Silhouettes and generic properties of subgroups of the modular group

Frédérique Bassino, `bassino@lipn.fr`

Université Sorbonne Paris Nord, LIPN, CNRS UMR 7030, F-93430 Villetaneuse, France

Cyril Nicaud, `cyril.nicaud@u-pem.fr`

LIGM, Univ Gustave Eiffel, CNRS, ESIEE Paris, F-77454, Marne-la-Vallée, France

Pascal Weil, `pascal.weil@labri.fr`

Univ. Bordeaux, LaBRI, CNRS UMR 5800, F-33400 Talence, France[*]

CNRS, ReLaX, UMI 2000, Siruseri, India

February 26, 2021

Abstract

We show how to count and randomly generate finitely generated subgroups of the modular group $\mathsf{PSL}_2(\mathbb{Z})$ of a given isomorphism type. We also prove that almost malnormality and non-parabolicity are negligible properties for these subgroups.

The combinatorial methods developed to achieve these results bring to light a natural map, which associates with any finitely generated subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ a graph which we call its silhouette, and which can be interpreted as a conjugacy class of free finite index subgroups of $\mathsf{PSL}_2(\mathbb{Z})$.

1 Introduction

The modular group $\mathsf{PSL}_2(\mathbb{Z})$ has played a central role in algebra, number theory and geometry since the late 19th century, notably the study of its subgroups.

A number of papers have concentrated on its finite index subgroups, with exact enumeration results for the index n subgroups and results on the asymptotic behavior of that number as n tends to infinity (Dey, Stothers, Muller, Schlage-Puchta and others, see *e.g.* [9, 31, 26]). Here, we deal instead with *all* finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$.

There are two main sets of results in this paper:

(R1) enumeration and random generation results for finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ of a given size and isomorphism type;

---

[*]LaBRI, Univ. Bordeaux, 351 cours de la Libération, 33400 Talence, France.

(R2) proofs that almost malnormality is negligible and parabolicity is generic for finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$.

Let us first make the notions underlying these two sets of results more explicit.

Recall that $\mathsf{PSL}_2(\mathbb{Z})$ is the free product of a copy of $\mathbb{Z}_2$ and a copy of $\mathbb{Z}_3$. By Kurosh's theorem (see, *e.g.*, [20, 21, 28]), any finitely generated subgroup H of $\mathsf{PSL}_2(\mathbb{Z})$ is isomorphic to a free product of ℓ_2 copies of $\mathbb{Z}_2$, ℓ_3 copies of $\mathbb{Z}_3$ and r copies of $\mathbb{Z}$: the *isomorphism type* of H mentioned in (R1) is the triple (ℓ_2, ℓ_3, r). As for results (R2), we remind the reader that H is *almost malnormal* if $H \cap H^x$ is finite for every $x \notin H$; it is *parabolic* if it contains a parabolic element, that is, a conjugate of a non-trivial power of ab, where a and b are the generators of the order 2 and order 3 free factors, respectively.

In addition, both sets of results refer implicitly to a distribution of probabilities on the set of finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$, that we now explain. Each finitely generated subgroup H of $\mathsf{PSL}_2(\mathbb{Z})$ can be represented uniquely by a finite labeled graph $\Gamma(H)$, called its *Stallings graph*. Stallings graphs, and their effective construction, were first introduced by Stallings [30] to represent finitely generated subgroups of free groups. The idea of using finite graphs to represent subgroups of infinite, non-free groups first appeared in work of Arzhantseva and Ol'shanskii [2, 1], Gitik [15] and Kapovich [18]. Markus-Epstein [25] gave an explicit construction associating a graph with each subgroup of an amalgamated product of two finite groups, which is very close to the one used here. Here we follow the definition and construction of Kharlampovich et al. [19]. In a nutshell, the Stallings graph of a subgroup H of $\mathsf{PSL}_2(\mathbb{Z})$ is the fragment of the Schreier (or coset) graph of H, spanned by the loops at vertex H labeled by a geodesic representative of an element of H, see Section 2.

We take the number of vertices of $\Gamma(H)$ to be the *size* of the subgroup H. In particular, there are only finitely many subgroups of a given size and we assume the uniform distribution on this finite set. A property of subgroups is *negligible* (resp. *generic*) if the proportion of size n subgroups with the property tends to 0 (resp. 1) when n tends to infinity.

Note that this randomness model strongly differs from those considered by Gilman *et al.* in [14] for subgroups of hyperbolic groups and by Maher and Sisto [23] for subgroups of acylindrically hyperbolic groups. Roughly speaking, these models rely on fixing an integer k, randomly choosing k elements of G using an n-step Markovian mechanism, considering the subgroup generated by these k elements, and letting n tend to infinity. It is interesting to note that in this *few generators* model, almost malnormality is generic [23, Theorem 1.1(2)], in contrast with our model. A similar situation is already known to arise for subgroups of free groups: in the k-generated model, malnormality is generic (Jitsukawa [17]), whereas in the so-called graph-based model, it is negligible (Bassino *et al.* [3]). Jitsukawa's result was extended also to the Gromov density model, where the number k of generators is allowed to vary as an exponential function of n (Bassino *et al.* [5]). One can argue that the model we consider in this paper is particularly natural since Stallings

graphs are in bijection with subgroups.

We now return to the contributions of this paper. In [7], the authors counted the finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ by size and they showed how to generate uniformly at random a subgroup of a given size. They also computed the average value of the isomorphism type of a random subgroup as a function of its size and proved a large deviations theorem for this isomorphism type. It follows that randomly generating a size n subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ will, with high probability, yield a subgroup whose isomorphism type is close to the average value. In particular, this algorithmic result does not help generate uniformly at random subgroups of a given size and isomorphism type.

In this paper, we use a completely different enumeration method for finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$, to get a polynomial time random generation algorithm for subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ of a given size and isomorphism type (Results (R1)). This is done by a combination of graph decomposition techniques and analytic combinatorics methods [10], involving graph operations on Stallings graphs and exponential generating series.

A construction which occurs naturally in the proofs of these results is what we call the *silhouetting* of the Stallings graph of a finitely generated subgroup of $\mathsf{PSL}_2(\mathbb{Z})$. It consists in a sequence of "simplifications" of the graph, leading (except in extremal cases) to a uniform degree loop-free graph, which represents a conjugacy class of finite index, free subgroups of $\mathsf{PSL}_2(\mathbb{Z})$. A remarkable, and somewhat surprising property is that the silhouetting construction preserves uniformity. More precisely, among the size n subgroups whose silhouette has size s, every size s silhouette graph is equally likely.

This property allows us to lift asymptotic properties of silhouette graphs, which are more easily understood, to all Stallings graphs of finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$. This leads to Results (R2), namely the negligibility of almost malnormality and the genericity of parabolicity. The proof of these results is of a combinatorial nature, and rather intricate.

We would like to point out in particular an intermediate result which may be of independent interest. We show that, with high probability, in a finite group of permutations generated by a pair of fixpoint-free permutations (σ_2, σ_3), of order 2 and 3 respectively, the composition $\sigma_2\sigma_3$ admits orbits of a certain, relatively small size (Proposition 6.3). Obtaining such results on the composition of two randomly chosen mappings is notoriously difficult. It is, for instance, a bottleneck in the study of the properties of random deterministic automata [27]. Most known results rely on a fine grain independent analysis of the mappings, but we know very little on their composition. Character theory has been used to tackle this kind of difficulties in the study of combinatorial maps [16, 12]: this approach yields enumeration results on triplets $(\sigma_1, \sigma_2, \tau)$ such that $\sigma_1 \circ \sigma_2 = \tau$, but for a fixed cyclic type of τ only, and it seems very difficult to exploit such results for our purposes (see also [8]).

We note that, while there are a good number of results in the literature about the genericity or negligibility of certain properties of subgroups of free groups ([17, 3, 4, 5, 6]), there are precious few such results for subgroups of other groups. We can cite in this

3

direction, for their pioneering methods, the results of Arzhantseva and Ol'shanskii [2] who show for instance that, for a very large (generic) class of r-generator, k-relator presentations (r, k fixed), all ℓ-generated subgroups ($\ell < r$) are free and quasi-convex; and the results mentioned above of Gilman *et al.* [14] and Maher and Sisto [23] on k-generated subgroups of a fixed hyperbolic or acylindrically hyperbolic group. To our knowledge, our results (R2) on almost malnormality and parabolicity for subgroups of the modular group are the first that are based on the distribution of subgroups given by Stallings graphs.

The paper is organized as follows. Readers can find in Section 2 the precise definitions of the Stallings graph of a subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ and its combinatorial type, and results from the literature relating this combinatorial information with algebraic properties of the subgroup such as its isomorphism type, its index or its freeness.

Section 3 introduces combinatorial operations on Stallings graphs. Iterating these operations is a confluent process, which leads to the so-called *silhouette* of the given graph or subgroup. We show there that silhouetting preserves uniformity (Theorems 3.4 and 3.9), and that the size of the silhouette of a size n subgroup is super-polynomially generically at least $n - 3n^{\frac{2}{3}}$ (Propositions 3.4 and 3.10). Also, silhouetting preserves the free rank component of the isomorphism type of a subgroup (Proposition 3.3).

In Section 4, we exploit a fine description of the operations defined in Section 3 to give exact counting formulas for the number of subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ of a given combinatorial or isomorphism type. A key ingredient here, namely the pointing operation on exponential generating series, is borrowed from the toolbox of analytic combinatorics [10].

Section 5 uses the operations from Section 3 in a different way to formulate an algorithm (which includes a rejection algorithm component) to generate uniformly at random a subgroup of a given size and isomorphism type.

The last section, Section 6, shows that, generically, subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ contain parabolic elements (Corollary 6.2) and fail to be almost malnormal (Theorem 6.4). Both results exploit the statistical result on the existence of cycles labeled by non-trivial powers of ab (where a and b are the order 2 and order 3 generators of $\mathsf{PSL}_2(\mathbb{Z})$) in the Stallings graph of a subgroup mentioned above (Proposition 6.3).

To conclude this introductory section, we note that, according to the results presented here, the silhouetting operation is combinatorially and asymptotically significant in the study of finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$. We are able to lift a statistical property of silhouette graphs to the class of all $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs, and it would be interesting to see what other properties can be lifted in that fashion. In addition, we think that the silhouetting operation also has a topological, or possibly a geometric interpretation, even for finite index subgroups, and we would be curious about its properties.

2 Preliminaries

We work with the following presentation of the modular group:

$$\mathsf{PSL}_2(\mathbb{Z}) = \langle a, b \mid a^2 = b^3 = 1 \rangle.$$

The elements of $\mathsf{PSL}_2(\mathbb{Z})$ are represented by words over the alphabet $\{a, b, a^{-1}, b^{-1}\}$. Since $a^{-1} = a$ in $\mathsf{PSL}_2(\mathbb{Z})$, we can eliminate the letter a^{-1} from this alphabet. Each element of $\mathsf{PSL}_2(\mathbb{Z})$ then has a unique shortest (or *normal*, or *geodesic*) representative, which is a freely reduced word without factors in $\{a^2, b^2, b^{-2}\}$. That is, the normal representatives are the words of length at most 1 and the words alternating letters a and letters in $\{b, b^{-1}\}$.

The *Schreier graph* (or *coset graph*) of a subgroup H of $\mathsf{PSL}_2(\mathbb{Z})$ is the graph whose vertices are the cosets Hg of H ($g \in \mathsf{PSL}_2(\mathbb{Z})$), with an a-labeled edge from Hg to Hga and a b-labeled edge from Hg to Hgb, for every $g \in G$. We think of b-edges as 2-way edges, reading b in the forward direction and b^{-1} in the backward direction. Since $a = a^2$, there is an a-edge from vertex v to vertex v' if and only there is one from v' to v: as a result, we think of the a-edges as undirected edges, that can be traveled in either direction, each time reading a.

Note that a word is in H if and only if it labels a loop at vertex $v_0 = H$ in the Schreier graph of H. The *Stallings graph* of H, written $(\Gamma(H), v_0)$, is the fragment of the Schreier graph of H spanned by the loops at v_0 reading the geodesic representatives of the elements of H, rooted at v_0. In particular, a word is in H if and only if its geodesic representative labels a loop in $\Gamma(H)$ at vertex v_0. We refer the reader to Remark 2.2 and to [19] for more details on these graphs. We note in particular that H has a finite Stallings graph if and only if it is finitely generated, and that $\Gamma(H)$ is efficiently algorithmically computable if H is given by a finite set of generators (words on the alphabet $\{a, b, b^{-1}\}$) [19, 7].

Example 2.1 Figure 1 shows examples of Stallings graphs. □

Remark 2.2 The definition of Stallings graphs given above is a generalization of that introduced by Stallings in 1983 [30] for finitely generated subgroups of free groups, and a particular instance of the definition first introduced by Gitik [15] in 1996 under the name of geodesic core, and systematized by Kharlampovich *et al.* [19] in 2017. Given a finitely presented group $G = \langle A \mid R \rangle$, a language L of representatives for G (a set of words over the alphabet $A \cup A^{-1}$) and a subgroup H, one considers the fragment of the Schreier graph of H spanned by the L-representatives of the elements of H. It is effectively computable if G is equipped with an automatic structure [19]. In the particular case where $G = \mathsf{PSL}_2(\mathbb{Z})$, the algorithm is quite straightforward, we refer the reader to [7] for an outline.

This notion is not the first usage of graphs (or automata-theoretic representations, see Gersten and Short [13, 29]) to reason about subgroups of infinite groups: in 1996, Arzhantseva and Ol'shanskii [2] used graphs with great success to investigate the subgroups of an exponentially generic class of k-relator groups; the same year, Kapovich [18] used

Figure 1: Top: the Stallings graphs of the subgroups $H = \langle abab^{-1}, babab \rangle$ and $K = \langle abab, babab^{-1} \rangle$ of $\mathsf{PSL}_2(\mathbb{Z})$. Bottom: the Stallings graph of $L = \langle (b^{-1}a)^2 bab, b^{-1}(ab)^2 ab^{-1}ab, (abab^{-1})^2, (ba)^2 b^{-1}a(ba)^3 b^{-1}a, (ab)^8 ab^{-1}a \rangle$. In each case, the root is the vertex labeled 1.

a different approach to compute the quasi-convexity constant of subgroups of automatic groups. However, the systematic approach and the unique representation provided by Stallings graphs are extremely fruitful in tackling decision and computability problems, see [19], or enumeration problems [7].

The particular case of interest here, namely the free product of two finite groups, was investigated from an algorithmic point of view in 2007 by Markus-Epstein [25]. The graphs she computes are different from (and a little larger than) the ones we consider here, because the language L of representatives she uses strictly contains the language of geodesics. $\square$

It is immediate from the definition of Stallings graphs that the a-edges (resp. b-edges) of $\Gamma(H)$ form a partial, injective map on the vertex set of the graph. Moreover, because $a^2 = b^3 = 1$, distinct a-edges are never adjacent to the same vertex: we distinguish therefore a-loops and so-called *isolated a-edges*. Similarly, if we have two consecutive b-edges, say from v_1 to v_2 and from v_2 to v_3, then $\Gamma(H)$ also has a b-edge from v_3 to v_1. Thus the b-edges are either loops, or *isolated b-edges*, or part of a b-triangle. Finally, every vertex except maybe the root vertex is adjacent to an a- and to a b-edge.

A rooted graph satisfying these conditions is called *$PSL_2(\mathbb{Z})$-reduced* and it is not difficult to see that every finite $PSL_2(\mathbb{Z})$-reduced rooted graph is the Stallings graph of a unique finitely generated subgroup of $PSL_2(\mathbb{Z})$. That is, the mapping $H \mapsto (\Gamma(H), v_0)$ is a bijection between finitely generated subgroups of $PSL_2(\mathbb{Z})$ and $PSL_2(\mathbb{Z})$-reduced rooted graphs.

The *combinatorial type* of a $PSL_2(\mathbb{Z})$-reduced graph Γ is the tuple $(n, k_2, k_3, \ell_2, \ell_3)$ where n is the number of vertices of Γ, k_2 and k_3 are the numbers of isolated a- and b-edges, and ℓ_2 and ℓ_3 are the numbers of a- and b-loops. We sometimes talk of the combinatorial type of a subgroup to mean the combinatorial type of its Stallings graph, and we refer to n (the number of vertices of a $PSL_2(\mathbb{Z})$-reduced graph) as the *size* of the graph or even the size of the subgroup. See [7] for a discussion of the possible combinatorial types.

An edge-labeled graph Γ is said to be *$PSL_2(\mathbb{Z})$-cyclically reduced* if it is $PSL_2(\mathbb{Z})$-reduced when rooted at every one of its vertices. We also say that a finitely generated subgroup of $PSL_2(\mathbb{Z})$ is $PSL_2(\mathbb{Z})$-cyclically reduced if its Stallings graph is. In that case, the combinatorial type $(n, k_2, k_3, \ell_2, \ell_3)$ satisfies the following constraints: $n = 2k_2 + \ell_2 = 2k_3 + \ell_3 + 3m$ where m is the number of b-triangles.

Let us also record the following results (see, *e.g.*, [7]).

Proposition 2.3 *A subgroup $H \leq PSL_2(\mathbb{Z})$ has finite index if and only if its Stallings graph is $PSL_2(\mathbb{Z})$-cyclically reduced and has combinatorial type of the form $(n, k_2, 0, \ell_2, \ell_3)$. It is free if and only if its combinatorial type is of the form $(n, k_2, k_3, 0, 0)$.*

Proper free $PSL_2(\mathbb{Z})$-cyclically reduced subgroups have even size, and proper free and finite index subgroups have size a positive multiple of 6.

By Kurosh's classical theorem on subgroups of free groups (*e.g.*, [21, Proposition III.3.6]), a subgroup H of $PSL_2(\mathbb{Z})$ is isomorphic to a free product of r_2 copies of $\mathbb{Z}_2$, r_3

copies of $\mathbb{Z}_3$ and a free group of rank r, for some non-negative integers r_2, r_3, r. The triple (r_2, r_3, r), which characterizes H up to isomorphism (but not up to an automorphism of $\mathsf{PSL}_2(\mathbb{Z})$) is called the *isomorphism type* of H. We record the following connection between the combinatorial and the isomorphism types of a subgroup [7, Proposition 2.9].

