Conjugacy Growth of Commutators

Peter S. Park

May 2017

Advisor: Professor Peter C. Sarnak

Submitted in partial fulfillment
of the requirements for the degree of
Bachelor of Arts
Department of Mathematics
Princeton University

This thesis represents my own work in accordance with University regulations.

Peter S. Park

I authorize Princeton University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize Princeton University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Peter S. Park

Abstract

We use the classification of commutators in free groups and in free products by Wicks [14] to asymptotically count for these groups the conjugacy classes of commutators with a given word length. Let F_r denote the free group on $r > 1$ generators. We show that the number of conjugacy classes of commutators in F_r with word length k is given by 0 for odd k and

$$\frac{(2r-2)^2(2r-1)^{\frac{k}{2}-1}}{96r}\left(k^2 + O_r\left(k\right)\right)$$

for even k, where the implied constant depends only on r and is effectively computable. This result builds on the work of Rivin [9], who counted the conjugacy classes of commutator-subgroup elements in F_r with a given word length.

Next, we show that the number of conjugacy classes of commutators in the free product $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \cong \mathrm{PSL}_2(\mathbb{Z})$ with word length k is given by 0 for $4 \nmid k$ and

$$\frac{2^{\frac{k}{4}}}{384}\left(k^2 + O\left(k\right)\right).$$

for $4 \mid k$, where the implied constant is effectively computable.

Finally, we give an algorithm to exhaustively compute all hyperbolic conjugacy classes of commutators of $\mathrm{PSL}_2(\mathbb{Z})$ with a given trace. We conclude by formulating several density-type conjectures suggested by the data from this algorithm.

Acknowledgements

First of all, I would like to thank my family: Mom, Dad, and John. They have always been there for me to support my dream of becoming a mathematician, and to support me unconditionally. I am especially grateful to Mom and Dad for helping me cultivate the interest in numbers that I've had ever since I was a little boy, and for granting me so many vital educational opportunities, including my attendance at Princeton, that I never take for granted.

Next, I would like to thank my advisor, Professor Peter Sarnak for introducing me to this fun problem, for numerous helpful discussions regarding it, and for making time in his busy schedule to give feedback on this thesis even while he was off-campus giving a public lecture the week before the due date. Most importantly, I am grateful to him for believing in me in the face of unexpected challenges.

I would also like to thank my math professors for teaching me so much with great care: not just about math, but also about life. In particular, I would like to thank Professors Manjul Bhargava, Richard Ehrenborg, Robert Gunning, Sophie Morel, Ken Ono, Peter Ozsvath, Margaret Readdy, Jerry Wang, and Shou-Wu Zhang for their invaluable advising in the classroom and/or in research. Additionally, I would like to thank all my Princeton professors in information theory, computer science, music, economics, and history for helping me develop a broad perspective on life.

Moreover, I would like to thank my friends in Colonial Club for laughing at my corny humor (at least it's clean, sometimes), for all the late-night discussions about serious and not-so-serious subjects, and for always being there as a "home away from home." I would also like to thank my friends in the *danjou pears* board game group for being a constant source of merriment in this polarized day and age; only we can save humanity from COdA-403d. In addition, I would like to thank my problem-set partners and research collaborators, with whom I've spent many a night working, talking, and bonding. In fact, these three groups have nonempty pairwise intersections, so I am thanking some of my friends more than once. I would also like to thank my friends (you know who you are!) who happen to not be in any of these three sets.

Last but not least, I would like to thank Jenny for being such a dependable significant other in my life. She has brought nothing but joy into my life, and I can't thank her enough for always being optimistic and for always being there when I need her the most.

Contents

Chapter 1

Introduction

Let G be a finitely generated group with a finite symmetric set of generators $\mathfrak{S}$. Any element $g \in G$ can then be written as a word in the letters of $\mathfrak{S}$, and one can define the *length* of g by

$$\inf_{\substack{k \in \mathbb{Z}_{\geq 0} : \exists c_1, \ldots, c_k \in \mathfrak{S} \\ g = c_1 \cdots c_k}} k.$$

Consider the closed ball $B_k(G, \mathfrak{S}) \subset G$ of radius k in the word metric, defined as the subset consisting of elements with length $\leq k$. One can then ask natural questions about the growth of G: how large is $|B_k(G, \mathfrak{S})|$ as $k \to \infty$, and more generally, what connections can be made between the properties of G and this notion of its growth rate? Since the middle of the 20th century, this group-theoretic question has been widely studied in various contexts largely arising from geometric motivations, such as characterizing the volume growth of Riemannian manifolds and Lie groups. One of the pioneering results on this question of geometric group theory is that of Gromov [6], who classified groups G with polynomial growth, i.e., those that satisfy $|B_k(G, \mathfrak{S})| \ll k^{O(1)}$. There are also groups with exponential growth, one of which is the free group F_r on $r > 1$ generators; more precisely, after fixing a symmetric generating set $\mathfrak{S} := \{x_1, \ldots, x_r, x_1^{-1}, \ldots, x_r^{-1}\}$, it is easy to see that

$$B_k(G, \mathfrak{S}) = 1 + \sum_{i=1}^{k} \partial B_i(G, \mathfrak{S}) = 1 + \sum_{i=1}^{k} 2r(2r-1)^{i-1} = \frac{r\left((2r-1)^k - 1\right)}{r-1},$$

where $\partial B_k(G, \mathfrak{S})$ denotes the subset of length-k elements.

In certain contexts, it is more natural to consider the growth rate of the conjugacy classes of G. For a given conjugacy class $\mathcal{C}$ of G, define the *length* of $\mathcal{C}$ by

$$\inf_{g\in\mathcal{C}} \operatorname{length}(g),$$

and define $\partial B_k^{\mathrm{conj}}(G,\mathfrak{S})$ as the set of conjugacy classes of G with length k. In the case of F_r, the minimal-length elements of a conjugacy class are precisely its cyclically reduced elements, all of which are cyclic conjugates of each other. The conjugacy growth of F_r can be described as $\partial B_k^{\mathrm{conj}}(G,\mathfrak{S}) \sim (2r-1)^k/k$, which agrees with the intuition of identifying the cyclic conjugates among the $2r(2r-1)^{k-1}$ words of length k; for the full explicit formula, see [7, Proposition 17.8].

One context for which conjugacy growth may be a more natural quantity to study than the growth rate in terms of elements is when characterizing the frequency with which a conjugacy-invariant property occurs in G. An example of such a property is membership in the commutator subgroup $[G,G]$. On this front, Rivin [9] computed the number c_k of length-k cyclically reduced words in F_r that are in the commutator subgroup (i.e., have trivial abelianization) to be the constant term in

$$(2\sqrt{2r-1})^k T_k\left(\frac{1}{2\sqrt{2r-1}}\sum_{i=1}^{r}\left(x_i+\frac{1}{x_i}\right)\right),$$

where T_k denotes the kth Chebyshev polynomial of the first kind. This quantity can asymptotically be described as $c_k \sim C_r(2r-1)^k/k^{r/2}$ for some positive constant C_r depending only on r. Furthermore, from the number of cyclically reduced words with trivial abelianization, one can derive the growth of conjugacy classes with trivial abelianization by using Möbius inversion, due to the following relationships:

$$c_k = \sum_{d\mid k} p_d,$$

where p_d denotes the number of primitive (i.e., not a proper power of any subword) length-d

words with trivial abelianization, and

$$|\partial B_k^{\text{conj}}(G, \mathfrak{S}) \cap [G, G]| = \sum_{d|k} \frac{p_d}{d},$$

which together imply by Möbius inversion that

$$\begin{aligned} |\partial B_k^{\text{conj}}(G, \mathfrak{S}) \cap [G, G]| &= \sum_{d|k} \frac{1}{d} \sum_{e|d} \mu\left(\frac{d}{e}\right) c_e = \sum_{e|k} \frac{c_e}{e} \left(\sum_{d'|\frac{k}{e}} \frac{\mu(d')}{d'} \right) \\ &= \sum_{e|k} \frac{c_e}{e} \cdot \frac{\phi(k/e)}{k/e} = \sum_{e|k} c_e \frac{\phi(k/e)}{k}. \end{aligned} \tag{1.1}$$

In the above, ϕ denotes the Euler totient function. For details on this derivation, the reader is directed to [7, Chapter 17] .

In this paper, we answer the analogous question for commutators rather than for commutator-subgroup elements. This new inquiry is structurally different in that it aims to solve a Diophantine equation over a group G (whether there exist X and Y such that $XYX^{-1}Y^{-1} = W$) for a given $W \in G$, rather than a subgroup-membership problem (whether W is in $[G, G]$). In particular, the set of commutators is not multiplicatively closed, so we cannot use primitive words as a bridge between counting cyclically reduced words and counting conjugacy classes as above. Instead, we use a theorem of Wicks [14], which states that an element of F_r is a commutator if and only if it is a cyclically reduced conjugate of a commutator satisfying the following definition.

Definition 1.1. A *Wicks commutator of* F_r is a word $W \in F_r$ of the form $ABCA^{-1}B^{-1}C^{-1}$, where the product is *cyclically reduced*; i.e., there are no cancellations between the subwords A, B, C, A^{-1}, B^{-1}, and C^{-1}, and the first and last letters are not inverses.

After proving this theorem for expository purposes, we count the number of conjugacy classes of commutators with length k in F_r by counting the number of Wicks commutators with length k.

Theorem 1.2. *Let $k \geq 0$ be even. The number of distinct conjugacy classes of commutators in F_r with length k is given by*

$$\frac{(2r-2)^2(2r-1)^{\frac{k}{2}-1}}{96r}\left(k^2 + O_r(k)\right),$$

where the implied constant depends only on r and is effectively computable.

Note that the number of conjugacy classes of commutators in F_r is roughly proportional to the square root of the number (1.1) of all conjugacy classes with trivial abelianization.

We also employ a similar argument, using Wicks' characterization of commutators in free products, to answer the analogous question for $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. This group is of independent interest as the isomorphism class of $\mathrm{PSL}_2(\mathbb{Z})$; specifically, for the usual generators

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.2}$$

of $\mathrm{PSL}_2(\mathbb{Z})$, we have that S corresponds to a generator of the $\mathbb{Z}/2\mathbb{Z}$ factor and ST, to a generator of the $\mathbb{Z}/3\mathbb{Z}$ factor. Let $\mathfrak{S} := \{r, r^{-1}, s\}$, where r denotes a generator of the $\mathbb{Z}/3\mathbb{Z}$ factor and s, the generator of the $\mathbb{Z}/2\mathbb{Z}$ factor. Then, a theorem of Wicks [14] analogous to the previous one, which we will again prove for expository purposes, implies that an element of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is a commutator if and only if it is a cyclically reduced conjugate of a commutator satisfying the following definition.

Definition 1.3. A *Wicks commutator of* $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is a word $W \in \mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ either of the form $ABA^{-1}B^{-1}$ or of the form $A\alpha B\beta C\alpha A^{-1}\beta B^{-1}\alpha C^{-1}\beta$ for $\alpha, \beta \in \{r, r^{-1}\}$. Here, the product is *fully cyclically reduced*; i.e., adjacent letters are in different factors of the free product, as are the first and last letters.

A fully cyclically reduced element W with length k in $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ alternates between $k/2$ letters in $\{r, r^{-1}\}$ and $k/2$ letters equal to s, where $k/2$ is necessarily an integer. Thus, the number of fully cyclically reduced elements with length k in $\mathbb{Z}/3\mathbb{Z}*\mathbb{Z}/2\mathbb{Z}$ is 0 if k is odd and $2^{k/2}$ if k is even. Furthermore, W has trivial abelianization if and only if $k/2$ is an even integer (so that the product of all the s factors is trivial) and the product of all the letters of W in $\{r, r^{-1}\}$ is trivial. In particular, this is necessary for W to be a Wicks commutator, so the length of any Wicks commutator of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is divisible by 4. Accordingly, for any k divisible by 4, we obtain the number of length-k conjugacy classes in $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ comprised of commutators.

Theorem 1.4. *Let $k \geq 0$ be a multiple of 4. The number of distinct conjugacy classes of commutators in $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ with length k is given by*

$$\frac{2^{\frac{k}{4}}}{384}\left(k^2 + O\left(k\right)\right),$$

where the implied constant is effectively computable.

Suppose that $4 \mid k$. Then, the cyclically reduced elements of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ with length k are in bijection with the closed paths of length $k/2$ on the triangle PQR with fixed basepoint P. Let p_n denote the number of paths with length n from P to itself and q_n, the number of paths with length n from Q to P. Then, note that $p_n = 2q_{n-1}$ for $n \geq 1$, and thus, q_n is the solution to the linear recurrence

$$q_0 = 0, \quad q_1 = 1, \quad \text{and} \quad q_n = q_{n-1} + p_{n-1} = q_{n-1} + 2q_{n-2} \text{ for } n \geq 2,$$

which is $(2^n + (-1)^{n+1})/3$. It follows that $p_n = 2q_{n-1} = \left(2^n + 2(-1)^n\right)/3 = 2^n/3 + O(1)$. Thus, the number of cyclically reduced words with length k in $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is $2^{k/2}/3 + O(1)$, and applying Möbius inversion as done in (1.1), we see that the number of conjugacy classes of commutators in $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is roughly comparable to the square root of the number of all conjugacy classes with trivial abelianization.

Counting conjugacy classes of commutators has a topological application. Let X be a connected CW complex with fundamental group G, and let $\mathcal{C}$ be a conjugacy class of G with trivial abelianization, corresponding to the free homotopy class of a homologically trivial loop $\gamma : S^1 \to X$. Then, the *commutator length* of $\mathcal{C}$, defined as the minimum number of commutators whose product is equal to an element of $\mathcal{C}$, is also the minimum genus of an orientable surface that continuously maps to X so that the boundary of the surface maps to γ [2, Section 2.1]. Thus, using the bijective correspondence between conjugacy classes of the fundamental group and free homotopy classes of loops $S^1 \to X$, our above results immediately yield the following corollaries.

Corollary 1.5. *Let X be a connected CW complex.*

1. *Suppose X has fundamental group F_r with a symmetric set of free generators $\mathfrak{S}$. Then, the number of free homotopy classes of loops $\gamma : S^1 \to X$ with length k (in the generators of $\mathfrak{S}$) such that there exists a genus-1 orientable surface Y and a continuous map $f : Y \to X$ satisfying $f(\partial Y) = \operatorname{Im}\gamma$ is given by*

$$\frac{(2r-2)^2(2r-1)^{\frac{k}{2}-1}}{96r}\left(k^2 + O_r(k)\right),$$

where the implied constant depends only on r and is effectively computable.

2. *Suppose X has fundamental group $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ with the symmetric set of generators $\mathfrak{S} = \{r, r^{-1}, s\}$, where r is a generator of the $\mathbb{Z}/3\mathbb{Z}$ factor and s, the generator of the $\mathbb{Z}/2\mathbb{Z}$ factor. Then, the number of free homotopy classes of loops $\gamma : S^1 \to X$ with length k (in the generators of $\mathfrak{S}$) such that there exists a genus-1 orientable surface Y and a continuous map $f : Y \to X$ satisfying $f(\partial Y) = \operatorname{Im}\gamma$ is given by*

$$\frac{2^{\frac{k}{4}}}{384}\left(k^2 + O(k)\right),$$

where the implied constant is effectively computable.

In addition, counting conjugacy classes of $\mathrm{PSL}_2(\mathbb{Z})$ arises in the following geometric context. Consider the upper-half plane $\mathbb{H}$ and a discrete subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ which acts on $\mathbb{H}$ by fractional linear transformations; in our case, $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. Then, the quotient surface $\Gamma\backslash\mathbb{H}$ is a hyperbolic manifold, and every hyperbolic element $h \in \Gamma$ gives rise to a closed geodesic of $\Gamma\backslash\mathbb{H}$ by projecting the geodesic of $\mathbb{H}$ connecting the fixed points of h to $\Gamma\backslash\mathbb{H}$. In fact, this gives a bijective correspondence between the closed geodesics of $\Gamma\backslash\mathbb{H}$ and the hyperbolic conjugacy classes of Γ. In this correspondence, the primitive hyperbolic conjugacy classes give rise to primitive closed geodesics. These are called prime geodesics because when ordered by trace, they satisfy equidistribution theorems analogous to those of prime numbers, such as the prime number theorem (generally credited to Selberg [12], while its analogue for surfaces of varying negative curvature was proven by Margulis [8]) and Chebotarev's density theorem (proven by Sarnak [10]). Specifically, this analogue of the prime number theorem is called the prime geodesic theorem, which states that the number of prime geodesics of $\Gamma\backslash\mathbb{H}$ with norm $\leq N$ is asymptotically given by $\sim N/\log N$. Furthermore, Sarnak's analogue of Chebotarev's density theorem implies that the number of prime geodesics of $\Gamma\backslash\mathbb{H}$ with norm $\leq N$ that correspond to elements of Γ with trivial abelianization is asymptotically given by $\sim N/(6\log N)$, since $[\Gamma,\Gamma]$ is an index-6 subgroup (in fact, a congruence subgroup) of Γ; see (3.3) for details.

For this application, we present an algorithm, based on Gauss' reduction theory of indefinite binary quadratic forms and Wicks' theorem, to exhaustively compute the hyperbolic conjugacy classes of commutators of Γ with a given trace. Note that the trace t of a hyperbolic element of Γ is connected to the norm N of the corresponding geodesic by the relationship

$$N = \left(\frac{t+\sqrt{t^2-4}}{2}\right)^2.$$

A commutator of Γ is precisely a coset $\{C,-C\}$ for a commutator $C = ABA^{-1}B^{-1}$ of $\mathrm{SL}_2(\mathbb{Z})$, where $A, B \in \mathrm{SL}_2(\mathbb{Z})$. In light of this, one application of this algorithm arises from the fact that commutators $ABA^{-1}B^{-1}$ of $\mathrm{SL}_2(\mathbb{Z})$ with a given trace t give rise to integral solutions

$$(\mathrm{Tr}(A), \mathrm{Tr}(B), \mathrm{Tr}(AB))$$

of the Markoff-type surface $x^2+y^2+z^2-xyz = t+2$, since we have the trace identity

$$\mathrm{Tr}(A)^2+\mathrm{Tr}(B)^2+\mathrm{Tr}(AB)^2-\mathrm{Tr}(A)\,\mathrm{Tr}(B)\,\mathrm{Tr}(AB) = \mathrm{Tr}(ABA^{-1}B^{-1})+2.$$

Integral points on this Markoff-type surface are of independent number-theoretic interest and have been studied in [1] and [5].

Finally, we conclude our paper with a discussion of the data arising from the algorithm, along with several conjectures suggested by our work.

Chapter 2

Commutators of the Free Group

2.1 Proof of Wicks' Theorem for the Free Group

In this section, we give an exposition of Wicks' proof of his theorem [14] that every commutator in F_r is conjugate to a Wicks commutator, i.e., a word of the fully cyclically reduced form $ABCA^{-1}B^{-1}C^{-1}$. In fact, this is a full characterization, since a Wicks commutator is indeed a commutator, as seen from

$$(AC^{-1})(CB)(AC^{-1})^{-1}(CB)^{-1} = ABCA^{-1}B^{-1}C^{-1}. \tag{2.1}$$

Suppose that W is a nontrivial commutator. Then, the set of commutators of the form $ABCA^{-1}B^{-1}C^{-1}$ (not necessarily cyclically reduced) that are conjugate to W is nonempty, and we can take the least-length such commutator $XYZX^{-1}Y^{-1}Z^{-1}$. We will show that this expression is cyclically reduced.

