THE MATHIEU GROUP M_{23} IS A GALOIS GROUP OVER $\mathbb{Q}$

XIAOYU HUANG, BLAKE JACKSON, KYU-HWAN LEE, BJORN POONEN, RACHEL PRIES, AND SHAOWU ZHANG

Abstract. Researchers studying the inverse Galois problem realized 25 of the 26 sporadic finite simple groups as Galois groups over $\mathbb{Q}$ during 1984–1989. We complete this program by proving that the last remaining sporadic group, the Mathieu group M_{23}, occurs as a Galois group over $\mathbb{Q}$. In fact, we produce an explicit degree 23 polynomial with rational coefficients whose splitting field has Galois group M_{23} over $\mathbb{Q}$. To accomplish this, we discover an unanticipated splitting of the Nielsen class associated to a non-rigid triple of conjugacy classes of M_{23}. We compute the Belyi maps associated with this Nielsen class to construct an explicit regular Galois extension of $\mathbb{Q}(t)$ with Galois group M_{23}. Essential for our computation is the numerical Belyi map algorithm developed and implemented by Costa, Klug, Musty, Schiavone, Sijsling, and Voight, inspired by ideas of Hejhal and Stark. As a bonus, one specialization of the regular extension yields an M_{22}-extension of $\mathbb{Q}$.

1. Introduction

1.1. **The inverse Galois problem.** The inverse Galois problem asks whether or not every finite group G occurs as the Galois group of some finite Galois extension of $\mathbb{Q}$ [Ser92, MM18, Wit25]. In particular, one can ask the question for finite simple groups, which fall into 18 infinite families and 26 "sporadic" groups. During 1984–1989, 25 of the 26 sporadic groups were realized as Galois groups over $\mathbb{Q}$.[1] The last sporadic group, the Mathieu group M_{23}, remained unrealized, despite many attempts; see Section 1.3. In this paper, we realize this group.

Theorem 1.1. *There exists a Galois extension of $\mathbb{Q}$ with Galois group M_{23}.*

Date: October 4, 2026.

2020 *Mathematics Subject Classification.* Primary 12F12; Secondary 11G32, 11R32, 12F10, 14H30, 14Q05.

Key words and phrases. Inverse Galois problem, Mathieu group, sporadic group, Belyi map, rigidity method.

X.H. was supported in part by an AMS–Simons Travel Grant and NSF grant DMS-2617281. B.J. was supported by ICARM through NSF grant DMS-2425401. K.-H.L. was supported by NSF grant DMS-2617278. B.P. was supported in part by NSF grant DMS-2601551 and Simons Foundation grant #402472. R.P. was supported by NSF grant DMS-2200418. Several authors received travel support from AIM.

[1]Strictly speaking, the baby monster B was realized only later, since there was a calculation error in the original construction of [Hun86], according to [MM18, p. 161].

Example 1.2. The splitting field of

$$\begin{aligned} x^{23} &- 184x^{21} - 1150x^{20} + 26151x^{19} + 18400x^{18} - 1808490x^{17} \\ &+ 1545462x^{16} + 67672923x^{15} - 42732528x^{14} - 1333395744x^{13} \\ &+ 290615166x^{12} + 10550424369x^{11} + 3700476348x^{10} + 35123826654x^{9} \\ &- 194398310718x^{8} - 1023887308293x^{7} + 3961650395556x^{6} \\ &+ 1949980486716x^{5} - 28142323927002x^{4} + 53599151839311x^{3} \\ &- 46185312415788x^{2} + 19169943578802x - 3150159884154 \end{aligned}$$

is a Galois extension of $\mathbb{Q}$ with Galois group M_{23}, unramified outside $\{2, 3, 23\}$. We certified that the Galois group is M_{23} with the `GaloisProof` command in Magma [BCP97].[2]

Prior to our work, it was known that 4952 of the 4953 transitive permutation groups of degree ≤ 23 were realizable over $\mathbb{Q}$ [vBCE+26]. Theorem 1.1 realizes the last remaining group in this program too. According to [SAI26], all 25000 transitive permutation groups of degree 24 have now been realized too.

There remain infinitely many finite simple groups of Lie type that have not been realized over $\mathbb{Q}$, especially those associated to non-prime finite fields. For a list of the unrealized ones of size $\leq 10^8$, see [Zyw25]. The inverse Galois problem for arbitrary finite groups remains far from being resolved.

1.2. **Regular Galois extensions.** A ***G*-extension** of a field k is a Galois field extension L/k, together with an isomorphism $\mathrm{Gal}(L/k) \simeq G$. An extension of k is **regular** if it contains no nontrivial algebraic extension of k (and is linearly disjoint from $k^{1/p}$ over k if k is of characteristic p). By a slight abuse of terminology, we call a finite extension of $k(t)$ **regular** if it is regular over k. If $G \neq \{1\}$ and a regular G-extension of $\mathbb{Q}(t)$ exists, then, by Hilbert's irreducibility theorem, specializing t to different rational numbers yields infinitely many G-extensions of $\mathbb{Q}$. Thus, to prove Theorem 1.1, we prove the following stronger result.

Theorem 1.3. *There exists a regular Galois extension of $\mathbb{Q}(t)$ with Galois group M_{23}.*

1.3. **Previous work.** The rigidity method, originally developed in [Shi74, Fri77, Bel79, Mat79, Mat84, Mat85, Tho84], was instrumental for constructing regular Galois extensions of $\mathbb{Q}(t)$. Variants of this method, often involving significant new ideas such as the braid group method of [Mat89, Mat91, FV91], were used to construct regular G-extensions of $\mathbb{Q}(t)$ for all the sporadic groups G except M_{23} [Tho84, Mat85, HS85, Hun86, HSM86, MZM86, MZM87, Mal88, Pah88, Pah89]; see [MM18, II.9] for a detailed exposition.

Prior attempts to realize M_{23} over $\mathbb{Q}$ resulted only in realizations over other fields:

- Hoyden-Siedersleben [HS85] and Häfner [Häf87] used regular M_{24}-extensions of $k(t)$ to construct regular M_{23}-extensions of $k(t)$ for $k = \mathbb{Q}(\sqrt{-23})$ and $k = \mathbb{Q}(\sqrt{-7})$, respectively.
- Granboulan [Gra96] used another M_{24}-extension to construct a regular M_{23}-extension over $k(t)$ for any field k over which a certain conic C has a k-point. Unfortunately, C has no $\mathbb{Q}$-point.
- Elkies [Elk13] calculated the four degree 23 polynomials $P(x) \in \mathbb{C}[x]$ (up to affine equivalence) such that the Galois group of $P(x) - t$ over $\mathbb{C}(t)$ is M_{23}. Each such $P(x)$

[2]Our code is available at `https://github.com/shaowuz/m23isgalois`.

has coefficients in a degree 4 number field F, so one obtains a regular M_{23}-extension of $F(t)$.

For more information and explicit computation of Hurwitz spaces for M_{23}-covers, see [Kön14], [Häf22], and [Seg25]. Finally, the problem of realizing M_{23} over $\mathbb{Q}$ was on the Epoch AI FrontierMath open problem list [Epo26] as a benchmark for AI capability since at least January 2026.

1.4. **Outline of our approach.**

1. The group M_{23} has 17 conjugacy classes, traditionally labeled by the order of a representative element followed by an uppercase letter to distinguish classes of the same order. The group $\mathfrak{G}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of conjugacy classes of M_{23}. It fixes the class $2 := 2\mathrm{A}$, and acts on 23A and 23B nontrivially through the quotient $\mathrm{Gal}(K/\mathbb{Q})$, where $K := \mathbb{Q}(\sqrt{-23})$. We explain in Section 3 why we looked at *these* classes.
2. Let $S \subset \mathbb{P}^1_{\mathbb{Q}}$ be the finite étale $\mathbb{Q}$-scheme whose geometric points are $0, \sqrt{-23}, -\sqrt{-23}$.
3. The Riemann existence theorem, together with a calculation in M_{23}, shows that there are exactly seven M_{23}-covers $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ ramified only over S with local monodromy (2,23A,23B). The quotient of each $Y_{\mathbb{C}}$ by the one-point stabilizer M_{22} is a genus 4 curve $X_{\mathbb{C}}$, and $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is the Galois closure of the degree 23 cover $X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$.
4. We compute these seven curves $X_{\mathbb{C}}$ numerically using the BelyiDB package [CMSV26], and recognize coefficients as algebraic numbers to compute *candidates* $X_1, \ldots, X_7$ for these curves over $\overline{\mathbb{Q}}$.
5. To verify the X_i, we construct a degree 23 map $X_i \to \mathbb{P}^1$ for each i, verify that it is ramified only over S with local monodromy (2,23A,23B), verify that its geometric monodromy group is M_{23} by working modulo a prime of good reduction, and verify that $X_1, \ldots, X_7$ are pairwise non-isomorphic over $\overline{\mathbb{Q}}$.
6. One might expect $\mathfrak{G}_{\mathbb{Q}}$ to act transitively on $\{X_1, \ldots, X_7\}$. Miraculously, instead the $\mathfrak{G}_{\mathbb{Q}}$-orbits have sizes 6 and 1! We do not have a conceptual explanation for this.
7. We prove that the $\mathfrak{G}_{\mathbb{Q}}$-fixed point descends to a cover $X \xrightarrow{t} \mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{Q}$ by computing an explicit birational map from X to a (singular) plane curve defined over $\mathbb{Q}$ under which t corresponds to the first coordinate projection.
8. Taking the Galois closure of the corresponding degree 23 field extension gives a regular M_{23}-extension of $\mathbb{Q}(t)$.

Details will be given in the subsequent sections.

Remark 1.4. That the M_{23}-cover corresponding to the $\mathfrak{G}_{\mathbb{Q}}$-fixed point descends to $\mathbb{Q}$ also follows from [CH85, Proposition 2.8(c)], since the center $Z(M_{23})$ is trivial.

1.5. **Consequences.**

Let k be a number field. Call a collection of G-extensions of k **mutually independent** if, for any $r \geq 1$, any r distinct extensions from the collection generate a G^r-extension of k.

Corollary 1.5. *Let G be a sporadic finite simple group. Let k be any number field.*

(a) *There exists a regular G-extension of $k(t)$.*
(b) *There exists a G-extension of k.*
(c) *There exists a G-extension of $\mathbb{Q}$ linearly disjoint from k.*
(d) *There exists an infinite collection of mutually independent G-extensions of k.*

Proof. Part (a) over $\mathbb{Q}$ is the combination of Theorem 1.3 and the work cited in Section 1.3. Take a compositum to get (a) over k. For (b,c,d) and other consequences of (a), see [Ser92, §3.3–3.4] and [Ser97, §10.1]. □

2. The rigidity method

2.1. **G-covers of the projective line.** Let G be a nonabelian finite simple group, so $Z(G) = 1$. Let $\mathrm{Inn}(G)$ be the group of inner automorphisms of G, so $\mathrm{Inn}(G) \simeq G$, and $\mathrm{Inn}(G)$ acts on G, on the right, say: g acts as $x \mapsto g^{-1}xg$. The set $\mathcal{C} := G/\mathrm{Inn}(G)$ is the set of conjugacy classes of G. Let $n \geq 1$ be such that $g^n = 1$ for all $g \in G$.

Let k be a field of characteristic 0. For each $m \geq 1$, let $\mu_m = \{x \in \overline{k}^\times : x^m = 1\}$. Let $\mathfrak{G}_k = \mathrm{Gal}(\overline{k}/k)$. Let $\epsilon\colon \mathfrak{G}_k \to \mathrm{Aut}(\mu_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ be the cyclotomic character describing the $\mathfrak{G}_k$-action on nth roots of unity. A choice of generator $\zeta \in \mu_n$ determines a bijection $\mathrm{Hom}(\mu_n, G) \simeq \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G) = G$. To make this bijection $\mathfrak{G}_k$-*equivariant*, we let $\sigma \in \mathfrak{G}_k$ act trivially on the target G in $\mathrm{Hom}(\mu_n, G)$ and as $g \mapsto g^{\epsilon(\sigma)^{-1}}$ on the set G on the right. Taking $\mathrm{Inn}(G)$-orbits, the latter action induces a $\mathfrak{G}_k$-action on $\mathcal{C}$.

