RANDOM QUOTIENTS OF THE MODULAR GROUP ARE RIGID AND ESSENTIALLY INCOMPRESSIBLE

ILYA KAPOVICH AND PAUL SCHUPP

Abstract. We show that for any positive integer \( m \geq 1 \), \( m \)-relator quotients of the modular group \( M = \text{PSL}(2, \mathbb{Z}) \) generically satisfy a very strong Mostow-type isomorphism rigidity. We also prove that such quotients are generically “essentially incompressible”. By this we mean that their “absolute \( T \)-invariant”, measuring the smallest size of any possible finite presentation of the group, is bounded below by a function which is almost linear in terms of the length of the given presentation. We compute the precise asymptotics of the number \( I_m(n) \) of isomorphism types of \( m \)-relator quotients of \( M \) where all the defining relators are cyclically reduced words of length \( n \) in \( M \). We obtain other algebraic results and show that such quotients are complete, Hopfian, co-Hopfian, one-ended, word-hyperbolic groups.

1. Introduction

The idea of genericity in Geometric Group Theory, understood as the study of algebraic properties of random group-theoretic objects, was introduced by Gromov [19, 20] when he indicated that finitely presented groups are “generically” word-hyperbolic. This approach was made precise by Ol’shanskii [38], Arzhantseva-Ol’shanskii [1] and Champetier [10, 11]. Investigations centered around genericity are now an active and important research area (see, for example [1, 2, 3, 4, 14, 34, 35, 36, 37, 38]). One of the main reasons for studying genericity is that one can use the probabilistic method to discover the existence of objects with new and interesting algebraic, algorithmic and geometric properties. A major example is Gromov’s recent construction [21] of a finitely presented group that is not uniformly embeddable into a Hilbert space, which is related to possible counter-examples to the Novikov conjecture.

There are many additional aspects of randomness and genericity. Work of the authors with other colleagues, [22, 23, 24, 25], introduced the notion of generic-case complexity for decision problems. It turns out that most classic group-theoretic decision problems, such as the word, conjugacy, membership and the isomorphism problems, have provably low complexity on “random” inputs even if their worst-case complexity is very high or
even unsolvable. This work subsequently led us to the discovery of “isomorphism rigidity” for generic groups \[24, 26\]. The famous Mostow Rigidity Theorem \[32\] states that if \(M_1\) and \(M_2\) are complete connected hyperbolic manifolds of finite volume and dimension \(n \geq 3\) then their fundamental groups are isomorphic if and only if the manifolds themselves are isometric. For a group \(G\) with a given finite generating set \(A\) the naturally associated geometric structure is the Cayley graph \(\Gamma(G, A)\). We thus say that a class of groups equipped with a specified finite generating set \(A\) is rigid if whenever two groups from this class are isomorphic then their Cayley graphs on \(A\) with the word metric are isometric. Phenomena of this type were known for various classes of Coxeter and Artin groups (e.g \[41, 40, 6, 8, 33\]). In \[26\] Kapovich, Schupp and Shpilrain proved the first such theorem for a “general” class of groups by establishing “isomorphism rigidity” for generic one-relator groups.

In most previously explored contexts rigidity comes from a careful analysis of some kind of particular structure. Thus proofs of quasi-isometric rigidity for non-uniform lattices in semi-simple Lie groups hinge on the study of the structure of flats (see, for example \[43\]). Generic groups provide a conceptually new source of group-theoretic rigidity where rigidity comes from the properties of randomness itself. Rigidity then opens the way to proving results about essential incompressibility and the exact asymptotics of the number of isomorphism classes.

Before stating the main results we introduce some definitions and notation.

**Convention 1.1** (The Modular group). It is well-known that the modular group \(PSL(2, \mathbb{Z})\) is isomorphic to the free product

\[M = \langle a, b | a^2 = b^3 = 1 \rangle.\]

For the remainder of the paper we identify the modular group with \(M\) and use the free product structure. We use \(\eta : M \to M\) to denote the automorphism of \(M\) defined by \(\eta(a) = a, \eta(b) = b^{-1}\).

We take the group alphabet to be \(A = \{a, b, b^{-1}\} \subseteq M\). If \(w\) is a word in the alphabet \(A\) then \(|w|\) denotes the length of \(w\). A word \(w\) in the alphabet \(A\) is reduced if it does not contain any subwords of the form \(aa, bb^{-1}, b^{-1}b, bb, b^{-1}b^{-1}\). A word \(w\) is cyclically reduced if all cyclic permutations of \(w\) are reduced. Note that if \(|w| > 1\) and \(w\) is cyclically reduced then \(|w|\) is necessarily even. As for free groups, every element \(g \in M\) is represented by a unique reduced word \(w\) in the alphabet \(A\) and we define \(|g| = |w|\).

If \(G\) is a group and \(R \subseteq G\), we denote by \(\langle\langle R\rangle\rangle\) the normal closure of \(R\) in \(G\), that is, the smallest normal subgroup of \(G\) containing \(R\).

**Notation 1.2.** We denote the set of all cyclically reduced words in the alphabet \(A\) by \(C\). If \(\tau = (r_1, \ldots, r_m) \in C^m\) is an \(m\)-tuple of cyclically reduced words, the symmetrized closure, \(R(\tau)\), of \(\tau\) in \(M\) is the set consisting
of all cyclic permutations of the elements of \( \tau \) and their inverses. A set is symmetrized if it is already equal to its symmetrized closure.

If \( \tau = (r_1, \ldots, r_m) \in M^m \) an \( m \)-tuple define

\[ |\tau| := \max_{1 \leq i \leq m} |r_i| \]

We set

\[ G_\tau := M/\langle\langle \tau \rangle\rangle = \langle a, b \mid a^2 = b^3 = r_1 = \cdots = r_m = 1 \rangle. \]

If \( m \geq 1 \) is an integer then \( T_m \) denotes the set of all \( m \)-tuples \( (r_1, \ldots, r_m) \in C^m \) such that \( |r_1| = \cdots = |r_m| \).

We next state the definition of “genericity” which we are using.

**Convention 1.3.** Let \( m \geq 1 \) and let \( S \subseteq (A^*)^m \) be a set of \( m \)-tuples of words in the alphabet \( A \) and let \( n \geq 0 \). Then

\[ \gamma(n, S) = \#\{ \tau \in S : |\tau| = n \} \]

and

\[ \rho(n, S) = \#\{ \tau \in S : |\tau| \leq n \}. \]

**Definition 1.4** (Genericity). Let \( m \geq 1 \) be an integer and let \( X \subseteq M^m \) be a nonempty subset. Let \( S \subseteq X \).

We say that \( S \) is exponentially generic in \( X \) if

\[ \lim_{n \to \infty} \frac{\rho(n, S)}{\rho(n, X)} = 1, \]

and the convergence is exponentially fast. Similarly, we say that \( S \) is exponentially negligible in \( X \) if

\[ \lim_{n \to \infty} \frac{\rho(n, S)}{\rho(n, X)} = 0, \]

and the convergence is exponentially fast.

Clearly, a subset of \( X \) is exponentially generic if and only if its complement in \( X \) is exponentially negligible. We will only be interested in the cases \( X = C^m \) and \( X = T_m \) in this paper.

Our first main result about random quotients of the modular group is:

**Theorem A.** [Isomorphism Rigidity] Let \( m \geq 1 \). There exist an exponentially generic subset \( Q_m \) of \( C^m \) and an exponentially generic subset \( U_m = Q_m \cap T_m \) of \( T_m \) such that the following hold:

1. There exists an algorithm that, given \( \tau \in C^m \), decides, in time quartic in \( |\tau| \), whether or not \( \tau \in Q_m \).
2. For every \( \tau \in Q_m \) the group \( G_\tau \) is word-hyperbolic and one-ended. Moreover, the elements \( a \) and \( b \) respectively have orders 2 and 3 in \( G_\tau \).
3. For every \( \tau \in Q_m \) the group \( G_\tau \) is complete, that is, the center of \( G_\tau \) is trivial and \( \text{Out}(G_\tau) = 1 \).
(4) For any \( \tau \in Q_m \) and any finite symmetrized \( S \subseteq C \) satisfying \( C'(1/8) \) we have \( G_\tau \cong M/\langle\langle S \rangle\rangle \) if and only if \( R(\tau) = S \) or \( R(\tau) = \eta(S) \) in \( M \).

(5) For \( \tau = (r_1, \ldots, r_m), \sigma = (s_1, \ldots, s_m) \in Q_m \) we have \( G_\tau \cong G_\sigma \) if and only if there exist a reordering \( \tau' = (r'_1, \ldots, r'_m) \) of \( \tau \) and \( \epsilon \in \{0, 1\} \) such that each \( r'_i \) is a cyclic permutation of \( \eta^\epsilon(s_i) \) or \( \eta^\epsilon(s_i^{-1}) \) for \( i = 1, \ldots, m \).

(6) If \( \tau \in U_m, \sigma \in U_p \) with \( |\tau| = |\sigma| \) but \( p > m \) then \( G_\tau \not\cong G_\sigma \).

Part (5) of the above theorem says that for \( \sigma, \tau \in Q_m \) the groups \( G_\sigma \) and \( G_\tau \) are isomorphic if and only if their Cayley graphs with respect to the given generating set \( a, b \) are isomorphic as labelled graphs by a graph isomorphism preserves labels \( a \) of edges and either preserves all labels \( b \) or inverts all of them.

**Theorem B.** [Homomorphism Rigidity] Let \( m \geq 1 \) be an integer. Then the following hold:

1. Let \( \tau \in Q_m \). Then for any homomorphism \( \psi : M \rightarrow G_\tau \) exactly one of the following occurs:
   - (a) The image \( \psi(M) \leq G_\tau \) is a finite cyclic group of order at most 3.
   - (b) The map \( \psi \) is injective but not surjective.
   - (c) The map \( \psi \) is surjective but not injective and the pair \( (\psi(a), \psi(b)) \) is conjugate in \( G_\tau \) to \( (a, b) \) or \( (a, b^{-1}) \).
2. If \( \sigma, \tau \in U_m \) and \( |\sigma| < |\tau| \) then for every homomorphism \( \psi : G_\sigma \rightarrow G_\tau \) the image \( \psi(G_\sigma) \) is a finite cyclic group of order at most 3.
3. If \( \sigma, \tau \in U_m \) and \( |\sigma| = |\tau| \) then for any homomorphism \( \psi : G_\sigma \rightarrow G_\tau \) either the image \( \psi(G_\sigma) \) is a finite cyclic group of order at most 3 or \( \psi \) is an isomorphism.
4. For every \( \tau \in Q_m \) the group \( G_\tau \) is a complete, Hopfian and co-Hopfian.

Since \( G \) is a complete, Hopfian, co-Hopfian group, if \( \psi \) is any endomorphism of \( G \) then \( \psi \) is injective if and only if \( \psi \) is surjective if and only if \( \psi \) is an inner automorphism. It seems likely that “endomorphism rigidity” is another general aspect of “randomness”: A random structure should not have any endomorphisms except those absolutely required by the nature of the structure.

The Hopficity and co-Hopficity of \( G_\tau \) in Theorem 3 are the analog of deep results of Sela about torsion-free hyperbolic groups [44, 45]. But the proofs here are much simpler precisely because of the limited torsion and do not require Rips’ machinery for analyzing group actions on \( \mathbb{R} \)-trees.

In considering quotients of the modular group we consider groups which are obviously presented as such quotients, that is, presentations of the form

\[
G = \langle a, b \mid a^2 = b^3 = 1, r_1 = 1, \ldots, r_m = 1 \rangle.
\]
Schupp [42] proved that the triviality problem restricted to such presentations remains undecidable. The isomorphism problem for such presentations is thus certainly undecidable. Indeed, the proof provided shows that the isomorphism problem restricted to a fixed class $P_m$ defined immediately below is undecidable for all $m \geq 15$. (This uses the fact that there is a 2-generator, 11-relator group with unsolvable word problem.) Nonetheless, rigidity shows that the isomorphism problem is generically easy (see [22] for the definitions of generic-case complexity):

**Corollary 1.5.** Let $m \geq 1$ be an arbitrary integer. Let $P_m$ be the class of presentations of the form

$$\langle a, b \mid a^2 = b^3 = 1, r_1 = 1, \ldots, r_m = 1 \rangle,$$

where $r_i$ are cyclically reduced words in $M$.