Proposition 2.4 *Let H be a subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ of size at least 2 and let $(n, k_2, k_3, \ell_2, \ell_3)$ be the combinatorial type of $\Gamma(H)$.*

If $\Gamma(H)$ is $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced, the isomorphism type of H is

$$(\ell_2, \ell_3, 1 + \frac{n - 2k_3 - 3\ell_2 - 4\ell_3}{6}).$$

If $\Gamma(H)$ is not $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced, the isomorphism type of H is

$$(\ell_2, \ell_3, \frac{1}{3} + \frac{n - 2k_3 - 3\ell_2 - 4\ell_3}{6}) \quad \textit{if the base vertex is adjacent to an a-edge}$$
$$(\ell_2, \ell_3, \frac{2}{3} + \frac{n - 2k_3 - 3\ell_2 - 4\ell_3}{6}) \quad \textit{if the base vertex is adjacent to a b-edge.}$$

One of our objectives in this paper is to count subgroups by isomorphism type or by combinatorial type. Since subgroups are in bijection with $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graphs (their Stallings graphs), it is equivalent to count these graphs. For technical reasons, it is easier to count *labeled graphs*, that is, graphs whose vertex set is equipped with a (labeling) bijection onto a set of the form $[n] = \{1, \ldots, n\}$. The graphs in Figure 1 are in fact labeled graphs.

The prefered tool to count and randomly generate labeled structures (graphs or rooted graphs in this paper) is the theory of exponential generating series (EGS), to which we can apply the powerful tools of analytic combinatorics, see [10]. More details are introduced where they are needed.

Example 2.5 The $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs Γ with 1 or 2 vertices are represented in Figure 2. There is only one with 1 vertex, and three with 2 vertices. Two of them can be labeled in two different ways while the third one admits only one labeling. □
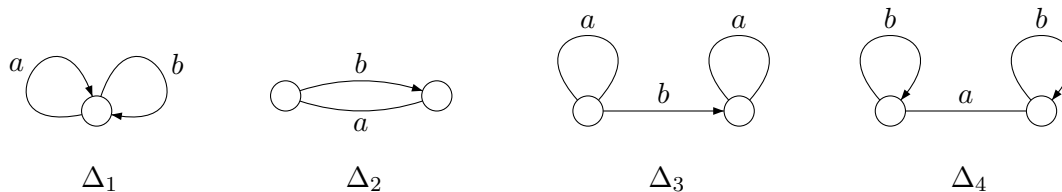

Figure 2: All $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs with at most 2 vertices.

8

3 Moves on $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs and silhouette of a subgroup

We will see in Section 4.1 below that counting and randomly generating subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ reduces to counting and randomly generating labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs. Before we embark on this task, we introduce a combinatorial construction on this class of graphs.

More precisely, we define in Section 3.1 a number of moves on a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph, depending on its geometry. They are used in Section 3.2 to identify an interesting structure within a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph, namely its *silhouette*. They will later be used in Section 4.2 to count subgroups of $\mathsf{PSL}_2(\mathbb{Z})$ and in Section 5 to randomly generate them.

Sections 3.3 and 3.4 discuss technical properties of the silhouetting operation, which will be used in Section 6 to establish certain asymptotic properties of subgroups of $\mathsf{PSL}_2(\mathbb{Z})$.

Finally, we examine in Section 3.5 how the silhouetting operation can be extended to all subgroups of $\mathsf{PSL}_2(\mathbb{Z})$, even if not $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced.

3.1 Moves on a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph

Here we define so-called λ_3-, $\lambda_{2,1}$-, $\lambda_{2,2}$-, κ_3- and exc-moves on quasi-labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs (see below for the definition of quasi-labeled structures).

Each of these moves deletes vertices from the input graph, so that the resulting graph has an injective labeling function (defined on the vertex set) which is into, but possibly not onto, a set of the form $[n]$. We then talk of a *quasi-labeled* graph. It is clear that a quasi-labeled graph Γ can be canonically relabeled (by a uniquely defined order-preserving map) into a properly labeled graph, which we write $\mathrm{norm}(\Gamma)$.

If Γ is a quasi-labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph, we also introduce the notion of *rank* of an isolated a-edge. Note that these edges are totally ordered by comparing the minimum label of one of their end vertices. We say that an isolated a-edge e has rank $i \geq 1$ if there are exactly $i - 1$ isolated a-edges that are less than e.

Let Γ be a quasi-labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph, with combinatorial type τ. To lighten up the description of the moves we define on Γ, we abusively identify the vertices of Γ with their labels. We also abusively write Δ_i ($i = 1, 2, 3, 4$) for any quasi-labeled version of the graphs in Example 2.5.

λ_3-moves   Let ℓ be a b-loop in Γ, say at vertex v (in fact, at the vertex labeled v). Then we are in exactly one of the following situations.

(1) v is adjacent to an isolated a-edge, connecting it with a vertex $w \neq v$.

(2) vertex v carries an a-loop; in that case, $\Gamma = \Delta_1$.
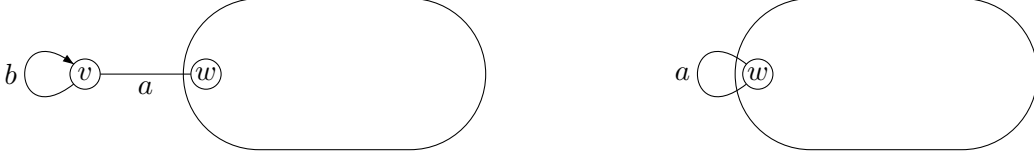
9

Figure 3: The graphs Γ and Δ in Case (1)

In Case (1), the (λ_3, v, w)-*move* consists in deleting vertex v and the adjacent edges, and adding an a-loop ℓ' at vertex w. The resulting quasi-labeled graph Δ (see Figure 3) is $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph and has combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_3$, where $\boldsymbol{\lambda}_3 = (-1, -1, 0, 1, -1)$.

Note that the pair (Γ, ℓ) can be retrieved unequivocally from Δ and the triple (λ_3, v, w) — provided that the quasi-labeled graph Δ has no vertex v, has a vertex w and has an a-loop at w, we say that Δ is *valid for* (λ_3, v, w).

Switching to labeled graphs (namely $\mathrm{norm}(\Gamma)$ and $\mathrm{norm}(\Delta)$), we note that λ_3-moves in general establish a bijection between the set of structures (Γ, ℓ) that arise from Case (1) with Γ (properly) labeled, of size n and combinatorial type $\boldsymbol{\tau}$, and the set of structures (Δ, ℓ', v) formed by a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ with combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_3$, an a-loop ℓ' in Δ and an integer $v \in [n]$.

No move is defined in Case (2).

λ_2-moves   Let ℓ be an a-loop in Γ, say at vertex v. Then we are in exactly one of the following situations.

(1) vertex v sits on a b-triangle (equivalently: it does not carry a b-loop, and it has an incoming and an outgoing b-edge).

(2) vertex v is adjacent to an isolated b-edge, linking it with a vertex $w \neq v$, which in turn is adjacent to an isolated a-edge linking it with a third vertex $w' \neq v, w$.

(3) vertex v is adjacent to an isolated b-edge, linking it with a vertex $w \neq v$, which carries an a-loop; in that case $\Gamma = \Delta_3$.

(4) vertex v carries a b-loop; in that case, $\Gamma = \Delta_1$.

In Case (1), let w and w' be the other extremities of the b-edges ending and starting at v, respectively. Then $w \neq w'$ and Γ has a (non-isolated) b-edge from w to w'. The $(\lambda_{2,1}, v, w')$-move consists in removing from Γ vertex v and the adjacent edges (the a-loop ℓ and two b-edges). The resulting graph Δ (see Figure 4) is $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced, it has an isolated b-edge from w' to w and combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,1}$, where $\boldsymbol{\lambda}_{2,1} = (-1, 0, 1, -1, 0)$.

Here too, the pair (Γ, ℓ) can be retrieved unequivocally from Δ and the triple $(\lambda_{2,1}, v, w')$ — provided that the quasi-labeled graph Δ has no vertex v, has a vertex w' and has an isolated b-edge starting at w', we say that Δ is *valid for* $(\lambda_{2,1}, v, w')$.
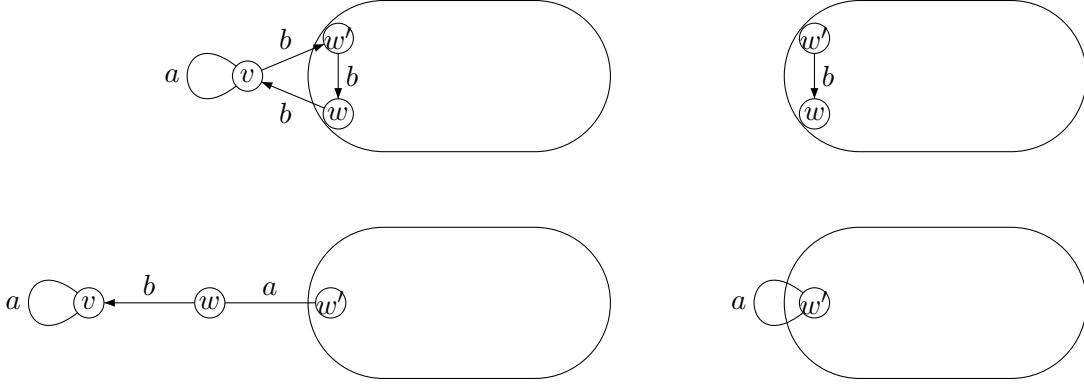
10

Figure 4: The labeled graphs Γ and Δ in Cases (1) and (2)

In particular, $\lambda_{2,1}$-moves establish a bijection between the set of structures (Γ, ℓ) that arise from Case (1) with Γ (properly) labeled, of size n and combinatorial type $\boldsymbol{\tau}$, and the set of structures (Δ, e', v) formed by a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ with combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,1}$, an isolated b-edge e' in Δ and an integer $v \in [n]$.

In Case (2), the $(\lambda_{2,2}, v \to w, w')$-move (resp. $(\lambda_{2,2}, v \leftarrow w, w')$, depending on the orientation of the b-edge adjacent to v) consists in deleting from Γ the vertices v and w and the edges adjacent to them, and adding an a-loop ℓ' at w'. The resulting graph Δ (see Figure 4) is $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced and has combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,2}$, where $\boldsymbol{\lambda}_{2,2} = (-2, -1, -1, 0, 0)$.

Here, the pair (Δ, ℓ') and the triple $(\lambda_{2,2}, v \to w, w')$ (resp. $(\lambda_{2,2}, v \leftarrow w, w')$) specify uniquely the input pair (Γ, ℓ) – provided that Δ is *valid for* $(\lambda_{2,2}, v, w, w')$, namely that Δ has no vertices v or w and has an a-loop at a vertex w'. Note that this validity allows reversing both a $(\lambda_{2,2}, v \to w, w')$-move and a $(\lambda_{2,2}, v \leftarrow w, w')$-move, yielding different quasi-labeled graphs Γ.

It follows that $\lambda_{2,2}$-moves establish a bijection between the set of structures (Γ, ℓ) that arise from Case (2) with Γ (properly) labeled, of size n and combinatorial type $\boldsymbol{\tau}$, and the set of structures $(\Delta, \ell', v, w, \varepsilon)$ formed by a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ with combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,2}$, an a-loop ℓ' in Δ, distinct integers $v, w \in [n]$ and a boolean ε (to account for the choice between a $(\lambda_{2,2}, v \to w, w')$- and a $(\lambda_{2,2}, v \leftarrow w, w')$-move).

No λ_2-move is defined in Cases (3) and (4).

κ_3-moves Let e be an isolated b-edge in Γ, say from vertex v to vertex $w \neq v$. Then we are in exactly one of the following situations.

(1) Vertices v and w are adjacent to isolated a-edges, linking them respectively to vertices v' and w', and v, w, v', w' are pairwise distinct.

(2) Exactly one of the v and w is adjacent to an a-loop.

11

(3) Vertices v and w are adjacent to the same isolated a-edge; in this case $\Gamma = \Delta_2$.

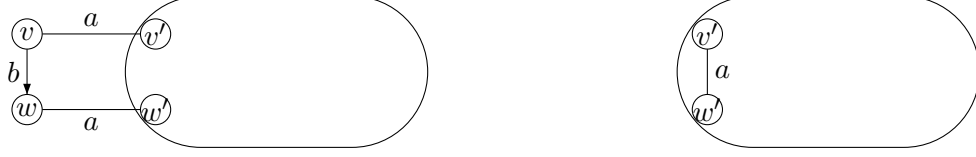(4) Vertices v and w are both adjacent to an a-loop; in that case, $\Gamma = \Delta_3$.

Figure 5: The labeled graphs Γ and Δ in Case (1)

In Case (1), deleting vertices v and w and the edges adjacent to them, and adding an a-edge e' between the v' and w' yields a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ with combinatorial type $\boldsymbol{\tau} + \boldsymbol{\kappa}_3$, where $\boldsymbol{\kappa}_3 = (-2, -1, -1, 0, 0)$. If i is the rank of the isolated a-edge e' in Δ, this move is called $(\kappa_3, v, w, i, -)$ if $v' < w'$ and $(\kappa_3, v, w, i, +)$ if $w' < v'$.

Again, the pair (Δ, e') and the tuple $(\kappa_3, v, w, i, -)$ (resp. $(\kappa_3, v, w, i, +)$) uniquely specify (Γ, e) — provided that Δ is *valid for* (κ_3, v, w, i), that is, has no vertex v or w and has at least i isolated a-edges. Here as for $\lambda_{2,2}$-moves, the same validity condition allows reversing a $(\kappa_3, v, w, i, -)$-move and a $(\kappa_3, v, w, i, +)$-move, yielding different quasi-labeled graphs Γ.

Thus κ_3-moves establish a bijection between the set of structures (Γ, e) arising from Case (1) with Γ labeled, of size n and combinatorial type $\boldsymbol{\tau}$, and the set of structures $(\Delta, e', v, w, \varepsilon)$ formed by a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ of combinatorial type $\boldsymbol{\tau} + \boldsymbol{\kappa}_3$, an isolated a-edge e' in Δ, distinct integers v and w in $[n]$ and a boolean ε (to distinguish the cases where (Δ, e') arises from a $(\kappa_3, v, w, i, -)$- or a $(\kappa_3, v, w, i, +)$-move).

No κ_3-move is defined in Cases (2), (3) and (4). Observe that, in Case (2), a $\lambda_{2,2}$-move is defined.

Remark 3.1 The description of κ_3-moves may seem unnaturally complicated, refering as it does to the rank of the isolated a-edge between v' and w', rather than to these vertices themselves. This encoding allows us to invert a κ_3-move in a unique fashion as long as we operate on a graph that is valid for it (a property that is determined by its set of vertex labels and its combinatorial type). This is used in a crucial manner in Section 6. $\square$

exc moves For completeness, we also introduce a last, exceptional category of moves, which can be applied only to a quasi-labeled version of Δ_3, turning it into a quasi-labeled version of Δ_1. More precisely, if the b-edge in Δ_3 goes from vertex v to vertex w, the $\mathsf{exc}(w)$-move returns Δ_1 where the only vertex is labeled v. This move can be seen as a degenerate version of a $\lambda_{2,2}$-move. To handle this move like the others, it modifies the combinatorial type by the addition of $\boldsymbol{exc} = (-1, 0, -1, -1, 1)$, the difference between the combinatorial types of Δ_1 and Δ_3.

12

3.2 Silhouette of a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph

In general, several moves can be applied to a quasi-labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Γ. However, the end result of a maximal sequence of λ_3-, $\lambda_{2,1}$-, $\lambda_{2,2}$- and κ_3- and exc-moves, in any order, yields the same quasi-labeled graph. Indeed, if two distinct moves are possible, then they modify the $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph in two disjoint areas which therefore do not interfere with one another: whichever move is performed first, the second one can be performed afterwards. There are however three exceptions.

(1) If a b-triangle carries exactly two a-loops, then two $\lambda_{2,1}$-moves are possible and once one is performed, the other cannot be; but then a $\lambda_{2,2}$-move (or, in a degenerate case, an exc-move) is possible and both options lead to the same quasi-labeled graph after that additional move.

(2) If Γ is a b-triangle with three a-loops, three $\lambda_{2,1}$-moves are possible, each preserving a different b-edge and yielding a different quasi-labeled version of Δ_3. We decide to keep the b-edge with maximal start vertex, say v. The next move can only be an exc-move, leading to the v-labeled version of Δ_1.

(3) If Γ is a cycle whose edges spell a word of the form $ab^{\varepsilon_1}ab^{\varepsilon_2}\cdots ab^{\varepsilon_n}$ where $\varepsilon_i = \pm 1$ for each i and $n \geq 2$, then every b-edge is isolated and the only possible moves are κ_3-moves. A maximal sequence of moves then eliminates all the b-edges but one, leading to a quasi-labeled version of Δ_2, with the labels corresponding to the b-edge of Γ that is not eliminated. We decide to keep the b-edge with maximal start vertex.

With this discussion in mind and if Γ is a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph, we define the *quasi-silhouette* $\mathsf{q\text{-}silh}(\Gamma)$ of Γ to be the quasi-labeled graph resulting from the application of a maximal sequence of moves, and the *silhouette* of Γ to be $\mathsf{silh}(\Gamma) = \mathsf{norm}(\mathsf{q\text{-}silh}(\Gamma))$.

Example 3.2 Consider the (labeled) Stallings graphs in Figure 1. The first is equal to its own silhouette. The (quasi-)silhouetting operation applied to the other ones lead to graphs shown in Figure 6. □
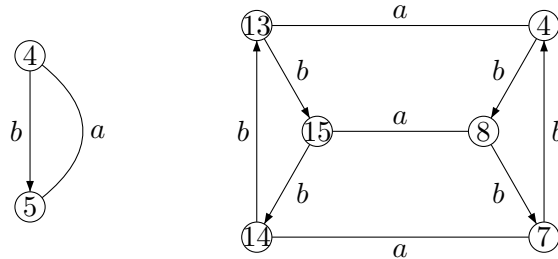

Figure 6: The (quasi-)silhouettes of the last two (labeled) Stallings graphs in Figure 1

If $\mathsf{silh}(\Gamma)$ is Δ_1 or Δ_2, we talk of a *small silhouette*. Otherwise, we talk of a *large silhouette*. We say that Γ is a *silhouette* graph if $\Gamma = \mathsf{silh}(\Gamma)$ and $\Gamma \neq \Delta_1, \Delta_2$. The combinatorial type of a silhouette graph is of the form $(n, n/2, 0, 0, 0)$ where n is a multiple of 6. Note that such a graph is the (unrooted) Stallings graph of a free finite index subgroup of $\mathsf{PSL}_2(\mathbb{Z})$, see Section 2.

