PIVOTING TECHNIQUE FOR THE CIRCLE HOMEOMORPHISM GROUP

INHYEOK CHOI

Abstract. We adapt Gouëzel's pivoting technique to the circle homeomorphism group. As an application, we give different proofs of Gilabert Vio's probabilistic Tits alternative and Malicet's exponential decay.

Keywords.
MSC classes: 20F67, 30F60, 57K20, 57M60, 60G50

1. Introduction

In this paper, we study two consequences of the weak Tits alternative of Margulis' and Ghys' weak Tits alternative on $\mathrm{Homeo}(S^1)$. These consequences are concerned with random walks on $\mathrm{Homeo}(S^1)$, and were proven earlier by Martín Gilabert Vio and Dominque Malicet, respectively. Our purpose is to give a different approach that gives an additional quantitative bound. This quantitative bound is stable under perturbation of the underlying measure for the random walk.

We make an important remark. We say that a probability measure μ on $\mathrm{Homeo}(S^1)$ is *nondegenerate* if its support $\langle\langle \operatorname{supp}\mu \rangle\rangle$, the complement of the largest open subset of $\mathrm{Homeo}(S^1)$ that attains zero hitting measure, is a *subgroup* of G. By nature, $\langle\langle \operatorname{supp}\mu \rangle\rangle$ is indeed a subsemigroup, but is not always a subgroup. This requirement is needed to implement Margulis-Ghys weak Tits alternative on $\mathrm{Homeo}(S^1)$.

To begin with, we recall the following theorem recently proven by Martín Gilabert Vio:

Theorem 1.1 ([GV24, Theorem A])**.** *Let μ_1, μ_2 be nondegenerate probability measures on $\mathrm{Diff}^1_+(S^1)$ such that the actions of $G_1 = \langle\langle \operatorname{supp}\mu_1 \rangle\rangle$ and of $G_2 = \langle\langle \operatorname{supp}\mu_2 \rangle\rangle$ are proximal, and such that for every $i = 1, 2$, either*

(1) the support of μ_i is finite, or
(2) the support of μ_i is included in $\mathrm{Diff}^{1+\tau}_+(S^1)$ for some $\tau \in (0,1)$ and the integrals

$$\int_{G_i} \max\left\{|g|_{Lip}, |g^{-1}|_{Lip}\right\}^{\delta} d\mu(g), \int_{G_i} |\log g'|_{\tau}\, d\mu(g),$$

are finite for some $\delta > 0$.

Let $(Z_n)_{n>0}$ and $(Z'_n)_{n>0}$ be independent (left) random walks generated by μ_1 and μ_2, respectively. Then there exists $q \in (0,1)$ such that

$$\mathbb{P}\left(Z_n \text{ and } Z'_n \text{ comprise a ping-pong pair}\right) \geq 1 - q^n$$

for all $n \in \mathbb{Z}_{>0}$.

We have not defined a ping-pong pair, which will come shortly after. For now, it suffices to know that ping-pong pairs in $\mathrm{Homeo}(S^1)$ generates a free subgroup. As a consequence of this exponential bound, Gilabert Vio proved that independent random walks eventually generate free subgroups almost surely.

The above Theorem 1.1 is concerned with random diffeomorphisms in a subgroup with proximal action. A companion result for more general homeomorphisms is as follows.

Date: February 20, 2025.

Theorem 1.2 ([GV24, Theorem C]). *Let μ_1, μ_2 be nondegenerate probability measures on* $\mathrm{Homeo}^1_+(S^1)$ *such that the actions of $G_1 = \langle\langle \operatorname{supp} \mu_1 \rangle\rangle$ and of $G_2 = \langle\langle \operatorname{supp} \mu_2 \rangle\rangle$ do not admit invariant probability measure. Let $(Z_n)_{n>0}$ and $(Z'_n)_{n>0}$ be independent (left) random walks generated by μ_1 and μ_2, respectively. Then the following holds almost surely:*

$$\lim_{N\to\infty} |\{0 \le n \le N \mid Z_n \text{ and } Z'_n \text{ comprise a ping-pong pair}\}| = 1.$$

Our first result is that one can describe exponential genericity of ping-pong pairs for independent random walks on $\mathrm{Homeo}(S^1)$.

Theorem A. *Let μ_1 and μ_2 be nondegenerate probability measures on* $\mathrm{Homeo}(S^1)$ *such that the actions of $G_1 = \langle\langle \operatorname{supp} \mu_1 \rangle\rangle$ and of $G_2 = \langle\langle \operatorname{supp} \mu_2 \rangle\rangle$ do not admit invariant probability measure. Let $(Z_n)_{n>0}$ and $(Z'_n)_{n>0}$ be independent random walks generated by μ_1 and μ_2, respectively. Then the following holds almost surely: Then there exists $\kappa > 0$ such that*

$$\mathbb{P}\left(Z_n \text{ and } Z'_n \text{ comprise a ping-pong pair}\right) \ge 1 - \frac{1}{\kappa} e^{-\kappa n} \tag{1.1}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ is stable under perturbation in the following sense: there exist neighborhoods $\mathcal{U}_1$ of μ_1 and $\mathcal{U}_2$ of μ_2 in the space of probability measures on $\mathrm{Homeo}(S^1)$ *(in the weak-$*$ topology), respectively, so that Inequality 1.1 holds even if $(Z_n)_{n>0}$ is driven by an arbitrary measure in $\mathcal{U}_1$ and $(Z'_n)_{n>0}$ is driven by an arbitrary measure in $\mathcal{U}_2$.*

Let us now recall the exponential synchronizing proven by Dominique Malicet.

Theorem 1.3 ([Mal17, Theorem A]). *Let μ be a probability measure on* $\mathrm{Homeo}(S^1)$ *such that the action of $G = \langle\langle \operatorname{supp} \mu \rangle\rangle$ does not admit invariant probability measure. Let $(Z_n)_{n>0}$ be independent (left) random walks generated by μ. Then there exists $q \in (0,1)$ such that for each $x \in S^1$, for almost every random path $(Z_n(\omega))_{n>0}$, there exists a neighborhood $I_{x,\omega}$ of x such that*

$$\operatorname{diam}\left(Z_n(\omega)(I)\right) \le q^n$$

for all $n \in \mathbb{Z}_{>0}$.

Our second result strengthens this result by providing an exponential bound on the error event:

Theorem B. *Let μ be a nondegenerate probability measure on* $\mathrm{Homeo}(S^1)$ *such that the action of $G = \langle\langle \operatorname{supp} \mu \rangle\rangle$ does not admit invariant probability measure. Let $(Z_n)_{n>0}$ be independent (left) random walks generated by μ. Then there exists $\kappa > 0$ such that for each $x \in S^1$,*

$$\mathbb{P}\left(\omega : \begin{array}{c}\text{there exists a neighborhood } I_{x,\omega} \text{ of } x \text{ such that} \\ \operatorname{diam}\left(Z_k(\omega)(I_{x,\omega})\right) \le q^k \text{ for } k \ge n\end{array}\right) \ge 1 - \frac{1}{\kappa} e^{-\kappa n} \tag{1.2}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ is stable under perturbation. That means, there exists a neighborhood $\mathcal{U}$ of μ in the space of probability measures on $\mathrm{Homeo}(S^1)$ *(in the weak-$*$ topology) so that Inequality 1.2 holds (for the same uniform $\kappa > 0$) even if $(Z_n)_{n>0}$ is driven by an arbitrary measure in $\mathcal{U}$.*

This theorem follows from the special case where the action of G is proximal. In such a case, one can give more description about $I_{x,\omega}$:

Theorem C. *Let μ be a nondegenerate probability measure on* $\mathrm{Homeo}(S^1)$ *such that the action of $G = \langle\langle \operatorname{supp} \mu \rangle\rangle$ is proximal. Let $(Z_n)_{n>0}$ be the (left) random walk generated by μ. Then there exists $\kappa > 0$ such that for each $x \in S^1$,*

$$\mathbb{P}\left(\omega : \begin{array}{c}\text{there exists a neighborhood } I_{x,\omega} \text{ of } x \text{ such that} \\ \operatorname{diam}(I_{x,\omega}) \ge 1 - q^n \text{ and } \operatorname{diam}\left(Z_k(\omega)(I_{x,\omega})\right) \le q^k \text{ for } k \ge n\end{array}\right) \ge 1 - \frac{1}{\kappa} e^{-\kappa n} \tag{1.3}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ *is stable under perturbation. That means, there exists a neighborhood* $\mathcal{U}$ *of* μ *in the space of probability measures on* $\mathrm{Homeo}(S^1)$ *(in the weak-* topology) so that Inequality 1.2 holds (for the same uniform* $\kappa > 0$*) even if* $(Z_n)_{n>0}$ *is driven by an arbitrary measure in* $\mathcal{U}$.

Remark 1.4. *In Theorem B and C, it is important that the choice of* $I_{x,\omega}$ depends on $I_{x,\omega}$. *It is easy to construct a random walk (say, a nearest-neighbor random walk on a surface group acting on* $S^1 = \partial\mathbb{H}^2$*) such that for any nonempty open set* O*, there exists* $\epsilon > 0$ *such that*

$$\mathbb{P}\left(\operatorname{diam}(Z_n \cdot O) > 1/2\right) > \epsilon$$

for each $n \in \mathbb{Z}_{>0}$.

The statements in Theorem A, B, C still hold even if the the step distributions for the random walk are independent but non-identical, as long as they are distributed according to measures chosen from $\mathcal{U}$ or $\mathcal{U}_1$ and $\mathcal{U}_2$, respectively.

We finally observe one another result for proximal actions.

Theorem D. *Let* μ *be a nondegenerate probability measure on* $\mathrm{Homeo}(S^1)$ *such that the action of* $G = \langle\langle \operatorname{supp}\mu \rangle\rangle$ *is proximal. Let* $(Z_n)_{n>0}$ *be the random walk generated by* μ. *Then there exists* $\kappa > 0$ *such that for each* $x, y \in S^1$,

$$\mathbb{P}_{Z_n \sim \mu^{*n}}\left(d(Z_n x, Z_n y) < e^{-\kappa n}\right) \geq 1 - \frac{1}{\kappa} e^{-\kappa n} \tag{1.4}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ *is stable under perturbation. That means, there exists a neighborhood* $\mathcal{U}$ *of* μ *in the space of probability measures on* $\mathrm{Homeo}(S^1)$ *(in the weak-* topology) so that Inequality 1.2 holds (for the same uniform* $\kappa > 0$*) even if* $(Z_n)_{n>0}$ *is driven by an arbitrary measure in* $\mathcal{U}$.

In Theorem A or D, it is not important if the random walk is a right random walk or left random walk. Indeed, the estimate is a snapshot at step n. In Antonov's work and Malicet's work [Mal17], the authors mainly discussed exponential synchronization for left random walk.

Our results are purely for homeomorphism groups. The only property of the group element that we use is the following: If I and J are nested intervals of S^1, their images are also nested.

Our method is based on Gouëzel's pivoting technique, which is first introduced in [Gou22] and led to a remarkable exponential estimate for random walks on Gromov hyperbolic spaces. There has been several attempts to generalize Gouëzel's technique to a broader setting, and this paper is in line with those efforts. We use Schottky dynamics exhibited by Schottky pairs of homeomorphisms to implement Gouëzel's pivoting time construction. It turns out that the 1-dimensionality of the ambient space is somehow crucial, but the more crucial thing is the nesting of the Schottky regions. For instance, the particular choice of Lebesgue measure (when measuring the diameter of intervals) is not important; we have:

Theorem 1.5. *The statement in Theorem B and C hold even if the diameter* $\operatorname{diam}(\cdot)$ *is replaced with* $\nu(\cdot)$ *for an arbitrary probability measure* ν *on* S^1.

So above, ν need not be absolutely continuous with respect to Leb, but could be e.g., a measure concentrated on a Cantor set or as such.

For brevity, we will only prove Theorem A for proximal actions, and Theorem C and D. The general case follows from Margulis' and Ghys' weak Tits alternative (see Remark 2.6).

2. Schottky sets and random walks

Throughout, we fix the circle S^1. We begin with the definition of Schottky pairs and Schottky sets.

Definition 2.1. *Let f be a circle homoemorphism and let U_1, U_2 be disjoint subsets of S^1. If*

$$f\big(S^1 \setminus U_1\big) \subseteq U_2,\ f\big(S^1 \setminus U_2\big) \subseteq U_1$$

*holds, we say that f is a (U_1, U_2)-*hyperbolic map*. We denote the collection of (U_1, U_2)-hyperbolic maps by $\mathfrak{S}(U_1, U_2)$.*

If U_1, U_2 are open sets (closed sets, resp.), then $\mathfrak{S}(U_1, U_2)$ is also open (closed, reps.) with respect to the C^0-topology.

Definition 2.2. *For disjoint closed intervals $I_1, \dots, I_N, J_1, \dots, J_N$ of S^1, we call $S := \mathfrak{S}(I_1, J_1) \cup \dots \cup \mathfrak{S}(I_N, J_N) \subseteq \mathrm{Homeo}(S^1)$ the* Schottky set *associated to $I_1, \dots, I_N, J_1, \dots, J_N$. We call the number N the* resolution *of S. For each $s \in S$ there exist unique i such that $s \in \mathfrak{S}(I_i, J_i)$; for such an i, we write $I(s) := I_i$ and $J(s) := J_i$.*

If there is an interval $\mathcal{I}$ such that $I_1 \cup \dots \cup I_N \subseteq \mathrm{int}(S^1 \setminus \mathcal{I})$ and $J_1 \cup \dots \cup J_N \subseteq \mathrm{int}\,\mathcal{I}$, we call $\mathcal{I}$ a median *for S.*

Let $\epsilon > 0$ and let S be a Schottky set associated with disjoint closed intervals $I_1, \dots, I_N, J_1, \dots, J_N$. If a (Borel) measure μ on $\mathrm{Homeo}(S^1)$ satisfies

$$\mu\big(\mathfrak{S}(I_i, J_i)\big) > \epsilon/N \text{ for each } i = 1, \dots, N,$$

*then we say that μ is a (S, ϵ)-*admissible measure*; if μ satisfies*

$$\mu\big(\mathfrak{S}(I_i, J_i)\big) = 1/N \text{ for each } i = 1, \dots, N,$$

then we say that $\mu$is Schottky-uniform *on S.*

Note that there are several Schottky-uniform measures on a single Schottky set (because $\mathfrak{S}(I, J)$ is not a singleton for most I and J).

For disjoint I, J, I', J' and elements $f \in \mathfrak{S}(I, J)$ and $g \in \mathfrak{S}(I', J')$, we say that (f, g) is a *Schottky pair*. We now recall the seminal result, asked by Ghys and first proved by Margulis. We follow Ghys' reformulation.

Theorem 2.3 ([Mar00], [Ghy01])**.** *Let G be any subgroup of $\mathrm{Homeo}(S^1)$. Then exactly one of the following holds:*

1. *There exists a probability measure on S^1 preserved by each element of G;*
2. *Up to semiconjugacy and finite-degree covering, G admits a Schottky pair. That means, there exists a monotone degree-1 map $c : S^1 \to S^!$ and a finite covering map $\pi : S^1 \to S^1$, together with a homomorphism $\rho : G \to \rho(G) \leq \mathrm{Homeo}(S^1)$ such that*

$$\pi \circ c \circ g = \rho(g) \circ \pi \circ c$$

holds, and such that there exist two elements $f, g \in \rho(G)$ that comprise a Schottky pair.

