

RANDOM EXTENSIONS OF FREE GROUPS AND SURFACE GROUPS ARE HYPERBOLIC

SAMUEL J. TAYLOR AND GIULIO TIOZZO

ABSTRACT. In this note, we prove that a random extension of either the free group F_N of rank $N \geq 3$ or of the fundamental group of a closed, orientable surface S_g of genus $g \geq 2$ is a hyperbolic group. Here, a random extension is one corresponding to a subgroup of either $\text{Out}(F_N)$ or $\text{Mod}(S_g)$ generated by k independent random walks. Our main theorem has several applications, including that a random subgroup of a weakly hyperbolic group is free and undistorted.

1. INTRODUCTION

Let $F = F_N$ denote the free group of rank $N \geq 3$ and $S = S_g$ the closed, orientable surface of genus $g \geq 2$. Group extensions of both F and $\pi_1(S)$ can be understood by investigating subgroups of their respective outer automorphism groups. For this, denote the outer automorphism group of F by $\text{Out}(F)$ and the mapping class group of S by $\text{Mod}(S)$.

For the surface S , there is the well-known Birman exact sequence [Bir69]

$$1 \rightarrow \pi_1(S) \rightarrow \text{Mod}(S; p) \xrightarrow{f} \text{Mod}(S) \rightarrow 1,$$

where $\text{Mod}(S; p)$ denotes the group of mapping classes that fix the marked point $p \in S$ and $f : \text{Mod}(S; p) \rightarrow \text{Mod}(S)$ is the surjective homomorphism that forgets this requirement. Given any finitely generated subgroup $\Gamma \leq \text{Mod}(S)$, its preimage $E_\Gamma = f^{-1}(\Gamma)$ in $\text{Mod}(S; p)$ is a finitely generated group fitting into the sequence

$$1 \rightarrow \pi_1(S) \rightarrow E_\Gamma \rightarrow \Gamma \rightarrow 1.$$

We say that E_Γ is the *surface group extension* corresponding to $\Gamma \leq \text{Mod}(S)$. Much work has gone into understanding what conditions on $\Gamma \leq \text{Mod}(S)$ imply that the corresponding extension E_Γ is hyperbolic. Such subgroups were introduced by Farb and Mosher as *convex cocompact* subgroups of the mapping class group [FM02] and have since become an active area of study. See for example [KL08, KL07, Ham05, DKL12, MT13] and Section 2.2 for details.

The situation for extensions of the free group F is similar; by definition there is the short exact sequence

$$1 \rightarrow F \rightarrow \text{Aut}(F) \xrightarrow{f} \text{Out}(F) \rightarrow 1,$$

where $f : \text{Aut}(F) \rightarrow \text{Out}(F)$ is now the induced quotient homomorphism. As before, a finitely generate subgroup $\Gamma \leq \text{Out}(F)$ pulls back via f to the corresponding *free*

group extension $E_\Gamma = f^{-1}(\Gamma)$. Conditions on $\Gamma \leq \text{Out}(F)$ which imply that the extension group E_Γ is hyperbolic were recently given by Dowdall and the first author in [DT14a]. See Section 2.3 for details.

In this note, we consider the following question:

Question 1.1. *Given a random subgroup Γ of either $\text{Mod}(S)$ or $\text{Out}(F)$, how likely is it that the corresponding extension group E_Γ is hyperbolic?*

By employing techniques developed by Maher and the second author in [MT14], we answer Question 1.1 by considering subgroups generated by random walks on either $\text{Mod}(S)$ or $\text{Out}(F)$. The point is that the references above characterize hyperbolicity of the extension group E_Γ (for both F and $\pi_1(S)$) solely in terms of the action of Γ on a certain hyperbolic graph. This is precisely the situation considered in [MT14]. For this reason, we can treat both the cases of free group extensions and surface group extensions at once.

1.1. Results. To state our main theorem, we briefly introduce our model of random subgroups. Additional background on random walks is given in Section 2.1.

First, let X be a separable hyperbolic metric space and G a countable group acting on X by isometries. The action $G \curvearrowright X$ is said to be *nonelementary* if there are $g, h \in G$ which are loxodromic for the action and whose quasiaxis determine 4 distinct endpoints on ∂X . A probability measure μ on G is *nonelementary* if the semigroup generated by its support is a subgroup of G whose action on X is nonelementary.

Now let μ be a nonelementary probability measure on G with respect to the action $G \curvearrowright X$ and consider k independent random walks $(w_n^1)_{n \in \mathbb{N}}, \dots, (w_n^k)_{n \in \mathbb{N}}$ whose increments are distributed according to μ . For each $n \in \mathbb{N}$, we can consider the subgroup generated by the n^{th} steps of our random walks,

$$\Gamma(n) = \langle w_n^1, \dots, w_n^k \rangle \leq G,$$

which we endow with the word metric coming from a given generating set.

Theorem 1.2. *Let G be a countable group with a nonelementary action by isometries on a separable hyperbolic space X . Let μ be a nonelementary probability measure on G and fix $x_0 \in X$. Then, the probability that the orbit map*

$$\begin{aligned} \Gamma(n) = \langle w_n^1, \dots, w_n^k \rangle &\rightarrow X \\ g &\mapsto g \cdot x_0 \end{aligned}$$

is a quasi-isometric embedding goes to 1 as $n \rightarrow \infty$.

