ESSENTIAL DIMENSION IN MIXED CHARACTERISTIC

PATRICK BROSNAN, ZINOVY REICHSTEIN, AND ANGELO VISTOLI

Abstract. Let R be a discrete valuation ring with residue field k and fraction field K. We say that a finite group G is weakly tame at a prime p if it has no non-trivial normal p-subgroups. By convention, every finite group is weakly tame at 0. We show that if G is weakly tame at $\mathrm{char}(k)$, then $\mathrm{ed}_K(G) \geqslant \mathrm{ed}_k(G)$. Here $\mathrm{ed}_F(G)$ denotes the essential dimension of G over the field F. We also prove a more general statement of this type, for a class of étale gerbes $\mathscr{X}$ over R.

As a corollary, we show that if G is weakly tame at p, then $\mathrm{ed}_K G \geqslant \mathrm{ed}_k G$ for any field K of characteristic 0 and any field k of characteristic p, provided that k contains $\overline{\mathbb{F}}_p$. We also show that a conjecture of A. Ledet, asserting that $\mathrm{ed}_k(\mathbb{Z}/p^n\mathbb{Z}) = n$ for a field k of characteristic $p > 0$ implies that $\mathrm{ed}_{\mathbb{C}}(G) \geqslant n$ for any finite group G which is weakly tame at p and contains an element of order p^n. To the best of our knowledge, an unconditional proof of the last inequality is out of the reach of all presently known techniques.

1. Introduction

Let R be a discrete valuation ring with residue field k and fraction field K, and let G be a finite group. In this paper we will compare $\mathrm{ed}_K(G)$ and $\mathrm{ed}_k(G)$. More generally, we will compare $\mathrm{ed}_K(\mathscr{X})$ to $\mathrm{ed}_k(\mathscr{X})$ for an étale gerbe $\mathscr{X}$ over R. For an overview of the theory of essential dimension, we refer the reader to [BRV11, Mer13, Rei10].

2010 *Mathematics Subject Classification.* 14A20, 13A18, 13A50.

Key words and phrases. Essential dimension, Ledet's conjecture, genericity theorem, gerbe, mixed characteristic.

Patrick Brosnan was partially supported by NSF grant DMS 1361159.

Zinovy Reichstein was partially supported by National Sciences and Engineering Research Council of Canada Discovery grant 253424-2017.

Angelo Vistoli was 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.

To state our main result, we will need some definitions.

Suppose S is a scheme. By an *étale gerbe* $\mathscr{X} \to S$ we mean an algebraic stack that is a gerbe in the étale topology on S. Furthermore, we will always assume that there exists an étale covering $\{S_i \to S\}$, such that the pullback $\mathscr{X}_{S_i}$ is of the form $\mathscr{B}_{S_i} G_i$, where $G_i \to S_i$ is a finite étale group scheme.

We say that a finite group G is *tame* (resp. *weakly tame*) at a prime number p if $p \nmid |G|$ (resp. G contains no non-trivial normal p-subgroup). Equivalently, G is tame at p if the trivial group is the (unique) p-Sylow subgroup of G, and G is weakly tame at p if the intersection of all p-Sylow subgroups of G is trivial. By convention we say that every finite group is both tame and weakly tame at 0.

By a geometric point of S, we mean a morphism $\operatorname{Spec} \Omega \to S$ with Ω an algebraically closed field. We say that a finite étale group scheme G over S is *tame* (resp. *weakly tame*) if, for every geometric point $\operatorname{Spec} \Omega \to S$, the group $G(\Omega)$ is tame (resp. weakly tame) at $\operatorname{char} \Omega$. Similarly, we say that an étale gerbe $\mathscr{X} \to S$ is *tame* (resp. *weakly tame*) if, for every object ξ over a geometric point $\operatorname{Spec} \Omega \to S$, the automorphism group $\operatorname{Aut}_\Omega \xi$ is tame (resp. weakly tame) at $\operatorname{char} \Omega$.

A key result of [BRV11] is the so called *Genericity Theorem* for tame Deligne–Mumford stacks, [BRV11, Theorem 6.1]. The proof of this result in [BRV11] was based on the following.

Theorem 1.1 ([BRV11, Theorem 5.11])**.** *Let R be a discrete valuation ring (DVR) with residue field k and fraction field K, and let*

$$\mathscr{X} \longrightarrow \operatorname{Spec} R$$

be a tame étale gerbe. Then $\operatorname{ed}_K \mathscr{X}_K \geqslant \operatorname{ed}_k \mathscr{X}_k$.

Here $\mathscr{X}_K$ and $\mathscr{X}_k$ are respectively the generic fiber and the special fiber of $\mathscr{X} \to \operatorname{Spec} R$.

