ESSENTIAL DIMENSION RELATIVE TO BRANCHED COVERS OF DEGREE AT MOST N

BENSON FARB AND JESSE WOLFSON

Abstract. We prove for various finite groups G and integers $n \geq 1$ that there are families of equations with Galois group G that cannot be simplified to a one-parameter family even after adjoining a root of a polynomial of degree at most n. In more geometric language, there are G-varieties X with the following property: for any G-equivariant branched cover $\widetilde{X} \to X$ of degree $\leq n$, there is no dominant rational G-map $\widetilde{X} \dashrightarrow C$ to any G-curve C. The method of proof is new, and applies in cases where previous methods do not.

1. Introduction

Let k be a perfect field. A *G-variety* over k is a k-variety X equipped with a faithful action of a finite group G on X by birational automorphisms. A *G-compression* is a dominant rational map

$$f : X \dashrightarrow Y$$

of G-varieties; equivalently, the G-action on X is the pullback via f of the G-action on Y. In classical language, a G-compression is a simplification of equations via a rational change of variables.

Example 1.1 (Kummer's theorem). Suppose that $\mathrm{char}(k) \nmid n$ and that k contains a primitive n^{th} root of unity $\zeta \in k$. Then every $\mathbb{Z}/n\mathbb{Z}$-variety compresses to $\mathbb{P}^1$ with its standard $\mathbb{Z}/n\mathbb{Z}$-action $z \mapsto \zeta \cdot z$. In Galois-theoretic terms, every cyclic extension of a function field of k-varieties is given by "adjoining an n^{th} root".

In contrast, Felix Klein proved that if $\mathrm{char}(k) = 0$ then there is an A_5-action on $\mathbb{P}^2$ that cannot be compressed to any A_5-action on a 1-dimensional variety. To state this result in modern terms we need the following definition of Buhler-Reichstein [BR97].

Definition 1.2 (Essential dimension). *Let k be a field. The* essential dimension *over k of a faithful G-variety X, denoted $\mathrm{ed}_k(X \dashrightarrow X/G)$ or $\mathrm{ed}_k(X)$, is the smallest $d \geq 1$ so that there is a G-compression $X \dashrightarrow Y$ over k to a d-dimensional faithful G-variety Y.*

Kummer's theorem gives $\mathrm{ed}_k(X) = 1$ for every $\mathbb{Z}/n\mathbb{Z}$-variety X over k with a primitive n^{th} root of unity; Klein's theorem gives $\mathrm{ed}_k(\mathbb{P}^2 \to \mathbb{P}^2/A_5) = 2$.[1] In contrast to his incompressibility result for A_5, Klein proved that every A_5 extension of function fields is indeed icosahedral after adjoining a square root. In more geometric language:

The authors are partially supported by NSF grants DMS- 2203355(BF), and DMS-1944862 and DMS-2506184 (JW).

[1] This holds for any field k not containing $\mathbb{F}_4$, cf. [Led07, Proposition 5] and [CHKZ08, Theorem 1.6].

Theorem 1.3 (Klein's Normalformsatz). *Let k be a field of characteristic 0 with $\sqrt{5} \in k$. Let X be any A_5-variety over k. Then X has an A_5-equivariant branched cover*[2] $\widetilde{X} \dashrightarrow X$ *of degree at most* 2 *such that there is an A_5-compression*

$$\widetilde{X} \dashrightarrow \mathbb{P}^1.$$

Klein's Normalformsatz is an example of a general classical problem, studied by Hamilton [Ha1836], Sylvester-Hammond [SH1887, p.1] and many others, which asks: can one reduce the number of variables in a system of polynomials by adjoining the solutions of a lower degree polynomial? In more geometric language [3]:

Problem 1.4 (Hamilton [Ha1836]**).** *Let k be a field. Compute, for a given faithful G-variety X and $n \geq 1$,*

$$\mathrm{ed}_k(X; \leq n) := \min\{\dim(Y) : \exists\ \widetilde{X} \overset{\leq n}{\dashrightarrow} X \text{ and } \exists\ G\text{-compression } \widetilde{X} \dashrightarrow Y\} \tag{1.1}$$

where the min ranges over all faithful G-varieties $\widetilde{X}$ and Y over k and all branched covers $\widetilde{X} \dashrightarrow X$ of degree at most n. Further, for a given finite group G, compute

$$\mathrm{ed}_k(G; \leq n) := \sup \mathrm{ed}_k(X; \leq n) \tag{1.2}$$

where the supremum is taken over all faithful G-varieties X. [4]

Remark 1.5.

