ESSENTIAL DIMENSION OF FINITE GROUPS IN PRIME CHARACTERISTIC

ZINOVY REICHSTEIN† AND ANGELO VISTOLI‡

Abstract. Let F be a field of characteristic $p > 0$ and G be a smooth finite algebraic group over F. We compute the essential dimension $\operatorname{ed}_F(G;p)$ of G at p. That is, we show that

$$\operatorname{ed}_F(G;p) = \begin{cases} 1, \text{ if } p \text{ divides } |G|, \text{ and} \\ 0, \text{ otherwise.} \end{cases}$$

1. Introduction

Let F be a field and G be an algebraic group over F. We begin by recalling the definition of the essential dimension of G.

Let K be a field containing F and $\tau\colon T \to \operatorname{Spec}(K)$ be a G-torsor. We will say that τ descends to an intermediate subfield $F \subset K_0 \subset K$ if τ is the pull-back of some G-torsor $\tau_0\colon T_0 \to \operatorname{Spec}(K_0)$, i.e., if there exists a Cartesian diagram of the form

$$\begin{tikzcd} T \arrow[r] \arrow[d, "\tau"] & T_0 \arrow[d, "\tau_0"] & \\ \operatorname{Spec}(K) \arrow[r] & \operatorname{Spec}(K_0) \arrow[r] & \operatorname{Spec}(F). \end{tikzcd}$$

The essential dimension of τ, denoted by $\operatorname{ed}_F(\tau)$, is the smallest value of the transcendence degree $\operatorname{trdeg}(K_0/F)$ such that τ descends to K_0. The essential dimension of G, denoted by $\operatorname{ed}_F(G)$, is the maximal value of $\operatorname{ed}_F(\tau)$, as K ranges over all fields containing F and τ ranges over all G-torsors $T \to \operatorname{Spec}(K)$.

Now let p be a prime integer. A field K is called p-closed if the degree of every finite extension L/K is a power of p. Equivalently, $\operatorname{Gal}(K^s/K)$ is a pro-p-group, where K^s is a separable closure of K. For example, the field of real numbers is 2-closed. The essential dimension $\operatorname{ed}_F(G;p)$ of G at p is the maximal value of $\operatorname{ed}_F(\tau)$, where K ranges over p-closed fields K containing F, and τ ranges over the G-torsors $T \to \operatorname{Spec}(K)$.

It is easy to see that if τ is a versal torsor in the sense of [Se03, Section 5], then $\operatorname{ed}_F(\tau) = \operatorname{ed}_F(G)$. In fact, $\operatorname{ed}_F(G)$ is the minimal value of $\operatorname{trdeg}(K/F)$ such that there exists a versal G-torsor over K. Similarly, $\operatorname{ed}_F(G;p)$ is the minimal value of $\operatorname{trdeg}(K/F)$

2010 *Mathematics Subject Classification.* 20G15, 14G17.

Key words and phrases. Essential dimension, torsor, Nottingham group, Harbater curve, reduction of structure, Serre's Conjecture I.

†Partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 253424-2017.

‡Partially supported by research funds from the Scuola Normale Superiore.

The authors are grateful to the Collaborative Research Group in Geometric and Cohomological Methods in Algebra at the Pacific Institute for the Mathematical Sciences for their support of this project.

such that there exists a p-versal G-torsor over K; see [DR15, Section 8]. For an overview of the theory of essential dimension, we refer the reader to the surveys [Rei10] and [Me13].