Furthermore, when the action of G is assumed to be proximal *(i.e., $\inf_{g \in G} d(gx, gy) = 0$ for every $x, y \in S^1$), then (2) must hold, in fact without passing through semiconjugacy and covering map.*

Remark 2.4. *In* [Ghy01]*, the theorem is stated for $\mathrm{Homeo}^+(S^1)$, the group of orientation-preserving circle homeomorphims. But it is not hard to lift this restriction.*

Meanwhile, at least to the best of the author's knowledge, the restriction that G is a subgroup (rather than subsemigroup) is serious.

So an immediate consequence is:

Corollary 2.5. *Let μ be a probability measure on* $\mathrm{Homeo}(S^1)$ *such that the semigroup $\langle\langle \operatorname{supp}\mu \rangle\rangle$ generated by the support of μ contains a subgroup of* $\mathrm{Homeo}(S^1)$ *whose action is proximal. Then there exists N such that* $\operatorname{supp}\mu^{*N}$ *contains a (interval) Schottky pair.*

Remark 2.6. *In the sequel, we will always assume that the probability measure μ generating the random walk is non-degenerate on a proximal subgroup. For general case, we consider the push-forward random walk on $\rho(G)$, which acts on S^1 and admits an (interval) Schottky pair. Here, on S^1 we endow the pushforward measure $(\pi\circ c)^*\mathrm{Leb}$ of the Lebesgue measure by $\pi\circ c$. Once the exponential synchronization is proven downstairs with resepct to $(\pi\circ c)^*\mathrm{Leb}$, one can recover the exponential synchronization upstairs with* Leb.

It is not hard to "amplify" a Schottky pair into larger Schottky set.

Lemma 2.7. *Let μ be a probability measure on* $\mathrm{Homeo}(S^1)$ *such that* $\operatorname{supp}\mu$ *contains a Schottky pair. Then for each $N\in\mathbb{Z}_{>0}$, there exists $\epsilon>0$, $m\in\mathbb{Z}_{>0}$ and a Schottky set S with median whose resolution is N and such that μ^{*m} is an (S,ϵ)-admissible measure.*

Proof. Let (f_1,f_2) be a Schottky pair in $\operatorname{supp}\mu$. Then there exists disjoint closed intervals I_1,I_2,J_1,J_2 on S^1 such that $f_i\in\mathfrak{S}(I_i,J_i)$ for each i.

If there exists an interval $\mathcal{I}$ such that $I_1\cup I_2\subseteq\mathcal{I}$ and $J_1\cup J_2\subseteq S^1\setminus\mathcal{I}$, we just record it. If there exists no such $\mathcal{I}$, it means that I_1,J_1,I_2,J_2 are arranged clockwise or counterclockwise along S^1. In either case, we can take an interval $\mathcal{I}$ that contains J_2 but does not intersect with I_1,J_1 and I_2. This $\mathcal{I}$ is not a median for (f_1,f_2) but is a median for $\{f_2^2,f_2f_1\}$. Indeed, for

$$f_1':=f_2f_1,\ f_2':=f_2^2,\ I_1':=I_1,\ J_1':=f_2J_1,\ I_2':=I_2,\ J_2':=f_2J_2,$$

we observe $f_i(S^1\setminus I_i')\subseteq J_i', f_i^{-1}(S^1\setminus J_i')\subseteq I_i'$ and

$$J_1'\cap J_2'=f_2(J_1\cap J_2)=\emptyset,\ (I_1'\cup I_2')\cap(J_1'\cup J_2')\subseteq(I_1\cup I_2)\cap f_2(S^1\setminus I_2)\subseteq(I_1\cup I_2)\cap J_2=\emptyset.$$

Furthermore, $\mathcal{I}$ does not intersect with I_1 and I_2 but its interior contains $\int J_2$, which in turn contains J_1' and J_2'. Hence, $\mathcal{I}$ is a median for $\{f_1',f_2'\}$. Note that $f_1',f_2'\in\operatorname{supp}\mu^{*2}$.

Thanks to the argument above, up to replacing μ with μ^{*2}, we can assume that the Schottky pair (f_1,f_2) taken in $\operatorname{supp}\mu$ has a median $\mathcal{I}$. Now we will label some 2^N homeomorphisms with elements of $\{1,2\}^N$. Given $\sigma\in\{1,2\}^N$, we construct

$$f_\sigma:=f_{\sigma(1)}f_{\sigma(2)}\cdots f_{\sigma(N)},\ I_\sigma:=f_\sigma^{-1}\left(\overline{S^1\setminus\mathcal{I}}\right),\ J_\sigma:=f_\sigma\mathcal{I}.$$

Note that f_σ^2 sends $S^1\setminus I_\sigma$ into J_σ and f_σ^{-2} sends $S^1\setminus J_\sigma$ into I_σ. Furthermore, we observe

$$\begin{aligned}J_\sigma&=f_{\sigma(1)}\cdots f_{\sigma(N)}\mathcal{I}=f_{\sigma(1)}\cdots f_{\sigma(N-1)}J_{\sigma(N)}\\&\subseteq f_{\sigma(1)}\cdots f_{\sigma(N-1)}\mathcal{I}=f_{\sigma(1)}\cdots f_{\sigma(N-2)}J_{\sigma(N-1)}\\&\subseteq\ldots\subseteq J_{\sigma(1)}\subseteq\operatorname{int}\mathcal{I}.\end{aligned}$$

For a similar reason we have $I_\sigma\subseteq\operatorname{int}(S^1\setminus\mathcal{I})$. In short, I_σ and $J_{\sigma'}$ does not overlap with each other for any $\sigma,\sigma'\in\{1,2\}^N$. Now let us take distinct elements σ and σ' of $\{1,2\}^N$. Then there exists i such that $\sigma(i)\neq\sigma'(i)$, and we take a minimal one. Then

$$J_\sigma\subseteq f_{\sigma(1)}\cdots f_{\sigma(i-1)}J_{\sigma(i)},\ J_{\sigma'}\subseteq f_{\sigma'(1)}\cdots f_{\sigma'(i-1)}J_{\sigma'(i)}$$

should not intersect. For a similar reason, I_σ and $I_{\sigma'}$ are disjoint. To sum up, the $2\cdot2^N$ intervals $\{I_\sigma,J_\sigma:\sigma\in\{1,2\}^N\}$ are all pairwise disjoint. It is clear that $(\operatorname{supp}\mu^{*N})$ intersects with each of $\mathcal{S}(I_\sigma,J_\sigma)$. Furthermore, $\mathcal{I}$ works as a median: $\cup_\sigma I_\sigma\subseteq\operatorname{int}\mathcal{I}$ and $\cup_\sigma J_\sigma\subseteq\operatorname{int}(S^1\setminus\mathcal{I})$ hold.

It is now time to enlarge I_σ,J_σ slightly so that they remain disjoint. That means, we can find pairwise disjoint closed intervals $\{I_\sigma',J_\sigma':\sigma\in\{1,2\}^N\}$ such that $I_\sigma\subseteq\operatorname{int}I_\sigma'$, $J_\sigma\subseteq\operatorname{int}J_\sigma'$ hold. It is also not hard to retain the property that $\cup_\sigma I_\sigma'\subseteq\operatorname{int}(S\setminus\mathcal{I})$ and $\cup_\sigma J_\sigma'\subseteq\operatorname{int}\mathcal{I}$.

The reason for the enlargement is as follows: for each $\sigma \in \{1,2\}^N$, $\mathcal{S}(\operatorname{int} I_\sigma, \operatorname{int} J_\sigma)$ is an *open* subset (of $\mathrm{Homeo}(S^1)$) that intersects with $\operatorname{supp} \mu^{*N}$, so attains strictly positive μ^{*N}-value. This implies that $S = \{\mathcal{S}(I'_\sigma, J_{\sigma'}) : \sigma \in \{1,2\}^N\}$ is a Schottky set with median $\mathcal{I}$, whose resolution is $2^N \geq N$, and such that μ^{*N} is (S,ϵ)-admissible for some $\epsilon > 0$. □

2.1. **Exponential Synchronization.** We now present a central proposition that follows from pivoting technique. We postpone its proof to the next section.

Proposition 2.8. *For each $\epsilon > 0$, $m \in \mathbb{Z}_{>0}$ and $N \in \mathbb{Z}_{>2500}$, there exists $\kappa = \kappa(\epsilon, m, N) > 0$ that satisfies the following.*

Let S be a Schottky set with median $\mathcal{I}$ and with resolution N. Let μ be a probability measure μ such that μ^{*m} is an (S,ϵ)-admissible measure.

Then for each $n \in \mathbb{Z}_{>0}$, there exists a probability space Ω_n, a measurable subset $A_n \subseteq \Omega_n$, a measurable partition $\mathcal{P}_n = \{\mathcal{E}_\alpha\}_\alpha$ of the set A_n, and $\mathrm{Homeo}(S^1)$-valued random variables

$$Z_n, \{w_i\}_{i=0,\dots,\lfloor \kappa n \rfloor}, \{s_i\}_{i=1,\dots,\lfloor \kappa n \rfloor}$$

such that the following holds:

(1) $\mathbb{P}(A_n) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}$.
(2) Restricted on each equivalence $\mathcal{E} \in \mathcal{P}_n$, $\mathcal{E}$ $w_0, \dots, w_{\lfloor \kappa n \rfloor}$ are constant *homeomorphisms and s_i are independently distributed according to a Schottky-uniform measures on S.*
(3) On A_n, $w_i \mathcal{I} \subseteq \mathcal{I}$ holds for each $i = 1, \dots, \lfloor \kappa n \rfloor - 1$.
(4) Z_n is distributed according to μ^{*n} and $Z_n = w_0 s_1 w_1 \cdots s_{\lfloor \kappa n \rfloor} w_{\lfloor \kappa n \rfloor}$ holds on A_n.

Assuming this proposition, we can now prove the exponential synchronization. Below is the first ingredient towards that. *From now on, we fix a measure* Len *on S^1. For the purpose of Theorem A, C, D, these can be taken as the Lebesgue measure. For Theorem 1.5, one can plug in an arbitrary measure.*

Lemma 2.9. *Let $w \in \mathrm{Homeo}(S^1)$, let S be a Schottky set with median $\mathcal{I}$ and with resolution N, and let μ be a Schottky-uniform measure on S. Then we have*

$$\mathbb{P}_{s\sim\mu}\left(\operatorname{Len}(ws\mathcal{I}) \leq \frac{1}{\sqrt{N}} \operatorname{Len}(w\mathcal{I})\right) \geq 1 - \frac{1}{\sqrt{N}}.$$

Proof. First, let us write $S = \mathfrak{S}(I_1, J_1) \cup \dots \cup \mathfrak{S}(I_N, J_N)$ for some disjoint closed intervals $I_1, \dots, I_N, J_1, \dots, J_N$. Recall that each element of $\mathfrak{S}(I_i, J_i)$ sends $\mathcal{I}$ into J_i. $(*)$ Note that $wJ_1, \dots, w_{J_N}$ are disjointly contained in $w\mathcal{I}$. Hence, the sum of their "lengths" is no greater than that of $\mathcal{I}$, which implies that

$$Ind := \left\{ i : \operatorname{Len}(wJ_i) \geq \frac{1}{\sqrt{N}} \operatorname{Len}(w\mathcal{I}) \right\}$$

has at most $\sqrt{N}$ elements. For each $i \notin Ind$, $(*)$ tells us that $\operatorname{Len}(ws\mathcal{I}) \leq \frac{1}{\sqrt{N}} \operatorname{Len}(w\mathcal{I})$ for each $s \in \mathfrak{S}(I_i, J_i)$. Summing up, we observe

$$\begin{aligned}\mathbb{P}_{s\sim\mu}\left(\operatorname{Len}(ws\mathcal{I}) \leq \frac{1}{\sqrt{N}} \operatorname{Len}(w\mathcal{I})\right) &\geq \mathbb{P}_{s\sim\mu}\left(s \in \mathfrak{S}(I_i, J_i) : i \notin Ind\right) \\ &\geq \frac{1}{N}(N - \sqrt{N}) = 1 - \frac{1}{\sqrt{N}}.\end{aligned}$$

□

Lemma 2.10. *Let S be a Schottky set with median $\mathcal{I}$ and with resolution $N \geq 100$. Fix homeomorphisms $w_0, \dots, w_n \in \mathrm{Homeo}(S^1)$ that satisfy $w_i \mathcal{I} \subseteq \mathcal{I}$ for $i = 1, \dots, n$. Then for random variables*

$s_1, \dots, s_n$ independently distributed according to Schottky-uniform measures on S, we have

$$\mathbb{P}\left(\mathrm{Len}\left(w_0 s_1 w_1 \cdots s_n w_n \cdot \mathcal{I}\right) \leq \frac{1}{N^{n/4}} \mathrm{Len}\left(w_0 \mathcal{I}\right)\right) \geq 1 - e^{-n/4}.$$

Proof. Again, we start by writing $S = \mathfrak{S}(I_1, J_1) \cup \ldots \cup \mathfrak{S}(I_N, J_N)$. Note that for each i, each element s of $\mathfrak{S}(I_i, J_i)$ sends $\mathcal{I}$ into J_i and satisfies $s\mathcal{I} \subseteq \mathcal{I}$. In other words, the inclusion

$$W_0\mathcal{I} \supseteq W_0 s_1 \mathcal{I} \supseteq W_1 \mathcal{I} \supseteq W_1 s_1 \mathcal{I} \supseteq \ldots \supseteq W_n \mathcal{I} \quad \left(W_k = W_k(s_0, \dots, s_k) := w_0 s_1 w_1 \dots s_k w_k\right)$$

holds regardless of the values of s_i's.

Now fixing $0 \leq k \leq n-1$ and the choices of $\{s_i : 1 \leq i \leq k\}$, we observe that

$$\mathbb{P}_{s_{k+1} \sim \text{Schottky-uniform on } S}\left(\mathrm{Len}(W_k s_{k+1} \mathcal{I}) \leq \frac{1}{\sqrt{N}} \mathrm{Len}(W_k \mathcal{I})\right) \geq 1 - \frac{1}{\sqrt{N}}$$

thanks to Lemma 2.9. In other words, for

$$E_k := \left\{(s_1, \dots, s_k) : \mathrm{Len}(W_{k-1} s_k \mathcal{I}) \leq \frac{1}{\sqrt{N}} \mathrm{Len}(W_{k-1} \mathcal{I})\right\},$$

we have $\mathbb{P}(E_{k+1} | s_1, \dots, s_k) \geq 1 - 1/\sqrt{N}$ regardless of the values of $s_1, \dots, s_k$. Summing up these conditional probabilities, we obtain

$$\mathbb{P}\left(\sum_{k=1}^{n} 1_{E_k} \geq n/2\right) \geq \mathbb{P}\left(B(n, 1 - 1/\sqrt{N}) \geq n/2\right). \tag{2.1}$$

Here, $B(n, 1-1/\sqrt{N})$ denotes the binomial random variable, the sum of N independent Bernoulli random variables with expectation $1 - 1/\sqrt{N}$. We use Markov's inequality to estimate the latter:

$$e^{-n/2} \cdot \mathbb{P}\left(B(n, 1-1/\sqrt{N}) \leq n/2\right) \leq \mathbb{E}\left[e^{-B(n, 1-1/\sqrt{N})}\right] \leq \left(\frac{1}{\sqrt{N}} + e^{-1}\right)^n.$$

Here, the assumption $\sqrt{N} \geq 10$ implies $1/\sqrt{N} + e^{-1} \leq e^{-3/4}$. This leads to the estimate $\mathbb{P}\left(B(n, 1-1/\sqrt{N}) \leq n/2\right) \leq e^{-n/4}$. Combining this with Inequality 2.1, we can conclude the proof. □

We have another analogous computations.