Suppose the contrary. If two of the factors X, Y, and Z are trivial, then we have that W is trivial, a contradiction. First, we suppose that one of X, Y, and Z is trivial. By conjugating, we may assume that Z is trivial. Then, in the expression $XYX^{-1}Y^{-1}$, we must have that two cyclically adjacent letters in distinct subwords (among X, Y, X^{-1}, and Y^{-1}) are inverses. Again, by conjugating, we may assume that these two letters are the first letter of X and the last letter of Y^{-1}. Then, we must have $X = \alpha X_1$ and $Y = \alpha Y_1$. But then, $X_1\alpha Y_1 X_1^{-1}\alpha^{-1}Y_1^{-1}$, which is also of the form $ABCA^{-1}B^{-1}C^{-1}$, is conjugate to

$\alpha X_1 \alpha Y_1 X_1^{-1} \alpha^{-1} Y_1^{-1} \alpha^{-1}$, and thus to W. This contradicts our minimality assumption.

Second, we suppose that none of X, Y, and Z are trivial. Then, in the expression $XYZX^{-1}Y^{-1}Z^{-1}$, we must have that two cyclically adjacent letters in distinct subwords (among X, Y, Z, X^{-1}, Y^{-1} and Z^{-1}) are inverses. By conjugating, we may assume that these two letters are the first letter of X and the last letter of Z^{-1}. Then, we must have $X = \alpha X_1$ and $Z = \alpha Z_1$. However, this implies that $X_1 Y \alpha Z_1 X_1^{-1} \alpha^{-1} Y^{-1} Z_1^{-1} = X_1(Y\alpha)Z_1 X_1^{-1}(Y\alpha)^{-1} Z_1^{-1}$, which is also of the form $ABCA^{-1}B^{-1}C^{-1}$, is conjugate to $\alpha X_1 Y \alpha Z_1 X_1^{-1} \alpha^{-1} Y^{-1} Z_1^{-1} \alpha^{-1}$, and thus to W. This contradicts our minimality assumption.

Thus, we have proven that a word in F_r is a commutator if and only if it is a conjugate of a Wicks commutator.

2.2 Proof of Theorem 1.2

Since the cyclically reduced conjugacy representative of F_r is unique up to cyclic permutation, it suffices to count equivalence classes (with respect to cyclic permutation) of Wicks commutators of length $k = 2X$. Let R_X denote the set of reduced words of length X, of which there are $2r \cdot (2r-1)^{X-1}$. For each such word W, the number of ways to decompose W into A, B, and C (i.e., $W = ABC$ without cancellation) is given by the number of ordered partitions p of X into three (not necessarily nontrivial) parts.

Let $p = (n_1, n_2, n_3)$. From this point, we suppose that $0 < n_1, n_2, n_3$. Define a pair (W, p) to be *viable* if the resulting word $W' := ABCA^{-1}B^{-1}C^{-1}$ is a Wicks commutator. We now show that for a fixed p, the proportion of $W \in R_X$ such that (W, p) is viable is given by

$$\frac{1}{2r} + O\left(\frac{1}{(2r-1)^{n_1-1}} + \frac{1}{(2r-1)^{n_2-1}} + \frac{1}{(2r-1)^{n_3-1}}\right).$$

For $s \in \mathfrak{S}$, let $R_n^s \subset R_n$ denote the subset of words that begin with s, which gives us a decomposition of R_n into the disjoint union $R_n = \bigcup_{s \in \mathfrak{S}} R_n^s$. The number q_n of words in R_n^s whose final letter is s is the solution to the linear recurrence given by $q_1 = 1$ and

$q_{i+1} = (2r-1)^{i-1} - q_i$, which is

$$q_n = \frac{(2r-1)^{n-1} + (-1)^{n-1} \cdot (2r-1)}{2r}.$$

Thus, we have that the proportion of words in R_n^s whose final letter is s is

$$\frac{q_n}{|R_n^s|} = \frac{(2r-1)^{n-1} + (-1)^{n-1} \cdot (2r-1)}{2r \cdot (2r-1)^{n-1}} = \frac{1}{2r} + O\left(\frac{1}{(2r-1)^{n-1}}\right),$$

while the proportion of words whose final letter is s^{-1} is

$$\frac{1}{2r-1}\left(1 - \frac{q_n}{|R_n^s|}\right) = \frac{1}{2r} + O\left(\frac{1}{(2r-1)^{n-1}}\right).$$

Now, fix a partition p, and consider R_X with the uniform probability measure placed on its elements. Within the decomposition $W = ABC$ in accordance with p, let the first letter and last letter of A respectively be a_0 and a_1, and define b_0, b_1, c_0, and c_1 similarly. We will compute the probability that (W, p) is viable for a random $W \in R_X$, i.e., the probability that $b_1 \neq a_0^{-1}$, $c_0 \neq a_0$, $c_1 \neq a_1$, and $c_1 \neq b_0^{-1}$.

Suppose that the first letter of W is s. Then, by our work above, the set of possible candidates for $a_1 b_0$ is the $2r(2r-1)$-element set $S = \{wz : w, z \in \mathfrak{S}, w \neq z^{-1}\}$, each of which has probability

$$\frac{1}{2r-1}\left(\frac{1}{2r} + O\left(\frac{1}{(2r-1)^{n_1-1}}\right)\right) = \frac{1}{2r(2r-1)} + O\left(\frac{1}{(2r-1)^{n_1}}\right).$$

We fix a choice of $a_1 b_0$ in S, and all probabilities from now on are conditional on this event. The set of possible candidates for $b_1 c_0$ is also S, each of which has probability $1/2r(2r-1) + O(1/(2r-1)^{n_2})$. Let $S' \subset S$ be the subset of possible candidates for $b_1 c_0$ that satisfy the conditions $a_0 \neq b_1^{-1}$ and $a_0 \neq c_0$. The cardinality of S' can be computed as follows: there are $2r-1$ choices for b_1 satisfying $s \neq b_1^{-1}$, and conditional on this, there are $2r-2$ choices for c_0 satisfying $s \neq c_0$ and $b_0 \neq c_0^{-1}$, for a total of $(2r-1)(2r-2)$ elements of S'. Fix a choice of $b_1 c_0$ in S', and all probabilities from now on are conditional on this event. Since $a_1 \neq b_0^{-1}$, the conditions $c_1 \neq a_1$ and $c_1 \neq b_0^{-1}$ leave precisely $2r-2$ (out of

$2r$) possible values for c_1, so the probability that c_1 satisfies these conditions is

$$\frac{2r-2}{2r} + O\left(\frac{1}{(2r-1)^{n_3}}\right).$$

Overall, we have that the probability that (W, p) is viable is

$$\begin{aligned}
&2r(2r-1) \cdot \left(\frac{1}{2r(2r-1)} + O\left(\frac{1}{(2r-1)^{n_1}}\right)\right)\\
&\cdot (2r-1)(2r-2)\left(\frac{1}{2r(2r-1)} + O\left(\frac{1}{(2r-1)^{n_2}}\right)\right)\\
&\cdot (2r-2)\left(\frac{1}{2r} + O\left(\frac{1}{(2r-1)^{n_3-1}}\right)\right)\\
&= \left(\frac{2r-2}{2r}\right)^2 \cdot \left(1 + O\left(\frac{1}{(2r-1)^{n_1-2}}\right)\right) \cdot \left(1 + O\left(\frac{1}{(2r-1)^{n_2-2}}\right)\right)\\
&\cdot \left(1 + O\left(\frac{1}{(2r-1)^{n_3-2}}\right)\right)\\
&= \left(\frac{2r-2}{2r}\right)^2 \left(1 + O\left(\frac{1}{(2r-1)^{n_1-2}} + \frac{1}{(2r-1)^{n_2-2}} + \frac{1}{(2r-1)^{n_3-2}}\right)\right).
\end{aligned}$$

The number of (W, p) that are viable is then given by

$$\begin{aligned}
&\sum_{\substack{0<n_1,n_2,n_3\\ n_1+n_2+n_3=X}} 2r(2r-1)^{X-1}\left(\frac{2r-2}{2r}\right)^2\\
&\cdot \left(1 + O\left(\frac{1}{(2r-1)^{n_1-2}} + \frac{1}{(2r-1)^{n_2-2}} + \frac{1}{(2r-1)^{n_3-2}}\right)\right)\\
&= \frac{(2r-2)^2(2r-1)^{X-1}}{2r}\\
&\cdot \left(\frac{(X-2)(X-1)}{2} + \sum_{\substack{0<n_1,n_2,n_3\\ n_1+n_2+n_3=X}} O\left(\frac{1}{(2r-1)^{n_1-2}} + \frac{1}{(2r-1)^{n_2-2}} + \frac{1}{(2r-1)^{n_3-2}}\right)\right)\\
&= \frac{(2r-2)^2(2r-1)^{X-1}}{2r}\left(\frac{(X-2)(X-1)}{2} + 3 \cdot O\left(\sum_{\substack{0<n_1,n_2,n_3\\ n_1+n_2+n_3=X}} \frac{1}{(2r-1)^{n_1-2}}\right)\right)\\
&= \frac{(2r-2)^2(2r-1)^{X-1}}{2r}\left(\frac{(X-2)(X-1)}{2} + O\left(\sum_{n_1=1}^{X-2}(X-1-n_1)\frac{1}{(2r-1)^{n_1-2}}\right)\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{(2r-2)^2(2r-1)^{X-1}}{2r} \\
&\cdot \left(\frac{(X-2)(X-1)}{2} + O\left(\frac{(2r-1)^2\left((2r-1)^{2-X} + X(2r-2) - 4r + 3\right)}{(2r-2)^2} \right) \right) \\
&= \frac{(2r-2)^2(2r-1)^{X-1}}{4r} \left(X^2 + O\left(\frac{r^2}{(2r-1)^X} + rX \right) \right).
\end{aligned}
$$

While all commutators arise from viable pairs (W, p), there could be a commutator $ABCA^{-1}B^{-1}C^{-1}$ arising from distinct viable pairs, say (W, p_1) and (W, p_2) for $p_1 = (n_1, n_2, n_3)$, and $p_2 = (m_1, m_2, m_3)$. We show that the number of such commutators is small.

Let $W = ABC$ be its decomposition with respect to p_1, and $W = A'B'C'$ its decomposition with respect to p_2. Consider the function $f : \{1, \ldots, X\} \to \{1, \ldots, X\}^2$ that maps i to (j, k) in the following way: the ith letter of $A^{-1}B^{-1}C^{-1}$, when corresponding to p_1, is the inverse of the jth letter of W, and when corresponding to p_2, is the inverse of the kth letter of W. For example, the first letter of $A^{-1}B^{-1}C^{-1}$ is defined to be the inverse of the n_1th when the decomposition is in terms of p_1, and is defined to be the m_1th letter of W when in terms of p_2, so $f(1) = (n_1, m_1)$. We consider two cases: when the two entries of $f(i)$ are distinct for all i, and otherwise. In the first case, the following algorithm allows us to reduce the degrees of freedom for the letters of W by at least half:

1. Let $i = 1$. For $f(i) = (j_i, k_i)$, do the following:

   - If neither the j_ith or the k_ith position has an indeterminate variable assigned to it, then assign a new indeterminate variable simultaneously to the j_ith and k_ith positions. This increases the number of indeterminate variables by two.
   - If just one of the j_ith and the k_ith positions has an indeterminate variable assigned to it, but the other does not, then assign this indeterminate variable to the former.
   - If both the j_ith and the k_ith positions have the same indeterminate variable assigned to them, make no changes.

- If the j_ith and the k_ith positions have distinct indeterminate variables assigned to them, set these indeterminate variables equal to each other. This decreases the number of indeterminate variables by one.

2. Increment i by one and repeat this procedure for all $1 \leq i \leq X$.

By our hypothesis that the two entries of $f(i)$ are distinct for all i, the number of indeterminate variables, which precisely represents the number of degrees of freedom for the word W such that (W, p_1) and (W, p_2) give rise to the same commutator, is $\leq X/2$. It follows that there are only $O((2r-1)^{X/2})$ of such words for each pair p_1, p_2.

Now, consider the next case that there exists an i such that the two entries of $f(i)$ are equal. Then, we consider the following three cases for W, p_1, and p_2:

Case 1. Suppose the smallest i such that the two entries of $f(i)$ are equal satisfies that this entry is a position in A. Then, $n_1 = m_1$ must be this entry and i must equal 1, since otherwise we can continue to decrement i so that the two entries of $f(i)$ are incremented and remain equal, a contradiction. Next, the subwords $B^{-1}C^{-1}$ and $B'^{-1}C'^{-1}$ must be equal. Without loss of generality, suppose that $n_2 > m_2$. Decompose $B = B'D$ so that our condition $B^{-1}C^{-1} = B'^{-1}C'^{-1}$ is precisely $CB'D = DCB'$. Since CB' and D commute, we have that they are both powers of a common subword V; without loss of generality, the powers are positive, since otherwise there would be cancellation, which contradicts that the commutator is cyclically reduced. We can bound the number of (W, p) satisfying this case by counting, for each $i = X - n_1$ and for each proper divisor $d \mid i$ (denoting the length of V), the number of ways to place V in the right subword of length i and the number of degrees of freedom. Thus, the number of additional Wicks commutators arising from this case can be upper-bounded by

$$\sum_{i=1}^{X-1} \sum_{\substack{d \mid i \\ d \neq i}} (i-d+1) \cdot (2r-1)^{X-i+d}$$

$$\leq (2r-1)^X \cdot \sum_{i=2}^{X-1} \sum_{1 \leq d \leq \frac{i}{2}} (i-d+1) \cdot (2r-1)^{-i+d}$$

$$
\begin{aligned}
&= (2r-1)^X \cdot \sum_{i=2}^{X-1} (2r-1)^{-i} \sum_{1 \le d \le \frac{i}{2}} (i-d+1) \cdot (2r-1)^d \\
&\le (2r-1)^X \cdot \sum_{i=2}^{X-1} (2r-1)^{-i+1} \frac{i(2r-2)\left((2r-1)^{\frac{i}{2}}-2\right) + 2(2r-1)\left((2r-1)^{\frac{i}{2}}-1\right)}{2(2r-2)^2} \\
&\ll (2r-1)^X,
\end{aligned}
$$

which is dominated by our error term.

Case 2. Suppose the smallest i such that the two entries of $f(i)$ are equal satisfies that this entry is a position in C. An argument symmetric to that above can be given to show that the above expression is also an upper bound for the number of (W, p) satisfying this case.

Case 3. Suppose the smallest i such that the two entries of $f(i)$ are equal satisfies that this entry is a position in B. Without loss of generality, suppose $n_1 > m_1$. Then, $f(m_1 + 1) = (n_1 - m_1, m_1 + m_2)$, and by an argument similar to that in Case (1), we have that the simultaneous entry of the aforementioned $f(i)$ must be $n_1 + n_2$, with $n_1 - m_1 = n_3 - m_3$ so that $f(m_1 + 1) = (n_1 - m_1, n_1 + n_2 + (n_1 - m_1))$. Thus, divide W into $DEFGH$ so that $|D| + |E| = n_1$, $|G| + |H| = n_3$, and $|E| = |G|$. Then, (W, p_1) gives rise to the commutator $WE^{-1}D^{-1}F^{-1}H^{-1}G^{-1}$, while (W, p_2) gives rise to the commutator $WD^{-1}G^{-1}F^{-1}E^{-1}H^{-1}$. Since these are equal, it follows that $DE = GD$ and $GH = HE$. Note that if a word $\square$ satisfies the equality $\square E = G\square$ without cancellation, then $\square$ is uniquely determined, since one can inductively identify the letters of $\square$ from left to right (or right to left). It follows that $D = H$. But this contradicts the assumption that $DEFGHD^{-1}G^{-1}F^{-1}E^{-1}H^{-1}$ is cyclically reduced.

Note that pairs (W, p) such that $n_i = 0$ for some $i \in \{1, 2, 3\}$ are counted in the above cases, which justifies our assumption of $n_1, n_2, n_3 > 0$ in our earlier counting of the main term.

We have shown that the number of Wicks commutators having length X is

$$
\frac{(2r-2)^2(2r-1)^{X-1}}{4r}\left(X^2 + O_r(X)\right).
$$

We need to count the number of conjugacy classes containing at least one such commutator. Consider the conjugacy class $\mathcal{C}$ of the Wicks commutator $W' = ABCA^{-1}B^{-1}C^{-1}$ arising from (W, p), where $p = (n_1, n_2, n_3)$. Note that the minimum-length elements in a conjugacy class are precisely the cyclically reduced words, and that two cyclically reduced words are conjugate if and only if they are cyclically conjugate. The Wicks commutators $BCA^{-1}B^{-1}C^{-1}A$, $CA^{-1}B^{-1}C^{-1}AB$, $A^{-1}B^{-1}C^{-1}ABC$, $B^{-1}C^{-1}ABCA^{-1}$, and $C^{-1}ABCA^{-1}B^{-1}$ are conjugates of W'. We show that the number of other Wicks commutators in $\mathcal{C}$ is on average negligible.

For an arbitrary $1 \leq \ell \leq n_3/2$ denoting the number of letters of the conjugation, let $C = DEF$ be a decomposition without cancellation such that $|D| = |F| = \ell$. Label the letters of W' by $A = a_1 \cdots a_{n_1}$, $B = b_1 \cdots b_{n_2}$, $D = d_1 \cdots d_\ell$, $E = e_1 \cdots e_{n_3-2\ell}$, and $F = f_1 \cdots f_\ell$. Consider the cyclic conjugate $W'' := D^{-1}ABDEFA^{-1}B^{-1}F^{-1}E^{-1}$ of W'. We wish to show that on average, W'' is not a Wicks commutator. Suppose the contrary, that there exists a partition $p' = (m_1, m_2, m_3)$ of X into three parts such that

$$W'' = D^{-1}ABDEFA^{-1}B^{-1}F^{-1}E^{-1} = w_1w_2w_3w_1^{-1}w_2^{-1}w_3^{-1}$$

for subwords w_1, w_2, and w_3 of lengths m_1, m_2, and m_3.

Label the letters of A from left to right as $a_1, \ldots, a_{n_1}$, and label the letters of B, C, D, E, and F similarly. We have that w_1, w_2, and w_3 as subwords comprised of the letters

$$d_\ell^{-1}, \ldots, d_1^{-1}, a_1, \ldots, a_{n_1}, b_1, \ldots, b_{n_2}, d_1, \ldots, d_\ell, e_1, \ldots, e_{n_3-2\ell}, \tag{2.2}$$

and we accordingly consider the subwords w_1^{-1}, w_2^{-1}, and w_3^{-1} as comprised of the inverses of these letters. Then, note that the second half of W' can be considered in two forms:

$$FA^{-1}B^{-1}F^{-1}E^{-1} = w_1^{-1}w_2^{-1}w_3^{-1}.$$

Equivalently, this equality can be written as

$$EFBAF^{-1} = w_3w_2w_1. \tag{2.3}$$

Consider the function g mapping the ordered set of symbols of the left-hand side,

$$\mathcal{A} := \{e_1, \ldots, e_{n_3-2\ell}, f_1, \ldots, f_\ell, b_1, \ldots, b_{n_2}, a_1, \ldots, a_{n_1}, f_\ell^{-1}, \ldots, f_1\}$$

to the ordered set $\mathcal{B}$ of symbols of the right-hand side (2.2). Specifically, g maps the ith leftmost letter of the left-hand side of (2.3) to the ith leftmost letter of the right-hand side.