Combining Theorem 1.2 with work of Farb–Mosher [FM02], Kent–Leininger [KL08], and Hamenstädt [Ham05] (see Section 2.2) answers Question 1.1 for surface group extensions:

Theorem 1.3 (Random surface group extensions). *Let μ be a nonelementary probability measure on $\text{Mod}(S)$ and let $\Gamma(n) = \langle w_n^1, \dots, w_n^k \rangle$ denote the subgroup generated by the n^{th} steps of k independent random walks. Then the probability that the surface group extension $E_{\Gamma(n)}$ is hyperbolic goes to 1 as $n \rightarrow \infty$.*

Proof. As discussed in Section 2.2, the mapping class group has a nonelementary action by isometries on the curve graph $\mathcal{C}(S)$. Theorem 1.2 then implies that the probability that the orbit map $\Gamma(n) \rightarrow \mathcal{C}(S)$ is a quasi-isometric embedding goes to 1 as $n \rightarrow \infty$. Since the extension $E_{\Gamma(n)}$ is hyperbolic whenever $\Gamma(n) \rightarrow \mathcal{C}(S)$ is a quasi-isometric embedding (Theorem 2.3), the theorem follows. \square

For extensions of free groups, we answer Question 1.1 by combining Theorem 1.2 with work of Dowdall and the first author [DT14a] (see Section 2.3):

Theorem 1.4 (Random free group extensions). *Let μ be a nonelementary probability measure on $\text{Out}(F)$ and let $\Gamma(n) = \langle w_n^1, \dots, w_n^k \rangle$. Then the probability that the free group extension $E_{\Gamma(n)}$ is hyperbolic goes to 1 as $n \rightarrow \infty$.*

Proof. As in Section 2.3, $\text{Out}(F)$ has a nonelementary action by isometries on the hyperbolic graph \mathcal{I} . The remainder of the proof follows exactly as in Theorem 1.3 after replacing $\mathcal{C}(S)$ with \mathcal{I} and using Theorem 2.5 in place of Theorem 2.3. \square

Remark 1.5. When $k = 1$, Theorem 1.3 is equivalent to the statement that the probability that w_n is pseudo-Anosov goes to 1 as $n \rightarrow \infty$. Versions of this result were proven by Rivin in [Riv08] and Maher in [Mah11]. Likewise, Theorem 1.4 was also previously known in the special case where $k = 1$, though by different methods. Indeed, Ilya Kapovich and Igor Rivin showed that for a random walk (w_n) on $\text{Out}(F)$ (with additional restrictions on the measure μ), the probability that w_n is atoroidal and fully irreducible goes to 1 as $n \rightarrow \infty$ [Riv10]. (See Section 2.3 for definitions.)

1.2. Further applications. Thanks to the generality of Theorem 1.2, which is made possible by the general framework of [MT14], we can provide several other applications of interest. Following [MT14], we say that G is *weakly hyperbolic* if G admits a nonelementary action on a separable hyperbolic space X . We say that a *random subgroup of G has property P* if

$$\mathbb{P}[\Gamma(n) \text{ has } P] \rightarrow 1$$

as $n \rightarrow \infty$. For any nonelementary measure μ , the proof of Theorem 1.2 additionally yields the following corollary.

Corollary 1.6. *A random subgroup of a weakly hyperbolic group is free and undistorted.*

We note that when G itself is a hyperbolic group, Gilman, Miasnikov, and Osin have shown that a random k -generated subgroup of G is free and undistorted [GMO10]. The novelty of Corollary 1.6 is that it applies to a much larger class of groups; e.g. mapping class groups, outer automorphism groups of free groups, right-angled Artin groups, acylindrically hyperbolic groups, and others. Our model of random subgroups appears in several other places in the literature: starting from Guivarc'h's random walk proof of the Tits alternative [Gui90], it is explicitly formulated by Rivin [Riv10], and Aoun [Aou11], who proves that a random subgroup of a non-virtually solvable linear group is free and undistorted. Moreover, Myasnikov and Ushakov [MU08] prove that random subgroups of pure braid groups are free, and provide applications of such

results to cryptography.

As in the situation of the actions $\text{Mod}(S) \curvearrowright \mathcal{C}(S)$ and $\text{Out}(F) \curvearrowright \mathcal{I}$ (discussed in Sections 2.2 and 2.3), one is often particularly interested in those elements that act as loxodromic isometries (i.e. have positive translation length). It is immediate from Theorem 1.2 that, under the hypotheses of the theorem, every element of a random subgroup of G is loxodromic.

In the special case of a right-angled Artin group $A(\Gamma)$, Kim and Koberda have introduced the extension graph Γ^e , a hyperbolic graph which admits a nonelementary action $A(\Gamma) \curvearrowright \Gamma^e$ [KK13]. The loxodromic isometries of $A(\Gamma)$ with respect to this action are precisely those $g \in A(\Gamma)$ with cyclic centralizers. In [KMT14], the authors study the properties of *purely loxodromic* subgroups of $A(\Gamma)$, i.e. the subgroups for which all nontrivial elements are loxodromic, and show their resemblance to convex cocompact subgroups of mapping class groups. From Theorem 1.2, we have the following:

Corollary 1.7. *Let Γ be a finite simplicial graph that does not decompose as a non-trivial join. Then a random subgroup of $A(\Gamma)$ is purely loxodromic.*

Acknowledgments. We would like to thank Joseph Maher for several useful conversations. The first named author is partially supported by NSF DMS-1204592.