A **curve** over k is a 1-dimensional smooth projective geometrically connected scheme of finite type over k. A **G-cover of $\mathbb{P}^1_k$** is a (possibly ramified) Galois morphism of curves $Y \to \mathbb{P}^1_k$ together with an isomorphism $\mathrm{Gal}(k(Y)/k(\mathbb{P}^1)) \simeq G$. Our convention is that groups act on the left on function field elements and on the right on geometric objects, so G acts on the left on $k(Y)$, and on the right on Y. An **isomorphism of G-covers** $Y \to \mathbb{P}^1_k$ and $Y' \to \mathbb{P}^1_k$ is a G-equivariant isomorphism $Y \to Y'$ over $\mathbb{P}^1_k$.

2.2. **Local monodromy.** Let $D \subset \mathbb{C}$ be the open unit disk. Let $D^\times = D - \{0\}$. We have $\mathbb{Z} \xrightarrow{\sim} \pi_1(D^\times)$ sending 1 to the standard counterclockwise generator.

Suppose that $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is a G-cover with branch locus S. For each $s \in S$, we have an analytic open embedding $D \to \mathbb{P}^1_{\mathbb{C}}$ sending 0 to s, such that s is the only point of S in the image; ignoring basepoints, this induces

$$\mathbb{Z} \simeq \pi_1(D^\times) \to \pi_1(\mathbb{P}^1(\mathbb{C}) - S) \twoheadrightarrow G$$

sending 1 to a generator of the local monodromy group (inertia group) at s. Changing basepoints conjugates the generator by an element of G, so we obtain a well-defined conjugacy class for each s, hence a map $\mathfrak{c}\colon S \to \mathcal{C}$, which we call the **local monodromy**.

Algebraically, if u is an analytic uniformizer at $s \in \mathbb{P}^1(\mathbb{C})$, the completion of $\mathbb{C}(\mathbb{P}^1)$ at s is $\mathbb{C}((u))$, and we have analogous homomorphisms involving étale fundamental groups

$$\hat{\mathbb{Z}}(1) \simeq \pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{C}((u))) \to \pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} - S) \twoheadrightarrow G,$$

factoring through μ_n, defined up to conjugation by elements of G.

Thus we get a canonical map

$$\mathfrak{c}\colon S \to \mathrm{Hom}(\mu_n, G)/\mathrm{Inn}(G) \simeq \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, G)/\mathrm{Inn}(G) \simeq G/\mathrm{Inn}(G) = \mathcal{C},$$

depending only on a choice of isomorphism $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$; we fix $e^{2\pi i/n} \mapsto 1$.

If $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is the base change of a G-cover $Y \to \mathbb{P}^1_{\mathbb{Q}}$, then S may be viewed as a finite étale subscheme of $\mathbb{P}^1_{\mathbb{Q}}$, and $\mathfrak{c}\colon S(\overline{\mathbb{Q}}) \to \mathcal{C}$ is $\mathfrak{G}_{\mathbb{Q}}$-equivariant. What we just described is Fried's branch cycle argument [Fri77, pp. 62–64].

2.3. **Rigidity.** See [FV91], especially Corollary 1, for details on the theory in this section. Fix a finite étale subscheme $S \subset \mathbb{P}^1_{\mathbb{Q}}$ and a $\mathfrak{G}_{\mathbb{Q}}$-equivariant map $\mathfrak{c}\colon S(\overline{\mathbb{Q}}) \to \mathcal{C}$. Write $S(\overline{\mathbb{Q}}) = \{s_1, \dots, s_r\}$, and $C_i := \mathfrak{c}(s_i)$ for $i = 1, \dots, r$.

Let $\mathcal{H}_{\mathfrak{c}}$ be the 0-dimensional Hurwitz scheme over $\mathbb{Q}$ parameterizing G-covers of $\mathbb{P}^1$ unramified outside S with local monodromy $\mathfrak{c}$. Because $Z(G) = 1$, $\mathcal{H}_{\mathfrak{c}}$ is a fine moduli space [CH85, Proposition 1.4(b)]. Define

$$\begin{aligned}\bar{\Sigma}_{\mathfrak{c}} &:= \{(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r : g_1 \cdots g_r = 1\},\\ \Sigma_{\mathfrak{c}} &:= \{(g_1, \dots, g_r) \in \bar{\Sigma}_{\mathfrak{c}} : g_1, \dots, g_r \text{ generate } G\},\\ \mathrm{Ni}_{\mathfrak{c}} &:= \Sigma_{\mathfrak{c}} / \operatorname{Inn}(G);\end{aligned}$$

here $g \in G \simeq \operatorname{Inn}(G)$ acts on r-tuples by simultaneous conjugation. The set $\mathrm{Ni}_{\mathfrak{c}}$ is called the **Nielsen class** of $\mathfrak{c}$. By the Riemann existence theorem, $\mathcal{H}_{\mathfrak{c}}(\mathbb{C})$ is in bijection with $\mathrm{Ni}_{\mathfrak{c}}$.

The size $|\bar{\Sigma}_{\mathfrak{c}}|$ can be computed from the character table of G; an inclusion–exclusion gives $|\Sigma_{\mathfrak{c}}|$; since the group $\operatorname{Inn}(G) \simeq G$ acts freely on $\Sigma_{\mathfrak{c}}$, dividing by $|G|$ gives $|\mathrm{Ni}_{\mathfrak{c}}|$, which depends only on the multiset $\{C_1, \dots, C_r\}$; see [Ser92, §7.2 and §7.3] for an exposition. When the branch locus is invariant under complex conjugation, Hurwitz described the action of complex conjugation on $\mathrm{Ni}_{\mathfrak{c}}$ in group-theoretic terms [MM18, Theorem 1.1.2]. The action of $\mathfrak{G}_{\mathbb{Q}}$ is more mysterious.

We restrict to the case $r = 3$. If $|\mathrm{Ni}_{\mathfrak{c}}| = 1$, then the triple (C_1, C_2, C_3) is called **rigid**; in that case, $\mathcal{H}_{\mathfrak{c}} \simeq \operatorname{Spec} \mathbb{Q}$ and the unique point corresponds to a G-cover $Y \to \mathbb{P}^1_{\mathbb{Q}}$ with local monodromy $\mathfrak{c}$.

3. The Mathieu group M_{23}

3.1. **A Nielsen class.** The Mathieu group M_{23} is a finite simple group of order $10{,}200{,}960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. It is the automorphism group of the unique Steiner system $S(4, 7, 23)$. It is a 4-transitive subgroup of S_{23}, generated by the permutations g_1, g_2 below. It has 17 conjugacy classes:

$$1,\quad 2,\quad 3,\quad 4,\quad 5,\quad 6,\quad 7\mathrm{A}, 7\mathrm{B},\quad 8,\quad 11\mathrm{A}, 11\mathrm{B},\quad 14\mathrm{A}, 14\mathrm{B},\quad 15\mathrm{A}, 15\mathrm{B},\quad 23\mathrm{A}, 23\mathrm{B}$$

(we drop the A in the label when there is a unique conjugacy class of elements of a particular order). We calculate $|\mathrm{Ni}_{\mathfrak{c}}|$ for all 86 $\mathfrak{G}_{\mathbb{Q}}$-stable 3-element multisets of nontrivial classes in $\mathcal{C}$, using character tables as in Section 2.3. We find that $|\mathrm{Ni}_{\mathfrak{c}}| = 0$ for 30 of these, but the value of $|\mathrm{Ni}_{\mathfrak{c}}|$ is never 1, so the rigidity method fails.

We next investigate the multiset for which $|\mathrm{Ni}_{\mathfrak{c}}|$ has smallest positive size. This is $\{2, 23\mathrm{A}, 23\mathrm{B}\}$, with $|\mathrm{Ni}_{\mathfrak{c}}| = 7$. In fact, M_{23} is small enough that a computer can quickly list triples representing all the elements of $\mathrm{Ni}_{\mathfrak{c}}$. We fix the following such triple of permutations in S_{23}:[3]

$$\begin{aligned}g_1 &:= (1, 11)(2, 23)(3, 8)(4, 16)(5, 21)(7, 20)(15, 19)(18, 22),\\ g_2 &:= (1, 2, 3, 4, 10, 11, 12, 7, 19, 18, 8, 6, 9, 16, 17, 21, 22, 5, 14, 20, 13, 15, 23),\\ g_3 &:= (1, 2, 11, 10, 16, 9, 6, 3, 23, 19, 20, 14, 21, 17, 4, 8, 22, 5, 18, 15, 13, 7, 12).\end{aligned}$$

Let S be the finite étale $\mathbb{Q}$-scheme whose geometric points are $0, \sqrt{-23}, -\sqrt{-23}$. Let $\mathfrak{c}\colon S(\overline{\mathbb{Q}}) \to \mathcal{C}$ send these points to classes 2, 23A, 23B, respectively. This $\mathfrak{c}$ is $\mathfrak{G}_{\mathbb{Q}}$-equivariant.

[3]We follow Magma's convention that S_{23} acts on the right on $\{1, \dots, 23\}$. For example, applying $g_1 g_2$ to 5 yields 22, not 14.

We have $(g_1, g_2, g_3) \in \Sigma_{\mathfrak{c}}$, representing a class in $\mathrm{Ni}_{\mathfrak{c}}$. By [MM18, Theorem 1.1.2], the map $(g_1, g_2, g_3) \mapsto (g_1^{-1}, g_3^{-1}, g_2^{-1})$ on $\Sigma_{\mathfrak{c}}$ induces complex conjugation on $\mathrm{Ni}_{\mathfrak{c}}$; thus we compute that the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-orbits in $\mathrm{Ni}_{\mathfrak{c}}$ have sizes $1, 1, 1, 2, 2$, though we will not need this fact.

Let $Y_{\mathbb{C}} \xrightarrow{\phi} \mathbb{P}^1_{\mathbb{C}}$ be the corresponding M_{23}-cover. Let $M_{22} := \mathrm{Stab}_{M_{23}}(1)$, where $M_{23} \leq S_{23}$ acts on $\{1, \ldots, 23\}$. Let $X_{\mathbb{C}}$ be the (variety) quotient $Y_{\mathbb{C}}/M_{22}$, so ϕ factors as $Y_{\mathbb{C}} \to X_{\mathbb{C}} \xrightarrow{t} \mathbb{P}^1_{\mathbb{C}}$. Then $X_{\mathbb{C}} \xrightarrow{t} \mathbb{P}^1_{\mathbb{C}}$ is a *non-Galois* degree 23 cover branched over $S(\mathbb{C})$, and its Galois closure is $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. Since $|\mathrm{Ni}_{\mathfrak{c}}| = 7$, and $\mathcal{H}_{\mathfrak{c}}$ is a fine moduli space, the cover $X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ descends to a cover $X_E \to \mathbb{P}^1_E$ defined over a number field E of degree ≤ 7 over $\mathbb{Q}$.

