On the conjugacy problem in $\mathrm{Aut}(F_2)$ and related problems

Óscar Fernández Ayala

Institut für Analysis und Algebra
TU Braunschweig

June 20, 2026

Introduction

Theorem 1

The group A_2 *is virtually free, while* $\mathrm{Aut}(F_n)$ *is not virtually free for* $n \geq 3$.

There is an algorithm for the conjugacy problem in $\mathrm{Out}(F_3)$[1] and for irreducible outer automorphisms[2].

[1] F Dahmani et al. "The conjugacy problem for $\mathrm{Out}(F_3)$". In: *Forum of Mathematics, Sigma* 13 (2025)

[2] J. E. Los. "On the conjugacy problem for automorphisms of free groups". In: *Topology* 35.3 (1996), pp. 779–806

Introduction

Theorem 1

The group A_2 *is virtually free, while* $\mathrm{Aut}(F_n)$ *is not virtually free for* $n \geq 3$.

There is an algorithm for the conjugacy problem in $\mathrm{Out}(F_3)$[1] and for irreducible outer automorphisms[2].

New contributions:

- An implementation in GAP of the known algorithms of A_2.
- A new algorithm for computing generating sets of centralizers of automorphisms of A_2.

[1] Dahmani et al., "The conjugacy problem for $\mathrm{Out}(F_3)$"
[2] Los, "On the conjugacy problem for automorphisms of free groups"

AAG cryptosystem

Let $G = \langle g_1, \ldots, g_n \rangle$ be a group, then the AAG[3] cryptosystem is defined as the following protocol.

- **Public key:** $\{g_1, \ldots, g_n\}$.
- **Private keys:** $a, b \in G$.
- **Shared secret key:** $k = a^{-1}a^b$.

  Alice sends to Bob the following elements: $g_1^a, \ldots g_n^a$.

  Bob sends to Alice the following elements: $g_1^b, \ldots g_n^b$.

Originally proposed for braid groups, but they are vulnerable to several attacks[4]. Another suggested family of platform groups is polycyclic groups[5].

[3] I Anshel, M Anshel, and D Goldfeld. "An algebraic method for public-key cryptography". In: *Mathematical Research Letters* 6.3 (1999), pp. 287–291

[4] D Garber. *Braid Group Cryptography*. 2008

[5] B. Eick and Kahrobaei D. *Polycyclic groups: A new platform for cryptology?* 2004

Problems

We consider practical algorithms for the following problems in A_2, where $\alpha, \beta \in \mathsf{A}_2$ and $g \in F_2$:

- The **basis fixed point problem**. It asks how to construct a free basis of the fixed point subgroup of α, $\mathrm{Fix}(\alpha) = \{v \in F_2 \mid \alpha(v) = v\}$.
- The **twisted fixed point problem**. It asks if there exists $h \in F_2$ such that $\alpha(h) = hg$ and, if so, to determine such an h.
- The **conjugacy problem for automorphisms**. It asks if there exists $\gamma \in \mathsf{A}_2$ such that $\alpha^\gamma = \beta$ and, if so, to determine such γ.
- The **centralizer problem for automorphisms**. It asks to construct a generating set for $C_{\mathsf{A}_2}(\alpha) = \{\beta \in \mathsf{A}_2 \mid \alpha\beta = \beta\alpha\}$.

Matrix groups

Theorem 2

There exists a practical algorithm that given $A \in \mathrm{GL}_2(\mathbb{Z})$ computes a set of generators S of $C_{\mathrm{GL}_2(\mathbb{Z})}(A)$.[6]

Remark

Let $A \in \mathrm{GL}_2(\mathbb{Z})$ be such that $A \neq \pm I$. Then $C_{\mathrm{GL}_2(\mathbb{Z})}(A)$ is generated by $\langle B \rangle$ or by $\langle -I, B \rangle$ for $B \in \mathrm{GL}_2(\mathbb{Z})$. The algorithm described in Theorem 2 can be modified to find $n \in \mathbb{Z}$ such that $B^n = A$.