Lemma 2.11. *Let $x, y \in S^1$, let $w \in \mathrm{Homeo}(S^1)$, let S be a Schottky set with median $\mathcal{I}$ and with resolution N, and let μ be a Schottky-uniform measure on S. Then we have*

$$\mathbb{P}_{s \sim \mu}\left(\{x, y\} \cap s\mathcal{I} = \emptyset\right) \geq 1 - 2/N$$

Proof. Let $S = \mathfrak{S}(I_1, J_1) \cup \ldots \cup \mathfrak{S}(I_N, J_N)$. Then for each i, every element of $\mathfrak{S}(I_i, J_i) \in S$ sends $\mathcal{I}$ into J_i. Since $J_1, \dots, J_N$ are disjoint, $Ind := \{i : \{x, y\} \cap J_i \neq \emptyset\}$ has cardinality at most 2. This implies

$$\mathbb{P}_{s \sim \mu}\left(\{x, y\} \cap I = \emptyset\right) \geq \mathbb{P}_{s \sim \mu}\left(s \in \mathfrak{S}(I_i, J_i) : i \notin Ind\right) \geq \frac{1}{N}(N-2).$$

□

Lemma 2.12. *Let $x, y \in S^1$, let $w \in \mathrm{Homeo}(S^1)$ and let S be a Schottky set with median $\mathcal{I}$ and with resolution $N \geq 6$. Fix homeomorphisms $w_0, \dots, w_n \in \mathrm{Homeo}(S^1)$ such that $w_i \mathcal{I} \subseteq \mathcal{I}$ for $i = 1, \dots, n$. Then for random variables $s_1, \dots, s_n$ independently distributed according to Schottky-uniform measures on S, we have*

$$\mathbb{P}\left(\{x, y\} \cap w_0 s_1 w_1 \cdots s_n w_n \mathcal{I} = \emptyset\right) \geq 1 - e^{-n}$$

Proof. As in the proof of Lemma 2.10,

$$W_0 I \supseteq W_0 s_1 \mathcal{I} \supseteq W_1 \mathcal{I} \supseteq W_1 s_1 \mathcal{I} \supseteq \ldots \supseteq W_n \mathcal{I} \quad \left(W_k = W_k(s_0, \ldots, s_k) := w_0 s_1 w_1 \ldots s_k w_k\right)$$

holds regardless of the choices of s_i's. Furthermore, when $0 \leq k \leq n-1$ and $\{s_i : 1 \leq i \leq k\}$ are given,

$$\mathbb{P}_{s_{k+1} \sim \text{Schottky-uniform on } S}\left(s_{k+1}\mathcal{I} \cap \{W_k^{-1}x, W_k^{-1}y\} = \emptyset\right) \geq 1 - 2/N$$

holds by Lemma 2.11. In other words, if we define

$$E_k := \left\{(s_1, \ldots, s_k) : \{x, y\} \cap W_{k-1} s_k \mathcal{I} = \emptyset\right\},$$

then we have $\mathbb{P}(E_{k+1}|s_1, \ldots, s_k) \geq 1 - 2/N$ for every choices of $s_1, \ldots, s_k$. This leads to

$$\mathbb{P}\left(\{x, y\} \cap W_n \mathcal{I} = \emptyset\right) \geq \mathbb{P}\left(E_1 \cup \ldots \cup E_n\right) \geq 1 - (2/N)^n \geq 1 - e^{-n}.$$

□

We can interpret the above lemma in the following way. Let $S = \cup_i \mathfrak{S}(I_i, J_i)$ be a Schottky set with median $\mathcal{I}$ and with resolution $N \geq 6$. Then $\check{S} := \cup_i \mathfrak{S}(J_i, I_i)$ becomes another Schottky set with median $S^1 \setminus \mathcal{I}$. Now, given a Schottky-uniform measure μ on S, the measure $\check{\mu}$ defined by $\check{\mu}(\cdot) := \mu(\cdot^{-1})$ becomes a Schottky-uniform measure on $\check{S}$. Finally, consider some homeomorphisms $w_0, \ldots, w_n$ that satisfy the following equivalent condition:

$$w_i \mathcal{I} \subseteq \mathcal{I} \text{ for } i = 0, \ldots, n-1 \Leftrightarrow w_i^{-1}(S^1 \setminus \mathcal{I}) \subseteq (S^1 \setminus \mathcal{I}) \text{ for } i = 0, \ldots, n-1.$$

Now by applying Lemma 2.12, we observe for arbitrary $x, y \in S^1$ that

$$\mathbb{P}_{s_i^{-1} \text{ independently Schottky-uniform on } \check{S}}\left(\{x, y\} \cap w_n^{-1} s_n^{-1} w_{n-1}^{-1} \cdots s_1^{-1} w_0^{-1}(S^1 \setminus \mathcal{I}) = \emptyset\right) \geq 1 - e^{-n}.$$

Equivalently, we can say

$$\mathbb{P}_{s_i \text{ independently Schottky-uniform on } S}\left(w_0 s_1 w_1 \cdots s_n w_n \cdot \{x, y\} \subseteq \mathcal{I}\right) \geq 1 - e^{-n}.$$

We record this as a separate lemma:

Lemma 2.13. *Let $x, y \in S^1$, let $w \in \text{Homeo}(S^1)$ and let S be a Schottky set with median $\mathcal{I}$ and with resolution $N \geq 6$. Fix homeomorphisms $w_0, \ldots, w_n \in \text{Homeo}(S^1)$ such that $w_i \mathcal{I} \subseteq \mathcal{I}$ for $i = 0, \ldots, n-1$. Then for random variables $s_1, \ldots, s_n$ independently distributed according to Schottky-uniform measures on S, we have*

$$\mathbb{P}\left(w_0 s_1 w_1 \cdots s_n w_n \cdot \{x, y\} \subseteq \mathcal{I}\right) \geq 1 - e^{-n}.$$

We can now prove Theorem D.

Theorem 2.14. *For each $\epsilon > 0$, $m \in \mathbb{Z}_{>0}$ and $N \in \mathbb{Z}_{>2500}$, there exists $\kappa_1 = \kappa_1(\epsilon, m, N) > 0$ such that the following holds.*

Let S be a Schottky set with median $\mathcal{I}$ and with resolution N and let μ be a probability measure such that μ^{*m} is (S, ϵ)-admissible. Then for everyx, $y \in S^1$ and for every $n \in \mathbb{Z}_{>0}$ we have

$$\mathbb{P}_{Z_n \sim \mu^{*n}}\left(d(Z_n x, Z_n y) \leq e^{-\kappa_1 n}\right) \geq 1 - \frac{1}{\kappa_1} e^{-\kappa_1 n}.$$

Proof. Let $\kappa = \kappa(\epsilon, m, N)$ be as in Proposition 2.8. Next, given a positive integer n, we fix the probability space Ω_n, the measurable subset A_n, the measurable partition $\mathcal{P}_n = \{\mathcal{E}_\alpha\}_\alpha$ of A_n and the random variables Z_n, $w_0, \ldots, w_{\lfloor \kappa n \rfloor}, s_1, \ldots, s_{\lfloor \kappa n \rfloor}$ as in Proposition 2.8.

Let $\mathcal{E} \in \mathcal{P}_n$ be an arbitrary equivalence class. Restricted on $\mathcal{E}$, $w_0, \ldots, w_{\lfloor \kappa n \rfloor}$ are constant homeomorphisms and $s_1, \ldots, s_{\lfloor \kappa n \rfloor}$ are independently distributed according to Schottky-uniform measures on S. Furthermore, each of $w_1, \ldots, w_{\lfloor \kappa n \rfloor}$ satisfy $w_i \mathcal{I} \subseteq \mathcal{I}$. This enables us to apply Lemma 2.10 and 2.13.

For convenience, let us define $w_0' := w_0 s_1 w_1 \cdots s_{\lfloor 0.5\kappa n\rfloor} w_{\lfloor 0.5\kappa n\rfloor}$. This map depends on the choices of $s_1, \dots, s_{\lfloor 0.5\kappa n\rfloor}$. By Lemma 2.10, we have

$$\mathbb{P}\left(\mathrm{Len}(w_0'\mathcal{I} = w_0 s_1 w_1 \cdots s_{\lfloor 0.5\kappa n\rfloor} w_{\lfloor 0.5\kappa n\rfloor} \cdot \mathcal{I}) \le \frac{1}{N^{\lfloor \kappa n\rfloor/8}} \cdot 1 \,\middle|\, \mathcal{E}\right) \ge 1 - e^{-n/4}.$$

The event depicted here does not depend on $s_{\lfloor 0.5\kappa n\rfloor+1}, \dots, s_{\lfloor \kappa n\rfloor}$ whatsoever. Moreover, by Lemma 2.13, we observe the following regardless of the nature of w_0':

$$\mathbb{P}\left(w_0' s_{\lfloor 0.5\kappa n\rfloor+1} w_{\lfloor 0.5\kappa n\rfloor+1} \cdots s_{\lfloor \kappa n\rfloor} w_{\lfloor \kappa n\rfloor} \cdot \{x, y\} \subseteq w_0'\mathcal{I} \,\middle|\, \mathcal{E}, w_0'\right) \ge 1 - e^{-n}.$$

Combined together, we have

$$\mathbb{P}\left(d(Z_n x, Z_n y) \le \mathrm{Len}(w_0' \cdot \mathcal{I}) \le \frac{1}{N^{\lfloor \kappa n\rfloor/8}} \,\middle|\, \mathcal{E}\right) \ge (1 - e^{-n/4})(1 - e^{-n}) \ge 1 - 2 \cdot e^{-n/4}.$$

Since we observe this lower bound on each of $\mathcal{E} \in \mathcal{P}_n$, we can sum up the conditional probability to deduce

$$\begin{aligned}
\mathbb{P}\left(d(Z_n x, Z_n y) \le N^{-\lfloor \kappa n\rfloor/8}\right) &\ge \sum_{\mathcal{E}\in\mathcal{P}_n} \mathbb{P}(\mathcal{E})\, \mathbb{P}\left(d(Z_n x, Z_n y) \le N^{-\lfloor \kappa n\rfloor/8} \,\middle|\, \mathcal{E}\right) \\
&\ge \sum_{\mathcal{E}\in\mathcal{P}_n} \mathbb{P}(\mathcal{E}) \cdot (1 - 2e^{-n/4}) \\
&= (1 - 2e^{-n/4})\, \mathbb{P}(A_n) \ge (1 - 2e^{-n/4})\big(1 - \frac{1}{\kappa} e^{-\kappa n}\big). \quad \square
\end{aligned}$$

Theorem D now follows from Theorem 2.14 together with Corollary 2.5 and Lemma 2.7 (assuming Proposition 2.8). For the perturbation part, it suffices to observe the following: if μ_0^{*m} is (S, ϵ)-admissible for some μ, m, S, ϵ, then μ^{*m} is $(S, \epsilon/2)$-admissible for every μ in a sufficiently small neighborhood of μ_0. We will prove this in the appendix.

2.2. **Probabilistic Tits alternative.** We now turn to the proof of Theorem A.

Lemma 2.15. *Let N be an integer greater than 4. Let $I_1, \dots, I_N, J_1, \dots, J_N$ be intervals such that $I_1, \dots, I_N$ are mutually disjoint and $J_1, \dots, J_N$ are mutually disjoint. Then for any homeomorphism $g \in \mathrm{Homeo}(S^1)$, we have*

$$\#\big\{(i, j) \in \{1, \dots, N\}^2 : I_i \text{ and } gJ_j \text{ intersect}\big\} \le 3N\sqrt{N}.$$

Proof. We first let

$$\mathcal{C} = \mathcal{C}(g) := \big\{I_i : \#\{j : I_i \cap gJ_j \neq \emptyset\} \ge \sqrt{N}\big\}$$

Then each element of $\mathcal{C}$ meets more than 2 out of $\{gJ_1, \dots, gJ_N\}$, so it is not completely contained in a single J_j. Hence, each gJ_j can meet at most 2 elements of $\mathcal{C}$ (otherwise gJ_j will contain an element of $\mathcal{C}$). Hence,

$$\begin{aligned}
2N = 2\#\{gJ_j : j = 1, \dots, N\} &\ge 2\#\{gJ_j : gJ_j \text{ meets some element of } \mathcal{C}\} \\
&\ge \#\big\{(I_i, gJ_i) : I_i \cap gJ_j \neq \emptyset, I_i \in \mathcal{C}\big\} \\
&\ge \#\mathcal{C} \cdot \min_{I_i \in \mathcal{C}} \#\{J_j : I_i \cap gJ_j \neq \emptyset\} \\
&\ge \#\mathcal{C}\sqrt{N}
\end{aligned}$$

holds, which implies that $\mathcal{C}$ has at most $2\sqrt{N}$ elements.