The $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroups with small silhouette admit the following algebraic characterization.

Proposition 3.3 *Let H be a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroup of $\mathsf{PSL}_2(\mathbb{Z})$, with Stallings graph Γ and isomorphism type (ℓ_2, ℓ_3, r). If $\mathsf{silh}(\Gamma)$ has isomorphism type (ℓ_2', ℓ_3', r'), then $r = r'$. In particular $\mathsf{silh}(\Gamma) = \Delta_1$ (resp. Δ_2) if and only if $r = 0$ (resp. $r = 1$).*

Proof. Let $\boldsymbol{\tau}$ be the combinatorial type of Γ. Proposition 2.4 shows that the free rank r in the isomorphism type of H is a function of $\boldsymbol{\tau}$; more precisely, if $\boldsymbol{\tau} = (n, k_2, k_3, \ell_2, \ell_3)$, then $6(r - 1) = n - 2k_3 - 3\ell_2 - 4\ell_3 = \varphi(\boldsymbol{\tau})$, and we observe that φ is a linear map.

By construction, $\mathsf{silh}(\Gamma)$ is obtained from Γ by a succession of λ_3-, $\lambda_{2,1}$-, $\lambda_{2,2}$-, κ_3-moves and the exc-move. Each of these moves modifies the combinatorial type by adding to it the vector $\boldsymbol{\lambda}_3$, $\boldsymbol{\lambda}_{2,1}$, $\boldsymbol{\lambda}_{2,2}$, $\boldsymbol{\kappa}_3$ or $\boldsymbol{exc}$. Every one of these vectors lies in the kernel of φ, so the free rank component of the isomorphism types of Γ and $\mathsf{silh}(\Gamma)$ coincide.

It is immediate that this free rank component is 0 for Δ_1, 1 for Δ_2 and $1 + n/6 \geq 2$ for each silhouette graph of size n. The proposition follows immediately. $\square$

3.3 Silhouetting preserves uniformity

In Section 6.1, we will use the fact that taking the silhouette of a uniformly random labeled $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph results in a uniformly random labeled silhouette graph.

More precisely, for $1 \leq s \leq n$, let $\mathfrak{G}(n, s)$ be the set of size n labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs whose silhouette has s vertices. Let also $\mathfrak{D}(n, s)$ denote the set of quasi-silhouettes of the elements of $\mathfrak{G}(n, s)$, $\mathfrak{D}(n, s) = \{\mathsf{q\text{-}silh}(\Gamma) \mid \Gamma \in \mathfrak{G}(n, s)\}$. Note that the graphs in $\mathfrak{D}(n, s)$ are labeled by functions into $[n]$ and that $\mathfrak{D}(s, s)$ is the set of silhouettes of size s. We prove the following statement.

Theorem 3.4 *Let $1 \leq s \leq n$. If Γ is an element of $\mathfrak{G}(n, s)$ taken uniformly at random, then $\mathsf{silh}(\Gamma)$ is a uniformly random element of $\mathfrak{D}(s, s)$. That is: for any $\Delta, \Delta' \in \mathfrak{D}(s, s)$,*

$$\mathbb{P}(\mathsf{silh}(\Gamma) = \Delta) = \mathbb{P}(\mathsf{silh}(\Gamma) = \Delta'),$$

where Γ is the $\mathfrak{G}(n, s)$-valued random variable with uniform distribution.

To begin with, we note that there is exactly one possible silhouette of size 1 (resp. size 2), so the statement is trivially true for $s \leq 2$. We now assume that $s \geq 3$.

Now we observe that silhouette graphs that differ only by their labeling function have the same probability, as stated in Lemma 3.5 below. If Δ is a quasi-labeled graph with labels in $[n]$ and σ is a permutation of $[n]$, we let $\sigma(\Delta)$ be the graph obtained from Δ by relabeling its vertices according to σ.

Lemma 3.5 *Let $3 \le s \le n$, let $\Delta \in \mathfrak{D}(n,s)$ and let σ be a permutation of $[n]$, then*

$$\mathbb{P}(\textit{q-silh}(\Gamma) = \Delta) = \mathbb{P}(\textit{q-silh}(\Gamma) = \sigma(\Delta)),$$

where Γ is the $\mathfrak{G}(n,s)$-valued random variable with uniform distribution. In particular, $\mathbb{P}(\textit{q-silh}(\Gamma) = \Delta) = \mathbb{P}(\textit{q-silh}(\Gamma) = \mathrm{norm}(\Delta))$.

Proof. Let $\mathfrak{G}$ (resp. $\mathfrak{G}_\sigma$) be the set of graphs of $\mathfrak{G}(n,s)$ with quasi-silhouette Δ (resp. $\sigma(\Delta)$). We have

$$\mathbb{P}(\mathsf{q\text{-}silh}(\Gamma) = \Delta) = \frac{|\mathfrak{G}|}{|\mathfrak{G}(n,s)|},$$

so we only need to establish that $|\mathfrak{G}| = |\mathfrak{G}_\sigma|$.

The moves defined in Section 3.1 do not depend on labels, only on the relative order of labels. So any sequence of moves used to build the quasi-silhouette Δ from an element $\Gamma \in \mathfrak{G}$, can be applied identically on $\sigma(\Gamma)$. This shows that $\mathsf{q\text{-}silh}(\sigma(\Gamma)) = \sigma(\Delta)$ and, in particular, $\sigma(\Gamma) \in \mathfrak{G}_\sigma$.

As σ is a bijection on $\mathfrak{G}(n,s)$, it follows that $|\mathfrak{G}| \le |\mathfrak{G}_\sigma|$. The reverse inequality holds by symmetry and this concludes the proof. $\qquad\square$

Recall, from Section 3.1, that if a quasi-labeled graph Δ is valid for a move m, then there exists a unique quasi-labeled graph Γ such that m transforms Γ into Δ. This extends to a sequence of moves $M = m_t \cdots m_1$: we say that Δ is *valid for M* if there exists a quasi-labeled graph Γ such that applying m_t, then m_{t-1}, etc, yields Δ. In that case, Γ is uniquely determined by Δ and M and we write $\Gamma = M \cdot \Delta$.

We now define, given Γ, a canonical sequence of moves transforming Γ into its quasi-silhouette $\mathsf{q\text{-}silh}(\Gamma)$. More precisely, the *minimal move* on Γ is chosen as follows.

- If Γ has a b-loop, the minimal move is the unique move of the form (λ_3, v, w), where v is the least vertex carrying a b-loop.

- If Γ has an a-loop but no b-loop and $\Gamma \ne \Delta_3$, the minimal move is the unique move of the form $(\lambda_{2,1}, v, w)$, $(\lambda_{2,2}, v \to w, w')$ or $(\lambda_{2,2}, v \leftarrow w, w')$ where v is the least vertex carrying an a-loop.

- If Γ has no loop and $\Gamma \ne \Delta_2$, the minimal move is the possible move of the form $(\kappa_3, v, w, i, -)$ or $(\kappa_3, v, w, i, +)$ with v minimal.

- Finally, if $\Gamma = \Delta_3$, the minimal move is exc.

The *minimal sequence* of a graph Γ is formed by the minimal move on Γ, followed by the minimal sequence on the resulting quasi-labeled graph. Observe that no minimal move is defined on Γ if $\Gamma = \mathsf{silh}(\Gamma)$: in that case, the minimal sequence is the empty sequence ε. Thus, the minimal sequence of Γ describes a particular way to transform Γ into $\mathsf{q\text{-}silh}(\Gamma)$.

Let $\Delta \in \mathfrak{D}(s,s)$ be a size s labeled silhouette graph. Recall that, by Lemma 3.5, the probability that $\mathsf{q\text{-}silh}(\Gamma)$ is Δ is the same as the probability of any other quasi-silhouette normalizing to Δ. We establish the following statement.

Lemma 3.6 *Let $\Delta \in \mathfrak{D}(s,s)$. Let $\mathfrak{M}_n(\Delta)$ be the set of all minimal sequences of the elements of $\mathfrak{G}(n,s)$ whose quasi-silhouette is Δ. For Γ taken uniformly at random in $\mathfrak{G}(n,s)$, we have*

$$\mathbb{P}(\mathsf{q\text{-}silh}(\Gamma) = \Delta) = \frac{|\mathfrak{M}_n(\Delta)|}{|\mathfrak{G}(n,s)|}.$$

Proof. Every graph $\Gamma \in \mathfrak{G}(n,s)$ such that $\mathsf{q\text{-}silh}(\Gamma) = \Delta$ has a unique minimal sequence, which belongs to $\mathfrak{M}_n(\Delta)$. Conversely, as discussed above, every sequence in $\mathfrak{M}_n(\Delta)$ uniquely determines the graph in $\mathfrak{G}(n,s)$ from which it starts. $\qquad\square$

The next lemma is the cornerstone of the proof of Theorem 3.4.

Lemma 3.7 *Let $2 < s \leq n$ and let Δ and Δ' be labeled silhouette graphs of $\mathfrak{D}(s,s)$. Then $\mathfrak{M}_n(\Delta) = \mathfrak{M}_n(\Delta')$.*

Proof. Let $M = m_t m_{t-1} \ldots m_1$ be a minimal sequence in $\mathfrak{M}_n(\Delta)$. For $0 \leq i \leq t$, let $M_i = m_i \ldots m_1$ be the suffix of M of length i, with the convention that M_0 is the empty sequence. We verify by induction on i that

- Δ' is valid for M_i,

- $M_i \cdot \Delta$ and $M_i \cdot \Delta'$ use the same set of labels,

- v has a a-loop (resp. b-loop) in $M_i \cdot \Delta$ iff v has a a-loop (resp. b-loop) in $M_i \cdot \Delta'$,

- $v \to w$ is an isolated b-edge in $M_i \cdot \Delta$ iff $v \to w$ is an isolated b-edge in $M_i \cdot \Delta'$,

- $M_i \cdot \Delta$ and $M_i \cdot \Delta'$ have the same combinatorial type,

- if $i \geq 1$, m_i is the minimal move of $M_i \cdot \Delta'$.

These properties are true for $i = 0$, since $M_0\Delta = \Delta$ and $M_0\Delta' = \Delta'$: both are labeled by $[s]$, have no loop and no isolated b-edge, and have combinatorial type $(s, s/2, 0, 0, 0)$.

For the induction step, we observe that inverting a move removes and adds loops with the same labels and on the same vertices on both graphs, and it also removes and adds

16

the same isolated b-edges. The only difference that might occur is for κ_3 moves: the a-edge in the move's description is specified by its rank in the order on isolated a-edges and not by the labels of its vertices, but the combinatorial type of the quasi-labeled graph evolves the same way. This covers all the items to be proved except for the last one, about the minimality of move m_i. This last verification follows directly from the definition of a minimal move.

More precisely, we note that, by definition, m_i is the minimal move for $M_i \cdot \Delta$.

- If $m_i = (\lambda_3, v, w)$ then $M_i \cdot \Delta$ has a b-loop at vertex v and v is minimal such vertex. As the vertices with b-loops have the same labels in $M_i \cdot \Delta$ and $M_i \cdot \Delta'$, m_i is also the minimal move of $M_i \cdot \Delta'$.

- If m_i is of the form $(\lambda_{2,1}, v, w)$, $(\lambda_{2,2}, v \to w, w')$ or $(\lambda_{2,2}, v \leftarrow w, w')$-move, then $M_i \cdot \Delta$ has an a-loop, no b-loop, an isolated b-edge from v to w or the reverse (for a $\lambda_{2,2}$-move) and v is the minimal vertex with an a-loop. The same holds by induction for $M_i \cdot \Delta'$ and m_i is minimal for $M_i \cdot \Delta'$.

- Similarly, if m_i is of the form $(\kappa_3, v, w, i, -)$ or $(\kappa_3, v, w, i, +)$, then both $M_i\Delta$ and $M_i\Delta'$ are loop-free and m_i is minimal for $M_i\Delta'$.

- Finally, if $m_i = \mathsf{exc}$, then $M_i \cdot \Delta = \Delta_3$, $M_i \cdot \Delta'$ has the same combinatorial type and hence $M_i \cdot \Delta' = \Delta_3$.

Thus every sequence of $\mathfrak{M}_n(\Delta)$ is also in $\mathfrak{M}_n(\Delta')$. By symmetry, these two sets are equal. $\qquad\square$

Proof of Theorem 3.4. As indicated before, we may assume that $s > 2$. Let Δ, Δ' be labeled size s silhouette graphs. We have

$$\mathbb{P}(\mathsf{silh}(\Gamma) = \Delta) = \sum \mathbb{P}(\mathsf{q\text{-}silh}(\Gamma) = \Xi)$$

where the sum runs over all $\Xi \in \mathfrak{G}(n, s)$ such that $\mathrm{norm}(\Xi) = \Delta$. There are $\binom{n}{s}$ such graphs Ξ, so Lemmas 3.5 and 3.6 imply that

$$\mathbb{P}(\mathsf{silh}(\Gamma) = \Delta) = \binom{n}{s} \mathbb{P}(\mathsf{q\text{-}silh}(\Gamma) = \Delta)$$
$$= \binom{n}{s} \frac{|\mathfrak{M}_n(\Delta)|}{|\mathfrak{G}(n, s)|}.$$

Similarly,

$$\mathbb{P}(\mathsf{silh}(\Gamma) = \Delta') = \binom{n}{s} \frac{|\mathfrak{M}_n(\Delta')|}{|\mathfrak{G}(n, s)|}.$$

We conclude since $\mathfrak{M}_n(\Delta) = \mathfrak{M}_n(\Delta')$ by Lemma 3.7. $\qquad\square$

3.4 Size of the silhouette of a $PSL_2(\mathbb{Z})$-cyclically reduced graph

Let Γ be a $PSL_2(\mathbb{Z})$-cyclically reduced graph. The computation of $silh(\Gamma)$ shows how vertices are deleted until there are no more loops or isolated b-edges, or until the process has led to Δ_1 or Δ_2. Statistically however, only a small number of vertices are deleted. Proposition 3.8 below quantifies this statement. It follows that most vertices and edges of Γ are untouched in the reduction to $silh(\Gamma)$. This observation will play an important role in our discussion of generic properties of subgroups, see Section 6, especially Theorem 6.1.

Proposition 3.8 *If Γ is a $PSL_2(\mathbb{Z})$-cyclically reduced graph of size n, the average number of vertices of $silh(\Gamma)$ is greater than $n - 2n^{\frac{2}{3}} + o(n^{\frac{2}{3}})$.*

Moreover, if $\mu > 0$, there exists $0 < \gamma < 1$ such that the probability that $silh(\Gamma)$ has less than $n - (2 + \mu)n^{\frac{2}{3}}$ vertices is $\mathcal{O}(\gamma^{n^{\frac{1}{3}}})$.

Proof. Let Γ be a $PSL_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $(n, k_2, k_3, \ell_2, \ell_3)$ and consider the computation of $silh(\Gamma)$, say by the application of the minimal sequence M of Γ.

The sequence M starts with ℓ_3 λ_3-moves, which delete ℓ_3 vertices and add ℓ_3 a-loops. After these moves, M has $\ell_2 + \ell_3$ λ_2-moves. Every $\lambda_{2,1}$-move deletes 1 vertex and 1 a-loop, and adds one isolated b-edge, so there can be at most ℓ_2 such moves. Every $\lambda_{2,2}$-moves deletes 2 vertices, 1 a-loop and 1 isolated b-edge. Therefore these $\ell_2 + \ell_3$ λ_2-moves delete at most $2(\ell_2 + \ell_3)$ vertices. They also create at most $\ell_2 + \ell_3$ isolated b-edges.

Then M has a sequence of κ_3-moves, of length the number of isolated b-edges, which is at most $k_3 + \ell_2 + \ell_3$. Each deletes 2 vertices, so together they delete at most $2(k_3 + \ell_2 + \ell_3)$ vertices.

Therefore the total number of vertices deleted in the computation of $silh(\Gamma)$ is at most

$$\ell_3 + 2(\ell_2 + \ell_3) + 2(k_3 + \ell_2 + \ell_3) = 2k_3 + 4\ell_2 + 5\ell_3.$$

The statement on average values is then a direct consequence of this computation and of [7, Proposition 5.3]. Moreover, [7, Theorem 5.5 and Section 7.2] establish that, for each $\mu > 0$, there exists $0 < \gamma < 1$ such that

$$\mathbb{P}\left(k_3 < (1 + \frac{\mu}{6})n^{\frac{2}{3}}\right) = 1 - \mathcal{O}\left(\gamma^{n^{\frac{2}{3}}}\right),$$

$$\mathbb{P}\left(\ell_2 < 2n^{\frac{1}{2}}\right) = 1 - \mathcal{O}\left(\gamma^{n^{\frac{1}{2}}}\right),$$

$$\mathbb{P}\left(\ell_3 < 2n^{\frac{1}{3}}\right) = 1 - \mathcal{O}\left(\gamma^{n^{\frac{1}{3}}}\right).$$

For n large enough, $2n^{\frac{1}{3}} < 2n^{\frac{1}{2}} < \frac{\mu}{15}n^{\frac{2}{3}}$. So

$$\mathbb{P}\left(2k_3 + 4\ell_2 + 5\ell_3 < (2 + \mu)n^{\frac{2}{3}}\right) = 1 - \mathcal{O}\left(\gamma^{n^{\frac{1}{3}}}\right),$$

18

which concludes the proof. □

3.5 Silhouetting all finitely generated subgroups of $\mathsf{PSL}_2(\mathbb{Z})$

Recall that a rooted graph (Γ, v) is not $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced if and only v is not adjacent to both an a- and a b-edge, and is the only such vertex. In particular, adding a loop at v labeled by the missing letter(s) yields a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph which we denote by Γ°. The only case where two loops are added is when Γ is the graph with one vertex and no edge (the Stallings graph of the trivial subgroup), which we do not need to consider in the rest of this section.