(1) The assumption that the G-actions are faithful is critical. Without this, there is always the trivial map to a point (with constant G-action).
(2) In classical language, the G-variety X encodes the problem of solving for $x \in X$ such that $f(x) = y$ for given y, where $f\colon X \to X/G = Y$ is the quotient. In this language, Problem 1.4 asks how simply an equation with Galois group G can be solved using elimination theory and an accessory algebraic function of degree at most n.

One reason for Klein's and others' interest in Problem 1.4 is that many of the known solutions to classical equations, for example those involving modular functions and those in enumerative geometry, are of this form; namely, where one can reduce the number of variables by adjoining the roots of a polynomial of lower degree. See [FW19] and [FKW23] for many examples. Klein's theorems mentioned above can be written as:

$$\mathrm{ed}_k(A_5) = 2 \quad \text{but} \quad \mathrm{ed}_k(A_5; \leq 2) = 1$$

for any k with $\mathrm{char}(k) = 0$ and with $\sqrt{5} \in k$.

While the literature of the last 200 years contains upper bounds for $\mathrm{ed}_{\mathbb{C}}(G; \leq n), n \geq 2$ for many examples, lower bounds are lacking, even in the simplest cases. For example,

[2] By a *degree n branched cover* we mean a generically n-to-1, dominant rational map $\tilde{X} \dashrightarrow X$.

[3] We leave it to the reader to write down the equivalent Galois-theoretic formulation.

[4] It is known that $\mathrm{ed}_k(G; \leq n) = \mathrm{ed}_k(V; \leq n)$ for any faithful linear G-variety V (e.g. [FKW23, Example 4.6 and Lemma 4.9]).

Klein proved that any $\mathrm{PSL}_2(\mathbb{F}_7)$-variety X has an at-most 4-sheeted branched cover $\widetilde{X}$ that compresses to the Klein quartic curve, so that

$$\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_7); \leq 4) = 1.$$

Can one do better, replacing $n = 4$ by $n = 2$ or $n = 3$? Corollary 1.7 below implies that the answer is "no" for $n = 2$; that is, $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_7); \leq 2) > 1$. The case $n = 3$ remains open.

Results. The main technical result of this paper is the following. Its proof exploits the classical geometry of G-curves (see below).

Theorem 1.6 (Main Theorem). *Let k be a perfect field. Let $n \geq 2$. Let G be a finite group such that:*

1. *G has no proper subgroup of index at most n (in particular $|G| > n$),*
2. *G contains a subgroup M with $|M| > n$ that acts faithfully on $\mathbb{P}^1$ over k, and*
3. *G does not act nontrivially on a smooth curve of genus $g \leq (n-1)^2$.*

Then $\mathrm{ed}_k(G; \leq n) > 1$.

Theorem 1.6 is applicable because its three hypotheses are easy to check in examples. Over $\mathbb{C}$, we can apply it to give the following.

Corollary 1.7 (Sample results).

1. *Let G be any non-abelian simple finite group except A_5. Then*
$$\mathrm{ed}_{\mathbb{C}}(G; \leq 2) > 1.$$
2. $\mathrm{ed}_{\mathbb{C}}(A_7; \leq 6) > 1$.
3. *Let $p \geq 7$ be prime, and let $n \leq \min\{p-1, 1 + \lfloor\sqrt{1 + \frac{p(p^2-1)}{168}}\rfloor\}$ (note that for $p > 163$ this min equals $p-1$). Then*
$$\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_p); \leq n) > 1.$$

Remarks 1.8.