First, suppose g has no fixed points ($\mathfrak{i}$ such that $g(\mathfrak{i}) = \mathfrak{i}$). Then, use an algorithm similar to the previous one to conclude that there are $\leq X/2$ degrees of freedom for $ABDEF$, so W must be one of only $O((2r-1)^{X/2})$ choices (for each choice of ℓ and p').

Now, suppose that there exists an $\mathfrak{i}$ such that $g(\mathfrak{i}) = \mathfrak{i}$. Such fixed points $\mathfrak{i}$ must be letters of A, B, or E. We first consider the case that all the fixed points are letters of only one of A, B, and E. In this case, we consider the following subcases for W, p, and p':

Case 1. Suppose that the fixed points are letters of E. Then, all of the fixed points must be in one of w_2 and w_3; they cannot be in w_1, since this would mean that w_1 contains e_1, but e_1 is necessarily located at different positions in the left-hand side and right-hand side of (2.3). Suppose that the fixed points of E are in w_3. Then, in order for the letters of E to match, we require that $w_3 = E$. This means that $g(f_1)$ is the first letter of w_2, which is adjacent to the last letter of w_1. But the last letter of w_1 is $g(f_1^{-1})$, which shows that we have adjacent letters that are inverses. This contradicts the fact that W' is cyclically reduced.

Next, suppose all the fixed points are in w_2. Then, we must have that $m_3 + 1 = n_3 - 2\ell - (m_2 + m_3)$ so that the first letter of w_2 is at the same position in both the left-hand and right-hand side. Thus, $m_2 + 2m_3 = n_3 - 2\ell - 1$, which means there are $\leq (n_3 - 2\ell - 1)/2$ choices for p' parametrized by $m_3 \leq (n_3 - 2\ell - 1)/2$. For each such choice of p', there are $m_2 = n_3 - 2\ell - (1 + m_3 + m_3) = n_3 - 2\ell - 2m_3 - 1$ fixed letters, from e_{m_3+1} to $e_{n_3-2\ell-m_3+1}$, and $(X - (n_3 - 2\ell - 2m_3 - 1))/2$ non-fixed letters. Counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X}\sum_{n_2=0}^{X-n_1}\sum_{\ell=1}^{\left\lfloor\frac{X-n_1-n_2}{2}\right\rfloor}\sum_{m_3=0}^{\left\lfloor\frac{n_3-2\ell-1}{2}\right\rfloor}(2r-1)^{\frac{X+n_3-2\ell-2m_3-1}{2}} \ll (2r-1)^X,$$

which is dominated by our error term.

Case 2. Suppose that the fixed points are letters of B. Then, all of the fixed points must be in one of w_1, w_2, and w_3. First, suppose they are in w_1. Then, note that $g(f_\ell) = a_{n_1}$, but we also have $g(a_{n_1})$ is next to $g(f_\ell^{-1})$, which leads to the contradiction that a letter cannot equal its inverse. Second, suppose the fixed letters are in w_3. Then, $g(d_1) = a_1$, but a_1 is adjacent to d_1^{-1}, a contradiction.

Thus, the fixed points of B must be in w_2. We consider three subcases: $n_2 > m_2$, $n_2 < m_2$, and $n_2 = m_2$. If $n_2 > m_2$, then in order for the letters of B to match, we require that the leftmost fixed letter of B is $b_{\frac{n_2+m_2}{2}}$. But then $b_{\frac{n_2+m_2}{2}-1}$ is both equal to f_1^{-1} (since $g(f^{-1}) = b_{\frac{n_2+m_2}{2}-1}$) and $e_{n_3-2\ell}$ (since $g(b_{\frac{n_2+m_2}{2}-1}) = e_{n_3-2\ell})$), which contradicts the fact that f_1 and $e_{n_3-2\ell}$ are adjacent. If $n_2 < m_2$, then $g(f_\ell) = a_{n_1}$, but also $g(a_{n_1})$ is the letter in $D^{-1}A$ that is left of the letter $g(f_\ell^{-1})$, giving us the contradiction that the value of f_ℓ is adjacent to f_ℓ^{-1}. This implies that $n_2 = m_2$, from which we can use an argument similar to that in Case 1 of the previous casework (showing that W' on average can be only decomposed as a commutator in one way) to conclude that A is a power of D^{-1} and E, a power of D. It follows that our original (W, p) is one of the pairs falling under Case 1 of the previous casework, which are negligible.

Case 3. Suppose that the fixed points are letters of A. Then, all of the fixed points must be in one of w_1 and w_2; they cannot be in w_3, since then there must be more than ℓ letters right of A. Suppose the fixed letters of A are in w_1. Then, we must have $g(b_{n_2}) = d_1^{-1}$, which contradicts the fact that b_{n_2} is adjacent to d_1. Therefore, the fixed points are necessarily in w_2. This requires that $m_1 - \ell + 1 = n_1 + \ell - (m_1 - m_2)$ in order for the letters of A to be in matching positions. Thus, we have $m_2 = n_1 + 2\ell - 2m_1 - 1$. Note then that p' is parametrized by $m_1 \leq (n_1 + 2\ell - 1)/2$. For each choice of p', we have n_1 fixed letters (and $(X + n_1)/2 \leq (X + n_1 - m_1 + \ell)/2$ overall degrees of freedom) if $m_1 \leq \ell$, and $n_1 - (m_1 - \ell)$

fixed letters (and $(X+n_1-m_1+\ell)/2$ overall degrees of freedom) if $m_1 > \ell$. Thus, counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X} \sum_{n_2=0}^{X-n_1} \sum_{\ell=1}^{\left\lfloor \frac{X-n_1-n_2}{2} \right\rfloor} \sum_{m_1=0}^{\left\lfloor \frac{n_1+2\ell-1}{2} \right\rfloor} (2r-1)^{\frac{X+n_1+\ell-m_1}{2}} \ll (2r-1)^X,$$

which is dominated by our error term.

Next, consider the case where the fixed points are in two of A, B, and E. It is necessary that the fixed letters inside these two subwords must respectively be in two distinct subwords among w_1, w_2, and w_3. However, we have shown above that the subwords w_1 and w_3 cannot contain fixed points, a contradiction. Finally, the fixed letters cannot be in all of A, B, and E. Indeed, if this were true, then in order for the letters of A and E to match, we require $m_1 = n_1 + 2\ell$ and $m_3 = n_3$. But then the letters of B cannot possibly match, a contradiction.

If $\ell \geq n_3/2$, then we can think of our commutator as a cyclic conjugate of $C^{-1}ABCA^{-1}B^{-1}$ such that the letters are moved from left to right. A symmetric argument like above gives us the same conclusion for this case. We have thus shown that the number of conjugacy classes of commutators with length $2X$ is given by

$$\begin{aligned} &\frac{1}{6} \cdot \frac{(2r-2)^2(2r-1)^{X-1}}{4r} \left(X^2 + O_r(X)\right) \\ &= \frac{(2r-2)^2(2r-1)^{X-1}}{24r} \left(X^2 + O_r(X)\right), \end{aligned}$$

as needed.

Chapter 3

Commutators of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$

3.1 Proof of Wicks' Theorem for Free Products

In addition to his theorem classifying commutators of free groups, Wicks [14] also proved the following analogous theorem characterizing all commutators of a free product of arbitrary groups.

Theorem 3.1 (Wicks). *A word in $*_{i\in I} G_i$ is a commutator if and only if it is a conjugate of one of the following fully cyclically reduced products:*

1. *a word comprised of a single letter that is a commutator in its factor G_i,*
2. *$X\alpha_1 X\alpha_2^{-1}$, where X is nontrivial and α_1, α_2 belong to the same factor G_i as conjugate elements,*
3. *$X\alpha_1 Y\alpha_2 X^{-1}\alpha_3 Y^{-1}\alpha_4$, where X and Y are both nontrivial, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ belong to the same factor G_i, and $\alpha_4\alpha_3\alpha_2\alpha_1$ is trivial,*
4. *$XYZX^{-1}Y^{-1}Z^{-1}$,*
5. *$XY\alpha_1 ZX^{-1}\alpha_2 Y^{-1}Z^{-1}\alpha_3$, where Y and at least one of X and Z is nontrivial, $\alpha_1, \alpha_2, \alpha_3$ belong to the same factor G_i, and $\alpha_3\alpha_2\alpha_1$ is trivial,*
6. *$X\alpha_1 Y\beta_1 Z\alpha_2 X^{-1}\beta_2 Y^{-1}\alpha_3 Z^{-1}\beta_3$, where $\alpha_1, \alpha_2, \alpha_3$ belong to the same factor G_i and $\beta_1, \beta_2, \beta_3$, to G_j, $\alpha_3\alpha_2\alpha_1 = \beta_3\beta_2\beta_1 = 1$, and either $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ are not all in the same factor or X, Y, Z are all nontrivial.*

Note that in the above, the Greek letters are assumed to be nontrivial. This convention is used later in the proof of Theorem 3.1 as well, where when a Greek letter α is said to satisfy $\alpha \in G_i$, we mean that α is a nontrivial element of G_i.

Theorem 3.1 implies our claim in the introduction that all commutators of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ are conjugates of Wicks commutators defined in Definition 1.3. Indeed, the free factors of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ are abelian, so the commutators of the form (1) are trivial. Also, if C is a commutator of the form (2), then α_1 and α_2 are conjugate elements in an abelian free factor and thus equal, which means C is of the form $ABA^{-1}B^{-1}$.

Next, we consider commutators C of the form (3). Then, we have that the commutators

- $XrYr^{-1}X^{-1}r^{-1}Y^{-1}r$, which is conjugate to

$$rXrYr^{-1}X^{-1}r^{-1}Y^{-1} = (rXr)Y(rXr)^{-1}Y^{-1},$$

- $Xr^{-1}YrX^{-1}rY^{-1}r^{-1}$, which is conjugate to

$$r^{-1}Xr^{-1}YrX^{-1}rY^{-1} = (r^{-1}Xr^{-1})Y(r^{-1}Xr^{-1})^{-1}Y,$$

- $Xr^{-1}Yr^{-1}XrY^{-1}r = X(r^{-1}Yr^{-1})X^{-1}(r^{-1}Yr^{-1})^{-1}$,
- $XrYrXr^{-1}Y^{-1}r^{-1} = X(rYr)X^{-1}(rYr)^{-1}$,
- $XrYr^{-1}X^{-1}rY^{-1}r^{-1} = X(rYr^{-1})X^{-1}(rYr^{-1})^{-1}$,
- $Xr^{-1}YrX^{-1}r^{-1}Y^{-1}r = X(r^{-1}Yr)X^{-1}(r^{-1}Yr)^{-1}$,

are of the form $ABA^{-1}B^{-1}$. Overall, we have that commutators of the form (3) must be of the cyclically reduced form $XYX^{-1}Y^{-1}$.

If C is of the form (4), then the last letter of X is in different factors compared to the first letter of Y and the last letter of Z, which must also be in different factors, a contradiction. If C is of the form (5), then we must have $\alpha_1 = \alpha_2 = \alpha_3 \in \{r, r^{-1}\}$. But this would imply that the last letter of Y is in different free factors compared to the first letter of Z and the first letter of X, which contradicts the similar implication that the first letter of Z and the first letter of X are in different factors. Finally, if C is of the form (6), then we must have $\alpha_1 = \alpha_2 = \alpha_3 \in \{r, r^{-1}\}$ and $\beta_1 = \beta_2 = \beta_3 \in \{r, r^{-1}\}$. Thus, commutators of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ must be of the fully cyclically reduced form $XYX^{-1}Y^{-1}$ or $X\alpha Y\beta Z\alpha X^{-1}\beta Y^{-1}\alpha Z^{-1}\beta$ for $\alpha, \beta \in \{r, r^{-1}\}$, as we have claimed.

We now exposit a proof of Theorem 3.1, Wicks' theorem for an arbitrary free product $G = *_{i\in I} G_i$. We follow the original proof in [14]. First, we check that the possible forms given in the statement of Theorem 3.1 are in fact commutators. (1) is clearly a commutator. Since $\alpha_1 = \xi\alpha_2\xi^{-1}$ in (2) for some $\xi \in G_i$, we have that $X\alpha_1X^{-1}\alpha_2^{-1} = X\xi\alpha_2\xi^{-1}X^{-1}\alpha_2^{-1} = (X\xi)\alpha_2(X\xi)^{-1}\alpha_2^{-1}$. Next, check that for (3), we have $\alpha_4 = \alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$, which gives that $X\alpha_1Y\alpha_2X^{-1}\alpha_3Y^{-1}\alpha_4 = X\alpha_1Y\alpha_2X^{-1}\alpha_3Y^{-1}\alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$ is conjugate to $\alpha_3^{-1}X\alpha_1Y\alpha_2X^{-1}\alpha_3Y^{-1}\alpha_1^{-1}\alpha_2^{-1} = (\alpha_3^{-1}X)(\alpha_1Y)\alpha_2(\alpha_3X)^{-1}(\alpha_1Y)^{-1}\alpha_2^{-1}$. (4) is a commutator, as shown in (2.1). (6) is a commutator because $\alpha_3 = \alpha_1^{-1}\alpha_2^{-1}$ and $\beta_3 = \beta_1^{-1}\beta_2^{-1}$, which shows that $X\alpha_1Y\beta_1Z\alpha_2X^{-1}\beta_2Y^{-1}\alpha_3Z^{-1}\beta_3 = X\alpha_1Y\beta_1Z\alpha_2X^{-1}\beta_2Y^{-1}\alpha_1^{-1}\alpha_2^{-1}Z^{-1}\beta_1^{-1}\beta_2^{-1}$ is conjugate to the following commutator of form (4): $\beta_2^{-1}X\alpha_1Y\beta_1Z\alpha_2X^{-1}\beta_2Y^{-1}\alpha_1^{-1}\alpha_2^{-1}Z^{-1}\beta_1^{-1}$ $= (\beta_2^{-1}X)(\alpha_1Y)(\beta_1Z\alpha_2)(\beta_2^{-1}X)^{-1}(\alpha_1Y)^{-1}(\beta_1Z\alpha_2)^{-1}$. Finally, (5) is a commutator by substituting $\alpha_1 = \alpha_2 = \alpha_3 = 1$ in the above expression for (6) and its conjugate.

Next, we show the other direction that every commutator is in one of these six forms. Define a word in G to be *fully reduced* if no adjacent pair of letters is in the same free factor G_i. Let C be a nontrivial commutator of G, and let V be the shortest word conjugate to C and of the form $XYZX^{-1}Y^{-1}Z^{-1}$ such that X, Y, and Z are fully reduced. If V is fully cyclically reduced, then we are done, so suppose V is not fully cyclically reduced. If two subwords among X, Y, and Z are trivial, then C must be trivial. We thus consider two cases: Case 1, that one of the subwords X, Y, and Z (without loss of generality, Z) is trivial; and Case 2, that none of them are trivial.

Case 1. Since V is not fully cyclically reduced, we can, by conjugation, assume that the first letter of X and the last letter of Y^{-1} are in the same free factor G_i. Let $X = \eta X_1$ and $Y = \xi Y_1$ for $\eta, \xi \in G_i$, and write $\zeta = \xi^{-1}\eta \in G_i$. Indeed, ζ cannot be trivial, since if this were true, then V would be conjugate to $X_1\xi Y_1X_1^{-1}\xi^{-1}Y_1^{-1}$, which contradicts the assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. Thus, we have that V is conjugate to $V_1 = X_1\xi Y_1X_1^{-1}\eta^{-1}Y_1^{-1}\zeta$. At this point, we consider four subcases:

Subcase 1, that both X_1 and Y_1 are trivial; Subcase 2, that only X_1 trivial; Subcase 3, that only Y_1 is trivial; and Subcase 4, that both X_1 and Y_1 are nontrivial.

Subcase 1. V is conjugate to $V_1 = \xi\eta^{-1}\xi^{-1}\eta$, which reduces to a single-letter commutator in G_i.

Subcase 2. We have $V_1 = X_1\xi X_1^{-1}\eta^{-1}\zeta$. Note that $\eta^{-1}\zeta$ reduces to some single-letter element $\nu \in G_i$ that is conjugate to ξ^{-1}, since $\eta^{-1}\zeta = \eta^{-1}\xi^{-1}\eta$. If the further reduced word $V_2 = X_1\xi X_1^{-1}\nu$ is fully cyclically reduced, then we are done. On the other hand, the only way V_2 is not fully cyclically reduced is if the last letter of X_1 is in G_i. If this is true, say $X_1 = X_2\epsilon$ for $\epsilon \in G_1$, we require that X_2 be nontrivial, since otherwise X_1 would begin with a letter in G_i, which contradicts that X is fully reduced. Thus, we have that $V_2 = X_2\epsilon\xi\epsilon^{-1}X_2^{-1}\nu$. Then, $\epsilon\xi\epsilon^{-1}$ is conjugate to ξ, and thus conjugate to ν^{-1}, so $\epsilon\xi\epsilon^{-1}$ reduces to a single-letter element of G_i that is conjugate to ν^{-1}, which yields a commutator of one of the desired forms.

Subcase 3. We have $V_1 = \xi Y_1\eta^{-1}Y_1^{-1}\zeta$, which is conjugate to $Y_1\eta^{-1}Y_1^{-1}\nu$ for $\nu = \zeta\xi = \xi^{-1}\eta\xi$. Thus, the argument in Subcase 2 can be immediately applied to this subcase to obtain the same conclusion.

Subcase 4. We have $V_1 = X_1\xi Y_1X_1^{-1}\eta^{-1}Y_1^{-1}\zeta$. If this is fully cyclically reduced, then we are done, so suppose not. We already have that the first letters of X_1 and Y_1 are in different free factors than G_i, so one of the following four must be true about the last letters of X_1 and Y_1: Subcase 4.a, they are both in G_i; Subcase 4.b, they are both in G_j for $j \neq i$; Subcase 4.c, the last letter of X_1 is in G_i while the last letter of Y_1 is in G_j for $j \neq i$; and Subcase 4.d, the last letter of Y_1 is in G_i while the last letter of X_1 is in G_j for $j \neq i$. We go through each of these subcases.

Subcase 4.a. Let $X_1 = X_2\nu$ and $Y_1 = Y_2\epsilon$ for $\nu, \epsilon \in G_i$. Since the first letters of X_1 and Y_1 must be in a free factor different from G_i, it follows that X_2 and Y_2 are nontrivial. We have $V_1 = X_2\epsilon\xi Y_2\nu\epsilon^{-1}X_2^{-1}\eta^{-1}\nu^{-1}Y_2^{-1}\zeta$. Note that $\zeta(\eta^{-1}\nu^{-1})(\nu\epsilon^{-1})(\epsilon\xi) = \zeta\eta^{-1}\xi = 1$, so by reducing $\epsilon\xi, \nu\epsilon^{-1}$, and $\eta^{-1}\nu^{-1}$ each to single-letter elements, we reduce V_1 to a commutator of one of the desired forms.