To deal with labeled $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graphs, we introduce a new move, which consists in removing the root and adding the missing loop (if there is a missing loop). More precisely, if (Γ, v) is a labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph, let $\alpha = a$ (resp. b) if v is not adjacent to an a- (resp. b-) edge and $\alpha = 0$ if v is adjacent to both an a- and a b-edge (that is: Γ is $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced). The ($\mathsf{unroot}, \alpha, v$)-*move* then turns (Γ, v) to the labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph $\Delta = \Gamma^\circ$ if $\alpha \neq 0$ and $\Delta = \Gamma$ if $\alpha = 0$. Note that exactly one unroot-move is defined on a given (Γ, v).

We say that a quasi-labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ is *valid* for ($\mathsf{unroot}, \alpha, v$) if Δ has a vertex labeled v and if either $\alpha = 0$ or $\alpha \neq 0$ and Δ has an α-loop at v.

We now define the (quasi-)silhouette of a labeled $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graph (Γ, v) to be the (quasi-)silhouette of the graph obtained after applying the appropriate unroot-move.

If $1 \leq s \leq n$, we let $\mathfrak{R}(n, s)$ be the set of size n labeled $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graphs whose silhouette has s vertices. Observe that the set $\mathfrak{D}(n, s)$ of quasi-silhouettes of the elements of $\mathfrak{G}(n, s)$, is also the set of quasi-silhouettes of the elements of $\mathfrak{R}(n, s)$. A statement parallel to Theorem 3.4 holds for rooted graphs.

Theorem 3.9 *Let* $1 \leq s \leq n$. *If* (Γ, v) *is an element of* $\mathfrak{R}(n, s)$ *taken uniformly at random, then* $\mathsf{silh}(\Gamma, v)$ *is a uniformly random element of* $\mathfrak{D}(s, s)$. *That is: for any* $\Delta, \Delta' \in \mathfrak{D}(s, s)$,

$$\mathbb{P}(\mathsf{silh}((\Gamma, v)) = \Delta) = \mathbb{P}(\mathsf{silh}((\Gamma, v)) = \Delta'),$$

where (Γ, v) *is the* $\mathfrak{R}(n, s)$-*valued random variable with uniform distribution.*

Proof. We first observe that Lemma 3.5 can be readily extended to $\mathfrak{R}(n, s)$. Then we set the unroot-move as the minimal move on a rooted graph. The *minimal sequence* of a rooted graph consists therefore in an unroot-move, followed by the minimal sequence of the resulting $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph. There is no difficulty in extending Lemma 3.7 to rooted graphs: we consider the sequence M_{t-1} starting at the second move (that is, removing the first move m_t, which is an unroot-move); the induction in the proof of the lemma ensures that M_1 is the minimal sequence of $M_1 \cdot \Delta$ and $M_1 \cdot \Delta'$, and that both have the same a- and b-loops. As the first move m_t is of the ($\mathsf{unroot}, \alpha, v$)-move that is valid for

$M_1 \cdot \Delta$, it is also valid for $M_1 \cdot \Delta'$ (and minimal since an unroot-move is always minimal). The proof is then completed as in Theorem 3.4. $\qquad\square$

We also establish a result similar to Proposition 3.8.

Proposition 3.10 *If (Γ, v) is a random labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph of size n, the average number of vertices of $\mathsf{silh}(\Gamma, v)$ is greater than $n - 2n^{\frac{2}{3}} + o(n^{\frac{2}{3}})$.*

Moreover, if $\mu > 0$, there exists $0 < \gamma < 1$ such that the probability that $\mathsf{silh}((\Gamma, v))$ has less than $n - (2 + \mu)n^{\frac{2}{3}}$ vertices is $\mathcal{O}(\gamma^{n^{\frac{1}{3}}})$.

Proof. Let $\mathfrak{G}(n)$ and $\mathfrak{R}(n)$ denote the set of labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs and $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graphs, respectively.

Let $(\Gamma, v) \in \mathfrak{R}(n)$ be a $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graph and let $\Delta = \mathsf{unroot}(\Gamma, v)$ be the $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ obtained after applying the unroot-move. If (Γ, v) has combinatorial type $(n, k_2, k_3, \ell_2, \ell_3)$, then Δ has type $(n, k_2, k_3, \ell'_2, \ell'_3)$ with $(\ell'_2, \ell'_3) = (\ell_2, \ell_3)$, $(\ell_2 + 1, \ell_3)$ or $(\ell_2, \ell_3 + 1)$.

Since we need to manipulate simultaneously random variables defined on different probability spaces (namely the uniform distributions on $\mathfrak{G}(n)$ and $\mathfrak{R}(n)$), we introduce the following notation.

- L_2 (resp. L_3, K_3) is the random variable defined on $\mathfrak{G}(n)$ such that $L_2(\Delta)$ (resp. $L_3(\Delta)$, $K_3(\Delta)$) is the number of a-loops (resp. b-loops, isolated b-edges) in Δ.

- L'_2 (resp. L'_3, K'_3) is the random variable defined on $\mathfrak{R}(n)$ such that $L'_2(\Gamma, v)$ (resp. $L'_3(\Gamma, v)$, $K'_3(\Gamma, v)$) is the number of a-loops (resp. b-loops, isolated b-edges) in $\Delta = \mathsf{unroot}(\Gamma, v)$ — that is, $L'_2 = L_2 \circ \mathsf{unroot}$, $L'_3 = L_3 \circ \mathsf{unroot}$, $K'_3 = K_3 \circ \mathsf{unroot}$.

We have
$$\mathbb{P}(L'_2(\Gamma, v) = i) = \frac{|\{(\Gamma, v) \in \mathfrak{R}(n) : L'_2(\Gamma, v) = i\}|}{|\mathfrak{R}(n)|}.$$

Observe that a given size n labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Δ is produced by an unroot-move starting from exactly $n + L_2(\Delta) + L_3(\Delta)$ labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs. If $n > 1$, $n + L_2(\Delta) + L_3(\Delta) \leq 2n$, so

$$|\{(\Gamma, v) \in \mathfrak{R}(n) : L'_2(\Gamma, v) = i\}| \;\; \leq \;\; 2n \, |\{\Delta \in \mathfrak{G}(n) : L_2(\Delta) = i\}|,$$

and since $|\mathfrak{R}(n)| \geq n|\mathfrak{G}(n)|$, we have

$$\mathbb{P}(L'_2(\Gamma, v) = i) \;\; \leq \;\; \frac{2 \, |\{\Delta \in \mathfrak{G}(n) : L_2(\Delta) = i\}|}{|\mathfrak{G}(n)|} \;\; = \;\; 2 \, \mathbb{P}(L_2(\Delta) = i).$$

Similarly we have

$$\mathbb{P}(K'_3(\Gamma, v) = i) \;\; \leq \;\; 2 \, \mathbb{P}(K_3(\Delta) = i) \quad \text{and} \quad \mathbb{P}(L'_3(\Gamma, v) = i) \;\; \leq \;\; 2 \, \mathbb{P}(L_3(\Delta) = i).$$

It follows that we can reproduce the proof of Proposition 3.8, multiplying the error terms by 2, which does not change the final statement, expressed using the $\mathcal{O}$ notation. For instance,

$$\mathbb{P}\left(L_3'(\Gamma, v) \geq 2n^{\frac{1}{3}}\right) \;\leq\; 2\,\mathbb{P}\left(L_3(\Delta) \geq 2n^{\frac{1}{3}}\right) \;=\; \mathcal{O}\left(\gamma^{n^{1/3}}\right)$$

for a well chosen value of γ. $\qquad\square$

4 Counting subgroups by isomorphism and by combinatorial type

Our aim in this section is to count subgroups of a given size, under some additional constraint: with a fixed isomorphism type or with a fixed combinatorial type. Since subgroups are uniquely represented by their Stallings graph, *i.e.*, by a rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph, this is equivalent to counting these graphs.

It turns out that, for each $n \geq 1$, there are exactly $n!$ distinct labelings of an n-vertex rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph, see *e.g.*, [7, Section 3.1]. Note that there is no such easy correlation between the number of labeled and unlabeled cyclically reduced graphs, as counting is perturbed by the number of symmetries.

Thus our task reduces to counting labeled $\mathsf{PSL}_2(\mathbb{Z})$-rooted graphs. It further reduces to counting labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs, as we explain below.

4.1 Reduction to the count of labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs

If $\boldsymbol{\tau} = (n, k_2, k_3, \ell_2, \ell_3)$ is a tuple of integers, we let $H(\boldsymbol{\tau})$ (resp. $L(\boldsymbol{\tau})$, $s(\boldsymbol{\tau})$) be the number of subgroups (resp. labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs, labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs) of combinatorial type $\boldsymbol{\tau}$.

Example 4.1 In view of Example 2.5, the non-zero values of H, L and s for tuples $(n, k_2, k_3, \ell_2, \ell_3)$ where $n = 1, 2$ are as follows:
   - $H(\boldsymbol{\tau}) = L(\boldsymbol{\tau}) = 1$ for $\boldsymbol{\tau} = (1, 0, 0, 1, 1), (1, 0, 0, 1, 0), (1, 0, 0, 0, 1)$ and $s(\boldsymbol{\tau}) = 1$ for $\boldsymbol{\tau} = (1, 0, 0, 1, 1)$;
   - $L(\boldsymbol{\tau}) = 4$ and $H(\boldsymbol{\tau}) = s(\boldsymbol{\tau}) = 2$ for $\boldsymbol{\tau} = (2, 1, 1, 0, 0), (2, 0, 1, 2, 0)$;
   - $L(\boldsymbol{\tau}) = 2$ and $H(\boldsymbol{\tau}) = s(\boldsymbol{\tau}) = 1$ for $\boldsymbol{\tau} = (2, 1, 0, 0, 2)$;
   - $L(\boldsymbol{\tau}) = 2$ and $H(\boldsymbol{\tau}) = 1$ for $\boldsymbol{\tau} = (2, 0, 1, 1, 0), (2, 1, 0, 0, 1)$; $\qquad\square$

We first establish the connection between the parameters $H(\boldsymbol{\tau})$, $L(\boldsymbol{\tau})$ and $s(\boldsymbol{\tau})$.

Proposition 4.2 *Let $\boldsymbol{\tau} = (n, k_2, k_3, \ell_2, \ell_3)$ be a combinatorial type with $n \geq 2$. The numbers $H(\boldsymbol{\tau})$, $L(\boldsymbol{\tau})$ and $s(\boldsymbol{\tau})$, respectively of subgroups, labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs and labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs of combinatorial type $\boldsymbol{\tau}$ are related as follows.*

$$L(\boldsymbol{\tau}) = n\, s(n, k_2, k_3, \ell_2, \ell_3) + (\ell_2 + 1)\, s(n, k_2, k_3, \ell_2 + 1, \ell_3) + (\ell_3 + 1)\, s(n, k_2, k_3, \ell_2, \ell_3 + 1)$$

$$H(\boldsymbol{\tau}) = \frac{1}{n!} \, L(\boldsymbol{\tau}).$$

Proof. Let (Γ, v) be a rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph with $n \geq 2$ vertices, such that Γ is not $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced. Then v is adjacent to an a-edge but no b-edge, or the opposite. Adding a b-loop at v in the first case, an a-loop in the second case, yields a rooted $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph (Γ', v). Conversely, if Γ' is $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced, we get rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs either by rooting Γ' at any one of its vertices, or by rooting Γ' at a vertex that carries a loop and deleting that loop. The first equality follows directly.

The second equality follows from the first since a rooted size n $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph has $n!$ distinct labelings. $\qquad\square$

Based on Proposition 2.4, which relates the isomorphism type and the combinatorial type of a subgroup, we get the following statement.

Proposition 4.3 *Let $\boldsymbol{\sigma} = (\ell_2, \ell_3, r)$ be an isomorphism type and let $k_2 = \frac{1}{2}(n - \ell_2)$.*

The number of $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroups of size n and isomorphism type $\boldsymbol{\sigma}$ is $n\, s(n, k_2, k_3, \ell_2, \ell_3)$, where $k_3 = \frac{1}{2}(n - 3\ell_2 - 4\ell_3 - 6r + 6)$.

The number of non-$\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroups of size n and isomorphism type $\boldsymbol{\sigma}$, where the base vertex is adjacent to an a-edge, is $(\ell_3 + 1)\, s(n, k_2, k_3', \ell_2, \ell_3 + 1)$, where $k_3' = \frac{1}{2}(n - 3\ell_2 - 4\ell_3 - 6r + 2)$.

The number of non-$\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroups of size n and isomorphism type $\boldsymbol{\sigma}$, where the base vertex is adjacent to a b-edge, is $(\ell_2 + 1)\, s(n, k_2, k_3'', \ell_2 + 1, \ell_3)$, where $k_3'' = \frac{1}{2}(n - 3\ell_2 - 4\ell_3 - 6r + 4)$.

Propositions 4.2 and 4.3 effectively reduce the counting of subgroups to the counting of labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs of a given combinatorial type, which is investigated in Section 4.2 below.

4.2   Counting $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs

Let S be the multivariate exponential generating series (EGS) of labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs, where the different variables account for the components of the combinatorial type, namely

$$S(z, x_2, x_3, y_2, y_3) = \sum_{n, k_2, k_3, \ell_2, \ell_3} \frac{s(n, k_2, k_3, \ell_2, \ell_3)}{n!} \, z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}.$$

For a series T over these variables, it is convenient to denote by $[z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_b^{\ell_3}] T$ the coefficient of $z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_b^{\ell_3}$ in T.

We use the so-called *pointing* construction [10, Theorem II.3] to produce recurrence relations for the $s(\boldsymbol{\tau})$. If u is one of x_2, x_3, y_2, y_3, let S_u denote the partial derivative $\frac{\partial}{\partial u}S$. For instance, if $u = x_3$,

$$S_{x_3}(z, x_2, x_3, y_2, y_3) = \sum_{n,k_2,k_3,\ell_2,\ell_3} k_3 \left([z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}]S\right) z^n x_2^{k_2} x_3^{k_3-1} y_2^{\ell_2} y_3^{\ell_3}.$$

In particular, the coefficient $[z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}](x_3 S_{x_3})$ counts the number of structures obtained by pointing (*i.e.*, distinguishing) an isolated b-edge in a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of type $(n, k_2, k_3, \ell_2, \ell_3)$ — that is: this coefficient is equal to the number of pairs of the form (Γ, e) where Γ is a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of type $(n, k_2, k_3, \ell_2, \ell_3)$ and e is an isolated b-edge in Γ, divided by $n!$.

An analogous reasoning relates the coefficients of $x_2 S_{x_2}$ (resp. $y_2 S_{y_2}$, $y_3 S_{y_3}$) with the couting of pairs of the form (Γ, e) where e is an isolated a-edge (resp. a b-loop, an a-loop).

In the definition of λ_3-, λ_2- and κ_3-moves (Section 3.1), we described bijections which translate into formulas on the partial derivatives of S as follows.

Let $\boldsymbol{\tau} = (n, k_2, k_3, \ell_2, \ell_3)$ be a combinatorial type with $n \geq 2$ and $\ell_3 > 0$. The discussion of λ_3-moves established a bijection between the set of pairs (Γ, ℓ) of a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph Γ with combinatorial type $\boldsymbol{\tau}$ with a designated b-loop ℓ, and the set of triples (Δ, ℓ', v) where Δ is a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of combinatorial type $\boldsymbol{\tau} + \boldsymbol{\lambda}_3 = (n-1, k_2-1, k_3, \ell_2+1, \ell_3-1)$, ℓ' is a designated a-loop in Δ and v is an integer in $[n]$. It follows that

$$n!\,[z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}]\,(y_3 S_{y_3}) = n\,\left((n-1)![z^{n-1} x_2^{k_2-1} x_3^{k_3} y_2^{\ell_2+1} y_3^{\ell_3-1}]\,(y_2 S_{y_2})\right)$$

$$[z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}]\,(y_3 S_{y_3}) = [z^{n-1} x_2^{k_2-1} x_3^{k_3} y_2^{\ell_2+1} y_3^{\ell_3-1}]\,(y_2 S_{y_2})$$

$$= [z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}]\left(\frac{z x_2 y_2 S_{y_2}}{y_2}\right).$$

This takes care of the coefficients of $y_3 S_{y_3}$ corresponding to Case (1) (that is, where $n > 1$). In Case (2), $\Gamma = \Delta_1$, there is only one b-loop to point, so the corresponding EGS is $z y_2 y_3$. Therefore we have

$$y_3 S_{y_3} = \frac{z x_2 y_3}{y_2}\,(y_2 S_{y_2}) + z y_2 y_3,$$

$$S_{y_3} = z x_2\,S_{y_2} + z y_2. \tag{1}$$

Similarly, the different cases in the discussion of λ_2-moves yield the following equalities:

$$y_2 S_{y_2} = \frac{z y_2}{x_3}\,(x_3 S_{x_3}) + 2 z^2 x_2 x_3\,(y_2 S_{y_2}) + z^2 x_3 y_2^2 + z y_2 y_3$$

$$S_{y_2} = z\,S_{x_3} + 2 z^2 x_2 x_3\,S_{y_2} + z^2 x_3 y_2 + z y_3. \tag{2}$$

Finally, the analysis of κ_3-moves shows that

$$S_{x_3} = 2 z^2 x_2^2\,S_{x_2} + 2 z^2 x_2 y_2\,S_{y_2} + z^2 x_2 + z^2 y_2^2. \tag{3}$$

23

4.2.1   Recurrence relations

We now use Equations (1), (2) and (3) to compute the coefficients $s(n, k_2, k_3, \ell_2, \ell_3)$, with all the arguments non-negative, $n \geq 3$ and $n = 2k_2 + \ell_2 \geq 2k_3 + \ell_3$ (see Example 2.5 for $n < 3$).