Lemma 3.1. *The genus g_X of $X_{\mathbb{C}}$ is 4.*

Proof. The ramification indices at the ramification points of $t\colon X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ are the lengths of the cycles in g_1, g_2, g_3, so the degree of the ramification divisor is $8(2-1)+(23-1)+(23-1) = 52$. The Riemann–Hurwitz formula gives $2g_X - 2 = 23(-2) + 52$, so $g_X = 4$. □

3.2. **A numerical Belyi map.** Model the hyperbolic plane by the open unit disk D. Let q denote the standard coordinate on D, and let $d(z, w)$ denote the hyperbolic distance between $z, w \in D$. Given $\theta \in (0, \pi/4)$, define

$$a := e^{-i\theta}\sqrt{\tan\left(\frac{\pi}{4} - \theta\right)}, \qquad b := 0, \qquad c := \sqrt{\cos 2\theta}.$$

Lemma 3.2. *The points a, b, c are the vertices of a hyperbolic triangle in D with corresponding interior angles $\pi/2$, θ, θ.*

Proof. Note that $|a|, |b|, |c| < 1$, and a does not lie on the geodesic through b and c, so a, b, c are the vertices of a hyperbolic triangle T_{abc} in D. Lengths of two of its sides satisfy

$$\cosh d(b, a) = \frac{1 + |a|^2}{1 - |a|^2} = \frac{1 + \frac{1-\tan\theta}{1+\tan\theta}}{1 - \frac{1-\tan\theta}{1+\tan\theta}} = \cot\theta, \quad \cosh d(b, c) = \frac{1 + |c|^2}{1 - |c|^2} = \frac{1 + \cos 2\theta}{1 - \cos 2\theta} = \cot^2\theta.$$

On the other hand, since $\pi/2 + \theta + \theta < \pi$, there exists a hyperbolic triangle $T_{\pi/2,\theta,\theta}$ with angles $\pi/2, \theta, \theta$ [Bea83, Theorem 7.16.2]. By [Bea83, Theorem 7.11.3], its leg lengths ℓ and hypotenuse h satisfy $\cosh\ell = \cot\theta$ and $\cosh h = \cot^2\theta$. Moreover, $\angle b = \arg(c) - \arg(a) = \theta$. By side-angle-side, $T_{abc} \cong T_{\pi/2,\theta,\theta}$. Thus $\angle a = \pi/2$ and $\angle c = \theta$. □

Set $\theta := \pi/23$. Let Δ be the triangle group generated by counterclockwise hyperbolic rotations by angles $2\pi/2$, $2\pi/23$, $2\pi/23$ around a, b, c:

$$\Delta := \langle\, \delta_a, \delta_b, \delta_c \mid \delta_a^2 = \delta_b^{23} = \delta_c^{23} = \delta_a\delta_b\delta_c = 1 \,\rangle.^4$$

Let $\psi\colon \Delta \to M_{23}$ be the surjection sending $\delta_a, \delta_b, \delta_c$ to g_1, g_2, g_3, respectively. Let $\Gamma := \psi^{-1}(M_{22}) \leq \Delta$. Then $D/\Gamma \to D/\Delta$ is the desired cover $X_{\mathbb{C}} \xrightarrow{t} \mathbb{P}^1_{\mathbb{C}}$ with monodromy given by (g_1, g_2, g_3). Let a', b', c' be the images of a, b, c under $D \twoheadrightarrow X_{\mathbb{C}}$.

Let $E' := E(\sqrt{-23}) \subset \mathbb{C}$. Let $X_{E'} := X_E \times_E E'$.

Lemma 3.3. *We have $b' \in X_E(E')$, and q corresponds to an analytic uniformizer at b'.*

[4]The papers [KMSV14, MSSV19] write $\delta_c\delta_b\delta_a = 1$ instead, because their convention is to let Δ act on the left.

Proof. The point $b' \in X_{\mathbb{C}}(\mathbb{C})$ is the unique geometric point mapping to $\sqrt{-23} \in \mathbb{P}^1(E') \subset \mathbb{P}^1(\mathbb{C})$ under $X_{E'} \to \mathbb{P}^1_{E'}$, so $b' \in X_E(E')$. The map $D \twoheadrightarrow X_{\mathbb{C}}$ is unramified at b since the ramification indices of b and b' over $\mathbb{P}^1$ are both 23, so the analytic uniformizer q at b corresponds to an analytic uniformizer at b'. □

A basis of $\mathrm{H}^0(X_{\mathbb{C}}, \Omega^1)$ pulls back to a 4-tuple $(f_0\,dq, \dots, f_3\,dq)$ for some $f_0, \dots, f_3 \in \mathbb{C}[[q]]$. For any field k and $r, d \in \mathbb{Z}_{\geq 0}$, let $k[x_0, \dots, x_r]_d$ be the space of degree d homogeneous polynomials in $k[x_0, \dots, x_r]$. If $d \leq 3$ and $R \in \mathbb{C}[x_0, \dots, x_3]_d$ and $R(f_0, \dots, f_3) \equiv 0 \pmod{q^{19}}$, then $R(f_0, \dots, f_3) = 0$, since the number of zeros of a nonzero global section of $(\Omega^1)^{\otimes d}$ is at most $\deg((\Omega^1)^{\otimes d}) = (2g_X - 2)d \leq 18$.

Given (g_1, g_2, g_3) and $N \geq 1$, the algorithm in [KMSV14, MSSV19], inspired by [Hej99] and [Sta84], computes the first N coefficients of each f_i numerically. The BelyiDB Magma package [CMSV26] implements this algorithm. We run it with $N = 19$ and compute 40 digits of precision for each coefficient. Below, we work numerically without controlling errors, so the intermediate steps of the calculation are not rigorous, but we return to rigor at the end by verifying *algebraically* that the claimed polynomials define M_{23}-extensions of $\mathbb{Q}$ and a regular M_{23}-extension of $\mathbb{Q}(t)$.

We echelonize the basis. This calculation shows that no nonzero 1-form vanishes at b' to order greater than 3; that is, b' is not a Weierstrass point. In other words, we obtain $f_i = q^i + O(q^4)$.

Lemma 3.4. *The genus 4 curve $X_{\mathbb{C}}$ is non-hyperelliptic.*

Proof. By [vBCPS26, Lemma 4.3], $\dim\{P \in \mathbb{C}[x_0, \dots, x_3]_2 : P(f_0, \dots, f_3) = 0\}$ is $\binom{4-1}{2} = 3$ if $X_{\mathbb{C}}$ is hyperelliptic, and $\binom{4-2}{2} = 1$ otherwise. We compute that the dimension is 1. □

The canonical model of a non-hyperelliptic curve of genus 4 over a field k is a complete intersection $P = Q = 0$ in $\mathbb{P}^3$, where $P \in k[x_0, \dots, x_3]_2$ and $Q \in k[x_0, \dots, x_3]_3$ [Har77, Example IV.5.2.2]. This curve in $\mathbb{P}^3$ does not determine P and Q uniquely: one can replace (P, Q) by $(\epsilon P, \epsilon' Q + \ell P)$ for any nonzero scalars ϵ, ϵ' and linear form ℓ.

By numerical linear algebra (singular value decomposition), we compute $P_1 \in \mathbb{C}[x_0, \dots, x_3]_2$ and $Q_1 \in \mathbb{C}[x_0, \dots, x_3]_3 - \mathbb{C}[x_0, \dots, x_3]_1 P_1$ such that $P_1(f_0, \dots, f_3) = Q_1(f_0, \dots, f_3) = 0$. Let X_1 be the curve $P_1 = Q_1 = 0$ in $\mathbb{P}^3_{\mathbb{C}}$.

3.3. **Recognition of algebraic coefficients.** Given Lemma 3.3, one might hope that

- X_1 is defined over E' in the sense that its homogeneous ideal $I \subset \mathbb{C}[x_0, \dots, x_3]$ is generated by polynomials in $E'[x_0, \dots, x_3]$; and
- $P_1, Q_1 \in E'[x_0, \dots, x_3]$.

But there are issues:

(i) We expanded 1-forms using an analytic uniformizer q over $\mathbb{C}$, not E', so we should not expect X_1 to be defined over E'.
(ii) Even if X_1 is defined over E', our P_1, Q_1 might not be, because P_1, Q_1 are not uniquely determined by X_1.

To address (i), for suitable $\lambda \in \mathbb{C}^\times$ we will re-echelonize the basis using the scaled parameter $q' := \lambda q$ instead of q. This amounts to making the substitution $x_i := \lambda^{-i} x'_i$ for $i = 0, \dots, 3$ in P_1, Q_1 to produce new polynomials P_λ, Q_λ; we then rename x'_i as x_i. Define the weight of a monomial by setting $\mathrm{wt}(x_i) := i$, so that each weight w monomial scales by λ^{-w}. Let X_λ be the curve $P_\lambda = Q_\lambda = 0$ in $\mathbb{P}^3_{\mathbb{C}}$.

Lemma 3.5. *The set of $\lambda \in \mathbb{C}^\times$ such that $P_\lambda \in \mathbb{C}^\times E'[x_0, \dots, x_3]_2$ is a coset C of $(E')^\times$ in $\mathbb{C}^\times$. For any $\lambda \in C$, we have $Q_\lambda \in \mathbb{C}^\times E'[x_0, \dots, x_3]_3 + \mathbb{C}[x_0, \dots, x_3]_1 P_\lambda$.*

Proof. The computed coefficients of x_0x_2 and x_0x_3 in P_1 are nonzero. The set of $\lambda \in \mathbb{C}^\times$ such that the ratio of these coefficients in P_λ is in E' is a coset of $(E')^\times$, since λ scales the ratio by $\lambda^{-2}/\lambda^{-3} = \lambda$. It remains to show that there exists λ such that X_λ is defined over E', since then $P_\lambda \in \mathbb{C}^\times E'[x_0, \dots, x_3]_2$ and $Q_\lambda \in \mathbb{C}^\times E'[x_0, \dots, x_3]_3 + \mathbb{C}[x_0, \dots, x_3]_1 P_\lambda$.

There is an analytic uniformizer τ at $b' \in X_{E'}$ such that τ^{23} is an analytic uniformizer at $\sqrt{-23} \in \mathbb{P}^1_{E'}$. Then $\tau = \sum_{n \geq 1} \lambda_n q^n$ for some $\lambda_1, \lambda_2, \dots \in \mathbb{C}$ with $\lambda_1 \neq 0$. Let $\zeta = e^{2\pi i/23}$. The rotation δ_b maps q to ζq; compatibly, the local monodromy generator g_2 at b' maps τ to $\zeta\tau$. Thus $\zeta\tau = \sum_{n \geq 1} \lambda_n (\zeta q)^n$. For each $n \geq 1$, comparing coefficients of q^n gives $\zeta\lambda_n = \lambda_n \zeta^n$, so $\lambda_n = 0$ when $n \not\equiv 1 \pmod{23}$. Thus $\tau = \lambda q + O(q^{24})$, where $\lambda := \lambda_1$.

Echelonizing using τ produces a curve $\mathcal{P} = \mathcal{Q} = 0$ in $\mathbb{P}^3_{E'}$ since τ is a uniformizer at an E'-point of a curve defined over E'. Echelonizing using λq produces X_λ. These curves are the *same* since the construction of $\mathcal{P}$ and $\mathcal{Q}$ examines only the first 19 coefficients of each expansion. Thus X_λ is defined over E'. □

Choose λ so that the ratio of the coefficients of x_0x_2 and x_0x_3 in P_λ is 1. Then scale P_λ to produce a polynomial P^1_λ whose coefficient of x_0x_2 is 1. A linear algebra computation shows that there is a unique $\ell \in \mathbb{C}[x_0, \dots, x_3]_1$ such that the coefficients of $x_0^2x_2$, $x_0x_1x_2$, $x_1^2x_2$, $x_1^2x_3$ in $Q_\lambda - \ell P^1_\lambda$ are 0; then scale to produce a polynomial Q^1_λ whose coefficient of $x_0^2x_3$ is 1. By Lemma 3.5, $P^1_\lambda, Q^1_\lambda \in E'[x_0, \dots, x_3]$.

