Illinois Journal of Mathematics
Volume 54, Number 1, Spring 2010, Pages 371–388
S 0019-2082

EXPONENTIALLY GENERIC SUBSETS OF GROUPS

ROBERT GILMAN, ALEXEI MIASNIKOV AND DENIS OSIN

To Paul Schupp as a token of our friendship

Abstract. In this paper, we study the generic, i.e., typical, behavior of finitely generated subgroups of hyperbolic groups and also the generic behavior of the word problem for amenable groups. We show that a random set of elements of a nonelementary word hyperbolic group is very likely to be a set of free generators for a nicely embedded free subgroup. We also exhibit some finitely presented amenable groups for which the restriction of the word problem is unsolvable on every sufficiently large subset of words.

1. Introduction

Natural sets of algebraic objects are often unions of two unequal parts, the larger part consisting of generic objects whose structure is uniform and relatively simple, and the smaller including exceptional cases which have much higher complexity and provide most of resistance to classification. The essence of this idea first appeared in the form of zero–one laws in probability, number theory, and combinatorics. In finite group theory the idea of genericity can be traced to a series of papers by Erdős and Turan in 1960–1970s (for recent results see [Sha]), while in combinatorial group theory the concept of generic behavior is due to Gromov. His inspirational works [Gro, Gro2, Gro3] turned the subject into an area of very active research, see, for example, [AO, Arz1, Arz2, BMR1, BMR2, BMR3, BV1, BV2, BMS, CERT, CS, BM, BV2, Cha1, Cha2, Jit, KMSS1, KMSS2, KSS, KRSS, KR, Oll, Olsh, Rom, MTV, Woe, Zuk].

Received May 7, 2010; received in final form November 16, 2010.
2000 *Mathematics Subject Classification.* Primary 20F10. Secondary 20F67, 43A07.

We mention in particular the remarkable results due to Kapovich and Schupp on generic properties of one-relator groups [KS1, KS2] and by Maher [Mah] and Rivin [Riv] on generic properties of random elements of mapping class groups and automorphisms of free groups, as well as the theorem by Kapovich, Rivin, Schupp and Shpilrain that generic cyclically reduced elements in free groups are of minimal length in their automorphic orbits [KRSS]. An earlier series of papers [Olsh, AO, Arz1, Arz2] by Arjantseva and Olshanskii established the theory of subgroups of random groups and related questions.

Knowledge of generic properties of objects can be used in design of simple practical algorithms that work very fast on most inputs. In cryptography, several successful attacks have exploited generic properties of randomly chosen objects to break cryptosystems [MU, MSU1, MSU2, RST]. Explicit generic case analysis of algorithmic problems first appeared in the papers [KMSS1, KMSS2, BMR1].

In the first part of this paper, we show that with high probability a random subgroup of a nonelementary hyperbolic group has a simple structure and is embedded without much distortion of its intrinsic metric. Arbitrary subgroups on the other hand, can be very complicated. A remarkable construction introduced by Rips [Rips] shows that every finitely presented group G is a quotient of a hyperbolic (in fact, small cancellation) group H by a finitely generated normal subgroup N. The Dehn function of G is intimately related to the metric distorsion of the subgroup N in H. In particular, as Rips noticed, the membership problem for N in H is undecidable provided the word problem in G is undecidable. A host of undecidability results for subgroups of hyperbolic groups has been proven by combining the Rips technique with known unsolvability results for finitely presented groups ([BauMS], [BW]). These results show that hyperbolic groups contain finitely generated subgroups with as much distortion as one pleases. However, it is widely believed that such subgroups are rare, and that most finitely generated subgroups of hyperbolic groups have an uncomplicated structure and not much distortion.

We prove here that for each $k \geq 1$, with overwhelming probability (relative to a natural distribution) k-tuples of words in a given finite set of generators of a nonelementary hyperbolic group freely generate a free subgroup which is quasi-isometrically embedded into the ambient group. The property that a random k-tuple of words is, with overwhelming probability, a set of free generators is sometimes referred to as the generic Nielsen property. In [MU], Myasnikov and Ushakov proved that similar results hold in pure braid groups, as well as right angled Artin groups. This result has been applied to a rigorous mathematical cryptanalysis of the Anshel–Anshel–Goldfeld public key exchange scheme [AAG], including an analysis of various length-based attacks ([HT], [GKTTV], [RST]). For free non-Abelian groups, the generic Nielsen property was shown earlier in [Jit] and [MTV]. Notice, that in the case of

free groups, all finitely generated subgroups are free and embedded quasi-isometrically.

For related results on free products with amalgamation and HNN extensions, we refer to [FMR]. Beyond cryptographic applications, our results on generic subgroups in hyperbolic groups provide a cubic time deterministic partial algorithm $\mathcal{A}$, which never lies and solves the membership problem for almost all (more precisely, for a certain exponentially generic subset $\mathcal{D}$) of finitely generated subgroups in a given nonelementary hyperbolic group. Furthermore, if a given subgroup is not in the set $\mathcal{D}$ the algorithm quickly recognizes this (in quadratic time) and halts with a failure message.

Another result we would like to mention here concerns with the complexity of the word problem in finitely presented groups. It turns out that many famous undecidable problems are, in fact, very easy on generic set of inputs. This is precisely the case for the halting problem of Turing machines with one-ended infinite tape [HM], and for the classical examples of finitely presented groups or semigroups with undecidable word problem [MUW]. The first examples of finitely presented semigroups where the word problem is undecidable on any generic set of inputs (words in the given set of generators) are constructed in [MR]. Whether there exist such examples in finitely presented groups is still an open problem. In this paper, we describe some finitely presented groups for which the word problem is undecidable on any exponentially generic set of words in given generators. The famous construction [Kh], due to Kharlampovich, of finitely presented solvable groups with undecidable word problem provide a host of examples of such groups.

In the next section, we describe our main results in detail, and prove them in the following sections. The last section contains several open problems in this area.

The authors are grateful to Pascal Weil, whose careful reading of the manuscript led to several corrections and improvements.

2. Statement of results

Fix a finite alphabet with formal inverses, $A = \{a_1, \dots, a_m, a_1^{-1}, \dots, a_m^{-1}\}$ for some $m \geq 2$. Use $|w|$ to denote the length of a word w over A and $|S|$ for the cardinality of a set S. Formal inverses, w^{-1}, are defined in the obvious way.

By W, we denote the free monoid with basis A, that is, the set of all words over the alphabet W with the binary operation of concatenation. The subset $W_n = \{w \in W \mid |w| \leq n\}$ is the disk of radius n in W, and $W = \bigcup_{n=1}^{\infty} W_n$ is the stratification of W by disks. Since every disk is finite, one may define the standard uniform distribution μ_n on W_n. The ensemble of distributions $\{\mu_n\}$, after a proper normalization, induces the standard "uniform distribution" μ on W relative to the stratification by disks.