Unfortunately, the proof of [BRV11, Theorem 5.11] contains an error in the case when $\operatorname{char} K = 0$ and $\operatorname{char} k > 0$. This was noticed by Amit Hogadi, to whom we are very grateful. (See Remark 4.2 for an explanation of the error.) For the applications in [BRV11] only the equicharacteristic case was needed, so this mistake in the proof of Theorem 1.1 does not affect any other results in [BRV11] (the genericity theorem, in particular). However, the assertion of Theorem 1.1 in the mixed characteristic case remained of interest to us, as a way of relating essential dimension in positive characteristic to essential dimension in characteristic 0. In this paper, our main result is the following strengthened version of Theorem 1.1.

Theorem 1.2. *Let R be a DVR with residue field k and fraction field K, and let*
$$\mathscr{X} \longrightarrow \operatorname{Spec} R$$
be a weakly tame étale gerbe. Then $\operatorname{ed}_K \mathscr{X}_K \geqslant \operatorname{ed}_k \mathscr{X}_k$.

In particular, [BRV11, Theorem 5.11] is valid as stated. Moreover, our new proof is considerably shorter than the one in [BRV11]. And in Section 3 we will deduce some rather surprising consequences.

We will give two proofs of our main result, one for gerbes of the form where $\mathscr{X} = \mathscr{B}_R G$, where G is a (constant) finite group (Theorem 2.4) and the other for the general case. The ideas in these two proofs are closely related; the proof of Theorem 2.4 allows us to introduce these ideas, initially, in the elementary setting of classical valuation theory. A separate proof of Theorem 2.4 also makes the applications in Section 3 accessible to those readers who are not familiar with, or don't care for, the language of gerbes.

2. Proof of Theorem 1.2 in the constant case

In this section we will prove a special case of Theorem 1.2, where $\mathscr{X} = \mathscr{B}_R G$ for G a finite group (viewed as a constant group scheme over $\operatorname{Spec} R$); see Theorem 2.4.

Throughout this section we will assume that L is a field equipped with a (surjective) discrete valuation $\nu\colon L^* \to \mathbb{Z}$ and K is a subfield of L such that $\nu(K^*) = \mathbb{Z}$. We will denote the residue fields of L and K by l and k, respectively. Similarly, we will denote the valuation rings by $\mathscr{O}_L$ and $\mathscr{O}_K$.

The following lemma is a special case of the Corollary to Theorem 1.20 in [Vaq06]. For the convenience of the reader, we supply a short proof.

Lemma 2.1. $\operatorname{trdeg}_k(l) \leqslant \operatorname{trdeg}_K(L)$.

Proof. Let $u_1, \dots, u_m \in l$ be algebraically independent over k. Lift each u_i to $v_i \in \mathscr{O}_L \subseteq L$. It now suffices to show that $v_1, \dots, v_m$ are algebraically independent over K. Assume the contrary: $f(v_1, \dots, v_m) = 0$ for some polynomial $0 \neq f(x_1, \dots, x_m) \in K[x_1, \dots, x_m]$. After clearing denominators we may assume that every coefficient of f lies in $\mathscr{O}_K$, and at least one of the coefficients has valuation 0. If f_0 is the image of f in $k[x_1, \dots, x_m]$ then $f_0 \neq 0$ and $f_0(u_1, \dots, u_m) = 0$. This contradicts our assumption that $u_1, \dots, u_m$ are algebraically independent over k. ♠

Let $L_m = \nu^{-1}(m) \cup \{0\}$ and $L_{\geqslant m} = \bigcup_{j \geqslant m} L_j$. Note that, by definition, $L_{\geqslant 0} = \mathscr{O}_L$ is the valuation ring of ν, $L_{\geqslant 1}$ is the maximal ideal, and $L_{\geqslant 0}/L_{\geqslant 1} = l$ is the residue field.

Lemma 2.2. *Assume that g is an automorphism of L of finite order $d \geqslant 1$, preserving the valuation ν. Let $p = \operatorname{char}(l) \geqslant 0$. If g induces a trivial automorphism on both $L_{\geqslant 0}/L_{\geqslant 1}$ and $L_{\geqslant 1}/L_{\geqslant 2}$, then*

(a) $d = 1$ (i.e., $g = \mathrm{id}$ is the identity automorphism) if $p = 0$, and

(b) d is a power of p, if $p > 0$.

Part (a) is proved in [BR97, Lemma 5.1]; a minor variant of the same argument also proves (b). Alternatively, with some additional work, Lemma 2.2 can be deduced from [ZS58, Theorem 25, p. 295]. For the reader's convenience we will give a short self-contained proof below.

Proof. In case (b), write $d = mp^r$, where m is not divisible by p. After replacing g by g^{p^r}, we may assume that d is prime to p. In both parts we need to conclude that g is the identity.