1. Item 1 shows that Klein's *Normalformsatz* (Theorem 1.3) is exceptional among finite simple groups.
2. In the spirit of Hilbert's 13th problem, Item 2 shows that the general degree 7 polynomial cannot be reduced to a 1-variable algebraic function even after allowing an accessory sextic.
3. Item 3 shows that for each $n \geq 1$ the theory of $\mathrm{ed}_{\mathbb{C}}(-; \leq n)$ is nontrivial.
4. A finite group G is the Galois group of a family of polynomials of degree $\mu(G)$, where $\mu(G)$ denotes the order of the smallest permutation representation. A sharpened version of Problem 1.4 asks for lower bounds on $\mathrm{ed}_k(G, \leq \mu(G) - 1)$.[5] Item 2 of Corollary 1.7 addresses this sharp version of Problem 1.4 over $\mathbb{C}$ for A_7. Similarly, for $p > 11$, Galois showed that $\mu(\mathrm{PSL}_2(\mathbb{F}_p)) = p + 1$. Thus, for $p > 163$, the n in Item 3 is only off by 1 from the natural choice of $n = p$.

[5] e.g. for $G = A_n$, this sharpened version asks how much we can simplify the general degree n polynomial using only the solution of a single polynomial of lower degree.

Remark 1.9 (**Previous methods**)**.** All work up to this point has given lower bounds only for the version of Problem 1.4 where for a given prime p, *any* degree prime to p branched cover $\widetilde{X} \to X$ is allowed; this is called the *"essential dimension at p"* and is denoted by $\mathrm{ed}(X;p)$. See, e.g. [BR99, RY00, KM08, Rei10, FKW21, BF24, FKW23, FKW24]. These methods applied to $\mathrm{ed}(G;\leq n)$ give exactly the following:

$$\mathrm{ed}_k(G;\leq n) \geq \max\{\{\mathrm{ed}_k(G;p)\}_{p>n}, \{\mathrm{ed}_k(P;\leq n)\}_{P\subset G\ p\text{-Sylow},\ p\leq n}\}. \tag{1.3}$$

Classical questions about the complexity of solving polynomials, e.g. Problem 1.4, impose a different set of requirements on the collection of branched covers allowed. To tackle these it is necessary to move beyond what essential dimension at p can give.

As an example, we claim that for $k = \mathbb{C}$, $G = A_7$ and $n = 6$ the inequality (1.3) is strict, and so does not suffice to prove Corollary 1.7 (2), since the right-hand side of (1.3) equals 1 in this case. To prove this claim, first note that

$$|A_7| = 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7$$

implies that $\mathrm{ed}_{\mathbb{C}}(A_7;p) \leq 1$ for $p \geq 5$. For $p = 2, 3$, the p-Sylow of A_7 is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, and since $6 = 2 \cdot 3$, we can kill off a $\mathbb{Z}/p\mathbb{Z}$ factor in both cases by adjoining a 6^{th} root. Kummer's theorem implies that the right-hand side of (1.3) for A_7 and $n = 6$ equals 1, as claimed. Similar arguments show that the special cases of Corollary 1.7

$$\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_7);\leq 2) > 1, \quad \mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_{11});\leq 3) > 1, \quad \text{and} \quad \mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_{13};\leq 4) > 1$$

give further examples where the inequality (1.3) is strict.

The outline of the proof of Theorem 1.6 proceeds as follows. We assume the theorem is false, and from this we construct a single G curve C to which every G-variety compresses after taking a degree $\leq n$ cover. We then construct a G-curve to violate this. The key invariant we use to prove certain curves cannot compress to others is the gonality of a curve.

Acknowledgements. It is a pleasure to thank Mark Kisin for many comments, questions and discussions which helped sharpen and improve this paper. We thank Curt McMullen and Zinovy Reichstein for helpful comments on a draft.

2. Rational functions on curves

We work throughout over a perfect field k. Our main tool is Castelnuovo's inequality (see [Sti09, Theorem 3.11.3] and also [Acc70, Proposition 1] for $k = \mathbb{C}$).