Then the isomorphism problem for groups defined by presentations from the class $P_m$ is strongly generically quartic time.

**Proof.** We will describe a partial algorithm that solves the isomorphism problem for $P_m$ strongly generically in quartic time.

The set of pairs of tuples $(\sigma, \tau) \in P_m \times P_m$ such that one of $R(\sigma), R(\tau)$ satisfies the $Q_m$ condition and the other satisfies the standard $C(1/8)$ small cancellation condition is exponentially generic. By Theorem A we can verify if this is indeed the case in quartic time.

If it is not the case, the algorithm does not return any answer. If the condition is satisfied then by Theorem A we know that $G_\tau$ is isomorphic to $G_\sigma$ if and only if $R(\tau) = R(\sigma)$ or $R(\tau) = \eta(R(\sigma))$. We can verify if one of these equalities holds in cubic time. If it does the groups are isomorphic and if not then the groups are not isomorphic. 

□

Once one has rigidity one can compute the exact asymptotics of the number of isomorphism types of groups given by relevant presentations. Note that the statement of Theorem C below does not involve the notion of genericity in any way.

**Theorem C.** [Counting Isomorphism Types] Let $m \geq 1$. Let $I_m(n)$ denote the number of isomorphism types of groups given by presentations of the form

$$M/\langle\langle r_1, \ldots, r_m \rangle\rangle,$$

where $r_1, \ldots, r_m$ are cyclically reduced words of length $n$ in $M$.

Then for even $n \to \infty$

$$I_m(n) \sim \frac{(2^{n/2}+1)^m}{2^m(2n)^m},$$

that is

$$\lim_{k \to \infty} \frac{2I_m(2k)}{(2^{k+1})^m} \frac{m!(4k)^m}{m!} = 1.$$
The theory of Kolmogorov complexity is a general theory of “descriptive complexity” and the first basic result is that a long random word over a finite alphabet is essentially its own shortest description. One might summarize this result by saying that random words are “essentially incompressible”.

Rigidity is inherent in this situation since two words are equal only if they are identical. In other situations where there is rigidity for algebraic structures, one can also investigate the appropriate descriptive complexity. In the case of groups, the idea of the $T$-invariant was introduced by Delzant [15]. We need here a slight variation which we call the absolute $T$-invariant.

**Definition 1.6.** [Absolute $T$-invariant] Let $\Pi = \langle a_1, \ldots, a_s | w_1, \ldots, w_t \rangle$ be a finite group presentation. We define $\ell_1(\Pi) := \sum_{i=1}^{t} |w_i|$.

For a finitely presentable group $G$ let $T_1(G)$ be the minimum of $\ell_1(\Pi)$ taken over all finite presentations $\Pi$ of $G$. The number $T_1(G)$ is called the absolute $T$-invariant or the descriptive complexity of $G$.

The definition of $T_1(G)$ differs slightly from Delzant’s $T$-invariant $T(G)$ of a finitely presentable group $G$ where the “length” being minimized is $\ell(\Pi) = \sum_{i=1}^{t} \max\{0, |w_i| - 2\}$. It turns out that $T(G)$ is better for certain topological arguments. In particular, Delzant proved that $T(G_1 * G_2) = T(G_1) + T(G_2)$. The $T$-invariant plays an important role in Delzant and Potyagailo’s proof of the strong accessibility (or “hierarchical decomposition”) theorem for finitely presented groups [16]. Both $T(G)$ and $T_1(G)$ are related to the notion of Matveev complexity for 3-manifolds, and this connection is explored in a recent paper of Pervova and Petronio [39].

**Theorem D.** [Essential Incompressibility] Let $m \geq 1$ be a fixed integer. For any $0 < \epsilon < 1$ there is an integer $n_0 > 0$ and a constant $L = L(m, \epsilon) > 0$ with the following property.

Let $J$ be the set of all tuples $\tau \in \mathcal{T}_m$ such that $T_1(G_\tau) \log_2 T_1(G_\tau) \geq L|\tau|$. Then for any $n \geq n_0$

$$\frac{\gamma(n, J)}{\gamma(n, \mathcal{T}_m)} \geq 1 - \epsilon.$$

Informally, Theorem D says that for an “almost generic” $m$-relator quotient $G_\tau$ of $M$ with relators of equal length the function $T_1(G_\tau)$ is bounded from below by an “almost linear” function in terms of the length of the given presentation of $G_\tau$. Thus “almost generic” $m$-relator quotients of $M$ are essentially incompressible in the sense that the given presentation is almost the shortest possible description of the group. While such a conclusion may not be unexpected, it is surprising that one is actually able to prove this result. Note that $T_1(G) = 0$ if and only if $G$ is a free group and that the only free quotient of the modular group is the trivial group. Since the
triviality problem is undecidable for quotients of the modular group [42], we cannot in general even decide if $T_1 = 0$. Theorem D is a generalization to the present situation of a similar result for random one-relator groups obtained by the authors in [25]. As to be expected, basic results about Kolmogorov complexity are crucial to the proof of Theorem D.

Our previous results on rigidity and related topics were restricted to one-relator groups [24, 25, 26] because the arguments relied on a classic result of Magnus [30]: If two elements $r$ and $s$ in a free group $F$ have the same normal closures then $r$ is conjugate to $s^{\pm 1}$ in $F$. Similar statements are generally false for subsets of free groups with more than one element. In this paper we overcome that difficulty in studying generic quotients of the modular group. First note that the set of infinite quotients of the modular group is in some sense “very ample”. Miller and Schupp [31] showed that every countable group can be embedded in a complete, Hopfian quotient of the modular group and the embedding preserves the property of being finitely presented. Schupp [42] later proved that every countable group can be embedded in a simple group which is quotient of the modular group. The presence of torsion of a very restricted nature greatly limits homomorphisms between quotients of $M$ and, like the papers cited above, we exploit that idea here. Given the extra control on homomorphisms, it turns out to be possible to replace the result of Magnus mentioned above by its general analog in small cancellation theory. Greendlinger [18] proved the following theorem: If $S$ and $R$ are symmetrized $C'(1/6)$-subsets of a free group with $\langle\langle S\rangle\rangle = \langle\langle R\rangle\rangle$ then $S = R$. The proof of the similar result is essentially unchanged for subsets of $M$ satisfying a suitable small cancellation condition.

We adopt the “Arzhantseva-Ol’shanskii method” to study quotients of the modular group. First, we shall use a version of the very strong “non-readability” small cancellation hypothesis introduced by Arzhantseva and Ol’shanskii [11]. Verifying that $m$-relator presentations over the modular group which satisfy such a condition is a generic set is simpler than for quotients of free groups. Second, we represent subgroups of $M$ by labelled graphs as usual. In our case, these are $A$-graphs, that is graphs where edges are labelled by the elements of $A = \{a, b, b^{-1}\} \subseteq M$. To take advantage of the strong small cancellation condition one needs to perform certain Arzhantseva- Ol’shanskii moves which preserve the subgroup of $G$ represented by an $A$-graph $\Gamma$. A crucial observation established in the present paper is that performing such moves on separating arcs results in Torelli equivalence at the level of generating tuples.

There are several places in the proofs of the main results of this paper where we substantially use the fact that we are working specifically with the quotients of $M$. First, it is important for our arguments to know that $M$ is a free product of finite cyclic groups. We use small cancellation considerations to conclude that for a generic quotient $G = M/N$ of $M$ every element of order 2 is conjugate to $a$ in $G$ and every element of order 3 is conjugate to $b^{-1}$. Thus we know that if $\psi : M \to G$ is a homomorphism with
ψ(a) ≠ 1 and ψ(b) ≠ 1 then (ψ(a), ψ(b)) = (u_1 a u_1^{-1}, u_2 b u_2^{-1}). Next we need to conclude that if ψ as above is not injective then in fact the 2-tuple (ψ(a), ψ(b)) is conjugate in G to (a, b^{±1}). At this point we use AO-moves and genericity assumptions to prove that (ψ(a), ψ(b)) is Torelli equivalent and hence conjugate to (a, b^{±1}). This is the place in the proof where it is critically important for the argument that the number of generators be equal two. Indeed, for 2-tuples of elements Torelli equivalence is the same as conjugacy. However, for k-tuples with k ≥ 3 Torelli equivalence is not the same thing as conjugacy and our arguments do not apply in that case. The reason for this is a well-known fact that for k ≥ 3 the Torelli subgroup of Aut(F_k), consisting of all automorphisms of F_k that induced the identity map in the abelianization of F_k, is strictly bigger than the group of inner automorphisms of F_k.

After establishing that (ψ(a), ψ(b)) is conjugate to (a, b^{±1}) in G, we apply Greendlinger’s Theorem that symmetrized small cancellation sets with the same normal closures are equal, to conclude the proof of Theorem A.

We strongly believe that the results of this paper should also hold for generic quotients of free groups of arbitrary finite rank k ≥ 2, and, more generally, of free products of k ≥ 2 cyclic groups. Carrying out a proof in that context requires establishing some version of the following “Stability Conjecture”. Our computer experiments so far tend to support the conjecture.

**Conjecture 1.7** (The Stability Conjecture). Fix k ≥ 2 and m ≥ 1 and let F = F(a_1, ..., a_k). Then there exists an algorithmically recognizable generic class Y of m-tuples of elements of F with the following property. If σ, τ ∈ Y and α ∈ Aut(F) are such that R(σ) and R(α(τ)) have the same normal closure in F then R(σ) = R(α(τ)).

2. Arzhantseva-Ol’shanskii moves on graphs and Torelli equivalence

Since we represent subgroups by labelled graphs we completely list our conventions. We follow the same conventions about graphs as Serre.

**Convention 2.1.** A graph is a tuple Γ = (V, E, o, t, −1) where V = V(Γ) is the vertex set of Γ, E = E(Γ) is the edge set of Γ and o : E → V, t : E → V and −1 : E → E are the origin, terminus and inverse maps. We require that −1 : E → E is an involution with e^{−1} ≠ e and t(e) = o(e^{−1}).

An orientation on Γ is a partition E = E^+ ∪ E^- such that e ∈ E^+ if and only if e^{−1} ∈ E^-.

An arc is a simple edge-path where all vertices have degree 2 in Γ, except possibly for the initial and the terminal vertices.

We discuss a version of Arzhantseva-Ol’shanskii moves in the general setting of abstract graphs. The key observation is that performing such a move on a separating arc of a graph naturally corresponds to the Torelli equivalence at the level of the free bases of the fundamental groups.
Definition 2.2 (Abstract AO-move). Let \( \Gamma \) be a connected graph. Let \( p_1, p_2 \) be a path in \( \Gamma \) such that \( \gamma \) is a non-loop arc of \( \Gamma \) and the paths \( p_1, p_2 \) do not pass through \( \gamma \) or \( \gamma^{-1} \).

Modify \( \Gamma \) by first attaching to \( \Gamma \) a new arc \( \gamma' \) (possibly consisting of several edges) from \( o(p_1) \) to \( t(p_2) \) and then removing the arc \( \gamma \). The resulting graph \( \Gamma' \) is said to be obtained from \( \Gamma \) by a move of type AO. We define the AO-map \( P : \Gamma \to \Gamma' \) associated to this AO-move as follows. We set \( P \) to be the identity map on all edges and vertices of \( \Gamma \) that are not changed by the AO-move and thus are common for \( \Gamma \) and \( \Gamma' \). This includes the endpoints of \( \gamma \) and \( \gamma' \). We define \( P \) on \( \gamma \) to “push” \( \gamma \) to the path \( p_{1}^{-1}/p_{2}^{-1} \). The map \( P : \Gamma \to \Gamma' \) is a homotopy equivalence. Indeed, undoing the AO move from \( \Gamma \) to \( \Gamma' \) is an AO-move from \( \Gamma' \) to \( \Gamma \) consisting in removing \( \gamma' \) and adding back \( \gamma \). The map \( P' : \Gamma' \to \Gamma \) defined similarly to \( P \) is easily seen to be a homotopy inverse of \( P \). Thus \( P : \Gamma \to \Gamma' \) is a homotopy equivalence.