[6] T. Velten. "Centralizers in Integral Matrix Groups". Master's thesis. Technische Universität Braunschweig, 2023.

Matrix groups

Theorem 3

Let $A, B \in \mathrm{GL}_2(\mathbb{Z})$. Then

1. *There exists a practical algorithm that decides whether A and B are conjugated, and if so, computes $C \in \mathrm{GL}_2(\mathbb{Z})$ such that $C^{-1}AC = B$.*[7]
2. *If $A \in \mathrm{SL}_2(\mathbb{Z})$ and $H = \langle A_1, \ldots, A_n \rangle \leq \mathrm{SL}_2(\mathbb{Z})$, then there exists a practical algorithm that decides whether $A \in H$, and if so, computes a word w in $\{A_1, \ldots, A_n\}$ that represents A.*[8]

[7] A. Behn and A. B. Van der Merwe. "An algorithmic version of the theorem by Latimer and MacDuffee for 2×2 integral matrices". In: *Linear Algebra Appl.* 346 (2002), pp. 1–14

[8] M. Kirschmer and C. Leedham-Green. "Computing with subgroups of the modular group". In: *Glasg. Math. J.* 57.1 (2015), pp. 173–180

Braid groups

Let B_4 denote the braid group on 4 strands. Then B_4 has the following presentation:

$$B_4 = \langle b_1, b_2, b_3 \mid b_2 b_1 b_2 = b_1 b_2 b_1,\ b_3 b_2 b_3 = b_2 b_3 b_2,\ b_1 b_3 = b_3 b_1 \rangle, \tag{1}$$

[9] E. A. El-Rifai and H. R. Morton. "Algorithms for positive braids". In: *Quart. J. Math. Oxford Ser. (2)* 45.180 (1994), pp. 479–497.

Braid groups

Let B_4 denote the braid group on 4 strands. Then B_4 has the following presentation:

$$B_4 = \langle b_1, b_2, b_3 \mid b_2 b_1 b_2 = b_1 b_2 b_1,\ b_3 b_2 b_3 = b_2 b_3 b_2,\ b_1 b_3 = b_3 b_1 \rangle, \tag{1}$$

Theorem 4 (El-Rifai and Morton[9])

Let $a \in B_4$. Then a admits a unique expression called the left canonical form,

$$a = \Delta^p a_1 a_2 \cdots a_l$$

where $p \in \mathbb{Z}$ and each a_i is a simple braid.

[9] El-Rifai and Morton, "Algorithms for positive braids".

Algorithms for braids

Theorem 5

Let $a, b \in B_4$. Then

1. *There exists a practical algorithm that computes the left canonical form of a.*[10]
2. *There exists a practical algorithm that computes a set of generators of $C_{B_4}(a)$.* [11]
3. *There exists a practical algorithm that decides whether a and b are conjugated, and if so, computes $c \in B_4$ such that $a^c = b$.* [12]

[10] El-Rifai and Morton, "Algorithms for positive braids".

[11] N. Franco and J. González-Meneses. "Computation of centralizers in braid groups and Garside groups". In: *Proceedings of the International Conference on Algebraic Geometry and Singularities (Spanish) (Sevilla, 2001)*. Vol. 19. 2. 2003, pp. 367–384.

[12] N Franco and J. González-Meneses. "Conjugacy problem for braid groups and Garside groups". In: *J. Algebra* 266.1 (2003), pp. 112–132.

Presentation of A_2

Using the methods of Gersten[13] a presentation of A_2 with 6 generators can be constructed. We simplify the obtained presentation to one with only 4 generators.

$$\begin{aligned} A_2 = \langle \sigma, \phi_1, \phi_2, \phi_3 \mid & \phi_1\phi_3 = \phi_1\phi_3, \quad \phi_2\phi_3\phi_2 = \phi_3\phi_2\phi_3, \quad \phi_2\phi_1\phi_2 = \phi_1\phi_2\phi_1, \\ & (\phi_1\phi_2\phi_3)^4 = 1, \quad \sigma^2 = 1, \quad \phi_1^\sigma = \phi_2, \\ & \phi_3\sigma = \sigma\phi_3^{-1}\phi_2^{-1}\phi_1^{-1}\phi_2\phi_3, \quad \phi_3^{-1}\sigma = \sigma\phi_3^{-1}\phi_2^{-1}\phi_1\phi_2\phi_3\rangle. \end{aligned}$$