The exponential asymptotic density of $X \subset W$ is defined as

$$\rho_e(X) = \lim_{n\to\infty} \frac{|X \cap W_n|}{|W_n|}$$

if the limit converges exponentially fast. In other words,

$$\rho_e(X) = \lambda \quad \Longleftrightarrow \quad \left|\lambda - \frac{|X \cap W_n|}{|W_n|}\right| \leq \alpha^n$$

for some constant $\alpha \in (0,1)$ and all sufficiently large n, or equivalently if

$$\left|\lambda - \frac{|X \cap W_n|}{|W_n|}\right| \leq M\beta^n$$

for some $\beta \in (0,1)$, positive constant M and all n.

$X \subset W$ is *exponentially generic* if $\rho_e(X) = 1$ and *exponentially negligible* if its complement is exponentially generic, that is, if $\rho_e(X) = 0$. It is clear that finite intersections of exponentially generic sets are exponentially generic and finite unions of exponentially negligible sets are exponentially negligible. See [BMS, BMR1] for more information on asymptotic density.

To study asymptotic properties of k-generated subgroups of groups generated by A, we need to extend the notions introduced above to subsets of k-tuples of words from W. For $k \geq 1$, put

$$W^{(k)} = \{(w_1, \ldots, w_k) \mid w_i \in W\}. \tag{2.1}$$

The disk of radius n in $W^{(k)}$ is defined to be

$$W_n^{(k)} = \overbrace{W_n \times \cdots \times W_n}^{k} = \big\{(w_1, \ldots, w_k) \in W^{(k)} \mid |w_i| \leq n\big\}. \tag{2.2}$$

Exponential asypmtotic density of subsets of $W^{(k)}$ is defined as above but with $W_n^{(k)}$ in place of W_n. When k is fixed or irrelevant, we write

$$\vec{w} \text{ for } (w_1, \ldots, w_k), \text{ and } |\vec{w}| \text{ for } \max\{|w_i| \mid i = 1, \ldots, k\}.$$

For any group G a monoid epimorphism $W \to G$ which respects inverses is called a choice of generators for G, and the image in G of $w \in W$ is denoted $\overline{w}$. Each choice of generators determines a word metric with distance $|g-h|$ equal to the length of the shortest word in W representing $g^{-1}h$. We abbreviate $|g-1|$ as $|g|$ or $|g|_G$ if the ambient group is not clear. Note that for $w \in W$, $|w|$ is the length of w while $|\overline{w}|$ is the length of the shortest word in W mapping to $\overline{w}$.

Let H be a finitely generated subgroup of G with a choice of generators $W' \to H$ where W' is the free monoid over a finite set of generators B with formal inverses. H is *undistorted* in G (with respect to the choices of generators for G and H) if it is *quasi-isometrically* embedded in G, that is, there is a

constant $\lambda > 1$ such that for every elements $f, h \in H$ the following inequality holds

$$\frac{1}{\lambda}|f-h|_H \le |f-h|_G.$$

A nontrivial subgroup H is undistorted if and only if the compression factor of H in G is positive. The compression factor of H in G (with respect to choices of generators $A \to G$ and $B \to H$) is defined as

$$\mathrm{Comp}(G, A; H, B) = \inf_{h \in H \setminus \{1\}} \frac{|h|_G}{|h|_{G,H}}, \tag{2.3}$$

where

$$|h|_{G,H} = \min_{h = b_{i_1} \cdots b_{i_s}} (|b_{i_1}|_G + \cdots + |b_{i_s}|_G),$$

and the minimum is taken over all representations of h in the form $b_{i_1} \cdots b_{i_s}$ with $b_{i_j} \in B$, $1 \le j \le s$.

Recall that the *gross cogrowth* θ of G with respect to a choice of generators $W \to G$ is defined by

$$\theta = \lim_{n \to \infty} \frac{1}{2n} \log_{2m} |V_{2n}|, \tag{2.4}$$

where for any r, V_r is the subset of all words of length r in W which represent the identity in G. It is known (see Section 3.2 for details and references) that G is amenable if and only if $\theta = 1$.

The main technical result of the paper is Lemma 4.3, which says that a certain set $\mathcal{C} \subset W^{(k)}$ which is defined in terms of a parameter $\varepsilon > 0$ is exponentially generic. The exponentially generic sets mentioned in the next two theorems all contain $\mathcal{C}$. Recall that a group is called *elementary* if it contains a cyclic subgroup of finite index.

THEOREM 2.1. *Let G be a nonelementary hyperbolic group. Then for any choice of generators $W \to G$ the following sets are exponentially generic*:

(1) *The set of all $(w_1, \dots, w_k) \in W^{(k)}$ for which $\overline{w}_1, \dots, \overline{w}_k$ generate a free subgroup of rank k in G.*
(2) *The set of all $(w_1, \dots, w_k) \in W^{(k)}$ for which $\overline{w}_1, \dots, \overline{w}_k$ generate a subgroup with compression factor at least $\frac{1-\theta}{\theta} - \varepsilon$, where θ is the gross cogrowth of G with respect to the given choice of generators and ε is any positive constant.*

It is easy to see that the first statement of Theorem 2.1 holds for any group G which has a surjective homomorphism onto a nonelementary hyperbolic group. Examples of such groups include many relatively hyperbolic groups, for example, nonelementary groups hyperbolic relative to proper residually finite subgroups [Osi]. The later class includes fundamental groups of complete finite volume manifolds of pinched negative curvature, $CAT(0)$ groups with isolated flats, groups acting freely on $\mathbb{R}^n$-trees, and many other examples.

THEOREM 2.2. *Let G be a nonelementary hyperbolic group. Then for any choice of generators $W \to G$ and $k \geq 1$ there exists a partial algorithm $\mathcal{A}$ which for each $\vec{w} = (w_1, \dots, w_k)$ in an exponentially generic subset $\mathcal{D} \subset W^{(k)}$ and an arbitrary $z \in W$ decides if $\overline{z}$ is in the subgroup $H = \langle \overline{w}_1, \dots, \overline{w}_k \rangle \subset G$. When the answer is yes, $\mathcal{A}$ decomposes $\overline{z}$ as a word in the generators $\overline{w}_1, \dots, \overline{w}_k$ and their inverses. On all inputs $\mathcal{A}$ runs in time $O((k|\vec{w}| + |z|)^3)$.*

By partial algorithm, we mean one which never gives a wrong answer but may say "Don't know" or "Fail."

THEOREM 2.3. *Let G be a finitely presented amenable group with unsolvable word problem. Then for any choice of generators $W \to G$ the word problem in G is not solvable on any exponentially generic subset of W.*

As we noted above, Kharlampovich [Kh] provides many groups to which Theorem 2.3 applies.

3. Preliminaries

In this section, we recall for convenience various known results and draw some elementary consequences. Recall the definitions of $W, W_n, W^{(k)}$ and $W_n^{(k)}$ from the preceding section.