Equation (1) states that:

$$\sum \frac{\ell_3}{n!} s(n, k_2, k_3, \ell_2, \ell_3) \; z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3-1}$$

$$= zy_2 + \sum \frac{\ell_2}{n!} s(n, k_2, k_3, \ell_2, \ell_3) \; z^{n+1} x_2^{k_2+1} x_3^{k_3} y_2^{\ell_2-1} y_3^{\ell_3}.$$

For $n \geq 3$, $\ell_3 \geq 1$, considering the coefficient of $z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3-1}$ in this equation, yields the equality

$$\frac{\ell_3}{n!} \; s(n, k_2, k_3, \ell_2, \ell_3) = \frac{\ell_2 + 1}{(n-1)!} \; s(n-1, k_2-1, k_3, \ell_2+1, \ell_3-1),$$

$$s(n, k_2, k_3, \ell_2, \ell_3) = \frac{n(\ell_2+1)}{\ell_3} \; s(n-1, k_2-1, k_3, \ell_2+1, \ell_3-1). \qquad (4)$$

Now turn to Equation (2):

$$\sum \frac{\ell_2}{n!} s(n, k_2, k_3, \ell_2, \ell_3) \; z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2-1} y_3^{\ell_3} = zy_3 + z^2 x_3 y_2$$

$$+ \sum \frac{k_3}{n!} s(n, k_2, k_3, \ell_2, \ell_3) \; z^{n+1} x_2^{k_2} x_3^{k_3-1} y_2^{\ell_2} y_3^{\ell_3}$$

$$+ \sum 2 \frac{\ell_2}{n!} \; s(n, k_2, k_3, \ell_2, \ell_3) \; z^{n+2} x_2^{k_2+1} x_3^{k_3+1} y_2^{\ell_2-1} y_3^{\ell_3}.$$

For $n \geq 3$, $\ell_2 \geq 1$, considering the coefficient of $z^n x_2^{k_2} x_3^{k_3} y_2^{\ell_2-1} y_3^{\ell_3}$ in this equation, yields

$$\frac{\ell_2}{n!} \; s(n, k_2, k_3, \ell_2, \ell_3) = \frac{k_3+1}{(n-1)!} \; s(n-1, k_2, k_3+1, \ell_2-1, \ell_3)$$

$$+ 2 \frac{\ell_2}{(n-2)!} \; s(n-2, k_2-1, k_3-1, \ell_2, \ell_3),$$

$$s(n, k_2, k_3, \ell_2, \ell_3) = \frac{n(k_3+1)}{\ell_2} \; s(n-1, k_2, k_3+1, \ell_2-1, \ell_3)$$

$$+ 2n(n-1) \; s(n-2, k_2-1, k_3-1, \ell_2, \ell_3). \qquad (5)$$

Finally Equation (3) reads as follows:

$$\sum \frac{k_3}{n!} s(n, k_2, k_3, \ell_2, \ell_3) z^n x_2^{k_2} x_3^{k_3-1} y_2^{\ell_2} y_3^{\ell_3} = z^2 x_2 + z^2 y_2^2$$

$$+ 2 \sum \frac{k_2}{n!} \; s(n, k_2, k_3, \ell_2, \ell_3) \; z^{n+2} x_2^{k_2+1} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}$$

$$+ 2 \sum \frac{\ell_2}{n!} \; s(n, k_2, k_3, \ell_2, \ell_3) \; z^{n+2} x_2^{k_2+1} x_3^{k_3} y_2^{\ell_2} y_3^{\ell_3}.$$

For $n \geq 3$, $k_3 \geq 1$, considering the coefficient of $z^n x_2^{k_2} x_3^{k_3-1} y_2^{\ell_2} y_3^{\ell_3}$ in this equation, yields

$$\frac{k_3}{n!} \, s(n, k_2, k_3, \ell_2, \ell_3) = 2 \, \frac{k_2 - 1}{(n-2)!} \, s(n-2, k_2-1, k_3-1, \ell_2, \ell_3)$$
$$+ 2 \, \frac{\ell_2}{(n-2)!} \, s(n-2, k_2-1, k_3-1, \ell_2, \ell_3),$$
$$s(n, k_2, k_3, \ell_2, \ell_3) = 2 \, \frac{n(n-1)(k_2-1)}{k_3} \, s(n-2, k_2-1, k_3-1, \ell_2, \ell_3)$$
$$+ 2 \, \frac{n(n-1)\ell_2}{k_3} \, s(n-2, k_2-1, k_3-1, \ell_2, \ell_3). \tag{6}$$

4.2.2 The base cases and the number of (labeled) silhouette graphs

We can use Equations (4), (5) and (6) to compute the coefficient $s(n, k_2, k_3, \ell_2, \ell_3)$, where $n \geq 3$: if one of k_3, ℓ_2 or ℓ_3 is greater than zero, every application of these equations reduces the first argument of the coefficients to compute by 1 or 2. We are therefore reduced to computing coefficients of the form $s(n, k_2, k_3, \ell_2, \ell_3)$ where $n \leq 2$, and this was done in Example 4.1, or of the form $s(n, k_2, 0, 0, 0)$, that is, the number of size n silhouette graphs.

The results of [7, Proposition 8.18 and Appendix A.4] can be used to compute the latter numbers and their asymptotic equivalent (see also the computation by Stothers [32] of the number of finite index, free subgroups of $\mathsf{PSL}_2(\mathbb{Z})$, that is, of subgroups having a silhouette Stallings graph).

Proposition 4.4 *Let T_2 (resp. T_3, $\tilde{g}$) be given, for $n \geq 1$, by*

$$T_2(2n) = \frac{(2n)!}{2^n \, n!} = \prod_{1 \leq i \leq n} (2i - 1), \quad T_3(3n) = \frac{(3n)!}{3^n \, n!} = \prod_{1 \leq i \leq n} (3i - 1)(3i - 2)$$

and $\tilde{g}(6n) = T_2(6n) \, T_3(6n)$. Then the number $s(6n, 3n, 0, 0, 0)$ of size $6n$ labeled silhouette graphs satisfies $s(0, 0, 0, 0, 0) = 0$ and for $n \geq 1$,

$$s(6n, 3n, 0, 0, 0) = \tilde{g}(6n) - \sum_{m=1}^{n-1} \tilde{g}(6m) \, s(6(n-m), 3(n-m), 0, 0, 0).$$

Moreover $s(6n, 3n, 0, 0, 0) \sim \sqrt{6} \, \exp\left(7n \log n - 7(1 - \log 6)n\right)$.

Proof. The first statements in the proposition are taken directly from [7, Appendix A.4]. Regarding the last statement, the proof of [7, Proposition 8.18] gives an asymptotic equivalent of the EGS $G^{\text{fr-fi}}$ of labeled silhouette graphs, namely:

$$[z^{6n}]G^{\text{fr-fi}} \sim \frac{1}{\sqrt{2\pi n}} \, \exp\left(n \log n - (1 - \log 6)n\right).$$

Since $s(6n, 3n, 0, 0, 0) = (6n)![z^{6n}]G^{\text{fr-fi}}$ and $(6n)! \sim \sqrt{12\pi n} \exp\left(-6n + 6n(\log(6n))\right)$ — by Stirling's formula, we have

$$s(6n, 3n, 0, 0, 0) \sim \sqrt{6} \exp\left(7n \log n - 7(1 - \log 6)n\right),$$

as announced. □

5 Random generation of subgroups of $\mathsf{PSL}_2(\mathbb{Z})$

As we saw in Example 4.1, there are exactly four size 1 subgroups, with pairwise distinct combinatorial and isomorphism type: the trivial subgroup, the subgroups generated by a and b, respectively, and $\mathsf{PSL}_2(\mathbb{Z})$ itself. We now concentrate on generating subgroups of size at least 2, and we assume that the parameters $L(\boldsymbol{\tau})$ and $s(\boldsymbol{\tau})$ have been pre-computed for all types of sufficient size.

Like in Section 4, generating uniformly at random a subgroup of a given combinatorial or isomorphism type reduces to randomly generating a labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph of a given combinatorial type and, before that, to randomly generating a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of a given type.

We start with the particular case of labeled silhouette graphs, then proceed to the general case of labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs and, finally, to labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs.

5.1 Random labeled silhouette graphs

Let n be a positive multiple of 6. The procedure to generate a size n labeled silhouette graph is simple and well known (see [7] for instance).

First randomly generate a fixpoint-free permutation on $[n]$ of order 2 and another of order 3. This is done in a standard fashion, by applying a random permutation to the permutation $(1\ 2)(3\ 4)\ldots(n-1\ n)$, and another random permutation to $(1\ 2\ 3)(4\ 5\ 6)\ldots(n-2\ n-1\ n)$. These two fixpoint-free permutations may determine a disconnected graph, but the proof of [7, Proposition 8.18] shows that this happens with vanishing probability (precisely: $\frac{5}{36}n^{-1} + o(n^{-1})$). Therefore a rejection algorithm (if the pair of permutations determines a disconnected graph, toss it and draw another pair) produces a silhouette graph after k iterations, with $\mathbb{E}(k) \sim 1$.

5.2 Random $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs

We now consider a tuple $\boldsymbol{\tau} = (n, k_2, k_3, \ell_2, \ell_3)$ such that $s(\boldsymbol{\tau}) > 0$, and we show how we can draw uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with type $\boldsymbol{\tau}$.

We saw in Section 3.2 how to construct the (quasi-)silhouette of a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph by a sequence of λ_3-, $\lambda_{2,1}$-, $\lambda_{2,2}$- and κ_3-moves, possibly followed by an

application of the exc-move, each move modifying the combinatorial type by a particular vector. Unwrapping this sequence of moves yields a random generation algorithm which we now explain in more detail.

We construct a finite stochastic path $\mathsf{path}(\boldsymbol{\tau})$ between types as follows. The edges of this path are labeled by symbols taken in the set $\{\lambda_3, \lambda_{2,1}, \lambda_{2,2}, \kappa_3, \mathsf{exc}\}$.

(1) If $\boldsymbol{\tau} = (1, 0, 0, 1, 1)$, $\boldsymbol{\tau} = (2, 1, 1, 0, 0)$ or $\boldsymbol{\tau}$ is of the form $(6s, 3s, 0, 0, 0)$ for some $s \geq 1$ (that is, if $\boldsymbol{\tau}$ is the type of Δ_1, Δ_2 or a silhouette graph), we let $\mathsf{path}(\boldsymbol{\tau})$ be the empty path at $\boldsymbol{\tau}$.

(2) If $\boldsymbol{\tau} = (2, 0, 1, 2, 0)$ (the type of Δ_3), we let $\mathsf{path}(\boldsymbol{\tau})$ be the length 1 path labeled exc, from $\boldsymbol{\tau}$ to $(1, 0, 0, 1, 1) = \boldsymbol{\tau} + \boldsymbol{exc}$.

(3) If $n \geq 2$ and $\ell_3 > 0$ (the case where we can apply a λ_3-move), we let $\mathsf{path}(\boldsymbol{\tau})$ consist in a λ_3-labeled edge from $\boldsymbol{\tau}$ to $\boldsymbol{\tau} + \boldsymbol{\lambda}_3$, followed by $\mathsf{path}(\boldsymbol{\tau} + \boldsymbol{\lambda}_3)$.

(4) If $n \geq 2$, no λ_3-move is possible ($\ell_3 = 0$) and $\ell_2 > 0$, we have (see Equation (5))

$$s(n, k_2, k_3, \ell_2, 0) = \frac{n(k_3 + 1)}{\ell_2} \, s(n - 1, k_2, k_3 + 1, \ell_2 - 1, 0)$$
$$+ 2n(n - 1) \, s(n - 2, k_2 - 1, k_3 - 1, \ell_2, 0).$$

We choose one of the two summands at random, along the distribution given by the pair $(\frac{n(k_3+1)}{\ell_2} \, s(n - 1, k_2, k_3 + 1, \ell_2 - 1, 0), 2n(n - 1) \, s(n - 2, k_2 - 1, k_3 - 1, \ell_2, 0))$. Depending on the outcome of this random choice, we let $\mathsf{path}(\boldsymbol{\tau})$ consist in either a $\lambda_{2,1}$-labeled edge from $\boldsymbol{\tau}$ to $\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,1}$, followed by $\mathsf{path}(\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,1})$; or a $\lambda_{2,2}$-labeled edge from $\boldsymbol{\tau}$ to $\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,2}$, followed by $\mathsf{path}(\boldsymbol{\tau} + \boldsymbol{\lambda}_{2,2})$.

(4) If $n > 2$, no λ_3- or λ_2-move is possible ($\ell_2 = \ell_3 = 0$) and a κ_3-move is possible ($k_3 > 0$), we let $\mathsf{path}(\boldsymbol{\tau})$ consist in an κ_3-labeled edge from $\boldsymbol{\tau}$ to $\boldsymbol{\tau} + \boldsymbol{\kappa}_3$, followed by $\mathsf{path}(\boldsymbol{\tau} + \boldsymbol{\kappa}_3)$.

The label of $\mathsf{path}(\boldsymbol{\tau})$ is a word $\mathsf{path\text{-}label}(\boldsymbol{\tau})$ in the language

$$\lambda_3^*(\lambda_{2,1} + \lambda_{2,2})^* \kappa_3^* (1 + \mathsf{exc}).$$

By construction, the last type along $\mathsf{path}(\boldsymbol{\tau})$ is the combinatorial type of $\mathsf{silh}(\Gamma)$, where Γ is any $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of type $\boldsymbol{\tau}$.

Let $\boldsymbol{\tau}_0 = \boldsymbol{\tau}, \boldsymbol{\tau}_1, \ldots, \boldsymbol{\tau}_q$ be the types along $\mathsf{path}(\boldsymbol{\tau})$ and let $m_1 \cdots m_q = \mathsf{path\text{-}label}(\boldsymbol{\tau})$. We build a sequence $(\Gamma_i)_{0 \leq i \leq q}$ of labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs with combinatorial type $\boldsymbol{\tau}_i$, respectively. The promised randomly chosen labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph is Γ_0.

In the large silhouette case (where $\boldsymbol{\tau}_q = (6s, 3s, 0, 0, 0)$ for some $s \geq 1$), we draw a labeled silhouette graph Γ_q with parameters $\boldsymbol{\tau}_q$ uniformly at random following the procedure

in Section 5.1. In the small silhouette case (where $\boldsymbol{\tau}_q$ is the combinatorial type of either Δ_1 or Δ_2), we draw Γ_q uniformly at random among the (very few) labeled graphs of type $\boldsymbol{\tau}_q$, see Examples 2.5 and 4.1. Suppose that we have built Γ_i for some $i > 0$.

If $m_i = \lambda_3$, we choose uniformly at random an a-loop in Γ_i (say, at vertex w). Then Γ_{i-1} is obtained from Γ_i by removing this a-loop, adding a new vertex v (with a new label), an a-edge between v and w, and a b-loop at v.

If $m_i = \lambda_{2,1}$, we choose uniformly at random an isolated b-edge in Γ_i (say, from vertex w to vertex w'). Then Γ_{i-1} is obtained from Γ_i by completing this b-edge into a b-triangle visiting a new vertex v (with a new label), and adding an a-loop at v.

If $m_i = \lambda_{2,2}$, we choose uniformly at random an a-loop in Γ_i (say, at vertex w'). Then Γ_{i-1} is obtained from Γ_i by removing that a-loop, adding new vertices v and w (with new labels), an isolated a-edge between w and w', an isolated b-edge between v and w, whose orientation (from v to w or from w to v) is chosen at random, and an a-loop at v.

Finally, if $m_j = \kappa_3$, we choose at random an isolated a-edge in Γ_i (say, between vertices v' and w'). Then Γ_{i-1} is obtained from Γ_i by removing that isolated a-edge, adding new vertices v and w (with new labels) and a-edges between v and v', and between w and w', and adding an isolated b-edge between v and w, whose orientation (from v to w or from w to v) is chosen at random.

To summarize: The algorithm to generate a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of type $\boldsymbol{\tau}$ consists in

(1) computing $\mathsf{path}(\boldsymbol{\tau})$;

(2) drawing uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with type the last vertex of $\mathsf{path}(\boldsymbol{\tau})$;

(3) working back along $\mathsf{path}(\boldsymbol{\tau})$ to generate uniformly at random $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs with type the vertices of $\mathsf{path}(\boldsymbol{\tau})$;

(4) outputting the graph which corresponds to the first vertex of $\mathsf{path}(\boldsymbol{\tau})$, that is, a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph of type $\boldsymbol{\tau}$.

Remark 5.1 The procedure outlined above lazily glosses over the question of labeling because the random generation process described in Section 5.3, which eventually calls for forgetting vertex labels, is blind to it. If, however, one wants to randomly generate a *labeled* $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph, the most expedient is to proceed as above, and then relabel vertices with a random permutation of $[n]$, as is commonly done in random sampling of combinatorial structures (see for instance [11, footnote p.12]). □

5.3 Random subgroups of $\mathsf{PSL}_2(\mathbb{Z})$

Let $\boldsymbol{\tau} = (n, k_2, k_3, \ell_2, \ell_3)$ be a combinatorial type. The formula for the number $L(\boldsymbol{\tau})$ of labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs of type $\boldsymbol{\tau}$, in Proposition 4.2 p. 21, suggests the

following algorithm to draw uniformly at random a labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph of combinatorial type $\boldsymbol{\tau}$.

(1) Draw an integer $1 \leq p \leq L(\boldsymbol{\tau})$ uniformly at random.

(2) If $p \leq n\, s(\boldsymbol{\tau})$ and q is the quotient of p by $s(\boldsymbol{\tau})$ (so that $0 \leq q < n$), draw uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $\boldsymbol{\tau}$ and root it at vertex $q + 1$.

(3) If $n\, s(\boldsymbol{\tau}) < p \leq n\, s(\boldsymbol{\tau}) + (\ell_2 + 1)\, s(n, k_2, k_3, \ell_2 + 1, \ell_3)$ and q is the quotient of $p - n\, s(\boldsymbol{\tau})$ by $s(n, k_2, k_3, \ell_2 + 1, \ell_3)$ (so that $0 \leq q \leq \ell_2$), draw uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $(n, k_2, k_3, \ell_2 + 1, \ell_3)$ (as in Section 5.2), delete the $(q+1)$st a-loop (following the order of vertex labels) and root the graph at the vertex where that loop used to be.

(4) If $n\, s(\boldsymbol{\tau}) + (\ell_2 + 1)\, s(n, k_2, k_3, \ell_2 + 1, \ell_3) < p$ and q is the quotient of $p - n\, s(\boldsymbol{\tau}) - (\ell_2 + 1)\, s(n, k_2, k_3, \ell_2 + 1, \ell_3)$ by $s(n, k_2, k_3, \ell_2, \ell_3 + 1)$ (so that $0 \leq q \leq \ell_3$), draw uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $(n, k_2, k_3, \ell_2, \ell_3 + 1)$ (as in Section 5.2), delete the $(q+1)$st b-loop (following the order of vertex labels) and root the graph at the vertex where that loop used to be.

