(\epsilon)$ is solvable much faster. All we need to do to decide if $w \in L(\epsilon)$ is to compute the frequencies with which the one- and two-letter subwords occur in w and then check if they belong to the required intervals. The number of one- and two-letter words that can occur in w only grows quadratically with k.

8. Stabilizers of generic elements

The above analysis also allows us to deduce that stabilizers of generic elements of F_k in $\mathrm{Aut}(F_k)$ and in $\mathrm{Out}(F_k)$ are very small.

We need to recall a property of automorphic orbits which is a direct corollary of [Lyndon and Schupp 1977, Chapter I, Proposition 4.17].

Proposition 8.1. *Let w, w' be minimal cyclically reduced words with $\|w\| = \|w'\|$ and let $\alpha \in \mathrm{Aut}(F_k)$ be such that $w' = \alpha(w)$. There exist Whitehead automorphisms τ_i, for $i = 1, \ldots, n$, such that $\alpha = \tau_n \ldots \tau_1$ in $\mathrm{Aut}(F_k)$ $\|\tau_i \ldots \tau_1(w)\| = \|w\|$ for each $i = 1, \ldots, n$.*

Recall that TS is the set of all $w \in SM$ such that w is not a proper power and such that for every nontrivial relabeling automorphism τ of F_k the elements w and $\tau(w)$ are not conjugate in F_k. Also, TS' is the set of elements of F_k whose cyclically reduced form is in TS.

It is easy to see that TS is closed under applying relabeling automorphisms and cyclic permutations.

Lemma 8.2. *Let $w \in TS$ be a nontrivial cyclically reduced word. Then*:

(1) *If $\alpha \in \mathrm{Aut}(F_k)$ is such that $\alpha(w)$ is conjugate to w then α is an inner automorphism of F_k.*

(2) *The stabilizer $\mathrm{Aut}(F_k)_w$ of w in $\mathrm{Aut}(F_k)$ is the infinite cyclic group generated by $ad(w)$.*

(3) *The stabilizer $\mathrm{Out}(F_k)_w$ of the conjugacy class of w in $\mathrm{Out}(F_k)$ is trivial.*

Proof. To see that (1) holds, suppose that $w \in TS$ and that $\alpha(w) = w$ for some $\alpha \in \mathrm{Aut}(F_k)$. Recall that $TS \subseteq SM$. Proposition 8.1 and the definition of SM imply that α is a product $\alpha = \omega\tau$ where ω is inner and where τ is a relabeling automorphism. The definition of TS now implies that τ is trivial and hence α is inner, as required.

Parts (2) and (3) follow directly from (1) since the centralizer of a nontrivial element w that is not a proper power in F_k is just the cyclic group generated by w. □

We will show that the set TS is exponentially C-generic.

Lemma 8.3. *Let τ be a nontrivial relabeling automorphism of F_k. Let $B(\tau)$ be the set consisting of all cyclically reduced words w such that $\tau(w)$ is conjugate to w. Then $B(\tau)$ is exponentially negligible in C.*

Proof. We only sketch the argument of the proof, leaving the details to the reader.

Let $|w| = n > 0$ and suppose that $\tau(w)$ is conjugate to w, that is $\tau(w)$ is a cyclic permutation of w. Suppose first that w is obtained as nontrivial cyclic permutation μ of the word $\tau(w)$. Then w is uniquely determined by its initial segment of length $n/2+1$ and by μ. Note that there are at most n possibilities for μ. Thus the number of such w is bounded above by the number $n\gamma(n/2+1, F_k)$ which grows

approximately as $n(2k-1)^{n/2+1}$ and thus, after dividing by $(2k-1)^n$, tends to zero exponentially fast.