3.1. Asymptotic density.

LEMMA 3.1. *Define $I_n = \{w \in W \mid |w| = n\}$ (the sphere of radius n). If $\lim_{n\to\infty} \frac{|X \cap I_n|}{|I_n|} < \alpha^n$ for some $\alpha \in (0,1)$, and all sufficiently large n, then X is exponentially negligible.*

Proof. Let r be the greatest integer less than $n/2$.

$$\begin{aligned}
\frac{|X \cap W_n|}{|W_n|} &\leq \frac{|W_r|}{|W_n|} + \frac{|X \cap I_{r+1}| + \cdots + |X \cap I_n|}{|W_n|} \\
&\leq (2m)^{-n/2} + \frac{|X \cap I_{r+1}|}{|I_{r+1}|} + \cdots + \frac{|X \cap I_n|}{|I_n|} \\
&\leq (2m)^{-n/2} + \alpha^{r+1} + \cdots + \alpha^n \text{ for } n \text{ sufficiently large} \\
&\leq (2m)^{-n/2} + \frac{\alpha^{n/2}}{1-\alpha}.
\end{aligned}$$

□

Concatenation of all entries of $\vec{w} = (w_1, \dots, w_k) \in W^{(k)}$ defines a map $\pi : W^{(k)} \to W$. It is easy to see that that $\pi(W_n^{(k)}) = W_{nk}$ whence $|W_n^{(k)}| \geq |W_{nk}|$. The k-tuples in $\pi^{-1}(w)$ correspond to ordered partitions $\ell_1 + \cdots + \ell_k = |w|$ with $0 \leq \ell_i \leq |w|$. There are at most $(|w|+1)^k$ such partitions, and it follows that the restriction of π to $W_n^{(k)}$ is at most $(nk+1)^k$ to 1. These conclusions still apply if we pick a fixed sequence of exponents $e_1, \dots, e_k$ with $e_i = \pm 1$ and define $\pi(\vec{w}) = w_1^{e_1} \cdots w_k^{e_k}$.

LEMMA 3.2. *Define* $\pi : W^{(k)} \to W$ *by* $\pi(\vec{w}) = w_1^{e_1} \cdots w_k^{e_k}$ *as above. If* $\pi(X)$ *is exponentially negligible, then so is* X.

Proof. If $\pi(X)$ is exponentially negligible, then $\frac{|\pi(X) \cap W_{kn}|}{|W_{kn}|} \leq \alpha^n$ for some $\alpha \in (0,1)$ and all sufficiently large n. Thus,

$$\frac{|X \cap W_n^{(k)}|}{|W_n^{(k)}|} \leq \frac{(nk+1)^k |\pi(X) \cap W_{kn}|}{|W_{kn}|} \leq (nk+1)^k \alpha^n$$

and a straightforward argument shows that X is exponentially negligible. □

3.2. Amenable groups. Let $W \to G$ be a choice of generators for a group G. Define V to be the subset of all words in W which map to 1 in G. $V_n = V \cap I_n$ is the set of all words of length n in V.

By [Gri1, Gri2] (see also [Coh] and [Kes2]) G is *amenable* if and only if

$$\limsup_{n\to\infty} (|V_n|/|I_n|)^{1/n} = 1.$$

Clearly, $|V_{n+p}| \geq |V_n||V_p|$, and V_{2n} includes all concatentations of n terms of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$. It follows that $|V_{2n}| \geq (2m)^n$; and if $|V_n| = 0$, then $|V_{n-2}| = 0$. Thus, $|V_n|$ is positive for all even n and either positive for all odd n greater than than some bound M or 0 for all odd n.

In first case, let $t = ks + r$ with $s > M$ and $M < r \leq M + s$. Then $|V_t| \geq |V_s|^k |V_r|$ implies $|V_t|^{1/t} \geq |V_s|^{1/s} (|V_s|^{-r} |V_r|)^{1/t}$ whence $\liminf_{t\to\infty} |V_t|^{1/t} \geq |V_s|^{1/s}$. It follows that $\liminf_{t\to\infty} |V_t|^{1/t} \geq \limsup_{s\to\infty} |V_s|^{1/s}$, which in turn implies that $\lim_{n\to\infty} |V_n|^{1/n}$ exists. In the second case, a similar argument show that $\lim_{n\to\infty} |V_{2n}|^{1/(2n)}$ exists. Thus, we may define

$$\lambda = \lim_{n\to\infty} (|V_{2n}|/|I_{2n}|)^{\frac{1}{2n}} = \frac{1}{2m} \lim_{n\to\infty} |V_{2n}|^{\frac{1}{2n}} = \frac{1}{2m} \limsup_{n\to\infty} |V_n|^{1/n}. \tag{3.1}$$

$|V_{2n}| \geq (2m)^n$ implies $1 \geq \lambda \geq 1/\sqrt{2m}$. Comparison of (3.1) with (2.4) yields

$$\theta = 1 + \log_{2m} \lambda = \limsup_{n\to\infty} \frac{1}{n} \log_{2m} |V_n| \tag{3.2}$$

whence

$$1/2 \leq \theta \leq 1. \tag{3.3}$$

Thus, amenability is equivalent to both $\lambda = 1$ and $\theta = 1$.

Also it follows from [Kes1, Corollary 1, p. 343] that every subgroup of an amenable group is amenable. Conversely, a group which contains a nonamenable subgroup is itself nonamenable.

LEMMA 3.3. *If* G *is nonamenable, then for any* $\epsilon > 0$ *and constant* K, $U = \{w \in W \mid |\overline{w}| > (\frac{1-\theta}{\theta} - \epsilon)|w| + K\}$ *is exponentially generic.*

Proof. First, suppose $K = 0$. Choose $\varepsilon > 0$ and let $\rho = (2m)^{\theta+\varepsilon}$. As $m \geq 2$, (3.3) implies $\rho \geq 2$. If $w \in I_{n,r} = \{w \in I_n \mid |\overline{w}| \leq r\}$, then $ww' \in V_{n+s}$ for some w' of length $s \leq r$. Thus, $I_{n,r} \subset V_n \cup \cdots \cup V_{n+r}$. For n sufficiently large, (3.2) yields

$$|I_{n,r}| \leq \rho^n + \cdots + \rho^{n+r} = \rho^n \frac{\rho^{r+1} - 1}{\rho - 1} \leq \rho^{n+r} \frac{\rho}{\rho - 1} \leq 2\rho^{n+r}.$$

Consequently, $\frac{|I_{n,r}|}{|I_n|} \leq 2(2m)^{(\theta+\varepsilon)(r+n)-n}$. If $r \leq (\frac{1-\theta}{\theta} - \varepsilon)n$, then $(\theta + \varepsilon) \times ((\frac{1-\theta}{\theta} - \varepsilon) + 1) - 1 = -\varepsilon^2$ implies $\frac{|I_{n,r}|}{|I_n|} \leq 2(2m)^{-\varepsilon^2}$ whence the complement of U is exponentially negligible by Lemma 3.1.