To draw uniformly at random a subgroup of combinatorial type $\boldsymbol{\tau}$, we first draw a labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-reduced graph of type $\boldsymbol{\tau}$, and then forget the labeling.

Remark 5.2 To draw uniformly at random a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroup of combinatorial type $\boldsymbol{\tau}$, the algorithm is modified as follows: in step (1), one draws an integer p between 1 and $n\, s(\boldsymbol{\tau})$; one then applies only step (2). $\qquad\square$

Now consider an isomorphism type $\boldsymbol{\sigma} = (\ell_2, \ell_3, r)$. Let $k_2 = \frac{1}{2}(n - \ell_2)$, $k_3 = \frac{1}{2}(n - 3\ell_2 - 4\ell_3 - 6r + 6)$, $k_3' = \frac{1}{2}(n - 3\ell_2 - 4\ell_3 - 6r + 2)$ and $k_3'' = \frac{1}{2}(n - 3\ell_2 - 4\ell_3 - 6r + 4)$.

Proposition 4.3 p. 22 suggests the following algorithm to draw uniformly at random a subgroup of size n and isomorphism type $\boldsymbol{\sigma}$.

(1) Draw uniformly at random an integer p between 1 and

$$n\, s(n, k_2, k_3, \ell_2, \ell_3) + (\ell_3 + 1)\, s(n, k_2, k_3', \ell_2, \ell_3 + 1) + (\ell_2 + 1)\, s(n, k_2, k_3'', \ell_2 + 1, \ell_3).$$

(2) If $p \leq n\, s(n, k_2, k_3, \ell_2, \ell_3)$, draw uniformly at random a labeled rooted $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $(n, k_2, k_3, \ell_2, \ell_3)$.

(3) If $n\, s(\boldsymbol{\tau}) < p \leq n\, s(\boldsymbol{\tau}) + (\ell_3 + 1)\, s(n, k_2, k_3', \ell_2, \ell_3 + 1)$ and q is the quotient of $p - n\, s(\boldsymbol{\tau})$ by $s(n, k_2, k_3', \ell_2, \ell_3 + 1)$ (so that $0 \leq q \leq \ell_3$), draw uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $(n, k_2, k_3', \ell_2, \ell_3 + 1)$, delete the $q + 1$st b-loop (following the order of vertex labels) and root the graph at the vertex where that loop used to be.

29

(4) If $n\,s(\boldsymbol{\tau}) + (\ell_3 + 1)\,s(n, k_2, k_3', \ell_2, \ell_3 + 1) < p$ and q is the quotient of $p - n\,s(\boldsymbol{\tau}) - (\ell_3 + 1)\,s(n, k_2, k_3', \ell_2, \ell_3 + 1)$ by $s(n, k_2, k_3'', \ell_2 + 1, \ell_3)$ (so that $0 \le q \le \ell_2$), draw uniformly at random a labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graph with combinatorial type $(n, k_2, k_3, \ell_2 + 1, \ell_3)$, delete the $q+1$st a-loop (following the order of vertex labels) and root the graph at the vertex where that loop used to be.

This algorithm can be modified as in Remark 5.2 to draw uniformly at random a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroup of a given isomorphism type.

Remark 5.3 Let us briefly consider the time complexity of this algorithm. The (pre-)computation of the $s(\boldsymbol{\tau})$ for combinatorial types $\boldsymbol{\tau}$ of size at most n takes at most quartic time if the multiplications and additions are performed in time $\mathcal{O}(1)$. As the numbers we consider grow very fast, it is more relevant to consider that encoding a number N takes $\lceil \log_2 N \rceil$ bits, and that the basic operations are not performed in constant time anymore. However, even in this more realistic setting, the pre-computation of the $s(\boldsymbol{\tau})$ is still performed in polynomial time.

For a given $\boldsymbol{\tau}$, of size n, computing $\mathsf{path\text{-}label}(\boldsymbol{\tau})$ and $\mathsf{path}(\boldsymbol{\tau})$ takes linear time. If the last type along $\mathsf{path}(\boldsymbol{\tau})$ has size $s > 2$, the rejection algorithm to produce a random silhouette graph of size s takes polynomial time in average (since the expected number of rejects is $o(1)$). Moreover, each step working back along this path updates the labeled graph constructed so far in a bounded amount of time, and the length of this path is at most n.

It follows therefore that the average complexity of the algorithms above, to randomly generate a subgroup of $\mathsf{PSL}_2(\mathbb{Z})$, or a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced subgroup, of type $\boldsymbol{\tau}$ is polynomial in n. □

6 Generic properties of subgroups of $\mathsf{PSL}_2(\mathbb{Z})$

We show that, generically, a finitely generated subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ contains parabolic elements (Corollary 6.2) and fails to be almost malnormal (Theorem 6.4).

Recall that the *parabolic elements* of $\mathsf{PSL}_2(\mathbb{Z})$ are the conjugates of non-trivial powers of ab. A subgroup H of $\mathsf{PSL}_2(\mathbb{Z})$ is said to be *non-parabolic* if it contains no parabolic element. Also, H is *almost malnormal* if, for every $x \notin H$, $H \cap H^x$ is finite. It is *malnormal* if each of these intersections is trivial: malnormality coincides with almost malnormality if H is torsion-free (*e.g.* a free subgroup of $\mathsf{PSL}_2(\mathbb{Z})$).

The proofs of the two results, on parabolic elements and on malnormality, are linked. Indeed, we show that a necessary condition for a subgroup $H \le \mathsf{PSL}_2(\mathbb{Z})$ to be almost malnormal is that $\Gamma(H)$ should not contain a cycle labeled by a power at least 2 of ab (Corollary 6.7).

If H has finite index, and in particular if $\Gamma(H)$ is a silhouette graph with at least 2 vertices, both letters a and b label permutations of the vertex set of $\Gamma(H)$ (see Proposition 2.3). As a result, $\Gamma(H)$ has a loop at every vertex v labeled $(ab)^{n_v}$ for some $n_v \geq 1$. It follows that H contains parabolic elements. Moreover, if H has size at least 2, then one of the n_v is greater than or equal to 2, so H is not almost malnormal.

Our strategy to deal with general $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted (resp. $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced) graphs is the following: we state in Section 6.1 a result on the generic existence of short ab-cycles in silhouette graphs (Proposition 6.3). The proof of this result is long and technical, and is deferred to Section 6.3. We then exploit Proposition 6.3 to show that, generically, a $\mathsf{PSL}_2(\mathbb{Z})$-reduced (resp. $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced) graph contains an ab-cycle of length at least 2 (Theorem 6.1). Our result on parabolic elements follows immediately.

In Section 6.2, we establish the announced characterization of almost malnormality, leading directly to the negligibility of this property.

6.1 ab-cycles in $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs

We prove the following theorem.

Theorem 6.1 *Let $0 < \alpha < \frac{1}{6}$. Then a random size n $\mathsf{PSL}_2(\mathbb{Z})$-reduced (resp. $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced) graph admits an ab-cycle of size at least 2 and and at most n^α with probability $1 - \mathcal{O}(n^{-\alpha})$.*

Corollary 6.2 *Let $0 < \alpha < \frac{1}{6}$. A random size n subgroup (resp. cyclically reduced subgroup) of $\mathsf{PSL}_2(\mathbb{Z})$ is non-parabolic with probability $\mathcal{O}(n^{-\alpha})$.*

The main ingredients of the proof of Theorem 6.1 are:

- Propositions 3.8 and 3.10, which state that there exists $0 < \gamma < 1$ such that a size n $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced (resp. $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted) graph has a silhouette with size at least $n - 3n^{\frac{2}{3}}$ with probability $1 - \mathcal{O}(\gamma^{n^{\frac{2}{3}}})$ (for the uniform distribution on $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced or $\mathsf{PSL}_2(\mathbb{Z})$-reduced graphs).

- Theorems 3.4 and 3.9 which state that, under appropriate size constraints, taking the silhouette of a $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced (resp. $\mathsf{PSL}_2(\mathbb{Z})$-reduced) graph chosen uniformly at random yields a uniformly random silhouette graph.

- Proposition 6.3 below, which states that, if $0 < \alpha < \frac{1}{6}$, then, with probability $1 - \mathcal{O}(n^{-\alpha})$, a silhouette graph of size n has an ab-cycle of size m, with $2 \leq m \leq n^\alpha$ (for the uniform distribution on silhouette graphs of a given size).

We note that, besides its importance in this proof, Proposition 6.3 is of independent interest, as it deals with the probability of the presence of short cycles in certain permutation groups, see the discussion in the introduction.

Proposition 6.3 *Let $0 < \alpha < \frac{1}{6}$ and let $n > 0$ be a multiple of 6. Then a random size n silhouette graph admits an ab-cycle of size at least 2 and at most n^α with probability $1 - \mathcal{O}(n^{-\alpha})$.*

Proof of Theorem 6.1. Recall that $\mathfrak{G}(n)$ and $\mathfrak{R}(n)$ denote the sets of size n labeled $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs and $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graphs, respectively. We first deal with $\mathsf{PSL}_2(\mathbb{Z})$-cyclically reduced graphs.

To begin with let $0 < \alpha < \frac{1}{6}$. Let $\mathfrak{p}_\alpha(n)$ be the probability that a graph in $\mathfrak{G}(n)$ has no *ab*-cycle of size in $[2, n^\alpha]$ and $\mathfrak{p}'_\alpha(n)$ be the probability that an element of $\mathfrak{G}(n)$ has a silhouette of size at least $n - 3n^{\frac{2}{3}}$ and has no *ab*-cycle of length in $[2, n^\alpha]$.

Since by Proposition 3.8, there exists $0 < \gamma < 1$ such that the probability that an element of $\mathfrak{G}(n)$ has a silhouette with size less than $n - 3n^{\frac{2}{3}}$ is $\mathcal{O}(\gamma^{n^{\frac{2}{3}}})$, we get

$$\mathfrak{p}_\alpha(n) \leq \mathfrak{p}'_\alpha(n) + \mathcal{O}(\gamma^{n^{\frac{2}{3}}}).$$

Let now $s \geq n - 3n^{\frac{2}{3}}$ and $\mathfrak{p}'_\alpha(n,s)$ be the probability that an element of $\mathfrak{G}(n,s)$ (the set of elements of $\mathfrak{G}(n)$ whose silhouette has size s) has no *ab*-cycle of length in $[2, n^\alpha]$. Then

$$\mathfrak{p}'_\alpha(n) = \sum_{s=n-3n^{2/3}}^{n} \mathbb{P}_n\left(\mathfrak{G}(n,s)\right)\ \mathfrak{p}'_\alpha(n,s),$$

where $\mathbb{P}_n$ is the uniform probability on $\mathfrak{G}(n)$.

Finally for Γ taken uniformly at random in $\mathfrak{G}(n,s)$ let $\mathfrak{q}_\alpha(n,s)$ be the probability that both $\mathsf{silh}(\Gamma)$ and Γ have no *ab*-cycle of size in $[2, n^\alpha]$, and $\mathfrak{q}'_\alpha(n,s)$ the probability that $\mathsf{silh}(\Gamma)$ has such a cycle but Γ does not. Then $\mathfrak{p}'_\alpha(n,s) \leq \mathfrak{q}_\alpha(n,s) + \mathfrak{q}'_\alpha(n,s)$.

Theorem 3.4 shows that $\mathfrak{q}_\alpha(n,s)$ is equal to the probability that a size s silhouette graph has no *ab*-cycle of size in $[2, n^\alpha]$. This is less than or equal to the probability that a size s silhouette graph has no *ab*-cycle of size in $[2, s^\alpha]$ and, according to Proposition 6.3, the latter is $\mathcal{O}(s^{-\alpha})$. Thus, there exists a constant C (independent of s or n) such that

$$\mathfrak{q}_\alpha(n,s) \leq C s^{-\alpha} \leq C(n - 3n^{\frac{2}{3}})^{-\alpha} \leq C' n^{-\alpha}$$

for another constant $C' > 0$.

About $\mathfrak{q}'_\alpha(n,s)$, we have

$$\mathfrak{q}'_\alpha(n,s) = \sum \mathbb{P}_{n,s}\left(\mathsf{silh}(\Gamma) = \Delta\right)\ \mathfrak{q}_\Delta,$$

where $\mathbb{P}_{n,s}$ is the uniform probability on $\mathfrak{G}(n,s)$, $\mathfrak{q}_\Delta$ is the probability that a graph in $\mathfrak{G}(n,s)$ having silhouette Δ has no *ab*-cycle of size in $[2, n^\alpha]$, and the sum is taken over all size s silhouette graphs Δ who do have an *ab*-cycle of such a size.

Let $2 \leq \lambda \leq n^\alpha$ be the length of an *ab*-cycle in Δ. Let $\Gamma \in \mathfrak{G}(n,s)$ such that $\mathsf{silh}(\Gamma) = \Delta$. In reconstructing Γ from Δ (as in Section 5.2), *a*-edges of Δ get deleted exactly when

32

undoing a κ_3-move: an a-edge is deleted, two new vertices are added and new a- and b-edges are added. Since Γ has at most $3n^{\frac{2}{3}}$ vertices more that than Δ, there at most $\frac{3}{2}n^{\frac{2}{3}}$ κ_3-moves to undo, and the majority of a-edges of Δ are also a-edges of Γ. More precisely, at most $\frac{3}{2}n^{\frac{2}{3}}$ of the $\frac{s}{2}$ a-edges of Δ are not a-edges of Γ. Thus the probability that an a-edge of Δ fails to be an edge of Γ is at most

$$\frac{3n^{\frac{2}{3}}}{s} \;\leq\; \frac{3n^{\frac{2}{3}}}{n - 3n^{\frac{2}{3}}} \;=\; 3n^{-\frac{1}{3}}\left(1 + \mathcal{O}\left(n^{-\frac{1}{3}}\right)\right).$$

Then the probability that at least one of the λ a-edges in the ab-cycle under consideration is broken in passing from Δ to Γ is bounded above by $3\lambda n^{-\frac{1}{3}}\left(1 + \mathcal{O}\left(n^{-\frac{1}{3}}\right)\right)$ and

$$\mathfrak{q}_\Delta \;\leq\; 3\lambda n^{-\frac{1}{3}}\left(1 + \mathcal{O}\left(n^{-\frac{1}{3}}\right)\right) \;\leq\; 3n^{\alpha-\frac{1}{3}}\left(1 + \mathcal{O}\left(n^{-\frac{1}{3}}\right)\right).$$

It follows that

$$\mathfrak{q}'_\alpha(n,s) \leq 3n^{\alpha-1/3}\left(1 + \mathcal{O}\left(n^{-1/3}\right)\right)$$

$$\mathfrak{p}'_\alpha(n,s) \leq \mathfrak{q}_\alpha(n,s) + \mathfrak{q}'_\alpha(n,s) \leq C'n^{-\alpha} + 3n^{\alpha-1/3}\left(1 + \mathcal{O}\left(n^{-1/3}\right)\right) \leq C''n^{-\alpha}$$

for some constant $C'' > 0$ (since $\alpha - \frac{1}{3} < -\frac{1}{6} < -\alpha$). This leads to $\mathfrak{p}'_\alpha(n) \leq C''n^{-\alpha}$ and to the announced result $\mathfrak{p}_\alpha(n) = \mathcal{O}(n^{-\alpha})$.

The same proof holds for $\mathsf{PSL}_2(\mathbb{Z})$-reduced rooted graphs, reasoning within $\mathfrak{R}(n)$ instead of $\mathfrak{G}(n)$, and using Proposition 3.10 and Theorem 3.9 instead of Proposition 3.8 and Theorem 3.4. $\square$

6.2 Almost malnormality is negligible

Here we prove the following theorem.

Theorem 6.4 *Let $0 < \alpha < \frac{1}{6}$. The probability that a size n subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ is almost malnormal is $\mathcal{O}(n^{-\alpha})$.*

We start with an elementary characterization of almost malnormality in terms of Stallings graphs given in Proposition 6.6 below (see [24, Theorem 7.14] and [19, Statements 6.7, 6.8, 6.10] for more general statements).

An element $g \neq 1$ in $\mathsf{PSL}_2(\mathbb{Z})$ is said to be *cyclically reduced* if it has length 1 or if its normal form starts with a and ends with $b^{\pm 1}$, or starts with $b^{\pm 1}$ and ends with a. It is immediate that every non trivial element of $\mathsf{PSL}_2(\mathbb{Z})$ is conjugated to a cyclically reduced element. Moreover [21, Theorem IV.2.8], two conjugated cyclically reduced elements are cyclic conjugates of one another (that is: their geodesic representatives are of the form, respectively, tt' and $t't$).

Lemma 6.5 *Let H be a finitely generated subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ with Stallings graph $(\Gamma(H), v_0)$, let $g \in H$ and let x be of minimal length such that $u = x^{-1}gx$ is cyclically reduced. Then $\Gamma(H)$ has an x-path from v_0 to some vertex v_1 and a u-loop at v_1.*

Proof. If $|u| = 1$, then xux^{-1} is the normal form of g, then $\Gamma(H)$ has a loop at v_0 labeled xux^{-1}. It follows that there is a u-loop at v_1, as announced.

If $|u| > 1$ and without loss of generality, we have $u = au'b^\varepsilon$ (for some $\varepsilon = \pm 1$). If $x = 1$, then $\Gamma(H)$ has a u-loop at $v_1 = v_0$. If $x \neq 1$, then x cannot end with a or b^ε by minimality of $|x|$, so $x = x'b^{-\varepsilon}$. The word $x'b^{-\varepsilon}au'b^{-\varepsilon}x'^{-1}$ is $\mathsf{PSL}_2(\mathbb{Z})$-reduced and hence is the normal form of $xux^{-1} = g$. Let v be the vertex reached from v_0 reading x'^{-1}. Considering the loop at v_0 labeled by $x'^{-1}b^{-\varepsilon}au'b^{-\varepsilon}x'$, we see that v and v_1 sit on the same b-triangle, and that u labels a loop at v_1. $\square$

We can now prove the announced characterization of almost malnormality.