Theorem 2.1 (Castelnuovo's Inequality)**.** *Let C be an irreducible algebraic curve over a perfect field k. Let $f_i\colon C \to D_i$ be rational maps of curves of degree $n_i \geq 1$ for $i = 1, 2$. Assume that the map $(f_1, f_2)\colon C \to D_1 \times D_2$ is birational onto its image. Then*

$$g(C) \leq n_1 g(D_1) + n_2 g(D_2) + (n_1 - 1)(n_2 - 1).$$

We need a slightly more general form of [Sti09, Corollary 3.11.4]; presumably the following lemma was known to Riemann.

Lemma 2.2. *Let C be an algebraic curve of genus $g(C)$ over a perfect field k. Let $j \geq 1$ and let $f_i \colon C \to \mathbb{P}^1$ (so $f_i \in k(C)$) have degree $n \geq 1$ for $i = 1, \dots, j$. If $k(f_1, \dots, f_j) = k(C)$, then*

$$g(C) \leq (n-1)^2.$$

We remark that $k(f_1, \dots, f_j)$ is the function field of the curve that is the image of the map $C \to \mathbb{P}^1_1 \times \cdots \times \mathbb{P}^1_j$ under the map $z \mapsto (f_1(z), \dots, f_j(z))$.

Proof. We prove this by induction on j. The case $j = 2$ is exactly the "Riemann Inequality", stated as [Sti09, Corollary 3.11.4]. For the induction step, let $F' = k(f_1, \dots, f_{j-1}) \subset k(C)$. Denote by $g(F')$ the genus of the smooth projective curve with function field F'. Let $n/m = [k(C) : F']$. Then $[F' : k(f_i)] = m$ for all $i = 1, \dots, j-1$, and by the inductive hypothesis,

$$g(F') \leq (m-1)^2.$$

By Castelnuovo's Inequality [Sti09, Theorem 3.11.3],

$$\begin{aligned} g(C) &\leq \frac{n}{m} g(F') + (\frac{n}{m} - 1)(n-1) \\ &\leq \frac{n}{m}(m-1)^2 + (\frac{n}{m} - 1)(n-1) \\ &= \frac{n^2}{m} - 3n + nm + 1 \\ &=: h_n(m). \end{aligned}$$

Because $m \mid n$, it suffices to prove that $h_n(m) \leq (n-1)^2$ for all $m \in [1, n]$. For this, consider the function $h_n(t) = \frac{n^2}{t} - 3n + nt + 1$ as an analytic function of t on the positive real line. For $t = 1, n$, we have

$$h_n(1) = h_n(n) = n^2 - 2n + 1 = (n-1)^2.$$

Taking the derivative in t, we see that $h_n'(t) = n - \left(\frac{n}{t}\right)^2$, and thus $h_n(t)$ has a unique critical point in the positive reals at $t = \sqrt{n} \in [1, n]$. Therefore, the maximum of $h_n(t)$ for $t \in [1, n]$ occurs at $t = \sqrt{n}$ or at one of the endpoints $t = 1, n$. But for $n > 1$:

$$\begin{aligned} h_n(\sqrt{n}) &= 2n\sqrt{n} - 3n + 1 \\ &= (2\sqrt{n} - 1)n - 2n + 1 \\ &\leq n^2 - 2n + 1 \\ &= h_n(1) = h_n(n) = (n-1)^2. \end{aligned}$$

We conclude that $h_n(t) \leq (n-1)^2$ for all $t \in [1, n]$ and thus conclude the inductive step as claimed. ☐

Corollary 2.3. *Let G be a finite group. Assume that $|G| \nmid n$ and that G does not act nontrivially on an algebraic curve of genus at most $(n-1)^2$. Then no faithful irreducible G-curve C admits a degree n rational function.*

Proof. Let C be a faithful G curve. Suppose the contrary, i.e. there exists a degree n map $f\colon C \to \mathbb{P}^1$. For $g \in G$, let $f_g\colon C \to \mathbb{P}^1$ denote the map $x \mapsto f(gx)$. Let

$$F = k(\{f_g\}_{g\in G}) \subset k(C)$$

denote the compositum. By construction, the field F is G-invariant. By Lemma 2.2, $g(F) \leq (n-1)^2$. Therefore, our assumption on G implies that $F \subset k(C)^G$, i.e. G fixes all the elements of F, and thus $F = k\left(\{f_g\}_{g\in G}\right) = k(f)$. But then,

$$\begin{aligned} n = [k(C) : k(f)] &= [k(C) : k(C)^G][k(C)^G : k(f)] \\ &= |G|[k(C)^G : k(f)] \end{aligned}$$

which contradicts our assumption that $|G| \nmid n$. □

We close this section with two additional lemmas. First, a standard exercise with the field norm shows the following.