Now suppose $K > 0$. For any $\varepsilon > 0$, $U' = \{w \in W \mid |\overline{w}| \geq (\frac{1-\theta}{\theta} - \epsilon/2)|w|\}$ is exponentially generic. But $w \in U'$ implies

$$|\overline{w}| \geq \left(\frac{1-\theta}{\theta} - \epsilon/2\right)|w| \geq \left(\frac{1-\theta}{\theta} - \epsilon\right)|w| + \varepsilon/2|w| \geq \left(\frac{1-\theta}{\theta} - \epsilon\right)|w| + K$$

for $|w|$ sufficiently large. Thus, U contains a co-finite subset of U'. □

LEMMA 3.4. *If G is nonamenable, then for any $\varepsilon > 0$:*

(1) *The set of words w with $|\overline{v}| \geq (\frac{1-\theta}{\theta} - \varepsilon)|v|$ for all subwords v of w with $|v| \geq \varepsilon|w|$ is exponentially generic;*
(2) *The set of words w with $|\overline{v}| \geq (\frac{1-\theta}{\theta} - \varepsilon)|v|$ for all subwords v of ww with $|w| \geq |v| \geq \varepsilon|w|$ is exponentially generic.*

Proof. Let $\rho = \frac{1-\theta}{\theta} - \varepsilon$. The words in I_n are obtained by filling a sequence of n locations $\ell_1, \ldots, \ell_n$ with letters from A in all possible ways. Fix i and j with $j - i + 1 \geq \varepsilon n$. It follows from the proof of Lemma 3.3 that for some $\alpha \in (0, 1)$ and n sufficiently large, the fraction of ways of filling the subsequence $\ell_i, \ldots, \ell_j$ with a word v such that $|\overline{v}| < \rho|v| = \rho(j - i + 1)$ is less than $\alpha^{|v|}$. Since each v extends to $w \in I_n$ in $(2m)^{n-|v|}$ ways, $\alpha^{|v|}$ also bounds the fraction of extensions which fail the condition at the subword v. There are n^2 choices of i, j, so we conclude that the fraction of words $w \in I_n$ which fail is at most $n^2\alpha^{\varepsilon n}$. Thus, the first assertion holds by Lemma 3.1. The second is proved similarly by counting the number of extensions of v to ww. The condition $|w| \geq |v|$ insures that v extends to a word of the form ww in $(2m)^{(n-|v|)}$ ways. □

3.3. Hyperbolic metric spaces. Recall that a metric space M is *geodesic* if distances between points are realized by geodesics, and a geodesic metric space is *δ-hyperbolic* for some $\delta \geq 0$ (or simply *hyperbolic*) if any geodesic triangle T in M is *δ-thin*. That is, each side of T belongs to the union of the closed δ-neighborhoods of the other two sides [Gro].

We denote a geodesic path in M from p to q by $[p, q]$ and its length by $|p - q|$. The next lemma is well known (see, e.g., [GdH]).

LEMMA 3.5.

(1) *For any geodesic quadrilateral with vertices* p, q, r, s,

$$|p-s| + |q-r| \leq 2\delta + \max\{|p-q| + |r-s|, |p-r| + |q-s|\}.$$

(2) *Let* T *be a geodesic triangle with vertices* p, q, r. *There are points* t_p, t_q, t_r *on the sides opposite* p, q, r *respectively such that*:
   (a) t_p, t_q, t_r *are a distance at most* 2δ *from each other*;
   (b) $|p - t_q| = |p - t_r|$, *and likewise for the other vertices*;
   (c) *points lying an equal distance from* p *along the segments of the sides of* T *from* p *to* t_q *and* p *to* t_r *are a distance at most* 2δ *from each other. Similar statements hold for the other vertices.*

The quantity $|p - t_q| = |p - t_r|$ is the *Gromov product* of q and r with respect to p, usually written $(q|r)_p$. It is not hard to show that

$$(q|r)_p = \frac{1}{2}(|p-q| + |p-r| - |q-r|). \tag{3.4}$$

Thus, $(q|r)_p$ is independent of the choice of geodesics forming the sides of a triangle with vertices p, q, r.

The following lemma improves [GdH, Theorem 16 in Chapter 5].

LEMMA 3.6. *If for some* $\kappa > 0$ *and* $n \geq 2$, *the points* $p_0, \ldots, p_n$ *satisfy*

$$|p_i - p_{i+2}| \geq \kappa + 2\delta + \max\{|p_i - p_{i+1}|, |p_{i+i} - p_{i+2}|\} \tag{3.5}$$

then

$$|p_0 - p_n| \geq |p_0 - p_{n-1}| + \kappa \geq |p_0 - p_1| + (n-1)\kappa \geq \kappa n.$$

Proof. The first inequality implies the second by induction, and the second implies the third as $|p_0 - p_1| \geq \kappa$ lest the hypothesis fail for $i = 0$. Thus, it suffices to prove

$$|p_0 - p_n| \geq |p_0 - p_{n-1}| + \kappa. \tag{3.6}$$

Clearly, (3.6) holds when $n = 2$; assume $n \geq 3$. By the first part of Lemma 3.5, either

$$|p_0 - p_{n-1}| + |p_{n-2} - p_n| \leq 2\delta + |p_0 - p_{n-2}| + |p_{n-1} - p_n| \tag{3.7}$$

or

$$|p_0 - p_{n-1}| + |p_{n-2} - p_n| \leq 2\delta + |p_{n-2} - p_{n-1}| + |p_0 - p_n|. \tag{3.8}$$

By induction and (3.5), the left-hand side of (3.7) is greater than or equal to $|p_0 - p_{n-2}| + 2\kappa + 2\delta + |p_{n-1} - p_n|$, which contradicts (3.7), as $\kappa > 0$. Consequently (3.8) holds. Applying (3.5) to the left-hand side of (3.8) yields $|p_0 - p_{n-1}| + \kappa + 2\delta \leq 2\delta + |p_0 - p_n|$ as desired. □

The following lemma is [BH, Proposition 1.6, Chapter III.H] and [CDP, Lemma 1.5, Chapter 3].

LEMMA 3.7. *Let γ be a path of length ℓ from p to q in a δ-hyperbolic space, and $[p,q]$ a geodesic from p to q. Any point on $[p,q]$ is a distance at most $1+2\delta\log_2\ell$ from some point on γ.*

4. Subgroups of hyperbolic groups

A group G with choice of generators $W \to G$ is *δ-hyperbolic* for some $\delta > 0$ (or simply *hyperbolic*) if its Cayley graph Γ (with edges isometric to the unit interval) is a δ-hyperbolic metric space. The word metric on G extends to a metric on Γ.

A hyperbolic group is called *elementary* if it contains a cyclic subgroup of finite index. Throughout this section, G denotes a nonelementary δ-hyperbolic group. As nonelementary hyperbolic groups contain non-Abelian free subgroups [Del], G is nonamenable.

For each word $w \in W$ and vertex x in Γ, there is a unique path in Γ with initial point x and label w. Thus, we will speak of the path w starting at x; w^{-1} is the same path traversed in the opposite direction starting at the endpoint of w.

LEMMA 4.1. *For any $\varepsilon > 0$, the set of $\vec{w} = (u,v) \in W^{(2)}$ with $(\overline{u}^{\pm1}|\overline{v}^{\pm1})_1 < \varepsilon\min\{|u|,|v|\}$ is exponentially generic.*

Proof. Without loss of generality, assume $\varepsilon < 1/2$. A straightforward counting argument shows that the fraction of $(u,v) \in W_n^{(2)}$ with $|u| < n/2$ or $|v| < n/2$ is less than $2(2m)^{-n/2}$. It follows that $\{\vec{w} \in W^{(2)} \mid \min\{|u|,|v|\} < |\vec{w}|/2\}$ is exponentially negligible.