Proposition 6.6 *Let H be a finitely generated subgroup of $\mathsf{PSL}_2(\mathbb{Z})$ and let (Γ, v_0) be its Stallings graph. Then H is almost malnormal if and only if there does not exist distinct vertices p and q in $\Gamma(H)$ and a $\mathsf{PSL}_2(\mathbb{Z})$-reduced word w such that (a) w is not a conjugate of a or b (that is: w has infinite order), and (b) w label loops in $\Gamma(H)$ at p and at q.*

Proof. Let $g, h \in \mathsf{PSL}_2(\mathbb{Z})$, such that $h \notin H$, $g \in H \cap H^h$ and g has infinite order. Up to conjugating H by an appropriate word, we may assume that g is cyclically reduced (and has length greater than 1). Then g labels a loop in $\Gamma(H)$ at v_0.

If $g = y^p$ for some (cyclically) reduced word y and $|p| > 1$, then g labels a loop at $|p|$ distinct vertices along the g-loop at v_0. We now assume that g is not a proper power.

Since $hgh^{-1} \in H$, Lemma 6.5 shows that $\Gamma(H)$ has an x-path from v_0 to a vertex v_1 and a loop labeled by a cyclically reduced word u such that $hgh^{-1} = xux^{-1}$. Moreover, since hgh^{-1} is conjugated to g, the word u is a cyclic conjugate of g, say, $g = tt'$ and $u = t't$. Let then v_2 be the vertex reached from v_1 reading t'. There are tt'-loops at v_0 and v_2 and we need to show that $v_0 \neq v_2$.

If $v_0 = v_2$, then $tx^{-1} \in H$. Moreover

$$hgh^{-1} = xux^{-1} = xt'tx^{-1} = xt^{-1}tt'tx^{-1} = (tx^{-1})^{-1}g(tx^{-1})$$

so $tx^{-1}h$ and g commute. By the classical characterization of commuting elements in free products [22, Theorem 4.5], it follows that either $tx^{-1}h$ and g sit in the same conjugate of $\langle a \rangle$ or $\langle b \rangle$, or $tx^{-1}h$ and g sit in the same cyclic subgroup.

The first case is impossible since we assumed that g has infinite order. Therefore there exist $y \in \mathsf{PSL}_2(\mathbb{Z})$, $p, q \in \mathbb{Z}$ such that $g = y^p$ and $tx^{-1}h = y^q$. We assumed that g is not a proper power, so $p = \pm 1$. Therefore $tx^{-1}h = g^{pq} \in H$ and hence $h \in H$, a contradiction. $\square$

34

In the proof of Theorem 6.4, we use the following consequence of Proposition 6.6.

Corollary 6.7 *Let H be a subgroup of $\mathsf{PSL}_2(\mathbb{Z})$. If there exists a $\mathsf{PSL}_2(\mathbb{Z})$-reduced word w which is not a conjugate of a or b and an integer $m \geq 2$ such that w^m labels a loop at some vertex p in the Stallings graph $\Gamma(H)$ but w does not label a loop at p, then H fails to be almost malnormal.*

Proof. The word w^m labels loops at every vertex reached from p reading w^i, for $0 \leq i < m$ and we conclude by Proposition 6.6. □

Proof of Theorem 6.4. Theorem 6.1 shows that the Stallings graph of a size n random subgroup H contains a simple loop labeled $(ab)^m$ (with $2 \leq m \leq n^\alpha$) with probability $1 - \mathcal{O}(n^{-\alpha})$. The result then follows from Corollary 6.7. □

6.3 ab-cycles in silhouette graphs: proof of Proposition 6.3

Let $\mathcal{G}$ be the set of labeled graphs that are disjoint unions of silhouette graphs. Recall that the set of n-vertex elements of $\mathcal{G}$ (n a multiple of 6) is in bijection with the set of pairs (σ_2, σ_3) of fixpoint-free permutations of $[n]$, the first of order 2 (the a-edges) and the second of order 3 (the b-edges).

If we fix σ_3, the set $\mathcal{G}_{\sigma_3}$ of elements of $\mathcal{G}$ characterized by pairs of the form (σ_2, σ_3) has cardinality the number of fixpoint-free, order 2 permutations on $[n]$, namely $(n-1)!!$, where the double factorial of an odd integer q is given by $q!! = q(q-2)(q-4)\dots 1$. Since this value does not depend on σ_3, it is sufficient to establish the restriction of Proposition 6.3 to an arbitrary $\mathcal{G}_{\sigma_3}$, provided that the constants in the $\mathcal{O}$-notation do not depend on σ_3.

For convenience, we fix $\sigma_3 = (1\,2\,3)(4\,5\,6)\dots(n-2\,n-1\,n)$, and we write $\mathcal{G}_n$ instead of $\mathcal{G}_{\sigma_3}$. We now concentrate on a particular set of ab-cycles. Say that an ab-cycle in a graph $G \in \mathcal{G}$ is *simple* if it visits at most one vertex in each b-triangle in G. Equivalently, walking along the corresponding $(ab)^m$-labeled path does not require traveling through an a-edge in both directions.

Now let $M = \lfloor n^\alpha \rfloor$ and $\mathbb{M} = \{2, \dots, M\}$. In the context of this proof, we say that a set is *small* if its cardinality is in $\mathbb{M}$. Then a *small* ab-cycle in an element of $\mathcal{G}_n$ visits a *small* set of b-triangles. We need to prove that, with probability $1 - \mathcal{O}(n^{-\alpha})$, a random size n silhouette graph admits a small simple ab-cycle.

Let $\mathcal{C}$ be the set of graphs in $\mathcal{G}_n$ with at least a small simple ab-cycle. Let also $\mathcal{S}$ be the set of all small sets of b-triangles in a graph of $\mathcal{G}_n$ (recall that all the graphs of $\mathcal{G}_n$ have the same b-triangles). If $I \in \mathcal{S}$, let $\mathcal{C}_I$ be the set of graphs in $\mathcal{G}_n$ containing a simple ab-cycle visiting exactly the b-triangles in I. Then

$$\mathcal{C} = \bigcup_{I \in \mathcal{S}} \mathcal{C}_I.$$

Finally, let $\overline{\mathcal{C}}$ denote the complement of $\mathcal{C}$ in $\mathcal{G}_n$ (the elements of $\mathcal{G}_n$ without a small simple ab-cycle). We want to show that $\frac{|\overline{\mathcal{C}}|}{|\mathcal{G}_n|} = \frac{|\overline{\mathcal{C}}|}{(n-1)!!}$ is of the form $\mathcal{O}(n^{-\alpha})$. By the inclusion-exclusion principle, we have

$$|\overline{\mathcal{C}}| = |\mathcal{G}_n| - \sum_{I \in \mathcal{S}} |\mathcal{C}_I| + \sum_{\substack{\{I_1, I_2\} \subseteq \mathcal{S} \\ I_1 \neq I_2}} |\mathcal{C}_{I_1} \cap \mathcal{C}_{I_2}| - \ldots = \sum_{\mathcal{I} \subseteq \mathcal{S}} (-1)^{|\mathcal{I}|} \left| \bigcap_{I \in \mathcal{I}} \mathcal{C}_I \right|$$

$$= \sum_k (-1)^k \sum_{\substack{\mathcal{I} \subseteq S \\ |\mathcal{I}| = k}} \left| \bigcap_{I \in \mathcal{I}} \mathcal{C}_I \right|.$$

Truncating the inclusion-exclusion formula on even or odd cardinalities for $\mathcal{I}$, yields upper and lower bounds for $|\overline{\mathcal{C}}|$. For any $\kappa \geq 0$ we have (if κ is too large, inequalities become equalities)

$$\sum_{k=0}^{2\kappa+1} (-1)^k \sum_{\substack{\mathcal{I} \subseteq S \\ |\mathcal{I}| = k}} \left| \bigcap_{I \in \mathcal{I}} \mathcal{C}_I \right| \ \leq \ |\overline{\mathcal{C}}| \ \leq \ \sum_{k=0}^{2\kappa} (-1)^k \sum_{\substack{\mathcal{I} \subseteq S \\ |\mathcal{I}| = k}} \left| \bigcap_{I \in \mathcal{I}} \mathcal{C}_I \right| \tag{7}$$

It turns out to be more convenient to work with tuples of b-triangles rather than sets. If $\mathcal{I} = \{I_1, \ldots, I_k\}$ is a small set of b-triangles with cardinality k, there are $k!$ tuples $\boldsymbol{J} = (J_1, \ldots, J_k) \in \mathcal{S}^k$ such that $\{J_1, \ldots, J_k\} = \mathcal{I}$, so

$$\left| \bigcap_{I \in \mathcal{I}} \mathcal{C}_I \right| = \frac{1}{k!} \sum_{\substack{(J_1, \ldots, J_k) \in \mathcal{S}^k \\ \{J_1, \ldots, J_k\} = \mathcal{I}}} |\mathcal{C}_{J_1} \cap \ldots \cap \mathcal{C}_{J_k}|. \tag{8}$$

Say that two simple ab-cycles *overlap* if they visit a same b-triangle (of course, on different vertices). We now distinguish the tuples $\boldsymbol{J} = (J_1, \ldots, J_k)$ in Equation (8) according to the cardinality of their components and to their overlaps. More precisely, if $\boldsymbol{d} = (d_1, \ldots, d_k) \in \mathbb{M}^k$, we let

$$\mathcal{P}^{\circ\circ}(\boldsymbol{d}) = \left\{ \boldsymbol{J} = (J_1, \ldots, J_k) \in \mathcal{S}^k \mid \forall i, \ |J_i| = d_i \text{ and the } J_i \text{ are pairwise disjoint} \right\}$$

$$\mathcal{P}^{\oplus}(\boldsymbol{d}) = \left\{ \boldsymbol{J} = (J_1, \ldots, J_k) \in \mathcal{S}^k \mid \forall i, \ |J_i| = d_i \text{ and the } J_i \text{ are pairwise distinct} \right.$$
$$\left. \text{but not pairwise disjoint} \right\}.$$

Returning to the summands in the estimation of the inclusion-exclusion bounds (Equa-

tion (7)), we now have, for every k,

$$\sum_{\substack{\mathcal{I} \subseteq S \\ |\mathcal{I}| = k}} \left| \bigcap_{I \in \mathcal{I}} \mathcal{C}_I \right| = \frac{1}{k!} \left(\underbrace{\sum_{\boldsymbol{d} \in \mathbb{M}^k} \sum_{\boldsymbol{J} \in \mathcal{P}^{\circ\circ}(\boldsymbol{d})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right|}_{A_k} + \underbrace{\sum_{\boldsymbol{d} \in \mathbb{M}^k} \sum_{\boldsymbol{J} \in \mathcal{P}^{\oplus}(\boldsymbol{d})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right|}_{B_k} \right) \qquad (9)$$

We now study successively the quantities A_k and B_k in Equation (9). If $q \geq 1$, we let H_q denote the partial sum $\sum_{i=1}^{q} \frac{1}{i}$ of the harmonic series. It is well known that $H_q = \log q + \gamma + o(1)$, where γ is Euler's constant.

Lemma 6.8 *Let n be a positive multiple of 6. Let $0 < \alpha < \frac{1}{2}$, $M = \lfloor n^\alpha \rfloor$, $0 < \beta < \frac{1}{2} - \alpha$ and $1 \leq k \leq n^\beta$. Finally, let $\delta = \alpha + \beta$ and let A_k be as in Equation (9). Then*

$$\frac{1}{(n-1)!!} A_k = (H_M - 1)^k \left(1 + \mathcal{O}\left(n^{2\delta - 1} \right) \right),$$

uniformly in k (that is: the constants intervening in the $\mathcal{O}$ notation do not depend on n or k).

Proof. Let $\boldsymbol{d} = (d_1, \ldots, d_k) \in \mathbb{M}^k$, $d = d_1 + \ldots + d_k$ and $\boldsymbol{J} = (J_1, \ldots, J_k) \in \mathcal{P}^{\circ\circ}(\boldsymbol{d})$. To construct a graph in $\bigcap_i \mathcal{C}_{J_i}$, that is, a graph in $\mathcal{G}_n$ with (non-overlapping) simple ab-cycles over the sets of b-triangles $J_1, \ldots, J_k$ respectively, we must

- select for each b-triangle in $J_1, \ldots, J_k$ a vertex belonging to the collection of simple ab-cycles; there are 3 possibilities for each b-triangle, and therefore a total of 3^d choices;

- cyclically order the triangles in each J_i; there are $(d_1 - 1)! \ldots (d_k - 1)!$ possibilities to do so; note that this second step fully determines the a-edges adjacent to the d vertices chosen in the first step;

- choose the missing a-edges arbitrarily: they connect the $n - 2d$ vertices not yet adjacent to an a-edge, and there are $(n - 2d - 1)!!$ ways to do so.

Thus, for every $\boldsymbol{J} = (J_1, \ldots, J_k) \in \mathcal{P}^{\circ\circ}(\boldsymbol{d})$, there are $3^d (d_1 - 1)! \cdots (d_k - 1)!(n - 2d - 1)!!$ graphs in $\bigcap_{i=1}^{k} \mathcal{C}_{J_i}$ (which is independent of the choice of $\boldsymbol{J}$ in $\mathcal{P}^{\circ\circ}(\boldsymbol{d})$).

Moreover, since a graph in $\mathcal{G}_n$ has $\frac{n}{3}$ b-triangles and the components of a tuple in $\mathcal{P}^{\circ\circ}(\boldsymbol{d})$ are pairwise disjoint, we have $|\mathcal{P}^{\circ\circ}(\boldsymbol{d})| = \binom{n/3}{d_1, \ldots, d_k, n-d}$. Thus

$$\sum_{\boldsymbol{J} \in \mathcal{P}^{\circ\circ}(\boldsymbol{d})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right| = \binom{n/3}{d_1, \ldots, d_k, n/3 - d} 3^d (d_1 - 1)! \cdots (d_k - 1)!(n - 2d - 1)!!.$$

37

Note that $\frac{(n-2d-1)!!}{(n-1)!!} = \prod_{i=0}^{d-1} \frac{1}{n-1-2i}$ and $\frac{(n/3)!3^d}{(n/3-d)!} = \prod_{i=0}^{d-1}(n-3i)$. Therefore

$$\frac{1}{(n-1)!!} \sum_{\boldsymbol{J} \in \mathcal{P}^{\circ\circ}(\boldsymbol{d})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right| = \frac{Q_d}{d_1 \cdots d_k}, \quad \text{with } Q_d = \prod_{i=0}^{d-1} \frac{n-3i}{n-1-2i}.$$

Now observe that

$$Q_d \leq \frac{n}{n-1} \quad \text{and} \tag{10}$$

$$Q_d = \prod_{i=0}^{d-1} \left(1 - \frac{i-1}{n-1-2i}\right) \geq \left(1 - \frac{d}{n-2d}\right)_d = \exp\left(d \log\left(1 - \frac{d}{n-2d}\right)\right)$$

$$\geq 1 + d \log\left(1 - \frac{d}{n-2d}\right). \tag{11}$$

The lower bound in Equation (11) for Q_d is a decreasing function of d and the possible values of d satisfy $1 \leq d \leq kM \leq n^{\alpha+\beta} = n^{\delta}$, so

$$1 + n^{\delta} \log\left(1 - \frac{n^{\delta}}{n - 2n^{\delta}}\right) \leq Q_d \leq \frac{n}{n-1}. \tag{12}$$

Let U and L be the upper and lower bounds of Q_d in Equation (12). Note that $\sum_{\boldsymbol{d} \in \mathbb{M}^k} \frac{1}{d_1 \cdots d_k} = (H_M - 1)^k$. Therefore

$$L(H_M - 1)^k = L \sum_{\boldsymbol{d} \in \mathbb{M}^k} \frac{1}{d_1 \dots d_k} \leq \frac{1}{(n-1)!!} A_k \leq U \sum_{\boldsymbol{d} \in \mathbb{M}^k} \frac{1}{d_1 \dots d_k} = U(H_M - 1)^k,$$

which concludes the proof of Lemma 6.8 since both U and L are of the form $1 + \mathcal{O}\left(n^{2\delta-1}\right)$. $\square$

Lemma 6.9 *Let n be a positive multiple of 6. Let $0 < \alpha < \frac{1}{6}$, $M = \lfloor n^{\alpha} \rfloor$, $0 < \beta < \frac{1}{6} - \alpha$ and $1 \leq k \leq n^{\beta}$. Finally, let $\delta = \alpha + \beta$ and let B_k be as in Equation (9). Then*

$$\frac{1}{(n-1)!!} B_k \leq \mathcal{O}\left(n^{6\delta-1}\right) (H_M - 1)^k$$

uniformly in k.

Proof. Let $\boldsymbol{d} = (d_1, \dots, d_k) \in \mathbb{M}^k$ and $d = d_1 + \dots + d_k$. Since every vertex of a silhouette graph occurs in exactly one ab-cycle, a b-triangle can occur in at most 3 ab-cycles. Let $\boldsymbol{t} = (t_1, t_2, t_3)$ be a tuple of non-negative integers such that $d = t_1 + 2t_2 + 3t_3$. We denote by $\mathcal{P}_k^{\oplus}(\boldsymbol{d}; \boldsymbol{t})$ the set of elements $\boldsymbol{J} = (J_1, \dots, J_k) \in \mathcal{P}_k^{\oplus}(\boldsymbol{d})$ such that there are t_1 (resp. t_2, t_3) b-triangles belonging to exactly 1 (resp. 2, 3) of the components of $\boldsymbol{J}$. We talk of b-triangles *of type* 1 (resp. 2, 3).

38

Lemma 6.10 *If $J \in \mathcal{P}_k^{\oplus}(d; t)$ and $\bigcap_{i=1}^k \mathcal{C}_{J_i} \neq \emptyset$, then $t_2 + t_3$ is even.*

Proof. Let $G \in \bigcap_{i=1}^k \mathcal{C}_{J_i}$. Consider the a-edges occurring in the k small simple ab-cycles visiting, respectively, $J_1, \ldots, J_k$. It is convenient at this point to think of the a-edges in our ab-cycles as matched pairs of half-edges, which we denote (T, e), where e is an a-edge and T is a b-triangle adjacent to e. Since no a-edge in a simple ab-cycle may connect vertices from the same b-triangle, each such a-edge e corresponds to a pair of distinct, matched half-edges (T, e) and (T', e).

Even though a-edges are undirected (or can be traversed in both directions), considering one in a simple ab-cycle uniquely defines a direction and we can talk of matched outgoing and incoming half-edges along a simple ab-cycle. Clearly, an a-edge is used in only one direction in a given ab-cycle, but it can be used in different directions by distinct ab-cycles. So we say that a half-edge (T, e) such that e occurs in the union of the k ab-cycles under consideration is *outgoing* (resp. *incoming*, *2-way*) if it only occurs as outgoing (resp. it only occurs as incoming, it occurs both as outgoing and incoming).