Definition 2.3 (Elementary Torelli moves). Let \( \tau = (g_1, \ldots, g_n) \) be an \( n \)-tuples of elements of a group \( G \). The following transformations of \( \tau \) will be called the elementary Torelli moves:

1. For some subset \( S \subseteq \{1, 2, \ldots, n\} \) and some \( h \in \langle \{g_j | j \in S\} \rangle \leq G \) for each \( i \in S \) replace \( g_i \) by \( h g_i h^{-1} \).
2. For some subset \( S \subseteq \{1, 2, \ldots, n\} \) and some \( g \in \langle \{g_j | j \notin S\} \rangle \leq G \) for each \( i \in S \) replace \( g_i \) by \( g g_i g^{-1} \).
3. Conjugate the entire tuple \( \tau \) by some element \( g \in G \).

Definition 2.4 (Torelli Equivalence). We say that two \( n \)-tuples \( \tau \) and \( \tau' \) of elements of \( G \) are Torelli-equivalent if there exists a finite chain of Torelli moves taking \( \tau \) to \( \tau' \).

Note that if \( n = 2 \) we have an ordered pair of elements and then any two Torelli-equivalent pairs generate conjugate subgroups of \( G \).

Notation 2.5. Let \( \Gamma \) be a finite connected graph free of rank \( n \geq 1 \). Let \( T \) be a maximal subtree of \( \Gamma \).

If \( x_0 \in VT \) is a base-vertex, then \( T \) defines a free basis of \( \pi_1(\Gamma, x_0) \) as follows. For each edge \( e \in E^+(\Gamma - T) \) define the path \( c(e) \) as \( c(e) := [x_0, o(e)]_{E}[t(e), x_0] \), where \([x, y]_E\) stands for the unique reduced edge-path from \( x \) to \( y \) in \( T \).

Choose an orientation \( ET = E^+ \Gamma \cup E^- \Gamma \) and choose an ordering \( e_1, \ldots, e_n \) of all the elements of \( E^+(\Gamma - T) \). Then the \( n \)-tuple \( (c(e_1), \ldots, c(e_n)) \) is a free basis of \( \pi_1(\Gamma, x_0) \). We will denote the tuple \( (c(e_1), \ldots, c(e_n)) \) by \( S_{T,x_0} \). While \( S_{T,x_0} \) does depend on the choice of an orientation on \( E(\Gamma - T) \) and on the choice of an ordering on \( E^+(\Gamma - T) \), these choices will usually be fixed and explicit references to them will be suppressed.

Convention 2.6 (AO move on a separating arc). Let \( \Gamma' \) be obtained from a finite connected graph \( \Gamma \) by an abstract AO-move via removing an arc \( \gamma \) and adding an arc \( \gamma' \), as in Definition 2.2. Suppose that \( \gamma \) is a separating
arc of $\Gamma$. Let $T$ be a maximal subtree in $\Gamma$, so that $T$ contains $\gamma$. Suppose that we fix an orientation on $\Gamma$ and an ordering on $E^+(\Gamma - T)$.

Put $T' := T - \{\gamma\} \cup \{\gamma'\}$. Thus $T'$ is a maximal subtree in $\Gamma'$.

Note that $E(\Gamma - T) = E(\Gamma' - T')$. We choose an orientation on $\Gamma'$ so that it agrees with $\Gamma$ on $\Gamma' - T'$, so that $E^+(\Gamma - T) = E^+(\Gamma' - T')$. We also order $E^+(\Gamma' - T')$ exactly as $E^+(\Gamma - T)$ was ordered.

Note also that $x_0 = o(\gamma) = P(x_0)$ is a vertex of both $\Gamma$ and $\Gamma'$.

The tuples $S_{T,x_0}$ and $S_{T',x_0}$ of elements of $\pi_1(\Gamma, x_0)$ and $\pi_1(\Gamma', x_0)$ are defined according to the above conventions regarding the orientations and the orderings of positive edges outside of the specified maximal trees.

In general, $A0$-moves on nonseparating arcs result in Nielsen equivalence at the level of the tuples $S_{T,x_0}$ (see [5] [24]). We observe here that if an $A0$-move is performed on a separating arc $\gamma$, this move results in Torelli equivalence:

**Proposition 2.7.** Let $\Gamma$ be a finite connected graph with the fundamental group free of rank $n \geq 1$ and without degree-one vertices. Let $\Gamma'$ be obtained from $\Gamma$ by an abstract $A0$-move removing an arc $\gamma$ and adding an arc $\gamma'$. Let $P : \Gamma \rightarrow \Gamma'$ be the $A0$-map corresponding to this $A0$-move. Let $x_0 = o(\gamma)$, so that $P(x_0) = x_0$.

Suppose that $\gamma$ is a separating arc of $\Gamma$.

Let $T$ be a maximal subtree in $\Gamma$ (and hence $T$ contains $\gamma$). Put $T' := T - \{\gamma\} \cup \{\gamma'\}$. Thus $T'$ is a maximal subtree in $\Gamma'$. Let the orientations and the orderings of positive edges outside of maximal trees are chosen as in Convention 2.6.

Let $P_\# : \pi_1(\Gamma, x_0) \rightarrow \pi_1(\Gamma', x_0)$ be the homomorphism of fundamental groups induced by the $A0$-map $P$ above. Then the tuples $P_\#(S_{T,x_0})$ and $S_{T',x_0}$ are Torelli-equivalent in $\pi_1(\Gamma', x_0)$.

**Proof.** Since $\gamma$ is a separating arc and is thus not a loop, the graph $\Gamma - \{\gamma\}$ consists of two connected components: $\Gamma_1$ containing $x_0 = o(\gamma)$ and $\Gamma_2$ containing $t(\gamma)$. The set $E^+(\Gamma - T)$ is partitioned as: $\{e_1, \ldots, e_k, f_1, \ldots, f_{n-k}\}$ where $e_i \in \Gamma_1$ and $f_j \in \Gamma_2$. Moreover, $T_q = T \cap \Gamma_q$ is a maximal tree in $\Gamma_q$ for $q = 1, 2$.

For future reference we need to explicitly write down the $n$-tuple $S_{T,x_0}$ corresponding to $T$. Let $y := [o(\gamma), o(p_1)]_T$ and let $z := [t(\gamma), t(p_2)]_T$. For each $e_i \in E^+(\Gamma_1 - T)$ let $y_i := [o(\gamma), o(e_i)]_T$ and let $y'_i := [t(e_i), o(\gamma)]_T$. Similarly for each $f_j$ let $z_j$ and $z'_j$ be the paths $[t(\gamma), o(f_j)]_T$ and of $[t(f_j), t(\gamma)]_T$ accordingly. Note that $[t(\gamma'), o(f_j)]_T$ is homotopic relative endpoints in $T$ to $z^{-1}z_j$ and that $[t(f_j), t(\gamma')]_T$ is homotopic relative endpoints in $T$ to $z'_jz$.

Recall that $x_0 = o(\gamma)$ is the base-vertex of $\Gamma$ and note that $x_0 = P(x_0)$ is still the base-point of $\Gamma'$.

Then by definition the $n$-tuple $S_{T,x_0}$ corresponding to $T$ has the form:

$$S_{T,x_0} = (r_1, \ldots, r_k, s_1, \ldots, s_{n-k}),$$

where $r_i = y_ie_iy'_i$ and $s_j = \gamma z_j f_j z'_j \gamma^{-1}$. 


Let $\Gamma'$ now be obtained from $\Gamma$ by removing $\gamma$ and adding an arc $\gamma'$ from $o(p_{1})$ to $t(p_{2})$. 

By definition of $P$ we have $P_{\#}(r_{i}) = r_{i}$ for $i = 1, \ldots, k$. Also for $j = 1, \ldots, n - k$ we have

$$P_{\#}(s_{j}) = p_{1}^{-1} \gamma' p_{2}^{-1} z_{j} f_{j} z_{j}^{-1} p_{2}(\gamma')^{-1} p_{1}.$$ 

Recall that $T' := T - \{e\} \cup \{\gamma'\}$ is a maximal subtree in $\Gamma'$ and We wish to compute explicitly the tuple $1$ as they were for $\Gamma$, that is the base-vertex.

Note that $E^+(\Gamma - T) = E^+(\Gamma' - T') = \{e_{1}, \ldots, e_{k}, f_{1}, \ldots, f_{n-k}\}$.

Clearly, the elements of $S_{T',x_{0}}$ corresponding to $e_{i}$ remain the same for $\Gamma'$ as they were for $\Gamma$, that is $r_{i} = y_{i} e_{i} y_{i}'$. The elements $s_{j}$ corresponding to the $f_{j}$ will change to

$$s_{j}' = y_{\gamma'} [t(\gamma'), o(f_{j})] r_{f_{j}}[t(f_{j}), t(\gamma')] T(\gamma')^{-1} y_{-1}^{-1} = y_{\gamma'} z_{-1} j f_{j} z_{j} z(\gamma')^{-1} y_{-1}^{-1}.$$ 

Since $y_{\gamma'} p_{1}$ is a loop at $x_{0}$ in $\Gamma_{1}$ and $y_{\gamma'} p_{2}^{-1} z(\gamma')^{-1} y_{-1}^{-1}$ is a loop at $x_{0}$ in $y \cup \gamma' \cup \Gamma_{2}$, we conclude that $y_{\gamma'} p_{1} = W_{1}(r_{1}, \ldots, r_{k})$ in $\pi_{1}(\Gamma, x_{0})$ and $y_{\gamma'} p_{2}^{-1} z(\gamma')^{-1} y_{-1}^{-1} = W_{2}(s_{1}', \ldots, s_{n-k}')$ in $\pi_{1}(\Gamma, x_{0})$ for some words $W_{1}, W_{2}$.

Recall also that $P(\gamma) = p_{1}^{-1} \gamma' p_{2}^{-1}$. Therefore in $\pi_{1}(\Gamma', x_{0})$ we have

$$P_{\#}(s_{j}) = p_{1}^{-1} \gamma' p_{2}^{-1} z_{j} f_{j} z_{j}^{-1} p_{2}(\gamma')^{-1} p_{1} = (p_{1}^{-1} y_{\gamma'} p_{2}^{-1} z(\gamma')^{-1} y_{-1})(y_{\gamma'} z_{-1} j f_{j} z_{j} z(\gamma')^{-1} y_{-1}^{-1})(y_{\gamma'} z_{-1} p_{2}(\gamma')^{-1} y_{-1}^{-1} y_{\gamma'} p_{1}) = W_{1} W_{2} s_{j}' W_{2}^{-1} W_{1}^{-1}.$$ 

Recall that $W_{1} = W_{1}(r_{1}, \ldots, r_{k})$ and $W_{2} = W_{2}(s_{1}', \ldots, s_{n-k}')$. Hence the $n$-tuples

$$S_{T',x_{0}} = (r_{1}, \ldots, r_{k}, s_{1}', \ldots, s_{n-k}')$$

and

$$P_{\#}(S_{T',x_{0}}) = (r_{1}, \ldots, r_{k}, W_{1} W_{2} s_{1}' W_{2}^{-1} W_{1}^{-1}, \ldots, W_{1} W_{2} s_{n-k}' W_{2}^{-1} W_{1}^{-1})$$

are Torelli-equivalent in $\pi_{1}(\Gamma', x_{0})$, as claimed.

\[\square\]

**Convention 2.8.** An $A$-graph is a graph $\Gamma$ where every edge $e$ is labelled by an element $\mu(e) \in A$ such that $\mu(e^{-1}) = (\mu(e))^{-1}$. Thus $\mu(e) = a$ iff $\mu(e^{-1}) = a$ and $\mu(e) = b$ iff $\mu(e^{-1}) = b^{-1}$. For an edge-path $p = e_{1} \ldots e_{i}$ in $\Gamma$ the label $\mu(p) = \mu(e_{1}) \ldots \mu(e_{i})$ is a word in the alphabet $A$.