To complete the proof, it suffices to show that for each $e = \pm1$ and $f = \pm1$

$$X = \left\{\vec{w} \in W^{(2)} \mid (\overline{u}^e|\overline{v}^f)_1 \geq \varepsilon|\vec{w}|/2 \text{ and } \min\{|u|,|v|\} \geq |\vec{w}|/2\right\}$$

is exponentially negligible. Consider $e = -1, f = 1$; the other cases are similar.

For any $\vec{w} \in X$ let T be a geodesic triangle in the Cayley diagram Γ with vertices 1, $\overline{u}^{-1}$ and $\overline{v}$ as in Figure 1. Pick points p and q a distance $\varepsilon|\vec{w}|/2$ from 1 along the geodesics $[1,\overline{u}^{-1}]$ and $[1,\overline{v}]$ respectively. By Lemma 3.5, $|p-q| \leq 2\delta$. As every point of Γ is a distance at most $1/2$ from a vertex, Lemma 3.7 yields $|p-r| \leq 3/2 + 2\delta\log_2|\vec{w}|$ for some vertex r on the path from $\overline{u}^{-1}$ to 1 with label u. Likewise, $|q-s| \leq 3/2 + 2\delta\log_2|\vec{w}|$ for some vertex s on the path from 1 to $\overline{v}$ with label v.

Let z be the subword of uv which labels the subpath from r to s. By construction

$$\begin{aligned} |\overline{z}| &= |r-s| \leq 3 + 2\delta + 4\delta\log_2|\vec{w}|, \\ |z| &\geq (|p| - |p-r|) + (|q| - |q-s|) \\ &\geq \varepsilon|\vec{w}| - (3 + 4\delta\log_2|\vec{w}|). \end{aligned}$$

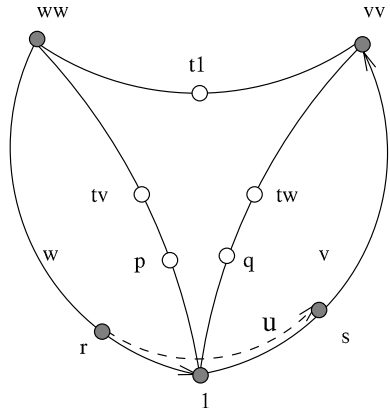

FIGURE 1. The triangle T from the proof of Lemma 4.1. Shaded dots are vertices of the Cayley diagram of G.

As $|\vec{w}| \le |uv| \le 2|\vec{w}|$, we have

$$|\overline{z}| \le \left(\frac{1-\theta}{\theta} - \frac{\varepsilon}{4}\right)|\vec{w}| \le \left(\frac{1-\theta}{\theta} - \frac{\varepsilon}{4}\right)|uv|,$$

$$|z| \ge \frac{\varepsilon|\vec{w}|}{2} \ge \frac{\varepsilon}{4}|uv|$$

for $|\vec{w}|$ large enough; that is, for all $\vec{w}$ in some co-finite subset X' of X. By Lemma 3.4(1), the image of X' under the map π of Lemma 3.2 is exponentially negligible. By Lemma 3.2, X' and hence X are exponentially negligible. □

LEMMA 4.2. *For any $\varepsilon > 0$, the set of $w \in W$ such that $(\overline{w}^{-1}|\overline{w})_1 < \varepsilon|w|$ is exponentially generic.*

Proof. The proof is similar to that of Lemma 4.1. Recall from Section 3.2 that $1/2 \le \theta \le 1$. As G is not amenable, $\theta < 1$; and it follows that $0 < \frac{\theta-1}{\theta} \le 1/2$. By Lemma 3.4(1) with $\varepsilon = \frac{\theta-1}{2\theta} \le 1/4$, the set

$$\left\{ w \;\middle|\; \text{for all subwords } v \text{ of } w, \text{ either } |v| < (1/4)|w| \text{ or } |\overline{v}| \ge \left(\frac{1-\theta}{2\theta}\right)|v| \right\}$$

is exponentially generic. Thus, it suffices to prove that for any $\varepsilon > 0$ the set X of all w with:

(1) $(\overline{w}^{-1}|\overline{w})_1 \ge \varepsilon|w|$ and
(2) for all subwords v or w, either $|v| < (1/4)|w|$ or $|\overline{v}| \ge (\frac{1-\theta}{2\theta})|v|$

is exponentially negligible. Without loss of generality, assume $\varepsilon \le \frac{1-\theta}{4\theta} \le 1/8$.

Consider $w \in X$. Form a geodesic triangle T with vertices 1, $\overline{w}^{-1}$, $\overline{w}$, and argue as in the proof of Lemma 4.1. The proof goes as before except that we must show the $|z| \le |w|$ in order to employ Lemma 3.4(2).

Let w_r and w_s be the subwords of w which label the paths from r to 1 and 1 to s. It suffices to show that for all $w \in X$ both these subwords have length at most $|w|/2$. We give the argument for w_r; the other case is similar.

Assume $|w_r| > |w|/4$. By definition of X and construction of w_r, we have

$$\begin{aligned}\frac{1-\theta}{2\theta}|w_r| &\le |\overline{w_r}| \le |r-p| + |p| \\ &\le 3/2 + 2\delta \log_2 |w| + \varepsilon|w|/2 \le 3/2 + 2\delta \log_2 |w| + \frac{1-\theta}{8\theta}|w|.\end{aligned}$$

Thus

$$|w_r| \le \frac{2\theta}{1-\theta}(3/2 + 2\delta \log_2 |w|) + |w|/4$$

from which it follows that $|w_r| \le |w|/2$ for $|w|$ large enough. □

LEMMA 4.3. *Fix $\varepsilon \in (0,1)$. The set $\mathcal{C}$ of all $\vec{w} = (w_1, \dots, w_k) \in W^{(k)}$ satisfying the following conditions is exponentially generic*:

(1) $|w_i| \ge |\vec{w}|(1-\varepsilon)$ *for* $1 \le i \le k$.
(2) $|\overline{w}_i| \ge (\frac{1-\theta}{\theta} - \varepsilon)|w_i| + 2\delta$.
(3) $(\overline{w}_i^{\pm 1} | \overline{w}_j^{\pm 1})_1 < \varepsilon|\vec{w}|$ *except when $i = j$ and the exponents are equal.*

Proof. It suffices to show that for each condition above the set of $\vec{w}$'s which satisfy that condition is exponentially generic. A straightforward counting argument suffices for (1), and (2) follows from Lemma 3.3. The remaining assertion follows from Lemmas 4.1 and 4.2. □

Now we complete the proof of Theorem 2.1.

Proof of Theroem 2.1. Pick $\varepsilon > 0$ as in the statement of Theorem 2.1(2). If $\varepsilon \ge \frac{1-\theta}{\theta}$, then Theorem 2.1(2) is vacuous, so we may assume $0 < \varepsilon < \frac{1-\theta}{\theta}$. Let $\varepsilon' = \varepsilon/4$. We apply Lemma 4.3 with ε' in place of ε to show that the conclusions of Theorem 2.1 hold for all $\vec{w} \in \mathcal{C}$.