Now fixing $I_i \notin \mathcal{C}$, the number of gJ_j that meets I_i is at most $\sqrt{N}$. Summing up, we have

$$\begin{aligned}
\#\big\{(i, j) \in \{1, \dots, N\}^2 : I_i \text{ and } gJ_j \text{ intersect}\big\} &\le \#\mathcal{C} \cdot N + (N - \#\mathcal{C}) \cdot \sqrt{N} \\
&\le 2N\sqrt{N} + N\sqrt{N} = 3N\sqrt{N}. \quad \square
\end{aligned}$$

Lemma 2.16. *Let S and S' be Schottky sets with median $\mathcal{I}$ and $\mathcal{I}'$, respectively, and with resolution $N \geq 4$. Let s and s' be independent random variables that are Schottky-uniform on S and S', respectively. Then for each $g \in \mathrm{Homeo}(S^1)$ we have*

$$\mathbb{P}\left(s'gs\bar{\mathcal{I}} \subseteq \operatorname{int}\mathcal{I}'\right) \geq 1 - 3/\sqrt{N}.$$

Proof. Let $S = \mathfrak{S}(I_1, J_1) \cup \ldots \cup \mathfrak{S}(I_N, J_N)$ and $S' = \mathfrak{S}(I'_1, J'_1) \cup \ldots \cup \mathfrak{S}(I'_N, J'_N)$. Then for each i, the inverse s'^{-1} of an arbitrary element s' of $\mathfrak{S}(I'_i, J'_i)$ sends $\overline{S^1 \setminus \mathcal{I}'}$ into I'_i. Meanwhile, an arbitrary element s of $\mathfrak{S}(I_i, J_i)$ sends $\overline{\mathcal{I}}$ into J_i. Now Lemma 2.15 tells us that

$$Ind := \left\{(i,j) : I'_i \text{ and } gJ_j \text{ intersect}\right\}$$

has at most $3N\sqrt{N}$ elements. Moreover, given $(i,j) \notin Ind$, for every $s \in \mathfrak{S}(I_i, J_i)$ and $s' \in \mathfrak{S}(I'_j, J'_j)$ we have

$$gs\overline{\mathcal{I}} \subseteq gJ_j \subseteq S^1 \setminus I'_i \subseteq s'^{-1} \operatorname{int}\mathcal{I}'$$

Summing up, we arrive at

$$\mathbb{P}\left(s'gs\bar{I} \subseteq \operatorname{int} I'\right) \geq \mathbb{P}\left(s \in \mathfrak{S}(I_i, J_i), s' \in \mathfrak{S}(I'_j, J'_j) : (i,j) \notin Ind\right) \geq 1 - 3/\sqrt{N}. \quad \square$$

Lemma 2.17. *Let S and S' be Schottky sets with median $\mathcal{I}$ and $\mathcal{I}'$, respectively, and with resolution $N \geq 100$. For $i = 1, \ldots, n$, let s_i be a Schottky-uniform measure on S and let s_{-i} be a Schottky-uniform measure on S'. Suppose that $\{s_i : 1 \leq |i| \leq n\}$ are all independent. Fix homeomorphisms $\{w_i : -n \leq i \leq n\}$ such that*

$$w_i\mathcal{I} \subseteq \mathcal{I},\ w_{-i}\mathcal{I}' \subseteq \mathcal{I}' \quad (1 \leq i \leq n).$$

Then we have

$$\mathbb{P}\left(w_{-n}s_{-n}\cdots w_{-1}s_{-1} \cdot w_0 \cdot s_1w_1\cdots s_nw_n \cdot \bar{\mathcal{I}} \subseteq \operatorname{int}\mathcal{I}'\right) \geq 1 - e^{-n}$$

Note that we have not assumed any restriction on w_0 in Lemma 2.17.

Proof. We define $W_0 := id$ and define $W_k := s_1w_1\cdots s_kw_k$, $W_{-k} := w_{-k}s_{-k}\cdots w_{-1}s_{-1}$. Then the following inclusion holds:

$$W_0\mathcal{I} \supseteq W_0s_1\mathcal{I} \supseteq W_1\mathcal{I} \supseteq W_1s_2\mathcal{I} \supseteq \ldots \supseteq W_n\mathcal{I},$$
$$W_0^{-1}\mathcal{I}' \subseteq (s_{-1}W_0)^{-1}\mathcal{I}' \subseteq W_{-1}^{-1}\mathcal{I}' \subseteq (s_{-2}W_{-1})^{-1}\mathcal{I}' \subseteq W_{-2}^{-1}\mathcal{I}' \subseteq \ldots \subseteq W_{-n}^{-1}\mathcal{I}',$$

regardless of the choices of s_i's. We now define

$$E_k := \left\{(s_{-k}, \ldots, s_{-1}, s_1, \ldots, s_k) : (s_{-k}W_{-(k-1)})^{-1} \operatorname{int}\mathcal{I}' \supseteq W_{k-1}s_k\bar{\mathcal{I}}\right\}.$$

Then Lemma 2.16 tells us that

$$\mathbb{P}\left(E_{k+1} \,\middle|\, s_{-k}, \ldots, s_k\right) \geq 1 - 3/\sqrt{N} \geq 1 - 1/e$$

holds regardless of the choices of $s_{-k}, \ldots, s_k$. Summing up the conditional probabilities, we conclude

$$\mathbb{P}\left(W_n\bar{I} \subseteq W_{-n}^{-1} \operatorname{int}\mathcal{I}'\right) \geq \mathbb{P}\left(E_1 \cup \ldots \cup E_n\right) \geq 1 - (1/e)^n \geq 1 - e^{-n}. \quad \square$$

Theorem 2.18. *Let S and S' be Schottky sets with median $\mathcal{I}$ and median $\mathcal{I}'$, respectively, with resolution $N \geq 100$. Let μ and μ' be Schottky-uniform measures on S and S', respectively. Fix homeomorphisms $w_0, v_0, w_1, v_1, \ldots, w_{2n}, v_{2n} \in \mathrm{Homeo}(S^1)$ such that*

$$w_i\mathcal{I} \subseteq \mathcal{I},\ v_i\mathcal{I}' \subseteq \mathcal{I}' \quad (i = 1, \ldots, 2n-1)$$

Let $s_1, \ldots, s_{2n}$ ($t_1, \ldots, t_{2n}$, resp.) be random variables distributed according to a Schottky-uniform measure on S (S', resp.), all independent. Then we have

$$\mathbb{P}\left(\begin{array}{c} w_0s_1w_1\cdots s_{2n}w_{2n} \text{ and } v_0t_1v_1\cdots t_{4n}v_{4n} \text{ comprise} \\ \text{a Schottky pair and generate a free subgroup} \end{array}\right) \geq 1 - 6e^{-n/10}.$$

Proof. We define the following events.

$$\begin{aligned}
E_1 &:= \left\{ s_{n+1}w_{n+1}\cdots s_{2n}w_{2n}\cdot w_0 s_1 w_1 \cdots s_n w_n \bar{\mathcal{I}} \subseteq \operatorname{int}\mathcal{I} \right\},\\
E_2 &:= \left\{ t_{n+1}v_{n+1}\cdots t_{2n}v_{2n}\cdot v_0 t_1 v_1 \cdots t_n v_n \bar{\mathcal{I}'} \subseteq \operatorname{int}\mathcal{I}' \right\},\\
E_3 &:= \left\{ s_{n+1}w_{n+1}\cdots s_{2n}w_{2n}\cdot v_0 t_1 v_1 \cdots t_n v_n \bar{\mathcal{I}'} \subseteq \operatorname{int}\mathcal{I} \right\},\\
E_4 &:= \left\{ t_{n+1}v_{n+1}\cdots t_{2n}v_{2n}\cdot w_0 s_1 w_1 \cdots s_n w_n \bar{\mathcal{I}} \subseteq \operatorname{int}\mathcal{I}' \right\},\\
E_5 &:= \left\{ s_{n+1}w_{n+1}\cdots s_{2n}w_{2n}\cdot v_{2n}^{-1}t_{2n}^{-1}\cdots v_{n+1}^{-1}t_{n+1}^{-1}\cdot \overline{S^1\setminus\mathcal{I}'} \subseteq \operatorname{int}\mathcal{I} \right\},\\
E_6 &:= \left\{ v_n^{-1}t_n^{-1}\cdots v_1^{-1}t_1^{-1}v_0^{-1}\cdot w_0 s_1 w_1\cdots s_n w_n \cdot \bar{\mathcal{I}} \subseteq \operatorname{int}(S^1\setminus\mathcal{I}') \right\}.
\end{aligned}$$

Let us study the first event. Here, s_i's are Schottky-uniformly and independently distributed on S, $\mathcal{I}$ is a median for S, and $w_i\mathcal{I}\subseteq\mathcal{I}$ holds for each $i\neq 0, 2n$. (Note that $w_{2n}\cdot w_0$ does not nest I.) By Lemma 2.17, we conclude $\mathbb{P}(E_1)\geq 1-e^{-n}$. For a similar reason, we conclude that the probabilities of E_2, E_3 and E_4 are all at least $1-e^{-n}$.

Before studying the fifth event, let us first write $S'=\mathfrak{S}(I_1',J_1')\cup\ldots\cup\mathfrak{S}(I_N',J_N')$ and revert it: $\check{S}':=\mathfrak{S}(J_1',I_1')\cup\ldots\cup\mathfrak{S}(J_N',I_N')$. Then s_i's are Schottky-uniformly and independently distributed on S, whereas t_i^{-1}'s are Schottky-uniformly and independently distributed on $\check{S}'$. Moreover, $\mathcal{I}$ is a median for S and $w_i\mathcal{I}\subseteq\mathcal{I}$ holds for each i, whereas $S^1\setminus\mathcal{I}'$ is a median for $\check{S}'$ and $v_i^{-1}(S^1\setminus\mathcal{I}')\subseteq(S^1\setminus\mathcal{I}')$ holds for each i, Now, Lemma 2.17 tells us taht $\mathbb{P}(E_5)\geq 1-e^{-n}$. A similar argument tells us that $\mathbb{P}(E_6)\geq 1-e^{-n}$.

Now in the event $E_1\cup E_2\cup E_3\cup E_4\cup E_5\cup E_6$, we will investigate the configuration of the intervals

$$\begin{aligned}
I^{(1)} &:= (s_{n+1}w_{n+1}\cdots s_{2n}w_{2n})^{-1}(S^1\setminus\operatorname{int}\mathcal{I}),\\
I^{(2)} &:= (t_{n+1}v_{n+1}\cdots t_{2n}v_{2n})^{-1}\cdot(S^1\setminus\operatorname{int}\mathcal{I}'),\\
J^{(1)} &:= w_0 s_1 w_1\cdots s_n w_n\overline{\mathcal{I}},\\
J^{(2)} &:= v_0 t_1 v_1\cdots t_n v_n\overline{\mathcal{I}'}.
\end{aligned}$$

First, since we are in the event E_1, $I^{(1)}$ and $J^{(1)}$ does not overlap with each other. Similarly, the definition of E_2 tells us that $I^{(2)}$ and $J^{(2)}$ do not meet. The definition of E_3 (E_4, E_5 and E_6, resp.) tells us that $I^{(1)}$ and $J^{(2)}$ ($I^{(2)}$ and $J^{(1)}$; $I^{(1)}$ and $I^{(2)}$; $J^{(1)}$ and $J^{(2)}$, resp.) do not meet. In summary, all the 4 intervals are mutually disjoint in the event $\cup_{k=1}^6 E_k$. Meanwhile, $w_0s_1w_1\cdots s_{2n}w_{2n}$ sends $S^1\setminus I^{(1)}$ into $\operatorname{int}J^{(1)}$ and $v_0t_1v_1\cdots t_{2n}v_{2n}$ sends $S^1\setminus I^{(2)}$ into $\operatorname{int}J^{(2)}$.

In conclusion, $w_0s_1w_1\cdots s_{2n}w_{2n}$ and $v_0t_1v_1\cdots t_{2n}v_{2n}$ comprise a Schottky pair associated with disjoint intervals $I^{(1)},I^{(2)},J^{(1)},J^{(2)}$ and generate a (rank-2) free subgroup of $\mathrm{Homeo}(S^1)$, when in the event $\cup_{k=1}^6E_k$. Since $\mathbb{P}(E_k^c)\leq e^{-n}$ for each k, we conclude that $\cup_{k=1}^6E_k$ has probability at least $1-6e^{-n}$. □

Now as in the proof of Theorem 2.14, we can derive the following theorem from Theorem 2.18 using the probability space and measurable partition guaranteed in Proposition 2.8.

Theorem 2.19. *For each $\epsilon>0$, $m\in\mathbb{Z}_{>0}$ and $N\in\mathbb{Z}_{>2500}$, there exists $\kappa_2=\kappa_2(\epsilon,m,N)>0$ that satisfies the following.*

Let S and S' be Schottky sets with medians, with resolution N. Let μ and μ' be probability measures on $\mathrm{Homeo}(S^1)$ *such that μ^{*m} is (S,ϵ)-admissible and μ'^{*m} is (S',ϵ)-admissible. Then for each $n\in\mathbb{Z}_{>0}$ we have*

$$\mathbb{P}_{(Z_n,Z_n')\sim\mu^{*n}\times\mu'^{*n}}\left(Z_n,Z_n' \text{ comprise a Schottky pair and generate a free subgroup}\right)\geq 1-\frac{1}{\kappa_2}e^{-\kappa_2 n}.$$

2.3. **Local contraction.** Note that Theorem A and D are regarding "snapshots" of a random walk at a certain step. Meanwhile, Theorem C asks for a specific choice of $I_{x,\omega}$, when the input $x \in S^1$ and a sample point ω in the probability space is given. This does not only rely on the distribution μ^{*n} of Z_n for each n, their entire joint distribution. In fact, the same result will not hold for right random walk.

Proof. To begin the proof, let κ be as in Proposition 2.8 for ϵ, m and N. To ease the notation, we will assume that $1/\kappa \in \mathbb{N}$. Then it suffices to prove the statement only for n being multiples of $100/\kappa$.

Let us consider a large ambient space

$$\Omega := (G^{\mathbb{Z}_{>0}}, \mu^{\mathbb{Z}_{>0}})$$

equipped with i.i.d.s g_i distributed according to μ. We adopt the left random walk convention in this proof, i.e., $Z_i := g_i \cdots g_1$.

We now regard Ω as a product space

$$\cdots \times \Omega_3 \times \Omega_2 \times \Omega_1 =: \Omega,$$

where Ω_k is the space for the coordinates $(g_{n(2^k-1)}, g_{n(2^k-1)-1}, \dots, g_{n(2^{k-1}-1)+1})$ for $k \geq 1$. Note the relation

$$g_{n(2^k-1)} \cdots g_{n(2^{k-1}-1)+l} = Z_{n(2^k-1)} \cdot Z^{-1}_{n(2^{k-1}-1+l)-1} \quad (l = 0, \dots, n2^{k-1}-1).$$

We now apply Proposition 2.8 for each of Ω_k. Then Ω_k is now equipped with a measurable subset $A^{(k)}$, a measurable partition $\mathcal{P}^{(k)} = \{\mathcal{E}^{(k)}_\alpha\}_\alpha$ of $A^{(k)}$, and random variables

$$\{w^{(k)}_i\}_{i=0,\dots,\kappa n 2^{k-1}},\ \{s^{(k)}_i\}_{i=1,\dots,\kappa n 2^{k-1}}$$

such that:

(1) $\mathbb{P}(A^{(k)}) \geq 1 - \frac{1}{\kappa} e^{-\kappa \cdot 2^{k-1}}$.
(2) Restricted on each equivalence $\mathcal{E} \in \mathcal{P}_k$, $w^{(k)}_0, \dots, w^{(k)}_{\kappa 2^{k-1}}$ are *constant* homeomorphisms and $s^{(k)}_i$ are independently distributed according to a Schottky-uniform measures on S.
(3) On $A^{(k)}$, $w^{(k)}_i \mathcal{I} \subseteq \mathcal{I}$ holds for each $i = 1, \dots, \kappa 2^{k-1} - 1$;
(4) For each $\omega \in A^{(k)}$ we have

$$\begin{aligned} w^{(k)}_0(\omega) s^{(k)}_1(\omega) \cdots s^{(k)}_{\kappa 2^{k-1}}(\omega) w^{(k)}_{\kappa 2^{k-1}}(\omega) &= g_{n(2^k-1)}(\omega) g_{n(2^k-1)-1}(\omega) \cdots g_{n(2^{k-1}-1)+1}(\omega) \\ &= Z_{n(2^k-1)}(\omega) \cdot Z^{-1}_{n(2^{k-1}-1)}(\omega). \end{aligned} \tag{2.2}$$

Also, the partitions $\mathcal{P}^{(k)}$'s for distinct k's are all independent.