Let G be the cyclic group generated by g; then G is linearly reductive. Since the action of G on ℓ is trivial, the induced action on $L_{\geqslant i}/L_{\geqslant i+1}$ is ℓ-linear. Furthermore, let $t \in L_1$ be a uniformizing parameter. By our assumption $g(t) = t \pmod{L_{\geqslant 2}}$. Thus multiplication by t^{i-1} induces the ℓ-linear G-equivariant isomorphism $(L_{\geqslant 1}/L_{\geqslant 2})^{\otimes i} \simeq L_{\geqslant i}/L_{\geqslant i+1}$. Consequently, G acts trivially on $L_{\geqslant i}/L_{\geqslant i+1}$ for all $i \geqslant 0$. Since G is linearly reductive, from the exact sequence

$$0 \longrightarrow L_{\geqslant i}/L_{\geqslant i+1} \longrightarrow L/L_{\geqslant i+1} \longrightarrow L/L_{\geqslant i} \longrightarrow 0$$

we deduce, by induction on i, that G acts trivially on $L/L_{\geqslant i}$ for every $i \geqslant 1$. Since $\bigcap_{i \geqslant 0} L_i = 0$, this implies that the action of G on L is trivial. Since G acts faithfully on L, we conclude that $G = \{1\}$, and the lemma follows. ♠

Proposition 2.3. *Consider a faithful action of a finite group G on L, such that G preserves ν and acts trivially on K. Let Δ be the kernel of the induced G-action on l. Then $\Delta = \{1\}$ if $\operatorname{char}(k) = 0$ and Δ is a p-subgroup if $\operatorname{char}(k) = p$.*

Proof. Assume the contrary. Then we can choose an element $g \in \Delta$ of prime order q, such that $q \neq \operatorname{char}(k)$. Let M be the maximal ideal of the valuation ring $\mathscr{O}_L$. Since we are assuming that $\nu(K^*) = \nu(L^*) = \mathbb{Z}$, we can choose a uniformizing parameter $t \in K$ for ν. Since $g \in \Delta$, g acts trivially on both $l = \mathscr{O}_L/M$ and $M/M^2 = l \cdot t$. By Lemma 2.2, g acts trivially on L. This contradicts our assumption that G acts faithfully on L. ♠

We are now ready to prove the main result of this section.

Theorem 2.4. *Let (R,ν) be a discrete valuation ring with residue field k and fraction field K, and G be a finite group. If $p = \mathrm{char}(k) > 0$, assume that G is weakly tame at p. Then $\mathrm{ed}_K(G) \geqslant \mathrm{ed}_k(G)$.*

Proof. Set $d := \mathrm{ed}_K(G)$. Let $R[G]$ be the group algebra of G and let $V_R = (\mathbb{A}_R)^{|G|}$ denote the corresponding R-scheme equipped with the (left) regular action of G. By definition d is the minimal transcendence degree $\mathrm{trdeg}_K(L)$, where L ranges over G-invariant intermediate subfields $K \subset L \subset K(V_K)$ such that the G-action on L is faithful; see [BR97]. Choose a G-invariant intermediate subfield L such that $\mathrm{trdeg}_K(L) = d$.

We will now construct a G-invariant intermediate subfield $k \subset l \subset k(V_k)$, where V_k is the regular representation of G over k, as follows. Lift the given valuation $\nu\colon K^* \to \mathbb{Z}$ to the purely transcendental extension $K(V_K)$ of K in the obvious way. That is, $\nu : K(V_K)^* \to \mathbb{Z}$ is the divisorial valuation corresponding to the fiber of V_R over the closed point in $\operatorname{Spec} R$. The residue field of $K(V_K)$ is then $k(V_k)$. By restriction, ν is a valuation on L with $\nu(L^*) = \mathbb{Z}$. Let l be the residue field of L. Clearly $k \subset l \subset k(V_k)$ and ν is invariant under G. By Proposition 2.3, G acts faithfully on l. Moreover, by Lemma 2.1, $\mathrm{trdeg}_k(l) \leqslant d$. Thus $\mathrm{ed}_k(G) \leqslant d = \mathrm{ed}_K(G)$, as desired. ♠

3. Applications and examples

We begin with the following easy corollary of Theorem 2.4.

Corollary 3.1. *Let p be a prime, G a finite group weakly tame at p. Then*

(a) (*cf.* [Tos17, Corollary 4.2]) $\mathrm{ed}_{\mathbb{Q}}\, G \geqslant \mathrm{ed}_{\mathbb{F}_p} G$.
(b) If K is a field of characteristic 0 and k a field of characteristic p containing $\overline{\mathbb{F}}_p$, then $\mathrm{ed}_K G \geqslant \mathrm{ed}_k G$.

Proof. (a) follows directly from Theorem 2.4 by taking R to be the localization of the ring of integers $\mathbb{Z}$ at a prime ideal $p\mathbb{Z}$.