Fix $\vec{w} = (w_1, \dots, w_k) \in \mathcal{C}$ and consider any freely reduced word z in the w_i's. Write $z = x_1 \cdots x_t$ where each x_j equals w_i or w_i^{-1} for some i. By equation (3.4) and Lemma 4.3

$$\begin{aligned}|\overline{x}_j - \overline{x}_{j+1}| &= |\overline{x}_j| + |\overline{x}_{j+1}| - 2(\overline{x}_j | \overline{x}_{j+1})_1 \\ &\ge \max\{|\overline{x}_j|, |\overline{x}_{j+1}|\} + \min\{|\overline{x}_j|, |\overline{x}_{j+1}|\} - 2\varepsilon'|\vec{w}| \\ &\ge \max\{|\overline{x}_j|, |\overline{x}_{j+1}|\} + \left(\frac{1-\theta}{\theta} - \varepsilon'\right)|\vec{w}|(1-\varepsilon') + 2\delta - 2\varepsilon'|\vec{w}| \\ &\ge \max\{|\overline{x}_j|, |\overline{x}_{j+1}|\} + \left(\frac{1-\theta}{\theta} - \varepsilon\right)|\vec{w}| + 2\delta,\end{aligned}$$

where the last step depends on the inequality $\theta \ge 1/2$ from Section 3.2.

For $1 < \ell \le t$ Lemma 3.6 yields

$$|\overline{x_1 \cdots x_\ell}| \ge |\overline{x_1 \cdots x_{\ell-1}}| + \left(\frac{1-\theta}{\theta} - \varepsilon\right)|\vec{w}| \ge \ell\left(\frac{1-\theta}{\theta} - \varepsilon\right)|\vec{w}| > 0.$$

Hence $|\overline{z}| > 0$, which implies that $Y = \{w_1, \ldots, w_k\}$ freely generates a free subgroup $H \subset G$. In addition, since $|\overline{z}|_G = |\overline{z}| \ge t(\frac{1-\theta}{\theta} - \varepsilon)|\vec{w}|$ and $|\overline{z}|_{G,H} \le t|\vec{w}|$, the compression factor is bounded below by $\frac{1-\theta}{\theta} - \varepsilon$. □

The last part of the preceding proof provides the following corollary.

COROLLARY 4.4. *Let $\mathcal{D}$ be the set of all K-tuples $\vec{w} = (w_1, \ldots, w_k)$ such that $|\overline{w_i}^{\pm 1} - \overline{w_j}^{\pm 1}| > \max|\overline{w_i}|, |\overline{w_j}| + 2\delta$ except when $i = j$ and the exponents agree. $\mathcal{D}$ is exponentially generic, and for each $\vec{w} = (w_1, \ldots, w_k) \in \mathcal{D}$ and freely reduced word $w_{i_1}^{e_1} \cdots w_{i_t}^{e_t}$, $|\overline{w_{i_1}^{e_1} \cdots w_{i_\ell}^{e_\ell}}| > |\overline{w_{i_1}^{e_1} \cdots w_{i_{\ell-1}}^{e_{\ell-1}}}|$ for $1 < \ell \le t$.*

Proof. D is exponentially generic because it contains $\mathcal{C}$. By hypothesis, there exists $\kappa > 0$ such that

$$|\overline{w}_j^{\pm 1} - \overline{w}_{j+1}^{\pm 1}| > \max\{|\overline{w}_i|, |\overline{w}_j|\} + \kappa + 2\delta$$

for all applicable cases. Lemma 3.6 applies. □

5. The membership problem for generic subgroups of hyperbolic groups

Let $W \to G$ be a choice of generators for G. The membership problem is to decide for words $z, w_1, \ldots, w_k \in W$ if $\overline{u}$ is in the subgroup generated by $\overline{w_1}, \ldots, \overline{w_k}$. Corollary 4.4 provides the basis for a procedure to solve the membership problem once we know how to compute geodesic representatives for $u \in W$, that is words of minimum length with the same image in G as u.

There is no uniform algorithm for computing geodesic representatives in presentations of hyperbolic groups. If there were, then since trivial groups are hyperbolic, there would be a feasible procedure to decide whether a finite presentation presents the trivial group; namely check the geodesic length of all the generators. However, this decision problem is unsolvable.

On the other hand given a presentation for a hyperbolic group G, one can precompute a strongly geodesic automatic structure for G with respect to the original choice of generators as well as an integer δ such that all geodesic triangles are δ-thin [EH]. For the reasons we have discussed, there is no computable bound (in terms of the size of the original presentation) for how long this precomputation will take. Nevertheless, once the precomputation is done, one can compute geodesic representatives in linear time by an algorithm due to Shapiro [EH2].

By Corollary 4.4, the following partial algorithm solves the membership problem for all $z \in W$ and $(w_1, \ldots, w_k) \in \mathcal{D}$. If in addition z is in the subgroup generated by the $w_1, \ldots, w_k$, the algorithm expresses z as a word in the w_i's.

ALGORITHM 5.1. INPUT $\vec{w} = (w_1, \dots, w_k) \in W$, and $z \in W$
IF the hypothesis of Corollary 4.4 does not hold, OUTPUT "Failure"
ELSE WHILE $|\overline{z}| > 0$
IF $|\overline{zw_j^e}| < |\overline{z}|$ for some j and $e = \pm 1$,
THEN OUTPUT w_j^e and set z equal to a geodesic representative of zw_j^e
ELSE OUTPUT "Failure" and halt
OUTPUT "z is in the subgroup generated by $w_1, \dots, w_k$."

Checking the hypothesis of Corollary 4.4 requires computing $O(k^2)$ geodesic lengths for words of length at most $2|\vec{w}|$. There will be no more than $|z|$ passes through the while loop, and during each pass $O(k)$ geodesic representatives are computed for words of length at most $|z| + |\vec{w}|$. Thus, the time complexity of Algorithm 5.1 is $O(k^2 + k|z|)(2|\vec{w}| + |z|) = O((k|\vec{w}| + |z|)^3)$.

6. The word problem for amenable groups

In this section, we prove Theorem 2.3.

Proof of Theorem 2.3. Let G be a finitely presented amenable group with choice of generators $W \to G$ and unsolvable word problem. Let $\mathcal{A}$ be a correct partial algorithm for the word problem in G. The input to $\mathcal{A}$ is a word $w \in W$. Assume that D, the domain of $\mathcal{A}$, is exponentially generic; that is, there exists a positive $\rho < 1$ such that

$$\frac{|W_n - D|}{|W_n|} \le \rho^n \quad \text{for } n \text{ large enough,} \tag{6.1}$$

where W_n is the set of words of length n. We shall obtain a contradiction by showing that under these conditions the word problem for G is solvable.

Let $\mathcal{B}$ be the partial algorithm which on input w recursively enumerates all words $v_1, v_2, \dots$ defining the identity in G and applies $\mathcal{A}$ to $wv_1, wv_2, \dots$. Since $\mathcal{A}$ does not always converge, we organize this computation as follows. For each $m = 1, 2, \dots, \mathcal{B}$ computes $v_1, \dots, v_m$, and applies the first m steps of $\mathcal{A}$ to each wv_i. If $\mathcal{A}$ halts for some i, then eventually $\mathcal{B}$ discovers that fact and halts too. $\mathcal{B}$ accepts w as a word defining the identity if and only if $\mathcal{A}$ accepts wv_i.