Suppose now that $w = \tau(w)$. Since τ is induced by a nontrivial permutation of Σ, this implies that w omits at least one letter of Σ. It is easy to see that for each $a \in \Sigma$ the set of all cyclically reduced words w with $w_a = 0$ is exponentially negligible in C. This yields the statement of Lemma 8.3. □

Proposition 8.4. *The set TS is exponentially generic in C.*

Proof. Arzhantseva and Ol′shanskii [1996] observed that the set of cyclically reduced words that are proper powers in F_k is exponentially C-negligible. It is easy to prove this directly by an argument similar to the one used in the proof of Lemma 8.3. Now Lemma 8.3 and the fact that SM is exponentially C-generic imply that $C - TS$ is contained in a finite union of exponentially negligible sets and hence is itself exponentially negligible. Therefore TS is exponentially C-generic. □

Proposition 6.2 implies that the set TS' of all freely reduced words, whose cyclically reduced form belongs to TS, is exponentially F_k-generic.

We summarize the good properties of TS in the following statement, which follows directly from Proposition 8.4 (compare Theorem B):

Theorem 8.5. *We have $TS = TS' \cap C$ and the following hold*:

(1) *The set TS is exponentially C-generic and the set TS' is exponentially F_k-generic.*

(2) *There is a linear-time algorithm which, given a freely reduced word w, decides if $w \in TS'$ or if $w \in TS$.*

(3) *For any nontrivial $w \in TS'$ the stabilizer $\mathrm{Aut}(F_k)_w$ of w in $\mathrm{Aut}(F_k)$ is the infinite cyclic group generated by $ad(w)$.*

(4) *For any nontrivial $w \in TS'$ the stabilizer $\mathrm{Out}(F_k)_w$ of the conjugacy class of w in $\mathrm{Out}(F_k)$ is trivial.*

For future use we also need to establish the genericity of the following set:

Definition 8.6. Let the set Z consist of all $w \in TS$ such that there is no relabeling automorphism τ such that $\tau(w)$ is a cyclic permutation of w^{-1}.

Proposition 8.7. *The following hold in F_k.*

(1) *If $w \in Z$ is a nontrivial word then for any $\alpha \in \mathrm{Aut}(F_k)$ we have $\alpha(w) \neq w^{-1}$.*

(2) *The set Z is exponentially C-generic.*

Proof. Note that by construction the sets TS and Z are closed under taking inverses. Let $w \in Z$ be a nontrivial element.

The definition of Z and Proposition 8.1 imply that if $\alpha(w) = w^{-1}$ for $\alpha \in \mathrm{Aut}(F_k)$ then α is a product of inner Whitehead automorphisms and hence is inner itself.

However in a free group a nontrivial element is not conjugate to its inverse. This proves (1).

For a fixed relabeling automorphism τ let $D(\tau)$ be the set of cyclically reduced words w such that w^{-1} is a cyclic permutation of $\tau(w)$.

Thus to see that (2) holds it suffices to show that for each nontrivial relabeling automorphism τ the set $D(\tau)$ is exponentially C-negligible. The proof is exactly the same as for Lemma 8.3. Namely, if $w \in C$, $|w| = n > 0$ and w^{-1} is obtained by a cyclic permutation μ of $\tau(w)$, then the word w is uniquely determined by μ and by the initial segment of w of length $n/2+1$. Since there are n choices for μ, the number of such w is bounded by $n\gamma(n/2+1, C)$, which is exponentially smaller than $(2k-1)^n$. □

9. Applications to generic one-relator groups

We recall a classical theorem of Magnus [1930]:

Proposition 9.1. *Let $G = \langle a_1, \dots, a_k | r = 1\rangle$ where r is a nontrivial cyclically reduced word in F_k. Let $\alpha \in \mathrm{Aut}(F_k)$. Then α factors through to an automorphism of G if and only if $\alpha(r)$ is conjugate to either r or r^{-1} in F_k.*

The following surprising result about "isomorphism rigidity" of generic one-relator groups was obtained by Kapovich and Schupp [2005a].