Let $G = M/N$ be a fixed quotient of the modular group. If $\Gamma$ is an $A$-graph with a base-vertex $x_{0}$, there is a natural labelling homomorphism $\phi : \pi_{1}(\Gamma, x_{0}) \rightarrow G$ that sends the homotopy class of a closed edge-path at $x_{0}$ to the element of $G$ represented by the label of that path. We say that $H = \phi(\pi_{1}(\Gamma, x_{0})) \leq G$ is the subgroup of $G$ represented by $(\Gamma, x_{0})$. If $\Gamma$ is connected then the conjugacy class of $H$ does not depend on the choice of the base-vertex.
Definition 2.9 (Arzhantseva-Ol’shanskii move: move AO on A-graphs).
Let \( N \triangleleft M \) and \( G = M/N \) be a fixed quotient of \( M \). Suppose \( \Gamma \) is a connected \( A \)-graph. Let \( p_1 \gamma p_2 \) be a path in \( \Gamma \) such that \( \gamma \) is a non-loop arc of \( \Gamma \) and the paths \( p_1, p_2 \) do not pass through \( \gamma \) or \( \gamma^{-1} \). Let \( u_1, u_2 \) be the labels of \( p_1, p_2 \) and let \( u \) be the label of \( \gamma \). Suppose \( v \) is a reduced word in \( A \) such that \( u_1 u u_1 = v \) in \( G \).

Modify \( \Gamma \) by first attaching to \( \Gamma \) a new arc \( \gamma' \) labelled \( v \) from \( o(p_1) \) to \( t(p_2) \) and then removing the arc \( \gamma \). The resulting \( A \)-graph \( \Gamma' \) is said to be obtained from \( \Gamma \) by an AO-move.

Proposition 2.7 immediately implies:

Corollary 2.10. Let \( N \triangleleft M \) and \( G = M/N \) be a fixed quotient of \( M \). Let \( \Gamma \) be a finite connected \( A \)-graph with the fundamental group free of rank \( n \geq 1 \).

Suppose that an AO-move applies to \( \Gamma \) and let \( p_1, \gamma, p_2, \gamma', \Gamma' \) be as in Definition 2.9.

Suppose also that \( \gamma \) is a separating arc of \( \Gamma \).

Let \( T \) be a maximal subtree in \( \Gamma \) (and hence \( T \) contains \( \gamma \)). Put \( T' := T - \{ \gamma \} \cup \{ \gamma' \} \). Thus \( T' \) is a maximal subtree in \( \Gamma' \).

Let \( x_0 \in V \Gamma \) and \( x_0' \in V \Gamma' \) be base-vertices. Let \( \phi : \pi_1(\Gamma, x_0) \to G \), \( \phi' : \pi_1(\Gamma', x_0') \to G \) be the labelling homomorphisms.

Then the tuples \( \phi(S_{\Gamma,x_0}) \) and \( \phi'(S_{\Gamma',x_0'}) \) are Torelli-equivalent in \( G \).

In particular, if \( n = 2 \), then the 2-tuples \( \phi(S_{\Gamma,x_0}) \) and \( \phi'(S_{\Gamma',x_0'}) \) are conjugate in \( G \).

3. The Generic Nonreadability Condition

Recall that we are using the group alphabet \( A = \{a,b,b^{-1}\} \subseteq M \). and that a word \( w \) in the alphabet \( A \) is reduced if it does not contain any subwords of the form \( aa, bb^{-1}, b^{-1}b, bb^{-1}b^{-1} \). Note that if \( w \in \mathcal{C} \) is a cyclically reduced word with \( |w| > 1 \) then either \( w \) begins with \( a \) and ends with \( b \) or \( w \) begins with \( b^{-1} \) and ends with \( a \) and so \( w \) has even length in both cases.

The following lemma is therefore straightforward.

Lemma 3.1. The following hold:

1. If \( n \geq 2 \) is an even integer then
   \[ \gamma(n, \mathcal{C}) = \gamma(n+1, \mathcal{C}) = 2 \cdot 2^{n/2}. \]
2. There exist constants \( c_1, c_2 > 0 \) such that for every \( n \geq 1 \)
   \[ c_1 2^{n/2} \leq \rho(n, \mathcal{C}) \leq c_2 2^{n/2}. \]

The following statement is a straightforward corollary of the definitions of genericity and of Lemma 3.1.

Proposition 3.2. Let \( m \geq 1 \) be an integer. Then the following hold:

1. A subset \( S \subseteq \mathcal{C}^m \) is exponentially negligible in \( \mathcal{C}^m \) if and only if
   \[ \lim_{n \to \infty} \frac{\rho(n, S)}{2^{mn/2}} = 0. \]
and the convergence is exponentially fast.

(2) Let \( S \subseteq T_m \). Then \( S \) is exponentially negligible in \( C_m \) if and only if \( S \) is exponentially negligible in \( T_m \).

(3) A subset \( S \subseteq T_m \) is exponentially negligible in \( T_m \) if and only if for even \( n \to \infty \)
\[
\frac{\gamma(n, S)}{2^{mn/2}} \to 0
\]
and the convergence is exponentially fast.

The idea of an Arzhantseva-Ol’shanskii condition is that large parts of the relators which one wants to consider are not “readable” along certain graphs. In studying quotients of the modular group we need only consider one type of graph.

**Definition 3.3** (Barbell graphs). Let \( u \) be a word in \( A^* \). The \( u \)-barbell is the graph \( \Gamma \) with a loop-edge \( e \) labelled \( a \), a loop-edge \( f \) labelled \( b \) and a simple arc \( p \) labelled by \( u \) connecting the vertex of \( e \) to the vertex of \( f \). A barbell graph \( \Gamma \) is reduced if \( u \) is a cyclically reduced word of length \( 2k \geq 2 \) which begins with \( b \) and ends with \( a \). A word \( w \) is readable in \( \Gamma \) if there exists a vertex \( v \in \Gamma \) and a path \( \gamma \) starting at \( v \) with label \( w \).

Even on a very simple example such as \( u = ba \), one quickly sees that the number of all words readable on the \( u \)-barbell is exponentially falling behind the number of all words. We first need to estimate the number of all words of length \( n \) readable in a fixed reduced barbell graph.

**Lemma 3.4.** Let \( \Gamma \) be a reduced \( u \)-barbell graph where \( |u| = 2k \) and \( k \geq 1 \). Then for \( n \geq 1 \) the number of all reduced words of length \( n \) readable in \( \Gamma \) is at most
\[
c_3 2^k 2^{n/(4k+2)},
\]
where \( c_3 > 1 \) is a constant independent of \( u,n,k \).

**Proof.** The graph \( \Gamma \) has \( (2k+1) \) vertices and for each vertex \( v \) on can begin reading in either of two directions. Let \( w \) be any word of length \( n \) readable in \( \Gamma \). Then \( w \) can be written as
\[
w = w_1 w' w_2
\]
where each \( |w_i| < (4k+1) \) and transverses the \( b \)-loop at most once, and where \( w' \) has the form
\[
w' = (aub^{\epsilon_1} u^{-1}) \ldots (aub^{\epsilon_t} u^{-1})
\]
with \( \epsilon_j \in \{1, -1\} \). The number of possibilities for such a \( w' \) is \( 2^t \leq 2^{n/(4k+2)} \) and so the number of all possibilities for \( w \) is at most
\[
2 \cdot 2 \cdot (2k+1) 2^{n/(4k+2)} \leq c_3 2^k 2^{n/(4k+2)}
\]
for \( c_3 2^k \geq 8k + 4 \) so \( c_3 \) is a constant independent of \( u,n,k \). \( \Box \)
Lemma 3.5. Let $0 < \theta < \frac{1}{30}$. Then the number of reduced words of length $n \geq 1$ that are readable as labels of some paths in reduced $u$-barbell graphs for some $u$ with $|u| \leq \theta n$ is at most

$$c_4 2^{n/5}$$

where $c_4 > 0$ is some constant independent of $n$ and $\theta$.

Proof. Let $0 < 2k \leq \theta n$. The number of reduced words $u$ of length $2k$ which start with $b^{\pm 1}$ and end with $a$ is equal to $2^{k}$.

Therefore by Lemma 3.4 the number of all reduced words of length $n \geq 1$ that are readable in $u$-barbell graphs with $|u| \leq \theta n$ is at most

$$c_3 \sum_{2 \leq 2k \leq \theta n} 2^{k} 2^{2n/(4k+2)} \leq c_3 \sum_{2 \leq 2k \leq \theta n} 2^{2n/2} 2^{n/(4k+2)} \leq c_3 \sum_{2 \leq 2k \leq \theta n} 2^{\theta n} 2^{n/6} \leq c_3 \frac{\theta n}{2} 2^{\theta n+n/6} \leq c_4 2^{n/5}$$

where $c_4 > 0$ is some constant independent of $\theta, n$ and where the last inequality holds since by the choice of $\theta$ we have

$$\frac{n}{6} + \theta n < \frac{n}{5}.$$

\[\Box\]

Definition 3.6. Let $0 < \theta \leq \frac{1}{120}$. A cyclically reduced word $w$ is said to be $\theta$-readable if there is a subword $v$ of some cyclic permutation of $w$ or $w^{-1}$ with $|v| \geq |w|/2$ such that $v$ is readable in some reduced $u$-barbell graph with $|u| \leq \theta |v|$.

Definition 3.7 (Genericity conditions). Let $0 < \lambda \leq \frac{1}{120}$. Let $m \geq 1$ be an integer. We say that a tuple $(r_1, \ldots, r_m)$ of cyclically reduced words in $M$ satisfies the $Q_m(\lambda)$-condition if the following hold:

1. For each $i = 1, \ldots, m$ the word $r_i$ is not $\frac{1}{30}$-readable.
2. The symmetrized closure of $\{r_1, \ldots, r_m\}$ satisfies the $C'(\lambda)$-small cancellation condition in $M$.
3. For each $i = 1, \ldots, m$ the word $r_i$ is not a proper power in $M$ (in particular, this means that $r_i$ is different from every cyclic permutation of $r_i$).
4. If $i \neq j$ then $r_i$ is not a cyclic permutation of $r_j^{\pm 1}$.
5. If $1 \leq i \leq m$ then no subword $z$ of any cyclic permutation of $\eta(r_i)$ with $|z| > |\eta(r_i)|/3$ occurs as a subword of any cyclic permutation of any $r_j^{\pm 1}$ for $j = 1, \ldots, m$.
6. For every $1 \leq i \leq m$ the word $r_i$ is not a cyclic permutation of $r_i^{-1}$.
7. For each $i = 1, \ldots, m$ we have $|r_i| \geq 1200$. 

\[\Box\]
The small cancellation condition of item (2) implies that (4) and (6) hold but we have listed them for convenience. We say that \((r_1, \ldots, r_m) \in C_m\) satisfies condition \(U_m(\lambda)\) if \((r_1, \ldots, r_m) \in Q_m(\lambda)\) and, in addition, \(|r_1| = \cdots = |r_m|\). Thus \(U_m(\lambda) = Q_m(\lambda) \cap T_m\).

**Remark 3.8.** Note that conditions \(Q_m(\lambda)\) and \(U_m(\lambda)\) are invariant under reordering the tuple, inverting member of the tuple, taking a cyclic permutation of a member of the tuple and applying \(\eta\) to the entire tuple.

Recall that \(R(\tau)\) is the symmetrized set generated by the elements in the tuple \(\tau\). If \(\tau = (r_1, \ldots, r_m) \in U_m(\lambda)\) and \(|r_i| = n = 2k > 0\) then
\[
\#R(\tau) = 2mn.
\]
and
\[
R(\tau) \cap \eta(R(\tau)) = \emptyset.
\]

**Proposition 3.9.** Let \(0 < \lambda < \frac{1}{120}\) and let \(m \geq 1\) be an integer. Then the set \(Q_m(\lambda)\) is exponentially generic in \(C_m\) and the set \(U_m(\lambda)\) is exponentially generic in \(T_m\).

**Proof.** We will prove that \(Q_m(\lambda)\) is exponentially generic in \(C_m\). The proof that \(U_m(\lambda)\) is exponentially generic in \(T_m\) is analogous.

It is well-known and easy to see that parts (2), (3), (4), (6) and (7) of Definition 3.7 are define exponentially generic subsets of \(C_m\). The proof that (5) defines an exponentially generic subset of \(C_m\) is a little more cumbersome but it is very similar to the proofs of Lemmas 4.6 and 4.7 in [25], where the free group case was considered. We leave the details to the reader.