Subcase 4.b. Let $X_1 = X_2\nu$ and $Y_1 = Y_2\epsilon$ for $\nu, \epsilon \in G_j$. If $\nu = \epsilon$, then V_1 is conjugate to

$$\eta X_2 \epsilon \xi Y_2 X_2^{-1} \eta^{-1} \epsilon^{-1} Y_2^{-1} \xi^{-1} = (\eta X_2)\epsilon \xi Y_2 (\eta X_2)^{-1} \epsilon^{-1} (\xi Y_2^{-1})^{-1},$$

which contradicts our assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. Thus, $\nu\epsilon^{-1} = \mu \in G_j$, and we have that

$$V_1 = X_2 \epsilon Z \xi Y_2 \mu X_2^{-1} \eta^{-1} Z^{-1} \nu^{-1} Y_2^{-1} \zeta$$

for $Z = 1$. This commutator is in one of our desired forms.

Subcase 4.c. Let $X_1 = X_2\nu$ for $\nu \in G_i$. If ν and ξ are inverses, then V_1 is conjugate to

$$\eta X_2 Y_1 \xi X_2^{-1} \eta^{-1} Y_1^{-1} \xi^{-1} = (\eta X_2) Y_1 \xi (\eta X_2)^{-1} Y_1^{-1} \xi^{-1},$$

which contradicts our assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. Thus, $\nu\xi = \mu \in G_i$, and we have that

$$V_1 = X_2 \mu Y_1 \nu^{-1} X_2^{-1} \eta^{-1} Y_1^{-1} \zeta.$$

Since $\zeta\eta^{-1}\nu^{-1}\mu = \zeta\eta^{-1}\nu^{-1}\nu\xi = 1$, this commutator is in one of our desired forms.

Subcase 4.d. Let $Y_1 = Y_2\nu$ for $\nu \in G_i$. If ν and η are inverses, then V_1 is conjugate to

$$\eta X_1 \xi Y_2 \eta^{-1} X_1^{-1} Y_2^{-1} \xi^{-1} = \eta X_1 (\xi Y_2) \eta^{-1} X_1^{-1} (\xi Y_2)^{-1},$$

which contradicts our assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. Thus, $\nu\eta = \mu \in G_i$, and we have that

$$V_1 = X_1 \xi Y_2 \nu X_2^{-1} \mu^{-1} Y_2^{-1} \zeta.$$

Since $\zeta\mu^{-1}\nu\xi = \zeta\eta^{-1}\nu^{-1}\nu\xi = 1$, this commutator is in one of our desired forms. This concludes our proof in Case 1.

Case 2. We assumed that $V = XYZX^{-1}Y^{-1}Z^{-1}$ is not fully cyclically reduced. By conjugation, we can suppose that the first letter of X and the first letter of Z are in the same free factor, say $X = \eta X_1$ and $Z = \xi Z_1$. Let $\zeta = \xi^{-1}\eta \in G_i$, which cannot be trivial; if it were, then $V = X_1(Y\xi)Z_1X_1^{-1}(Y\xi)^{-1}Z_1^{-1}$, which contradicts our assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. We then have that V is conjugate to

$$V_1 = X_1Y\xi Z_1X_1^{-1}\eta^{-1}Y^{-1}Z_1^{-1}\zeta. \tag{3.1}$$

If V_1 is fully cyclically reduced, then we are done. Consequently, suppose not. First, suppose for the sake of a contradiction that the last letter of Y is in G_i, say $Y = Y_1\nu$ for $\nu \in G_i$. Then,

$$V_1 = X_1Y_1\nu\xi Z_1X_1^{-1}\eta^{-1}\nu^{-1}Y^{-1}Z_1^{-1}\zeta = X_1(Y_1\mu)(\zeta Z_1)X_1^{-1}(Y_1\mu)^{-1}(\zeta Z_1)^{-1}$$

for $\mu = \nu\eta$. We have used that $\mu\zeta^{-1} = \nu\eta\eta^{-1}\xi = \nu\xi$. This contradicts our assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. Thus, the last letter of Y must be in a free factor different from G_i. In light of this, it follows from our assumption that V_1 is not fully cyclically reduced that one of four subcases must hold: Subcase 1, that both X_1 and Z_1 are trivial; Subcase 2, that only X_1 is trivial; Subcase 3, that only Z_1 is trivial; and Subcase 4, that both X_1 and Z_1 are nontrivial.

Subcase 1. We have $V_1 = Y\xi\eta^{-1}Y^{-1}\zeta$, where $\xi\eta^{-1}$ is a conjugate of $\zeta^{-1} = \eta^{-1}\xi$. Thus, reducing $\xi\eta^{-1}$ to a single-letter element of G_i, we obtain one of our desired commutator forms.

Subcase 2. We have that $V_1 = Y\xi Z_1\eta^{-1}Y^{-1}Z_1^{-1}\zeta$ is conjugate to $V_2 = Z_1\eta^{-1}Y^{-1}Z_1^{-1}\zeta Y\xi$. Since $(\eta^{-1})^{-1}\zeta^{-1} = \eta\eta^{-1}\xi = \xi$, this subcase is equivalent to Case 1 Subcase 4.

Subcase 3. We have that $V_1 = X_1Y\xi X_1^{-1}\eta^{-1}Y^{-1}\zeta$ is conjugate to $V_2 = Y^{-1}\zeta X_1Y\xi X_1^{-1}\eta^{-1}$. Since $\zeta^{-1}\xi^{-1} = \eta^{-1}\xi\xi^{-1} = \eta^{-1}$, this subcase is also equivalent to Case 1 Subcase 4.

Subcase 4. Since (3.1) is not fully cyclically reduced, one of the following must be true: the last letter of X_1 and the first letter of Y are in the same free factor, the last letter of Z_1 and the last letter of X_1 are in the same free factor, or the first letter of Y and the last letter of Z_1 are in the same factor. Given this, we consider the following four subcases: Subcase

4.a, that the first letter of Y, the last letter of X_1, and the last letter of Z_1 are all in the same factor G_j; Subcase 4.b, that the first letter of Y and the last letter of X_1, but not the last letter of Z_1, are in the same factor G_j; Subcase 4.c, that the first letter of Y and the last letter of Z_1, but not the last letter of X_1, are in the same factor G_j; and Subcase 4.d, the last letters of X_1 and Z_1, but not the first letter of Y, are in the same factor G_j.

Subcase 4.a. Let $Y = \epsilon Y_1$, $X_1 = X_2\nu$, and $Z_1 = Z_2\mu$ for $\epsilon, \nu, \mu \in G_j$. Then, we have

$$V_1 = X_2\nu\epsilon Y_1\xi Z_2\mu\nu^{-1}X_2^{-1}\eta^{-1}Y_1^{-1}\epsilon^{-1}\mu^{-1}Z_2^{-1}\zeta.$$

Note that $\nu\epsilon, \mu\nu^{-1}$, and $\epsilon^{-1}\mu^{-1}$ each reduce to a single-letter element of G_j, say $\alpha_1 = \nu\epsilon$, $\alpha_2 = \mu\nu^{-1}$, and $\alpha_3 = \epsilon^{-1}\mu^{-1}$. Indeed, none of these three can be trivial. For instance, suppose that $\nu\epsilon = 1$. Then, $\alpha_2 = \alpha_3^{-1}$, which means that

$$V_1 = X_2Y_1\xi Z_2\alpha_2X_2^{-1}\eta^{-1}Y_1^{-1}\alpha_2^{-1}Z_2^{-1}\zeta$$

is conjugate to

$$V_2 = \eta X_2Y_1\xi Z_2\alpha_2X_2^{-1}\eta^{-1}Y_1^{-1}\alpha_2^{-1}Z_2^{-1}\xi^{-1} = (\eta X_2)Y_1(\xi Z_2\alpha_2)(\eta X_2)^{-1}Y_1^{-1}(\xi Z_2\alpha_2)^{-1},$$

which contradicts our assumption that $V = XYZX^{-1}Y^{-1}Z^{-1}$ was taken to have minimum length. Analogous arguments show that α_2 and α_3 are also nontrivial. If $i \neq j$, then the further reduced expression for V_1, given by

$$X_2\alpha_1Y_1\xi Z_2\alpha_2X_2^{-1}\eta^{-1}Y_1^{-1}\alpha_3Z_2^{-1}\zeta,$$

is fully cyclically reduced. Even if $j = i$, this expression must be fully cyclically reduced; this is because Y_1, X_2, and Z_2 must be nontrivial, since the first letters of X_1 and Z_1 and the last letter of Y_1 must not be in G_i. Since $\zeta\eta^{-1}\xi = 1$ and $\alpha_3\alpha_2\alpha_1 = 1$, we have obtained one of our desired commutator forms.

Subcase 4.b. Let $Y = \epsilon Y_1$ and $X_1 = X_2\nu$ for $\epsilon, \nu \in G_j$. Then, we have

$$V_1 = X_2\nu\epsilon Y_1\xi Z_1\nu^{-1}X_2^{-1}\eta^{-1}Y_1^{-1}\epsilon^{-1}Z_1^{-1}\zeta.$$

By the argument used in Case 2 Subcase 4.a, $\nu\epsilon$ reduces to a (nontrivial) single-letter element of G_j, say $\alpha \in G_j$. If $i \neq j$, then the further reduced expression for V_1, given by

$$X_2\alpha Y_1\xi Z_1\nu^{-1}X_2^{-1}\eta^{-1}Y_1^{-1}\epsilon^{-1}Z_1^{-1}\zeta,$$

is fully cyclically reduced. Even if $j = i$, this expression must be fully cyclically reduced; this is because Y_1 and X_2 must be nontrivial, since the first letter of X_1 and the last letter of Y_1 must not be in G_i. Since $\zeta\eta^{-1}\xi = 1$ and $\epsilon^{-1}\nu^{-1}\alpha = 1$, we have obtained one of our desired commutator forms.

Subcase 4.c. Let $Y = \epsilon Y_1$ and $Z_1 = Z_2\mu$ for $\epsilon, \mu \in G_j$. Then, we have

$$V_1 = X_2\epsilon Y_1\xi Z_2\mu X_2^{-1}\eta^{-1}Y_1^{-1}\epsilon^{-1}\mu^{-1}Z_2^{-1}\zeta.$$

By the argument used in Case 2 Subcase 4.a, $\epsilon^{-1}\mu^{-1}$ reduces to a (nontrivial) single-letter element of G_j, say $\alpha \in G_j$. If $i \neq j$, then the further reduced expression for V_1, given by

$$X_2\epsilon Y_1\xi Z_2\mu X_2^{-1}\eta^{-1}Y_1^{-1}\alpha Z_2^{-1}\zeta$$

is fully cyclically reduced. Even if $j = i$, this expression must be fully cyclically reduced; this is because Y_1 and Z_2 must be nontrivial, since the first letter of Z_1 and the last letter of Y_1 must not be in G_i. Since $\zeta\eta^{-1}\xi = 1$ and $\alpha\mu\epsilon = 1$, we have obtained one of our desired commutator forms.

Subcase 4.d. Let $X_1 = X_2\nu$ and $Z_1 = Z_2\mu$ for $\nu, \mu \in G_j$. Then, we have

$$V_1 = X_2\nu Y_1\xi Z_2\mu\nu^{-1}X_2^{-1}\eta^{-1}Y_1^{-1}\mu^{-1}Z_2^{-1}\zeta.$$

By the argument used in Case 2 Subcase 4.a, $\mu\nu^{-1}$ reduces to a (nontrivial) single-letter element of G_j, say $\alpha \in G_j$. If $i \neq j$, then the further reduced expression for V_1, given by

$$X_2 \nu Y_1 \xi Z_2 \alpha X_2^{-1} \eta^{-1} Y_1^{-1} \mu^{-1} Z_2^{-1} \zeta$$

is fully cyclically reduced. Even if $j = i$, this expression must be fully cyclically reduced; this is because X_2 and X_2 must be nontrivial, since the first letter of X_1 and the last letter of Y_1 must not be in G_i. Since $\zeta \eta^{-1} \xi = 1$ and $\mu^{-1} \alpha \nu = 1$, we have obtained one of our desired commutator forms.

3.2 Proof of Theorem 1.4

By Wicks' theorem for free products, we need to count cyclic conjugacy classes of Wicks commutators of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. As discussed before, a Wicks commutator of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ must, when going from left to right, alternate between letters of the $\mathbb{Z}/3\mathbb{Z}$ factor, r and r^{-1}, and the letter of the $\mathbb{Z}/2\mathbb{Z}$ factor, s. Thus, the occurrences of s provide no information when writing our word in terms of the generators in $\mathfrak{S}$, so from this point, we abuse notation by omitting all occurrences of s and writing all words and subwords in terms of only r and r^{-1}. For example, the element $srsr^{-1}$ would be written as rr^{-1}.

Consider a Wicks commutator W of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ having length k, where k is a multiple of 4. Let $X = k/4$, so that the left-half subword of W contains X letters of the $\mathbb{Z}/3\mathbb{Z}$ factor and X letters of the $\mathbb{Z}/2\mathbb{Z}$ factor, which are placed in an alternating way. As seen from our work in Section 3.1, W can either be of the fully cyclically reduced form $ABA^{-1}B^{-1}$ or the fully cyclically reduced form $A\alpha B\beta C\alpha A^{-1}\beta B^{-1}\alpha C^{-1}\beta$, where $\alpha, \beta \in \{r, r^{-1}\}$ and A, B, and C are nontrivial. However, by using the arguments of Section 2.2, we see that the number of the former is $O(X \cdot 2^X)$, while the number of the latter is

$$4 \cdot \frac{(X-5)(X-4)}{2} \cdot 2^{X-3},$$

since we have four choices of $(d, e) \in \{r, r^{-1}\}^2$, $(X-5)(X-4)/2$ partitions of $X-3$ into three nontrivial parts giving the lengths of A, B, and C, and $X-3$ degrees of freedom for choosing the letters of A, B, and C, with no cancellation between the extremal letters of A,

B, and C (the key difference between counting commutators of $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ and counting those of a free group). Thus, the number of Wicks commutators of the form $ABA^{-1}B^{-1}$ is negligible.

Next, we need to count the number of conjugacy classes containing at least one Wicks commutator of the form $A\alpha B\beta C\alpha A^{-1}\beta B^{-1}\alpha C^{-1}\beta$. As before, let $\mathcal{C}$ be the conjugacy class of the Wicks commutator $W := A\alpha B\beta C\alpha A^{-1}\beta B^{-1}\alpha C^{-1}\beta$, with $|A| = n_1$, $B = n_2$, and $C = n_3$. We wish to show that on average, $\mathcal{C}$ does not contain Wicks commutators other than the six obvious ones: W, $B\beta C\alpha A^{-1}\beta B^{-1}\alpha C^{-1}\beta A\alpha$, $C\alpha A^{-1}\beta B^{-1}\alpha C^{-1}\beta A\alpha B\beta$, $A^{-1}\beta B^{-1}\alpha C^{-1}\beta A\alpha B\beta C\alpha$, $B^{-1}\alpha C^{-1}\beta A\alpha B\beta C\alpha A^{-1}\beta$, and $C^{-1}\beta A\alpha B\beta C\alpha A^{-1}\beta B^{-1}\alpha$. Suppose the number of letters of the conjugation is $\ell \leq n_3/2$, and accordingly decompose $C = DEF$ without cancellation so that $|D| = |F| = \ell$. Label the letters of W by $A = a_1 \cdots a_{n_1}$, $B = b_1 \cdots b_{n_2}$, $D = d_1 \cdots d_\ell$, $E = e_1 \cdots e_{n_3-2\ell}$, and $F = f_1 \cdots f_\ell$. Consider the cyclic conjugate $W' := D^{-1}\beta A\alpha B\beta DEF\alpha A^{-1}\beta B^{-1}\alpha F^{-1}E^{-1}$ of W. We wish to show that on average, W' is not a Wicks commutator. Suppose the contrary, i.e., that there exists a partition $p' = (m_1, m_2, m_3)$ of $X - 3$ into three parts such that

$$W' = D^{-1}\beta A\alpha B\beta DEF\alpha A^{-1}\beta B^{-1}\alpha F^{-1}E^{-1} = w_1\alpha' w_2\beta' w_3\alpha' w_1^{-1}\beta' w_2^{-1}\alpha' w_3^{-1}\beta' \quad (3.2)$$

for subwords w_1, w_2, and w_3 of lengths m_1, m_2, and m_3, and $\alpha', \beta' \in \{r, r^{-1}\}$.

As before, label the letters of A as $a_1, \ldots, a_{n_1}$, and label the letters of B, C, D, E, and F similarly. Also, label the three incidences of α from left to right as α_1, α_2, and α_3, and similarly for β, α', and β'. We have that w_1, w_2, and w_3 are subwords comprised of the letters

$$d_\ell^{-1}, \ldots, d_1^{-1}, \beta_3, a_1, \ldots, a_{n_1}, \alpha_1, b_1, \ldots, b_{n_2}, \beta_1, d_1, \ldots, d_\ell, e_1, \ldots, e_{n_3-2\ell},$$

and we accordingly consider the subwords w_1^{-1}, w_2^{-1}, and w_3^{-1} as comprised of the inverses of these letters. Then, note that the second half of W' can be considered in two forms:

$$F\alpha_2 A^{-1}\beta_3 B^{-1}\alpha_3 F^{-1}E^{-1} = w_1^{-1}\beta_2' w_2^{-1}\alpha_3' w_3^{-1}\beta_3'.$$

Equivalently, this equality can be written as

$$EF\alpha_3^{-1}B\beta_3^{-1}A\alpha_2^{-1}F^{-1} = \beta_3'^{-1}w_3\alpha_3'^{-1}w_2\beta_2'^{-1}w_1.$$

Consider the function g mapping the ordered set of symbols of the left-hand side,

$$\mathcal{A} := \{e_1, \ldots, e_{n_3-2\ell}, f_1, \ldots, f_\ell, \alpha_3^{-1}, b_1, \ldots, b_{n_2}, \beta_3^{-1}, a_1, \ldots, a_{n_1}, \alpha_2^{-1}, f_\ell^{-1}, \ldots, f_1\}$$

to the set $\mathcal{B}$ of symbols of the right-hand side, which are given by replacing the (m_1+1)th, (m_1+m_2+2)th, and $(m_1+m_2+m_3+3)$th letters of (3.2) (note that the $(m_1+m_2+m_3+3)$th letter is always $e_{n_3-2\ell}$) with $\beta_2'^{-1}, \alpha_3'^{-1}$, and $\beta_3'^{-1}$. Specifically, g maps the ith leftmost letter of the left-hand side of (3.2) to the ith leftmost letter of the right-hand side.