2. BACKGROUND

2.1. Random walks. Let μ be a probability measure on a countable group G . In order to define a random walk on G , let us consider a probability space (Ω, \mathbb{P}) , and for each $n \in \mathbb{N}$, let $g_n : \Omega \rightarrow G$ be a G -valued random variable such that the g_n 's are independent and identically distributed with distribution μ . We define the n^{th} step of the random walk to be the variable $w_n : \Omega \rightarrow G$

$$w_n := g_1 g_2 \cdots g_n.$$

The sequence $(w_n)_{n \in \mathbb{N}}$ is called a *sample path* of the random walk. We denote as μ_n the distribution of w_n , which equals the n -fold convolution of μ with itself. That is,

$$\mu_n(x) = \mathbb{P}[w_n = x] = \sum_{x=g_1 \cdots g_n} \mu(g_1) \cdots \mu(g_n),$$

which describes the probability that the n^{th} step of the random walk lands at $x \in G$.

Moreover, the *reflected measure* $\check{\mu}$ is defined as $\check{\mu}(g) := \mu(g^{-1})$. We note that for the random walk (w_n) , the distribution of w_n^{-1} , the inverse of the n^{th} step of the random walk, is given by $(\check{\mu})_n = (\check{\mu}_n)$.

Just as a random walk allows one to speak of a “random” element of G , we can use k independent random walks to model a (k -generator) random subgroup of G . In details, fix a probability measure μ on G and let $(w_n^1)_{n \in \mathbb{N}}, \dots, (w_n^k)_{n \in \mathbb{N}}$ be k independent random walks each of whose increments are distributed according to μ . For each $n \in \mathbb{N}$, we can consider the subgroup generated by the n^{th} steps of our sample

paths,

$$\Gamma(n) = \langle w_n^1, \dots, w_n^k \rangle \leq G.$$

For example, if G is finitely generated and μ is supported on a finite, symmetric generating set S for G , then $\Gamma(n)$ is the subgroup generated by selecting k (unreduced) words of length n in the basis S uniformly at random.

We remark that this model for a random subgroup of G appears several places in the literature, see for example [Gui90], [MU08], [GMO10], [Riv10], and [Aou11].

Now suppose that X is a separable hyperbolic space and that G acts on X by isometries. The action $G \curvearrowright X$ is *nonelementary* if there are $g, h \in G$ which act loxodromically on X and whose fixed point sets on the Gromov boundary of X are disjoint. Recall that an isometry g of X is *loxodromic* if it has positive translation length on X , i.e. $\liminf_{n \rightarrow \infty} d(x_0, gx_0)/n > 0$ for some $x_0 \in X$. A probability measure μ on G is said to be *nonelementary* with respect to the action $G \curvearrowright X$ if the semigroup generated by the support of μ is a subgroup of G whose action on X is nonelementary. In this note, we are interested in the behavior of the image of a random walk (w_n) under an orbit map $G \rightarrow X$. Hence, we fix once and for all a basepoint $x_0 \in X$ and consider the orbit map $G \rightarrow X$ given by $g \mapsto gx_0$.

Central to Maher and Tiozzo's study of random walks on G is the notion of shadows, which we now summarize. Given $x_0, x \in X$ and $R \geq 0$, the *shadow* $S_{x_0}(x, R) \subset X$ is by definition the set

$$S_{x_0}(x, R) = \{y \in X : (x \cdot y)_{x_0} \geq d_X(x_0, x) - R\}.$$

When $R < 0$, we declare that $S_{x_0}(x, R) = \emptyset$. The *distance parameter* of the shadow $S_{x_0}(x, R)$ is the quantity $d(x_0, x) - R$, which is coarsely equal to the distance from x_0 to the shadow. It follows easily from hyperbolicity of X that there is a constant C , depending only on the hyperbolicity constant of X , such that

$$(1) \quad (X \setminus S_{x_0}(x, R)) \subset S_x(x_0, d(x_0, x) - R + C).$$

See [MT14] for details.

We will need two additional results from [MT14]. The first roughly states that the measure of a shadow decays to zero as the distance parameter goes to infinity. For the precise statement, set

$$Sh(x_0, r) = \{S_{x_0}(gx_0, R) : g \in G \text{ and } d(x_0, gx_0) - R \geq r\}.$$

This is the set of shadows based at x_0 and centered at points in the orbit of x_0 with distance parameter at least r . The following is Corollary 5.3 of [MT14].

Lemma 2.1 (Maher–Tiozzo). *Let G be a countable group which acts by isometries on a separable hyperbolic space X , and let μ be a nonelementary probability distribution on G . Then there is a function $f(r)$, with $f(r) \rightarrow 0$ as $r \rightarrow \infty$ such that for all n*

$$\sup_{S \in Sh(x_0, r)} \left\{ \begin{array}{l} \mu_n(S) \\ \check{\mu}_n(S) \end{array} \right\} \leq f(r).$$

Finally, we will need the fact that a random walk on G whose increments are distributed according to a nonelementary measure has positive drift in X . This is Theorem 1.2 of [MT14].

Theorem 2.2 (Maher–Tiozzo). *Let G be a countable group which acts by isometries on a separable hyperbolic space X , and let μ be a nonelementary probability distribution on G . Fix $x_0 \in X$. Then, there is a constant $L > 0$ such that for almost every sample path*

$$\liminf_{n \rightarrow \infty} \frac{d(x_0, w_n x_0)}{n} = L > 0.$$

The constant $L > 0$ in Theorem 2.2 is called the *drift* of the random walk (w_n) .