(b) Let $\overline{K}$ be the algebraic closure of K. Since $\mathrm{ed}_K(G) \geqslant \mathrm{ed}_{\overline{K}}(G)$, we may replace that K by $\overline{K}$ and thus assume that K is algebraically closed. Note that $\mathrm{ed}_K G = \mathrm{ed}_{\overline{\mathbb{Q}}} G$ and $\mathrm{ed}_k G = \mathrm{ed}_{\overline{\mathbb{F}}_p} G$; see [BRV07, Proposition 2.14] or [Tos17, Example 4.10].

Choose a number field $E \subseteq \overline{\mathbb{Q}}$ such that $\mathrm{ed}_E G = \mathrm{ed}_{\overline{\mathbb{Q}}} G$ and let $\mathfrak{p} \subseteq \mathscr{O}_E$ a prime in the ring $\mathscr{O}_E$ of algebraic integers in E lying over p. Set $E_0 \overset{\mathrm{def}}{=} \mathscr{O}_E/\mathfrak{p}$. Since k contains $\overline{\mathbb{F}}_p$, there is an embedding $E_0 \subseteq k$. By Theorem 2.4, $\mathrm{ed}_E(G) \geqslant \mathrm{ed}_{E_0}(G)$ and since $E_0 \subset k$, $\mathrm{ed}_{E_0} G \geqslant \mathrm{ed}_k G$. ♠

Remark 3.2. One could reasonably conjecture that, under the hypotheses of Corollary 3.1(b), $\operatorname{ed}_K G = \operatorname{ed}_k G$, provided that K is algebraically closed.

For our second application, recall the following conjecture of A. Ledet [Led04].

Conjecture 3.3. If k is a field of characteristic $p > 0$, n is a natural number, and C_{p^n} is a cyclic group of order p^n, then $\operatorname{ed}_k(\mathrm{C}_{p^n}) = n$.

It is known that in characteristic p, $\operatorname{ed}(\mathrm{C}_{p^n}) \leqslant n$ for every $n \geqslant 1$ (see [Led04]) and $\operatorname{ed}(\mathrm{C}_{p^n}) \geqslant 2$ if $n \geqslant 2$ ([Led07, Theorems 5 and 7]). Thus the conjecture holds for $n = 1$ and $n = 2$; it remains open for every $n \geqslant 3$.

Conjecture 3.3 has the following surprising consequence.

Corollary 3.4. *Assume that a finite group G is weakly tame at a prime p and contains an element of order p^n. Let K be a field of characteristic 0. If Conjecture 3.3 holds for C_{p^n}, then $\operatorname{ed}_K(G) \geqslant n$.*

Proof. By Corollary 3.1(b), with $k = \overline{\mathbb{F}}_p$, we have $\operatorname{ed}_K(G) \geqslant \operatorname{ed}_k(G)$. Since G contains C_{p^n}, $\operatorname{ed}_k(G) \geqslant \operatorname{ed}_k(\mathrm{C}_{p^n})$, and by Conjecture 3.3, $\operatorname{ed}_k(\mathrm{C}_{p^n}) = n$. ♠

Example 3.5. Let p be a prime and n a positive integer. Choose a positive integer m such that $q \stackrel{\text{def}}{=} mp^n + 1$ is a prime. (By Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many such m.) Let C_q be a cyclic group of order q. Then $\operatorname{Aut}\mathrm{C}_q = (\mathbb{Z}/q\mathbb{Z})^*$ is cyclic of order mp^n; let $\mathrm{C}_{p^n} \subseteq (\mathbb{Z}/q\mathbb{Z})^*$ denote the subgroup of order p^n. Set $G \stackrel{\text{def}}{=} \mathrm{C}_{p^n} \ltimes \mathrm{C}_q$. Then

(a) G is weakly tame at p, and

(b) if Conjecture 3.3 holds, then $\operatorname{ed}_K(G) \geqslant n$ for any field K of characteristic 0.

To prove (a), suppose $S \subseteq G$ is a normal p-subgroup. Then S lies in every Sylow p-subgroup of G, in particular, in C_{p^n}. Our goal is to show that $S = \{1\}$. The cyclic group C_q of prime order q acts on S by conjugation. Since $q > p^n \geqslant |S|$, this action is trivial. In other words, S is a central subgroup of G. In particular, S acts trivially on C_q by conjugation. On the other hand, by the definition of G, C_{p^n} acts faithfully on C_q by conjugation. We conclude that $S = \{1\}$, as desired. Part (b) follows from Corollary 3.4. ♠