Since the intersection of two exponentially generic sets is exponentially generic, it suffices to prove that condition (1) of Definition 3.7 is exponentially generic, that is, that the complement of condition (1) in \(C_m\) is exponentially negligible in \(C_m\).

Let \(M = (r_1, \ldots, r_m)\) be an \(m\)-tuple of cyclically reduced words such that \(|r_i| \leq n\) and that part (1) of Definition 3.7 fails for \(M\). Thus there is some \(r_i\) such that a subword \(v\) of a cyclic permutation of \(r_i^\pm 1\) with \(|v| \geq |r_i|/2\) has the property that \(v\) is readable in a \(u\)-barbell graph with \(|u| \leq \frac{1}{10}|v|\).

Let \(c_1, c_2 > 0\) be the constants provided by Lemma 3.1. We may assume that \(c_2 \geq 1\).

Suppose first that \(|r_i| \leq 9n/10\). Then the number of possibilities for \(M\) is at most
\[
c_2^m 2^{9n/10} (2n/2)^{m-1}.
\]
This number is exponentially smaller, as \(n\) tends to infinity, than the number \(K_m(n)\) of all \(M\) among all \(m\)-tuples of cyclically reduced words of length at most \(n\) since \(K_m(n)\) satisfies
\[
K_m(n) \geq c_1^m (2n/2)^m.
\]

Suppose now that \(|r_i| > 9n/10\). Then \(r_i\) or \(r_i^{-1}\) is a cyclic permutation of a word \(zz'\) where \(|z| \geq |r_i|/2 > 9n/20\) and where \(z\) can be read in is
readable in a $u$-barbell graph with $|u| \leq \frac{1}{10}|r_i|$. Hence $|u| < n/60 < \frac{1}{30}|z|$. By Lemma 3.5, the number of such $z$ is at most $c_22^{n/5}$. The number of choices for the word $z'$ of length $|z'| \leq 11n/20$ is at most $c_2c_42^{n/5}2^{11n/40} = c_52^{19n/40}$. The number of cyclic permutations of any such $r_i$ and its inverse is at most $2n$. Thus there are at most $2nc_52^{19n/40}$ possibilities for $r_i$. Since there are at most $m$ choices for $i$, the number of possibilities for $M$ in this case is at most

$$2mnc_5c_2^{m-1}c_2^{19n/40}(2^{n/2})^{m-1}.$$  

Again, this number is exponentially smaller than the number $K_m(n)$ of all $m$-tuples of cyclically reduced words of length at most $n$ in $M$. This proves that the set of all $m$-tuples $(r_1, \ldots, r_m)$ of cyclically reduced words satisfying condition $Q_m(\lambda)$ is exponentially generic in $C^m$. □

Lemma 3.10. There is a quartic-time algorithm which, when given an $m$-tuple $\tau = (r_1, \ldots, r_m)$ verifies whether or not $\tau$ satisfies the genericity condition $Q_m(\lambda)$.  

Proof. We first show that the condition that each $r_i$ is not $\frac{1}{n}$-readable can be verified in quartic time. If any cyclic permutation of $r_i$ is readable in a $u$-barbell graph $\Gamma$ we can assume that $u$ is a subword of $r_{\pm 1}$. There are at most 

$$2|r_i| \frac{|r_i|}{60} \frac{|r_i|}{120} = \frac{|r_i|^3}{3600}$$

such words. We can thus construct all possible relevant $\Gamma$ in cubic time and for each graph we can verify if $r_i$ is readable on it in linear time.

We have noted that the standard small cancellation $C'(\lambda)$, item (2) of the genericity condition, already implies both items (4) and (6) of the condition. Let $s$ be the sum of all the $|r_i|$. For a particular $r_i$ there are at most $2|r_i| \leq 2s|r_i|/6$ subwords of length not exceeding $\lambda |r_i|$. Whether or not a particular word $z$ is a subword of another word $w$ can be verified in time linear in $|z| + |w|$. (For example, using the Knuth-Morris-Pratt algorithm.) Verifying $C'(\lambda)$ thus takes at most quadratic time $cms^2$.

The remaining conditions can all be verified in linear time and the lemma holds. □

4. The Subgroup Theorem

We can now prove the key result determining the structure of subgroups generated by the images of $a$ and $b$ in random quotients of $M$. We first need to remark that while we are writing words as reduced words on $a,b,b^{-1}$ and measure lengths accordingly, when considering small cancellation quotients of the modular group we must use the theory over free products. See Lyndon-Schupp [29] for details. In considering a van Kampen diagram for a word
equal to the identity in a small cancellation quotient, the theory guarantees
as usual the existence of a region labelled by a relator \( |r| \) which has an interior
arc \( \eta \) with label \( |u| \) where \( |u| < 3|\lambda| \).
There is the slight technicality that
the arc \( \eta \) might begin and/or end at secondary vertices. This could mean
that the portion of \( r \) left on the boundary of the whole diagram could be
two letters shorter than one might think without taking this point into
consideration. By our assumption that all defining relators have length at
least 100 it follows that \( 2 < \lambda |r| \) for any defining relator and we add extra
factor of \( \lambda \) to the lengths of interior arcs guaranteed by the general theory.

**Proposition 4.1** (Subgroup Theorem). Let \( 0 < \lambda \leq \frac{1}{120} \), let \( m \geq 1 \) and let
\[
G = M/N(\tau)
\]
where the tuple \( \tau = (r_1, \ldots, r_m) \) of cyclically reduced words satisfies the
\( Q_m(\lambda) \) condition. Then the following holds.

Suppose \( g_1, g_2 \in G \) are elements of orders two and three respectively and
let \( H = \langle g_1, g_2 \rangle \leq G \). Then either
\[
H = \langle g_1 \rangle \ast \langle g_2 \rangle
\]
or the pair \( (g_1, g_2) \) is conjugate to the pair \((a, b)\) or \((a, b^{-1})\) in \( G \).

**Proof.** Let \( R \) denote the symmetrized closure of \( \{r_1, \ldots, r_m\} \). After conju-
gating the pair \((g_1, g_2)\) we may assume that \( g_1 = a \) and \( g_2 = h b^\delta h^{-1} \) for
some \( h \in G \) and some \( \delta \in \{1, -1\} \).

Among all pairs \((a, h b^\delta h^{-1})\) conjugate to \((g_1, g_2)\) choose the pair where
\( |h|_G \) is the smallest possible. If \( h = 1 \) then \((g_1, g_2)\) is conjugate to \((a, b^\delta)\) as
required. Suppose now that \( h \neq 1 \) in \( G \).

Let \( u \) be a geodesic word representing \( h \). By minimality, \( u \) is a reduced
word which ends in \( a \) and begins with \( b^\delta \). Let \( \Gamma \) be the barbell graph with
a segment \( p \) labelled by \( u \) joining a loop-edge \( e \) labelled \( a \) to a loop-edge \( f \nlabelled \( b \). This means that \( \Gamma \) is folded and that the label of every reduced
path in \( \Gamma \) is a reduced word in \( M \), provided that path does not contain
subpaths of the form \( e'e' \) where \( e' \) is a loop-edge. Note that \( \Gamma \) has \( |u| + 2 \)
non-oriented edges.

Suppose now that \( H \neq \langle g_1 \rangle \ast \langle g_2 \rangle \). Then there exists a nontrivial closed
cyclically reduced path \( \alpha \) in \( \Gamma \) with label \( w \) such that \( w = \alpha \) 1 and such that
\( \alpha \) does not contain subpaths of the form \( e'e' \) where \( e' \) is a loop-edge. Note
that the word \( w \) is reduced in \( M \) by assumptions on \( \Gamma \). Then \( \alpha \) contains a
subpath \( \beta \) labelled by a word \( v \) such that \( v \) is a subword of some \( \tau \in R \) with
\( |v| > (1 - 3\lambda)|r| \).

The maximal arcs \( p, e, f \) of \( \Gamma \) subdivide \( \beta \) as a concatenation
\[
\beta = p_1 \ldots p_s
\]
where \( p_j \) are maximal arcs of \( \Gamma \) (possibly traversed with the opposite ori-
tentation) for \( 1 < j < s \) and where \( p_1, p_s \) are contained in such maximal
arcs.

There are two cases to consider.
Case 1. There is some \( p_i \) such that \( |p_i| \geq 6\lambda|r| \).
In this case \( p_i \) is a subpath of \( p^{\pm 1} \). After inverting \( \alpha \) and \( w \) if needed, we may assume that in fact \( p_i \) is a subpath of \( p \). Note that the label on any part of \( p_i \) which is also read in \( \beta \) in some different \( p_j \) is a piece by definition. Then the small cancellation condition \( C'(\lambda) \) implies that there is a subsegment \( q_i \) of \( p \) such that \( |q_i| \geq 3\lambda|r| \) and that \( q_i \) does not overlap \( p_j \) for \( j \neq i \).

We then perform an \( AO \)-move by deleting the interior of the arc \( q_i \) and adding an arc labelled by the missing in \( v \) part of \( r \), going from \( o(\alpha) \) to \( t(\alpha') \). This results in a graph \( \Gamma' \) with the smaller number of edges than in \( \Gamma \). By Corollary 2.10 the pair of elements of \( G \) defined by \( \Gamma' \) is conjugate to the pair \((g_1, g_2)\). Note that \( \Gamma' \) is obtained from \( \Gamma \) by removing a subsegment of \( p \) and then adding an arc connecting some vertex of one of the two components of the remainder of \( p \) to some vertex of the other remaining component of \( p \).

After removing the spikes ending in degree-one vertices if necessary, we obtain another barbell-graph representing the pair \((g_1, g_2)\) but with a smaller number of edges than in \( \Gamma \) (where the label of the “bar” in this barbell need not be reduced). This contradicts the minimal choice of \( h \).

Case 2. Suppose that \( |p_i| < 6\lambda|r| \) for \( 1 \leq i \leq s \).
Since \( \alpha \) is cyclically reduced closed path that is not a single loop-edge, it follows that for some \( i \) we have \( p_i = p^{\pm 1} \) and hence \( |p| < 6\lambda|r| \).

Since \( |v| > (1 - 4\lambda)|r| \geq |r|/2 \), it follows that \( v \) is readable in a \( u \)-barbell graph with \( |u| = |p| < 6\lambda|r| \) and so with \( |u|/|v| < \frac{6\lambda}{\frac{1}{2}} \leq \frac{1}{10} \). This contradicts the assumption that the tuple \((r_1, \ldots, r_m)\) satisfies condition \( Q_m(\lambda) \).

This main result now allows us to establish the desired rigidity theorem.

5. Rigidity of random quotients of the modular group

Convention 5.1. For the remainder of this section, unless specified otherwise, let \( m \geq 1 \) be an integer, let \( 0 < \lambda \leq \frac{1}{120} \) and let

\[ G = M/\langle \langle r_1, \ldots, r_m \rangle \rangle, \]

where the tuple \( \tau = (r_1, \ldots, r_m) \) of cyclically reduced words satisfies the \( Q_m(\lambda) \) condition.

Proposition 5.2. The following hold:

1. The group \( G \) is one-ended and word-hyperbolic.
2. The cyclic subgroups \( \langle a \rangle \leq G \) or \( \langle b \rangle \leq G \) have orders 2 and 3, correspondingly, and these subgroups are malnormal in \( G \).
3. Every nontrivial element of finite order in \( G \) is conjugate to either \( a \) or \( b^{\pm 1} \).
4. Every finite subgroup of \( G \) is conjugate to a subgroup of \( \langle a \rangle \) or \( \langle b \rangle \).
5. The center of \( G \) is trivial.
Proof. Statements (2),(3),(4) and (5) are straightforward applications of the small cancellation theory over free products, as explained in Section V.11 of Lyndon-Schupp \[29\]. Also, Theorem 11.2 in Section V.11 of \[29\] implies that presentation (\dagger) is a Dehn presentation and hence \(G\) is word-hyperbolic.