Clearly, $\mathcal{B}$ converges on w if and only if $\mathcal{A}$ converges on some wv_i. Hence, there must exist a word w such that $\mathcal{A}$ does not halt on any wv_i. Fix $n > |w|$. For any v_i of length $n - |w|$, we have $wv_i \in W_n - D$ because $\mathcal{A}$ does not halt on wv_i. We conclude

$$|W_n - D| \ge \left|V_{n-|w|}\right|,$$

where for any $k \ge 0$, V_k is the set of words of length k which define the identity in G. Since G is amenable, we have

$$\lim_{k \to \infty, 2|k} \left(\frac{|V_k|}{|W_k|} \right)^{1/k} = 1.$$

It follows from the equations above that for n large enough and even,

$$\left|V_{n-|w|}\right| \geq \left(\frac{1+\rho}{2}\right)^{(n-|w|)} \left|W_{(n-|w|)}\right|,$$

whence

$$|W_n - D| \geq \left(\frac{1+\rho}{2}\right)^{(n-|w|)} \left|W_{(n-|w|)}\right|$$

which implies

$$\rho^n \geq \frac{|W_n - D|}{|W_n|} \geq C_w \left(\frac{1+\rho}{2}\right)^n$$

for some constant C_w (depending on w) and infinitely many n, which is impossible since $\rho < \frac{1+\rho}{2}$. □

7. Open problems

In this section, we formulate some open problems which seem to be interesting in this area.

Let G be a group generated by a finite set A and W the free monoid with basis $A \cup A^{-1}$. For $k \geq 1$, put $W^{(k)} = \{(w_1, \ldots, w_k) \mid w_i \in W\}$ and define the disk of radius n in $W^{(k)}$ by $W_n^{(k)} = \{(w_1, \ldots, w_k) \in W^{(k)} \mid |w_i| \leq n\}$.

We say that a group G satisfies the *generic free basis* property if for each choice of generators $W \to G$ and every $k \geq 1$ the set of all tuples $(w_1, \ldots, w_k) \in W^{(k)}$ for which $\overline{w}_1, \ldots, \overline{w}_k$ generate a free subgroup of rank k in G, is generic with respect to the stratification $W^{(k)} = \bigcup_{n=1}^{\infty} W_n^{(k)}$.

Problem 7.1. Does a finitely generated group G have the generic free basis property if some of its subgroups of finite index has it?

Problem 7.2. Does the group $SL(n, \mathbb{Z})$, $n \geq 3$, have the generic free basis property?

Problem 7.3. Construct a finitely presented group where the word problem is undecidable on every generic set of inputs (which are words in a given finite generating set).

References

[AAG] I. Anshel, M. Anshel and D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), 287–291. MR 1713130

[AO] G. Arzhantseva and A. Olshanskii, *Generality of the class of groups in which subgroups with a lesser number of generators are free*, (Russian) Mat. Zametki **59** (1996), 489–496; translation in Math. Notes **59** (1996), 350–355. MR 1445193

[Arz1] G. Arzhantseva, *On groups in which subgroups with a fixed number of generators are free*, (Russian) Fundam. Prikl. Mat. **3** (1997), 675–683. MR 1794135

[Arz2] G. Arzhantseva, *Generic properties of finitely presented groups and Howson's theorem*, Comm. Algebra **26** (1998), 3783–3792. MR 1647075

[BauMS] G. Baumslag, C. F. Miller III and H. Short, *Unsolvable problems about small cancellation and word hyperbolic groups*, Bull. London Math. Soc. **26** (1994), 97–101. MR 1246477

[BV1] O. Bogopolski and E. Ventura, *The mean Dehn function of Abelian groups*, J. Group Theory **11** (2008), 569–586. MR 2429356

[BV2] J. Burillo and E. Ventura, *Counting primitive elements in free groups*, Geom. Dedicata **93** (2002), 143–162. MR 1934695

[BH] M. Bridson and A. Haefliger, *Metric spaces of non-positive curvature*, Springer, Berlin, 1999. MR 1744486

[BW] M. Bridson and D. Wise, *Malnormality is undecidable in hyperbolic groups*, Israel J. of Math. **124** (2001), 313–316. MR 1856523

[BMS] A. V. Borovik, A. G. Myasnikov and V. Shpilrain, *Measuring sets in infinite groups*, Computational and statistical group theory, Contemporary Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 21–42. MR 1929714

[BMR1] A. Borovik, A. Myasnikov and V. Remeslennikov, *Multiplicative measures on free groups*, Internat. J. Algebra Comput. **13** (2003), 705–731. MR 2028100

[BMR2] A. V. Borovik, A. G. Myasnikov and V. N. Remeslennikov, *Algorithmic stratification of the conjugacy problem in Miller's groups*, Internat. J. Algebra Comput. **17** (2007), 963–997. MR 2355678

[BMR3] A. V. Borovik, A. G. Myasnikov and V. N. Remeslennikov, *The conjugacy problem in amalgamated products I: regular elements and black holes*, Internat. J. Algebra Comput. **17** (2007), 1301–1335 MR 2372599

[BM] A. V. Borovik and A. G. Myasnikov, *Quotient tests and random walks in computational group theory*, Topological and asymptotic aspects of group theory, Contemp. Math., vol. 394, Amer. Math. Soc., Providence, RI, 2006, pp. 31–45. MR 2216704

[Cha1] C. Champetier, *Proprietes statistiques des groupes de presentation finie*, Adv. Math. **116** (1995), 197–262. MR 1363765

[Cha2] C. Champetier, *The space of finitely generated groups*, Topology **39** (2000), 657–680. MR 1760424

[CS] P.-A. Cherix and G. Schaeffer, *An asymptotic Freiheitssatz for finitely generated groups*, Enseign. Math. **44** (1998), 9–22. MR 1643258

[CERT] S. Cleary, M. Elder, A. Rechnitzer and J. Taback, *Random subgroups of Thompson's group F*, Groups Geom. Dyn. **4** (2010), 91–126. MR 2566302

[Coh] J. M. Cohen, *Cogrowth and amenability of discrete groups*, J. Funct. Anal. **48** (1982), 301–309. MR 0678175

[CDP] M. Coornaert, T. Delzant and A. Papadopoulos, *Géométrie et théorie des groupes*, Lecture Notes in Math., vol. 1441, Springer, Berlin, 1990. MR 1075994

[Del] T. Delzant, *Sous-groupes à deux générateurs des groupes hyperboliques*, Group theory from a geometrical viewpoint (Trieste, 1990), World Scientific Publ., River Edge, NJ, 1991, pp. 177–189. MR 1170366

[EH] D. B. A. Epstein and D. F. Holt, *Computation in word-hyperbolic groups*, Internat. J. Algebra Comput. **11** (2001), 467–487. MR 1850213

[EH2] D. B. A. Epstein and D. F. Holt, *The linearity of the conjugacy problem in word–hyperbolic groups*, Internat. J. Algebra Comput. **16** (2006), 287–305. MR 2228514

[FMR] B. Fine, A. Myasnikov and G. Rosenberger, *Generic subgroups of group amalgams*, Groups Complexity Cryptology **1** (2009), 51–61. MR 2502936