2.2. Hyperbolic extensions of surface groups. Here, we briefly recall some background on convex cocompact subgroups of mapping class groups. See [FM02, KL08] for details.

Fix $S = S_g$, a closed, orientable surface of genus $g \geq 2$. Associated to S are its mapping class group $\text{Mod}(S)$, its Teichmüller space $\mathcal{T}(S)$ (considered with the Teichmüller metric), and its curve graph $\mathcal{C}(S)$. We refer the reader to [FM12] for definitions and background on these standard objects in surface topology. We recall that there are natural actions $\text{Mod}(S) \curvearrowright \mathcal{T}(S)$ and $\text{Mod}(S) \curvearrowright \mathcal{C}(S)$; the former given by remarking and the latter given by the action of mapping classes on isotopy classes of simple closed curves (see remarks following Theorem 2.3 for details). While the action $\text{Mod}(S) \curvearrowright \mathcal{T}(S)$ is properly discontinuous, $\mathcal{T}(S)$ is not negatively curved [Mas75, MW94]. On the other hand, $\mathcal{C}(S)$ is a locally infinite graph and the action $\text{Mod}(S) \curvearrowright \mathcal{C}(S)$ has large vertex stabilizers, but $\mathcal{C}(S)$ is hyperbolic by the foundational work of Masur and Minsky [MM99]. Much can be learned about the coarse geometry of $\text{Mod}(S)$ by studying its action on both $\mathcal{T}(S)$ and $\mathcal{C}(S)$ in conjunction with the equivalent coarsely-Lipschitz map $\mathcal{T}(S) \rightarrow \mathcal{C}(S)$, which associates to each marked hyperbolic surface its collection of shortest curves.

In [FM02], Farb and Mosher introduced convex cocompact subgroups of $\text{Mod}(S)$ as those finitely generated subgroups $\Gamma \leq \text{Mod}(S)$ for which the orbit $\Gamma \cdot X \subset \mathcal{T}(S)$ of some $X \in \mathcal{T}(S)$ is quasiconvex with respect to the Teichmüller metric. Our interest in convex cocompact subgroups of $\text{Mod}(S)$ comes from their connection to hyperbolicity of surface group extensions. This connection is summarized in the following theorem. For additional characterizations of convex cocompactness, see [KL08, DT14b].

Theorem 2.3 (Farb–Mosher, Kent–Leininger, Hamenstädt). *Let Γ be a finitely generated subgroup of $\text{Mod}(S)$. Then the following are equivalent*

- (1) Γ is convex cocompact,
- (2) the orbit map $\Gamma \rightarrow \mathcal{C}(S)$ is a quasi-isometric embedding, and
- (3) the extension E_Γ is hyperbolic.

In Theorem 2.3, the implication (3) \implies (1) is due to Farb–Mosher, as is the converse (1) \implies (3) when Γ is free [FM02]. The general case of (1) \implies (3) is due to Hamenstädt [Ham05]. Finally, the equivalence (1) \iff (2) is due to Kent–Leininger [KL08] and, independently, Hamenstädt [Ham05]. To show that random

subgroups of $\text{Mod}(S)$ induce hyperbolic extensions of $\pi_1(S)$ (Theorem 1.3), we only need the implication (2) \implies (3) in Theorem 2.3. For this, it suffices to know a few details about the action $\text{Mod}(S) \curvearrowright \mathcal{C}(S)$, which we summarize here.

The curve graph $\mathcal{C}(S)$ is the graph whose vertices are isotopy classes of essential simple closed curve and whose edges join vertices that have disjoint representatives on S . As stated above, Masur–Minsky showed that $\mathcal{C}(S)$ is hyperbolic and that the loxodromic elements of the action $\text{Mod}(S) \curvearrowright \mathcal{C}(S)$, i.e. those elements with positive translation length, are precisely the pseudo-Anosov mapping classes [MM99]. From this, it easily follows that the action $\text{Mod}(S) \curvearrowright \mathcal{C}(S)$ is nonelementary. In fact, it is known that the action satisfies the much stronger property of being acylindrical [Bow08], however, we will not need this fact here.

2.3. Hyperbolic extensions of free groups. Here, we recall some background on hyperbolic extensions of free groups. See [DT14a] for additional detail.

Fix $F = F_N$, the free group of rank $N \geq 3$. In [DT14a], Dowdall and the first author study conditions on $\Gamma \leq \text{Out}(F)$ which imply that the extension E_Γ is hyperbolic. In this note, we require a (possibly weaker) version of their main theorem. We begin by describing the particular $\text{Out}(F)$ analog of the curve graph that we will require. This is a version of the intersection graph \mathcal{I} ; an $\text{Out}(F)$ –graph introduced by Kapovich and Lustig in [KL09].