The case where G is a finite group (viewed as a constant group over F) is of particular interest. A theorem of N. A. Karpenko and A. S. Merkurjev [KM08] asserts that in this case

$$\mathrm{ed}_F(G;p) = \mathrm{ed}_F(G_p;p) = \mathrm{ed}_F(G_p) = \mathrm{rdim}_F(G_p)\,, \tag{1}$$

provided that F contains a primitive p-th root of unity ζ_p. Here G_p is any Sylow p-subgroup of G, and $\mathrm{rdim}_F(G_p)$ denotes the minimal dimension of a faithful representation of G_p defined over F. For example, assuming that $\zeta_p \in F$, $\mathrm{ed}_F(G) = \mathrm{ed}(G;p) = r$, if $G = (\mathbb{Z}/p\mathbb{Z})^r$ and $\mathrm{ed}(G) = \mathrm{ed}(G;p) = p$, if G is a non-abelian group of order p^3. Further examples can be found in [MR10].

Little is known about essential dimension of finite groups over a field F of characteristic $p > 0$. A. Ledet [Led04] conjectured that

$$\mathrm{ed}_F(\mathbb{Z}/p^r\mathbb{Z}) = r \tag{2}$$

for every $r \geqslant 1$. This conjecture remains open for every $r \geqslant 3$. In this paper we will prove the following surprising result.

Theorem 1. *Let F be a field of characteristic $p > 0$ and G be a smooth finite algebraic group over F. Then*

$$\mathrm{ed}_F(G;p) = \begin{cases} 1, & \text{if } p \text{ divides } |G|, \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

In particular, Ledet's conjecture (2) fails dramatically if essential dimension is replaced by essential dimension at p.

Before proceeding with the proof of Theorem 1, we remark that the condition that G is smooth cannot be dropped. Indeed, it is well known that $\mathrm{ed}_F(\mu_p^r;p) = r$ for any $r \geqslant 0$. More generally, if G is a group scheme of finite type over a field F of characteristic p (not necessarily finite or smooth), then $\mathrm{ed}_F(G;p) \geqslant \dim(\mathcal{G}) - \dim(G)$, where $\mathcal{G}$ is the Lie algebra of G; see [TV13, Theorem 1.2].

2. Proof of Theorem 1

By [MR10, Lemma 4.1], if the index $[G:G']$ of a subgroup of $G' \subset G$ is prime to p, then

$$\mathrm{ed}_F(G;p) = \mathrm{ed}_F(G';p). \tag{3}$$

In particular, if p does not divide $|G|$, then taking $G' = \{1\}$, we conclude that $\mathrm{ed}_F(G;p) = 0$. On the other hand, if p divides $|G|$, then $\mathrm{ed}_F(G;p) \geqslant 1$; see [Me09, Proposition 4.4] or [LMMR13, Lemma 10.1].

Our goal is thus to show that $\mathrm{ed}_F(G;p) \leqslant 1$. First let us consider the case where G is a finite group, viewed as a constant algebraic group over F. By (3), we may replace G by a Sylow subgroup G_p. In other words, we may assume without loss of generality that G is a p-group. Moreover, since $\mathbb{F}_p \subset F$, $\mathrm{ed}_F(G;p) \leqslant \mathrm{ed}_{\mathbb{F}_p}(G;p)$. Thus, for the purpose of proving the inequality $\mathrm{ed}_F(G;p) \leqslant 1$, we may assume that $F = \mathbb{F}_p$.

Recall that the Nottingham group $\mathrm{Aut}_0(F[[t]])$ is the group of automorphisms σ of the algebra $F[[t]]$ of formal power series such that $\sigma(t) = t + a_2t^2 + a_2t^3 + \dots$, for some $a_2, a_3, \dots \in F$. By a theorem of of Leedham-Green and Weiss [C97, Theorem 3], every finite p-group G embeds into $\mathrm{Aut}_0(F[[t]])$. Fix an embedding $\phi\colon G \hookrightarrow \mathrm{Aut}_0(F[[t]])$. By a theorem of D. Harbater [Ha80, Section 2], there exists a smooth curve X with a G-action defined over F, and an F-point $x \in X$ fixed by G, such that the G-action in the formal neighborhood of x is given by ϕ; see also [Ka86, Theorem 1.4.1] and [BCPS17, Theorem 4.8]. Since ϕ is injective, the G-action on X is faithful. By [DR15, Corollary 8.6(b)], the G-action on X is p-versal. Since $\mathrm{ed}_F(G;p)$ is the minimal dimension of an F-variety Y with a faithful p-versal G-action, we conclude that $\mathrm{ed}_F(G;p) \leqslant 1$. This completes the proof of Theorem 1 in the case where G is a constant group.