Proposition 9.2. *Let $k \geq 2$ and $F_k = F(a_1, \dots, a_k)$. There exists a exponentially C-generic set P_k of nontrivial cyclically reduced words with the following properties*:

(1) *There is an exponential time algorithm which, given a cyclically reduced word w, decides whether or not $w \in P_k$.*

(2) *Let $u \in P_k$. Then G_u is an one-ended torsion-free word-hyperbolic group and every automorphism of G_u is induced by an automorphism of F_k.*

(3) *Let $u \in P_k$ and let v be a nontrivial cyclically reduced word in F_k. Then the one-relator groups G_u and G_v are isomorphic if and only if there exists $\alpha \in \mathrm{Aut}(F_k)$ such that $\alpha(u) = v$ or $\alpha(u) = v^{-1}$ in F_k.*

We now prove Theorem C stated in Section 3.

Proof of Theorem C. Let $Q_k = P_k \cap Z$, where P_k is from Proposition 9.2. The set Z is exponentially C-generic by Proposition 8.7 and the set P_k is exponentially C-generic by Proposition 9.2. Hence Q_k is exponentially C-generic as the intersection of two exponentially C-generic sets and part (1) of Theorem C follows from part (1) of Proposition 9.2.

Suppose $u \in P_k$, as in part (2) of Theorem C. Let β be an automorphism of G_u. By Proposition 9.2 β is induced by an automorphism α of F_k. Proposition 9.1 implies that $\alpha(u)$ is conjugate to either u or u^{-1} in F_k. The latter is impossible by

Proposition 8.7 since $u \in Z$. Thus $\alpha(u)$ is conjugate to u. Since $u \in TS$, Lemma 8.2 implies that $\alpha \in \mathrm{Inn}(F_k)$ and hence $\beta \in \mathrm{Inn}(G)$. Thus $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ and $\mathrm{Out}(G) = 1$. Since G_u is nonelementary torsion-free and word-hyperbolic, the center of G_u is trivial and so G_u is complete.

Since G_u is torsion-free one-ended word-hyperbolic and $\mathrm{Out}(G_u)$ is finite, the results of Paulin [1991] show that G_u does not admit any essential cyclic splittings. By a theorem of Bowditch [1998], the boundary of G_u is therefore connected and has no local cut-points. Since G_u is a torsion-free one-relator group, G_u has cohomological dimension two. Thus G_u is one-ended torsion-free hyperbolic of cohomological dimension two and such that ∂G_u is connected and has no local cut-points. A theorem of Kapovich and Kleiner [2000] now implies that ∂G_u is homeomorphic to either the Menger curve or the Sierpiński carpet and, moreover, if the boundary is the Sierpiński carpet then G_u must have negative Euler characteristic.

If $k = 2$, the presentation complex of G_u is topologically aspherical [Chiswell et al. 1981] (since G_u is a torsion-free one-relator group) and can thus be used to compute the Euler characteristic of G_u. The complex has one 0-cell, two 1-cells and one 2-cell so that the Euler characteristic of G_u is $1 - 2 + 1 = 0$. This rules out the Sierpiński carpet and hence ∂G_u is homeomorphic to the Menger curve in this case. This completes the proof of parts (2) and (3) of Theorem C.

Since $Q_k \subseteq TS$, part (4) of Theorem C follows from Proposition 9.2 and Proposition 8.1.

By construction the set $Q_k \subseteq TS \subseteq SM$ and $Q_k \subseteq P_k$. Now part (5) of Theorem C follows from Proposition 9.2 and Theorem A. □

Acknowledgements

We are grateful to Richard Sowers and Ofer Zeitouni for very illuminating discussions regarding large deviation theory. We thank Jean-François Lafont for raising the question of counting the number of isomorphism types of one-relator groups. We are also grateful to the referee for a number of comments that improved the paper.