First, let \mathcal{I}' be the graph whose vertices are conjugacy classes of F and two vertices are joined by an edge if there is a very small simplicial tree $F \curvearrowright T$ in which each conjugacy class fixes a point. (Recall that a simplicial tree is very small if edge stabilizers are maximal cyclic and tripod stabilizers are trivial.) Define \mathcal{I} to be the connected component of \mathcal{I}' that contains the primitive conjugacy classes, i.e. those conjugacy classes that belong to some basis for F . Note that we have a simplicial action $\text{Out}(F) \curvearrowright \mathcal{I}$. The following theorem appears in [DT14a], where it is attributed to Brian Mann and Patrick Reynolds:

Theorem 2.4 (Mann–Reynolds [MR]). *The graph \mathcal{I} is hyperbolic and $f \in \text{Out}(F)$ acts with positive translation length on \mathcal{I} if and only if f is atoroidal and fully irreducible.*

Although we will only require the statement of Theorem 2.5, we recall that $f \in \text{Out}(F)$ is fully irreducible if no positive power of f fixes any conjugacy class of any free factor of F . Also, $f \in \text{Out}(F)$ is atoroidal if no positive power fixes any conjugacy class of elements of F . If the extension E_Γ of $\Gamma \leq \text{Out}(F)$ is hyperbolic then it is necessarily the case that each infinite order element of Γ is atoroidal. The following appears as Theorem 9.2 of [DT14a].

Theorem 2.5 (Dowdall–Taylor). *Let Γ be a finitely generated subgroup of $\text{Out}(F)$. Suppose that the orbit map $\Gamma \rightarrow \mathcal{I}$ is a quasi-isometric embedding for some $x_0 \in \mathcal{I}$. Then the corresponding extension E_Γ is hyperbolic.*

Just as in the situation of the mapping class group acting on the curve graph, it follows from Theorem 2.4 that the action $\text{Out}(F) \curvearrowright \mathcal{I}$ is nonelementary, i.e. there exists a pair loxodromic elements with no common fixed points on $\partial\mathcal{I}$. In fact,

according to Mann–Reynolds [MR], the action $\text{Out} \curvearrowright \mathcal{I}$ satisfies the stronger property of being WPD.

3. PROOF OF THEOREM 1.2

We begin by providing conditions for when the orbit map from a k -generator group into a hyperbolic space is a quasi-isometric embedding. We require the following well-known lemma; see, for example, [Gro87, GdlH90, GMO10]. First, recall that for $x, y, z \in X$, the *Gromov product*, denoted $(y \cdot z)_x$, is defined as

$$(y \cdot z)_x = \frac{1}{2}(d(x, y) + d(x, z) - d(y, z)).$$

When X is hyperbolic, the Gromov product $(y \cdot z)_z$ coarsely agrees with the distance from x to any geodesic between y and x . See [BH09] for details.

Lemma 3.1. *Let X be a δ -hyperbolic metric space with points p_0, \dots, p_n satisfying*

$$(2) \quad \min \{d(p_{i-1}, p_i), d(p_i, p_{i+1})\} \geq 2(p_{i-1} \cdot p_{i+1})_{p_i} + 18\delta + 1.$$

Then, $d(p_0, p_n) \geq n$.

Lemma 3.1 easily implies the following:

Lemma 3.2. *Let X be a δ -hyperbolic space and, for $1 \leq i \leq k$, let $g_i \in \text{Isom}(X)$ be isometries of X such that for some $x_0 \in X$ we have*

$$(3) \quad d(x_0, g_i x_0) \geq 2(g_j^{\pm 1} x_0 \cdot g_l^{\pm 1} x_0)_{x_0} + 18\delta + 1$$

for all $1 \leq i, j, l \leq k$ except when $j = l$ and the exponent on the g_j and g_l are the same. Then the orbit map $\langle g_1, \dots, g_k \rangle \rightarrow X$ given by $g \mapsto gx_0$ is a quasi-isometric embedding.

Proof. Set $\Gamma = \langle g_1, \dots, g_k \rangle$. As the orbit map $\Gamma \rightarrow X$ is always coarsely Lipschitz, it suffices to prove that for any $g \in \Gamma$,

$$|g|_\Gamma \leq d(x_0, gx_0).$$

To see this, write $g = s_0 \dots s_n$ as a reduced word where $s_i \in \{g_0^{\pm 1}, \dots, g_k^{\pm 1}\}$ and $n = |g|_\Gamma$. Letting $p_i = (s_0 s_1 \dots s_i) x_0$, we note that by Lemma 3.1 it suffices to show that Inequality (2) holds for these points. Observe that since the action of Γ is by isometries on X ,

$$\begin{aligned} \min \{d(p_{i-1}, p_i), d(p_i, p_{i+1})\} &= \min \{d(x_0, s_i x_0), d(x_0, s_{i+1} x_0)\} \\ &\geq 2(s_i^{-1} x_0 \cdot s_{i+1} x_0)_{x_0} + 18\delta + 1 \\ &= 2(p_{i-1} \cdot p_{i+1})_{p_i} + 18\delta + 1 \end{aligned}$$

where the first inequality holds by (3) and the fact that $s_i \neq s_{i+1}^{-1}$. This completes the proof. \square

Lemma 3.3. *Let G be a countable group with a nonelementary action by isometries on a hyperbolic space X . Let μ be a nonelementary probability measure on G and fix $x_0 \in X$. Suppose that (w_n) and (u_n) be independent random walks on G whose increments are distributed according to μ . Then*

$$(4) \quad \mathbb{P}[(w_n^{\pm 1}x_0 \cdot u_n^{\pm 1}x_0)_{x_0} \leq l(n)] \rightarrow 1,$$

as $n \rightarrow \infty$. Here, $l : \mathbb{N} \rightarrow \mathbb{N}$ is any function with $l(n) \rightarrow \infty$ as $n \rightarrow \infty$.