Where

$$\sigma = \begin{cases} x \mapsto y, \\ y \mapsto x, \end{cases} \qquad \phi_1 = \begin{cases} x \mapsto xy^{-1}, \\ y \mapsto y, \end{cases} \qquad \phi_2 = \begin{cases} x \mapsto x, \\ y \mapsto yx, \end{cases} \qquad \phi_3 = \begin{cases} x \mapsto y^{-1}x, \\ y \mapsto y. \end{cases}$$

[13] S. M. Gersten. "A presentation for the special automorphism group of a free group". In: *J. Pure Appl. Algebra* 33.3 (1984), pp. 269–279.

Special automorphisms

Theorem 6

There exists a homomorphism Ψ from A_2 to $\mathrm{GL}_2(\mathbb{Z})$ with kernel $\operatorname{Inn} F_2$, that is

$$A_2/\operatorname{Inn} F_2 \cong \mathrm{GL}_2(\mathbb{Z})$$

Denote by SA_2 the subgroup of A_2 consisting of automorphisms that are mapped into $\mathrm{SL}_2(\mathbb{Z})$ under Ψ.

Special automorphisms

SA_2 has the following presentation.

$$SA_2 = \langle \phi_1, \phi_2, \phi_3 \mid \phi_1\phi_3 = \phi_1\phi_3, \quad \phi_2\phi_3\phi_2 = \phi_3\phi_2\phi_3, \quad \phi_2\phi_1\phi_2 = \phi_1\phi_2\phi_1, \\ (\phi_1\phi_2\phi_3)^4 = 1 \rangle.$$

Theorem 7 (Dyer, Formanek, and Grossman[14])

$$SA_2 \cong B_4/Z(B_4).$$

[14] J. L. Dyer, E. Formanek, and E. K. Grossman. "On the linearity of automorphism groups of free groups". In: *Arch. Math. (Basel)* 38.5 (1982), pp. 404–409

Left canonical forms

Theorem 8

Let $\alpha \in A_2$. Then there exists a unique expression, called the left canonical form

$$\alpha = \sigma^{\varepsilon_1}\Delta^{\varepsilon_2}\alpha_1\alpha_2\cdots\alpha_k$$

where $\varepsilon_1, \varepsilon_2 = \{0, 1\}$, $\Delta = \phi_1(\phi_2\phi_1)(\phi_3\phi_2\phi_1)$, and $\alpha_1, \ldots \alpha_k \in \mathsf{SA}_2$ are such that their images under the isomorphism of Theorem 7 are simple braids.

Whitehead algorithm

Theorem 9 (Whitehead algorithm [15])

Given u and v in F_n, there is a practical algorithm that decides whether there exists $\phi \in \mathrm{Aut}(F_n)$ such that $\phi(u) = v$.

Theorem 10

Let $\alpha \in A_2$ and let $w = \alpha(x)$ and $v = \alpha(y)$. If $\beta \in A_2$ is such that $w = \beta(x)$, then there exists a finite chain of Whitehead automorphisms $\tau_1, \ldots, \tau_n$, each fixing x, such that

$$\alpha = \tau_1 \cdots \tau_n \beta.$$

[15] J. H. C. Whitehead. "On equivalent sets of elements in a free group". In: *Ann. of Math. (2)* 37.4 (1936), pp. 782–800

Fixed points

For $\alpha \in \mathsf{A}_2$, let $\mathsf{Fix}(\alpha) = \{x \in F_2 \mid \alpha(x) = x\}$.