References

[Arzhantseva 1997] G. N. Arzhantseva, "Groups in which subgroups with a fixed number of generators are free", *Fundam. Prikl. Mat.* **3**:3 (1997), 675–683. In Russian. MR 1794135 Zbl 0929.20025

[Arzhantseva 1998] G. N. Arzhantseva, "Generic properties of finitely presented groups and Howson's theorem", *Comm. Algebra* **26**:11 (1998), 3783–3792. MR 99j:20036 Zbl 0911.20027

[Arzhantseva 2000] G. N. Arzhantseva, "A property of subgroups of infinite index in a free group", *Proc. Amer. Math. Soc.* **128**:11 (2000), 3205–3210. MR 2001b:20040 Zbl 0976.20014

[Arzhantseva and Ol′shanskiĭ 1996] G. N. Arzhantseva and A. Y. Ol′shanskiĭ, "The class of groups all of whose subgroups with lesser number of generators are free is generic", *Mat. Zametki* **59**:4 (1996), 489–496. In Russian; translated in *Math. Notes* **59**:4 (1996), 350–355. MR 98k:20040

[Bahls 2003] P. Bahls, "A new class of rigid Coxeter groups", *Internat. J. Algebra Comput.* **13**:1 (2003), 87–94. MR 2004a:20042 Zbl 02084170

[Birman et al. 1998] J. Birman, K. H. Ko, and S. J. Lee, "A new approach to the word and conjugacy problems in the braid groups", *Adv. Math.* **139**:2 (1998), 322–353. MR 99m:20082 Zbl 0937.20016

[Booth et al. 2004] R. F. Booth, D. Y. Bormotov, and A. V. Borovik, "Genetic algorithms and equations in free groups and semigroups", pp. 63–81 in *Computational and experimental group theory* (Baltimore, 2003), edited by A. V. Borovik and A. G. Myasnikov, Contemp. Math. **349**, Amer. Math. Soc., Providence, RI, 2004. MR 2005h:20050 Zbl 02144696

[Borovik, Myasnikov and Shpilrain 2002] A. V. Borovik, A. G. Myasnikov, and V. Shpilrain, "Measuring sets in infinite groups", pp. 21–42 in *Computational and statistical group theory* (Las Vegas and Hoboken, 2001), edited by R. Gilman et al., Contemp. Math. **298**, Amer. Math. Soc., Providence, RI, 2002. MR 2003m:20024 Zbl 1022.20010

[Bowditch 1998] B. H. Bowditch, "Cut points and canonical splittings of hyperbolic groups", *Acta Math.* **180**:2 (1998), 145–186. MR 99g:20069 Zbl 0911.57001

[Brady et al. 2002] N. Brady, J. P. McCammond, B. Mühlherr, and W. D. Neumann, "Rigidity of Coxeter groups and Artin groups", *Geom. Dedicata* **94** (2002), 91–109. MR 2004b:20052 Zbl 1031.20035

[Burillo and Ventura 2002] J. Burillo and E. Ventura, "Counting primitive elements in free groups", *Geom. Dedicata* **93** (2002), 143–162. MR 2003i:20066 Zbl 1038.20015

[Champetier 1994] C. Champetier, "Petite simplification dans les groupes hyperboliques", *Ann. Fac. Sci. Toulouse Math.* (6) **3**:2 (1994), 161–221. MR 95e:20050 Zbl 0803.53026

[Champetier 1995] C. Champetier, "Propriétés statistiques des groupes de présentation finie", *Adv. Math.* **116**:2 (1995), 197–262. MR 96m:20056 Zbl 0847.20030

[Champetier 2000] C. Champetier, "L'espace des groupes de type fini", *Topology* **39**:4 (2000), 657–680. MR 2001i:20084 Zbl 0959.20041

[Cherix and Schaeffer 1998] P.-A. Cherix and G. Schaeffer, "An asymptotic Freiheitssatz for finitely generated groups", *Enseign. Math.* (2) **44**:1-2 (1998), 9–22. MR 99m:20066 Zbl 0987.20012

[Cherix and Valette 1996] P.-A. Cherix and A. Valette, "On spectra of simple random walks on one-relator groups", *Pacific J. Math.* **175**:2 (1996), 417–438. MR 98b:43001 Zbl 0865.60059

[Chiswell et al. 1981] I. M. Chiswell, D. J. Collins, and J. Huebschmann, "Aspherical group presentations", *Math. Z.* **178**:1 (1981), 1–36. MR 83a:20046 Zbl 0443.20030