Now consider the general case, where G is a smooth finite algebraic group over F. In other words, $G = {}^{\tau}\Gamma$, where Γ is a constant finite group, $A = \mathrm{Aut}_{\mathrm{grp}}(\Gamma)$ is the group of automorphisms of Γ and τ is a cocycle representing a class in $H^1(F, A)$.

Lemma 2. (a) $\mathrm{ed}_F(G) \leqslant \mathrm{ed}_F(\Gamma \rtimes A)$, (b) $\mathrm{ed}_F(G;p) \leqslant \mathrm{ed}(\Gamma \rtimes A;p)$.

The semidirect product $\Gamma \rtimes A$ is a constant finite group. Hence, as we showed above, $\mathrm{ed}_F(\Gamma \rtimes A;p) \leqslant 1$. Theorem 1 now follows from Lemma 2(b). It thus remains to prove Lemma 2.

3. Proof of Lemma 2

We will make use of the following description of $\mathrm{ed}_F(G)$ and $\mathrm{ed}_F(G;p)$ in the case, where G is a finite algebraic group over F. Let $G \to \mathrm{GL}(V)$ be a faitful representation. A compression (respectively, a p-compression) of V is a dominant G-equivariant rational map $V \dashrightarrow X$ (respectively, a dominant G-equivariant correspondence $V \rightsquigarrow X$ of degree prime to p), where G acts faithfully on X. Recall that $\mathrm{ed}_F(G)$ (respectively, $\mathrm{ed}_F(G;p)$) equals the minimal value of $\dim(X)$ taken over all compressions $V \dashrightarrow X$ (respectively all p-compressions $V \rightsquigarrow X$). In particular, these numbers depend only on G and F and not on the choice of the generically free representation V. For details, see [Rei10].

We are now ready to proceed with the proof of Lemma 2. To prove part (a), let V be a generically free representation of $\Gamma \rtimes A$ and let $f\colon V \dashrightarrow X$ be a $\Gamma \rtimes A$-compression, with X of minimal possible dimension. That is, $\dim_F(X) = \mathrm{ed}_F(\Gamma \rtimes A)$. Twisting by τ, we obtain a $G = {}^{\tau}\Gamma$-equivariant map ${}^{\tau}f\colon {}^{\tau}V \dashrightarrow {}^{\tau}X$; see e.g., [FR17, Proposition 2.6(a)]. Now observe that by Hilbert's Theorem 90, ${}^{\tau}V$ is a vector space with a linear action of $G = {}^{\tau}\Gamma$ and ${}^{\tau}f\colon {}^{\tau}V \dashrightarrow {}^{\tau}X$ is a compression. (To see that the G-action on ${}^{\tau}V$ and ${}^{\tau}X$ are faithful, we may pass to the algebraic closure $\overline{F}$ of F. Over $\overline{F}$, τ is split, so that $G = \Gamma$, ${}^{\tau}V = V$, ${}^{\tau}X = X$ and ${}^{\tau}f = f$, and it becomes obvious that the G-actions on ${}^{\tau}V$ and ${}^{\tau}X$ are faithful.) We conclude that $\mathrm{ed}_F(G) \leqslant \dim_F({}^{\tau}X) = \dim_F(X) = \mathrm{ed}_F(\Gamma \rtimes A)$, as desired.

