ESSENTIAL DIMENSION AND CANONICAL DIMENSION OF GERBES BANDED BY GROUPS OF MULTIPLICATIVE TYPE

ROLAND LÖTSCHER

ABSTRACT. We prove the formula $\mathrm{ed}(\mathcal{X}) = \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A)$ for any gerbe $\mathcal{X}$ banded by an algebraic group A which is the kernel of a homomorphism of algebraic tori $Q \to S$ with Q invertible and S split. This result is applied to prove new results on the essential dimension of algebraic groups.

1. INTRODUCTION

Essential dimension is a notion of complexity of algebraic and geometric objects, introduced by J. Buhler and Z. Reichstein [BR97] around 1995 and in its most general form by A. Merkurjev [BF03].

The essential dimension of an algebraic group G over a field F is defined as the least integer n such that every G-torsor over a field extension K/F is obtained up to isomorphism by scalar extension from a G-torsor over an intermediate field K_0 of transcendence degree at most n over F. It is denoted by $\mathrm{ed}(G)$.

The essential dimension of an algebraic stack $\mathcal{X}$ over F is defined similarly (see section 2), where G-torsors are replaced by objects of $\mathcal{X}$. For every algebraic group (and every group algebraic space) G over F there is the classifying stack BG, whose objects are G-torsors. In particular $\mathrm{ed}(G) = \mathrm{ed}(BG)$.

An algebraic stack $\mathcal{X}$ of finite type over F is called a *gerbe*, if it becomes isomorphic to BG for some group algebraic space G over a finite extension of F (see [Stacks, Definition 06QC and Lemma 06QH]). In particular BG is a gerbe for any algebraic group G.

Let A be an abelian algebraic group over F. If there are natural isomorphisms $\mathbf{Aut}(x) \simeq A_U$ for $x \in \mathcal{X}(U)$, $U \in \mathrm{Sch}_F$, then the gerbe $\mathcal{X}$ is said to be *banded* by A. Gerbes banded by A over F are classified by the second Galois cohomology set $H^2(F, A)$, see [Gir71]. A typical example for a gerbe banded by A is the quotient stack $[X/G]$ for some exact sequence of algebraic groups

$$1 \to A \to G \to H \to 1$$

with A central in G, where X is an H-torsor over F. These gerbes have been used extensively in the computation of the essential dimension of algebraic groups G like finite p-groups, algebraic tori, Spin groups etc. when A is diagonalizable (see [Lö12] for a survey). A key ingredient is the inequality

$$(1) \qquad \mathrm{ed}(G) \geq \mathrm{ed}[X/G] - \dim H$$

from [Me09, Theorem 4.8], which bounds $\mathrm{ed}(G)$ from below in terms of the essential dimension of the gerbe $[X/G]$.

Our aim is to study gerbes whose band comes from a larger class of groups of multiplicative type and to obtain new applications.

Our main result relates essential dimension and canonical dimension of such gerbes $\mathcal{X}$. It is well known that

$$\text{(2)} \qquad \qquad \mathrm{cdim}(\mathcal{X}) \leq \mathrm{ed}(\mathcal{X}) \leq \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A),$$

for any gerbe $\mathcal{X}$ banded by an abelian algebraic group A, see [Me08, Proposition 4.9] (for a more general version see [Lö12, Lemma 3.1]). Here $\mathrm{cdim}(\mathcal{X})$ stands for the canonical dimension of $\mathcal{X}$, defined as the least integer n such that for every field extension K/F with $\mathcal{X}(K) \neq \emptyset$ there exists an intermediate field K_0 of K/F of transcendence degree at most n such that $\mathcal{X}(K_0) \neq \emptyset$ (see section 2 for details). The canonical dimension of an algebraic stack $\mathcal{X}$ is often more accessible than its essential dimension, since it only depends on the splitting fields of $\mathcal{X}$, i.e., the field extensions K/F such that $\mathcal{X}(K) \neq \emptyset$. For instance, if $\mathcal{X}_A$ is the μ_n-gerbe associated with a central simple algebra A of exponent dividing n, then $\mathrm{cdim}(\mathcal{X}_A)$ coincides with the canonical dimension of the Severi Brauer variety of A. This is equal to $\mathrm{ind}\, A - 1$ when the index of A is a prime power by a result of N. Karpenko [Ka00, Theorem 2.1].

The following question was asked by A. Merkurjev [Me08, Question 4.10]:

Question 1. Do we have the equality $\mathrm{ed}(\mathcal{X}) = \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A)$ for any gerbe $\mathcal{X}$ banded by an abelian group A?