Lattice reduction [LLL82] lets us recognize algebraic numbers of small degree and height from numerical approximations; our precision turns out to be sufficient to recognize the coefficients of P^1_λ, but not Q^1_λ. It would be expensive to re-run BelyiDB with greater precision to recognize Q^1_λ, so instead we will find a better $\lambda \in C$ to reduce the height. Let $\mathcal{O}$ be the ring of integers of E'.

Lemma 3.6. *The set of $\alpha \in (E')^\times$ such that $P^1_{\lambda/\alpha} \in \mathcal{O}[x_0, \dots, x_3]$, together with 0, is a fractional ideal $\mathfrak{a}$ of E'.*

Proof. Replacing λ by λ/α multiplies each weight w monomial in P_λ by α^w, and in P^1_λ by α^{w-2}. Examining the coefficient of q^2 in $P_1(f_0, \dots, f_3)$ shows that the coefficients of the weight 2 monomials x_0x_2 and x_1^2 in P_1 are negatives of each other, so these coefficients in P^1_λ are 1 and -1. Each other monomial appearing in P^1_λ has weight $w > 2$, so the condition that its coefficient in $P^1_{\lambda/\alpha}$ lie in $\mathcal{O}$ is that α^{w-2} belongs to some fractional ideal. Therefore, the set in question is an intersection of finitely many fractional ideals, hence a fractional ideal. □

Using the exact coefficients of P^1_λ, we compute the fractional ideal $\mathfrak{a}$ of Lemma 3.6. It might not be principal, but we choose $\alpha \in \mathfrak{a} - \{0\}$ minimizing $\sup\{|\iota(\alpha)| : \iota \in \mathrm{Hom}(K, \mathbb{C})\}$ to reduce the coefficient heights. Now it turns out that $P := P^1_{\lambda/\alpha}$ and $Q := Q^1_{\lambda/\alpha}$ are of small enough height that we succeed in recognizing their coefficients in E'.

Miraculously, they lie in $K = \mathbb{Q}(\sqrt{-23})$, suggesting that $X_{\mathbb{C}}$ might descend to $\mathbb{Q}$! The exact P and Q define a canonically embedded smooth genus 4 curve $X_K \subset \mathbb{P}^3_K$. Evaluating the renormalized $(f_0 : \cdots : f_3)$ at a, b, c gives $a', b', c' \in X_K(\mathbb{C}) \subset \mathbb{P}^3(\mathbb{C})$ with $b' = (1 : 0 : 0 : 0)$, and lattice reduction recognizes $c' \in X_K(K) \subset \mathbb{P}^3(K)$.

3.4. **Canonical equation for the degree 23 cover.** In describing our computations in this section, we assume that there exists a degree 23 cover $X \xrightarrow{t} \mathbb{P}^1_{\mathbb{Q}}$ with Galois group M_{23} and

local monodromy (2,23A,23B) above S whose base change to K is X_K, such that $\mathrm{Gal}(K/\mathbb{Q})$ interchanges b' and c'. This descent assumption is not yet justified, but later we will verify independently that the computed cover $X \xrightarrow{t} \mathbb{P}^1_{\mathbb{Q}}$ has the correct Galois group and local monodromy.

Specifically, given the exact P, Q, b', c' over K, we will describe rational functions t, v generating the function field $\mathbb{Q}(X)$, and the output of this section will be an irreducible polynomial $F \in \mathbb{Q}[T, V]$ such that $F(t, v) = 0$.

Construction of t: We first construct $X_K \xrightarrow{u} \mathbb{P}^1_K$ ramified over 1, 0, ∞ instead of 0, $\sqrt{-23}$, $-\sqrt{-23}$, with ramification index 23 above 0 and ∞. A Riemann–Roch space computation produces $u \in K(X_K)$ such that $\mathrm{div}(u) = 23b' - 23c'$. The degree 23 map $u\colon X_K \to \mathbb{P}^1_K$ is ramified above 0, ∞, and one other point above which the fiber is $D_7 + 2D_8$ for some reduced effective divisors D_7 and D_8 of degrees 7 and 8, respectively. Then $\mathrm{div}(du/u) = D_8 - b' - c'$ (there can be no more zeros, since $\deg \mathrm{div}(du/u) = 2g_X - 2 = 6$). We compute the zeros of du/u, and scale u so that its value on them is 1. Let $\rho \in \mathrm{Aut}(\mathbb{P}^1_K)$ send $1, 0, \infty$ to $0, \sqrt{-23}, -\sqrt{-23}$, respectively. We compute $t = \rho \circ u$.

Construction of v: We compute that the K-vector space $L(D_8 - 3b' - 2c')$ is 1-dimensional. Compute a generator f. Computation shows that $\sum_{x \in D_7} f(x) \neq 0$, where the sum is over the 7 geometric points of D_7. Normalize f to make this sum 1. Likewise, compute a generator $g \in L(D_8 - 2b' - 3c')$ such that $\sum_{x \in D_7} g(x) = 1$. Then $\{f, g\}$ is a K-basis for the linear system $L(D_8 - 2b' - 2c')$. For the intended $\mathbb{Q}$-structure on X_K, the generator of $\mathrm{Gal}(K/\mathbb{Q})$ fixes D_8 and interchanges b', c' and interchanges f, g. Let $v = \sqrt{-23}(f - g)/(f + g)$, which is a rational function of degree 4.

Construction of F: If $F \in \mathbb{Q}[T, V]$ has $\deg_T F = m$ and $\deg_V F = n$, say that F has bidegree (m, n). By linear algebra, we compute the bidegree $(4, 23)$ polynomial $F_0 \in \mathbb{Q}[T, V]$ vanishing at (t, v) whose coefficient of T^4V^{23} is 1. Actually, to avoid coefficient growth in the calculations, we compute t, f, g, v, F_0 modulo many primes p of size about 10^7 which split in K and reconstruct the rational coefficients of F_0. Because we have no a priori bound on the numerators and denominators of the rational coefficients, the reconstruction could be wrong, but we will verify the result later. Finally, for aesthetic purposes, we clear denominators to get $F \in \mathbb{Z}[T, V]$.

Remark 3.7. Any rational function v such that $\mathbb{Q}(t, v) = \mathbb{Q}(X)$, or the polynomial relation between t and v, can be used to prove Theorems 1.1 and 1.3. In the first version of this paper, we used a relation $F_8 \in \mathbb{Q}[T, V]$ of bidegree $(8, 23)$ instead of $(4, 23)$. There we also gave a theoretical description of one of bidegree $(4, 23)$. Le Lay [LL26, Theorem 1.1] was the first to compute an explicit polynomial of bidegree $(4, 23)$; he simplified our F_8 model by using an adjoint calculation. Our construction of F of bidegree $(4, 23)$ does not rely on [LL26] and does not use F_8.

Remark 3.8. In fact, degree 4 in T is best possible. The only nonconstant rational maps $X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ of degree ≤ 3 come from the rulings on the quadric $P = 0$ [Har77, Example IV.5.5.2]. Since the discriminant of P is not a square in K, the rulings are not defined over K, let alone over $\mathbb{Q}$.

Remark 3.9. The largest coefficient of F has 63 digits. By substituting $V = \frac{37W - 40}{49W + 32}$, clearing denominators, and dividing by the content, we produce a polynomial $F_{\mathrm{small}} \in \mathbb{Z}[T, W]$ of bidegree $(4, 23)$ whose largest coefficient has only 21 digits.

3.5. **Verification of ramification.** Now that we have a candidate $F(T,V)=0$, we need to verify that it produces an M_{23}-cover of $\mathbb{P}^1_{\mathbb{Q}}$ with the correct local monodromy. Let X_0 be the closure of $F(T,V)=0$ in $\mathbb{P}^1_{\mathbb{Q}}\times\mathbb{P}^1_{\mathbb{Q}}$.

Proposition 3.10. *The singular locus of X_0 consists of 62 geometric points, each a node, and their T-coordinates are distinct.*

Proof. We calculate $\operatorname{disc}_V F = eT^8(T^2+23)^{22}h_{62}^2$ for some nonzero $e\in\mathbb{Z}$ and degree 62 irreducible polynomial $h_{62}\in\mathbb{Z}[T]$. Thus X_0 is smooth except possibly at points where $T=\infty$, $T=0$, $T^2+23=0$, or $h_{62}=0$. Above a root β of h_{62}, we verify that $F(\beta,V)$ has 22 distinct roots, with one being a double root; since the valuation at β of $\operatorname{disc}_V F$ is 2, this implies that the double root is a node. We check partial derivatives at the points above $T=\infty$, $T=0$, $T^2+23=0$. □

Let X be the normalization of X_0. Let t be the projection $X\twoheadrightarrow X_0\xrightarrow{T}\mathbb{P}^1$.

Proposition 3.11. *The curve X is geometrically irreducible. The morphism $X\xrightarrow{t}\mathbb{P}^1_{\mathbb{Q}}$ is unramified outside S. The local monodromy above each of $\pm\sqrt{-23}$ is a 23-cycle, and above 0 it has cycle type $1^7 2^8$.*

Proof. Ramification can occur at most above ∞ and zeros of $\operatorname{disc}_V F$. Above $h_{62}=0$, the curve X_0 has only nodes, so $X\to\mathbb{P}^1_{\mathbb{Q}}$ is unramified there. Above ∞, 0, $\pm\sqrt{-23}$, the fibers of X and X_0 agree, and we compute the latter. Since $X\to\mathbb{P}^1_{\mathbb{Q}}$ is totally ramified above $\pm\sqrt{-23}$, it is geometrically irreducible. □

The genus of X is $(4-1)(23-1)-62=4$. Let $Y\to\mathbb{P}^1_{\mathbb{Q}}$ be the Galois closure of the degree 23 morphism $X\xrightarrow{t}\mathbb{P}^1_{\mathbb{Q}}$. We will prove that $Y\to\mathbb{P}^1_{\mathbb{Q}}$ is an M_{23}-cover.

3.6. **Verification of Galois groups.** Let G_{geom} and G_{arith} be the geometric and arithmetic monodromy groups of $F(t,V)\in\mathbb{Q}(t)[V]$. Thus $G_{\mathrm{geom}}\lhd G_{\mathrm{arith}}\le S_{23}$.

Proposition 3.12. *We have $G_{\mathrm{geom}}=M_{23}$.*

Proof. By the local monodromy in Proposition 3.11 and the classification of transitive groups of degree 23, we have $M_{23}\subseteq G_{\mathrm{geom}}$.

Recall the factorization $\operatorname{disc}_V F = et^8(t^2+23)^{22}h_{62}^2$. Let S' be the subscheme of $\mathbb{A}^1_{\mathbb{Z}}\subset\mathbb{P}^1_{\mathbb{Z}}$ defined by $t(t^2+23)h_{62}=0$. To calculate G_{geom}, we reduce modulo $p=411000011$; see Appendix A for the reason. We check that $p\nmid e$, and S' remains étale modulo p. Let $G_{\mathrm{geom},p}$ and $G_{\mathrm{arith},p}$ be the geometric and arithmetic monodromy groups of F mod p. The specialization map on prime-to-p fundamental groups of $\mathbb{P}^1-S'$ is an isomorphism ([Gro03, XIII.2]; see also [OV00, Théorème 4.4]), so $G_{\mathrm{geom},p}=G_{\mathrm{geom}}$. Using Appendix A, we certify that $G_{\mathrm{arith},p}=M_{23}$. Thus $M_{23}\subseteq G_{\mathrm{geom}}=G_{\mathrm{geom},p}\subseteq G_{\mathrm{arith},p}=M_{23}$, so all are equal. □

Corollary 3.13. *We have $G_{\mathrm{arith}}=M_{23}$.*

Proof. By Proposition 3.12, $G_{\mathrm{geom}}=M_{23}$. The group G_{geom} is normal in G_{arith}, and M_{23} is not normal in any larger subgroup of S_{23} (i.e., it is self-normalizing in S_{23}). □

By Proposition 3.12 and Corollary 3.13, since $G_{\mathrm{geom}}=G_{\mathrm{arith}}$, the splitting field of F over $\mathbb{Q}(t)$ is a regular extension with Galois group M_{23}. This proves Theorem 1.3.