If T is a b-triangle in $\bigcup J_i$, occurring in just one of the k small simple ab-cycles, then T is a component of exactly 1 incoming and 1 outgoing half-edges; if T occurs in two of these ab-cycles, it is a component of 1 incoming, 1 outgoing and 1 2-way half-edges; finally, if T occurs in three ab-cycles, it is a component of 3 2-way half-edges.

The result follows since a 2-way half-edge must be matched with another, distinct, 2-way half-edge, and we have $t_2 + 3t_3$ such half-edges. □

Let $J = (J_1, \ldots, J_k) \in \mathcal{P}_k^{\oplus}(d; t)$. Then $|\bigcup_i J_i| = t_1 + t_2 + t_3$ whereas $d = \sum_i |J_i| = t_1 + 2t_2 + 3t_3$. The overlaps between the J_i determine which b-triangles in $\bigcup_i J_i$ are of type 1, 2 or 3. To construct an n-vertex graph in $\bigcap_i \mathcal{C}_{J_i}$, that is, a graph in $\mathcal{G}_n$ with (overlapping) simple ab-cycles over the sets of b-triangles $J_1, \ldots, J_k$ respectively, we must

- select for each b-triangle of type 1 a vertex belonging to the collection of simple ab-cycles; there are 3^{t_1} choices. Similarly, for each b-triangle of type 2, select two vertices belonging to the collection of simple ab-cycles; there are 3^{t_2} choices. Note that every vertex of a type 3 b-triangle belongs to the collection of simple ab-cycles. As discussed in the proof of Lemma 6.10, the choice of these $t_1 + 2t_2 + 3t_3$ vertices in the ab-cycles implies the presence of $2t_1 + 3t_2 + 3t_3$ vertices along the corresponding $(ab)^{d_i}$-labeled loops.

- cyclically order the triangles in each J_i; there are $(d_1 - 1)! \ldots (d_k - 1)!$ possibilities to do so; note that this second step fully determines the a-edges adjacent to the $2t_1 + 3t_2 + 3t_3$ vertices determined in the first step;

- choose the missing a-edges arbitrarily: they connect the $n - (2t_1 + 3t_2 + 3t_3)$ vertices not yet selected, and there are $(n - (2t_1 + 3t_2 + 3t_3) - 1)!!$ ways to do so.

Thus, for every $\boldsymbol{J} = (J_1, \ldots, J_k) \in \mathcal{P}_k^{\oplus}(\boldsymbol{d}; \boldsymbol{t})$, we have

$$\left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right| = 3^{t_1+t_2}(d_1-1)! \cdots (d_k-1)!(n-2t_1-3t_2-3t_3-1)!!.$$

Now, to construct a tuple in $\mathcal{P}_k^{\oplus}(\boldsymbol{d}; \boldsymbol{t})$, we must

- choose t_i b-triangles of type i $(i = 1, 2, 3)$; there are $\binom{n/3}{t_1, t_2, t_3, n/3-t_1-t_2-t_3}$ choices;
- allocate the $t_1 + t_2 + t_3$ selected b-triangles to sets $J_1, \ldots, J_k$ respecting multiplicities and the required cardinality of the J_i; there are at most $\binom{t_1+2t_2+3t_3}{d_1, \ldots, d_k} = \binom{d}{d_1, \ldots, d_k}$ choices (this is an upper bound as some choices may be unrealizable or produce cycles that are not simple).

Therefore we have

$$|\mathcal{P}_k^{\oplus}(\boldsymbol{d}; \boldsymbol{t})| \leq \binom{n/3}{t_1, t_2, t_3, n/3-t_1-t_2-t_3} \binom{d}{d_1, \ldots, d_k}$$

and $\sum_{\boldsymbol{J} \in \mathcal{P}^{\oplus}(\boldsymbol{d}; \boldsymbol{t})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right|$ is bounded above by

$$\binom{n/3}{t_1, t_2, t_3, n/3-t_1-t_2-t_3} \binom{d}{d_1, \ldots, d_k} 3^{t_1+t_2}(d_1-1)! \cdots (d_k-1)!(n-2t_1-3t_2-3t_3-1)!!.$$

Dividing by $(n-1)!!$, we get

$$\frac{\sum_{\boldsymbol{J} \in \mathcal{P}^{\oplus}(\boldsymbol{d}; \boldsymbol{t})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right|}{(n-1)!!} \leq \frac{d!}{d_1 \cdots d_k \, t_1! t_2! t_3! \, 3^{t_3}} \frac{n(n-3) \cdots (n-3(t_1+t_2+t_3-1))}{(n-1)(n-3) \cdots (n-2t_1-3t_2-3t_3+1)}.$$

Let $t = t_1 + t_2 + t_3$, so that $t_1 = d - 2t_2 - 3t_3$. Recall that $Q_t = \prod_{i=0}^{t-1} \frac{n-3i}{n-1-2i} \leq \frac{n}{n-1}$ (Equation (10)). Then

$$\frac{\sum_{\boldsymbol{J} \in \mathcal{P}^{\oplus}(\boldsymbol{d}; \boldsymbol{t})} \left| \bigcap_{i=1}^{k} \mathcal{C}_{J_i} \right|}{(n-1)!!} \leq \frac{1}{d_1 \cdots d_k} \cdot \frac{d!}{(d-2t_2-3t_3)!} \cdot \frac{Q_t}{\prod_{i=t}^{t_1+\frac{3}{2}(t_2+t_3)-1}(n-1-2i)}$$

$$\leq \frac{n \, d^{2t_2+3t_3}}{(n-1) \, d_1 \cdots d_k \, (n-2t_1-3t_2-3t_3+1)^{\frac{1}{2}(t_2+t_3)}} \qquad (13)$$

Since $d = t_1 + 2t_2 + 3t_3$ and $d \leq kM \leq n^{\alpha+\beta} = n^{\delta}$, we have $2t_1 + 3t_2 + 3t_3 \leq 2d \leq 2n^{\delta}$, yielding

$$\frac{d^{2t_2+3t_3}}{(n-2t_1-3t_2-3t_3+1)^{\frac{1}{2}(t_2+t_3)}} \leq \frac{n^{\delta(2t_2+3t_3)}}{(n-2n^{\delta})^{\frac{1}{2}(t_2+t_3)}}.$$

40

Moreover, $\frac{1}{2}(t_2 + t_3) \leq \frac{1}{4}d \leq \frac{1}{4}n^\delta$ and we have

$$(n - 2n^\delta)^{\frac{1}{2}(t_2+t_3)} = n^{\frac{1}{2}(t_2+t_3)} \exp\left(\left(\frac{1}{2}(t_2 + t_3)\right)\log\left(1 - 2n^{\delta-1}\right)\right)$$

$$\geq n^{\frac{1}{2}(t_2+t_3)} \exp\left(\frac{1}{4}n^\delta \log\left(1 - 2n^{\delta-1}\right)\right)$$

The term under the exponential is

$$\frac{1}{4}n^\delta \log\left(1 - 2n^{\delta-1}\right) \sim -\frac{1}{2}n^{3\delta-1},$$

which tends to 0 (since $\delta < \frac{1}{6} < \frac{1}{3}$). Therefore, for n sufficiently large,

$$(n - 2n^\delta)^{\frac{1}{2}(t_2+t_3)} \geq \frac{1}{2}n^{\frac{1}{2}(t_2+t_3)}.$$

Going back to Equation (13), we have

$$\frac{\sum_{\boldsymbol{J} \in \mathcal{P}^\circledast(\boldsymbol{d};\boldsymbol{t})}\left|\bigcap_{i=1}^k \mathcal{C}_{J_i}\right|}{(n - 1)!!} \leq \frac{1}{d_1 \cdots d_k}\frac{n^{\delta(2t_2+3t_3)}}{n^{\frac{1}{2}(t_2+t_3)}} = \frac{1}{d_1 \cdots d_k}\, n^{\delta(2t_2+3t_3)-\frac{1}{2}(t_2+t_3)} \qquad (14)$$

Equation (14) must be summed over $\boldsymbol{t}$ and $\boldsymbol{d}$. Let us first fix $\boldsymbol{d}$ and recall that $\boldsymbol{t} = (t_1, t_2, t_3)$ with $(t_2, t_3) \neq (0, 0)$ and $t_2 + t_3$ even (Lemma 6.10).

Consider first the $\boldsymbol{t}$ of the form $(t_1, t_2, 0) = (t_1, 2s, 0)$ ($s \geq 1$). The corresponding subsum of powers of n is bounded above (for $n \geq 2$) by

$$\sum_{s \geq 1}\left(n^{2\delta-\frac{1}{2}}\right)^{2s} = \frac{n^{4\delta-1}}{1 - n^{4\delta-1}} \leq 2n^{4\delta-1}.$$

Similarly, the subsum of powers of n corresponding to the $\boldsymbol{t}$ of the form $(t_1, 0, t_3)$ is bounded above by $2n^{6\delta-1}$.

Next, the subsum corresponding to the $\boldsymbol{t}$ where both t_2 and t_3 are non-zero is bounded above by

$$\sum_{t_2 \geq 1}\sum_{t_3 \geq 1}\left(n^{2\delta-\frac{1}{2}}\right)^{t_2}\left(n^{3\delta-\frac{1}{2}}\right)^{t_3} \leq \left(\sum_{t_2 \geq 1}\left(n^{2\delta-\frac{1}{2}}\right)^{t_2}\right)\left(\sum_{t_3 \geq 1}\left(n^{3\delta-\frac{1}{2}}\right)^{t_3}\right) \leq 2n^{5\delta-1}$$

It follows that, for a fixed tuple $\boldsymbol{d}$,

$$\frac{\sum_{\boldsymbol{J} \in \mathcal{P}^\circledast(\boldsymbol{d};\boldsymbol{t})}\left|\bigcap_{i=1}^k \mathcal{C}_{J_i}\right|}{(n - 1)!!} \leq \frac{2(n^{4\delta-1} + n^{5\delta-1} + n^{6\delta-1})}{d_1 \cdots d_k}.$$

41

Now, summing over $\boldsymbol{d}$, we get

$$\frac{\sum_{\boldsymbol{J}\in\mathcal{P}^{\oplus}(\boldsymbol{d};\boldsymbol{t})}\left|\bigcap_{i=1}^{k}\mathcal{C}_{J_i}\right|}{(n-1)!!} \leq 2(n^{4\delta-1}+n^{5\delta-1}+n^{6\delta-1})\sum_{\boldsymbol{d}}\frac{1}{d_1\cdots d_k}$$

$$\leq 2(n^{4\delta-1}+n^{5\delta-1}+n^{6\delta-1})(H_M-1)^k$$

Since $n^{4\delta-1}+n^{5\delta-1}+n^{6\delta-1}=\mathcal{O}\left(n^{6\delta-1}\right)$, we have, for n large enough,

$$\frac{\sum_{\boldsymbol{J}\in\mathcal{P}^{\oplus}(\boldsymbol{d};\boldsymbol{t})}\left|\bigcap_{i=1}^{k}\mathcal{C}_{J_i}\right|}{(n-1)!!} = (H_M-1)^k\mathcal{O}(n^{6\delta-1}),$$

thus concluding the proof of Lemma 6.9. □

We can now conclude the proof of Proposition 6.3. By Equations (7) and (9), we want to show that, for $\kappa=\lfloor n^\beta\rfloor$ and $\kappa=\lfloor n^\beta\rfloor-1$,

$$\frac{1}{(n-1)!!}\sum_{k=0}^{\kappa}(-1)^k\sum_{\substack{\mathcal{I}\subseteq S\\|\mathcal{I}|=k}}\left|\bigcap_{I\in\mathcal{I}}\mathcal{C}_I\right| = \sum_{k=0}^{\kappa}\frac{(-1)^k}{k!}\frac{A_k}{(n-1)!!}+\sum_{k=0}^{\kappa}\frac{(-1)^k}{k!}\frac{B_k}{(n-1)!!}$$

is $\mathcal{O}(n^{-\alpha})$. By Lemma 6.8, the absolute value of the first sum is bounded above by

$$(1+\mathcal{O}(n^{2\delta-1}))\exp(-(H_M-1)) = e^{1-\gamma}n^{-\alpha}(1+\mathcal{O}(n^{2\delta-1})).$$

And by Lemma 6.9, the absolute value of the second sum is bounded above by

$$\exp(-(H_M-1))\,\mathcal{O}(n^{6\delta-1}) = e^{1-\gamma}n^{-\alpha}\mathcal{O}(n^{6\delta-1}).$$

Thus the whole sum is $\mathcal{O}(n^{-\alpha})$, establishing the expected bound for disjoint unions of silhouette graphs.

Such a union, of size n (a multiple of 6), is connected (and hence silhouette) with probability $1-\frac{5}{6}n^{-1}+o(n^{-1})$ by [7, Proof of Proposition 8.18]. Thus the probability that a silhouette graph has no small simple ab-cycle is, again, $\mathcal{O}(n^{-\alpha})$.

References

[1] G. N. Arzhantseva. Generic properties of finitely presented groups and Howson's theorem. *Comm. Algebra*, 26(11):3783–3792, 1998.

[2] G. N. Arzhantseva and A. Y. Ol'shanskiĭ. Generality of the class of groups in which subgroups with a lesser number of generators are free. *Mat. Zametki*, 59(4):489–496, 638, 1996.

[3] F. Bassino, A. Martino, C. Nicaud, E. Ventura, and P. Weil. Statistical properties of subgroups of free groups. *Random Struct. Algorithms*, 42(3):349–373, 2013.

[4] F. Bassino, C. Nicaud, and P. Weil. Random generation of finitely generated subgroups of a free group. *Internat. J. Algebra Comput.*, 18(2):375–405, 2008.

[5] F. Bassino, C. Nicaud, and P. Weil. Generic properties of subgroups of free groups and finite presentations. In *Algebra and computer science*, volume 677 of *Contemp. Math.*, pages 1–43. Amer. Math. Soc., Providence, RI, 2016.

[6] F. Bassino, C. Nicaud, and P. Weil. On the genericity of Whitehead minimality. *J. Group Theory*, 19(1):137–159, 2016.

[7] F. Bassino, C. Nicaud, and P. Weil. Statistics of subgroups of the modular group. Technical report, `arXiv:2004.00437`, 2020.

[8] T. Budzinski, N. Curien, and B. Petri. The diameter of random Belyi surfaces. Technical report, `arXiv:1910.11809`, 2019.

[9] I. M. S. Dey. Schreier systems in free products. *Proc. Glasgow Math. Assoc.*, 7:61–79 (1965), 1965.

[10] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, 2009.

[11] P. Flajolet, P. Zimmermann, and B. Van Cutsem. A calculus for the random generation of labelled combinatorial structures. *Theor. Comput. Sci.*, 132(2):1–35, 1994.

[12] A. Gamburd. Poisson-Dirichlet distribution for random Belyi surfaces. *Ann. Probab.*, 34(5):1827–1848, 2006.

[13] S. M. Gersten and H. B. Short. Rational subgroups of biautomatic groups. *Ann. of Math. (2)*, 134(1):125–158, 1991.

[14] R. Gilman, A. Miasnikov, and D. Osin. Exponentially generic subsets of groups. *Illinois J. Math.*, 54(1):371–388, 2010.

[15] R. Gitik. Nielsen generating sets and quasiconvexity of subgroups. *J. Pure Appl. Algebra*, 112(3):287–292, 1996.

[16] D. M. Jackson and T. I. Visentin. A character-theoretic approach to embeddings of rooted maps in an orientable surface of given genus. *Trans. Am. Math. Soc.*, 322(1):343–363, 1990.

[17] T. Jitsukawa. Malnormal subgroups of free groups. In *Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001)*, volume 298 of *Contemp. Math.*, pages 83–95. Amer. Math. Soc., Providence, RI, 2002.

[18] I. Kapovich. Detecting quasiconvexity: algorithmic aspects. In *Geometric and computational perspectives on infinite groups (Minneapolis, MN and New Brunswick, NJ, 1994)*, volume 25 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 91–99. Amer. Math. Soc., Providence, RI, 1996.

[19] O. Kharlampovich, A. Miasnikov, and P. Weil. Stallings graphs for quasi-convex subgroups. *J. Algebra*, 488:442–483, 2017.

[20] A. G. Kurosh. *The theory of groups. Vol. II.* Chelsea Publishing Company, New York, N.Y., 1956. Translated from the Russian and edited by K. A. Hirsch.

[21] R. C. Lyndon and P. E. Schupp. *Combinatorial group theory.* Springer-Verlag, 1977.

[22] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial group theory.* Dover, 1976.

[23] J. Maher and A. Sisto. Random subgroups of acylindrically hyperbolic groups and hyperbolic embeddings. *Int. Math. Res. Not. IMRN*, (13):3941–3980, 2019.

[24] L. Markus-Epstein. Algorithmic problems in amalgams of finite groups: Conjugacy and intersection properties. Technical report, `arXiv:0707.0165`, 2007.

[25] L. Markus-Epstein. Stallings foldings and subgroups of amalgams of finite groups. *Internat. J. Algebra Comput.*, 17(8):1493–1535, 2007.

[26] T. W. Müller and J.-C. Schlage-Puchta. Classification and statistics of finite index subgroups in free products. *Adv. Math.*, 188(1):1–50, 2004.

[27] C. Nicaud. Random deterministic automata. In E. Csuhaj-Varjú, M. Dietzfelbinger, and Z. Ésik, editors, *Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part I*, volume 8634 of *Lecture Notes in Computer Science*, pages 5–23. Springer, 2014.

[28] J. J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[29] H. Short. Quasiconvexity and a theorem of Howson's. In *Group theory from a geometrical viewpoint (Trieste, 1990)*, pages 168–176. World Sci. Publ., River Edge, NJ, 1991.

[30] J. R. Stallings. Topology of finite graphs. *Invent. Math.*, 71(3):551–565, 1983.

[31] W. W. Stothers. The number of subgroups of given index in the modular group. *Proc. Roy. Soc. Edinburgh Sect. A*, 78(1-2):105–112, 1977/78.

[32] W. W. Stothers. Free subgroups of the free product of cyclic groups. *Math. Comp.*, 32(144):1274–1280, 1978.