First, suppose g has no fixed points ($\mathfrak{i}$ such that $g(\mathfrak{i}) = \mathfrak{i}$). Then, use an algorithm similar to the one used in Section 2.2 to conclude that there are $\leq X/2$ degrees of freedom for $ABDEF$, so W must be one of only $O(2^{X/2})$ choices (for each choice of ℓ and p').

Now, suppose that there exists an $\mathfrak{i}$ such that $g(\mathfrak{i}) = \mathfrak{i}$. Such fixed points $\mathfrak{i}$ must be letters of A, B, or E. We first consider the case that all the fixed points are letters of only one of A, B, and E. In this case, we consider the following subcases for W, p, and p':

Case 1. Suppose that the fixed points are letters of E. Then, all of the fixed points must be in one of w_2 and w_3; they cannot be in w_1 since this would mean that w_1 contains e_1, but e_1 is necessarily located at different positions in the left-hand side and right-hand side of (3.2). If all the fixed points are in w_2, then we require that $2+m_3 = n_3-2\ell-(m_2+m_3+1)$ in order for the first letter of w_2 to be at the same position in both the left-hand and right-hand side. Hence, we have $m_2+2m_3 = n_3-2\ell-3$, which means there are $\leq (n_3-2\ell-3)/2$ choices for p' parametrized by $m_3 \leq (n_3-2\ell-3)/2$. For each such choice of p', there are $n_3-2\ell-(2+m_3+m_3) = n_3-2\ell-2m_3-2$ fixed letters, from e_{m_3+3} to $e_{n_3-2\ell-m_3}$, and $(X-(n_3-2\ell-2m_3-2))/2$ non-fixed letters. Thus, counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor}\sum_{m_3=0}^{\left\lfloor\frac{n_3-2\ell-3}{2}\right\rfloor} 2^{\frac{X+n_3-2\ell-2m_3-2}{2}} \ll 2^X,$$

which is dominated by our error term.

Next, suppose the fixed letters are in w_3. Then, it is necessary that $\beta_3'^{-1} = e_1$ and $w_3 = e_2 \cdots e_{n_3-2\ell-1}$. Thus, we have that $m_3 = n_3 - 2\ell - 2$, so the number of possible choices for p' is at most the number of partitions of $X - 1 - n_3 + 2\ell$ into two nontrivial parts, which is $X - 1 - n_3 + 2\ell$. For each choice of p', the non-fixed letters have $\leq (X - n_3 + 2\ell + 1)/2$ degrees of freedom, along with the $n_3 - 2\ell - 1$ degrees of freedom from the letters $e_2, \ldots, e_{n_3-2\ell}$. Counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\begin{aligned}
&\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor} (X-1-n_3+2\ell)\cdot 2^{n_3-2\ell-1+\frac{X-n_3+2\ell+1}{2}} \\
&= \sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor} (n_1+n_2+2\ell+2)\cdot 2^{\frac{2X-n_1-n_2-2\ell-4}{2}} \ll 2^X,
\end{aligned}$$

which is dominated by our error term.

Case 2. Suppose that the fixed points are letters of B. Then, all of the fixed points must be in one of w_1, w_2, and w_3. First, suppose they are in w_1. This requires that $w_1 = D^{-1}\beta_3 A\alpha_1 BV$, where V is the left subword of $\beta_1 DE$ having length $n_1 + 2 + \ell$ (the length of $A\alpha_2^{-1}F^{-1}$). All letters of B are thus included in w_1. We have $m_1 = \ell + 1 + n_1 + 1 + n_2 + (n_1 + 2 + \ell) = 2n_1 + n_2 + 2\ell + 4$, so the number of possible choices for p' is at most the number of partitions of $X - 3 - 2n_1 - n_2 - 2\ell - 4$ into two nontrivial parts, which is $X - 2n_1 - n_2 - 2\ell - 7 \leq X - 3 - n_1 - n_2 - 2\ell$ (the latter is guaranteed to be nonnegative for any choice of p). For each choice of p', the non-fixed letters have $\leq (X - n_2)/2$ degrees of freedom, along with the n_2 degrees of freedom from the letters of B. Counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor}(X-3-n_1-n_2-2\ell)\cdot 2^{\frac{X+n_2}{2}} \ll 2^X,$$

which is dominated by our error term.

Next, suppose that the fixed points are in w_2. Then, we require that the difference between the lengths of $EF\alpha_3^{-1}$ (length $n_3-\ell+1$) and $\beta_3^{-1}A\alpha_2^{-1}F^{-1}$ (length $n_1+\ell+2$) is the same as that between $\beta_3'^{-1}w_3\alpha_3'^{-1}$ (length m_3+2) and $\beta_2'^{-1}w_1$ (length m_1+1). Furthermore, the number of letters of B in w_2 is n_2 if $j = n_1+\ell+2-(m_1+1) = n_3-\ell+1-(m_3+2)$ is negative and n_2-j if $j \geq 0$. First, suppose that $j \geq 0$. In this case, p' is determined by the choice of $j \leq n_2/2$, for which there are n_2-2j fixed letters of B. The non-fixed letters have $\leq (X-n_2+2j)/2$ degrees of freedom, so overall, we can count across all choices of values for the letters, p, j, and ℓ to get that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\begin{aligned}
&\sum_{n_1=0}^{X-3}\sum_{n_3=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{n_3}{2}\right\rfloor}\sum_{j=0}^{\left\lfloor\frac{X-3-n_1-n_3}{2}\right\rfloor}2^{\frac{X+n_2-2j}{2}}\\
&\leq \sum_{n_1=0}^{X-3}\sum_{n_3=0}^{X-3-n_1}\frac{n_3}{2}\sum_{j=0}^{\left\lfloor\frac{X-3-n_1-n_3}{2}\right\rfloor}2^{\frac{X+n_2-2j}{2}} \ll 2^X,
\end{aligned}$$

which is dominated by our error term.

Now, suppose that $j < 0$. In this case, $-j = n_1-m_1+\ell+1 = n_3-m_3-\ell-1$ is a positive integer less than or equal to $\min(n_1+\ell+1, n_3-\ell-1) \leq X-n_2$, and p' is determined by the choice of $-j$, for which there are n_2 fixed letters of B. The non-fixed letters have $\leq (X-n_2)/2$ degrees of freedom, so overall, we can count across all choices of values for the letters, p, $-j$, and ℓ to get that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor}(X-n_2)\cdot 2^{\frac{X+n_2}{2}} \ll 2^X$$

Finally, suppose that the fixed points are in w_3. This requires that $w_3 = VB\beta_1 De_1 \cdots e_{n_3-2\ell-1}$, where V is the right subword of $D^{-1}\beta_3 A\alpha_1$ having length $n_3-2\ell+\ell+1-1 = n_3-\ell$. All letters of B are thus included in w_3. We have $m_3 = n_3-\ell+n_2+1+\ell+n_3-2\ell-1 = n_2+2n_3-2\ell$, so the number of possible choices for p' is at most the number of partitions of $X-3-n_2-2n_3+2\ell$ into two nontrivial parts, which is $X-3-n_2-2n_3+2\ell \leq X-3-n_2+2\ell$ (the latter is guaranteed to be nonnegative for any choice of p). For each choice of p', the non-fixed letters have $\leq (X-n_2)/2$ degrees of freedom, along with the n_2 degrees of freedom from the letters of B. Counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor}(X-3-n_2+2\ell)\cdot 2^{\frac{X+n_2}{2}} \ll 2^X,$$

which is dominated by our error term.

Case 3. Suppose that the fixed points are letters of A. Then, all of the fixed points must be in one of w_1 and w_2; they cannot be in w_3, since then there must be more than $\ell+1$ letters right of A. First, suppose they are in w_1. This requires that $w_1 = D^{-1}\beta_3^{-1}AV$, where V is the left subword of $\alpha_1^{-1}B\beta_1^{-1}DE$ having length $\ell+1$. All letters of A are thus included in w_1. The number of possible choices for p' is at most the number of partitions of $X-3-m_1 = X-3-(\ell+1+n_1+\ell+1) = X-5-2\ell-n_1$ into two nontrivial parts, which is $X-5-2\ell-n_1 \leq X-3-2\ell-n_1$ (the latter is guaranteed to be nonnegative for any choice of p). For each choice of p', the non-fixed letters have $\leq (X-n_1)/2$ degrees of freedom, along with the n_1 degrees of freedom from the letters of A. Counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor}(X-3-2\ell-n_1)\cdot 2^{\frac{X+n_1}{2}} \ll 2^X,$$

which is dominated by our error term.

Finally, suppose the fixed points are in w_2. This requires that w_2 is the word between the (m_1+2)th letter and the $(n_1+2\ell+1-m_1)$th letter, so that the letters of A will be in matching positions. Thus, we have $m_2 = n_1+2\ell-2m_1-2$. Note then that p' is parametrized by $m_1 \le (n_1+2\ell-2)/2$. For each choice of p', we have n_1 fixed letters (and $(X+n_1)/2 \le (X+n_1-m_1+\ell)/2$ overall degrees of freedom) if $m_1 \le \ell$, and $n_1-(m_1-\ell)$ fixed letters (and $(X+n_1-m_1+\ell)/2$ overall degrees of freedom) if $m_1 > \ell$. Thus, counting across all choices of values for the letters, p, p', and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor}\sum_{m_1=0}^{\left\lfloor\frac{n_1+2\ell-2}{2}\right\rfloor} 2^{\frac{X+n_1+\ell-m_1}{2}} \ll 2^X,$$

which is dominated by our error term.

Next, we suppose that the fixed letters of g are in two of the three subwords A, B, and E. Consider the following subcases:

Case 1. Suppose the fixed letters of g are in A and B. It is necessary that the fixed letters of A and those of B are in w_i and w_j, respectively, such that $i<j$; otherwise, the fixed letters of A would come before the fixed letters of B, a contradiction. First, suppose that the fixed letters of B are in w_2, which implies that the fixed letters of A are in w_1. Then, we require that $w_1 = D^{-1}\beta_3^{-1}AV$, where V is the left subword of $\alpha_1 B\beta_1 DE$ having length $\ell+1$. Furthermore, since we have fixed letters of B, we require that V does not include all of B, i.e., $n_2>\ell$. Next, for the fixed letters of B to match in position, we require that w_2 ends at the letter $b_{n_2-\ell}$, which gives us $m_2 = n_2-\ell-\ell-1-1 = n_2-2\ell-2>0$. It follows that w_3 is the subword of $b_{n_2-\ell+1}\cdots b_{n_2}\beta_1 DE$ omitting the leftmost letter. In particular, m_3 is automatically determined, and for this p' corresponding to p, we have n_1 fixed letters of A and $n_2-2\ell-2$ fixed letters of B. Next, we upper-bound the degrees of freedom of the non-fixed letters. Note that $EF\alpha_3^{-1}b_1\cdots b_\ell = \beta_3'^{-1}b_{n_2-\ell+2}\cdots b_{n_2}\beta_1 DE$, but g maps $f_\ell^{-1},\ldots,f_1^{-1}$ to $b_1,\ldots,b_\ell$ and $b_{n_2-\ell+1},\ldots,b_{n_2}$, to $d_\ell^{-1},\ldots,d_1^{-1}$. Thus, arguing inductively by translation, we see that that choosing the letters of F determines the letters of E, and thus also determines those of D, thereby determining all non-fixed letters (while not caring about the constant number of α and β letters). Counting across all choices of values for the letters, p, and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor} 2^{n_1+n_2-2\ell-2+\ell} \ll X\cdot 2^X,$$

which is dominated by our error term.

Next, suppose that the fixed letters of B are in w_3. Then, we require that $w_3 = VB\beta_1 DE$, where V is the right subword of $D^{-1}\beta_3 A\alpha_1$ having length $n_2-\ell$. Furthermore, since we have fixed letters of A, we require that V does not include all of A, i.e., $n_1 > n_2-\ell-1$. Next, for the fixed letters of A to match in position, we require that they are in w_2, and specifically that $w_2 = a_{n_3-\ell+1}\cdots a_{n_1-n_3+\ell}$. This gives us $m_2 = n_1-2n_3+2\ell-2>0$, and it follows that w_1 is the subword of $D^{-1}\beta_3 a_1\cdots a_{n_3-\ell}$ omitting the rightmost letter. In particular, m_1 is automatically determined, and for this p' corresponding to p, we have n_2 fixed letters of B and $n_1-2n_3+2\ell-2$ fixed letters of A. Next, we upper-bound the degrees of freedom of the non-fixed letters. Note that $a_{n_1-n_3+\ell+2}\cdots a_{n_1}\alpha_2^{-1}F^{-1} = D^{-1}\beta_3 a_1\cdots a_{n_3-\ell-1}$, but g maps $d_1,\dots,d_\ell,e_1,\dots,e_{n_3-2\ell}$ to $a_1,\dots,a_{n_3-\ell}$ and $a_{n_1-n_3+\ell+1}\cdots a_{n_1}$, to $e_1,\dots,e_{n_3-2\ell},f_1,\dots,f_\ell$. Thus, arguing inductively by translation, we see that that choosing the letters of F determines the letters of E, and thus also determines those of D, thereby determining all non-fixed letters (while not caring about the constant number of α and β letters). Counting across all choices of values for the letters, p, and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3}\sum_{n_2=0}^{X-3-n_1}\sum_{\ell=0}^{\left\lfloor\frac{X-3-n_1-n_2}{2}\right\rfloor} 2^{n_2+(n_1-2n_3+2\ell-2)+\ell} \ll X\cdot 2^X,$$

which is dominated by our error term.

Case 2. Suppose the fixed letters of g are in B and E. Similarly to before, it is necessary that the fixed letters of B and those of E are in w_i and w_j, respectively, such that $i < j$. First, suppose that the fixed letters of B are in w_1. Then, we require that $w_1 = D^{-1}\beta_3 A\alpha_1 BV$, where V is the left subword of $\beta_1 DE$ having length $2+n_1+\ell$. Then, w_2 must start with e_{n_1+3}, which means in order to have the letters of E match, we must have $m_3+2 = n_1+2$. Since $m_2+m_3+2+n_1+\ell = n_3-\ell$, there are $m_2 = n_3-2n_1-2\ell-2 > 0$ fixed letters of E in w_2, and n_2 fixed letters of B. Next, we upper-bound the degrees of freedom of the non-fixed letters. Note that $A\alpha_2^{-1}F^{-1} = De_1 \cdots e_{n_1+1}$ and $e_{n_3-n_1-2\ell} \cdots e_{n_3-2\ell}F = D^{-1}\beta_3 A$. However, we also have $e_1 \cdots e_{n_1+1} = \beta_3'^{-1} e_{n_3-n_1-2\ell} \cdots e_{n_3-2\ell-1}$, which overall gives us that $A\alpha_2^{-1}F^{-1}e_{n_3-2\ell}F = D\beta_3'^{-1}D^{-1}\beta_3 A$. Thus, arguing inductively by translation, we see that that choosing the letters of F determines the letters of A, and thus also determines those of D, thereby determining all non-fixed letters (while not caring about the constant number of α and β letters, including $e_{n_3-2\ell} = b_3'$). Counting across all choices of values for the letters, p, and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3} \sum_{n_2=0}^{X-3-n_1} \sum_{\ell=0}^{\left\lfloor \frac{X-3-n_1-n_2}{2} \right\rfloor} 2^{n_2+(n_3-2n_1-2\ell-2)+\ell} \ll X \cdot 2^X,$$

which is dominated by our error term.

Next, suppose that the fixed letters of B are in w_2, which implies the fixed letters of E are in w_3. Then, we require that $w_3 = e_2 \cdots e_{n_3-2\ell-1}$. Furthermore, in order for the letters of B to match in position, we must have that $w_2 = V\alpha_1 B\beta_1 D$, where V is the right subword of $D^{-1}\beta_3 A$ having length ℓ. We thus have $n_3-2\ell-2$ fixed letters in E and n_2 fixed letters in B. Now, we upper-bound the degrees of freedom of the non-fixed letters. First, suppose that $n_1 > \ell$. Note then that $F = a_{n_1-\ell+1} \cdots a_{n_1}$ and $A\alpha_2^{-1}F^{-1} = D\beta_2'^{-1}D^{-1}\beta_3 a_1 \cdots a_{n_1-\ell-1}$. Thus, we have $a_1 \cdots a_{n_1-\ell-1}a_{n_1-\ell}F\alpha_2^{-1}F^{-1} = D\beta_2'^{-1}D^{-1}\beta_3 a_1 \cdots a_{n_1-\ell-1}$. Thus, arguing inductively by translation, we see that that choosing the letters of F determines the letters of $a_1 \cdots a_{n_1-\ell-1}$, and thus also determines those of the rest of A and of D, thereby determining all non-fixed letters (while not caring about the constant number of α and β letters). In the other case of $n_1 \leq \ell$, the notation above for $a_1 \cdots a_{n_1-\ell-1}$ becomes inviable, but nevertheless we can use a similar argument as above to conclude that F determines all the non-fixed letters. Counting across all choices of values for the letters, p, and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3} \sum_{n_2=0}^{X-3-n_1} \sum_{\ell=0}^{\left\lfloor \frac{X-3-n_1-n_2}{2} \right\rfloor} 2^{n_2+(n_3-2\ell-2)+\ell} \ll X \cdot 2^X,$$

which is dominated by our error term.

Case 3. Finally, suppose the fixed letters of g are in A and E. Similarly to before, it is necessary that the fixed letters of A and those of E are in w_i and w_j, respectively, such that $i < j$. First, suppose that the fixed letters of E are in w_3. Then, we require that $w_3 = e_2 \cdots e_{n_3-2\ell-1}$. Furthermore, in order for the letters of A to match in position, we need that the fixed letters of A are contained in w_1, and in particular, that $w_1 = D^{-1}\beta_3 A\alpha_1 V$, where V is the left subword of $B\beta_1 DE$ having length ℓ. We thus have $n_3 - 2\ell - 2$ fixed letters in E and n_1 fixed letters in A. Now, we upper-bound the degrees of freedom of the non-fixed letters. First, suppose that $n_2 > \ell$. Note then that $F^{-1} = b_1 \cdots b_\ell$ and $F\alpha_3^{-1}B = \alpha_3'^{-1} b_{\ell+2} \cdots b_{n_2}\beta_1 D\beta_2'^{-1}D^{-1}$. Thus, we have $F\alpha_3^{-1}F^{-1}b_{\ell+1} \cdots b_{n_2} = \alpha_3'^{-1} b_{\ell+2} \cdots b_{n_2}\beta_1 D\beta_2'^{-1}D^{-1}$. Arguing inductively by translation, we see that that choosing the letters of F determines the letters of B of D, thereby determining all non-fixed letters. In the other case of $n_2 \leq \ell$, the notation above for $b_1 \cdots b_\ell$ becomes inviable, but nevertheless we can use a similar argument as above to conclude that F determines all the non-fixed letters. Counting across all choices of values for the letters, p, and ℓ, we have that the number of additional Wicks commutators arising from this case is upper-bounded by

$$\sum_{n_1=0}^{X-3} \sum_{n_2=0}^{X-3-n_1} \sum_{\ell=0}^{\left\lfloor \frac{X-3-n_1-n_2}{2} \right\rfloor} 2^{n_1+(n_3-2\ell-2)+\ell} \ll X \cdot 2^X,$$

which is dominated by our error term.