Let us now define the event

$$F_k := \Big\{ \omega : s^{(k+1)}_{0.9\kappa n 2^k+1} w^{(k+1)}_{0.9\kappa n 2^k+1} \cdots s^{(k+1)}_{\kappa n 2^k} w^{(k+1)}_{\kappa n 2^k} \cdot w^{(k)}_0 s^{(k)}_1 w^{(k)}_1 \cdots s^{(k)}_{0.1\kappa n 2^{k-1}} w^{(k)}_{0.1\kappa n 2^{k-1}} \mathcal{I} \subseteq \mathcal{I} \Big\}.$$

For each $\mathcal{E}' \in \mathcal{P}^{(k+1)}$ and $\mathcal{E} \in \mathcal{P}^{(k)}$, the conditional probability of F_k on $\mathcal{E}' \times \mathcal{E}$ is at least $1 - e^{-0.1\kappa 2^{k-1}}$ by Lemma 2.17. Also, the probability of $A^{(k+1)} \times A^{(k)}$ is at least $1 - \frac{2}{\kappa} e^{-\kappa 2^{k-1}}$. Summing up the conditional probability, we conclude

$$\mathbb{P}(F_k) \geq 1 - (2/\kappa + 1) e^{-0.1\kappa n 2^{k-1}}. \quad (k = 1, 2, \dots)$$

Next, for each $k \geq 1$ and for each $n(2^k - 1) < t \leq n(2^{k+1} - 1)$, we define

$$End_t := \Big\{ \operatorname{Len}\left(Z_t Z^{-1}_{n(2^k-1)} \cdot w^{(k)}_0 s^{(k)}_1 w^{(k)}_1 \cdots s^{(k)}_{0.5\kappa n 2^{k-1}} w^{(k)}_{0.5\kappa n 2^{k-1}} \cdot \mathcal{I} \right) \leq \frac{1}{e^{0.01\kappa t}} \Big\}.$$

For each choice of $(g_{n(2^{k+1}-1)}, \dots, g_{n(2^k-1)+1}) \in \Omega_{k+1}$ and each $\mathcal{E} \in \mathcal{P}^{(k)}$, $Z_t Z_{n(2^k-1)}^{-1}$ is pinned down together with $w_0^{(k)}, w_1^{(k)}, \dots$, whereas $s_1^{(k)}, s_2^{(k)}, \dots$ are independently Schottky-uniformly distributed on S. Now Lemma 2.10 tells us that $\mathbb{P}(End_t \,|\, g_{n(2^{k+1}-1)}, \dots, g_{n(2^k-1)+1}, \mathcal{E}) \geq 1 - e^{-0.01\kappa t}$. Summing up the conditional probability across $\Omega_{k+1} \times A^{(k)}$, whose total probability is at least $1 - \frac{1}{\kappa} e^{-\kappa 2^{k-1}}$, we conclude that

$$\mathbb{P}(End_t) \geq 1 - (1/\kappa + 1)e^{-0.01\kappa t}. \quad (t = n, n+1, n+2, \dots).$$

We now claim:

Claim 2.20. *Let $\omega \in \left(\cup_{k=1}^{\infty} F_k\right) \cap \left(\cup_{t=n}^{\infty} End_t\right)$. Then for each $t \geq n$ and for each interval I such that*

$$I \subseteq \left(s_{0.5\kappa n+1}^{(1)} w_{0.5\kappa n+1}^{(1)} \cdots s_{\kappa n}^{(1)} w_{\kappa n}^{(1)}\right)^{-1} \cdot \mathcal{I},$$

we have $\mathrm{Len}(Z_t I) \leq e^{-0.01\kappa t}$.

To prove the claim let $t \geq n$ and let $k \geq 1$ be such that $n(2^k - 1) \leq t \leq n(2^{k+1} - 1)$. If $k = 1$, the claim follows from the definition that

$$Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.5\kappa n 2^{k-1}}^{(k)} w_{0.5\kappa n 2^{k-1}}^{(k)} = \left(s_{0.5\kappa+1}^{(1)} w_{0.5\kappa n+1}^{(1)} \cdots s_{\kappa n}^{(1)} w_{\kappa n}^{(1)}\right)^{-1}.$$

and that $\omega \in End_t$. When k is larger than 1, we note that

$$\begin{aligned}
&Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.5\kappa n 2^{k-1}}^{(k)} w_{0.5\kappa n 2^{k-1}}^{(k)} \cdot \mathcal{I} \\
\supseteq\ & Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.9\kappa n 2^{k-1}-1}^{(k)} w_{0.9\kappa n 2^{k-1}-1}^{(k)} \cdot \mathcal{I} \\
\supseteq\ & Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.9\kappa n 2^{k-1}-1}^{(k)} w_{0.9\kappa n 2^{k-1}-1}^{(k)} \cdot \\
& s_{0.9\kappa n 2^{k-1}}^{(k)} w_{0.9\kappa n 2^{k-1}}^{(k)} \cdots s_{\kappa n 2^{k-1}}^{(k)} w_{\kappa n 2^{k-1}}^{(k)} \cdot w_0^{(k-1)} s_1^{(k-1)} w_1^{(k-1)} \cdots s_{0.1\kappa n 2^{k-2}}^{(k-1)} w_{0.1\kappa n 2^{k-2}}^{(k-1)} \mathcal{I} \\
=\ & Z_t \cdot Z_{n(2^{k-1}-1)}^{-1} \cdot w_0^{(k-1)} s_1^{(k-1)} w_1^{(k-1)} \cdots s_{0.1\kappa n 2^{k-2}}^{(k-1)} w_{0.1\kappa n 2^{k-2}}^{(k-1)} \mathcal{I}.
\end{aligned}$$

Here, the first inclusion is due to the fact that $s\mathcal{I} \subseteq \mathcal{I}$ and $w_i^{(k)} \mathcal{I} \subseteq \mathcal{I}$ for any $s \in S$ and any $w_i^{(j)}$. The second inclusion is because of $\omega \in F_{k-1}$, and the third equality is using Equation 2.2.

We can keep going like this and arrive at the inclusion

$$Z_t \cdot Z_0^{-1} \cdot w_0^{(1)} s_1^{(1)} w_{(1)} \cdots s_l^{(1)} w_l^{(2)},$$

for any l between $0.1\kappa n$ and $\kappa n - 1$ (thanks to the fact that $s\mathcal{I} \subseteq \mathcal{I}$ and $w_i^{(1)} \mathcal{I} \subseteq \mathcal{I}$). By using the relation for $l = 0.5\kappa n$ we establish the claim.

Finally, let us estimate the probability of

$$Dec := \left\{ \begin{array}{c} \mathrm{Len}\left(\left(s_{0.5\kappa n+1}^{(1)} w_{0.5\kappa n+1}^{(1)} \cdots s_{\kappa n}^{(1)} w_{\kappa n}^{(1)}\right)^{-1} \cdot \mathcal{I}\right) \\ = 1 - \mathrm{Len}\left((w_{\kappa n}^{(1)})^{-1} (s_{\kappa n}^{(1)})^{-1} \cdots (w_{0.5\kappa n+1}^{(1)})^{-1} (s_{0.5\kappa n+1}^{(1)})^{-1} \cdot (S^1 \setminus \mathcal{I})\right) \\ \geq 1 - 0.01^{n/4} \end{array} \right\}.$$

Here, note that $S^1 \setminus \mathcal{I}$ is a median for $\check{S}$, the reverted version of S, on which each $(s_i^{(1)})^{-1}$ are independently distributed according to Schottky-uniform measures. Moreover, $(w_i^{(1)})^{-1}(S^1 \setminus \mathcal{I}$ holds for each $i \neq 0, \kappa n$. Hence, we can apply Lemma 2.10 and conclude that $\mathbb{P}(Dec) \geq 1 - e^{-n/4}$.

In conclusion, we have found a set $\left(\cup_{k=1}^{\infty} F_k\right) \cap \left(\cup_{t=n}^{\infty} End_t\right) \cap Dec$, whose complement has exponentially decaying probability in n, such that for each sample ω in the set, there exists an interval of length at least $1 - 0.01^{n/4}$ that gets exponentially contracted at every step $t \geq n$. This finishes the proof of Theorem C.

□

3. Pivoting technique

In this section, we explain Gouëzel's pivoting technique that was introduced in [Gou22]. It was later applied to a broader setting in [Cho22].

As a warm-up, we observe the following.

Lemma 3.1. *For each $\epsilon > 0$ and $m \in \mathbb{Z}_{>0}$, there exists $\kappa = \kappa(\epsilon, m, N)$ such that the following holds.*

Let S be a Schottky set and let μ be a probability measure on $\mathrm{Homeo}(S^1)$ such that μ^{*m} is an (S, ϵ)-admissible measure. Then for each $n \in \mathbb{Z}_{n>0}$, there exists a probability space Ω_n, a measurable subset $A_n \subseteq \Omega_n$, a measurable partition $\mathcal{P}_n = \{\mathcal{E}_\alpha\}_\alpha$ of A_n, and $\mathrm{Homeo}(S^1)$-valued random variables

$$Z_n, \{w_i\}_{i=0,\dots,\lfloor \kappa n \rfloor}, \{r_i, s_i, t_i\}_{i=1,\dots,\lfloor \kappa n \rfloor}$$

that satisfy the following.

1. *$\mathbb{P}(A_n) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}$.*
2. *When restricted on each equivalence class $\mathcal{E} \in \mathcal{P}_n$, $w_0, \dots, w_{\lfloor \kappa n \rfloor}$ are each fixed constant maps and r_i, s_i, t_i are independent random variables distributed according to a Schottky-uniform measure on S.*
3. *Z_n is distributed according to μ^{*n} on Ω_n, and*

$$Z_n = w_0 r_1 s_1 t_1 w_1 \cdots r_{\lfloor \kappa n \rfloor} s_{\lfloor \kappa n \rfloor} t_{\lfloor \kappa n \rfloor} w_{\lfloor \kappa n \rfloor}$$

holds on A_n.

Proof. It suffices to prove this for n being a multiple of $3m$. Indeed, for $n = 3mk+l$ ($1 \leq l \leq 3m-1$) we can treat as follows: we first take Ω_{3mk}, $\mathcal{P}_{mk}$, $(w_i)_i$, $(r_i, s_i, t_i)_i$ using the proposition and consider (G^l, μ^l) (where $G = \mathrm{Homeo}(S^1)$). And then we define

$$\Omega_{3mk+l} := \Omega_{mk} \times G^l,$$
$$\mathcal{P}_{3mk+l} := \mathcal{P}_{mk} \times G^l = \{\mathcal{E}_\alpha \times (g_1, \dots, g_l) : \mathcal{E}_\alpha \in \mathcal{P}_{3mk}, (g_1, \dots, g_l) \in G^l\}$$

We then keep $(w_i)_i, (r_i, s_i, t_i)_i$ but replace $w_{\lfloor \kappa n \rfloor}$ with $w_{\lfloor \kappa n \rfloor} \cdot g_1 \cdots g_l$ to realize the conclusions for $n = 3mk + l$.

We now begin our proof for $3m|n$. Since μ^{*m} is (S, ϵ)-admissible, we can construct a probability measure μ_S that is Schottky-uniform on S and another probability measure ν on $\mathrm{Homeo}(S^1)$ such that

$$\mu^{*3m} = \epsilon^3 \mu_S^{*3} + (1 - \epsilon^3)\nu$$

holds. Now, we construct Bernoulli RVs $(\rho_i)_{i=0}^\infty$ with expectation ϵ, RVs $(\eta_i^{(1)})_{i=1}^\infty$, $(\eta_i^{(2)})_{i=1}^\infty$ and $(\eta_i^{(3)})_{i=1}^\infty$ each distributed according to μ_S, RVs $(\nu_i)_{i=1}^\infty$ distributed according to ν, all independently, and then define g_i's by

$$g_i := \eta_i^{(1)} \cdot \eta_i^{(2)} \cdot \eta_i^{(3)} \text{ when } \rho_i = 1, \;\; g_i = \nu_i \text{ when } \rho_i = 0.$$

This way, $g_1, g_2, \dots$ become i.i.d.s distributed according to μ^{3m}. We now collect the indices at which ρ_i attains value 1:

$$\{i(1) < i(2) < \dots\} := \{1 \leq i \leq n/3m : \rho_i = 1\}, \; N := \#\{1 \leq i \leq n/3m : \rho_i = 1\}.$$

Then Markov's inequality implies

$$e^{-\epsilon n/10m} \cdot \mathbb{P}\left(N \leq \epsilon n/10m\right) \leq \mathbb{E}\left[e^{-B(n/3m,\epsilon)}\right] \leq \left(1 - \epsilon(1 - e^{-1})\right)^{n/3m} \leq (1 - 0.6\epsilon)^{n/3m} \leq e^{-0.6 \cdot \epsilon n/3m}.$$

Hence, the probability of $N \leq \epsilon n/10m$ is at most $e^{-\epsilon n/10m}$. Now on the event $\{N \geq \epsilon n/10m\}$ we construct

$$\begin{aligned} w_0 &:= \prod_{i=1}^{i(1)-1} g_i = \nu_1 \cdots \nu_{i(1)-1}, \\ w_l &:= \prod_{i=i(l)+1}^{i(l+1)-1} g_i = \nu_{i(l)+1} \cdots \nu_{i(l+1)-1} \qquad (l = 1, \ldots, \lfloor \epsilon n/10m \rfloor - 1) \\ w_{\lfloor \epsilon n/10m \rfloor} &:= \prod_{i=i(\lfloor \epsilon n/10m \rfloor)+1}^{n/3m} g_i = \nu_{i(\lfloor \epsilon n/10m \rfloor)+1} \cdots \nu_{n/3m} \end{aligned}$$

and set $(r_l, s_l, t_l) := \big(\eta^{(1)}_{i(l)}, \eta^{(2)}_{i(l)}, \eta^{(3)}_{i(l)}\big)$ for each $l = 1, \ldots, \lfloor \epsilon n/10m \rfloor$. Then

$$Z_n := g_1 g_2 \cdots g_{n/3} = w_0 r_1 s_1 t_1 w_1 \cdots r_{\lfloor \epsilon n/10m \rfloor} s_{\lfloor \epsilon n/10m \rfloor} t_{\lfloor \epsilon n/10m \rfloor} w_{\lfloor \epsilon n/10m \rfloor}$$

is distributed according to μ^{*n}. We can then finish the proof by declaring the equivalence relation based on the values of $\{\rho_l, \eta_l : l\}$ and $\big\{\eta^{(1)}_l, \eta^{(2)}_l, \eta^{(3)}_l : l > i(\lfloor \epsilon n/10m \rfloor)\big\}$. □

Let us now recall the trick we used in Lemma 2.15.

Definition 3.2. *Let $S = \cup_{i=1}^N \mathfrak{S}(I_i, J_i)$ be a Schottky set with resolution N. For each $g \in$ Homeo(S^1), we define*

$$\mathcal{C}(g; S) := \big\{I_i : \#\{j : \bar{I}_i \cap g\bar{J}_j \neq \emptyset\} \geq \sqrt{N}\big\}.$$

Furthermore, for each interval $I \subseteq S^1$ we define

$$\mathcal{R}(I; S) := \{J_i : \bar{J}_i \cap \bar{I} \neq \emptyset\}.$$

Lemma 3.3. *Let S be a Schottky set with resolution N and let $g \in$ Homeo(S^1) be a homeomorphism. Then the cardinality of $\mathcal{C}(g; S)$ is at most $2\sqrt{N}$. Furthermore, for every $I \in \mathcal{C}(g; S)$, the cardinality of $\mathcal{R}(g^{-1}I; S)$ is at most $2\sqrt{N}$.*

Before proceeding to the definition of pivotal times, we recall the notation introduced earlier: when a Schottky set $S = \cup_{i=1}^N \mathfrak{S}(I_i, J_i)$ is understood, each element s of S belongs to some $\mathfrak{S}(I_i, J_i)$. In this situation, we write $I(s)$ for I_i and $J(s)$ for J_i.