[Dembo and Zeitouni 1998] A. Dembo and O. Zeitouni, *Large deviations techniques and applications*, 2nd ed., Applications of Mathematics **38**, Springer, New York, 1998. MR 99d:60030 Zbl 0896.60013

[Franco and González-Meneses 2003] N. Franco and J. González-Meneses, "Conjugacy problem for braid groups and Garside groups", *J. Algebra* **266**:1 (2003), 112–132. MR 2004g:20050 Zbl 1043.20019

[Garside 1969] F. A. Garside, "The braid group and other groups", *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 235–254. MR 40 #2051 Zbl 0194.03303

[Ghys 2004] É. Ghys, "Groupes aléatoires (d'après Misha Gromov, ...)", pp. 173–204 in *Séminaire Bourbaki, 2002/2003*, Astérisque **294**, Soc. Math. de France, Paris, 2004. MR 2005j:20049 Zbl 02123627

[Gromov 1987] M. Gromov, "Hyperbolic groups", pp. 75–263 in *Essays in group theory*, edited by S. M. Gersten, Math. Sciences Research Inst. Publ. **8**, Springer, New York, 1987. MR 89e:20070 Zbl 0634.20015

[Gromov 1993] M. Gromov, "Asymptotic invariants of infinite groups", pp. 1–295 in *Geometric group theory* (Sussex, 1991), vol. 2, edited by G. A. Niblo and M. A. Roller, London Math. Soc. Lecture Note Ser. **182**, Cambridge Univ. Press, Cambridge, 1993. MR 95m:20041 Zbl 0841.20039

[Gromov 2003] M. Gromov, "Random walk in random groups", *Geom. Funct. Anal.* **13**:1 (2003), 73–146. MR 2004j:20088a Zbl 01971826

[Gusfield 1997] D. Gusfield, *Algorithms on strings, trees, and sequences*, Cambridge University Press, Cambridge, 1997. MR 99b:68095 Zbl 0934.68103

[Haralick et al. 2005] R. M. Haralick, A. D. Miasnikov, and A. G. Myasnikov, "Heuristics for the Whitehead minimization problem", *Experiment. Math.* **14**:1 (2005), 7–14. MR 2146515

[Kapovich and Kleiner 2000] M. Kapovich and B. Kleiner, "Hyperbolic groups with low-dimensional boundary", *Ann. Sci. École Normale Sup.* (4) **33**:5 (2000), 647–669. MR 2002j:20077 Zbl 0989.20031

[Kapovich and Schupp 2005a] I. Kapovich and P. Schupp, "Genericity, the Arzhantseva–Ol′shanskii method and the isomorphism problem for one-relator groups", *Math. Ann.* **331**:1 (2005), 1–19. MR 2005h:20079 Zbl 02132961

[Kapovich and Schupp 2005b] I. Kapovich and P. Schupp, "Delzant's T-invariant, Kolmogorov complexity and one-relator groups", *Commentari Math. Helv.* **80**:4 (2005), 911–933.

[Kapovich et al. 2003] 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. MR 1981427 Zbl 1041.20021

[Kapovich et al. 2005] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, "Average-case complexity and decision problems in group theory", *Adv. Math.* **190** (2005), 343–359. MR 2005i:20053 Zbl 1065.20044

[Khan 2004] B. Khan, "The structure of automorphic conjugacy in the free group of rank two", pp. 115–196 in *Computational and experimental group theory* (Baltimore, 2003), edited by A. V. Borovik and A. G. Myasnikov, Contemp. Math. **349**, Amer. Math. Soc., Providence, RI, 2004. MR 2005f:20066 Zbl 02144699

[Lee 2003] D. Lee, "Counting words of minimum length in an automorphic orbit", preprint, Tulane University, 2003. math.GR/0311410

[Lyndon and Schupp 1977] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer, Berlin, 1977. MR 58 #28182 Zbl 0368.20023

[Magnus 1930] W. Magnus, "Über diskontinuierliche Gruppen mit einer definierenden Relation (der Freiheitssatz)", *J. rein. angew. Math.* **163** (1930), 141–165. JFM 56.0134.03