We already know from (2),(3),(4) that \(G\) is not cyclic and hence has rank two. Suppose that \(G\) is freely decomposable as \(G = G_1 \ast G_2\) where \(G_i \neq 1\). Grushko’s theorem then implies that each \(G_i\) is 1-generated, that is, cyclic. Since elements of finite order are always elliptic with respect to free product decompositions, it follows that \(a\) is conjugate to an element of some factor \(G_i\) and \(b\) is conjugate to an element of some factor \(G_j\). It follows that one of \(G_1, G_2\) must be cyclic of order 2 and the other must be cyclic of order 3. Hence \(G = \langle r_1, \ldots, r_m \rangle \not\simeq M\), which contradicts the fact that \(M\) is Hopfian. Thus \(G\) is freely indecomposable.

Suppose now that \(G\) admits a nontrivial splitting over a nontrivial finite group \(H\). Since \(G\) is generated by two elements of finite order, this splitting is not an HNN-extension. Thus \(G = K \ast_H L\) where \(K, L \leq G\) and \(H \neq 1, H \neq K, H \neq L\). Since \(H \neq 1\) is finite, (4) implies that \(H\) is conjugate to \(\langle a \rangle\) or \(\langle b \rangle\). Therefore by (2) \(H\) is malnormal in \(G\). A theorem of Karrass and Solitar \[27\] then implies that \(G\) cannot be generated by two elements, yielding a contradiction.

Thus \(G\) does not split nontrivially over a finite subgroup and hence, by Stallings’ classic theorem \[46\], \(G\) is one-ended. □

Proposition 4.1 and Proposition 5.2 immediately imply:

**Theorem 5.3.** Let \(\psi : M \to G\) be a homomorphism. Then exactly one of the following mutually exclusive alternatives holds:

1. The map \(\psi\) is injective but not onto.
2. The image of \(\psi\) is a finite cyclic group of order 1, 2 or 3.
3. The map \(\psi\) is surjective and the pair \((\psi(a), \psi(b))\) is conjugate to \((a, b)\) or \((a, b^{-1})\) in \(G\).

**Theorem 5.4.** Let \(\psi : G \to G\) be a homomorphism. Then the following hold:

1. If \(\psi\) is onto then \(\psi\) is injective. Hence \(G\) is Hopfian.
2. If \(\psi\) is injective then \(\psi\) is onto. Hence \(G\) is co-Hopfian.
3. If \(\psi\) is an automorphism of \(G\) then \(\psi\) is inner. Hence \(\text{Out}(G) = 1\) and \(G\) is a complete group.

Proof. Part (1) follows directly from Theorem 5.3. Indeed, suppose \(\psi : G \to G\) is an onto endomorphism. Then by Theorem 5.3 we know that \((\psi(a), \psi(b))\) is conjugate to \((a, b)\) or \((a, b^{-1})\) in \(G\). Suppose the latter holds. Then \(\eta(r_1) =_G 1\). Hence by the small cancellation assumption on \(\tau\) it follows that \(\eta(r_1)\) contains a subword that is more than a half of a cyclic permutation of some \(r_i^{\pm 1}\). This contradicts condition (5) in Definition 3.7 of \(Q_m(\lambda)\). Thus \((\psi(a), \psi(b))\) is conjugate to \((a, b)\) in \(G\). Therefore \(\psi\) is an inner automorphism of \(G\) and in particular, \(\psi\) is injective.
For part (2), suppose that $\psi : G \to G$ is an injective endomorphism. We need to show that $\psi$ is onto.

Theorem 5.3 implies that either the image of $\psi$ is isomorphic to $M$ or, after a post-composition with an inner automorphism we have $(\psi(a), \psi(b)) = (a, b^{\pm 1})$. The former is impossible since $G$ is one-ended while $M$ is not. In the latter case the image of $\psi$ is generated by a tuple conjugate to $(a, b^{\pm 1})$ and hence $\psi$ is onto, as required.

For part (3), let $\psi : G \to G$ be an automorphism of $G$. Since $G$ is one-ended, Proposition 4.1 implies that $(\psi(a), \psi(b))$ is conjugate in $G$ to either $(a, b)$ or $(a, b^1)$. In the former case $\psi$ is inner, as required. In the latter case we obtain a contradiction, exactly as in the proof of part (1). $\square$

The following result is essentially due to Greendlinger [15] who proved it in the context of small cancellation quotients of a free group. We present an argument for completeness.

**Proposition 5.5** (Greendlinger’s Theorem). Let $R_1, R_2$ be finite nonempty symmetrized sets of cyclically reduced words in $M$ such that each $R_i$ satisfies the $C'(1/8)$ small cancellation condition and such that $\langle\langle R_1 \rangle\rangle = \langle\langle R_2 \rangle\rangle$ in $M$. Then $R_1 = R_2$.

**Proof.** Suppose that the result fails and that $R_1 \neq R_2$. Let $r$ be the shortest element from the symmetric difference of $R_1$ and $R_2$. Without loss of generality we may assume that $r \in R_1 - R_2$.

Since $r \in \langle\langle R_2 \rangle\rangle$, the normal closure of $R_2$, there exists a reduced van Kampen diagram $\Delta$ over $R_2$ with $r$ being the label of the boundary cycle. If $\Delta$ contains a single region then $r \in R_2$, contrary to our assumptions. Thus $\Delta$ contains at least two regions. Since $R_2$ satisfies the $C'(1/8)$-small cancellation condition, the perimeter of $\Delta$ is longer than the perimeter of every region in $\Delta$. Thus all regions of $\Delta$ have boundaries labelled by elements of $R_2$ that are shorter than $r$. The minimal choice of $r$ implies that these elements of $R_2$ also belong to $R_1$.

Thus $\Delta$ is a reduced diagram over $R_1$ with the boundary cycle $r$ and with at least two regions. Again since $R_1$ is $C'(1/8)$, it follows that there is a region $D_0$ of $\Delta$ with boundary cycle labelled by $r' \in R_1$ such that $|r'| < |\partial D| = |r|$ and such that there is an arc in the boundary cycle of $D_0$ that is contained in the boundary cycle of $\Delta$ and such that this arc has length at least $|r'|/2$. Since $r,r' \in R_1$ and $|r'| < |r|$, this contradicts the $C'(1/8)$-small cancellation condition for $R_1$. $\square$

**Theorem 5.6.** [Isomorphism Rigidity for random quotients] Let $m \geq 1$. Then for any $\tau = (r_1, \ldots, r_m)$ satisfying condition $Q_m(\frac{1}{10m})$ and any finite symmetrized $S \subseteq C$ satisfying the standard small cancellation condition $C'(1/8)$ we have $G_\tau \simeq M/\langle\langle S \rangle\rangle$ if and only if $R(\tau) = S$ or $R(\tau) = \eta(S)$.

**Proof.** The “if” direction is obvious. Suppose now that $G_\tau \simeq M/\langle\langle S \rangle\rangle$ and let $\psi : M/\langle\langle S \rangle\rangle \to G_\tau$ be an isomorphism. Since $\psi$ is onto, Theorem 5.3 implies that the pair $(\psi(a), \psi(b))$ is conjugate to $(a, b)$ or $(a, b^{-1})$ in $G_\tau$. 


After composing $\psi$ with an inner automorphism of $G_\tau$, we may assume that $\psi(a) = a$ and $\psi(b) = b^{\pm 1}$. Then in $M$ we have
\[
\langle \langle r_1, \ldots, r_m \rangle \rangle = \langle \langle \eta^\delta(S) \rangle \rangle
\]
for some $\epsilon \in \{0, 1\}$. Since both $R(\tau)$ and $S$ satisfy the $C'(1/8)$ small cancellation condition over $M$, Proposition 5.5 implies that $R(\tau) = \eta^\delta(S)$, as required.

Theorem 5.6 and the definition of $Q_m(\lambda)$ immediately imply:

**Corollary 5.7.** Let $m \geq 1$ and let $\sigma = (r_1, \ldots, r_m), \tau = (s_1, \ldots, s_m) \in Q_m(\frac{1}{120})$. Then $G_\sigma \simeq G_\tau$ if and only if there exists a reordering $\tau' = (s'_1, \ldots, s'_m)$ of $\tau$ and $\delta \in \{0, 1\}$ such that each $s'_i$ is a cyclic permutation of $\eta^\delta(r_i)$ or $\eta^\delta(r_i^{-1})$ for $i = 1, \ldots, m$.

**Corollary 5.8.** Let $m \geq 1$ be an integer and let $\sigma, \tau \in U_m(\frac{1}{120})$ be such that $|\sigma| \leq |	au|$. Suppose that $\psi : G_\sigma \rightarrow G_\tau$ is a homomorphism. Then the following hold:

1. If $|\sigma| < |\tau|$ then $\psi(G_\sigma)$ is a finite cyclic group of order at most 3.
2. If $|\sigma| = |\tau|$ then either $\psi(G_\sigma)$ is a finite cyclic group of order at most 3 or $\psi$ is an isomorphism. In the latter case, after a possible post-composition of $\psi$ with an inner automorphism of $G_\tau$, we have $\psi(a) = \eta^\delta(a) = a$ and $\psi(b) = \eta^\delta(b) = b^{\pm 1}$ for some $\delta \in \{0, 1\}$ and, moreover, $\eta^\delta(R(\sigma)) = R(\tau)$.

**Proof.**

1. Suppose that $|\tau| < |\sigma|$. Since $M$ is Hopfian, Theorem 5.3 implies that either $\psi(G_\tau)$ is a finite cyclic group of order at most 3 or, after composing $\psi$ with an inner automorphism we have $\psi(a) = a$ and $\psi(b) = b^{\pm 1}$. Hence for some $\delta \in \{0, 1\}$ we have $\eta^\delta(\tau) \subseteq \langle \langle \sigma \rangle \rangle$. However, $R(\sigma)$ satisfies the $C'(1/8)$ small cancellation condition, and therefore every nontrivial element from $\langle \langle \sigma \rangle \rangle$ in $M$ has length $\geq |\sigma|$. On the other hand, $\eta^\delta(\tau) \subseteq \langle \langle \sigma \rangle \rangle$ and $|\tau| < |\sigma|$, yielding a contradiction. This proves part (1) of Corollary 5.8.

2. Suppose now that $|\tau| = |\sigma|$. Again, since $M$ is Hopfian, Theorem 5.3 implies that either $\psi(G_\tau)$ is a finite cyclic group of order at most 3 or, after composing $\psi$ with an inner automorphism we have $\psi(a) = a$ and $\psi(b) = b^{\pm 1}$. Thus, as before for some $\delta \in \{0, 1\}$ we have $\eta^\delta(\tau) \subseteq \langle \langle \sigma \rangle \rangle$. Since $R(\sigma)$ satisfies the $C'(1/8)$ small cancellation condition, if a nontrivial cyclically reduced word $r$ belongs to $\langle \langle \sigma \rangle \rangle$ then either $|r| > |\sigma|$ or $r \in R(\sigma)$. Since $|\tau| = |\sigma|$ and $\eta^\delta(\tau) \subseteq \langle \langle \sigma \rangle \rangle$, it follows that $\eta^\delta(\tau) \subseteq R(\sigma)$ and hence $\eta^\delta(R(\tau)) \subseteq R(\sigma)$. By definition of $U(\lambda)$ it follows that
\[\#R(\sigma) = \#R(\tau) = \#\eta^\delta(R(\tau)) = 2mn\]
where $n = |\tau| = |\sigma|$. Hence $\eta^\delta(R(\tau)) = R(\sigma)$ and therefore $\psi$ is an isomorphism, as claimed.

**Corollary 5.9.** Let $p > m \geq 1$ be integers. Let $\sigma = (r_1, \ldots, r_m) \in U_m(\frac{1}{120})$ and $\tau = (s_1, \ldots, s_p) \in U_p(\frac{1}{120})$ be such that $|\tau| = |\sigma|$. Then $G_\tau \not\simeq G_\sigma$.
Proof. Let \( n := |r_i| = |s_j| \).

Suppose that \( G_\tau \simeq G_\sigma \) and let \( \psi : G_\sigma \to G_\tau \) be an isomorphism. Then by Theorem 5.6 either \( R(\tau) = R(\sigma) \) or \( R(\tau) = \eta(R(\sigma)) \). The definition of \( U_m(\frac{1}{120}) \) and \( U_p(\frac{1}{120}) \) implies that

\[
\#R(\tau) = 2mn, \quad \#R(\sigma) = \#\eta(R(\sigma)) = 2pn
\]

This is a contradiction since \( m \neq p \) and thus \( 2pn \neq 2mn \). \( \square \)

The following sections of the paper can each be read in any order. Both essential incompressibility and counting isomorphism types follow directly from rigidity and are independent of each other.