Lemma 2.4. *Let C be an irreducible curve. Suppose there exists a dominant map $H \to C$ and a degree n rational function $h\colon H \to \mathbb{P}^1$. Then C has a degree n rational function $f\colon C \to \mathbb{P}^1$.*

Proof. Let $h\colon H \to \mathbb{P}^1$ be a degree n map. Let $N_{k(H)/k(C)}\colon k(H)^\times \to k(C)^\times$ denote the field norm. Then $f := N_{k(H)/k(C)}(h) \in k(C)$ is degree n. □

3. Induced Actions on Unions of Rational Curves

As above, we work over a perfect field k. Our main invariant for showing $\mathrm{ed}_k(-;\leq n) > 1$ comes from studying actions on unions of rational curves induced from a finite subgroup of $\mathrm{PSL}_2(k)$. We can now state and prove our key lemma.

Lemma 3.1. *Let G be a finite group. Let k be a perfect field. Suppose that:*

1. $\mathrm{ed}_k(G;\leq n) = 1$,
2. *G has no proper subgroup of index at most n, and*
3. *G contains a subgroup $M \subset G$ such that $M \hookrightarrow \mathrm{PSL}_2(k)$ and $|M| > n$.*

Then there exists a smooth, irreducible, projective faithful G-curve $\tilde{C}$ with a degree m rational function $f\colon \widetilde{C} \to \mathbb{P}^1$ for some $m \leq n$.

Proof. We work throughout in the birational category, i.e. the category of varieties and rational maps.

Let V be a faithful representation of G, viewed as a linear variety. By assumption, there exists a branched cover $\pi\colon E \dashrightarrow V/G$, of degree $\leq n$ such that $\pi^*(V \to V/G)$ arises (rationally) by pullback from a G-cover of smooth projective curves $\tilde{C} \to C$. Extend the inclusion of function fields $\kappa(V/G) \to \kappa(E)$ to an inclusion of separably closed fields $\bar{\kappa}(V/G) \to \bar{\kappa}(E)$, and consider the maps

$$\mathrm{Gal}(\bar{\kappa}(E)/\kappa(E)) \to \mathrm{Gal}(\bar{\kappa}(V/G) \to \kappa(V/G)) \to G.$$

corresponding to $V \to V/G$. The second map is surjective, and the image of the composite map has index $\leq n$, as π has degree $\leq n$. By our assumption on G, we conclude that the composite map is surjective, and hence $\pi^*(V) \to E$ is an irreducible G-cover. In particular, $\tilde{C}$ is irreducible.

Next we remark that since $V \to V/G$ is G-versal, it is M-versal. Indeed, if X is any M-variety, one may apply G-versality to $(X \times G)/M$. Thus there is a rational, M-equivariant map $\mathbb{P}^1 \to V$, corresponding to $Y := \mathbb{P}^1/M \to V/G$. Let $Y_E = \pi^*(Y)$, let $\kappa(Y_E) \supset \kappa(Y)$, be the function field at some generic point of Y_E, and let $\bar{\kappa}(Y_E)$ be a separable closure of $\kappa(Y_E)$. Consider the composite

$$\mathrm{Gal}(\bar{\kappa}(Y_E)/\kappa(Y_E)) \to \mathrm{Gal}(\bar{\kappa}(Y_E)/\kappa(Y)) \to M.$$

The second map is surjective, and the image of the composite has index $\leq n$. In particular, this image is non-trivial, as $|M| > n$. Hence the composite map

$$Y_E \to E \to C$$

is non-constant, and so the corresponding M-equivariant map $\tilde{Y}_E : \pi^*(\mathbb{P}^1) \to \tilde{C}$ is nonconstant. As $\tilde{Y}_E \to \mathbb{P}^1$ has degree $\leq n$, we conclude by Lemma 2.4, that $\widetilde{C}$ admits a map $h\colon \widetilde{C} \to \mathbb{P}^1$ of degree $\leq n$. □

4. Finishing the proofs of Theorem 1.6 and Corollary 1.7

We now complete the proofs of the theorems stated in the introduction.