3.7. **Galois action on the Nielsen class.** We now repeat the computations of Sections 3.2–3.6 for a triple representing a *different element* of the size 7 Nielsen class $\mathrm{Ni}_{\mathfrak{c}}$. We use BelyiDB and recognize[5] the coefficients of the new P and Q as elements of $L' := L(\sqrt{-23})$, where $L := \mathbb{Q}[x]/(x^6 - x^5 - 3x^4 - 3x^3 + x^2 + 5x + 4)$. Here L is a degree 6 number field whose Galois closure $\widetilde{L}$ has Galois group S_6. The discriminant of L is $2^4 \cdot 11 \cdot 23^4$, divisible only by primes dividing $|M_{23}|$, as required by [Bec89, Theorem 5.5]. The signature of L is $(2, 2)$, compatible with the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-action on $\mathrm{Ni}_{\mathfrak{c}}$. Since L has real places, $\sqrt{-23} \notin L$. We compute a bidegree (4,23) polynomial $\mathcal{F} \in L[T, V]$. We check that it defines a degree 23 cover $\mathcal{X} \to \mathbb{P}^1_L$ ramified only over S, with the correct ramification indices. We reduce modulo the degree 1 prime above $p = 411000011$, and use Appendix A to verify that it has Galois group M_{23}. Because $\sqrt{-23} \notin L$, the local monodromy is $\mathfrak{G}_L$-stable, and hence can only be (2,23A,23B) or (2,23B,23A). In the latter case, compose with the involution of $\mathbb{P}^1_L$ sending $0, \sqrt{-23}, -\sqrt{-23}$ to $0, -\sqrt{-23}, \sqrt{-23}$, respectively, to switch the 23A and 23B.

The cover $\mathcal{X} \to \mathbb{P}^1_L$ defines a point of $\mathcal{H}_{\mathfrak{c}}(L)$, but a priori, it could be defined over any *subfield* of L. Since $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \simeq S_6$, the only subfields are $\mathbb{Q}$ and L. The following rules out $\mathbb{Q}$.

Proposition 3.14. *The curve $\mathcal{X}$ does not descend to $\mathbb{Q}$.*

Proof. For a prime ideal $\mathfrak{p}$ of L, let $\mathbb{F}_{\mathfrak{p}}$ be the residue field. For two of the three degree 1 prime ideals above 53, say $\mathfrak{p}_1$ and $\mathfrak{p}_2$, we compute $\#\mathcal{X}(\mathbb{F}_{\mathfrak{p}_1}) = 45$ and $\#\mathcal{X}(\mathbb{F}_{\mathfrak{p}_2}) = 52$. If $\mathcal{X}$ were defined over $\mathbb{Q}$, both would equal $\#\mathcal{X}(\mathbb{F}_{53})$. □

Thus $\mathcal{H}_{\mathfrak{c}}$ contains a closed point $\operatorname{Spec} L$. On the other hand, the cover $X \to \mathbb{P}^1_{\mathbb{Q}}$ we computed earlier shows that $\mathcal{H}_{\mathfrak{c}}$ contains $\operatorname{Spec} \mathbb{Q}$. Since $\deg \mathcal{H}_{\mathfrak{c}} = 7$, we have $\mathcal{H}_{\mathfrak{c}} = \operatorname{Spec} \mathbb{Q} \sqcup \operatorname{Spec} L$. In particular, $\mathfrak{G}_{\mathbb{Q}}$ acts on $\mathrm{Ni}_{\mathfrak{c}} = \mathcal{H}_{\mathfrak{c}}(\overline{\mathbb{Q}})$ with orbits of size 1 and 6.

3.8. **Automorphisms of the M_{23}-cover.** The topological Euler characteristic of the quotient stack $[Y/M_{23}]$ is

$$\chi([Y/M_{23}]) = 2 - (1 - \tfrac{1}{2}) - (1 - \tfrac{1}{23}) - (1 - \tfrac{1}{23}) = -19/46.$$

By the Riemann–Hurwitz formula, the genus g_Y of Y satisfies

$$2 - 2g_Y = \chi(Y) = |M_{23}|\ \chi([Y/M_{23}]),$$

so $g_Y = 2{,}106{,}721$.

Proposition 3.15. *We have* $\operatorname{Aut} Y = \operatorname{Aut} Y_{\mathbb{C}} \simeq M_{23}$.

Proof. First, here are two ways to see that $(\operatorname{Aut} Y_{\mathbb{C}} : M_{23}) \leq 2$:

(i) Every finite-index overgroup of the triangle group $\Delta = \Delta(2, 23, 23)$ is another triangle group. The classification of inclusions of triangle groups shows that the only nontrivial possibility is the index 2 overgroup $\Delta(2, 4, 23)$. See [Sin72, Theorem 1].

[5]Some modifications to the recognition procedure of Section 3.3 were necessary. First, we ran BelyiDB with 60 digits of precision instead of just 40. Second, we actually ran BelyiDB on all six other Nielsen class elements, in order to recover P and Q together with their conjugates simultaneously. Third, it turned out that 60 digits of precision were not sufficient to recognize *all* the coefficients of P^1_λ; we recognized only the coefficients of monomials of weight ≤ 4, and defined $\mathfrak{a}$ using only the conditions on those coefficients. Then, after choosing a small $\alpha \in \mathfrak{a}$, we succeeded in recognizing all coefficients of $P^1_{\lambda/\alpha}$ and $Q^1_{\lambda/\alpha}$.

(ii) If $n = (\operatorname{Aut} Y_{\mathbb{C}} : M_{23})$, then $\chi([Y_{\mathbb{C}}/\operatorname{Aut} Y_{\mathbb{C}}]) = (-19/46)/n$, but for $n \geq 3$, elementary number theory shows that $2 - \sum(1 - \frac{1}{m_i}) = (-19/46)/n$ has no solutions in integers $m_i \geq 2$.

If $(\operatorname{Aut} Y_{\mathbb{C}} : M_{23}) = 2$, then there would be an involution of $[Y/M_{23}]$ interchanging the points with local monodromy 23A and 23B, and M_{23} would have an outer automorphism interchanging conjugacy classes 23A and 23B. But all automorphisms of M_{23} are inner. □

Remark 3.16. The proof of [MM18, Theorem II.9.9] finds an M_{23}-cover of $\mathbb{P}^1_{\mathbb{Q}(\sqrt{-23})}$ that is also an M_{24}-cover of $\mathbb{P}^1_{\mathbb{Q}(\sqrt{-23})}$. Proposition 3.15 implies that our M_{23}-cover Y cannot be an M_{24}-cover of $\mathbb{P}^1_{\mathbb{Q}}$.

3.9. **Specializations.** By specializing T in $F(T, V)$ to an element $\mathsf{q} \in \mathbb{Q}$, we obtain a degree 23 polynomial $f_{\mathsf{q}} \in \mathbb{Q}[V]$ (the leading coefficient never vanishes). Also define $f_\infty \in \mathbb{Q}[V]$ by setting $\tau = 0$ in $\tau^4 F(1/\tau, V)$. Let K_{q} be the splitting field of f_{q} over $\mathbb{Q}$. Let $\operatorname{Gal}(f_{\mathsf{q}}) = \operatorname{Gal}(K_{\mathsf{q}}/\mathbb{Q})$.

For another perspective, let X_{q} be the fiber of $X \xrightarrow{t} \mathbb{P}^1_{\mathbb{Q}}$ above $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$, so X_{q} is a $\mathbb{Q}$-scheme. A computation shows that the singularities of the plane model $F(T, V) = 0$ birational to X do not lie above rational points of $\mathbb{P}^1_{\mathbb{Q}}$, so the set of roots of f_{q} is in bijection with $X_{\mathsf{q}}(\overline{\mathbb{Q}})$, and the irreducible factors of f_{q} correspond to the $\operatorname{Gal}(f_{\mathsf{q}})$-orbits in $X_{\mathsf{q}}(\overline{\mathbb{Q}})$. For $\mathsf{q} \neq 0$ (not the rational branch point), we may identify $\operatorname{Gal}(f_{\mathsf{q}})$ with a subgroup of M_{23}, well defined up to M_{23}-conjugation. We have $\operatorname{Gal}(f_{\mathsf{q}}) \simeq M_{23}$ for all q outside a finite set: see Theorem 3.25.

Given $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q}) - \{0\}$, we apply the PARI/GP routine `polredbest` [CDyD91, PAR26] repeatedly to find lower-height monic polynomials in $\mathbb{Z}[x]$ defining the same number field as f_{q}, and use `GaloisProof` to certify their Galois groups. The specialization $\mathsf{q} = 2$ gives in this way the polynomial in Example 1.2. The specialization $\mathsf{q} = -3703/947$ gives the following, which is the lowest-height M_{23} polynomial we found so far.

Example 3.17. The splitting field of

$$\begin{aligned} x^{23} &+ 46x^{21} - 598x^{20} + 1679x^{19} - 21620x^{18} + 127420x^{17} \\ &- 361974x^{16} + 2223732x^{15} - 9392096x^{14} + 17344116x^{13} \\ &- 71999476x^{12} + 320807726x^{11} - 436105484x^{10} + 83587888x^9 \\ &- 2463757240x^8 + 9451874955x^7 - 5728074376x^6 - 26037806834x^5 \\ &+ 63691532334x^4 - 67357061907x^3 + 38754121124x^2 \\ &- 11217790920x + 1243077066 \end{aligned}$$

is an M_{23}-extension of $\mathbb{Q}$ unramified outside $\{2, 7, 23\}$.

3.10. **Other specializations.** In this section, we prove that there is a value of q such that $\operatorname{Gal}(f_{\mathsf{q}}) \simeq M_{22}$, and prove Theorem 3.25 which states that there are only finitely many values of q such that $\operatorname{Gal}(f_{\mathsf{q}}) \not\simeq M_{23}$.

Proposition 3.18.

(a) *The fiber $X_0(\overline{\mathbb{Q}})$ of X above the branch point 0 consists of $\operatorname{Gal}(f_0)$-orbits of sizes 7 and 8, in which every point has ramification index 1 or 2, respectively. The action of $\operatorname{Gal}(f_0)$ on*

$X_0(\overline{\mathbb{Q}})$ is equivalent to $\mathrm{AGL}_3(\mathbb{F}_2)$ *acting on the set* $\check{\mathbb{P}}^2(\mathbb{F}_2) \sqcup \mathbb{A}^3(\mathbb{F}_2)$ *of size* $7+8$*, where* $\check{\mathbb{P}}^2$ *denotes the space of* lines *in the plane at infinity in* $\mathbb{P}^3$.[6]

(b) *For each* $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$*, complex conjugation gives an order* 2 *element in* $\mathrm{Gal}(f_{\mathsf{q}})$.

(c) *For each* $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$,

$$\mathrm{Gal}(f_{\mathsf{q}}) \simeq M_{23} \quad \iff \quad f_{\mathsf{q}} \text{ is irreducible over } \mathbb{Q}.$$

Proof.

(a) As in the proof of Lemma 3.1, the fiber $X_0(\overline{\mathbb{Q}})$ consists of 7 unramified points and 8 points of ramification index 2, so $f_0 = g_7 g_8^2$ for some $g_7, g_8 \in \mathbb{Q}[x]$ of degree 7 and 8. We use Magma to verify that g_7 and g_8 are irreducible, and `GaloisProof` to compute $\mathrm{Gal}(f_0)$ as a permutation group.