The proof of part (b) proceeds along the same lines. The starting point is a p-compression $f\colon V \rightsquigarrow X$ with X of minimal possible dimension, $\dim_F(X) = \mathrm{ed}_F(\Gamma \rtimes A;p)$. We twist f by τ to obtain a p-compression ${}^{\tau}f\colon {}^{\tau}V \rightsquigarrow {}^{\tau}X$ of the linear action of $G = {}^{\tau}\Gamma$ on ${}^{\tau}V$. The rest of the argument is the same as in part (a). This completes the proof of Lemma 2 and thus of Theorem 1. ♠

4. An application

In this section G will denote a connected reductive linear algebraic group over a field F. It is shown in [CGR06, Theorem 1.1(c)] that there exists a finite F-subgroup $S \subset G$ such that every Γ-torsor over every field K/F admits reduction of structure to S; see also [CGR08, Corollary 1.4]. In other words, the map $H^1(K,S) \to H^1(K,G)$ is surjective for every field K containing F. If this happens, we will say that "G admits reduction of structure to S".

We will now use Theorem 1 to show that if $\mathrm{char}(F) = p > 0$ and p is a torsion prime for G, then S cannot be smooth. For the definition of torsion primes, a discussion of their properties and further references, see [Se00]. Note, in particular, that by a theorem of A. Grothendieck [Gr58], if G is not special (i.e., if $H^1(K,G) \neq \{1\}$ for some field K containing F), then G has at least one torsion prime; see also [Se00, 1.5.1].

Corollary 3. *Let G be a connected linear algebraic group over an algebraically closed field F of characteristic $p > 0$.*

(a) If S is a smooth finite subgroup of G defined over F, then the natural map

$$f_K \colon H^1(K,S) \to H^1(K,G)$$

is trivial for any p-closed field K containing F. In other words, f_K sends every $\alpha \in H^1(K,S)$ to $1 \in H^1(K,G)$.

(b) If p is a torsion prime for G, then G does not admit reduction of structure to any smooth finite subgroup.

Proof. (a) Let $\alpha \in H^1(K,S)$ and $\beta = f_K(\alpha) \in H^1(K,G)$. By Theorem 1, α descents to $\alpha_0 \in H^1(K_0,S)$ for some intermediate field $F \subset K_0 \subset K$, where $\mathrm{trdeg}(K_0/F) \leqslant 1$. It now suffices to show that $H^1(K_0,G) = \{1\}$. If we can do this, then the diagram

$$\begin{tikzcd}
H^1(K_0,S) \arrow[rrr, "f_{K_0}"] \arrow[ddd] & & & H^1(K_0,G) \arrow[ddd] \\
& \alpha_0 \arrow[r, mapsto] \arrow[d, mapsto] & 1 \arrow[d, mapsto] & \\
& \alpha \arrow[r, mapsto] & \beta & \\
H^1(K,S) \arrow[rrr, "f_K"] & & & H^1(K,G)
\end{tikzcd}$$

shows that $\beta = 1$. Since F is algebraically closed and $\mathrm{trdeg}(K_0/F) \leqslant 1$, the cohomological dimension of K_0 is $\leqslant 1$; see [Se97, §II.3.2]. By Serre's Conjecture I,

$$H^1(K_0,G) = \{1\}, \tag{4}$$

as desired. Note that (4) was proved by R. Steinberg [St65] in the case where K_0 is perfect, and by A. Borel and T. A. Springer [BS68, §8.6] for general K.

(b) If p is a torsion prime for G, then $H^1(K, G) \neq \{1\}$ for some p-closed field K containing F; see [Me09, Proposition 4.4]. In view of part (a), this implies that f_K is not surjective. ♠

References

[BCPS17] F. M. Bleher, T. Chinburg, B. Poonen, P. Symonds, *Automorphisms of Harbater-Katz-Gabber curves*, Math. Ann. **368** (2017), no. 1-2, 811–836. MR3651589

[BS68] A. Borel and T. A. Springer, *Rationality properties of linear algebraic groups. II*, Tôhoku Math. J. (2) **20** (1968), 443–497. MR0244259

[CGR06] V. Chernousov, P. Gille and Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), no. 2, 561–581. MR2201056