Proof. First note that since (w_n) and (u_n) are independent random walks with increments distributed according to μ , both w_n and u_n have distribution μ_n . Moreover, w_n^{-1} and u_n^{-1} , the inverses of the n^{th} steps, have distribution $\check{\mu}_n$ as noted at the beginning of Section 2.1. Since the proofs of (4) in each of the 4 possible cases are identical, we show

$$\mathbb{P}[(w_nx_0 \cdot u_n^{-1}x_0)_{x_0} \leq l(n)] \rightarrow 1,$$

as $n \rightarrow \infty$.

By setting $R_n = d(x_0, u_nx_0) - l(n)$, we have

$$\mathbb{P}[(w_nx_0 \cdot u_n^{-1}x_0)_{x_0} \leq l(n)] = 1 - \mathbb{P}[w_nx_0 \in S_{x_0}(u_n^{-1}x_0, R_n)],$$

where the shadow $S_{x_0}(u_nx_0, R_n)$ has distance parameter $l(n)$. As w_n and u_n^{-1} are independent with distributions μ_n and $\check{\mu}_n$, respectively, we have that

$$\begin{aligned} \mathbb{P}[w_nx_0 \in S_{x_0}(u_n^{-1}x_0, R_n)] &= \sum_{g \in G} \mathbb{P}[w_nx_0 \in S_{x_0}(u_n^{-1}x_0, R_n) \mid u_n^{-1} = g] \cdot \check{\mu}_n(g) \\ &= \sum_{g \in G} \mu_n(S_{x_0}(gx_0, R_n)) \check{\mu}_n(g) \\ &\leq f(l(n)), \end{aligned}$$

where the last inequality uses the decay of shadows (Lemma 2.1). Since $f(l(n)) \rightarrow 0$ as $n \rightarrow \infty$, the lemma follows. \square

Lemma 3.4. *Let G be a countable group with a nonelementary action by isometries on a hyperbolic space X . Let μ be a nonelementary probability measure on G and fix $x_0 \in X$. Suppose that (w_n) is a random walk on G whose increments are distributed according to μ . Then*

$$\mathbb{P}[(w_nx_0 \cdot w_n^{-1}x_0)_{x_0} \leq l(n)] \rightarrow 1,$$

as $n \rightarrow \infty$. Here, $l : \mathbb{N} \rightarrow \mathbb{N}$ is any function with $l(n) \rightarrow \infty$ as $n \rightarrow \infty$ and $\limsup \frac{l(n)}{n} < \frac{L}{2}$, where L is the drift of (w_n) .

Proof. We follow the argument in [MT14]. For each n , let $m := \lfloor \frac{n}{2} \rfloor$, and we can write $w_n = w_m u_m$, with $u_m := w_m^{-1} w_n = g_{m+1} \dots g_n$. Note that the random walks w_m and u_m are independent, and u_m has distribution μ_{n-m} . We first claim that

$$\mathbb{P}[(w_nx_0 \cdot w_mx_0)_{x_0} \geq l(n)] \rightarrow 1 \quad \text{as } n \rightarrow \infty.$$

Proof of claim. Indeed,

$$\begin{aligned} \mathbb{P}[(w_n x_0 \cdot w_m x_0)_{x_0} \geq l(n)] &= \mathbb{P}[(u_m x_0 \cdot x_0)_{w_m^{-1} x_0} \geq l(n)] \\ &= \mathbb{P}[u_m x_0 \in S_{w_m^{-1} x_0}(x_0, R)] \end{aligned}$$

where $R := d(x_0, w_m^{-1} x_0) - l(n)$. Using Observation (1), we note that

$$(X \setminus S_{w_m^{-1} x_0}(x_0, R)) \subset S_{x_0}(w_m^{-1} x_0, R_n),$$

where $R_n = l(n) + C$, and C depends only on the hyperbolicity constant of X . This implies that

$$\mathbb{P}[(w_n x_0 \cdot w_m x_0)_{x_0} \geq l(n)] \geq 1 - \mathbb{P}[u_m x_0 \in S_{x_0}(w_m^{-1} x_0, R_n)].$$

Further, using independence of w_m and u_m , we see

$$\begin{aligned} \mathbb{P}[u_m x_0 \in S_{x_0}(w_m^{-1} x_0, R_n)] &= \sum_{g \in G} \mathbb{P}[u_m x_0 \in S_{x_0}(w_m^{-1} x_0, R_n) \mid w_m = g] \cdot \mu_m(g) \\ (5) \qquad \qquad \qquad &= \sum_{g \in G} \mu_{n-m}(S_{x_0}(g^{-1} x_0, R_n)) \mu_m(g). \end{aligned}$$

Let us now pick $\epsilon > 0$ such that $\limsup \frac{l(n) + \epsilon n}{n} < \frac{L}{2}$, where L is the drift of (w_n) ; then by considering in Equation (5) only the g such that $d(x_0, g^{-1} x_0) \geq l(n) + \epsilon n$, and using the estimate for the distance parameter of $S_{x_0}(g^{-1} x_0, R_n)$ we get

$$\mathbb{P}[u_m x_0 \in S_{x_0}(w_m^{-1} x_0, R_n)] \leq f(\epsilon n - C) + \mathbb{P}[d(x_0, w_m x_0) \leq l(n) + \epsilon n].$$

The first term tends to 0 by the decay of shadows (Lemma 2.1) and the second because of linear progress (Theorem 2.2). This proves the claim. \square