6. COUNTING THE ISOMORPHISM TYPES OF RANDOM QUOTIENTS

**Definition 6.1.** For an even integer \( n = 2k > 0 \) let \( I_m(n) \) denote the number of isomorphism types of groups given by presentations

\[
M/\langle\langle r_1, \ldots, r_m \rangle\rangle,
\]

where \( r_1, \ldots, r_m \) are cyclically reduced words of length \( n \) in \( M \).

**Theorem 6.2.** We have for even \( n \to \infty \)

\[
I_m(n) \sim \frac{(2^{n/2+1})^m}{2 \ m!(2n)^m},
\]

that is

\[
\lim_{k \to \infty} \frac{2I_m(2k) \ m!(4k)^m}{(2k+1)^m} = 1.
\]

**Proof.** Let \( V_m := U_m(\frac{1}{120}) \cap T_m \). Then \( V_m \) is exponentially generic in \( T_m \). Let \( X_m \) be the complement of \( V_m \) in \( T_m \).

Recall that the number of cyclically reduced words of even length \( n = 2k \) is \( 2 \ 2^k = 2^{k+1} \). For every \( \tau = (r_1, \ldots, r_m) \in V_m \) with \( |r_i| = n \) there are precisely \( 2 \ m!(2n)^m \) tuples \( \sigma \in Q'_m \) such that \( G_\tau \simeq G_\sigma \). Let \( \gamma(n, V_m) \) be the number of tuples from \( V_m \) with entries of length \( n \). Then the tuples \( \tau \) from \( V_m \) with entries of length \( n \) represent exactly \( I'_m(n) := \frac{\gamma(n, V_m)}{2 \ m!(2n)^m} \) distinct isomorphism types of groups \( G_\tau \). Let \( I''_m(n) \) be the number of isomorphism types of groups \( G_\tau \) corresponding to \( \tau \in X_m \) with entries of length \( n \). Thus

\[
I_m(n) = I'_m(n) + I''_m(n).
\]

Since \( V_m \) is exponentially generic in \( T_m \), we have

\[
\lim_{k \to \infty} \frac{\gamma(2k, V_m)}{(2k+1)^m} = 1
\]

and

\[
\lim_{k \to \infty} \frac{\gamma(2k, X_m)}{(2k+1)^m} = 0
\]

with exponentially fast convergence. Therefore

\[
\lim_{k \to \infty} \frac{2I'_m(2k) \ m!(4k)^m}{(2k+1)^m} = 1.
\]
Moreover $I_m''(2k) \leq \gamma(2k, X_m)$ and, since the convergence in (*) is exponentially fast, we have

$$\lim_{k \to \infty} \frac{2I_m''(2k) m!(4k)^m}{(2k+1)^m} = 0.$$  

Since $I_m(n) = I_m'(n) + I_m''(n)$, we conclude that

$$\lim_{k \to \infty} \frac{2I_m(2k) m!(4k)^m}{(2k+1)^m} = 1,$$

as required. \hfill \Box

7. Kolmogorov Complexity and the $T$-invariant

Intuitively, the Kolmogorov complexity $K(x)$ of a finite binary string $x$ is the size of the smallest computer program $M$ that can compute $x$. In order to make this notion precise one needs to first fix a “programming language” but it turns out that all reasonable choices yield measures which are equivalent up to an additive constant. We refer the reader to the book of Li and Vitanyi [28] for a detailed treatment of the subject and we recall only a few relevant facts and definitions here.

**Definition 7.1.** Fix a universal Turing machine $U$ with the alphabet

$\Sigma := \{0, 1\}$. Then $U$ computes a universal partial recursive function $\phi$ from $\Sigma^*$ to $\Sigma^*$. That is, for any partial recursive function $\psi$ there is a string $z \in \Sigma^*$ such that for all $x \in \Sigma^*$, $\phi(zx) = \psi(x)$.

For a finite binary string $x \in \Sigma^*$ we define the **Kolmogorov complexity** $K(x)$ as

$$K(x) := \min\{|p| : p \in \Sigma^*, \phi(p) = x\}.$$  

Let $B$ be another finite nonempty alphabet. We choose a recursive bijection $h : B^* \to \{0, 1\}^*$.  

For any string $x \in B^*$ define its **Kolmogorov complexity** $K_B(x)$ as

$$K_B(x) := K(h(x)).$$  

Let $\hat{A}$ denote the alphabet consisting of $A$ together with the extra symbols “(”, “)” and “,“”. We regard tuples $\tau = (r_1, \ldots, r_m) \in C^m$ as words in the alphabet $\hat{A}$. For an $m$-tuple $\tau = (r_1, \ldots, r_m) \in C^m$ define the **Kolmogorov complexity** $K(\tau)$ as

$$K(\tau) := K_{\hat{A}}(\tau).$$

**Remark 7.2.** The notations in the present paper differ slightly from those use in [25]. In [25] $K(x)$ stood for the prefix complexity of $x$ while the Kolmogorov complexity of $x$ was denoted by $C(x)$.

**Remark 7.3** (The General Enumeration Argument). Let $\mathcal{P}$ be a recursively enumerable class of finite group presentations. Then there is an algorithm which, when given a finite presentation of a group $G$ known to be isomorphic
to a group defined by some presentation from $\mathcal{P}$, actually finds a presentation $\Pi$ of $G$ which is in $\mathcal{P}$.

Say $G$ is given by a presentation $G = \langle X | R \rangle$. We start enumerating all presentations $\Pi = \langle Y | S \rangle \in \mathcal{P}$. For each such presentation we start enumerating pairs of maps $(\alpha, \beta)$ where $\alpha : X \to F(Y)$ and $\beta : Y \to F(X)$. For each such pair start enumerating $\langle \langle S \rangle \rangle \leq F(Y)$ and $\langle \langle R \rangle \rangle \leq F(X)$ and start checking if $\alpha, \beta$ extend to homomorphisms $\alpha : G \to G(\Pi)$ and $\beta : G(\Pi) \to G$, where $G(\Pi)$ is the group defined by $\Pi$. If we find a pair $(\alpha, \beta)$ where both $\alpha, \beta$ extend to such homomorphisms, we start checking if $x^{-1} \beta \alpha(x) \in \langle \langle R \rangle \rangle$ and $y^{-1} \alpha \beta(y) \in \langle \langle S \rangle \rangle$ for all $x \in X, y \in Y$. If yes, then $\alpha : G \to G(\Pi)$ and $\beta : G(\Pi) \to G$ are mutually inverse isomorphisms. Since $G$ is known to be isomorphic to some group defined by a presentation from $\mathcal{P}$, this process is guaranteed to terminate.

We refer to the above algorithm constructed above as the general enumeration algorithm for $\mathcal{P}$.

We will need the following statement that follows directly from Proposition 2.5 and Lemma 2.7 in [25].

**Proposition 7.4.** Let $m \geq 1$ be a fixed integer. Let $\Omega \subseteq T_m$ be a nonempty subset equipped with a discrete non-vanishing probability measure $P$, so that $\sum_{\tau \in \Omega} P(\{\tau\}) = 1$. Denote $\mu(\tau) := P(\{\tau\})$ for any $\tau \in \Omega$.

Then for any $\delta > 0$ we have

$$P(2^K(\tau) \geq - \log_2 \mu(\tau) - \log_2 \delta - c) \geq 1 - \frac{1}{\delta},$$

where $c = c(m) > 0$ is a constant independent of $\Omega, P$.

**Corollary 7.5.** Let $\delta > 0$ and let $Z_\delta \subseteq T_m$ be the set of all tuples $\tau \in T_m$ such that

$$2^K(\tau) \geq m(n/2 + 1) - \log_2 \delta - c,$$

where $n$ is the length of each entry of $\tau$. Then for all even $n > 0$ we have

$$\gamma(n, Z_\delta) \geq \gamma(n, T_m) \geq 1 - \frac{1}{\delta}.$$

**Proof.** Let $n > 0$ be an even integer and let $\Omega$ be the set of all tuples in $T_m$ with entries of length $n$. Let $P$ be the uniform probability measure on $\Omega$. Then for every $\tau \in \Omega$ we have

$$\mu(\tau) = \frac{1}{2^{m(n/2+1)}}.$$

Hence

$$- \log_2 \mu(\tau) = m(n/2 + 1).$$

Applying Proposition 7.4 we get

$$P(2^K(\tau) \geq m(n/2 + 1) - \log_2 \delta - c) \geq 1 - \frac{1}{\delta},$$

as required. 

\[\square\]
Definition 7.6. Let $0 < \lambda \leq \frac{1}{120}$ and let $m \geq 1$ be an integer. Let $U_m'(\lambda)$ denote the set of all $\tau = (r_1, \ldots, r_m) \in U_m(\lambda)$ with the following property.

Whenever $\tau' = (r'_1, \ldots, r'_m)$ is obtained from $\tau$ by a formally nontrivial combination of reordering the elements of $\tau$, taking cyclic permutations and possible inverses of its entries and possibly applying $\eta$ to the tuple, then

$$(v_1, \ldots, v_m) \neq (v'_1, \ldots, v'_m)$$

where $v_i$ is the initial segment of $r_i$ of length $\lfloor \lambda n \rfloor$, where $v'_i$ is the initial segment of $r'_i$ of length $\lfloor \lambda n \rfloor$ and where $n = |r_i| = |r'_i|$.

Proposition 7.7. Let $0 < \lambda \leq \frac{1}{120}$ and let $m \geq 1$ be an integer. Then $U_m'(\lambda)$ is exponentially generic in $T_m$.

Proof. The proof is a straightforward generalization of the proofs of Lemmas 4.5, 4.6 and 4.8 in [25], where a similar statement was considered for the case of a free group. We leave the details to the reader. \hfill \Box

Lemma 7.8. There exists a constant $N = N(m) > 0$ with the following property. Let $0 < \lambda \leq 1/24$ be a rational number and let $\tau \in U_m'(\lambda)$ be a tuple consisting of words of length $n \geq 2$.

Suppose $G_\tau$ can be presented by a finite presentation

$$(\dagger) \quad \Pi = \langle b_1, \ldots, b_s | w_1, \ldots, w_t \rangle$$

where $t \geq 1$.

Then $K(\tau) \leq N\ell_1(\Pi) \log_2 \ell_1(\Pi) + nN\lambda + N$.

Proof. We describe an algorithm $A$, which, given a presentation (\dagger) for $G_\tau$ and a tuple $(u_1, \ldots, u_m)$ of initial segment $u_i$ of $r_i$ of length $\lfloor \lambda n \rfloor$, will recover the tuple $\tau$.

First, note that we are assuming that (\dagger) defines a group isomorphic to a group $G_\sigma$ for some $\sigma \in U_m'(\lambda)$. Since the set $U_m'(\lambda)$ is recursive, by a general enumeration algorithm we can algorithmically find some $\sigma \in U_m'(\lambda)$ such that (\dagger) defines a group isomorphic to $G_\sigma$ and hence to $G_\tau$.

We then perform all possible ways of applying to $\sigma$ a combination of reordering of the tuple entries, cyclic permutations and possible inversions of its entries and possibly applying $\eta$ to the tuple. Corollary 5.7 implies that this collection of tuples will contain $\tau$.

For each of the resulting tuples we record the sequence of initial segments of its entries of length $\lfloor \lambda n \rfloor$ and compare it with $(u_1, \ldots, u_m)$. The definition of $U_m'(\lambda)$ that there will be exactly one tuple for which this sequence of initial entries coincides with $(u_1, \ldots, u_m)$ and this tuple is $\tau$.

The general enumeration algorithm is fixed. The further input of $A$, required to compute $\tau$, consists of the presentation (\dagger) and tuple of the initial segments $(u_1, \ldots, u_m)$ of $r_1, \ldots, r_m$ with $|u_i| = \lfloor \lambda n \rfloor$.