Question 1 has a partial positive answer in case $A = \mu_n$ (where $n > 1$) [BRV11, Theorem 4.1] and $A = (\mu_p)^s$ [KM08, Theorem 3.1]. It clearly also holds when $\mathrm{ed}(A) = 0$ (equivalently A is special, i.e. all A-torsors over field extensions are trivial, see [Me09, Proposition 4.4]). Our main theorem gives an affirmative answer to Question 1 for a larger class of group, which includes all diagonalizable algebraic groups A as well as many non-diagonalizable algebraic groups like norm 1 tori $A = R_{L/F}^{(1)}(\mathbf{G}_m)$ for an étale F-algebra L:

Theorem 1.1. *Let $f\colon Q \to S$ be a homomorphism of algebraic tori over a field F with Q invertible and S split. Let $\mathcal{X}$ be a gerbe over F banded by $A := \ker(f)$. Then*

$$\mathrm{ed}(\mathcal{X}) = \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A).$$

Moreover if Q_d denotes the largest split subtorus of Q we have

$$\mathrm{ed}(A) = \mathrm{ed}(A \cap Q_d)$$

and this is equal to the rank (=minimal number of generators) of the torsion of the character group of the diagonalizable group $A \cap Q_d$.

Note that in order to prove the theorem we may always assume that f is surjective. So f will be assumed to be surjective in sequel. Moreover A lies between the invertible torus Q and its largest anisotropic subtorus Q_{an}. Conversely every algebraic group, which lies between Q_{an} and Q for an invertible torus Q can be written as the kernel of a homomorphism $f\colon Q \to S$ with S split (take $S = Q/A$, which is a split torus as a quotient of the split torus Q/Q_{an}).

The rest of the paper is structured as follows. In section 2 we recall some background material on essential dimension and canonical dimension and make some general observations about gerbes banded by groups of multiplicative type. These will be used in section 3, which contains a proof of Theorem 1.1. Finally section 4 contains applications of this theorem.

2. Preliminaries

2.1. Preliminaries on essential dimension and canonical dimension.

Let $\mathcal{X}$ be a category fibered in groupoids over F (for instance a gerbe over F). For every field extension K/F we have the groupoid $\mathcal{X}(K)$ of objects of $\mathcal{X}$ over $\operatorname{Spec}(K)$. If L/K is a field extension over F and $x \in \mathcal{X}(K)$ we have a pullback $x_L \in \mathcal{X}(L)$, defined uniquely up to isomorphism.

Let K/F be a field extension, $x \in \mathcal{X}(K)$ and let K_0 be an intermediate field of K/F. We say that x is *detected* over K_0 if $\mathcal{X}(K_0) \neq \emptyset$. We say that x is *defined* over K_0 if there exists $x_0 \in \mathcal{X}(K_0)$ with $(x_0)_K \simeq x$. Note that "being detected" over K_0 is weaker than "being defined" over K_0 and depends on x only through the field K (as K_0 is required to be a subfield of K).

Definition 2.1. The canonical dimension $\operatorname{cdim}(x)$ of $x \in \mathcal{X}(K)$ (resp. the essential dimension $\operatorname{ed}(x)$ of x) is defined as the least transcendence degree of an intermediate field K_0 of K/F over which x is detected (resp. defined).

If p is a prime integer, the canonical p-dimension $\operatorname{cdim}_p(x)$ and the essential p-dimension $\operatorname{ed}_p(x)$ of x are defined as the minimal value of $\operatorname{cdim}_p(x_{K'})$ and $\operatorname{ed}_p(x_{K'})$, respectively, where K'/K runs through all extensions of degree prime to p. We will write $\operatorname{cdim}_0(x) = \operatorname{cdim}(x)$, $\operatorname{ed}_0(x) = \operatorname{ed}(x)$ for notational convenience.

The numbers $\operatorname{cdim}(\mathcal{X})$, $\operatorname{ed}(\mathcal{X})$, $\operatorname{cdim}_p(\mathcal{X})$ and $\operatorname{ed}_p(\mathcal{X})$ are defined as the maximal values of $\operatorname{cdim}(x)$, $\operatorname{ed}(x)$, $\operatorname{cdim}_p(x)$ and $\operatorname{ed}_p(x)$, respectively, where x runs through all objects $x \in \mathcal{X}(K)$ over field extensions K/F.

The following inequalities follow immediately from the definitions: $\operatorname{cdim}_p(x) \leq \operatorname{ed}_p(x)$, $\operatorname{cdim}_p(\mathcal{X}) \leq \operatorname{ed}_p(\mathcal{X})$, $\operatorname{cdim}_p(x) \leq \operatorname{cdim}(x)$, $\operatorname{ed}_p(x) \leq \operatorname{ed}(x)$, $\operatorname{cdim}_p(\mathcal{X}) \leq \operatorname{cdim}(\mathcal{X})$ and $\operatorname{ed}_p(\mathcal{X}) \leq \operatorname{ed}(\mathcal{X})$ for any prime p (for $p = 0$ as well).