[CGR08] V. Chernousov, P. Gille and Z. Reichstein, *Reduction of structure for torsors over semilocal rings*, Manuscripta Math. **126** (2008), no. 4, 465–480. MR2425436

[C97] R. Camina, *Subgroups of the Nottingham group*, J. Algebra **196** (1997), no. 1, 101–113. MR1474165

[CGR06] V. Chernousov, P. Gille and Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), no. 2, 561–581. MR2201056

[DR15] A. Duncan and Z. Reichstein, *Versality of algebraic group actions and rational points on twisted varieties*, J. Algebraic Geom. **24** (2015), no. 3, 499–530. MR3344763

[FR17] M. Florence, Z. Reichstein, *The rationality problem for forms of moduli spaces of stable marked curves of positive genus*, arXiv:1709.05696.

[Gr58] A. Grothendieck, *Torsion homologique et sections rationnelles, SÃČÂľm. Chevalley*, Anneaux de Chow et Applications, exposé 5, 1958.

[Ha80] D. Harbater, *Moduli of p-covers of curves*, Comm. Algebra **8** (1980), no. 12, 1095–1122. MR0579791

[KM08] N. A. Karpenko and A. S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508. MR2393078

[Ka86] N. M. Katz, *Local-to-global extensions of representations of fundamental groups*, Ann. Inst. Fourier (Grenoble) **36** (1986), no. 4, 69–106. MR0867916

[Led04] A. Ledet, On the essential dimension of p-groups, in *Galois theory and modular forms*, 159–172, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004. MR2059762

[LMMR13] R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein, *Essential p-dimension of algebraic groups whose connected component is a torus*, Algebra Number Theory **7** (2013), no. 8, 1817–1840. MR3134035

[Me09] A. S. Merkurjev, Essential dimension, in *Quadratic forms—algebra, arithmetic, and geometry*, 299–325, Contemp. Math., 493, Amer. Math. Soc., Providence, RI, 2009. MR2537108

[Me13] A. S. Merkurjev, *Essential dimension: a survey*, Transform. Groups, 18 (2013), no. 2, 415–481, 2013.

[MR09] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory 3, no. 4 (2009), 467–487.

[MR10] A. Meyer and Z. Reichstein, *Some consequences of the Karpenko-Merkurjev theorem*, Doc. Math. **2010**, Extra vol.: Andrei A. Suslin sixtieth birthday, 445–457. MR2804261

[Rei10] Z. Reichstein, Essential dimension, in *Proceedings of the International Congress of Mathematicians. Volume II*, 162–188, Hindustan Book Agency, New Delhi, 2010.

[Se97] J.-P. Serre, *Galois cohomology*, translated from the French by Patrick Ion and revised by the author, Springer-Verlag, Berlin, 1997. MR1466966

[Se00] J.-P. Serre, *Sous-groupes finis des groupes de Lie*, Astérisque No. 266 (2000), Exp. No. 864, 5, 415–430. MR1772682

[Se03] J.-P. Serre, *Cohomological invariants, Witt invariants, and trace forms*, in Cohomological invariants in Galois cohomology, **28** Univ. Lecture Ser., pp. 1–100. Amer. Math. Soc., Providence, RI, 2003. Notes by Skip Garibaldi.

[St65] R. Steinberg, *Regular elements of semisimple algebraic groups*, Inst. Hautes Études Sci. Publ. Math., no. 25 (1965), 49–80. MR0180554

[TV13] D. Tossici and A. Vistoli, On the essential dimension of infinitesimal group schemes, Amer. J. Math. **135** (2013), no. 1, 103–114. MR3022958

(Reichstein) Department of Mathematics, University of British Columbia, Vancouver, B.C., Canada V6T 1Z2
E-mail address: reichst@math.ubc.ca

(Vistoli) Scuola Normale Superiore, Piazza dei Cavalieri 7, 56126 Pisa, Italy
E-mail address: angelo.vistoli@sns.it