We return to the proof of Lemma 3.4. As in the proof of the claim, replacing w_n with w_n^{-1} and w_m with $w_n^{-1} w_m = u_m^{-1}$ it follows that

$$\mathbb{P}[(w_n^{-1} x_0 \cdot w_n^{-1} w_m x_0)_{x_0} \geq l(n)] \rightarrow 1 \quad \text{as } n \rightarrow \infty.$$

Then, by Lemma 3.4 (using that w_m and u_m are independent)

$$\mathbb{P}[(w_m x_0 \cdot w_n^{-1} w_m x_0)_{x_0} \leq l(n) - 3\delta] \rightarrow 1 \quad \text{as } n \rightarrow \infty.$$

Finally, by δ -hyperbolicity (Lemma 3.5 below),

$$\mathbb{P}[(w_n x_0 \cdot w_n^{-1} x_0)_{x_0} \leq l(n) + 2\delta] \rightarrow 1 \quad \text{as } n \rightarrow \infty.$$

This completes the proof. \square

The following lemma was used in the proof of Lemma 3.4. It appears as Lemma 5.9 in [MT14], but is proven here for convenience to the reader.

Lemma 3.5 (Fellow traveling is contagious). *Suppose that X is a δ -hyperbolic space with basepoint x_0 and suppose that $A \geq 0$. If $a, b, c, d \in X$ are points of X with $(a \cdot b)_{x_0} \geq A$, $(c \cdot d)_{x_0} \geq A$, and $(a \cdot c)_{x_0} \leq A - 3\delta$. Then $(b \cdot d)_{x_0} - 2\delta \leq (a \cdot c)_{x_0} \leq (b \cdot d)_{x_0} + 2\delta$.*

Proof. By hyperbolicity, $(a \cdot c)_{x_0} \geq \min\{(a \cdot b)_{x_0}, (b \cdot c)_{x_0}\} - \delta$. Since $(a \cdot c)_{x_0} \leq (a \cdot b)_{x_0} - 3\delta$, it must be that $(a \cdot c)_{x_0} \geq (b \cdot c)_{x_0} - \delta$. Exactly the same reasoning using the inequality $(a \cdot c)_{x_0} \geq \min\{(a \cdot d)_{x_0}, (d \cdot c)_{x_0}\} - \delta$ gives that $(a \cdot c)_{x_0} \geq (a \cdot d)_{x_0} - \delta$. Hence, $(a \cdot d)_{x_0} \leq (a \cdot c)_{x_0} + \delta \leq (a \cdot b)_{x_0} - 2\delta$.

Another application of hyperbolicity yields $(a \cdot d)_{x_0} \geq \min\{(a \cdot c)_{x_0}, (c \cdot d)_{x_0}\} - \delta = (a \cdot c)_{x_0} - \delta$. Combining these facts we have

$$\begin{aligned} (b \cdot d)_{x_0} &\geq \min\{(a \cdot b)_{x_0}, (a \cdot d)_{x_0}\} - \delta \\ &= (a \cdot d)_{x_0} - \delta \\ &\geq (a \cdot c)_{x_0} - 2\delta. \end{aligned}$$

To prove the reverse inequality, first note that the inequality $(a \cdot d)_{x_0} \leq (a \cdot b)_{x_0} - 2\delta$ obtained above implies that $(a \cdot d)_{x_0} \geq \min\{(a \cdot b)_{x_0}, (b \cdot d)_{x_0}\} - \delta = (b \cdot d)_{x_0} - \delta$. Then

$$\begin{aligned} (a \cdot c)_{x_0} &\geq \min\{(a \cdot d)_{x_0}, (d \cdot c)_{x_0}\} - \delta \\ &= (a \cdot d)_{x_0} - \delta \\ &\geq (b \cdot d)_{x_0} - 2\delta, \end{aligned}$$

as required. \square

We can now complete the proof of Theorem 1.2.

Proof of Theorem 1.2. Fix $x_0 \in X$ and set $\Gamma(n) = \langle w_n^1, \dots, w_n^k \rangle$. By Lemma 3.2, the probability that $\Gamma(n) \rightarrow X$ is a quasi-isometric embedding is bounded below by the probability that

$$(6) \quad d(x_0, w_n^i x_0) \geq 2((w_n^j)^{\pm 1} x_0 \cdot (w_n^l)^{\pm 1} x_0)_{x_0} + 18\delta + 1$$

for all choices of indices $1 \leq i, j, l \leq k$, excluding the cases that produce terms involving the Gromov product of a point with itself.

It is easily verified that the probability of (6) goes to 1 as $n \rightarrow \infty$. Indeed, by Theorem 2.2,

$$\mathbb{P}[d(x_0, w_n^i x_0) \geq Ln] \rightarrow 1$$

as $n \rightarrow \infty$, for each $1 \leq i \leq k$, where L is the drift of the random walks. Moreover, combining Lemma 3.3 and Lemma 3.4, we see that for $j \neq l$,

$$\mathbb{P}[(w_n^j)^{\pm 1} x_0 \cdot (w_n^l)^{\pm 1} x_0)_{x_0} \leq l(n)] \rightarrow 1$$

and for each $1 \leq j \leq k$,

$$\mathbb{P}[(w_n^j x_0 \cdot (w_n^j)^{-1} x_0)_{x_0} \leq l(n)] \rightarrow 1,$$

for any function $l(n)$ with $l(n) \rightarrow \infty$ as $n \rightarrow \infty$ and $\limsup \frac{l(n)}{n} \leq \frac{1}{2}L$. Additionally choosing $l(n)$ so that $2l(n) + 18\delta + 1 \leq Ln$ completes the proof. \square