Theorem 11 (Bestvina and Handel[16])

Let F_n be a free group of rank n and let $\alpha \in \mathsf{Aut}(F_n)$. Then

$$\mathsf{rk}(\mathsf{Fix}(\alpha)) \leq n.$$

Theorem 12 (Bogopolski[17])

There exists a practical algorithm that given $\alpha \in \mathsf{A}_2$ computes a basis of $\mathsf{Fix}(\alpha)$.

[16] M. Bestvina and M. Handel. "Train tracks and automorphisms of free groups". In: *Ann. of Math. (2)* 135.1 (1992), pp. 1–51

[17] O. Bogopolski. "Classification of automorphisms of the free group of rank 2 by ranks of fixed-point subgroups". In: *J. Group Theory* 3.3 (2000), pp. 339–351

Twisted fixed points

We want to solve the following: given $g \in F_2$ and $\alpha \in A_2$ decide whether there exists $h \in F_2$ such that $\alpha(h) = hg$ and, if so, to determine such an h. There exists an algorithm to solve this problem but is impractical. However, we have the following

Theorem 13 (Bogopolski[18])

There exists a practical algorithm that given $g \in F_2$ and $\alpha \in A_2$ decides whether there exists $h \in \mathrm{Fix}(\alpha^2)$ such that $\alpha(h) = hg$ and, if so, to determine such an h.

Theorem 14

There exists a practical algorithm that given $g \in F_2$ and $\alpha \in A_2$ of order 2 decides whether there exists $h \in F_2$ such that $\alpha(h) = hg$ and, if so, to determine such an h.

[18] Bogopolski, "Classification of automorphisms of the free group of rank 2 by ranks of fixed-point subgroups"

Conjugacy problem

For a braid $a \in B_4$, let $\exp(a)$ denote the sum of the exponents of the generators in its left canonical form.

Algorithm

Given $\alpha, \beta \in \mathrm{SA}_2$, the following steps determine whether α and β are conjugate and if so, compute $\delta \in \mathrm{SA}_2$ such that $\alpha^\delta = \beta$.

(1) Using the isomorphism from Theorem 7, compute $b_1, b_2 \in B_4$ such that $\alpha \mapsto b_1 Z(B_4)$ and $\beta \mapsto b_2 Z(B_4)$.

(2) If $\exp(b_1) \not\equiv \exp(b_2) \mod 12$, then b_1 and b_2 are not conjugate in $B_4/Z(B_4)$. Otherwise, multiply b_2 by an appropriate power of Δ^2 so that $\exp(b_1) = \exp(b_2)$.

(3) By Theorem 5, we can determine whether b_1 and b_2 are conjugate. If they are not, return false. Otherwise, let $c \in B_4$ be such that $b_1^c = b_2$. Return $\delta \in \mathrm{SA}_2$ such that $\delta \mapsto cZ(B_4)$ under the isomorphism of Theorem 7.

Conjugacy problem

Theorem 15 (Bogopolski[19])

Let $\alpha, \beta \in \mathsf{A}_2$. Assume that $\beta_0 \in A_2$ satisfies $C_{\mathsf{GL}_2(\mathbb{Z})}(\Psi(\beta)) = \langle -\Psi(\beta_0), \Psi(\beta_0) \rangle$ and $k \in \mathbb{Z}$ is the maximal integer such that $\Psi(\beta) = \Psi(\beta_0)^k$. Then α and β are conjugate in A_2 if and only if:

1. *There exists $\delta \in \mathsf{A}_2$ such that $\Psi(\alpha)^{\Psi(\delta)} = \Psi(\beta)$. Define $\phi_v = \beta^{-1}\alpha^\delta$.*
2. *There exists $\varepsilon \in \{0, 1\}$ and $e \in \{0, \dots, k-1\}$ such that for $\beta_1 = \sigma_2^\varepsilon \beta_0^e$, $\phi_z = \beta_1^{-1}\beta^{-1}\beta_1\beta\phi_v$ and $\alpha_1 = \beta^{\beta_1}$ the following conditions hold.*
   - i. *α_1^2 and $(\alpha_1\phi_z)^2$ are conjugated.*
   - ii. *$\Psi(\theta) \in \Psi(C_{\mathsf{SA}_2}(\alpha_1^2))$ where θ is a conjugating element between α_1^2 and $(\alpha_1\phi_z)^2$.*
   - iii. *There exists $h \in \mathsf{Fix}(\alpha_1^2)$ such that $\alpha_1(h) = hg$ for $g \in F_2$ defined as $\phi_g = \phi_f\phi_z^{-1}\alpha_1^{-1}\phi_f^{-1}\alpha_1$ where $\phi_f = \theta_0\theta$ and $\theta_0 \in C_{\mathsf{SA}_2}(\alpha_1^2)$ such that $\Psi(\theta_0) = \Psi(\theta^{-1})$.*