Proof of Theorem 1.6. Let $n \geq 1$. Let G be a finite group satisfying the assumptions of the theorem. Suppose to the contrary that $\mathrm{ed}_k(G; \leq n) = 1$. By Lemma 3.1, there exists a smooth, irreducible projective curve $\widetilde{C}$ with a faithful G-action and a degree m rational function for some $m \leq n$. By Corollary 2.3, this implies that G acts nontrivially on a curve of genus at most $(m-1)^2 \leq (n-1)^2$. But this contradicts Assumption (3) of the theorem. Thus $\mathrm{ed}_k(G; \leq n) > 1$. □

There are infinitely many examples of (k, G, n) to which Theorem 1.6 applies: e.g. for $k = \mathbb{C}$, G simple, and for

$$n \leq \min\{d(G), \max\{m \mid C_{m+1} \subset G, 1 + \sqrt{1 + |G|/84}\}\} \tag{4.1}$$

where $d(G)$ denotes the size of the smallest permutation representation of G. For the finite groups G of classical type, a complete list of $d(G)$ is given in [Coo78, Table 1]. For every finite simple group G the number $d(G)$ can be extracted from the classification of finite simple groups (e.g. see the Atlas [CCN+85] for the sporadic simple groups), and by Cauchy's Lemma, one can replace the max over cyclic subgroups in (4.1) by $p-1$ for p the largest prime dividing $|G|$. As the labeling implies, Corollary 1.7 gives a set of such examples.

Proof of Corollary 1.7. We start with statement 1. Let G be a non-abelian finite simple group not isomorphic to A_5. As every index 2 subgroup is normal, G has no proper subgroup of index 2. Further, there exists an odd prime p such that $p \mid |G|$, and thus by Cauchy's lemma, a cyclic subgroup $C_p \subset G$ of order greater than 2. By Theorem 1.6, it suffices to prove that G does not act on an elliptic or rational curve over $\mathbb{C}$. Because the hyperelliptic involution is unique and central in the automorphism group of a hyperelliptic curve [FK92, Ch. III, Corollaries 2, 3, p. 108], we see that every group acting faithfully on a rational, elliptic or hyperelliptic curve is a subquotient of a C_2-central extension

$$1 \to C_2 \to G \to \bar{G} \to 1$$

with $\bar{G} \subset \mathrm{PGL}_2(\mathbb{C})$. Combining Theorem 1.6 with Klein's [Kl1884] classification of finite Möbius groups, we obtain statement 1.

For statement 2, note that A_7 has no subgroup of index less than 7, and there exists a $C_7 \subset A_7$ (pick a 7-cycle). The argument above combines with the Hurwitz bound to show that A_7 does not act nontrivially on any curve of genus less than 31. But $31 > (6-1)^2 = 25$, so the statement follows from Theorem 1.6.

For the final statement 3, as observed above, for $p \geq 7$ the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple and does not act on a rational or elliptic curve. Therefore, by the Hurwitz bound, $\mathrm{PSL}_2(\mathbb{F}_p)$ does not act on a curve of genus less than $|\mathrm{PSL}_2(\mathbb{F}_p)|/84 + 1$. It remains to verify the first two assumptions of Theorem 1.6. For $p = 7, 11$, $\mathrm{PSL}_2(\mathbb{F}_p)$ has no subgroup of index less than p, and the upper bound on n above is equal to $1 + \lfloor\sqrt{1 + \frac{p(p^2-1)}{168}} < p - 1$. For $p > 11$, Galois showed that $\mathrm{PSL}_2(\mathbb{F}_p)$ has no subgroup of index less than $p+1$ (cf. [Coo78, p. 213]). In all cases, we see that $\mathrm{PSL}_2(\mathbb{F}_p)$ satisfies the first assumption in the statement of Theorem 1.6. For the second assumption, note that for all $p > 2$, we have $|\mathrm{PSL}_2(\mathbb{F}_p)| = \frac{p(p^2-1)}{2}$. By Cauchy's Lemma, $C_p \subset \mathrm{PSL}_2(\mathbb{F}_p)$. In each case, we conclude by Theorem 1.6 that $\mathrm{ed}_{\mathbb{C}}(\mathrm{PSL}_2(\mathbb{F}_p); \leq n) > 1$. □