(b) The space $\mathbb{P}^1(\mathbb{R}) - \{0\}$ is connected and contains no branch points of t, so the conjugacy class of complex conjugation acting on $X_{\mathsf{q}}(\mathbb{C})$ is the same for all $\mathsf{q} \in \mathbb{P}^1(\mathbb{R}) - \{0\}$; checking $\mathsf{q} = 1$, say, shows that it is the class 2, so 2 divides $|\mathrm{Gal}(f_{\mathsf{q}})|$. We check $\mathsf{q} = 0$ separately.

(c) We may assume that $\mathsf{q} \neq 0$. If f_{q} is reducible, then $\mathrm{Gal}(f_{\mathsf{q}})$ is contained in a product of symmetric groups of degree less than 23, so 23 does not divide $|\mathrm{Gal}(f_{\mathsf{q}})|$, so $\mathrm{Gal}(f_{\mathsf{q}}) \not\simeq M_{23}$.

Now suppose that f_{q} is irreducible. Then $\mathrm{Gal}(f_{\mathsf{q}})$ acts transitively on a set of size 23, so 23 divides $|\mathrm{Gal}(f_{\mathsf{q}})|$. Also, 2 divides $|\mathrm{Gal}(f_{\mathsf{q}})|$, by (b). The only subgroup of M_{23} of order divisible by both 2 and 23 is M_{23} itself. □

Proposition 3.19. *The genus* 4 *curve* X *has a rational point.*

Proof. A search produced $(-1545209/264829, -1/27)$ on the plane model $F(T, V) = 0$. □

Remark 3.20. Under the change of coordinate in Remark 3.9, $V = -1/27$ corresponds to $W = 1$.

Proposition 3.21. *If* $\mathsf{q} = -1545209/264829$*, then* $\mathrm{Gal}(f_{\mathsf{q}}) \simeq M_{22}$.

Proof. We have $f_{\mathsf{q}} = (V + 1/27)h_{22}$, where $h_{22} \in \mathbb{Q}[V]$ is of degree 22. We certify using `GaloisProof` that h_{22} has Galois group M_{22} over $\mathbb{Q}$. □

Example 3.22. Running `polredbest` produces a polynomial

$$\begin{aligned} x^{22} &- 10x^{21} - 171x^{20} + 4948x^{19} - 3160x^{18} - 878184x^{17} \\ &+ 1612816x^{16} + 57499538x^{15} - 104404974x^{14} - 1334363150x^{13} \\ &+ 222611762x^{12} + 13957937472x^{11} + 44873894586x^{10} + 48162643482x^{9} \\ &- 396850048164x^{8} - 2898168029276x^{7} - 8595497273752x^{6} \\ &- 12865403779026x^{5} - 5309597045808x^{4} + 12770814291390x^{3} \\ &+ 19223398109406x^{2} + 8150987444096x + 212425572022 \end{aligned}$$

defining the same number field as h_{22}. Its splitting field is an M_{22}-extension of $\mathbb{Q}$.

Conjecture 3.23. For all $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q}) - \{0, -1545209/264829\}$, we have $\mathrm{Gal}(f_{\mathsf{q}}) \simeq M_{23}$.

The rest of this section collects theoretical and computational evidence for Conjecture 3.23.

[6] A version of this description of $\mathrm{Gal}(f_0)$ was independently computed in [LL26, Section 3], using an equation for $X \to \mathbb{P}^1_{\mathbb{Q}}$ that we provided in the first version of this paper.

Remark 3.24. Write $\mathsf{q} = a/b$ in lowest terms with $a, b \in \mathbb{Z}$ and $b \neq 0$. If $a^2 + 23b^2$ is not of the form $2^i 3^j 23^k w^{23}$ for some $i, j, k, w \in \mathbb{Z}_{\geq 0}$, then $\mathbb{Q}[V]/(f_{\mathsf{q}})$ over $\mathbb{Q}$ is totally ramified of degree 23 above a prime $p \neq 2, 3, 23$ with $23 \nmid v_p(a^2 + 23b^2)$, so $\mathrm{Gal}(f_{\mathsf{q}}) \simeq M_{23}$. Therefore we search through integers of this form (imposing other necessary local conditions at a few primes), use Cornacchia's algorithm [HMW90, Bas04] to find representations of each as $a^2 + 23b^2$, and check for the resulting $\mathsf{q} = a/b$ that f_{q} is irreducible. This proves that $\mathrm{Gal}(f_{\mathsf{q}}) \simeq M_{23}$ for all nonzero q with $|a|, |b| \leq 10^{50}$ except for $\mathsf{q} = -1545209/264829$. Moreover, f_∞ is irreducible, so $\mathrm{Gal}(f_\infty) \simeq M_{23}$ too.

Table 1 summarizes the information we computed about the specializations. The second column gives the degrees of the irreducible factors of f_{q} in $\mathbb{Q}[V]$; they sum to 23 except when $\mathsf{q} = 0$ (the rational branch point).

q	irreducible factors of f_{q}	$\mathrm{Gal}(f_{\mathsf{q}})$	$\lvert\mathrm{Gal}(f_{\mathsf{q}})\rvert$
0	$7 + 8$	$\mathrm{AGL}_3(\mathbb{F}_2)$	1344
$-1545209/264829$	$1 + 22$	M_{22}	443520
∞, all other a/b with $\lvert a\rvert, \lvert b\rvert \leq 10^{50}$	23	M_{23}	10200960

TABLE 1. Specializations of the regular M_{23}-extension

Theorem 3.25. *The set of* $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$ *such that* $\mathrm{Gal}(f_{\mathsf{q}}) \not\simeq M_{23}$ *is finite.*

Proof. Let $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q}) - \{0\}$. If $\mathrm{Gal}(f_{\mathsf{q}}) \not\simeq M_{23}$, then $\mathrm{Gal}(f_{\mathsf{q}})$ is contained in some maximal subgroup $H \leq M_{23}$. In this case, q lifts to a rational point of the quotient curve Y/H. Information about the maximal subgroups H of M_{23} can be found in the ATLAS [CCN+85] and [Wil09, Section 5.2.8]. We summarize this information in Table 2 using ATLAS notation.

For each H, intersecting H with the classes 2, 23A, 23B gives the ramification of $Y \to Y/H$, and then the Riemann–Hurwitz formula gives the genus of Y/H. Each quotient has genus greater than 1, and hence only finitely many rational points [Fal83]. □

H	$\lvert H\rvert$	$(M_{23} : H)$	orbit sizes	genus of Y/H	$\mathbb{Q}$-points on Y/H?
M_{22}	443520	23	$1 + 22$	4	yes, Proposition 3.19
$L_3(4){:}2_2$	40320	253	$2 + 21$	46	maybe
$2^4{:}A_7$	40320	253	$7 + 16$	46	yes, Proposition 3.26
A_8	20160	506	$8 + 15$	95	maybe
M_{11}	7920	1288	$11 + 12$	253	no, Remark 3.28
$2^4{:}(3 \times A_5){:}2$	5760	1771	$3 + 20$	344	maybe
23:11	253	40320	23	8327	no, Remark 3.27

TABLE 2. Maximal subgroups $H \leq M_{23}$ up to conjugacy, and quotient curves

Proposition 3.26. *Let* $H \leq M_{23}$ *be a maximal subgroup.*

(a) *If* $H \simeq 2^4{:}A_7$, *then* Y/H *has a unique rational point above* $\mathsf{q} = 0$.

(b) *If* $H \not\simeq 2^4{:}A_7$, *then* Y/H *has no rational point above* $\mathsf{q} = 0$.

Proof. Let Y_0 be the fiber of $Y \to \mathbb{P}^1$ above 0. Let $I \lhd D$ in M_{23} be the inertia and decomposition groups at a closed point $y \in Y_0$. As y varies, I ranges over the conjugates of $\langle g_1 \rangle$, which are the order 2 subgroups of M_{23}. We have $D/I \simeq \mathrm{Gal}(f_0) \simeq \mathrm{AGL}_3(\mathbb{F}_2)$ by Proposition 3.18(a), so $|D| = 2|\mathrm{AGL}_3(\mathbb{F}_2)| = 2688$. On the other hand, D is contained in the normalizer $N(I)$, which also has order 2688, so $D = N(I)$. The map of transitive M_{23}-sets $Y_0 \to \{\text{order 2 subgroups of } M_{23}\}$ given by $y \mapsto I$ is bijective since corresponding one-point stabilizers D and $N(I)$ coincide. Also, the residue field degree $[\kappa(y) : \mathbb{Q}]$ is $(D : I)$.

For a maximal subgroup H, let $X_H = Y/H$. The fiber $(X_H)_0$ above $\mathsf{q} = 0$ is $Y_0/H \simeq \{\text{order 2 subgroups}\}/H$. The inertia and decomposition groups at y for $Y \to X_H$ are $I \cap H$ and $D \cap H$ [Ser79, I.§7, Proposition 22(a)], so if $x \in X_H$ is the image of y, then $[\kappa(y) : \kappa(x)] = (D \cap H : I \cap H)$ and

$$[\kappa(x) : \mathbb{Q}] = \frac{[\kappa(y) : \mathbb{Q}]}{[\kappa(y) : \kappa(x)]} = \frac{(D : I)}{(D \cap H : I \cap H)} = \frac{(N(I) : I)}{(N(I) \cap H : I \cap H)}. \tag{1}$$

For each H, varying I and computing the right side of (1) shows that $\kappa(x) = \mathbb{Q}$ occurs only for $H = 2^4{:}A_7$, and then only for I in a single H-orbit, hence for only one point of $(X_H)_0$. □

Conjecture 3.23 is equivalent to the statement that the quotients Y/H (for H a maximal subgroup of M_{23}) have no rational points other than the points in Propositions 3.19 and 3.26.

Remark 3.27. By the proof of Proposition 3.18(b), there is no $\mathsf{q} \in \mathbb{P}^1(\mathbb{R})$ for which the splitting field of f_q over $\mathbb{R}$ is contained in the odd-order group 23:11. In other words, the genus 8327 curve $Y/(23{:}11)$ has no $\mathbb{R}$-point.

Remark 3.28. Let us prove that there is no $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q}_{23})$ for which the Galois group of f_q over $\mathbb{Q}_{23}$ is contained in M_{11}; equivalently, the genus 253 curve Y/M_{11} has no $\mathbb{Q}_{23}$-point. As displayed in Table 3, the valuation $v_{23}(\mathsf{q})$ determines the 23-adic Newton polygon of $F(\mathsf{q}, V)$, which in turn forces the inertia group to have an element of order 7, 15, or 23. But M_{11} has no element of order 7, 15, or 23.

$v_{23}(\mathsf{q})$	slopes of Newton polygon	inertia group
≤ -1	$-\mathbf{2/5}$ (width 20), $-\mathbf{1/3}$ (width 3)	$\mathbb{Z}/15\mathbb{Z}$
$= 0$	$-\mathbf{10/23}$ (width 23)	23 divides order
$= 1$	$-\mathbf{11/23}$ (width 23)	23 divides order
$= 2$	$-\mathbf{10/23}$ (width 23)	23 divides order
≥ 3	$-\mathbf{3/7}$ (width 21), others $\geq \mathbf{0}$	$\mathbb{Z}/7\mathbb{Z}$

TABLE 3. 23-adic Newton polygons of specializations

Remark 3.29. Table 3 also shows that if q is the T-coordinate of a rational point on X, then $v_{23}(\mathsf{q}) \geq 3$.

Appendix A. Rigorous calculation of function field Galois groups

A.1. **Insufficiency of Magma's Galois group routines over function fields.** Magma has two routines for computing the Galois group of a polynomial:

- `GaloisGroup` is fast and we have not heard of cases where it gives the wrong answer, but it is not guaranteed to be 100% rigorous;
- `GaloisProof` is slower, but 100% rigorous.