Note that the inequality of part (b) is equivalent to

$$\operatorname{ed}_{\mathbb{C}}(\mathrm{C}_{p^n} \ltimes \mathrm{C}_q) \geqslant n\,, \tag{3.1}$$

where $\mathbb{C}$ is the field of complex numbers (once again, see [BRV07, Proposition 2.14] or [Tos17, Example 4.10]). The essential dimension of $\mathrm{C}_{p^n} \ltimes \mathrm{C}_q$ at a prime r is given by

$$\mathrm{ed}_{\mathbb{C}}(G; r) = \begin{cases} \mathrm{ed}_{\mathbb{C}}(\mathrm{C}_{p^n}; p) = 1, \text{ if } r = p \\ \mathrm{ed}_{\mathbb{C}}(\mathrm{C}_q; q) = 1, \text{ if } r = q, \text{ and} \\ \mathrm{ed}_{\mathbb{C}}(\{1\}; r) = 0, \text{ if } r \neq p \text{ or } q. \end{cases}$$

In this case, the inequality (3.1) can be proved unconditionally (i.e., without assuming Conjecture 3.3) for $n = 2$ and 3 by appealing to the classifications of finite groups of essential dimension 1 and 2 over $\mathbb{C}$ in [BR97, Theorem 6.2] and [Dun13, Theorem 1.1] respectively. So, for $n \geqslant 2$, $\mathrm{ed}_{\mathbb{C}}(G; r)$ is smaller than the (absolute) essential dimension $\mathrm{ed}_{\mathbb{C}}(C_{p^n} \ltimes C_q)$. Thus, in the language of [Rei10, Section 5], proving the inequality (3.1) is a "Type 2 problem". As is explained in [Rei10], such problems are only accessible by existing techniques in low dimensions. To the best of our knowledge, an unconditional proof of (3.1), or even of the inequality $\mathrm{ed}_{\mathbb{C}}(\mathrm{C}_{p^n} \ltimes \mathrm{C}_q) \geqslant 4$ for any $n \geqslant 4$, is out of the reach of all currently available techniques.

Remark 3.6. It is shown in [RV17] that if G is a finite group and k is a field of characteristic p, then

$$\mathrm{ed}_k(G; p) = \begin{cases} 1, \text{ if } p \text{ divides } |G|, \text{ and} \\ 0, \text{ otherwise.} \end{cases} \tag{3.2}$$

In particular, Conjecture 3.3 is also a Type 2 problem. Note also that in view of (3.2), Corollary 3.1(b) continues to hold if we replace essential dimension by essential dimension at p, for trivial reasons. Moreover, under the assumptions of Corollary 3.1, (a′) $\mathrm{ed}_{\mathbb{Q}}(G; p) \geqslant \mathrm{ed}_{\mathbb{F}_p}(G; p)$ and (b′) $\mathrm{ed}_K(G; p) \geqslant \mathrm{ed}_k(G; p)$, for any finite group G, not necessarily weakly tame. In (b′) we can also drop the requirement that k should contain $\overline{\mathbb{F}}_p$. Note however that our proof of Theorem 2.4 breaks down if we replace essential dimension by essential dimension at p.

Example 3.7. The following example shows that Theorem 2.4 fails if we do not assume that G is weakly tame. Choose R so that $\mathrm{char}\, K = 0$, $\mathrm{char}\, k = p > 0$, and K contains a p^2-th root of 1. Let $G = C_{p^2}$ be the cyclic group of order p^2. Since K contains a primitive p^2-th root of 1, $\mathrm{ed}_K(G) = \mathrm{ed}_K(\mathrm{C}_{p^2}) = 1$. On the other hand, as we pointed out above, Conjecture 3.3 is known for $n = 2$, and thus $\mathrm{ed}_k(G) = \mathrm{ed}_k(\mathrm{C}_{p^2}) = 2$.

Example 3.8. Here is an example showing that Theorem 2.4 fails if we do not assume that R is a DVR. Let $R \subseteq \mathbb{C}[[t]]$ be the subring consisting of power series in t with constant coefficient, whose constant term is real. Then R is a one-dimensional complete Noetherian local ring with quotient field $K = \mathbb{C}((t))$ and residue field $k = \mathbb{R}$, but not a DVR. In this situation $\operatorname{ed}_K(G) = \operatorname{ed}_{\mathbb{C}((t))}(\mathrm{C}_4) = 1$, while $\operatorname{ed}_k(G) = \operatorname{ed}_{\mathbb{R}}(\mathrm{C}_4) = 2$; see [BF03, Theorem 7.6].