Definition 3.4. *Let*

$$S := \cup_{i=1}^N \mathfrak{S}(I_i, J_i)$$

be a Schottky set with a median $\mathcal{I}$. Fixing a sequence $\mathbf{w} = (w_i)_{i=0}^\infty$ in Homeo(S^1)*, we draw sequences $\mathbf{r} = (r_i)_{i=1}^\infty, \mathbf{s} = (s_i)_{i=1}^\infty, \mathbf{t} = (t_i)_{i=1}^\infty$ from S. We use the following recursive notation:*

$$W_0 := w_0, \ W_n := W_{n-1} \cdot r_n s_n t_n \cdot w_n \ (n > 0).$$

For each $n \in Z_{\geq 0}$, we define the pivotal intervals $L_n = L_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \subseteq S^1$ *and the* set of pivotal times $P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \subseteq \{1, \ldots, n\}$ *in the following recursive manner:*

(1) for $n = 0$, we let $L_0 := \mathcal{I}, P_0 := \emptyset$.
(2) for each $n \geq 1$, we divide into the following two cases:
  (A) If $J(r_n) \subseteq W_{n-1}^{-1} L_{n-1}$ AND $I(t_n) \notin \mathcal{C}(w_n; S)$ holds, then we define $L_n := W_{n-1} r_n s_n \mathcal{I}$ and $P_n := P_{n-1} \cup \{n\}$.
  (B) If $J(r_n) \subseteq W_{n-1}^{-1} L_{n-1}$ OR $I(t_n) \notin \mathcal{C}(w_n; S)$ does not hold, we consider the set

$$\mathcal{Q} := \Big\{i \in P_{n-1} : I(t_i) \notin \mathcal{C}\big(w_i \cdot W_i^{-1} \cdot W_n; S\big)\Big\}.$$

(i) *If $\mathcal{Q}$ is nonempty, we set $k := \max \mathcal{Q}$ and define $L_n := W_{k-1} r_k s_k \mathcal{I}$, $P_n := P_{n-1} \cap \{1, \dots, k\}$.*
(ii) *If $\mathcal{Q}$ is empty, then we set $L_n := W_n \mathcal{I}$, $P_n := \emptyset$.*

The following observation is immediate.

Lemma 3.5. *In the setting of Definition 3.4, for each $n \in \mathbb{Z}_{>0}$, the outputs $P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$ and $L_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$ depend only on the values of $(r_i, s_i, t_i)_{i=1}^n, (w_i)_{i=0}^n$ and not on the values of $(r_i, s_i, t_i, w_i)_{i=n+1}^\infty$.*

Next, we observe that the images of $\mathcal{I}$ at the pivotal times are nested. This follows from:

Lemma 3.6. *In the setting of Definition 3.4, let $u \in \mathbb{Z}_{>0}$ and let $l < m$ be two consecutive elements in P_u, i..e, $l, m \in P_u$ and $l = \max(P_u \cap \{1, \dots, m-1\})$. Then we have $W_{l-1} r_l s_l \mathcal{I} \supseteq W_{l-1} r_l s_l t_l (S \setminus I(t_l)) \supseteq W_{m-1} r_m \mathcal{I}$.*

Proof. Recall first the property of medians for a Schottky set: we have $S^1 \setminus I(t) \subseteq t^{-1}\mathcal{I}$ for every $t \in S$. This implies the first desired inclusion. For the second desired inclusion, we claim that:

Claim 3.7. *The index l must have been added when P_l was constructed out of P_{l-1}. In other words, $P_{l-1} = P_l \cup \{l\}$ holds.*

Suppose to the contrary that P_l is a subset of $P_{l-1} \subseteq \{1, \dots, l-1\}$. Then not only P_l, but all of P_{l+1}, P_{l+2}, ... cannot contain l. This is because there is no mechanism l can be added at the time of the construction P_{l+1}, P_{l+2}, ... This contradicts the fact that $P_u \ni l$, and the claim follows.

For a similar reason, we have $m \in P_m$. Hence, scenario (2-A) must have held at step $n = l$ and $n = m$.

Next claim is as follows.

Claim 3.8. *$P_u \cap \{1, \dots, m-1\} = P_{m-1}$ holds.*

First, note that the elements of P_u smaller than or equal to $m-1$ must have been acquired no later than step $m-1$, and then must have never been lost thereafter. Hence, they all belong to P_{m-1}. Meanwhile, all elements P_{m-1} should have remained till step u for the following reason. If an element of $P_{m-1} \subseteq \{1, \dots, m-1\}$ was lost at some step n ($n = m, \dots, u$), it would mean that scenario (2-B) was the case at step n, with $k = \max \mathcal{Q}$ being smaller than $m-1$. This means that P_n lost not only P_{m-1} but also m, which contradicts $P_u \ni m$. Hence the claim follows.

We now finish the proof by dividing into two cases.

(1) $l = m-1$: this means that scenario (2-A) was the case at both step l and step $m = l+1$. Hence, $J(r_{l+1}) \subseteq W_l^{-1} L_l := (t_l w_l)^{-1} \mathcal{I}$ must be the case. This implies
$$r_{l+1}\mathcal{I} \subseteq J(r_{l+1}) \subseteq (t_l w_l)^{-1}\mathcal{I},\ W_l r_{l+1} \mathcal{I} \subseteq W_l (t_l w_l)^{-1} \mathcal{I} = W_{l-1} r_l s_l \mathcal{I}$$
as desired.

(2) $l < m-1$: in this case, $P_{m-1} = P_u \cap \{1, \dots, m-1\} \subseteq \{1, \dots, l\}$ does not contain $m-1$ so scenario (2-B) must have been the case at step $n = m-1$. But still, $P_{m-1} = P_u \cap \{1, \dots, m-1\}$ contains an element l so scenario (2-B-ii) is ruled out. Thus, scenario (2-B-i) was the case and l must have been the maximum element of $\mathcal{Q}$. This leads to $L_{m-1} := W_{l-1} r_l s_l \mathcal{I}$. We now know that scenario (2-A) was the case at step $n = m$, which implies $J(r_m) \subseteq W_m^{-1} L_{m-1}$. Hence, we conclude
$$W_m r_m \mathcal{I} \subseteq W_m J(r_m) \subseteq L_{m-1} = W_{l-1} r_l s_l \mathcal{I}.$$

□

Recall once again that $\mathcal{I} \supseteq s\mathcal{I}$ for every $s \in S$. This combined with Lemma 3.6 implies:

Corollary 3.9. *In the setting of Definition 3.4, let $n \in \mathbb{Z}_{\geq 0}$ and let $P_n := \{i(1) < i(2) < \ldots < i(\#P_n)\}$. Then we have*

$$W_{i(1)-1}r_{i(1)}\mathcal{I} \supseteq W_{i(1)-1}r_{i(1)}s_{i(1)}\mathcal{I} \supseteq W_{i(2)-1}r_{i(2)}\mathcal{I} \supseteq W_{i(2)-1}r_{i(2)}s_{i(2)}\mathcal{I} \supseteq \\ \ldots \supseteq W_{i(\#P_n)-1}r_{i(\#P_n)}\mathcal{I} \supseteq W_{i(\#P_n)-1}r_{i(\#P_n)}s_{i(\#P_n)}\mathcal{I}.$$

Next, we will observe that scenario (2-A) have high chance in Definition 3.4, when $\mathbf{r}, \mathbf{s}, \mathbf{t}$ are drawn based on a Schottky-uniform measure.

Lemma 3.10. *Let S be a Schottky set with median, with resolution N, and let $n \in \mathbb{Z}_{>0}$. Fix a sequence $\mathbf{w} = (w_i)_{i=0}^{\infty}$ in $\mathrm{Homeo}(S^1)$ and a sequence $\mathbf{s} = (s_i)_{i=1}^{\infty}$ in S. Further, fix two sequences $\mathbf{r} = (r_i)_{i=1}^{\infty}$, $\mathbf{t} = (t_i)_{i=1}^{\infty}$ in S* except the n-th entries. *Then for any Schottky-uniform probability measure on S, we have*

$$\mathbb{P}_{r_n,t_n:\ i.i.d.\ \sim \mu}\left(\#P_n(\mathbf{r},\mathbf{s},\mathbf{t};\mathbf{w}) = \#P_{n-1}(\mathbf{r},\mathbf{s},\mathbf{t};\mathbf{w}) + 1\right) \geq 1 - 4/\sqrt{N}.$$

Proof. Let us denote the disjoint intervals associated with S by $\{I_i, J_i : i = 1, \ldots, N\}$. Note that the set P_{n-1} and the interval L_{n-1} are determined from the fixed inputs. Now at step $n-1$ of the pivotal set construction, three possibilities arise:

(1) scenario (2-A) holds: Then we have$I(t_{n-1}) \in \mathcal{C}(w_{n-1}; S)$ $L_{n-1} = W_{n-2}r_{n-1}s_{n-1}\mathcal{I}$.
(2) scenario (2-B-i) holds: Then $I(t_k) \in \mathcal{C}(w_k W_k^{-1} W_{n-1}; S)$ and $L_{n-1} := W_{k-1}r_k s_k \mathcal{I}$ holds for $k = \max P_{n-1}$.
(3) scenario (2-B-ii) holds: Then $L_{n-1} := W_{n-1}\mathcal{I}$ contains every $W_{n-1}J_i$.

The event under consideration is equivalent to saying that scenario (2-A) takes place at step n. First, Lemma 3.3 asserts that

$$\mathbb{P}_{t_n \sim \mu}\left(I(t_n) \in \mathcal{C}(w_n; S)\right) \leq \frac{1}{N} \cdot 2\sqrt{N} = \frac{2}{\sqrt{N}}.$$

Let us now observe the condition $J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}$ in the three possibilities above.

(1) scenario (2-A) holds: using Lemma 3.3 and the fact that $I(t_{n-1}) \in \mathcal{C}(w_{n-1}; S)$, we realize that $\mathcal{R}\big(w_{n-1}^{-1}I(t_{n-1}); S\big)$ has at most $2\sqrt{N}$ elements. Moreover, when $J(r_n) \notin \mathcal{R}\big(w_{n-1}^{-1}I(t_{n-1}); S\big)$ holds true,

$$J(r_n) \subseteq S^1 \setminus (\operatorname{int} w_{n-1}^{-1}I(t_{n-1})) \subseteq w_{n-1}^{-1}t_{n-1}^{-1}\mathcal{I} = W_{n-1}^{-1}W_{n-2}r_{n-1}s_{n-1}\mathcal{I} = W_{n-1}^{-1}L_{n-1}$$

also follows. In view of this, we conclude

$$\mathbb{P}_{r_n \sim \mu}\left(J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}\right) \geq \mathbb{P}_{r_n \sim \mu}\left(J(r_n) \notin \mathcal{R}\big(w_{n-1}^{-1}I(t_{n-1}); S\big)\right) \geq 1 - 2/\sqrt{N}.$$

(2) scenario (2-B-i) holds: using Lemma 3.3 and the $I(t_k) \in \mathcal{C}(w_k W_k^{-1} W_{n-1}; S)$, we realize that $\mathcal{R}\big(W_{n-1}^{-1}W_k w_k^{-1} I(t_k); S\big)$ has at most $2\sqrt{N}$ elements. Moreover, when $J(r_n) \notin \mathcal{R}\big(W_{n-1}^{-1}W_k w_k^{-1} I(t_k); S\big)$ holds true,

$$J(r_n) \subseteq S^1 \setminus (\operatorname{int} W_{n-1}^{-1}W_k w_k^{-1}I(t_k)) \subseteq W_{n-1}^{-1}W_k w_k^{-1}t_k^{-1}\mathcal{I} = W_{n-1}^{-1}W_{k-1}r_k s_k \mathcal{I} = W_{n-1}^{-1}L_{n-1}$$

follows. Now a calculation analogous to the one in Item (1) tells us that $J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}$ happens for probability at least $1 - 2/\sqrt{N}$.
(3) scenario (2-B-ii) holds: Then whatever $J(r_n)$ is among $J_1, \ldots, J_N$, $W_{n-1}^{-1}L_{n-1} = \mathcal{I}$ holds.

Based on our estimates for the probabilities for $I(t_n) \notin \mathcal{C}(w_n; S)$ and $J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}$ in the above three cases, we can conclude that $\#P_{n+1} = \#P_n$ happens for probability at least $1 - 4/\sqrt{N}$. □

We now prove a crucial lemma. Roughly speaking, it asserts that changing choices for $\mathbf{s}$ at the pivotal times does not change the set of pivotal times.

Lemma 3.11. *Let S be a Schottky set with a median, let $n \in \mathbb{Z}_{>0}$ and let $\mathbf{w} = (w_i)_{i=0}^n$ be a sequence in* Homeo(S^1). *Let $\mathbf{r} = (r_i)_{i=1}^\infty, \mathbf{s} = (s_i)_{i=1}^\infty, \bar{\mathbf{s}} = (\mathbf{s}_i)_{i=1}^\infty, \mathbf{t} = (t_i)_{i=1}^\infty$ be sequences in S. If we have:*

$$s_i = \bar{s}_i \text{ for each } i \in \{1, \dots, n\} \setminus P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}),$$

then $fP_l(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = P_l(\mathbf{r}, \bar{\mathbf{s}}, \mathbf{t}; \mathbf{w})$ holds for each $1 \leq l \leq n$.

Proof. As an elementary version of this lemma, let us consider:

Claim 3.12. *In the setting as above, let $k \in P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$ be an arbitrary pivotal time. If $s_l = \bar{s}_l$ holds for all $l \neq k$, then $P_l(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = P_l(\mathbf{r}, \bar{\mathbf{s}}, \mathbf{t}; \mathbf{w})$ holds for all $1 \leq l \leq n$.*

Put in other words, this claim asserts that changing the choice at a *single* pivotal time does not change the set of pivotal times (at step $1, \dots, n$). Assuming this claim, in the setting of lemma, we can move from $\mathbf{s}$ to $\bar{\mathbf{s}}$ by changing the choices at the pivotal times, one per each time; then P_l's remain unchanged, and the desired statement holds.

It remains to prove the claim. We will omit $\mathbf{w}, \mathbf{r}, \mathbf{t}$ in the sequel as they are fixed forever. When l is smaller than k, $P_l(\mathbf{s})$ only depends on $s_1, \dots, s_{k-1}$ (and other fixed inputs $\mathbf{w}, \mathbf{r}, \mathbf{t}$), so it coincides with $P_l(\bar{\mathbf{s}})$. Similarly, the value of L_l should coincide for the two inputs.