When G is an algebraic group (not necessarily smooth) we write $\operatorname{ed}_p(G)$ in place of $\operatorname{ed}_p(BG)$ for any prime p and for $p = 0$. Here $BG \simeq [\operatorname{Spec} F/G]$ is the classifying stack of G. The groupoid $BG(K)$ is simply the category of G-torsors over $\operatorname{Spec}(K)$.

We will use the following result on essential dimension of diagonalizable groups (see [Lö10, Corollary 5.8]):

Lemma 2.1. *Let D be a diagonalizable algebraic group. Let D^* denote the character group of D and D^*_{tors} its torsion. Then*

$$\operatorname{ed}(D) = \operatorname{rk}(D^*_{\mathrm{tors}}),$$

where rk *stands for the minimal number of generators.*

Moreover we will use the following inequality from [BF03, Theorem 6.19]: If H is a subgroup of an algebraic group H' then

$$(3) \qquad \operatorname{ed}(H) + \dim(H) \leq \operatorname{ed}(H') + \dim(H').$$

2.2. **Preliminaries on Gerbes.** Every gerbe over F banded by the multiplicative group $\mathbf{G}_m$ is associated to a central simple F-algebra A. The objects $\mathcal{X}_A(K)$ over a field extension K/F are given by couples (V, α) of a K-vector space V together with an isomorphism $\alpha\colon A_K := A \otimes_F K \xrightarrow{\cong} \mathrm{End}_K(V)$. Let $n = \deg(A)$. The gerbe $\mathcal{X}_A$ can be seen as the quotient stack $[X/\mathbf{GL}_n]$, where $X = \mathrm{Isom}(A, M_n(F))$ is the $\mathbf{PGL}_n$-torsor over F corresponding to A.

Alternatively, if L denotes a maximal étale subalgebra of A, the gerbe $\mathcal{X}_A$ can be represented as the quotient $[U/R_{L/F}(\mathbf{G}_m)]$ for some $R_{L/F}(\mathbf{G}_m)/\mathbf{G}_m$-torsor Y over F. Explicitly Y is the scheme of isomorphisms $\beta\colon A_K \xrightarrow{\cong} \mathrm{End}_K(V)$ that are compatible with the inclusion of $L \otimes_F K$ in A_K and $\mathrm{End}_K(V)$ (by left multiplications), respectively.

The following lemma shows that in fact every gerbe banded by a group scheme of multiplicative type can be realized as the stack quotient of a torsor under a torus by a quasi-trivial torus.

Lemma 2.2. *Let $\mathcal{X}$ be a gerbe banded by a group A of multiplicative type over F. Let L/F be a Galois extension such that $\mathcal{X}(L) \neq \emptyset$ and A_L is diagonalizable.*

Then there exists a quasi-split algebraic torus P over F containing A and split over L and a P/A-torsor U over F such that $\mathcal{X} \simeq [U/P]$.

The splitting fields of $\mathcal{X}$ coincide with the splitting fields of U. In particular $\mathrm{cdim}\,\mathcal{X} = \mathrm{cdim}\,U = \mathrm{cdim}(x)$, *for any $x \in \mathcal{X}(F(U)) \neq \emptyset$.*

Proof. Embed A_L in $\mathbf{G}_m^n$ for some $n \geq 0$. This induces an embedding of $R_{L/F}(A_L)$ in the quasi-split torus $P = R_{L/F}(\mathbf{G}_m)^n$ split over L. The class of $\mathcal{X}$ lies in the kernel of the map $H^2(F, A) \to H^2(F, R_{L/F}(A_L)) = H^2(L, A)$ taking $\mathcal{X}$ to $\mathcal{X}_L$. Hence it also lies in the kernel of the map $H^2(F, A) \to H^2(F, P)$ induced by the composition $A \to R_{L/F}(A_L) \to P$, which is injective. Therefore the class of $\mathcal{X}$ lies in the image of the connecting map $H^1(F, P/A) \to H^2(F, A)$. In other words, there exists a P/A-torsor U over F such that $\mathcal{X} \simeq [U/P]$.

Now a field extension K/F is a splitting field of $\mathcal{X}$ if and only if U lifts to a P-torsor over K. This happens if and only if K is a splitting field of U. Hence $\mathcal{X}$ and U have the same splitting fields, whence the same canonical dimension. The last equality follows from the fact that U has a smooth projective compactification with the same splitting fields, see [KV84], and the proof of [Me13, Prop. 4.2]. $\square$

Remark 2.1. With notations as in Lemma 2.2 let $\bar{U}$ be a smooth projective compactification of U. Then $\mathrm{cdim}(\mathcal{X}) = \mathrm{cdim}(U)$ is the least dimension of the image of a rational map $\bar{U} \dashrightarrow \bar{U}$ by [KM06, Corollary 4.6]. Hence the computation of $\mathrm{cdim}(\mathcal{X})$ can be approached with geometric methods. We will not use this description within this paper, however.