Example 3.9. (cf. [Tos17, Remark 4.5(ii)]) This example shows that essential dimension does not satisfy any reasonable semicontinuity, even in characteristic 0. Consider the scheme

$$S \overset{\text{def}}{=} \operatorname{Spec} \mathbb{Q}[u, x]/(x^2 - u)\,.$$

The embedding $\mathbb{Q}[u] \subseteq \mathbb{Q}[u, x]/(x^2 - u)$ gives a finite map $S \to \mathbb{A}^1_{\mathbb{Q}}$. If p is an odd prime, the inverse image of the prime $(u - p) \subseteq \mathbb{Q}[u]$ in S consists of a point s_p with residue field $k(p) = \mathbb{Q}[x](x^2 - p)$. Then $\operatorname{ed}_{k(p)}(\mathrm{C}_4) = 1$ if -1 is a square modulo p, and $\operatorname{ed}_{k(p)} \mathrm{C}_4 = 2$ if -1 is not a square modulo p; once again, see [BF03, Theorem 7.6]. Equivalently, $\operatorname{ed}_{k(p)}(\mathrm{C}_4) = 1$ if $p \equiv 1 \pmod 4$, and $\operatorname{ed}_{k(p)} \mathrm{C}_4 = 2$ is $p \equiv 3 \pmod 4$. We conclude that the set of points $s \in S$ with $\operatorname{ed}_{k(s)} \mathrm{C}_4 = 1$ is dense in S, and likewise for the set of points $s \in S$ with $\operatorname{ed}_{k(s)} \mathrm{C}_4 = 2$ is also dense in S.

4. Proof of Theorem 1.2

We begin by remarking that an étale gerbe $\mathscr{X} \to S$ is weakly tame if and only if there exists an étale cover $\{S_i \to S\}$ such that each $\mathscr{X}_{S_i} \to S_i$ is equivalent to $\mathscr{B}_{S_i} G_i \to S_i$ with G_i weakly tame étale group schemes over S_i.

Our proof of Theorem 1.2 will rely on the following fact.

Lemma 4.1. *Let $\mathscr{X}_F \to \operatorname{Spec} F$ be a finite étale gerbe over a field F. Suppose that A is a non-zero finite F-algebra, and that the morphism $\operatorname{Spec} A \to \operatorname{Spec} F$ has a lifting $\phi\colon \operatorname{Spec} A \to \mathscr{X}_F$. Consider the locally free sheaf $\phi_* \mathscr{O}_{\operatorname{Spec} A}$ on $\mathscr{X}_F$; call $\mathscr{V} \to \mathscr{X}_F$ the corresponding vector bundle on $\mathscr{X}_F$. Then $\mathscr{V}$ has a non-empty open subscheme $U \subseteq \mathscr{V}$. Furthermore, if $k(U)$ is the field of rational functions on U, the composite $\operatorname{Spec} k(U) \to U \subseteq \mathscr{V} \to \mathscr{X}_F$ gives a versal object of $\mathscr{X}_F\big(k(U)\big)$.*

Proof. Let us show that $\mathscr{V}$ is generically a scheme. We can extend the base field F, so that it is algebraically closed; in this case $\mathscr{X}_F$ is the classifying space $\mathscr{B}_F G$ of a finite group G, and there exists a homomorphism of F-algebras $A \to F$. The vector bundle $\mathscr{V} \to \mathscr{S}_F$ corresponds to a representation V of G; by the semicontinuity of the degree of the stabilizer for finite group actions, it is enough to show that V has a point with trivial stabilizer. The homomorphism $A \to F$ gives a morphism $\operatorname{Spec} F \to \operatorname{Spec} A$, and the composite $\operatorname{Spec} F \to \operatorname{Spec} A \to$

$\mathscr{B}_F G$ corresponds to the trivial G-torsor on $\operatorname{Spec} F$. If we call $\mathscr{W}$ the pushforward of $\mathscr{O}_{\operatorname{Spec} F}$ to $\mathscr{B}_F G$, then $\mathscr{W} \subseteq \mathscr{V}$. On the other hand $\mathscr{W}$ corresponds to the regular representation of G, and so the generic stabilizer is trivial, which proves what we want.

Let us show that the composite $\operatorname{Spec} k(U) \to U \subseteq \mathscr{V} \to \mathscr{X}_F$ is versal; the argument is standard. Suppose that K is an extension of F that is an infinite field, and consider a morphism $\operatorname{Spec} K \to \mathscr{X}_F$. It is enough to prove that for any open subscheme $U \to \mathscr{V}$, the morphism $\operatorname{Spec} K \to \mathscr{X}_F$ factors through $u \subseteq \mathscr{V} \to \mathscr{X}_F$. The pullback $V_K \to \operatorname{Spec} K$ of $\mathscr{V} \to \mathscr{X}_F$ is a vector space on K, and the inverse image $U_K \subseteq V_K$ of $U \subseteq \mathscr{V}$ is a non-empty open subscheme; hence $U_K(K) \neq \emptyset$, which ends the proof. ♠

Proof of Theorem 1.2. Let $\widehat{R}$ be the completion of R and $\widehat{K}$ be the fraction field of $\widehat{R}$. Then clearly $K \subset \widehat{K}$ and thus $\operatorname{ed}_K(\mathscr{X}_K) \geqslant \operatorname{ed}_{\widehat{K}}(\mathscr{X}_{\widehat{K}}$. Thus for the purpose of proving Theorem 1.2, we may replace R by $\widehat{R}$. In other words, we may (and will) assume that R is complete.