Next, suppose that the fixed letters of E are in w_2. Then, the fixed letters of A are contained in w_1, which requires that $w_1 = D^{-1}\beta_3 A\alpha_1 V$, where V is the left subword of $B\beta_1 DE$ having length ℓ. But then w_2 must start on a letter not in E, which makes it impossible for the letters of E to match in position.

Finally, if there are fixed letters in A, B, and C, then it is necessarily that $\ell = 0$ and $p = p'$, which does not need to be considered.

If $\ell \geq n_3/2$, then we can think of our commutator as a cyclic conjugate of $C^{-1}ABCA^{-1}B^{-1}$ such that the letters are moved from left to right. A symmetric argument like above gives us the conclusion that $W' = D^{-1}\beta A\alpha B\beta DEF\alpha A^{-1}\beta B^{-1}\alpha F^{-1}E^{-1}$ is on average not a Wicks commutator of the form $w_1\alpha' w_2\beta' w_3\alpha' w_1^{-1}\beta' w_2^{-1}\alpha' w_3^{-1}\beta'$. Note that this entire argument can then be repeated *mutatis mutandis* to show that W' is on average also not a Wicks commutator of the form $w_1 w_2 w_1^{-1} w_2^{-1}$. Indeed, the only difference from the previous case is that w_3 is taken to be trivial there are no extra letters α or β, and the latter only affects error bounds by at most a multiplicative constant.

Thus, W' is on average not a Wicks commutator, and furthermore, the $\ell = 0$ case shows that W' is on average only decomposable as a Wicks commutator in one way.We have thus shown that the number of conjugacy classes of commutators with length $4X$ is given by

$$\frac{2^X}{24}\left(X^2 + O(X)\right),$$

as needed.

3.3 Algorithm to List Commutators of $\mathrm{PSL}_2(\mathbb{Z})$ by Trace

In this section, we give an algorithm that exhaustively computes all hyperbolic (i.e., having trace greater than 2) commutators of $\mathrm{PSL}_2(\mathbb{Z})$ with a given trace. The algorithm uses a bijective correspondence between the hyperbolic conjugacy classes of $\mathrm{PSL}_2(\mathbb{Z})$ whose traces have absolute value $t > 2$ and the $\mathrm{SL}_2(\mathbb{Z})$-orbits of binary quadratic forms with discriminant $t^2 - 4$, where the action of $\mathrm{SL}_2(\mathbb{Z})$ is defined as follows: for a binary quadratic form $q(x, y)$ and $M \in \mathrm{SL}_2(\mathbb{Z})$,

$$M \cdot q(x, y) = q((x, y)M^t).$$

We now describe this correspondence, following the exposition in [11]. Let t be an integer greater than 2. Define $\mathrm{PSL}_2(\mathbb{Z})_t$ to be the set of elements in $\mathrm{PSL}_2(\mathbb{Z})$ that contain a matrix of trace t as a coset element, and define Q_D to be the set of quadratic forms of discriminant D. We first construct a bijective correspondence $\Phi : \mathrm{PSL}_2(\mathbb{Z})_t \to Q_{t^2-4}$ as follows.

Let $\sigma = \overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} \in \mathrm{PSL}_2(\mathbb{Z})$ be the coset containing the given matrix such that the trace $a+d$ is equal to t. Then, σ is an automorphism of $\mathbb{H}$ with two hyperbolic fixed points, given by the solutions to $\sigma z = z$. Rewriting this equation as $(az+b)/(cz+d) = z$, we see that the fixed points are roots of the quadratic $cz^2 + (d-a)z - b$, which has discriminant

$$(d-a)^2 + 4bc = a^2 - 2ad + d^2 + 4bc = a^2 + 2ad + d^2 - 4(ad-bc) = (a+d)^2 - 4.$$

By projectivizing the coordinates, we obtain $q(x,y) = cx^2 + (d-a)xy - by^2$, the binary quadratic form corresponding to σ.

Next, we define a map $\Psi : Q_{t^2-4} \to \mathrm{PSL}_2(\mathbb{Z})_t$ and show that it is the inverse of Φ. Suppose we have a binary quadratic form $q(x,y) = Ax^2 + Bxy + Cy^2$ of discriminant t^2-4. Then, define $\Psi(q(x,y)) \in \mathrm{PSL}_2(\mathbb{Z})_t$ as the coset containing the matrix

$$\begin{pmatrix} \frac{-B+t}{2} & -C \\ A & \frac{B+t}{2} \end{pmatrix}.$$

Note that B and t have the same parity, as one can see from reducing $B^2 - 4AC = t^2 - 4$ to $B^2 \equiv t^2 \pmod 2$. This shows that the above matrix is integral. Furthermore, it has determinant

$$\frac{t^2 - B^2}{4} + AC = \frac{t^2 - (B^2 - 4AC)}{4} = 1,$$

which shows that Ψ is well-defined. It is straightforward to check that Φ and Ψ are inverses, so Φ is bijective, as claimed.

We next show that two elements of $\mathrm{PSL}_2(\mathbb{Z})_t$ are conjugate if and only if their corresponding binary quadratic forms are in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit. Consider $\overline{M_1}, \overline{M_2} \in \mathrm{PSL}_2(\mathbb{Z})_t$, where the matrix representatives $M_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right)$ are chosen so that $a_1 + d_1 = a_2 + d_2 = t$. We have that $\overline{M_1}$ is conjugate to $\overline{M_2}$ if and only if there exists $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $M_1 = S^{-1}M_2S$. However, we have

$$\begin{aligned}
&\exists S \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } M_1 = S^{-1}M_2S \\
&\quad\iff \exists S \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \overline{S^{-1}M_2S}z = z \text{ gives the same quadratic form as } \overline{M_1}z = z \\
&\quad\iff \exists S \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \overline{M_2}\cdot\overline{S}z = \overline{S}z \text{ gives the same quadratic form as } \overline{M_1}z = z \\
&\quad\iff \exists S \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \overline{M_2}\cdot\overline{S}\frac{x}{y} = \overline{S}\frac{x}{y} \text{ gives the same quadratic form as } \overline{M_1}\frac{x}{y} = \frac{x}{y} \\
&\quad\iff \exists S \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \Phi(\overline{M_1}) = S\cdot\Phi(\overline{M_2}).
\end{aligned}$$

Thus, we have shown that the conjugacy classes of $\mathrm{PSL}_2(\mathbb{Z})$ with trace $\pm t$ correspond to the $\mathrm{SL}_2(\mathbb{Z})$-orbits of binary quadratic forms with discriminant $t^2 - 4$. This allows us to use Gauss' reduction theory of indefinite binary quadratic forms, which yields a full set of representatives for the $\mathrm{SL}_2(\mathbb{Z})$-orbits of binary quadratic forms of any positive discriminant, to exhaustively list matrix representatives for the conjugacy classes of $\mathrm{PSL}_2(\mathbb{Z})$ with any given trace.

Next, we check whether or not each conjugacy class $\overline{M} \in \mathrm{PSL}_2(\mathbb{Z})_t$ is in the commutator subgroup $[\mathrm{PSL}_2(\mathbb{Z}), \mathrm{PSL}_2(\mathbb{Z})]$. Doing this is straightforward, since $[\mathrm{PSL}_2(\mathbb{Z}), \mathrm{PSL}_2(\mathbb{Z})]$ is precisely

$$\left\{ \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} : (1-c^2)(bd + 3(c-1)d + c + 3) + c(a+d-3) \equiv 0 \pmod{12} \right. \tag{3.3}$$

$$\left. \text{or } (1-c^2)(bd + 3(c+1)d - c + 3) + c(a+d+3) \equiv 0 \pmod{12} \right\} \tag{3.4}$$

a congruence subgroup of index 6. This follows from the fact that $[\mathrm{SL}_2(\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z})] = \ker \chi$ for the surjective homomorphism $\chi : \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{Z}/12\mathbb{Z}$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (1-c^2)(bd + 3(c-1)d + c + 3) + c(a+d-3),$$

as shown in [3, Proof of Theorem 3.8]. Note that this step is done to save time that would otherwise be spent unnecessarily on combinatorially checking whether conjugacy classes that are not even in the commutator subgroup are commutators. If M satisfies the condition (3.3), then it is a commutator in $\mathrm{SL}_2(\mathbb{Z})$, whereas if M satisfies the condition (3.4), then $-M$ is a commutator in $\mathrm{SL}_2(\mathbb{Z})$. Exactly one of these two possibilities is true if and only if $\overline{M}$ is a commutator in $\mathrm{PSL}_2(\mathbb{Z})$.

Afterwards, our algorithm writes the representative $\overline{M}$ of each conjugacy class of $\mathrm{PSL}_2(\mathbb{Z})_t$ in terms of the generators in $\mathfrak{S} = \{r, r^{-1}, s\}$. Here, s denotes the coset containing S and is a generator of the $\mathbb{Z}/2\mathbb{Z}$ factor of $\mathrm{PSL}_2(\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$, while r is the coset containing ST and is a generator of the $\mathbb{Z}/3\mathbb{Z}$ factor; the matrices S and T are defined in (1.2). We use the well-known reduction process to write any matrix in $\mathrm{SL}_2(\mathbb{Z})$ in terms of S and T; for a reference, see [3, Section 2]. First, note that

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \qquad \text{and} \qquad T^n\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}.$$

In light of this, we follow the following steps to reduce $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, which we can assume to have trace t, to a product of powers of S and of T.

1. If $c = 0$, then skip this step. Otherwise, consider whether $|a|$ is less than $|c|$ or not. If $|a| \geq |c|$, then write $a = cq + \tau$ for $0 \leq \tau < |c|$. Then, $T^{-q}M = \left(\begin{smallmatrix} a-qc & b-qc \\ c & d \end{smallmatrix}\right)$ has its upper-left entry equal to τ. Then, we apply S to $T^{-q}M$ (or to M, if $|a| < |c|$), which switches the absolute values of the upper-left and lower-left entries, yielding a matrix with the upper-left entry having a greater absolute value than the lower-left entry. We repeat this process, and every iteration of this process decreases $\min(a, c)$, so eventually we obtain that M is equal to a product of powers of S and of T, right-multiplied by a matrix with lower-left entry 0.

2. A matrix with lower-left entry 0 and determinant 1 must be either of the form $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) = T^n$ or of the form $\left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right) = -T^n = S^2T^n$. Thus, we overall have that M is a product of powers of S and of T.

Since $\overline{T} = \overline{S^{-1}}r = sr$, we can substitute s for S and sr for T to get an expression for $\overline{M}$ that is a product of powers of s and of r. By repeatedly canceling adjacent entries that are in the same free factor, we can, without loss of generality, assume that this product expression W is fully cyclically reduced.

Finally, the algorithm checks whether there is a cyclic conjugate of W that is of the form $XYX^{-1}Y^{-1}$ or of the form $X\alpha Y\beta Z\alpha X^{-1}\beta Y^{-1}\alpha Z^{-1}\beta$ for $\alpha, \beta \in \{r, r^{-1}\}$, which have been shown in Section 3.1 to be the only possible Wicks commutator forms for $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. If $\overline{M} = W$ is a commutator in $\mathrm{PSL}_2(\mathbb{Z})$, then we can conclude that either M or $-M$ is a commutator, depending on whether M satisfies the condition (3.3) or the condition (3.4).

We have run the above algorithm for $3 \le t \le 3000$. For each such t, our program computes the conjugacy classes (and their matrix representatives with trace t) in $\mathrm{PSL}_2(\mathbb{Z})_t$, determines which of these conjugacy classes are in the commutator subgroup by checking the congruence condition (3.3), and determines which of the conjugacy classes in the commutator subgroup are in fact commutators. First, below is a table of our full set of data for $3 \le t \le 100$, which displays any conjugacy classes of trace t and $-t$ that have trivial abelianization, whether each such conjugacy class is comprised of commutators (say, containing $ABA^{-1}B^{-1}$ for $A, B \in \mathrm{SL}_2(\mathbb{Z})$), and the matrices A and B in this description.

Trace	Conj. class representative	Commutator?	A	B
3	$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$
6	$\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$
7	$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}$
-9	$\begin{pmatrix} -1 & -7 \\ -1 & -8 \end{pmatrix}$	true	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -1 & 7 \\ 1 & -8 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -4 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
11	$\begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 3 & 1 \\ -1 & 0 \end{pmatrix}$
15	$\begin{pmatrix} 2 & 5 \\ 5 & 13 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix}$
	$\begin{pmatrix} 2 & -5 \\ -5 & 13 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 13 \\ 1 & 14 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -13 \\ -1 & 14 \end{pmatrix}$	false		
18	$\begin{pmatrix} 1 & 4 \\ 4 & 17 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix}$

-18	$\begin{pmatrix} -1 & 8 \\ 2 & -17 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 5 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
	$\begin{pmatrix} -1 & -8 \\ -2 & -17 \end{pmatrix}$	true	$\begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
-21	$\begin{pmatrix} -1 & -19 \\ -1 & -20 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 19 \\ 1 & -20 \end{pmatrix}$	false		
-25	$\begin{pmatrix} -2 & -15 \\ -3 & -23 \end{pmatrix}$	true	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -2 & 15 \\ 3 & -23 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -4 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
27	$\begin{pmatrix} 4 & 13 \\ 7 & 23 \end{pmatrix}$	true	$\begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 4 & -13 \\ -7 & 23 \end{pmatrix}$	true	$\begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 5 \\ 5 & 26 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & -25 \\ -1 & 26 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & 25 \\ 1 & 26 \end{pmatrix}$	false		
-29	$\begin{pmatrix} -1 & -9 \\ -3 & -28 \end{pmatrix}$	true	$\begin{pmatrix} 6 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -1 & 9 \\ 3 & -28 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -6 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
30	$\begin{pmatrix} 7 & -16 \\ -10 & 23 \end{pmatrix}$	true	$\begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 7 & 16 \\ 10 & 23 \end{pmatrix}$	true	$\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 14 \\ 2 & 29 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -14 \\ -2 & 29 \end{pmatrix}$	false		
-30	$\begin{pmatrix} -3 & -20 \\ -4 & -27 \end{pmatrix}$	true	$\begin{pmatrix} -7 & -4 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -3 & 20 \\ 4 & -27 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 2 \\ -4 & -7 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
-33	$\begin{pmatrix} -1 & -31 \\ -1 & -32 \end{pmatrix}$	false		
	$\begin{pmatrix} -6 & -7 \\ -23 & -27 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 31 \\ 1 & -32 \end{pmatrix}$	false		
	$\begin{pmatrix} -6 & 7 \\ 23 & -27 \end{pmatrix}$	false		
34	$\begin{pmatrix} 5 & 12 \\ 12 & 29 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & 5 \\ -1 & -2 \end{pmatrix}$
-34	$\begin{pmatrix} -5 & 24 \\ 6 & -29 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 3 \\ -3 & -8 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
	$\begin{pmatrix} -5 & -24 \\ -6 & -29 \end{pmatrix}$	true	$\begin{pmatrix} -8 & -3 \\ 3 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
38	$\begin{pmatrix} 1 & 6 \\ 6 & 37 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 6 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 7 & -18 \\ -12 & 31 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 2 \\ -2 & -3 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$
39	$\begin{pmatrix} 5 & 13 \\ 13 & 34 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -5 & -3 \\ 2 & 1 \end{pmatrix}$

	$\begin{pmatrix} 5 & -13 \\ -13 & 34 \end{pmatrix}$	true	$\begin{pmatrix} -1 & -2 \\ 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 37 \\ 1 & 38 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -37 \\ -1 & 38 \end{pmatrix}$	false		
-42	$\begin{pmatrix} -1 & 4 \\ 10 & -41 \end{pmatrix}$	true	$\begin{pmatrix} 7 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -1 & -4 \\ -10 & -41 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 7 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
	$\begin{pmatrix} -1 & -20 \\ -2 & -41 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 20 \\ 2 & -41 \end{pmatrix}$	false		
43	$\begin{pmatrix} 2 & 9 \\ 9 & 41 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -4 & -5 \\ 1 & 1 \end{pmatrix}$
	$\begin{pmatrix} 2 & -9 \\ -9 & 41 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 1 \\ -5 & -4 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 2 & 27 \\ 3 & 41 \end{pmatrix}$	false		
	$\begin{pmatrix} 2 & -27 \\ -3 & 41 \end{pmatrix}$	false		
-45	$\begin{pmatrix} -2 & -17 \\ -5 & -43 \end{pmatrix}$	true	$\begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -17 & -19 \\ -25 & -28 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -4 \end{pmatrix}$	$\begin{pmatrix} -4 & 1 \\ 3 & -1 \end{pmatrix}$
	$\begin{pmatrix} -2 & 17 \\ 5 & -43 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 5 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
	$\begin{pmatrix} -17 & 19 \\ 25 & -28 \end{pmatrix}$	true	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 3 \\ 1 & -4 \end{pmatrix}$
	$\begin{pmatrix} -1 & -43 \\ -1 & -44 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 43 \\ 1 & -44 \end{pmatrix}$	false		
47	$\begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$
	$\begin{pmatrix} 1 & 3 \\ 15 & 46 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -3 \\ -15 & 46 \end{pmatrix}$	false		
51	$\begin{pmatrix} 4 & 17 \\ 11 & 47 \end{pmatrix}$	true	$\begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 9 & 29 \\ 13 & 42 \end{pmatrix}$	true	$\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 4 & -17 \\ -11 & 47 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 9 & -29 \\ -13 & 42 \end{pmatrix}$	true	$\begin{pmatrix} -2 & -1 \\ 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 7 \\ 7 & 50 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 7 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & -49 \\ -1 & 50 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & 49 \\ 1 & 50 \end{pmatrix}$	false		
54	$\begin{pmatrix} 1 & 26 \\ 2 & 53 \end{pmatrix}$	false		
	$\begin{pmatrix} 13 & 38 \\ 14 & 41 \end{pmatrix}$	false		