We used `GaloisProof` to certify the Galois group of each explicit polynomial over $\mathbb{Q}$ in our paper. In principle, `GaloisProof` also works over $\mathbb{Q}(t)$ and $L(t)$, but it did not terminate on our degree 23 examples over these fields, so instead we reduced the problem to computing a Galois group over $\mathbb{F}_p(t)$ for a prime p. Unfortunately, it appears that `GaloisProof` has not been implemented over $\mathbb{F}_p(t)$.

Therefore we use a different approach for the certification, due to Elkies [Elk13, §3]. We improve the bounds slightly by using Artin L-functions instead of full zeta functions as he did.

A.2. **Character sums.** Let B be a **nice** curve over a finite field $\mathbb{F}_q$, that is, a smooth projective geometrically integral scheme of dimension 1 over $\mathbb{F}_q$. Let $\mathbb{F}_q(B)$ be its function field. Let $f \in \mathbb{F}_q(B)[x]$ be a separable polynomial of degree n. Its splitting field is the function field of a connected Galois étale cover $\pi\colon Y \to U$ of some dense affine open subscheme $U \subset B$. Let G be the Galois group of π, so $G \le S_n$. For each closed point $u \in U$, we have the arithmetic Frobenius conjugacy class Frob_u in G.

By the Chebotarev density theorem, G is determined by the distribution of the classes Frob_u. Effective versions of Chebotarev density theorem with explicit error terms allow one to determine G with only *finitely many* Frob_u. Although one could use the count of Frob_u giving a single conjugacy class, one gets better error bounds by taking *combinations* of conjugacy classes weighted according to the values of a character. Better error bounds permit us to use a smaller q, to shorten the running time. The following summarizes what we need.

Theorem A.1. *Let B be a nice curve of genus g over a finite field $\mathbb{F}_q$. Let $U \subset B$ be a dense affine open subscheme. Let G be a finite group. Let $\pi\colon Y \to U$ be a connected G-torsor. Let $G_{\mathrm{geom}} \lhd G$ be the geometric monodromy group. Let V be a $\mathbb{C}$-representation of G, with degree d, character χ, and Artin conductor $\mathfrak{f}$. For $b \in B - U$, let $I_b \le G$ be the inertia group, and V^{I_b} the fixed subspace.*

(a) *If π is tamely ramified at each point of $B - U$, then*

$$\deg \mathfrak{f} = \sum_{b \in B-U} (\deg b)(d - \dim V^{I_b}).$$

(b) *If $V^{G^{\mathrm{geom}}} = 0$, then the Artin L-function*

$$L_V(T) := \prod_{\text{closed points } b \in B} \det\bigl(1 - T^{\deg b}\,\mathrm{Frob}_b\,|V^{I_b}\bigr)^{-1}$$

is a polynomial of the form

$$\prod_{i=1}^{d(2g-2)+\deg \mathfrak{f}} (1 - \alpha_i T)$$

for some $\alpha_i \in \mathbb{C}$ satisfying $|\alpha_i| = q^{1/2}$.

(c) *If* $V^{G^{\mathrm{geom}}} = 0$*, then the character sum*

$$N_\chi := \sum_{u \in U(\mathbb{F}_q)} \chi(\mathrm{Frob}_u)$$

satisfies

$$|N_\chi| \le \big(d(2g-2) + \deg \mathfrak{f}\big)\, q^{1/2} + \sum_{b \in (B-U)(\mathbb{F}_q)} \dim V^{I_b}.$$

Proof.

(a) By [Ser79, VI.§2, Corollary 1′], for each $b \in B - U$, the multiplicity of b in $\mathfrak{f}$ is $d - \dim V^{I_b}$ plus a Swan conductor term that is 0 in the tame case.

(b) This is Weil's Riemann hypothesis for Artin L-functions [Wei48, §V].

(c) Equating coefficients of T in (b) gives

$$\sum_{u \in U(\mathbb{F}_q)} \chi(\mathrm{Frob}_u) + \sum_{b \in (B-U)(\mathbb{F}_q)} \mathrm{Tr}(\mathrm{Frob}_b \,|V^{I_b}) \quad = \quad - \sum_{i=1}^{d(2g-2)+\deg \mathfrak{f}} \alpha_i.$$

The first sum is N_χ. In the second sum, $\mathrm{Frob}_b \,|V^{I_b}$ has finite order, so $\big|\mathrm{Tr}(\mathrm{Frob}_b \,|V^{I_b})\big| \le \dim V^{I_b}$. In the third sum, $|\alpha_i| \le q^{1/2}$ by (b). □

Remark A.2. In Theorem A.1, G/G^{geom} is the Galois group of an extension of finite fields, hence cyclic. Thus, if G is a nonabelian simple group, then $G^{\mathrm{geom}} = G$.

Remark A.3. Suppose that G is a nonabelian simple group. Let $\mathbb{1}$ be the trivial character, so $\langle \chi, \mathbb{1} \rangle$ is the multiplicity of $\mathbb{1}$ in χ. If χ is a character of G such that $\langle \chi, \mathbb{1} \rangle = 0$, then Remark A.2 shows that Theorem A.1(c) applies, so N_χ is $O(q^{1/2})$. On the other hand, $N_{\mathbb{1}}$ is $q + O(q^{1/2})$ by the Hasse–Weil bound. Taking a combination shows that for any χ, if q is large enough, then $\langle \chi, \mathbb{1} \rangle$ is the integer closest to N_χ/q.

A.3. **Application to M_{23}.** In our application, we choose a prime $p > 23$, and $B = \mathbb{P}^1_{\mathbb{F}_p}$, and $U = \mathbb{P}^1_{\mathbb{F}_p} - \{0, \sqrt{-23}, -\sqrt{-23}\}$. We have $f \in \mathbb{F}_p(t)[x]$ defining an étale cover of U with ramification of type $1^7 2^8$ above 0, and type 23 above $\pm\sqrt{-23}$. For simplicity, assume that $\sqrt{-23} \in \mathbb{F}_p$. Let G be the Galois group of f. For the chosen p, we will check that $\mathrm{disc}(f) \in \mathbb{F}_p(t)^{\times 2}$, so $G \le A_{23}$. We wish to prove that the Galois group G of f is M_{23}.

Lemma A.4. *Either* $G = M_{23}$ *or* $G = A_{23}$.

Proof. We have $G \le A_{23}$. The ramification shows that $2 \cdot 23$ divides $|G|$. The result now follows from the classification of transitive groups on 23 elements. □

For $r \ge 0$, let $\binom{[23]}{r}$ be the set of r-element subsets of $[23] := \{1, \dots, 23\}$. Let V_r be the corresponding permutation representation, and let χ_r be its character.

Lemma A.5. *Let* G *be* M_{23} *or* A_{23}.

(i) *We have* $\langle \chi_4, \mathbb{1} \rangle = 1$ *for either group.*

(ii) *We have* $\langle \chi_5, \mathbb{1} \rangle = \begin{cases} 2, & \text{if } G = M_{23}, \\ 1, & \text{if } G = A_{23}. \end{cases}$

Proof. The integer $\langle \chi_r, \mathbb{1} \rangle$ is the number of G-orbits in $\binom{[23]}{r}$.

(i) Both M_{23} and A_{23} are 4-transitive, so the number of orbits in $\binom{[23]}{4}$ is 1.

(ii) The group A_{23} is 5-transitive, but M_{23} has *two* orbits on $\binom{[23]}{5}$: some 5-element subsets are contained in a 7-element block of $S(4, 7, 23)$, and some are not. □

There is an injection $V_4 \hookrightarrow V_5$ sending each 4-element subset to the formal sum of the 5-element subsets containing it [Got66]. Thus $\eta := \chi_5 - \chi_4$ is the character of a representation. By Lemma A.5, the multiplicity $\langle \eta, \mathbb{1} \rangle$ is 1 if $G = M_{23}$, and 0 if $G = A_{23}$. Define χ by

$$\eta = \begin{cases} \mathbb{1} + \chi, & \text{if } G = M_{23}, \\ \chi, & \text{if } G = A_{23}. \end{cases}$$

Thus χ is a character of a representation V to which Theorem A.1 applies.

Let us do the computations for A_{23}. First, $\dim V = \binom{23}{5} - \binom{23}{4} = 24794$. For each branch point b, the cycle type of the I_b-generator on [23] determines the cycle types on $\binom{[23]}{5}$ and $\binom{[23]}{4}$, from which we calculate $\dim V^{I_b}$. Now Theorem A.1 calculates $\deg \mathfrak{f}$ and a bound on $|N_\chi|$. For M_{23}, we have $\chi = \eta - \mathbb{1}$, so $\dim V$ and each $\dim V^{I_b}$ are 1 smaller. See Table 4.

G	#orbits on $\binom{[23]}{5}$	$\dim V$	$\dim V^{I_0}$	$\dim V^{I_{\pm\sqrt{-23}}}$	$\deg \mathfrak{f}$	bound on N_χ
M_{23}	2	24793	12529	1077	59696	$10110p^{1/2} + 14683$
A_{23}	1	24794	12530	1078	59696	$10108p^{1/2} + 14686$

TABLE 4. Data for M_{23} vs. A_{23}

Let $N = N_\eta$. If $G = M_{23}$, then $N = (p - 2) + N_\chi$.

Corollary A.6.

- *If $G = M_{23}$, then $|N - (p - 2)| \le 10110p^{1/2} + 14683$.*
- *If $G = A_{23}$, then $|N| \le 10108p^{1/2} + 14686$.*

If p is large enough, the ranges for N in the two cases of Corollary A.6 do not overlap, so N determines G. In particular, $p = 411000011$ is large enough, and $\sqrt{-23} \in \mathbb{F}_p$.

It remains to compute N. Given $u \in U(\mathbb{F}_p)$, the degrees of the factors of the specialization of f at u tell us the cycle type of Frob_u (except that an easy local Galois group calculation may be needed if the specialization is not separable). The cycle type gives $\eta(\mathrm{Frob}_u)$. We compute N by looping over all $u \in U(\mathbb{F}_p)$. This takes time, but it requires very little memory and parallelizes easily. For the reductions of the curves over $\mathbb{Q}(t)$ and $L(t)$ from Sections 3.6 and 3.7, respectively, we find $N = 411207463$ and $N = 411071392$, which are both in the M_{23} range.

USE OF AI

No text in this article was written by AI. Our work relies on longstanding domain knowledge and techniques for computing curves of positive genus [KMSV14]. The key strategic decisions and the conceptual analysis for this project were made by the human team.

AI served as a tool that accelerated a large part of our work, particularly the computations. We used Claude Fable 5 and 5.1, Claude Opus 4.8, and ChatGPT 5.6 Sol for searching the literature, generating code, checking results, and proofreading. The workflow that eventually succeeded was a tightly controlled collaboration in which the computational work was much faster with AI, while the human collaborators continued to direct the research and verify

the results. AI systems increased our confidence in tackling difficult problems and helped us communicate more efficiently across our different areas of expertise.

Our analysis of the literature alongside our new computations suggested that the 4-branch-point M_{23}-covers $X \to \mathbb{P}^1$ most likely to descend to a low-degree number field were those obtained by pullback along a degree 2 morphism $\mathbb{P}^1 \to \mathbb{P}^1$ from a 3-branch-point cover. We therefore turned our focus to the most promising of the 3-branch-point covers, those with local monodromy $(2, 23\text{A}, 23\text{B})$.

The computational work needed to construct the polynomials took 11 CPU-hours on a single core of a 12th Gen Intel Core i5-12600KF processor. We verified our final results in Magma 2.29-9 and PARI/GP 2.17.4 without the use of AI; the calculations (done in Magma) in Appendix A for each of the two curves took 40 CPU-hours on a single core of an AMD EPYC 7713 processor.