Let $R \to A$ be an étale faithfully flat algebra such that $\mathscr{X}(A) \neq \emptyset$; since R is henselian, by passing to a component of $\operatorname{Spec} A$ we can assume that $R \to A$ is finite. Consider the lifting $\phi\colon \operatorname{Spec} A \to \mathscr{X}$; this is flat and finite. Let $\mathscr{V} \to \mathscr{X}$ be the vector bundle corresponding to $\phi_* \mathscr{O}_{\operatorname{Spec} A}$. If $U \to \mathscr{V}$ is the largest open subscheme of $\mathscr{V}$, the Lemma above implies that $U \to \operatorname{Spec} R$ is surjective. Denote by U_K and U_k respectively the generic and special fiber of $U \to \operatorname{Spec} R$; call E and E_0 the fields of rational functions on U_K and U_k respectively. Again because of the Lemma, the objects $\xi\colon \operatorname{Spec} E \to \mathscr{X}_K$ and $\xi_0\colon \operatorname{Spec} E_0 \to \mathscr{X}_k$ are versal.

Consider the local ring $\mathscr{O}_E$ of U at the generic point of U_k, which is a DVR. The residue field of $\mathscr{O}_E$ is E_0, and we have a morphism $\Xi\colon \operatorname{Spec} \mathscr{O}_E \to \mathscr{X}$ whose restrictions to $\operatorname{Spec} K$ and $\operatorname{Spec} k$ are isomorphic to ξ and ξ_0 respectively.

Set $m \overset{\text{def}}{=} \operatorname{ed}_K \mathscr{X}_K$; we need to show that ξ_0 has a compression of transcendence degree at most m.

There exists a field of definition $K \subseteq L \subseteq E$ for ξ such that $\operatorname{trdeg}_K L = m$; call $\theta\colon \operatorname{Spec} L \to \mathscr{X}$ the corresponding morphism, so that we have a factorization $\operatorname{Spec} E \to \operatorname{Spec} L \xrightarrow{\theta} \mathscr{X}$ for ξ. Consider the intersection $\mathscr{O}_L \overset{\text{def}}{=} \mathscr{O}_E \cap L \subseteq E$; then $\mathscr{O}_L$ is a DVR with quotient field L. Call L_0 it residue field; we have $L_0 \subseteq E_0$. By Lemma 2.1, $\operatorname{trdeg}_k L_0 \leqslant \operatorname{trdeg}_K L$.

Now it suffices to show that $\xi_0\colon \operatorname{Spec} E_0 \to \mathscr{X}$ factors through $\operatorname{Spec} L_0$. Assume that we have proved that the morphism $\theta\colon \operatorname{Spec} L \to \mathscr{X}$ extends to a morphism $\Theta\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$. The composite $\operatorname{Spec} E \subseteq$

$\operatorname{Spec} \mathscr{O}_E \xrightarrow{\Xi} \mathscr{X}$ is isomorphic to the composite $\operatorname{Spec} E \to \operatorname{Spec} L \subseteq \operatorname{Spec} \mathscr{O}_L \xrightarrow{\Theta} \mathscr{X}$; since $\mathscr{X}$ is separated, it follows from the valuative criterion of separation that the composite $\operatorname{Spec} \mathscr{O}_E \xrightarrow{\Theta} \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$ is isomorphic to $\Xi\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$. By restricting to the central fibers we deduce that $\xi_0\colon \operatorname{Spec} E_0 \to \mathscr{X}$ is isomorphic to the composite $\operatorname{Spec} E_0 \to \operatorname{Spec} L_0 \to \mathscr{X}$, and we are done.

To prove the existence of the extension $\Theta\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$, notice that the uniqueness of such extension implies that to prove its existence we can pass to a finite étale extension $R \subseteq R'$, where R' is a DVR; it is straightforward to check that formation of $\mathscr{O}_L$ and $\mathscr{O}_E$ commutes with such a base change. Hence we can assume that $\mathscr{X}$ has a section, so that $\mathscr{X} = \mathscr{B}_R G$, where $G \to \operatorname{Spec} R$ is a finite étale weakly tame group scheme. By passing to a further covering we can assume that $G \to \operatorname{Spec} R$ is constant, that is, the product of $\operatorname{Spec} R$ with a finite group Γ. If A is an R-algebra, an action of G on $\operatorname{Spec} A$ correspond to action of Γ.