[GKTTV] D. Garber, S. Kaplan, M. Teicher, B. Tsaban and U. Vishne, *Length-based conjugacy search in the Braid group*, Algebraic methods in cryptography, Contemporary Mathematics, vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 75–88. MR 2389290

[GdH] E. Ghys and P. de la Harpe, eds., *Sur les groupes hyperboliques d'aprés Mikhael Gromov*, Progress in Math., vol. 83, Birkhäuser, Boston, 1990. MR 1086648

[Gri1] R. I. Grigorchuk, *Symmetric random walks on discrete groups*, Russian Math. Surv. **32** (1977), 217–218. MR 0474511

[Gri2] R. I. Grigorchuk, *Symmetrical random walks on discrete groups*, Multicomponent random systems (R. L. Dobrushin and Y. G. Sinai, eds.), Dekker, New York, 1980, pp. 285–325. MR 0599539

[Gro] M. Gromov, *Hyperbolic groups*, Essays in group theory, MSRI Series, vol. 8, (S. M. Gersten, ed.), Springer, New York, 1987, pp. 75–263. MR 0919829

[Gro2] M. Gromov, *Asymptotic invariants of infinite groups*, Geometric group theory, vol. 2 (Sussex, 1991), London Math. Soc. Lecture Note Ser., vol. 182, Cambridge Univ. Press, Cambridge, 1993, pp. 1–295. MR 1253544

[Gro3] M. Gromov, *Random walks in random groups*, Geom. Funct. Anal. **13** (2003), 73–146. MR 1978492

[HM] J. Hamkins and A. Myasnikov, *The halting problem is almost always decidable*, Notre Dame Journal of Formal Logic **47** (2006), 515–524. MR 2272085

[HT] J. Hughes and A. Tannenbaum, *Length-based attacks for certain group based encryption rewriting systems*, Workshop SECI02 Securite de la Communication sur Intenet, September 2002, Tunis, Tunisia.

[Jit] T. Jitsukawa, *Malnormal subgroups of free groups*, Computational and statistical group theory, Contemporary Mathematics, vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 83–96. MR 1929717

[KMSS1] I. Kapovich, A. Myasnikov, P. Schupp and V. Shpilrain, *Generic-case complexity and decision problems in group theory*, J. Algebra **264** (2003), 665–694. MR 1981427

[KMSS2] I. Kapovich, A. Myasnikov, P. Schupp and V. Shpilrain, *Average-case complexity for the word and membership problems in group theory*, Adv. Math. **190** (2005), 343–359. MR 2102661

[KSS] 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** (2006), 113–140. MR 2221020

[KS1] I. Kapovich and P. Schupp, *Genericity, the Arzhantseva–Olshanskii method and the isomorphism problem for one-relator groups*, Math. Ann. **331** (2005), 1–19. MR 2107437

[KS2] I. Kapovich and P. Schupp, *Delzant's T-ivariant, one-relator groups and Kolmogorov complexity*, Comment. Math. Helv. **80** (2005), 911–933. MR 2182705

[KRSS] I. Kapovich, I. Rivin, P. Schupp and V. Shpilrain, *Densities in free groups and $\mathbb{Z}^k$, visible points and test elements*, Math. Res. Lett. **14** (2007), 263–284. MR 2318624

[Kes1] H. Kesten, *Symmetric random walks on groups*, Trans. Amer. Math. Soc. **92** (1959), 336–354. MR 0109367

[Kes2] H. Kesten, *Full Banach mean values on countable groups*, Math. Scand. **7** (1959), 146–156. MR 0112053

[Kh] O. Kharlampovich, *A finitely presented solvable group with unsolvable word problem*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), 852–873, 928. MR 0631441

[KR] E. G. Kukina and V. A. Roman'kov, *Subquadratic growth of the averaged Dehn function for free Abelian groups*, Siberian Math. J. **44** (2003), 605–610. MR 2010125

[Mah] J. Maher, *Random walks on the mapping class group*, to appear in Duke Math. J.; available at `arXiv:math/0604433`, 2008.

[MTV] A. Martino, T. Turner and E. Ventura, *The density of injective endomorphisms of a free group*, preprint, 2008.

[MR] A. G. Myasnikov and A. N. Rybalov, *Generic complexity of undecidable problems*, J. Symbolic Logic **73** (2008), 656–673. MR 2414470

[MU] A. G. Myasnikov and A. Ushakov, *Random subgroups and analysis of the length-based and quotient attacks*, J. Math. Cryptol. **1** (2007), 15–47. MR 2451658

[MSU1] A. G. Myasnikov, V. Shpilrain and A. Ushakov, *Advanced course on group-based cryptography*, Quaderns, vol. 42, CRM, Barcelona, 2007. MR 2437984

[MSU2] A. G. Myasnikov, V. Shpilrain and A. Ushakov, *Random subgroups of braid groups: an approach to cryptanalysis of a braid group based cryptographic protocol*, PKC 2006, Lecture Notes Comp. Sci., vol. 3958, Springer, Berlin, 2006, pp. 302–314. MR 2423197

[MUW] A. Myasnikov, A. Ushakov and D. W. Won, *On the word problem for balanced semigroups and groups*, preprint, 2009.

[Oll] Y. Ollivier, *Critical densities for random quotients of hyperbolic groups*, C. R. Math. Acad. Sci. Paris **336** (2003), 391–394. MR 1979351

[Olsh] A. Y. Olshanskii, *Almost every group is hyperbolic*, Internat. J. Algebra Comput. **2** (1992), 1–17. MR 1167524

[Osi] D. Osin, *Peripheral fillings of relatively hyperbolic groups*, Invent. Math. **167** (2007), 295–326. MR 2270456

[Rips] E. Rips, *Subgroups of small cancellation groups*, Bull. London Math. Soc. **14** (1982), 45–47. MR 0642423

[Riv] I. Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. **142** (2008), 353–379. MR 2401624

[Rom] V. A. Roman'kov, *Asymptotic growth of averaged Dehn functions for nilpotent groups*, Algebra Logic **46** (2007), 37–45. MR 2321080

[RST] D. Ruinsky, A. Shamir and B. Tsaban, *Cryptanalysis of group-based key agreement protocols using subgroup distance functions*, Advances in cryptology—PKC 2007, Lecture Notes in Computer Science, vol. 4450, Springer, Berlin, 2007, pp. 61–75. MR 2404112

[Sha] A. Shalev, *Probabilistic group theory*, Groups St. Andrews 1997 in Bath, II, London Math. Soc., Lecture Notes Ser., vol. 261, Cambridge Univ. Press, pp. 648–679. MR 1676661

[Woe] W. Woess, *Cogrowth of groups and simple random walks*, Arch. Math. **41** (1983), 363–370. MR 0731608

[Zuk] A. Zuk, *On property (T) for discrete groups*, Rigidity in dynamics and geometry (Cambridge, 2000), Springer, Berlin, 2002, pp. 473–482. MR 1919418

Robert Gilman, Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken, NJ 07030, USA

E-mail address: rgilman@stevens.edu

Alexei Miasnikov, Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken, NJ 07030, USA

E-mail address: amiasnikov@gmail.com

Denis Osin, Mathematics Department, Vanderbilt University, Nashville, TN 37240, USA

E-mail address: denis.v.osin@vanderbilt.edu