	$\begin{pmatrix} 1 & -26 \\ -2 & 53 \end{pmatrix}$	false		
	$\begin{pmatrix} 13 & -38 \\ -14 & 41 \end{pmatrix}$	false		
-57	$\begin{pmatrix} -8 & -23 \\ -17 & -49 \end{pmatrix}$	true	$\begin{pmatrix} 5 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$
	$\begin{pmatrix} -1 & -11 \\ -5 & -56 \end{pmatrix}$	true	$\begin{pmatrix} 8 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -15 & -37 \\ -17 & -42 \end{pmatrix}$	true	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -3 & 1 \\ 5 & -2 \end{pmatrix}$
	$\begin{pmatrix} -8 & 23 \\ 17 & -49 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 5 \end{pmatrix}$	$\begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -1 & 11 \\ 5 & -56 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -8 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
	$\begin{pmatrix} -15 & 37 \\ 17 & -42 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -4 \end{pmatrix}$	$\begin{pmatrix} -2 & 5 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -1 & -55 \\ -1 & -56 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 55 \\ 1 & -56 \end{pmatrix}$	false		
-61	$\begin{pmatrix} -2 & -39 \\ -3 & -59 \end{pmatrix}$	false		
	$\begin{pmatrix} -2 & 39 \\ 3 & -59 \end{pmatrix}$	false		
63	$\begin{pmatrix} 6 & 31 \\ 11 & 57 \end{pmatrix}$	true	$\begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 10 & 23 \\ 23 & 53 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -2 & -7 \\ 1 & 3 \end{pmatrix}$
	$\begin{pmatrix} 6 & -31 \\ -11 & 57 \end{pmatrix}$	true	$\begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 10 & -23 \\ -23 & 53 \end{pmatrix}$	true	$\begin{pmatrix} 3 & 1 \\ -7 & -2 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 61 \\ 1 & 62 \end{pmatrix}$	false		
	$\begin{pmatrix} 4 & 47 \\ 5 & 59 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -61 \\ -1 & 62 \end{pmatrix}$	false		
	$\begin{pmatrix} 4 & -47 \\ -5 & 59 \end{pmatrix}$	false		
-65	$\begin{pmatrix} -1 & -21 \\ -3 & -64 \end{pmatrix}$	false		
	$\begin{pmatrix} -4 & -27 \\ -9 & -61 \end{pmatrix}$	false		
	$\begin{pmatrix} -4 & -9 \\ -27 & -61 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 21 \\ 3 & -64 \end{pmatrix}$	false		
	$\begin{pmatrix} -4 & 27 \\ 9 & -61 \end{pmatrix}$	false		
	$\begin{pmatrix} -4 & 9 \\ 27 & -61 \end{pmatrix}$	false		
66	$\begin{pmatrix} 1 & 8 \\ 8 & 65 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 8 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 9 & 32 \\ 16 & 57 \end{pmatrix}$	true	$\begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 16 \\ 4 & 65 \end{pmatrix}$	false		

	$\begin{pmatrix}1&-16\\-4&65\end{pmatrix}$	false		
-66	$\begin{pmatrix}-17&-32\\-26&-49\end{pmatrix}$	true	$\begin{pmatrix}5&1\\-1&0\end{pmatrix}$	$\begin{pmatrix}1&-2\\-2&5\end{pmatrix}$
	$\begin{pmatrix}-17&32\\26&-49\end{pmatrix}$	true	$\begin{pmatrix}0&-1\\1&5\end{pmatrix}$	$\begin{pmatrix}5&-2\\-2&1\end{pmatrix}$
	$\begin{pmatrix}-1&-32\\-2&-65\end{pmatrix}$	false		
	$\begin{pmatrix}-1&32\\2&-65\end{pmatrix}$	false		
-69	$\begin{pmatrix}-9&-49\\-11&-60\end{pmatrix}$	true	$\begin{pmatrix}10&3\\-7&-2\end{pmatrix}$	$\begin{pmatrix}-1&1\\1&-2\end{pmatrix}$
	$\begin{pmatrix}-2&19\\7&-67\end{pmatrix}$	true	$\begin{pmatrix}0&1\\-1&-6\end{pmatrix}$	$\begin{pmatrix}3&-1\\-2&1\end{pmatrix}$
	$\begin{pmatrix}-2&7\\19&-67\end{pmatrix}$	true	$\begin{pmatrix}7&1\\-1&0\end{pmatrix}$	$\begin{pmatrix}1&-1\\-2&3\end{pmatrix}$
	$\begin{pmatrix}-9&-11\\-49&-60\end{pmatrix}$	true	$\begin{pmatrix}2&5\\-5&-12\end{pmatrix}$	$\begin{pmatrix}-2&1\\1&-1\end{pmatrix}$
	$\begin{pmatrix}-9&49\\11&-60\end{pmatrix}$	true	$\begin{pmatrix}2&7\\-3&-10\end{pmatrix}$	$\begin{pmatrix}-2&1\\1&-1\end{pmatrix}$
	$\begin{pmatrix}-2&-19\\-7&-67\end{pmatrix}$	true	$\begin{pmatrix}6&1\\-1&0\end{pmatrix}$	$\begin{pmatrix}-1&2\\1&-3\end{pmatrix}$
	$\begin{pmatrix}-2&-7\\-19&-67\end{pmatrix}$	true	$\begin{pmatrix}0&-1\\1&7\end{pmatrix}$	$\begin{pmatrix}-3&2\\1&-1\end{pmatrix}$
	$\begin{pmatrix}-9&11\\49&-60\end{pmatrix}$	true	$\begin{pmatrix}12&5\\-5&-2\end{pmatrix}$	$\begin{pmatrix}-1&1\\1&-2\end{pmatrix}$
	$\begin{pmatrix}-1&-67\\-1&-68\end{pmatrix}$	false		
	$\begin{pmatrix}-1&67\\1&-68\end{pmatrix}$	false		
70	$\begin{pmatrix}11&36\\18&59\end{pmatrix}$	true	$\begin{pmatrix}1&2\\-4&-7\end{pmatrix}$	$\begin{pmatrix}0&-1\\1&0\end{pmatrix}$
	$\begin{pmatrix}11&-36\\-18&59\end{pmatrix}$	true	$\begin{pmatrix}-7&-4\\2&1\end{pmatrix}$	$\begin{pmatrix}0&-1\\1&0\end{pmatrix}$
	$\begin{pmatrix}5&54\\6&65\end{pmatrix}$	false		
	$\begin{pmatrix}5&-54\\-6&65\end{pmatrix}$	false		
-74	$\begin{pmatrix}-1&-12\\-6&-73\end{pmatrix}$	true	$\begin{pmatrix}9&1\\-1&0\end{pmatrix}$	$\begin{pmatrix}-1&1\\1&-2\end{pmatrix}$
	$\begin{pmatrix}-1&12\\6&-73\end{pmatrix}$	true	$\begin{pmatrix}0&-1\\1&9\end{pmatrix}$	$\begin{pmatrix}-2&1\\1&-1\end{pmatrix}$
75	$\begin{pmatrix}11&-37\\-19&64\end{pmatrix}$	true	$\begin{pmatrix}-5&-3\\2&1\end{pmatrix}$	$\begin{pmatrix}-1&1\\-1&0\end{pmatrix}$
	$\begin{pmatrix}13&35\\23&62\end{pmatrix}$	true	$\begin{pmatrix}-1&3\\-2&5\end{pmatrix}$	$\begin{pmatrix}1&1\\-1&0\end{pmatrix}$
	$\begin{pmatrix}11&37\\19&64\end{pmatrix}$	true	$\begin{pmatrix}-1&-2\\3&5\end{pmatrix}$	$\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$
	$\begin{pmatrix}13&-35\\-23&62\end{pmatrix}$	true	$\begin{pmatrix}-1&-3\\2&5\end{pmatrix}$	$\begin{pmatrix}-1&1\\-1&0\end{pmatrix}$
	$\begin{pmatrix}1&73\\1&74\end{pmatrix}$	false		
	$\begin{pmatrix}2&29\\5&73\end{pmatrix}$	false		
	$\begin{pmatrix}6&-59\\-7&69\end{pmatrix}$	false		
	$\begin{pmatrix}15&29\\31&60\end{pmatrix}$	false		

	$\begin{pmatrix} 1 & -73 \\ -1 & 74 \end{pmatrix}$	false		
	$\begin{pmatrix} 2 & -29 \\ -5 & 73 \end{pmatrix}$	false		
	$\begin{pmatrix} 6 & 59 \\ 7 & 69 \end{pmatrix}$	false		
	$\begin{pmatrix} 15 & -29 \\ -31 & 60 \end{pmatrix}$	false		
78	$\begin{pmatrix} 3 & 16 \\ 14 & 75 \end{pmatrix}$	true	$\begin{pmatrix} -1 & 1 \\ -5 & 4 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 11 & 16 \\ 46 & 67 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & -3 \end{pmatrix}$	$\begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$
	$\begin{pmatrix} 3 & -16 \\ -14 & 75 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 1 \\ -5 & -4 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 11 & -16 \\ -46 & 67 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}$	$\begin{pmatrix} -1 & 3 \\ -1 & 2 \end{pmatrix}$
	$\begin{pmatrix} 1 & 38 \\ 2 & 77 \end{pmatrix}$	false		
	$\begin{pmatrix} 9 & 62 \\ 10 & 69 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -38 \\ -2 & 77 \end{pmatrix}$	false		
	$\begin{pmatrix} 9 & -62 \\ -10 & 69 \end{pmatrix}$	false		
−78	$\begin{pmatrix} -3 & -8 \\ -28 & -75 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 7 \end{pmatrix}$	$\begin{pmatrix} -4 & 3 \\ 1 & -1 \end{pmatrix}$
	$\begin{pmatrix} -3 & 8 \\ 28 & -75 \end{pmatrix}$	true	$\begin{pmatrix} 7 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 3 & -4 \end{pmatrix}$
	$\begin{pmatrix} -3 & -56 \\ -4 & -75 \end{pmatrix}$	false		
	$\begin{pmatrix} -3 & 56 \\ 4 & -75 \end{pmatrix}$	false		
79	$\begin{pmatrix} 2 & 51 \\ 3 & 77 \end{pmatrix}$	false		
	$\begin{pmatrix} 8 & -27 \\ -21 & 71 \end{pmatrix}$	false		
	$\begin{pmatrix} 2 & -51 \\ -3 & 77 \end{pmatrix}$	false		
	$\begin{pmatrix} 8 & 27 \\ 21 & 71 \end{pmatrix}$	false		
	$\begin{pmatrix} 8 & 63 \\ 9 & 71 \end{pmatrix}$	false		
	$\begin{pmatrix} 8 & -63 \\ -9 & 71 \end{pmatrix}$	false		
−81	$\begin{pmatrix} -1 & -79 \\ -1 & -80 \end{pmatrix}$	false		
	$\begin{pmatrix} -7 & -47 \\ -11 & -74 \end{pmatrix}$	false		
	$\begin{pmatrix} -15 & -43 \\ -23 & -66 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 79 \\ 1 & -80 \end{pmatrix}$	false		
	$\begin{pmatrix} -7 & 47 \\ 11 & -74 \end{pmatrix}$	false		
	$\begin{pmatrix} -15 & 43 \\ 23 & -66 \end{pmatrix}$	false		
83	$\begin{pmatrix} 16 & 51 \\ 21 & 67 \end{pmatrix}$	true	$\begin{pmatrix} -3 & 1 \\ -4 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$

	$\begin{pmatrix} 16 & -51 \\ -21 & 67 \end{pmatrix}$	true	$\begin{pmatrix} -3 & -1 \\ 4 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 9 \\ 9 & 82 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 9 & 1 \\ -1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 10 & 27 \\ 27 & 73 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -8 & -3 \\ 3 & 1 \end{pmatrix}$
	$\begin{pmatrix} 1 & 27 \\ 3 & 82 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -27 \\ -3 & 82 \end{pmatrix}$	false		
87	$\begin{pmatrix} 2 & 13 \\ 13 & 85 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -6 & -7 \\ 1 & 1 \end{pmatrix}$
	$\begin{pmatrix} 29 & 41 \\ 41 & 58 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 7 & 3 \\ -5 & -2 \end{pmatrix}$
	$\begin{pmatrix} 2 & -13 \\ -13 & 85 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 29 & -41 \\ -41 & 58 \end{pmatrix}$	true	$\begin{pmatrix} -2 & -5 \\ 3 & 7 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
	$\begin{pmatrix} 1 & 85 \\ 1 & 86 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & 17 \\ 5 & 86 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -85 \\ -1 & 86 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -17 \\ -5 & 86 \end{pmatrix}$	false		
-90	$\begin{pmatrix} -9 & -28 \\ -26 & -81 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 2 \\ -6 & -11 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
	$\begin{pmatrix} -29 & -34 \\ -52 & -61 \end{pmatrix}$	true	$\begin{pmatrix} 1 & 4 \\ -2 & -7 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
	$\begin{pmatrix} -11 & 62 \\ 14 & -79 \end{pmatrix}$	true	$\begin{pmatrix} 3 & 5 \\ -8 & -13 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
	$\begin{pmatrix} -7 & 58 \\ 10 & -83 \end{pmatrix}$	true	$\begin{pmatrix} 3 & 4 \\ -10 & -13 \end{pmatrix}$	$\begin{pmatrix} 5 & -1 \\ -4 & 1 \end{pmatrix}$
	$\begin{pmatrix} -9 & 28 \\ 26 & -81 \end{pmatrix}$	true	$\begin{pmatrix} -11 & -6 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -29 & 34 \\ 52 & -61 \end{pmatrix}$	true	$\begin{pmatrix} -7 & -2 \\ 4 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -11 & -62 \\ -14 & -79 \end{pmatrix}$	true	$\begin{pmatrix} 13 & 8 \\ -5 & -3 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -7 & -58 \\ -10 & -83 \end{pmatrix}$	true	$\begin{pmatrix} -13 & -10 \\ 4 & 3 \end{pmatrix}$	$\begin{pmatrix} -1 & 4 \\ 1 & -5 \end{pmatrix}$
	$\begin{pmatrix} -1 & -44 \\ -2 & -89 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & -22 \\ -4 & -89 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 44 \\ 2 & -89 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 22 \\ 4 & -89 \end{pmatrix}$	false		
-93	$\begin{pmatrix} -1 & -13 \\ -7 & -92 \end{pmatrix}$	true	$\begin{pmatrix} 10 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -14 & -65 \\ -17 & -79 \end{pmatrix}$	true	$\begin{pmatrix} 13 & 5 \\ -8 & -3 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$
	$\begin{pmatrix} -1 & 13 \\ 7 & -92 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -10 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$
	$\begin{pmatrix} -14 & 65 \\ 17 & -79 \end{pmatrix}$	true	$\begin{pmatrix} 3 & 8 \\ -5 & -13 \end{pmatrix}$	$\begin{pmatrix} -2 & 1 \\ 1 & -1 \end{pmatrix}$

	$\begin{pmatrix} -1 & -91 \\ -1 & -92 \end{pmatrix}$	false		
	$\begin{pmatrix} -4 & -71 \\ -5 & -89 \end{pmatrix}$	false		
	$\begin{pmatrix} -1 & 91 \\ 1 & -92 \end{pmatrix}$	false		
	$\begin{pmatrix} -4 & 71 \\ 5 & -89 \end{pmatrix}$	false		
-97	$\begin{pmatrix} -2 & -21 \\ -9 & -95 \end{pmatrix}$	true	$\begin{pmatrix} 7 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 2 \\ 1 & -3 \end{pmatrix}$
	$\begin{pmatrix} -20 & -57 \\ -27 & -77 \end{pmatrix}$	true	$\begin{pmatrix} -9 & -5 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix}$
	$\begin{pmatrix} -5 & -51 \\ -9 & -92 \end{pmatrix}$	true	$\begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 5 \\ 1 & -6 \end{pmatrix}$
	$\begin{pmatrix} -2 & 21 \\ 9 & -95 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 7 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$
	$\begin{pmatrix} -20 & 57 \\ 27 & -77 \end{pmatrix}$	true	$\begin{pmatrix} -1 & -2 \\ 5 & 9 \end{pmatrix}$	$\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$
	$\begin{pmatrix} -5 & 51 \\ 9 & -92 \end{pmatrix}$	true	$\begin{pmatrix} 0 & 1 \\ -1 & -4 \end{pmatrix}$	$\begin{pmatrix} -6 & 1 \\ 5 & -1 \end{pmatrix}$
	$\begin{pmatrix} -2 & -63 \\ -3 & -95 \end{pmatrix}$	false		
	$\begin{pmatrix} -2 & 63 \\ 3 & -95 \end{pmatrix}$	false		
99	$\begin{pmatrix} 19 & 31 \\ 49 & 80 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 3 & 5 \\ -2 & -3 \end{pmatrix}$
	$\begin{pmatrix} 19 & -31 \\ -49 & 80 \end{pmatrix}$	true	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -5 \\ 2 & -3 \end{pmatrix}$
	$\begin{pmatrix} 1 & 97 \\ 1 & 98 \end{pmatrix}$	false		
	$\begin{pmatrix} 5 & 67 \\ 7 & 94 \end{pmatrix}$	false		
	$\begin{pmatrix} 3 & -41 \\ -7 & 96 \end{pmatrix}$	false		
	$\begin{pmatrix} 1 & -97 \\ -1 & 98 \end{pmatrix}$	false		
	$\begin{pmatrix} 5 & -67 \\ -7 & 94 \end{pmatrix}$	false		
	$\begin{pmatrix} 3 & 41 \\ 7 & 96 \end{pmatrix}$	false		

Table 3.1: Full set of data for $3 \leq t \leq 100$ outputted by our algorithm. The provided commutator decomposition $ABA^{-1}B^{-1}$ is of an element in the corresponding conjugacy class $\mathcal{C}$, but this element is not necessarily the matrix representative listed in the table.

Second, below is table of summarized data for $3 \leq t \leq 3000$. For $n \in 100\mathbb{Z} \cap [3, 3000]$, the table displays the ratios

$$R_1(n) := \frac{|\{t : 3 \leq |t| \leq n \text{ and } t \text{ is the trace of a commutator of } \mathrm{SL}_2(\mathbb{Z})\}|}{|\{t : 3 \leq |t| \leq n\}|},$$

$$R_2(n) := \frac{|\{t : 3 \leq |t| \leq n \text{ and } t \text{ is the trace of a commutator of } \mathrm{SL}_2(\mathbb{Z})\}|}{|\{t : 3 \leq |t| \leq n \text{ and } t \text{ is the trace of a commutator-subgroup element of } \mathrm{SL}_2(\mathbb{Z})\}|},$$

and

$$R_3(n) := \frac{|\{\text{conj. class } \mathcal{C} \text{ of commutators in } \mathrm{SL}_2(\mathbb{Z}) : 3 \leq |\operatorname{Tr}\mathcal{C}| \leq n\}|}{|\{\text{conj. class } \mathcal{C} \text{ of commutator-subgroup elements in } \mathrm{SL}_2(\mathbb{Z}) : 3 \leq |\operatorname{Tr}\mathcal{C}| \leq n\}|},$$

rounded to three decimal places. This information is also sufficient to obtain the ratio between $|\{t : 3 \leq |t| \leq n$ and t is the trace of a commutator-subgroup element of $\mathrm{SL}_2(\mathbb{Z})\}|$ and $|\{t : 3 \leq |t| \leq n$ and t is the trace of a commutator of $\mathrm{SL}_2(\mathbb{Z})\}|$, which is given by the ratio $R_2(n)/R_1(n)$.

n	$R_1(n)$	$R_2(n)$	$R_3(n)$
100	0.232	0.844	0.524
200	0.242	0.779	0.418
300	0.244	0.752	0.341
400	0.242	0.750	0.300
500	0.243	0.739	0.277
600	0.243	0.734	0.255
700	0.242	0.725	0.236
800	0.243	0.724	0.226
900	0.244	0.714	0.209
1000	0.242	0.716	0.200
1100	0.243	0.720	0.192
1200	0.244	0.714	0.185
1300	0.243	0.712	0.177
1400	0.242	0.708	0.168
1500	0.243	0.709	0.164

1600	0.243	0.706	0.158
1700	0.243	0.702	0.154
1800	0.243	0.703	0.149
1900	0.243	0.700	0.144
2000	0.243	0.701	0.141
2100	0.243	0.701	0.137
2200	0.243	0.698	0.133
2300	0.243	0.693	0.130
2400	0.243	0.694	0.128
2500	0.243	0.693	0.125
2600	0.243	0.694	0.122
2700	0.243	0.695	0.120
2800	0.243	0.696	0.118
2900	0.243	0.695	0.116
3000	0.243	0.689	0.112

Table 3.2: Summarized data for $3 \leq t \leq 3000$.