We want to estimate the length of this input when expressed as a binary sequence. Put $T = \ell_1(\Pi)$. First note that in (\dagger) every $b_i$ must occur in some $w_j^{\pm 1}$ since $G_\tau$ is a one-ended group by Theorem 5.6 and therefore $s \leq T$. 


We can now encode the presentation \((\hat{\xi})\) by writing each subscript \(i = 1, \ldots, s\) for each occurrence of \(b_i\) in \((\hat{\xi})\) as a binary integer. Using \(\hat{i}\) to denote the binary expression for \(i\), we replace each occurrence of \(b_i\) in \((\hat{\xi})\) by \(b^{\hat{i}}\) and each occurrence of \(b_i^{-1}\) by \(-b^{\hat{i}}\). Note that the bit-length of the binary expression \(\hat{i}\) of \(i\) is at most \(\log_2 i\). This produces an unambiguous encoding of \((\hat{\xi})\) as a string \(W\) of length at most \(O(T \log_2 T)\) over the six letter alphabet
\[
b \ 0 \ 1 \ - \ |
\]
and this alphabet can then be block-coded into binary in the standard way.

Since the number \(m\) and the alphabet \(A = \{a, b, b^{-1}\}\) are fixed, describing \((u_1, \ldots, u_m)\) requires at most \(O(\lambda n)\) number of bits.

Hence there exist a constant \(N = N(m) > 0\) independent of \(\tau\) such that
\[
K(\tau) \leq NT \log_2 T + N\lambda + N.
\]

\(\square\)

**Theorem 7.9.** Let \(m \geq 1\) be a fixed integer. For any \(0 < \epsilon < 1\) there is an integer \(n_0 > 0\) and a constant \(L = L(m, \epsilon) > 0\) with the following property.

Let \(J\) be the set of all tuples \(\tau \in T_m\) such that
\[
T_1(G_{\tau}) \log_2 T_1(G_{\tau}) \geq L |\tau|.
\]

Then for any \(n \geq n_0\)
\[
\frac{\gamma(n, J)}{\gamma(n, T_m)} \geq 1 - \epsilon.
\]

**Proof.** Let \(N > 0\) be the constant provided by Lemma 7.8. Choose a rational number \(\lambda, 0 < \lambda < 2/135\) so that \(\frac{m}{2} - N\lambda > 0\).

Let \(0 < \epsilon < 1\) be arbitrary and let \(\delta > 0\) be such that \(\frac{2\delta}{3} < \epsilon\).

As in Corollary 7.5 let \(Z_\delta\) be let \(Z_\delta \subseteq T_m\) be the set of all tuples \(\tau \in T_m\) such that
\[
K(\tau) \geq \frac{1}{2} [m(n/2 + 1) - \log_2 \delta - c],
\]
where \(n\) is the length of each entry of \(\tau\). Then for all even \(n > 0\) we have
\[
\frac{\gamma(n, Z_\delta)}{\gamma(n, T_m)} \geq 1 - \frac{1}{\delta}.
\]

Since by Proposition 7.7 \(U^\prime_m(\lambda)\) is exponentially generic in \(T_m\), there is \(n_1 > 0\) such that for any \(n \geq n_1\)
\[
\frac{\gamma(n, Z_\delta \cap U^\prime_m(\lambda))}{\gamma(n, T_m)} \geq 1 - \frac{2}{\delta} \geq 1 - \epsilon.
\]

Now suppose \(\tau \in Z_\delta \cap U^\prime_m(\lambda)\) and \(n := |\tau| \geq n_1\).

Then by Lemma 7.8
\[
\frac{1}{2} [m(n/2 + 1) - \log_2 \delta - c] \leq K(\tau) \leq NT_1(G_{\tau}) \log_2 T_1(G_{\tau}) + N\lambda + N.
\]
Hence for $n \geq n_1$

$\left(\frac{m}{4} - N\lambda\right)n + \frac{m}{2} - \log_2 \delta - c - N \leq NT_1(G_\tau) \log_2 T_1(G_\tau)$.

This implies the statement of the theorem.

\[\square\]

**References**

[1] G. Arzhantseva and A. Ol’shanskii, *Genericity of the class of groups in which subgroups with a lesser number of generators are free*, (Russian) Mat. Zametki 59 (1996), no. 4, 489–496.

[2] G. Arzhantseva, *On groups in which subgroups with a fixed number of generators are free*, (Russian) Fundam. Prikl. Mat. 3 (1997), no. 3, 675–683.

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

[4] G. Arzhantseva, *A property of subgroups of infinite index in a free group*, Proc. Amer. Math. Soc. 128 (2000), 3205–3210.

[5] G. Arzhantseva, *A dichotomy for finitely generated subgroups of word-hyperbolic groups*, Topological and Asymptotic Aspects of Group Theory (R. Grigorchuk, M. Mihalik, M. Sapir and Z. Sunik, Editors), AMS Contemporary Mathematics Series, vol. 394, 2006, pp. 1-10.

[6] P. Bahls, *A new class of rigid Coxeter groups*. Internat. J. Algebra Comput. 13 (2003), no. 1, 87–94.

[7] A. Borovik, A. G. Myasnikov and V. Shpilrain, *Measuring sets in infinite groups*, Computational and Statistical Group Theory (R. Gilman et al., Editors), Contemp. Math., Amer. Math. Soc. 298 (2002), 21–42.

[8] N. Brady, J. McCammond, B. M"{u}hlherr, and W. Neumann, *Rigidity of Coxeter groups and Artin groups*. Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part I (Haifa, 2000). Geom. Dedicata 94 (2002), 91–109.

[9] J. Birman, K. H. Ko, S. J. Lee, *A new approach to the word and conjugacy problems in the braid groups*. Adv. Math. 139 (1998), no. 2, 322–353.

[10] C. Champetier, *Petite simplification dans les groupes hyperboliques*, Ann. Fac. Sci. Toulouse Math. (6) 3 (1994), no. 2, 161–221.

[11] C. Champetier, *Propriétés statistiques des groupes de présentation finie*, Adv. Math. 116 (1995), 197–262.

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

[13] P.-A. Cherix and A. Valette, *On spectra of simple random walks on one-relator groups*, With an appendix by Paul Jolissaint. Pacific J. Math. 175 (1996), 417–438.

[14] P.-A. Cherix and G. Schaeffer, *An asymptotic Freiheitssatz for finitely generated groups*, Enseign. Math. (2) 44 (1998), 9–22.

[15] T. Delzant, Décomposition d’un groupe en produit libre ou somme amalgamée, J. Reine Angew. Math. 470 (1996) 153–180.

[16] T. Delzant and L. Potyagailo, *Accessibilité hiérarchique des groupes de présentation finie*. Topology 40 (2001), no. 3, 617–629.

[17] E. Ghys, *Groupes Aléatoires*. Seminar Bourbaki (March 2003), to appear in Astérisque.

[18] M. Greendlinger, *An analogue of a theorem of Magnus*. Arch. Math. 12 (1961), 94–96.

[19] M. Gromov, *Hyperbolic Groups*, in "Essays in Group Theory (G.M.Gersten, editor)", MSRI publ. 8, 1987, 75–263.
[20] M. Gromov, *Asymptotic invariants of infinite groups*. Geometric group theory, Vol. 2 (Sussex, 1991), 1–295, London Math. Soc. Lecture Note Ser., 182, Cambridge Univ. Press, Cambridge, 1993

[21] M. Gromov, *Random walks in random groups*, Geom. Funct. Analysis **13** (2003), no. 1, 73–146

[22] I. Kapovich, A. Myasnikov, P. Schupp and V. Shpilrain, *Generic-case complexity, Decision problems in group theory and Random walks*, J. Algebra **264** (2003), no. 2, 665–694

[23] I. Kapovich, A. Myasnikov, P. Schupp and V. Shpilrain, *Average-case complexity for the word and membership problems in group theory*, Advances in Mathematics **190** (2005), no. 2, 343–359

[24] I. Kapovich and P. Schupp, *Genericity, the Arzhantseva-Ol’shanskii method and the isomorphism problem for one-relator groups*, Math. Ann. **331** (2005), no. 1, 1–19

[25] I. Kapovich and P. Schupp, *Delzant’s $T$-invariant, one-relator groups and Kolmogorov complexity*, Commentari Math. Helv. **80** (2005), no. 4, 911–933

[26] I. Kapovich, P. Schupp and V. Shpilrain, *Generic properties of Whitehead’s Algorithm and isomorphism rigidity of random one-relator groups*, Pacific J. Math. **223** (2006), no. 1, 113–140

[27] A. Karrass, and D. Solitar, *The free product of two groups with a malnormal amalgamated subgroup*, Canad. J. Math. **23** (1971), 933–959

[28] M. Li and P. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications* (2-nd edition), Graduate Texts in Computer Science, Springer, 1997

[29] R. Lyndon and P. Schupp, *Combinatorial Group Theory*, Springer-Verlag, 1977. Reprinted in the “Classics in mathematics” series, 2000.

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

[31] C. F. Miller, III and P. Schupp, *Embeddings into Hopfian groups*, J. Algebra **17** (1971), 171–176.

[32] G. D. Mostow, *Strong rigidity of locally symmetric spaces*. Annals of Mathematics Studies, No. 78. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1973

[33] B. Mühlherr, and R. Weidmann, *Rigidity of skew-angled Coxeter groups*, Adv. Geom. **2** (2002), no. 4, 391–415.

[34] Y. Ollivier, *Critical densities for random quotients of hyperbolic groups*, C. R. Math. Acad. Sci. Paris **336** (2003), no. 5, 391–394

[35] Y. Ollivier, *Sharp phase transition theorems for hyperbolicity of random groups*, Geom. Funct. Anal. **14** (2004), no. 3, 595–679

[36] Y. Ollivier, *Cogrowth and spectral gap of generic groups*, Ann. Inst. Fourier (Grenoble) **55** (2005), no. 1, 289–31

[37] Y. Ollivier, *Effondrement de quotients aléatoires de groupes hyperboliques avec torsion*, C. R. Math. Acad. Sci. Paris **341** (2005), no. 3, 137–140

[38] A. Yu. Ol’shanskii, *Almost every group is hyperbolic*, Internat. J. Algebra Comput. **2** (1992), 1–17.

[39] E. Pervova and C. Petronio, *Complexity and $T$-invariant of Abelian and Milnor groups, and complexity of 3-manifolds*, preprint, 2004; [http://front.math.ucdavis.edu/math.GT/0412187](http://front.math.ucdavis.edu/math.GT/0412187)

[40] S. Prassidis, and B. Spieler, *Rigidity of Coxeter groups*, Trans. Amer. Math. Soc. **352** (2000), no. 6, 2619–2642

[41] E. Rosas, *Rigidity theorems for right angled reflection groups*, Trans. Amer. Math. Soc. **308** (1988), no. 2, 837–848

[42] P. Schupp, *Embeddings into simple groups*, J. London Math. Soc. (2) **13** (1977), 90–94.
[43] R. Schwartz, The quasi-isometry classification of rank one lattices, Inst. Hautes Etudes Sci. Publ. Math. 82 (1995), 133-168
[44] Z. Sela, Structure and rigidity in (Gromov) hyperbolic groups and discrete groups in rank 1 Lie groups. II, Geometric and Functional Analysis 7 (1997), 561–593
[45] Z. Sela, Endomorphisms of hyperbolic groups. I. The Hopf property. Topology 38 (1999), no. 2, 301–321
[46] J. Stallings, Groups of cohomological dimension one. 1970 Applications of Categorical Algebra (Proc. Sympos. Pure Math., Vol. XVIII, New York, 1968) pp. 124–128 Amer. Math. Soc., Providence, R.I.
[47] J. H. C. Whitehead, On equivalent sets of elements in free groups, Annals of Mathematics 37 (1936), 782–800
[48] A. Zuk, On property (T) for discrete groups. Rigidity in dynamics and geometry (Cambridge, 2000), 473–482, Springer, Berlin, 2002

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801, USA

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

E-mail address: kapovich@math.uiuc.edu

Current address: Department of Mathematics, Johann Wolfgang Goethe University, Robert Mayer Strasse 6-8, 60325 Frankfurt, Germany

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801, USA

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

E-mail address: schupp@math.uiuc.edu