[McCool 1975] J. McCool, "Some finitely presented subgroups of the automorphism group of a free group", *J. Algebra* **35** (1975), 205–213. MR 53 #624 Zbl 0325.20025

[Miasnikov and Myasnikov 2004] A. D. Miasnikov and A. G. Myasnikov, "Whitehead method and genetic algorithms", pp. 89–114 in *Computational and experimental group theory* (Baltimore, 2003), edited by A. V. Borovik and A. G. Myasnikov, Contemp. Math. **349**, Amer. Math. Soc., Providence, RI, 2004. MR 2005g:20055 Zbl 02144698

[Mostow 1973] G. D. Mostow, *Strong rigidity of locally symmetric spaces*, Annals of Mathematics Studies **78**, Princeton University Press, Princeton, NJ, 1973. MR 52 #5874 Zbl 0265.53039

[Mühlherr and Weidmann 2002] B. Mühlherr and R. Weidmann, "Rigidity of skew-angled Coxeter groups", *Adv. Geom.* **2**:4 (2002), 391–415. MR 2003h:20073 Zbl 1015.20029

[Myasnikov and Shpilrain 2003] A. G. Myasnikov and V. Shpilrain, "Automorphic orbits in free groups", *J. Algebra* **269**:1 (2003), 18–27. MR 2004j:20051 Zbl 1035.20019

[Ollivier 2003] Y. Ollivier, "Critical densities for random quotients of hyperbolic groups", *C. R. Math. Acad. Sci. Paris* **336**:5 (2003), 391–394. MR 2004b:20106 Zbl 1050.20048

[Ol′shanskiĭ 1992] A. Y. Ol′shanskiĭ, "Almost every group is hyperbolic", *Internat. J. Algebra Comput.* **2**:1 (1992), 1–17. MR 93j:20068 Zbl 0779.20016

[Paulin 1991] F. Paulin, "Outer automorphisms of hyperbolic groups and small actions on **R**-trees", pp. 331–343 in *Arboreal group theory* (Berkeley, 1988), edited by R. C. Alperin, Math. Sci. Res. Inst. Publ. **19**, Springer, New York, 1991. MR 92g:57003 Zbl 0804.57002

[Prassidis and Spieler 2000] S. Prassidis and B. Spieler, "Rigidity of Coxeter groups", *Trans. Amer. Math. Soc.* **352**:6 (2000), 2619–2642. MR 2000j:57077 Zbl 0972.57022

[Rosas 1988] E. Rosas, "Rigidity theorems for right angled reflection groups", *Trans. Amer. Math. Soc.* **308**:2 (1988), 837–848. MR 89k:57081 Zbl 0658.57022

[Whitehead 1936] J. H. C. Whitehead, "On equivalent sets of elements in a free group", *Ann. of Math.* (2) **37**:4 (1936), 782–800. MR 1503309 Zbl 0015.24804

[Żuk 2002] A. Żuk, "On property (T) for discrete groups", pp. 473–482 in *Rigidity in dynamics and geometry* (Cambridge, 2000), edited by M. Burger and A. Iozzi, Springer, Berlin, 2002. MR 2003g:22025 Zbl 1007.22011

Received April 24, 2004. Revised August 11, 2004.

ILYA KAPOVICH
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS AT URBANA–CHAMPAIGN
1409 WEST GREEN STREET
URBANA, IL 61801

kapovich@math.uiuc.edu
http://www.math.uiuc.edu/~kapovich/

PAUL SCHUPP
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS AT URBANA–CHAMPAIGN
1409 WEST GREEN STREET
URBANA, IL 61801

schupp@math.uiuc.edu
http://www.math.uiuc.edu/People/schupp.html

VLADIMIR SHPILRAIN
DEPARTMENT OF MATHEMATICS
THE CITY COLLEGE OF NEW YORK
NEW YORK, NY 10031

shpil@groups.sci.ccny.cuny.edu
http://www.sci.ccny.cuny.edu/~shpil