Chapter 4

Concluding Remarks

The data of Table 3.2 suggest that $R_1(n)$ and $R_2(n)$ are each converging to a nonzero proportion. In light of this, we conjecture that the set of $t \geq 3$ that are absolute values of traces of commutators appear to be a positive-proportion subset within the set of all $t \geq 3$, with a proportion close to 0.243. We similarly conjecture that the set of $t \geq 3$ that are absolute values of traces of commutator-subgroup elements also seem to be a positive-proportion subset within the set of all $t \geq 3$, with a proportion somewhere within or close to the interval $[R_2(2000), R_2(3000)] = [0.689, 0.701]$. If these conjectures were to be proven true, then it would follow that the values of $t \geq 3$ that are absolute values of traces of commutators would have positive density within the set of $t \geq 3$ that are absolute values of traces of commutator-subgroup elements.

On the other hand, it is less clear from the data of Table 3.2 whether $R_3(n)$ is converging to a positive proportion or to 0. We observed in Section 1 that the number of conjugacy classes of commutators in $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \cong \mathrm{PSL}_2(\mathbb{Z})$ with a given word length k is roughly comparable to the square root of the number of all conjugacy classes with trivial abelianization, and we expect the same to occur when counting by trace rather than word length, which, if true, would imply that $R_3(n)$ converges to 0 as $n \to \infty$. We anticipate collecting more data from our algorithm to investigate the asymptotic behavior of $R_3(n)$.

To check which conjugacy classes are comprised of commutators, our algorithm represents each conjugacy-class representative $\overline{M}$ in terms of the generators of $\mathrm{PSL}_2(\mathbb{Z})$ and group-theoretically determines whether or not it is a commutator. A natural question to ask on this front is: does there exist a purely number-theoretic criterion (i.e., one which only uses the matrix entries of M) that is necessary and sufficient for $\overline{M}$ to be a commutator in $\mathrm{PSL}_2(\mathbb{Z})$? Such a criterion could both improve the speed of the algorithm and help explain some of the asymptotic phenomena shown by our data, such as the asymptotic behavior of the ratios $R_1(n), R_2(n)$, and $R_3(n)$.

While we have solved the problem of counting conjugacy classes of commutators ordered by word length for any free group and for $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$, there are a number of directions in which Theorems 1.2 and 1.4 can be generalized. First, one can ask: how many conjugacy classes of commutators with word length k are in an arbitrary finitely-generated free product $G = *_{i \in I} G_i$? While one can define the word length in this context to be with respect to an arbitrary generating set $\mathfrak{S}$, a natural notion of length to use in this setting would be the *free product length*, which can be defined as the word length with respect to

$$\mathfrak{S} := \{g \in G \setminus \{1\} : g \in G_i \text{ for some } i \in I\}.$$

Note that word length with respect to our choice of $\mathfrak{S}$ for $\mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ coincides with the free product length.

Also, let the *n-commutators* of a given group be defined by the elements with trivial abelianization and commutator length n. A second direction for generalizing Theorems 1.2 and 1.4 is to, for any n, count the number of conjugacy classes of n-commutators with word length k in a free group or free product (such as $\mathbb{Z}/3\mathbb{Z}*\mathbb{Z}/2\mathbb{Z}$, or more generally, an arbitrary finitely-generated free product $G = *_{i \in I} G_i$). This is natural to ask, given that Culler [4] has classified the possible forms of n-commutators for a free group and Vdovina [13] has done this for an arbitrary free product. In fact, Culler has also classified the possible forms that a product of n square elements can take for a free group, so an analogous question can be asked for the number of conjugacy classes comprised of products of n square elements.

References

[1] Jean Bourgain, Alexander Gamburd, and Peter Sarnak, *Markoff triples and strong approximation*, C. R. Math. Acad. Sci. Paris **354** (2016), no. 2, 131–135. MR 3456887

[2] Danny Calegari, *Stable commutator length is rational in free groups*, J. Amer. Math. Soc. **22** (2009), no. 4, 941–961. MR 2525776

[3] Keith Conrad, $SL_2(\mathbb{Z})$, expository notes, `http://www.math.uconn.edu/kconrad/blurbs/grouptheory/SL(2,Z).pdf`, 2016.

[4] Marc Culler, *Using surfaces to solve equations in free groups*, Topology **20** (1981), no. 2, 133–145. MR 605653

[5] Amit Ghosh and Peter Sarnak, *Integral points on Markoff-type cubic surfaces*, unpublished preprint, 2017.

[6] Mikhael Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 53, 53–73. MR 623534

[7] Avinoam Mann, *How groups grow*, London Mathematical Society Lecture Note Series, vol. 395, Cambridge University Press, Cambridge, 2012. MR 2894945

[8] Grigory A. Margulis, *Certain applications of ergodic theory to the investigation of manifolds of negative curvature*, Funkcional. Anal. i Priložen. **3** (1969), no. 4, 89–90. MR 0257933

[9] Igor Rivin, *Growth in free groups (and other stories)—twelve years later*, Illinois J. Math. **54** (2010), no. 1, 327–370. MR 2776999

[10] Peter Sarnak, *Prime geodesic theorems*, ProQuest LLC, Ann Arbor, MI, 1980, Thesis (Ph.D.)–Stanford University. MR 2630950

[11] ———, *Reciprocal geodesics*, Analytic number theory, Clay Math. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 2007, pp. 217–237. MR 2362203

[12] Atle Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc. (N.S.) **20** (1956), 47–87. MR 0088511

[13] Alina Vdovina, *Products of commutators in free products*, Internat. J. Algebra Comput. **7** (1997), no. 4, 471–485. MR 1459623

[14] Malcolm J. Wicks, *Commutators in free products*, J. London Math. Soc. **37** (1962), 433–444. MR 0142610

Appendix: Code

```
Subs:=function(str,pos,length)
    if length ge 1 then
        return Substring(str,pos,length);
    else
        return "";
    end if;
end function;

negatee:=function(str)
    if str eq "r" then
        return "i";
    elif str eq "i" then
        return "r";
    else
        return "s";
    end if;
end function;

concat:=function(str1,str2)
    n:=1;
    length1:=#str1;
    length2:=#str2;
    length1p1:=length1+1;
    while n le length1 and n le length2
      and negatee(str1[length1p1-n])
        eq str2[n] do
        n:=n+1;
    end while;
    if n gt length2 then
     return Substring(str1,1,length1p1-n);
    else
     x:=length1p1-n;
        if x gt 0 and str1[x] eq "r" and str2[n] eq "r" then
            return Subs(str1,1,x-1) cat "i"
              cat Substring(str2,n+1,length2);
```

```
        elif x gt 0 and str1[x] eq "i" and str2[n] eq "i" then
            return Subs(str1,1,x-1) cat "r"
              cat Substring(str2,n+1,length2);
        else
            return Subs(str1,1,x) cat Substring(str2,n,length2);
        end if;
    end if;
end function;

genform := function(A,B,C,D)
    a:=A;
    b:=B;
    c:=C;
    d:=D;
    str:="";
    while c ne 0 do
        if a*a ge c*c then
            q:=a div c;
            a:=a mod c;
            b:=b-q*d;
            if q gt 0 then
                str:=concat(str,"sr"^q);
            else
                str:=concat(str,"is"^(-q));
            end if;
        end if;
        temp:=d;
        d:=b;
        b:=-temp;
        temp:=c;
        c:=a;
        a:=-temp;
        strlength:=#str;
        if strlength gt 0 and str[strlength] eq "s" then
                    str:=Substring(str,1,strlength-1);
        else
         str:=str cat "s";
        end if;
    end while;
    if a eq 1 then
        if b ge 0 then
            str:=concat(str,"sr"^b);
        else
            str:=concat(str,"is"^(-b));
        end if;
    else
        if b ge 0 then
            str:=concat(str,"is"^b);
```

```
        else
            str:=concat(str,"sr"^(-b));
        end if;
    end if;
    return str;
end function;

SSubstring:=function(str,length)
    if length ge 1 then
        return Substring(str,1,length);
    else
        return "";
    end if;
end function;

Checkinvv:=function(str1,str2)
    length1:=#str1;
    length1p1:=length1+1;
    if length1 ne #str2 then
        return false;
    end if;
    count:=1;
        while count le length1 do
            if str1[count] ne negatee(str2[length1p1-count]) then
                return false;
            end if;
            count:=count+1;
        end while;
    return true;
end function;

matrixform:=function(str)
    M:=Matrix(IntegerRing(), 2, 2, [1,0,0,1]);
        for n in [1..#str] do
            if str[n] eq "s" then
                M:=M*Matrix(IntegerRing(), 2, 2, [0,-1,1,0]);
            elif str[n] eq "r" then
                M:=M*Matrix(IntegerRing(), 2, 2, [0,-1,1,1]);
            elif str[n] eq "i" then
                M:=M*Matrix(IntegerRing(), 2, 2, [1,1,-1,0]);
            end if;
        end for;
    return M;
end function;

checkcommdetailed:= function(string2)
    latest:=string2;
    seclength:=#string2;
```

```
lastbit:=latest[seclength];
if lastbit eq "s" then
    if latest[1] eq "s" and seclength gt 1 then
        latest:=Substring(latest,2,seclength-2);
    end if;
elif lastbit eq "r" then
    if latest[1] eq lastbit and seclength gt 1 then
        latest:= "i" cat Substring(latest,2,seclength-2);
    elif latest[1] eq "i" and seclength gt 1 then
        latest:= Substring(latest,1,seclength-1);
    end if;
else
    if latest[1] eq lastbit and seclength gt 1 then
        latest:= "r" cat Substring(latest,2,seclength-2);
    elif latest[1] eq "r" and seclength gt 1 then
        latest:= Substring(latest,1,seclength-1);
    end if;
end if;
length:=#latest;
list2:=[latest];
for n in [1..length] do
    tempstr:= Substring(latest,length,1)
      cat Substring(latest,1,length-1);
    list2:=Append(list2,tempstr);
    latest:=tempstr;
end for;
for str in list2 do
    if length mod 2 eq 1 then
        return false;
    end if;
    if length mod 4 eq 0 then
        hlength:=length div 2;
        hlengthp1:=hlength+1;
        qlength:=hlength div 2;
        for a in [1..qlength] do
            x:=Substring(str,1,a*2-1);
            y:=Substring(str,a*2,hlengthp1-a*2);
            if Checkinvv(x,Substring(str,hlengthp1,a*2-1))
              and Checkinvv(y,
              Substring(str,a*2+hlength,hlengthp1-a*2)) then
                mattx:=matrixform(x);
                matty:=matrixform(y);
                return <true, ";", mattx[1,1], ";", mattx[1,2],";",
                  mattx[2,1], ";", mattx[2,2], ";", matty[1,1], ";",
                  matty[1,2],";", matty[2,1], ";", matty[2,2]>;
            end if;
        end for;
    end if;
```

```
        lengthm6:=length-6;
        if str[length] ne "s" and lengthm6 mod 4 eq 2 then
            v:=str[hlength];
            hlength:=lengthm6 div 2;
    qlength:=lengthm6 div 4;
    for a in [1..qlength] do
        if str[a*2] eq v and str[hlength+3+a*2] eq str[length] then
            for b in [1..qlength-a+1] do
                if str[a*2+b*2] eq str[length]
                  and str[hlength+3+a*2+b*2] eq v then
            x:=Substring(str,1,a*2-1);
            y:=Substring(str,a*2+1,b*2-1);
            z:=Substring(str,a*2+b*2+1,hlength-a*2-b*2+2);
            zinv:=Substring(str,hlength+a*2+b*2+4,hlength-a*2-b*2+2);
            if Checkinvv(x,Substring(str,4+hlength,a*2-1))
              and Checkinvv(y,Substring(str,hlength+a*2+4,b*2-1))
              and Checkinvv(z,zinv) then
                mattx:=matrixform(negatee(str[length]) cat x cat negatee(v)
                  cat zinv cat negatee(str[length]));
                matty:=matrixform(str[length] cat z cat negatee(v) cat y);
                return <true, ";", mattx[1,1], ";", mattx[1,2],";",
                mattx[2,1], ";", mattx[2,2], ";", matty[1,1], ";",
                matty[1,2],";", matty[2,1], ";", matty[2,2]>;
            end if;
        end if;
    end for;
end if;
    end for;
        end if;
    end for;
    return false;
end function;


checkcomm:= function(string2)
    latest:=string2;
    seclength:=#string2;
    lastbit:=latest[seclength];
    if lastbit eq "s" then
        if latest[1] eq "s" and seclength gt 1 then
            latest:=Substring(latest,2,seclength-2);
        end if;
    elif lastbit eq "r" then
        if latest[1] eq lastbit and seclength gt 1 then
            latest:= "i" cat Substring(latest,2,seclength-2);
        elif latest[1] eq "i" and seclength gt 1 then
            latest:= Substring(latest,1,seclength-1);
        end if;
```

```
else
    if latest[1] eq lastbit and seclength gt 1 then
        latest:= "r" cat Substring(latest,2,seclength-2);
    elif latest[1] eq "r" and seclength gt 1 then
        latest:= Substring(latest,1,seclength-1);
    end if;
end if;
length:=#latest;
list2:=[latest];
for n in [1..length] do
    tempstr:= Substring(latest,length,1)
      cat Substring(latest,1,length-1);
    list2:=Append(list2,tempstr);
    latest:=tempstr;
end for;
for str in list2 do
    if length mod 2 eq 1 then
        return false;
    end if;
    if length mod 4 eq 0 then
        hlength:=length div 2;
        hlengthp1:=hlength+1;
        qlength:=hlength div 2;
        for a in [1..qlength] do
            x:=Substring(str,1,a*2-1);
            y:=Substring(str,a*2,hlengthp1-a*2);
            if Checkinvv(x,Substring(str,hlengthp1,a*2-1))
              and Checkinvv(y,
              Substring(str,a*2+hlength,hlengthp1-a*2)) then
                return true;
            end if;
        end for;
    end if;
    lengthm6:=length-6;
    if str[length] ne "s" and lengthm6 mod 4 eq 2 then
        v:=str[hlength];
        hlength:=lengthm6 div 2;
qlength:=lengthm6 div 4;
for a in [1..qlength] do
    if str[a*2] eq v and str[hlength+3+a*2] eq str[length] then
        for b in [1..qlength-a+1] do
            if str[a*2+b*2] eq str[length]
              and str[hlength+3+a*2+b*2] eq v then
        x:=Substring(str,1,a*2-1);
        y:=Substring(str,a*2+1,b*2-1);
        z:=Substring(str,a*2+b*2+1,hlength-a*2-b*2+2);
        zinv:=Substring(str,hlength+a*2+b*2+4,hlength-a*2-b*2+2);
        if Checkinvv(x,Substring(str,4+hlength,a*2-1))
```

```
          and Checkinvv(y,Substring(str,hlength+a*2+4,b*2-1))
          and Checkinvv(z,zinv) then
            return true;
        end if;
      end if;
    end for;
end if;
    end for;
        end if;
    end for;
    return false;
end function;

for t in [3..100] do
    D:=t*t-4;
    modt:=t mod 12;
    for dd in Divisors(D) do
        Disc:=Round(D/dd);
        if IsSquare(dd) ne false and (Disc mod 4) le 1  then
            mult:=Round(SquareRoot(dd));
            Q := BinaryQuadraticForms(Disc);
            QQ:=ReducedForms(Q);
            for quad in QQ do
                a:=mult*quad[1];
                b:=mult*quad[2];
                c:=mult*quad[3];
                ma:=Round((-b+t)/2);
                mb:=-c;
                mc:=a;
                md:=Round((b+t)/2);
                a:=ma mod 12;
                b:=mb mod 12;
                c:=mc mod 12;
                d:=md mod 12;
                if modt in [0, 2, 3, 4, 6, 7, 8, 10, 11]
                  and ((1-c*c)*(b*d+3*(c-1)*d+c+3)+c*(a+d-3)) mod 12
                  eq 0 then
                    thegenform:=genform(ma,mb,mc,md);
                    answer:=checkcommdetailed(thegenform);
                    t, ";", ma, ";", mb, ";", mc, ";", md , ";", answer;
                elif modt in [0,1,2, 4,5 ,6, 8,9, 10]
                  and ((1-c*c)*(b*d+3*(-c-1)*(-d)-c+3)-c*(-a-d-3)) mod 12
                  eq 0 then
                    thegenform:=genform(-ma,-mb,-mc,-md);
                    answer:=checkcommdetailed(thegenform);
                    -t, ";", -ma, ";", -mb, ";", -mc, ";", -md , ";", answer ;
                end if;
            end for;
```

```
        end if;
    end for;
end for;

num:=0;
den:=0;
for t in [3..3000] do
    D:=t*t-4;
    modt:=t mod 12;
    cnumberplus:=0;
    cnumberminus:=0;
    mnumberplus:=0;
    mnumberminus:=0;
    for dd in Divisors(D) do
        Disc:=Round(D/dd);
        if IsSquare(dd) ne false and (Disc mod 4) le 1  then
            mult:=Round(SquareRoot(dd));
            Q := BinaryQuadraticForms(Disc);
            QQ:=ReducedForms(Q);
            for quad in QQ do
                a:=mult*quad[1];
                b:=mult*quad[2];
                c:=mult*quad[3];
                ma:=Round((-b+t)/2);
                mb:=-c;
                mc:=a;
                md:=Round((b+t)/2);
                a:=ma mod 12;
                b:=mb mod 12;
                c:=mc mod 12;
                d:=md mod 12;
                if modt in [0, 2, 3, 4, 6, 7, 8, 10, 11]
                  and ((1-c*c)*(b*d+3*(c-1)*d+c+3)+c*(a+d-3)) mod 12
                  eq 0 then
                     thegenform:=genform(ma,mb,mc,md);
                     answer:=checkcomm(thegenform);
                     if answer cmpne false then
                        mnumberplus:=mnumberplus+1;
                    end if;
                     cnumberplus:=cnumberplus+1;
                elif modt in [0,1,2, 4,5 ,6, 8,9, 10]
                  and ((1-c*c)*(b*d+3*(-c-1)*(-d)-c+3)-c*(-a-d-3)) mod 12
                  eq 0 then
                     thegenform:=genform(-ma,-mb,-mc,-md);
                     answer:=checkcomm(thegenform);
                     if answer cmpne false then
                        mnumberminus:=mnumberminus+1;
                    end if;
```

```
                    cnumberminus:=cnumberminus+1;
                end if;
            end for;
        end if;
    end for;
    num:=num+mnumberplus+mnumberminus;
    den:=den+cnumberplus+cnumberminus;
    if cnumberplus ne 0 then
        t,";",D,";", mnumberplus,";",
          cnumberplus,";", mnumberplus ne 0,";", num, ";", den;
    end if;
    if cnumberminus ne 0 then
        -t,";",D,";", mnumberminus,";",
          cnumberminus,";", mnumberminus ne 0 ,";", num, ";", den;
    end if;
end for;
```