At step $l = k$, we note that $k \in P_n(\mathbf{s})$. Hence, scenario (2-A) must have held. Here, note that the two conditions

$$J(r_k) \subseteq W_{k-1}^{-1} L_{k-1}, \ I(t_k) \notin \mathcal{C}(w_k; S)$$

only depend on $s_1, \dots, s_{k-1}$ (and other fixed inputs $\mathbf{w}, \mathbf{r}, \mathbf{t}$). Hence, these conditions are unchanged after switching s_k to $\bar{s}_k$, and we have

$$P_k(\bar{\mathbf{s}}) = P_{k-1}(\bar{\mathbf{s}}) \cup \{k\} = P_{k-1}(\mathbf{s}) \cup \{k\} = P_k(\mathbf{s}).$$

At this moment, note the relation

$$L_k(\mathbf{s}) = W_{k-1} r_k s_k \mathcal{I}, \ L_k(\bar{\mathbf{s}}) = W_{k-1} r_k \bar{s}_k \mathcal{I} = g \cdot W_{k-1} r_k s_k \mathcal{I} \quad (g := W_{k-1} r_k \bar{s}_k s_k^{-1} r_k^{-1} W_{k-1}^{-1}).$$

and $W_l(\bar{\mathbf{s}}) = g \cdot W_l(\mathbf{s})$ for each $k \leq l \leq n$.

Now, we inductively prove the following for $k < l \leq n$:

(1) If scenario (2-A) holds at step l for the input $\mathbf{s}$, the same is true for the input $\bar{\mathbf{s}}$.
(2) If scenario (2-B-i) holds at step l for the input $\mathbf{s}$, the same is true for the input $\bar{\mathbf{s}}$
(3) scenario (2-B-ii) does not happen at step l.
(4) In every case, $P_l(\mathbf{s}) = P_l(\bar{\mathbf{s}})$ and $L_l(\bar{\mathbf{s}}) = gL_l(\mathbf{s})$ hold.

As the base case, we have observed Item (4) for $l = k$. For general $k < l \leq n$, we will start by assuming Item(4) for $l - 1$. Recall the conditions for scenario (2-A) at step l, for the input $\mathbf{s}$:

$$J(r_l) \subseteq W_{l-1}(\mathbf{s})^{-1} L_{l-1}(\mathbf{s}), \ I(t_l) \notin \mathcal{C}(w_l; S).$$

The latter one is clearly independent of the inputs $\mathbf{s}$. Furthermore, the inductive hypothesis tells us that

$$\big[J(r_l) \subseteq W_{l-1}(\mathbf{s})^{-1} L_{l-1}(\mathbf{s})\big] \Leftrightarrow \big[J(r_l) \subseteq W_{l-1}(\mathbf{s})^{-1} g^{-1} \cdot g L_{l-1}(\mathbf{s}) = W_{l-1}(\bar{\mathbf{s}})^{-1} L_{l-1}(\bar{\mathbf{s}})\big].$$

In summary, scenario (2-A) at step l for the input $\mathbf{s}$ is equivalent to the one for $\bar{\mathbf{s}}$. Furthermore, when these equivalent conditions hold true,

$$P_l(\bar{\mathbf{s}}) = P_{l-1}(\bar{\mathbf{s}}) \cup \{l\} = P_{l-1}(\mathbf{s}) \cup \{l\} = P_l(\mathbf{s})$$

and

$$L_l(\bar{\mathbf{s}}) := W_l(\bar{\mathbf{s}}) \cdot (t_l w_l)^{-1} \mathcal{I} = g W_l(\bar{\mathbf{s}}) \cdot (t_l w_l)^{-1} \mathcal{I} = g L_l(\mathbf{s})$$

also holds.

If scenario (2-B) holds for the input $\mathbf{s}$, the same is true for $\mathbf{s}'$ because of the observation just before. We then focus on the set

$$\mathcal{Q}(\mathbf{s}) = \mathcal{Q}(\mathbf{s}; l) := \left\{ i \in P_{l-1} : I(t_i) \notin \mathcal{C}\big(w_k \cdot W_i(\mathbf{s})^{-1} W_l(\mathbf{s}); S\big) \right\}$$

Here, recall that $W_i(\bar{\mathbf{s}}) = gW_i(\mathbf{s})$ for $i \geq k$. This implies that

$$\mathcal{Q}(\mathbf{s}; l) \cap \{k, k+1, \dots, l-1\} = \mathcal{Q}(\bar{\mathbf{s}}; l) \cap \{k, k+1, \dots, l-1\}.$$

Meanwhile, we know that k is alive in $P_n(\mathbf{s})$. This means that k must not have been lost at step l. In other words, even if scenario (2-B) is in effect at step l, $\mathcal{Q}(\mathbf{s}; l)$ must contain an element greater than or equal to k. Hence, scenario (2-B-ii) is ruled out.

For this reason, $\mathcal{Q}(\bar{\mathbf{s}}; l) \cap \{k, k+1, \dots, l-1\} = \mathcal{Q}(\mathbf{s}; l) \cap \{k, k+1, \dots, l-1\}$ is nonempty. Because the maximum elements of $\mathcal{Q}(\mathbf{s})$ and $\mathcal{Q}(\bar{\mathbf{s}})$ are taken in this upper sections, we conclude that the two sets have the same maximum u. We then conclude

$$P_l(\bar{\mathbf{s}}) = P_{l-1}(\bar{\mathbf{s}}) \cap \{1, \dots, u\} = P_{l-1}(\mathbf{s}) \cap \{1, \dots, u\} = P_l(\mathbf{s})$$

and

$$L_l(\bar{\mathbf{s}}) := W_u(\bar{\mathbf{s}}) \cdot (t_u w_u)^{-1} \mathcal{I} = gW_u(\mathbf{s})(t_u w_u)^{-1} \mathcal{I} = gL_l(\mathbf{s})$$

Here we used the fact that $u \geq k$. This ends the proof. □

Thanks to the previous lemma, we can now declare an equivalence relation based on the change of choices at the pivotal times, or in short, *pivoting*.

Definition 3.13. *Let S be a Schottky set with a median and let $\mathbf{w}$ be a sequence in $\mathrm{Homeo}(S^1)$, as in the setting of Definition 3.4. We fix an integer $n \in \mathbb{Z}_{>0}$. Now, on the ambient set $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ parametrized by coordinates $(\mathbf{r}, \mathbf{s}, \mathbf{t})$, we declare the following equivalence relation:*

$$\left[(\mathbf{r}, \mathbf{s}, \mathbf{t}) \sim_n (\bar{\mathbf{r}}, \bar{\mathbf{s}}, \bar{\mathbf{t}})\right] \Leftrightarrow \left[\begin{array}{c} r_i = \bar{r}_i \text{ and } t_i = \bar{t}_i \text{ for each } i \in \mathbb{Z}_{>0} \setminus \{n+1\} \text{ and} \\ \bar{s}_i = s_i \text{ for each } i \in \mathbb{Z}_{>0} \setminus P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \end{array} \right].$$

The fact that this is indeed an equivalence relation follows from Lemma 3.5 and Lemma 3.11. Note that this equivalence relation crucially depends on the value of n.

By abuse of notation, we will use $(\mathbf{r}, \mathbf{s}, \mathbf{t})$ for the coordinate functions on $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$; each element will be characterized by its value of $r_1, r_2, \dots, s_1, s_2, \dots, t_1, t_2, \dots$. Now consider an arbitrary equivalence class $\mathcal{E} \subseteq S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ made by $\sim_n$. Then every element of $\mathcal{E}$ have the common (n-th step) set of pivotal times P_n, which we denote by $P_n(\mathcal{E})$. On $\mathcal{E}$, r_i and t_i can take arbitrary values in S for $i = n+1$ and are fixed for $i \neq n+1$. On $\mathcal{E}$, s_i can take arbitrary values in S for $i \in P_n(\mathcal{E})$ and is fixed for $i \notin P_n(\mathcal{E})$.

When S is endowed with a probability measure μ, the ambient space $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ also becomes a probability space (with the product measure of μ's). Here, r_i, s_i, t_i's become μ-i.i.d.s. Now if we restrict ourselves on $\mathcal{E}$–the arbitrary equivalence rlation, $\{r_i, t_i : i \neq n+1\}$, $\{s_i : i \notin P_n(\mathcal{E})\}$ are all fixed constants and $\{s_i : i \in P_n(\mathcal{E})\}$, $\{r_{n+1}, t_{n+1}\}$ are μ-i.i.d.s.

Proposition 3.14. *Let S be a Schottky set with a median and with resolution N, and let μ be a Schottky-uniform measure on S. Fix a sequence $\mathbf{w}$ in $\mathrm{Homeo}(S^1)$ and fix $n \in \mathbb{Z}_{>0}$. Let $\mathcal{E}f$ be an equivalence class made by $\sim_n$ given on $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$. Then for each $j \geq 0$, we have*

$$\mathbb{P}_{\{r_i, s_i, t_i \,:\, i > 0\}:\ \mu\text{-i.i.d.s}} \left(\#P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) < \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) - j \,\middle|\, \mathcal{E} \right) \leq (4/\sqrt{N})^{j+1}$$

Proof. For notational convenience, we denote $P_n(\mathcal{E})$, the common n-th step set of pivotal times, by $\{i(M) < i(M-1) < \ldots < i(2) < i(1)\}$ (with $M = \#\mathcal{P}_n(\mathcal{E})$). Here, M and $i(1), i(2), \dots, i(M)$ are fixed information across $\mathcal{E}$, as well as $\{w_i : i > 0\}, \{r_i, t_i : i \neq n+1\}, \{s_i : i \notin P_n(\mathcal{E})\}$. In other words, elements in $\mathcal{E}$ are pinned down by the values of $(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1})$which are μ-i.i.d.s.

We will now define sets

$$\begin{aligned} A_0 &\subseteq S \times S, \\ A_1(r_{n+1}, t_{n+1}) &\subseteq S, \\ A_2(s_{i(1)}, r_{n+1}, t_{n+1}) &\subseteq S, \\ &\cdots, \\ A_M(s_{i(M-1)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}) &\subseteq S \end{aligned}$$

and prove:

Claim 3.15. *(1)* $\mathbb{P}_{\mu\times\mu}(A_0) \geq 1 - 4/\sqrt{N}$.

(2) For every $(s_{i(M)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{M+2}$, *if* $(r_{n+1}, t_{n+1}) \in A_0$ *holds, then we have*

$$\#P_n(s_{i(M)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}) = \#P_n(s_{i(M)}, \ldots, s_{i(1)}) + 1.$$

(3) For every $1 \leq l \leq M$ *and for every* $(s_{i(l-1)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{l+1}$ *we have*

$$\mathbb{P}_{s_{i(l)}\sim\mu}\left(s_{i(l)} \in A_l(s_{i(l-1)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1})\right) \geq 1 - 4/\sqrt{N}.$$

(4) For every $(s_{i(M)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{M+2}$ *and* $1 \leq l \leq M$, *if* $s_{i(l)}$ *belongs to* $A_l(s_{i(l-1)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+}$ *then we have*

$$\#P_n(s_{i(M)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}) \geq \#P_n(s_{i(M)}, \ldots, s_{i(1)}) - l$$

Let us now prove the proposition from this claim. We let

$$B_0 := \left\{(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in \mathcal{E} : (r_{n+1}, t_{n+1}) \notin A_0\right\}$$

and inductively define

$$B_l := \left\{(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in B_{l-1} : s_{i(l)} \notin A_{l-1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})\right\}$$

for $l = 1, \ldots, M$. Then by Claim 3.15(3),

$$\begin{aligned} \mathbb{P}_{\mathcal{E}}\left(B_l\right) &= \int_{(\mathbf{r},\mathbf{s},\mathbf{t})\in B_{l-1}} \mathbb{P}_{s_{i(l)}\sim\mu}\left(s_{i(l)} \notin A_{l-1} \,\middle|\, s_{i(l-1)}, \ldots, s_{i(1)}, r_{n+1}, t_{n+1}\right) d\mu(s_{i(l-1)}) \cdots d\mu(s_{i(1)})\, d\mu(r_{n+1})\, d\mu(t_{n+1}) \\ &\leq \frac{4}{\sqrt{N}} \cdot \mathbb{P}_{\mathcal{E}}\left(B_{l-1}\right) \end{aligned}$$

holds. Moreover, Claim 3.15(1) implies $\mathbb{P}_{\mathcal{E}}(B_0) \leq \frac{4}{\sqrt{N}}$. Combined together, we observe $\mathbb{P}_{\mathcal{E}}(B_l) \leq (4/\sqrt{N})^{l+1}$ for $l = 0, \ldots, M$.

Next,

$$(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in \mathcal{E} \setminus B_0 \Rightarrow \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \geq \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$$

holds true; we also have

$$(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in B_{l-1} \setminus B_l \Rightarrow \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \geq \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) - l$$

for $l = 1, \ldots, M$. In other words, we have

$$(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in \mathcal{E} \setminus B_l \Rightarrow \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \geq \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) - l$$

for each l. Since we have seen that the probability of B_l is at most $(4/\sqrt{N})^{l+1}$, the proposition follows.

It remains to prove the claim. The claim regarding A_0 was already estabilshed in Lemma 3.10. That means, regardless of the values of $(s_{i(M)}, \ldots, s_{i(1)})$, we proved that the probability for (r_{n+1}, t_{n+1}) to satisfy $\#P_{n+1} = \#P_n + 1$ is at least $1 - 4/\sqrt{N}$. We will prove something more: we claim that the candidates for r_{n+1}, t_{n+1} that make $\#P_{n+1} = \#P_n + 1$ are independent of

$(s_{i(M)}, \dots, s_{i(1)})$. When restricted to $\mathcal{E}$, $\#P_{n+1}(\mathbf{r},\mathbf{s},\mathbf{t};\mathbf{w}) = \#P_n(\mathbf{r},\mathbf{s},\mathbf{t};\mathbf{w}) + 1$ holds if and only if $I(t_{n+1}) \in \mathcal{C}(w_{n+1}; S)$ and $J(r_{n+1}) \subseteq W_n^{-1} L_n \mathcal{I}$. Here,

$$W_n^{-1} L_n \mathcal{I} = \begin{cases} W_n^{-1} W_{\max P_n - 1} r_{\max P_n} s_{\max P_n} \mathcal{I} \\ = \big(t_{i(1)} w_{i(1)} r_{i(1)+1} s_{i(1)+1} t_{i(1)+1} w_{i(1)+1} \cdots r_n s_n t_n w_n\big)^{-1} \mathcal{I} & (\text{when } P_n(\mathcal{E}) \neq \emptyset) \\ \mathcal{I} & (\text{when } P_n(\mathcal{E}) = \emptyset) \end{cases}$$

are fixed throughout $\mathcal{E}$. This is why $\#P_{n+1} = \#P_n + 1$ depends on the choice of r_{n+1} and s_{n+1}, regardless of the values of $s_{i(1)}, \dots, s_{i(M)}$. This settles Claim 3.15(1), (2) and also the construction of A_0.