Acknowledgments

We are very grateful to the American Institute of Mathematics for inviting us to participate in the May 27–30, 2026 workshop "AI and Number Theory," organized in collaboration with the Institute for Computer-Aided Reasoning in Mathematics; we began our research at this workshop. We are also very grateful to workshop participants Michele Tarquini and Zhiyu Zhang for discussions when we were learning the theory and exploring approaches at the beginning of our project. We thank Anthropic for providing workshop participants with a three-month Claude Max subscription. We thank Jean-Pierre Serre for suggestions on the exposition. S. Zhang is especially grateful to his Ph.D. advisor, Tony Yue Yu, for generously supporting and encouraging his independent research, and to his mentor, Liam Li, for insightful discussions on AI and encouragement to pursue this problem.

References

[Bas04] Julius Magalona Basilla, *On the solution of $x^2 + dy^2 = m$*, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), no. 5, 40–41. MR 2062797 14

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478 2

[Bea83] Alan F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics, vol. 91, Springer-Verlag, New York, 1983. MR 698777 6

[Bec89] Sybilla Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra **125** (1989), no. 1, 236–255. MR 1012673 11

[Bel79] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR 534593 2

[CCN+85] John H. Conway, Robert T. Curtis, Simon P. Norton, Richard A. Parker, and Robert A. Wilson, *Atlas of finite groups: Maximal subgroups and ordinary characters for simple groups*, Oxford University Press, Oxford, 1985. 14

[CDyD91] Henri Cohen and Francisco Diaz y Diaz, *A polynomial reduction algorithm*, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 2, 351–360. MR 1149802 12

[CH85] Kevin Coombes and David Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), no. 4, 821–839. MR 816387 3, 5

[CMSV26] Edgar Costa, Michael Musty, Sam Schiavone, and John Voight, *BelyiDB*, `https://github.com`, 2026, Commit 7d5b899. Accessed August 1, 2026. 3, 7

[Elk13] Noam D. Elkies, *The complex polynomials $P(x)$ with* $\mathrm{Gal}(P(x)-t) \cong M_{23}$, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 359–367. MR 3207422 2, 16

[Epo26] Epoch AI, *FrontierMath: Open Problems*, `https://epoch.ai/frontiermath/open-problems`, 2026, Accessed 2026-08-11. 3

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German), English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic Geometry (Storrs, Conn., 1984)*, Springer, New York, 1986. Erratum in: Invent. Math. **75** (1984), 381. MR 718935 (85g:11026a) 14

[Fri77] M. Fried, *Fields of definition of function fields and Hurwitz families—groups as Galois groups*, Comm. Algebra **5** (1977), no. 1, 17–82. MR 453746 2, 4

[FV91] Michael D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800. MR 1119950 2, 5

[Got66] Daniel Henry Gottlieb, *A certain class of incidence matrices*, Proc. Amer. Math. Soc. **17** (1966), no. 6, 1233–1237. 18

[Gra96] Louis Granboulan, *Construction d'une extension régulière de* $\mathbf{Q}(T)$ *de groupe de Galois* M_{24}, Exp. Math. **5** (1996), no. 1, 3–14. MR 1412950 2

[Gro03] Alexander Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques, vol. 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61. Augmenté de deux exposés de M. Raynaud. Updated and annotated reprint of the 1971 original (Lecture Notes in Math. 224, Springer). MR 2017446 10

[Häf87] Frank Häfner, *Realisierung der Mathieugruppen* M_{23} *und* M_{24} *als Galoisgruppen*, Diplomarbeit, Universität Karlsruhe, Karlsruhe, 1987. 2

[Häf22] ———, *Braid orbits and the Mathieu group* M_{23} *as Galois group*, arXiv:2202.08222v3 [math.NT], 2022. 3

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 463157 7, 9

[Hej99] Dennis A. Hejhal, *On eigenfunctions of the Laplacian for Hecke triangle groups*, Emerging applications of number theory (Minneapolis, MN, 1996), IMA Vol. Math. Appl., vol. 109, Springer, New York, 1999, pp. 291–315. MR 1691537 7

[HMW90] Kenneth Hardy, Joseph B. Muskat, and Kenneth S. Williams, *A deterministic algorithm for solving* $n = fu^2 + gv^2$ *in coprime integers* u *and* v, Math. Comp. **55** (1990), no. 191, 327–343. MR 1023762 14

[HS85] Gudrun Hoyden-Siedersleben, *Realisierung der Jankogruppen* J_1 *und* J_2 *als Galoisgruppen über* $\mathbf{Q}$, J. Algebra **97** (1985), no. 1, 17–22. MR 812166 2

[HSM86] Gudrun Hoyden-Siedersleben and B. Heinrich Matzat, *Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilungskörpern*, J. Algebra **101** (1986), no. 1, 273–286. MR 843705 2

[Hun86] David C. Hunt, *Rational rigidity and the sporadic groups*, J. Algebra **99** (1986), no. 2, 577–592. MR 837564 1, 2

[KMSV14] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS J. Comput. Math. **17** (2014), no. 1, 379–430. MR 3356040 6, 7, 18

[Kön14] Joachim König, *The inverse Galois problem and explicit computation of families of covers of* $\mathbb{P}^1_{\mathbb{C}}$ *with prescribed ramification*, Ph.D. thesis, Universität Würzburg, 2014, `https://opus.bibliothek.uni-wuerzburg.de/opus4-wuerzburg/frontdoor/deliver/index/docId/10014/file/Koenig_Joachim_Dissertation.pdf`. 3

[LL26] François Le Lay, *Minimal-degree projection, Fano-plane arithmetic, and the finite Hurwitz scheme of a regular Mathieu* M_{23}*-cover*, preprint, 2026. 9, 13

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534. MR 682664 8

[Mal88] Gunter Malle, *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$*,* M_{22}*, and* $\mathrm{PSL}_3(\mathbf{F}_4) \cdot 2_2$ *over* $\mathbf{Q}$, Math. Comp. **51** (1988), no. 184, 761–768. MR 958642 2

[Mat79] B. Heinrich Matzat, *Konstruktion von Zahlkörpern mit der Galoisgruppe* M_{11} *über* $\mathbf{Q}(\sqrt{-11})$, Manuscripta Math. **27** (1979), no. 1, 103–111. MR 524980 2

[Mat84] ———, *Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe*, J. Reine Angew. Math. **349** (1984), 179–220. MR 743971 2

[Mat85] ———, *Zwei Aspekte konstruktiver Galoistheorie*, J. Algebra **96** (1985), no. 2, 499–531. MR 810543 2

[Mat89] ———, *Rationality criteria for Galois extensions*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 361–383. MR 1012171 2

[Mat91] ———, *Zöpfe und Galoissche Gruppen*, J. Reine Angew. Math. **420** (1991), 99–159. MR 1124568 2

[MM18] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, second ed., Springer Monographs in Mathematics, Springer, Berlin, 2018. MR 3822366 1, 2, 5, 6, 12

[MSSV19] Michael Musty, Sam Schiavone, Jeroen Sijsling, and John Voight, *A database of Belyi maps*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 375–392. MR 3952023 6, 7

[MZM86] B. Heinrich Matzat and Andreas Zeh-Marschke, *Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über* **Q**, J. Number Theory **23** (1986), no. 2, 195–202. MR 845901 2

[MZM87] ———, *Polynome mit der Galoisgruppe M_{11} über* **Q**, J. Symbolic Comput. **4** (1987), no. 1, 93–97. MR 908416 2

[OV00] Fabrice Orgogozo and Isabelle Vidal, *Le théorème de spécialisation du groupe fondamental*, Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., vol. 187, Birkhäuser, Basel, 2000, pp. 169–184. MR 1768100 10

[Pah88] H. Pahlings, *Some sporadic groups as Galois groups*, Rend. Sem. Mat. Univ. Padova **79** (1988), 97–107. MR 964023 2

[Pah89] ———, *Some sporadic groups as Galois groups. II*, Rend. Sem. Mat. Univ. Padova **82** (1989), 163–171, Errata corrige: Rend. Sem. Mat. Univ. Padova **85** (1991), 309–310, MR 1142546, `https://www.numdam.org/item?id=RSMUP_1991__85__309_0`. MR 1049591 2

[PAR26] The PARI Group, Univ. Bordeaux, *PARI/GP version 2.17.4*, 2026, available from `https://pari.math.u-bordeaux.fr/`. 12

[SAI26] SAIR Foundation, *Inverse Galois Problem (IGP24): The inverse Galois Problem in degree 24*, `https://competition.sair.foundation/competitions/igp24/overview`, 2026, Accessed September 7, 2026. 2

[Seg25] Béranger Seguin, *Fields of definition of components of Hurwitz spaces*, Annali della Scuola Normale Superiore - Classe di Scienze (2025), 1–26, `https://journals.sns.it/index.php/annaliscienze/article/view/6924/2382`. 3

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 15, 17

[Ser92] ———, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Darmon, with a foreword by Darmon and the author. MR 1162313 1, 4, 5

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, edited by Martin Brown and Michel Waldschmidt, with a foreword by Brown and Serre. MR 1757192 4

[Shi74] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120. MR 332725 2

[Sin72] David Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38. MR 322165 11

[Sta84] H. M. Stark, *Fourier coefficients of Maass waveforms*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 263–269. MR 803370 7

[Tho84] John G. Thompson, *Some finite groups which appear as* $\mathrm{Gal}(L/K)$*, where* $K \subseteq \mathbf{Q}(\mu_n)$, J. Algebra **89** (1984), no. 2, 437–499. MR 751155 2

[vBCE+26] Raymond van Bommel, Edgar Costa, Noam D. Elkies, Timo Keller, Sam Schiavone, and John Voight, *The constructive inverse Galois problem via Hilbert modular forms: realizing the transitive group 17T7*, 2026, arXiv:2411.07857v4. 2

[vBCPS26] Raymond van Bommel, Edgar Costa, Bjorn Poonen, and Padmavathi Srinivasan, *Curve equations from expansions of 1-forms at a nonrational point*, LuCaNT: databases, algorithms, and

computational number theory, Contemp. Math., vol. 840, Amer. Math. Soc., [Providence], RI, 2026, pp. 345–354. MR 5070733 7

[Wei48] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publications de l'Institut de Mathématiques de l'Université de Strasbourg [Publications of the Mathematical Institute of the University of Strasbourg], vol. 7 (1945), Hermann & Cie, Paris, 1948, Actualités Scientifiques et Industrielles, No. 1041. [Current Scientific and Industrial Topics]. MR 27151 17

[Wil09] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009. MR 2562037 14

[Wit25] Olivier Wittenberg, *Around the inverse Galois problem*, Number theory informed by computation, IAS/Park City Math. Ser., vol. 29, Amer. Math. Soc., Providence, RI, 2025, pp. 291–322. MR 5026007 1

[Zyw25] David Zywina, *Inverse Galois problem for small simple groups*, 2025, Accessed August 11, 2026. Available at `https://davidzywina.github.io/papers/smallGalois.pdf`. 2

Department of Mathematics, Temple University, Philadelphia, PA 19122, USA
Email address: `xiaoyu.huang@temple.edu`
URL: `https://sites.google.com/view/xiaoyuhuang/home`

Institute for Computer-Aided Reasoning in Mathematics, Carnegie Mellon University, Pittsburgh, PA 15213, USA
Email address: `jackson@icarm.io`
URL: `https://www.blakejacksonmath.com/`

Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA
Korea Institute for Advanced Study, Seoul 02455, Republic of Korea
Email address: `khlee@math.uconn.edu`
URL: `https://khlee-math.github.io/`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: `poonen@math.mit.edu`
URL: `http://math.mit.edu/~poonen/`

Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA
Email address: `pries@colostate.edu`
URL: `http://math.colostate.edu/~pries/`

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA
Email address: `szhang7@caltech.edu`
URL: `https://www.shaowuzhang.com/`