The vector bundle $\mathscr{V} \to \mathscr{X}$ corresponds to a vector bundle $V_R \to \operatorname{Spec} R$ with an R-linear action of Γ, such that the induced representations of Γ on V_K and V_k are faithful. Call $\widetilde{E}$ the function field of V_K and $\widetilde{E}_0$ the function field of V_k; then $\widetilde{E}^\Gamma = E$, and therefore $\mathscr{O}_{\widetilde{E}}^\Gamma = \mathscr{O}_E$. The factorization $\operatorname{Spec} E \to \operatorname{Spec} L \to \mathscr{X}$ gives a Γ-torsor $\operatorname{Spec} \widetilde{L} \to \operatorname{Spec} L$ whose lift to $\operatorname{Spec} E$ is isomorphic to $\operatorname{Spec} \widetilde{E} \to \operatorname{Spec} E$; then $\widetilde{L}$ is a Γ-invariant subfield of $\widetilde{E}$. Then $\mathscr{O}_{\widetilde{L}} \overset{\text{def}}{=} \widetilde{L} \cap \mathscr{O}_{\widetilde{E}}$ is a Γ-invariant DVR, and $\mathscr{O}_{\widetilde{L}}^\Gamma = \widetilde{L}^\Gamma \cap \mathscr{O}_{\widetilde{E}}^\Gamma = \mathscr{O}_L$.

Call $\mathfrak{m}_{\widetilde{L}} \subseteq \mathscr{O}_{\widetilde{L}}$ the maximal ideal; then $\mathscr{O}_{\widetilde{L}}/\mathfrak{m}_{\widetilde{L}} = \widetilde{L}_0$. If $t \in R$ is the uniformizing parameter, the image of t in $\mathscr{O}_{\widetilde{L}}$, which we denote again by t, is a uniformizing parameter; this is Γ-invariant. The action of Γ on $\mathscr{O}_{\widetilde{L}}$ descends to an action of Γ on $\widetilde{L}_0$. By Proposition 2.3, this action is faithful.

So the action of Γ on $\operatorname{Spec} L_0$ is free over k; this implies that the action of Γ on $\operatorname{Spec} \mathscr{O}_{\widetilde{L}} \to \operatorname{Spec} R$ is free, so $\operatorname{Spec} \mathscr{O}_{\widetilde{L}} \to (\operatorname{Spec} \mathscr{O}_{\widetilde{L}})/G = \operatorname{Spec} \mathscr{O}_L$ is a Γ-torsor. This gives the desired morphism $\Theta\colon \operatorname{Spec} \mathscr{O}_L \to \mathscr{X}$, and ends the proof of the Theorem. ♠

Remark 4.2. The problem with the proof of [BRV11, Theorem 5.11] was in the last sentence of the second paragraph on page 1094. It is the claim there that we can replace the discrete valuation ring R in the proof with the ring called $W(k(s))$. Since the essential dimension of the generic point can go up when we make this replacement, this is, in fact, not allowable. (In effect, our mistake boils down to using an inequality in the wrong direction.)

Note also that the proof of the characteristic 0 genericity theorem in [BRV07] does not rely on Theorem 1.1. For that argument, which was different from the proof of [BRV11, Theorem 6.1], see [BRV07, Theorem 4.1].

Acknowledgments

We are grateful to Najmuddin Fakhruddin for helpful comments.

References

[BF03] Grégory Berhuy and Giordano Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330.

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

[BRV07] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension and algebraic stacks*, 2007, `arXiv:math/0701903v1 [math.AG]`.

[BRV11] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1079–1112, With an appendix by Najmuddin Fakhruddin. MR 2800485

[Dun13] Alexander Duncan, *Finite groups of essential dimension 2*, Comment. Math. Helv. **88** (2013), no. 3, 555–585.

[Led04] Arne Ledet, *On the essential dimension of p-groups*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 159–172. MR 2059762

[Led07] ———, *Finite groups of essential dimension one*, J. Algebra **311** (2007), no. 1, 31–37. MR 2309876

[Mer13] Alexander S. Merkurjev, *Essential dimension: a survey*, Transform. Groups **18** (2013), no. 2, 415–481. MR 3055773

[Rei10] Zinovy Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians. Volume II, Hindustan Book Agency, New Delhi, 2010, pp. 162–188. MR 2827790

[RV17] Z. Reichstein and A. Vistoli, *Essential dimension of finite groups in prime characteristic*, preprint, 2017.

[Tos17] Dajano Tossici, *Essential dimension of group schemes over a local scheme*, J. Algebra **492** (2017), 1–27. MR 3709138

[Vaq06] Michel Vaquié, *Valuations and local uniformization*, Singularity theory and its applications, Adv. Stud. Pure Math., vol. 43, Math. Soc. Japan, Tokyo, 2006, pp. 477–527. MR 2325152

[ZS58] Oscar Zariski and Pierre Samuel, *Commutative algebra, Volume I*, The University Series in Higher Mathematics, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, With the cooperation of I. S. Cohen. MR 0090581

(Brosnan) Department of Mathematics, 1301 Mathematics Building, University of Maryland, College Park, MD 20742-4015, USA
E-mail address: pbrosnan@umd.edu

(Reichstein) Department of Mathematics, 1984 Mathematics Road, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
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