Now for each $l \in \{1, \dots, M\}$ and for each choices $(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{l+1}$, we define

$$\begin{aligned} A_l &:= \Big\{ s \in S : I(s) \notin \mathcal{C}\big(t_{i(l)} w_{i(l)} \cdot W_{i(l)}^{-1} W_{n+1}; S\big) \Big\} \\ &= \Big\{ s \in S : I(s) \notin \mathcal{C}\big(t_{i(l)} w_{i(l)} \cdot (r_{i(l)+1} s_{i(l)+1} t_{i(l)+1} w_{i(l)+1}) \cdots (r_n s_n t_n w_n) \cdot (r_{n+1} s_{n+1} t_{n+1} w_{n+1}); S\big) \Big\}. \end{aligned}$$

Recall that $\{r_i, t_i : i \neq n\}$ and $\{s_i : i \notin P_n(\mathcal{E})\}$ are all fixed maps; hence, this A_l depends only on the choices of $s_{i(l-1)}, \dots, s_{i(1)}$ and r_{n+1}, t_{n+1}. Furthermore, Lemma 3.3 tells us that $\mathbb{P}_\mu(A_l) \geq 1 - 2/\sqrt{N}$.

Now for an arbitrary $(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{M+2}$, suppose that $s_{i(l)} \in A_l(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1})$. Then by definition we have

$$\#\big\{ j : \bar{I}(s_{i(l)}) \cap t_{i(l)} w_{i(l)} \cdot W_{i(l)}^{-1} W_{n+1} \bar{J}_j \neq \emptyset \big\} \geq \sqrt{N}. \tag{3.1}$$

Meanwhile, Lemma 3.6 tells us that

$$W_{i(l+1)-1} r_{i(l+1)} s_{i(l+1)} t_{i(l+1)} \big(S^1 \setminus I(t_{i(l+1)})\big) \supseteq W_{i(l)-1} r_{i(l)} \mathcal{I}.$$

Finally, the property of $\mathcal{I}$ as a median for S, we have$s_{i(l)} I(s_{i(l)}) \supseteq S^1 \setminus \mathcal{I}$. Combining these two facts yields

$$W_{i(l+1)} w_{i(l+1)}^{-1} \bar{I}(t_{i(l+1)}) \subseteq \operatorname{int}\big(S^1 \setminus W_{i(l)-1} r_{i(l)} \mathcal{I}\big) \subseteq W_{i(l)-1} r_{i(l)} s_{i(l)} I(s_{i(l)}).$$

Using Inequality 3.1, we observe

$$\#\big\{ j : \bar{I}(t_{i(l+1)}) \cap (W_{i(l+1)} w_{i(l+1)}^{-1})^{-1} \cdot (W_{i(l)-1} r_{i(l)} s_{i(l)}) \cdot t_{i(l)} w_{i(l)} \cdot W_{i(l)}^{-1} W_{n+1} \bar{J}_j \neq \emptyset \big\} \geq \sqrt{N}.$$

In other words, $I(t_{i(l+1)}) \in \mathcal{C}\big(w_{i(l+1)} \cdot (W_{i(l+1)})^{-1} \cdot W_{n+1}; S\big)$ hols true. This implies that the set $\mathcal{Q}$ in scenario (2-B) at step $n+1$ contains $i(l+1)$. Hence, $P_{n+1}(\mathbf{r},\mathbf{s},\mathbf{t})$ contains $P_n(\mathcal{E}) \cap \{1, \dots, i(l+1)\} = \{i(M) < \dots < i(l+1)\}$ at least, which leads to the inequality $\#P_{n+1} \geq \#P_n - l$. This concludes Claim 3.15(3), (4) and the entire proof. □

Corollary 3.16. *Let S be a Schottky set with a median and with resolution N, and let μ be a Schottky-uniform measure on S. Fix a sequence $\mathbf{w}$ in* Homeo(S^1). *When $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ is endowed with the product measure of μ, we have the following for each integer $j, k, n \geq 0$:*

$$\mathbb{P}\Big(\#P_{n+1}(\mathbf{r},\mathbf{s},\mathbf{t};\mathbf{w}) < k - j \,\Big|\, \#P_{n+1}(\mathbf{r},\mathbf{s},\mathbf{t};\mathbf{w}) = k \Big) \leq (4/\sqrt{N})^{j+1}. \tag{3.2}$$

Proof. First fix n and give the equivalence relation $\sim_n$ on $(S^{\mathbb{Z}_{>0}})^3$. On each equivalence class, the n-th step set of pivotal times P_n is fixed so its cardinality is also constant. Considering this, in order to prove Inequality 3.2 when conditioned on the size of P_n, it suffices to observe it on each equivalence class. This is then reduced to Proposition 3.14. □

Corollary 3.17. *Let S be a Schottky set with a median and with resolution N, and let μ be a Schottky-uniform measure on S. Fix a sequence $\mathbf{w}$ in $\mathrm{Homeo}(S^1)$. Let $X_1, X_2, \ldots$ be i.i.d.s with distribution*

$$\mathbb{P}(X_i = j) = \begin{cases} (N-4)/N & \text{if } j = 1, \\ (N-4)4^{-j}/N^{-j+1} & \text{if } j < 0, \\ 0 & \text{otherwise.} \end{cases} \tag{3.3}$$

When $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ is endowed with the product measure of μ, $\#P_n$ dominates $X_1 + \ldots + X_n$ in distribution for each n. That means,

$$\mathbb{P}(\#P_n(s) \geq T) \geq \mathbb{P}(X_1 + \ldots + X_n \geq T) \quad (T \in \mathbb{Z}_{\geq 0}).$$

Proof. Let X_i be the RVs as in 3.3; we can require them to be independent from $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$, the ambient probability space on which $P_1, P_2, \ldots$ are define. Now Lemma 3.10 and Corollary 3.16 tells us the following for each $0 \leq k \leq n$ and $i, j \geq 0$:

$$\mathbb{P}\left(\#P_{k+1}(s) \geq i + j \,\middle|\, \#P_k(s) = i\right) \geq \begin{cases} 1 - \frac{4}{N} & \text{if } j = 1, \\ 1 - \left(\frac{4}{N}\right)^{-j+1} & \text{if } j < 0. \end{cases} \tag{3.4}$$

Let us prove that for each $k = 1, \ldots, n$ and for each $i \in \mathbb{Z}_{\geq 0}$ we have $\mathbb{P}(\#P_k \geq i) \geq \mathbb{P}(X_1 + \ldots + X_k \geq i)$. For $k = 1$, the claim follows from Inequality 3.4 because $\#P_{k-1} = 0$ always. Now, assuming the statement for k as an induction hypothesis, we observe

$$\begin{aligned} \mathbb{P}(\#P_{k+1} \geq i) &\geq \mathbb{P}(\#P_k + X_{k+1} \geq i) = \sum_j \mathbb{P}(\#P_k \geq j)\, \mathbb{P}(X_{k+1} = i - j) \\ &\geq \sum_j \mathbb{P}(X_1 + \cdots + X_k \geq j)\, \mathbb{P}(X_{k+1} = i - j) \\ &= \mathbb{P}(X_1 + \cdots + X_k + X_{k+1} \geq i). \quad \square \end{aligned}$$

Corollary 3.18. *Let S be a Schottky set with a median and with resolution $N \geq 2500$, and let μ be a Schottky-uniform measure on S. Fix a sequence $\mathbf{w}$ in $\mathrm{Homeo}(S^1)$. When $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ is endowed with the product measure of μ, we have*

$$\mathbb{P}\left(\#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \leq n/2\right) \leq \left(3\sqrt[4]{4/N}\right)^n \leq 0.6^n$$

for each $n \in \mathbb{Z}_{>0}$.

Proof. Let us prove this with Chebyshev's inequality. First recall X_i's in Display 3.4. We have

$$\begin{aligned} \mathbb{E}\left[\sqrt{4/N}^{X_i}\right] &= \left(1 - \frac{4}{N}\right) \cdot \left[\sqrt{\frac{4}{N}} + \sum_{j=1}^{\infty} \sqrt{\frac{N}{4}}^j \cdot \left(\frac{4}{N}\right)^j\right] \\ &= \left(1 - \frac{4}{N}\right) \sqrt{\frac{4}{N}} \left(1 + \frac{1}{1 - \sqrt{4/N}}\right) \\ &= 2\sqrt{4/N} + \sqrt{4/N}^2 - \sqrt{4/N}^3 \leq 3\sqrt{4/N}. \end{aligned}$$

Here, the last inequality used the fact that $\sqrt{4/N} \leq 1$. Now Corollary 3.17 and the independence of X_i's imply that

$$\mathbb{E}\left[\sqrt{4/N}^{\#P_n(\mathbf{s})}\right] \leq \mathbb{E}\left[\sqrt{4/N}^{\sum_{i=1}^n X_i}\right] = \prod_{i=1}^n \mathbb{E}\left[\sqrt{4/N}^{X_i}\right] \leq \left(3\sqrt{4/N}\right)^n.$$

Now Chebyshev's inequality tells us that

$$\mathbb{E}\left[\sqrt{4/N}^{\#P_n(\mathbf{s})}\right] \geq \mathbb{P}(\#P_n(\mathbf{s}) \leq n/2) \cdot \sqrt{4/N}^{n/2}.$$

The conclusion follows by combining the two inequalities. □

We now finally prove Proposition2.8.

Proof of Proposition 2.8. In view of Lemma 3.1, it suffices to prove the following.

Claim 3.19. *Let S be a Schottky set with a median and with resolution $N \geq 2500$, and let μ be a Schottky-uniform measure on S. Fix an integer $n \in \mathbb{Z}_{>0}$ and a sequence $\mathbf{w}$ in* Homeo(S^1)*. Let $\Omega = S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ be the probability space endowed with the product measure of μ. Then there exists a measurable subset A of Ω, a measurable partition $\mathcal{P} = \{\mathcal{E}_\alpha\}_\alpha$ of A, and* Homeo(S^1)*-valued random variables $\{w'_i\}_{i=0,\dots,\lfloor n/2 \rfloor}, \{s'_i\}_{i=1,\dots,\lfloor n/2 \rfloor}$ such that the following hold:*

(1) $\mathbb{P}(A) \geq 1 - 0.6^n$.
(2) When restricted on each equivalence class $\mathcal{E} \in \mathcal{P}$, $w'_0, \dots, w_{\lfloor n/2 \rfloor}$ are each fixed maps and s'_i's are μ-i.i.d.s.
(3) On A, the following equality holds:

$$w_0 r_1 s_1 t_1 w_1 \dots r_n s_n t_n w_n = w'_0 s'_1 w'_1 \cdots s'_{\lfloor n/2 \rfloor} w'_{\lfloor n/2 \rfloor}.$$

Corollary 3.18 tells us that

$$\mathbb{P}\left(A := \left\{ (\mathbf{r}, \mathbf{s}, \mathbf{t}) \in (S^{\mathbb{Z}_{>0}})^3 : \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) > n/2 \right\} \right) \geq 1 - 0.6^n.$$

Next, we declare an equivalence relation on $(S^{\mathbb{Z}_{>0}})^3$ as follows:

$$\left[(\mathbf{r}, \mathbf{s}, \mathbf{t}) \sim'_n (\bar{\mathbf{r}}, \bar{\mathbf{s}}, \bar{\mathbf{t}}) \right] \Leftrightarrow \left[\begin{array}{c} r_i = \bar{r}_i \text{ and } t_i = \bar{t}_i \text{ for each } i \in \mathbb{Z}_{>0}, \\ \bar{s}_i = s_i \text{ unless } i \text{ is among the } n/2 \text{ smallest pivotal times of } P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \end{array} \right]$$

As observed in Lemma 3.11, changing the coordinate of $\mathbf{s}$ at a pivotal times does not change the set of pivotal times, and hence does not change the "$n/2$ smallest pivotal times". Therefore, $\sim_n$ is indeed an equivalence relation. Note that the cardinality of the set of pivotal times is constant across each equivalence class, so every equivalence class is either contained in A or disjoint from A. In other words, A is a (disjoint) union of some equivalence classes and $\sim_n$ restricts to an equivalence relation on A.

Next, fix a $\sim_n$-equivalence class $\mathcal{E}$ contained in A. Its all element share the n-th step set of pivotal times $P_n(\mathcal{E})$, which we denote by $\{i(1) < i(2) < \dots)\}$. Since we are assuming $\mathcal{E} \subseteq A$, there are at least $n/2$ elements of $P_n(\mathcal{E})$. We then construct

$$\begin{aligned}
w'_0 &:= W_{i(1)-1} r_{i(1)} = w_0 \cdot r_1 s_1 t_1 w_1 \cdots r_{i(1)-1} s_{i(1)-1} t_{i(1)-1} w_{i(1)} r_{i(1)}, \\
w'_l &:= t_{i(l)} w_{i(l)} W_{i(l)}^{-1} W_{i(l+1)-1} r_{i(l+1)} \\
&= t_{i(l)} w_{i(l)} \cdot r_{i(l)+1} s_{i(l)+1} t_{i(l)+1} w_{i(l)+1} \cdots r_{i(l+1)-1} s_{i(l+1)-1} t_{i(l+1)-1} w_{i(l+1)} r_{i(l+1)}, \quad (l = 1, \dots, \lfloor n/2 \rfloor) \\
w'_{\lfloor n/2 \rfloor} &:= t_{i(\lfloor n/2 \rfloor)} w_{i(\lfloor n/2 \rfloor)} W_{i(\lfloor n/2 \rfloor)}^{-1} W_n \\
&= t_{i(\lfloor n/2 \rfloor)} w_{i(\lfloor n/2 \rfloor)} \cdot r_{i(\lfloor n/2 \rfloor)+1} s_{i(\lfloor n/2 \rfloor)+1} t_{i(\lfloor n/2 \rfloor)+1} w_{i(\lfloor n/2 \rfloor)+1} \cdots r_m s_n t_n w_n.
\end{aligned}$$

The definition of $\sim_n$ tells us that the maps $w'_0, w'_1, \dots, w'_M$ are fixed throughout $\mathcal{E}$. Moreover, we observed in Lemma 3.6 that $w'_l \mathcal{I} \subseteq \mathcal{I}$ holds for $l = 1, \dots, M$. Furthermore, $s'_l := s_{i(l)}$'s are μ-i.i.d.s when restricted on $\mathcal{E}$. The equality

$$w'_0 s'_1 w'_1 \cdots s'_{\lfloor n/2 \rfloor} w'_{i(M)} = w_0 r_1 s_1 t_1 w_1 \cdots r_n s_n t_n w_n$$

is clear on $\mathcal{E}$. This ends the proof. □

References

[Cho22] Inhyeok Choi. Random walks and contracting elements I: Deviation inequality and limit laws. *arXiv preprint arXiv:2207.06597v2*, 2022.

[Ghy01] Étienne Ghys. Groups acting on the circle. *Enseign. Math. (2)*, 47(3-4):329–407, 2001.

[Gou22] Sébastien Gouëzel. Exponential bounds for random walks on hyperbolic spaces without moment conditions. *Tunis. J. Math.*, 4(4):635–671, 2022.

[GV24] Martín Gilabert Vio. Probabilistic tits alternative for circle diffeomorphisms. *arXiv preprint arXiv:2412.08779*, 2024.

[Mal17] Dominique Malicet. Random walks on Homeo(S^1). *Comm. Math. Phys.*, 356(3):1083–1116, 2017.

[Mar00] Gregory Margulis. Free subgroups of the homeomorphism group of the circle. *C. R. Acad. Sci. Paris Sér. I Math.*, 331(9):669–674, 2000.

Cornell University, 310 Malott Hall, Ithaca, New York, 14850, USA
Email address: inhyeokchoi48@gmail.com