[19] O. Bogopolski. "On the conjugacy problem for automorphisms of free groups". In: *Algebra i Logika* 28.1 (1989), pp. 18–28, 122

Centralizers of automorphisms

Corollary 16

Let $\alpha \in \mathsf{SA}_2$. *Then*

$$C_{\mathsf{SA}_2}(\alpha) \cong C_{B_4}(b)/Z(B_4),$$

where b *is any preimage of* α *in* B_4 *under the isomorphism of Theorem 7.*

Lemma 17

Let $\alpha \in \mathsf{A}_2$. *Then* $\mathsf{Fix}(\alpha) = \{z \in F_2 \mid \phi_z \in C_{\mathsf{A}_2}(\alpha)\}$.

Lemma 18

Let $\alpha \in \mathsf{A}_2$, *then*

$$C_{\mathsf{A}_2}(\alpha)/\mathsf{Fix}(\alpha) \lesssim C_{\mathsf{GL}_2(\mathbb{Z})}(\Psi(\alpha)).$$

Centralizers of automorphisms

Lemma 19

Let $\alpha \in \mathsf{A}_2$ be such that $C_{\mathsf{GL}_2(\mathbb{Z})}(\Psi(\alpha)) \cong C_2 \times \mathbb{Z}$. We can assume that $C_{\mathsf{GL}_2(\mathbb{Z})}(\Psi(\alpha)) = \langle -I, B \rangle$ where $B \in \mathsf{GL}_2(\mathbb{Z})$ is such that there exists a maximal $n \in \mathbb{Z}$ such that $B^n = \Psi(\alpha)$. If $\beta \in \mathsf{A}_2$ is such that $\Psi(\beta) = B$, then $C_{\mathsf{A}_2}(\alpha)/\operatorname{Fix}(\alpha)$ is generated by one of the following:

- $\langle \beta^e \rangle$ *with e a divisor of n.*
- $\langle \sigma_2 \beta^e \rangle$ *with $2e$ a divisor of n.*
- $\langle \sigma_2, \beta^e \rangle$ *with e a divisor of n.*

Centralizers of automorphisms

Lemma 19

Let $\alpha \in \mathsf{A}_2$ be such that $C_{\mathsf{GL}_2(\mathbb{Z})}(\Psi(\alpha)) \cong C_2 \times \mathbb{Z}$. We can assume that $C_{\mathsf{GL}_2(\mathbb{Z})}(\Psi(\alpha)) = \langle -I, B \rangle$ where $B \in \mathsf{GL}_2(\mathbb{Z})$ is such that there exists a maximal $n \in \mathbb{Z}$ such that $B^n = \Psi(\alpha)$. If $\beta \in \mathsf{A}_2$ is such that $\Psi(\beta) = B$, then $C_{\mathsf{A}_2}(\alpha)/\operatorname{Fix}(\alpha)$ is generated by one of the following:

- $\langle \beta^e \rangle$ *with e a divisor of n.*
- $\langle \sigma_2 \beta^e \rangle$ *with $2e$ a divisor of n.*
- $\langle \sigma_2, \beta^e \rangle$ *with e a divisor of n.*

Theorem 20

Given $\alpha \in \mathsf{A}_2$, there exists a practical algorithm that computes a set of generators of $C_{\mathsf{A}_2}(\alpha)$.