REFERENCES

- [Aou11] Richard Aoun, *Random subgroups of linear groups are free*, Duke Mathematical Journal **160** (2011), no. 1, 117–173.
- [BH09] Martin R. Bridson and Andre Haefliger, *Metric spaces of non-positive curvature*, vol. 319, Springer, 2009.
- [Bir69] Joan S. Birman, *Mapping class groups and their relationship to braid groups*, Communications on Pure and Applied Mathematics **22** (1969), no. 2, 213–238.
- [Bow08] Brian H. Bowditch, *Tight geodesics in the curve complex*, Invent. Math. **171** (2008), no. 2, 281–300.
- [DKL12] Spencer Dowdall, Richard P. Kent, IV, and Christopher J. Leininger, *Pseudo-Anosov subgroups of fibered 3-manifold groups*, arXiv preprint arXiv:1208.2495 (2012).
- [DT14a] Spencer Dowdall and Samuel J. Taylor, *Hyperbolic extensions of free groups*, arXiv preprint arXiv:1406.2567 (2014).
- [DT14b] Matthew Gentry Durham and Samuel J. Taylor, *Convex cocompactness and stability in mapping class groups*, preprint (2014), arxiv:1404.4803.
- [FM02] Benson Farb and Lee Mosher, *Convex cocompact subgroups of mapping class groups*, Geom. Topol. **6** (2002), 91–152 (electronic). MR 1914566 (2003i:20069)
- [FM12] Benson Farb and Dan Margalit, *A primer on mapping class groups*, Princeton Mathematical Series, vol. 49, Princeton University Press, Princeton, NJ, 2012.
- [GdH90] Etienne Ghys and Pierre de la Harpe, *Sur les groupes hyperboliques d’apres mikhael gomov*, Birkhauser, 1990.
- [GMO10] Robert Gilman, Alexei Miasnikov, and Denis Osin, *Exponentially generic subsets of groups*, Illinois Journal of Mathematics **54** (2010), no. 1, 371–388.
- [Gro87] Mikhael Gromov, *Hyperbolic groups*, Springer, 1987.
- [Gui90] Yves Guivarc’h, *Produits de matrices aleatoires et applications aux proprietes geometriques des sous-groupes du groupe lineaire*, Ergodic Theory Dynam. Sys. **10** (1990), no. 03, 483–512.
- [Ham05] Ursula Hamenstädt, *Word hyperbolic extensions of surface groups*, arxiv:0807.4891v2, 2005.
- [KK13] Sang-hyun Kim and Thomas Koberda, *Embedability between right-angled Artin groups*, Geom. Topol. **17** (2013), no. 1, 493–530.
- [KL07] Richard P. Kent, IV and Christopher J. Leininger, *Subgroups of mapping class groups from the geometrical viewpoint*, In the tradition of Ahlfors-Bers. IV, Contemp. Math., vol. 432, Amer. Math. Soc., Providence, RI, 2007, pp. 119–141.
- [KL08] Richard P. Kent, IV and Christopher J. Leininger, *Shadows of mapping class groups: capturing convex cocompactness*, Geom. Funct. Anal. **18** (2008), no. 4, 1270–1325. MR 2465691 (2009j:20056)
- [KL09] Ilya Kapovich and Martin Lustig, *Geometric intersection number and analogues of the curve complex for free groups*, Geom. Topol. **13** (2009), no. 3, 1805–1833.
- [KMT14] Thomas Koberda, Johanna Mangahas, and Samuel J Taylor, *The geometry of purely loxodromic subgroups of right-angled Artin groups*, arXiv preprint arXiv:1412.3663 (2014).
- [Mah11] Joseph Maher, *Random walks on the mapping class group*, Duke Math. J. **156** (2011), no. 3, 429–468.
- [Mas75] Howard Masur, *On a class of geodesics in Teichmuller space*, Annals of Mathematics (1975), 205–221.
- [MM99] Howard A. Masur and Yair N. Minsky, *Geometry of the complex of curves. I. Hyperbolicity*, Invent. Math. **138** (1999), no. 1, 103–149.
- [MR] Brian Mann and Patrick Reynolds, In preparation.
- [MT13] Johanna Mangahas and Samuel J. Taylor, *Convex cocompactness in mapping class groups via quasiconvexity in right-angled Artin groups*, arXiv preprint arXiv:1306.5278 (2013).

- [MT14] Joseph Maher and Giulio Tiozzo, *Random walks on weakly hyperbolic groups*, arXiv preprint arXiv:1410.4173 (2014).
- [MU08] Alexei Myasnikov and Alexander Ushakov, *Random subgroups and analysis of the length-based and quotient attacks*, J. Math. Cryptol. **2** (2008), no. 1, 29–61.
- [MW94] Howard A Masur and Michael Wolf, *Teichmuller space is not Gromov hyperbolic*, Math. Sci. Res. Inst. preprint (1994), no. 011-94.
- [Riv08] Igor Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. **142** (2008), no. 2, 353–379.
- [Riv10] ———, *Zariski density and genericity*, International Mathematics Research Notices (2010), rnnq043.

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, 20 HILLHOUSE AVE, NEW HAVEN, CT 06520, USA

E-mail address: s.taylor@yale.edu

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, 20 HILLHOUSE AVE, NEW HAVEN, CT 06520, USA

E-mail address: giulio.tiozzo@yale.edu