References

[Acc70] R. Accola, *Strongly branched coverings of closed Riemann surfaces*, Proc. Amer. Math. Soc. **26** (1970), 315322.

[BF24] Patrick Brosnan and Najmudden Fakhruddin, *Fixed points in toroidal compactifications of Shimura varieties and essential dimension of congruence covers*, J. Alg. Geom. **33** (2024), no. 2, 295–346.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.

[BR99] Joe Buhler and Zinovy Reichstein, *On Tschirnhaus transformations*, Topics in number theory (University Park, PA, 1997) **467** (1999), no. 2, 127–142.

[CCN+85] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of Finite Groups - Maximal Subgroups and Ordinary Characters for Simple Groups*, Clarendon Press, Oxford, 1985.

[CGR06] V. Chernousov, P. Gille, and Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), 561–581.

[CHKZ08] H. Chu, S.-J. Hu, M.-C. Kang, and J. Zhang, *Groups with essential dimension one*, Asian J. Math. **12** (2008), no. 2, 177-192.

[Coo78] B. Cooperstein, *Minimal degree for a permutation representation of a classical group*, Israel J. Math. **30** (1978), 213235.

[FW19] B. Farb and J. Wolfson, *Resolvent degree, Hilbert's 13th Problem and Geometry*, L'Enseignement Math. **65** (2019), no. 3, 303–376.

[FKW21] B. Farb, M. Kisin, and J. Wolfson, *The essential dimension of congruence covers*, Compos. Math. **157** (2021), no. 11, 2407-2432.

[FKW23] ———, *Modular functions and resolvent problems (with an appendix by Nate Harman)*, Math. Ann. **386** (2023), 113–150.

[FKW24] ———, *Essential dimension via prismatic cohomology)*, Duke Math. J. **173** (2024), 3059–3106.

[FK92] H. Farkas and I. Kra, *Riemann Surfaces*, Springer, 1992.

[Ha1836] W.R. Hamilton, *Inquiry into the validity of a method recently proposed by George B. Jerrard, esq., for transforming and resolving equations of elevated degrees*, Report of the Sixth Meeting of the British Association for the Advancement of Science (Bristol) (1836), 295-348.

[Ish92] N. Ishii, *Coverings over d-gonal curves*, Tsukuba J. Math. **16** (1992), no. 1, 173189.

[Ish95] ———, *Remarks on d-gonal curves*, Tsukuba J. Math. **19** (1995), no. 2, 329345.

[KM08] N. Karpenko and A. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), 491–508.

[Kl1884] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fnften Grade (Lectures on the Icosahedron and the Solution of the Equation of the Fifth Degree)*, Leipzig, Tübner, 1884.

[Kl1879] ———, *Ueber die Auflösung gewisser Gleichungen vom siebenten und achten Grade*, Math. Ann. **15** (1879), 252-282.

[Led07] A. Ledet, *Finite groups of essential dimension one*, J. Alg. **311** (2007), 31-37.

[Rei10] Z. Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians **II** (2010), 162-188.

[RY00] Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056. With an appendix by János Kollár and Endre Szabó.

[Sti09] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 2009.

[SH1887] J.J. Sylvester and J. Hammond, *On Hamilton's Numbers*, Phil. Trans. R. Soc. London A **178** (1887), 285–312.

Department of Mathematics, University of Chicago
E-mail address: farb@math.uchicago.edu

Department of Mathematics, University of California-Irvine
E-mail address: wolfson@uci.edu