We will also be interested in objects of the gerbe $\mathcal{X}$ over local F-algebras.

Corollary 2.1. *With notations as in Lemma 2.2:*
  (a) *If R is any local F-algebra then $\mathcal{X}(R) \neq \emptyset$ if and only $U(R) \neq \emptyset$.*
  (b) *Let R be a local F-algebra which is a valuation ring whose residue field is linearly disjoint from L over F. Let M be the field of fractions of R. Then $\mathcal{X}(M) \neq \emptyset$ if and only if $\mathcal{X}(R) \neq \emptyset$.*

Proof.   (a) This follows like in the proof of Lemma 2.2 and the fact that every P-torsor over R is trivial when P is quasi-split and R local.

(b) Clearly $\mathcal{X}(R) \neq \emptyset$ implies $\mathcal{X}(M) \neq \emptyset$. Conversely assume $\mathcal{X}(M) \neq \emptyset$. Let P and U be as above and let $T = P/A$. Then $U(M) \neq \emptyset$ and so $(U/T_d)(M) \neq \emptyset$, where T_d denotes the largest split subtorus of T over F. Let X be a smooth projective T/T_d-equivariant compactification of U/T_d. Then $X(M) \neq \emptyset$ and since X is complete, $X(R) \neq \emptyset$.

By assumption $R/\mathfrak{m}$ is linearly disjoint from L (which is a Galois splitting field of T/T_d) and therefore T/T_d is anisotropic over $R/\mathfrak{m}$. By [Gi04, Proposition 1.1] $X(R/\mathfrak{m}) = (U/T_d)(R/\mathfrak{m})$. Therefore the image of $X(R)$ under the map $X(R) \to X(R/\mathfrak{m})$ is contained in $(U/T_d)(R/\mathfrak{m})$. It follows that $(U/T_d)(R) = X(R) \neq \emptyset$, i.e. U/T_d splits over R. Since R is local U splits over R as well. It follows that $\mathcal{X}(R) \neq \emptyset$.

$\square$

Torsors over a local F-algebra under a group of multiplicative type can always be obtained as fibers between morphisms of algebraic tori, see the following well-known lemma.

Lemma 2.3. *Let A be a subgroup of an invertible torus Q. If R is a local F-algebra, then every A-torsor over R is the fiber of $Q \to Q/A$ over some $s \in (Q/A)(R)$.*

Proof. The exact sequence $1 \to A \to Q \to Q/A \to 1$ induces an exact sequence $Q(R) \to S(R) \to H^1(R, A) \to H^1(R, Q) = 1$, where the map $S(R) \to H^1(R, A)$ takes $s \in S(R)$ to the fiber of $Q \to S$ over s. $\square$

3. Proof of Main Theorem

In this section we will prove Theorem 1.1. We start with a lemma, which will be used in the proof.

Lemma 3.1. *Let $g \colon V \to W$ a homomorphism of free abelian groups of finite rank and U a subgroup of V with $\mathrm{rk}(U) \leq \mathrm{rk}(W)$. Then $\mathrm{rk}((V/U)_{tors}) \leq \mathrm{rk}(W/g(U))$.*

Proof. Let $m = \mathrm{rk}((V/U)_{\mathrm{tors}})$ and $r = \mathrm{rk}(U)$, $r' = \mathrm{rk}(W)$, $s = \mathrm{rk}(V)$. By the elementary divisor theorem, there exist a basis $e_1, \ldots, e_s$ of the $\mathbb{Z}$-module V and integers $c_1, \ldots, c_m > 1$ with $c_1 | c_2 | \cdots | c_m$ such that the elements

$$c_1 e_1, \ldots, c_m e_m, e_{m+1}, \ldots, e_r$$

form a basis of U. Let p be a prime dividing c_1 (hence dividing every c_i). Then $W/g(U)$ surjects onto
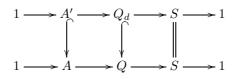
$$W/(g(U) + pW) \simeq (\mathbb{Z}/p\mathbb{Z})^{r'} / \langle \overline{g(e_{m+1})}, \ldots, \overline{g(e_r)} \rangle$$

which has rank $\geq m$. Therefore $\mathrm{rk}(W/g(U)) \geq m = \mathrm{rk}((V/U)_{tors})$. $\square$

Proof of Theorem 1.1. The last assertion of the Theorem follows from Lemma 2.1. Moreover recall inequality (2) $\mathrm{ed}(\mathcal{X}) \leq \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A)$ from the introduction. Let $A' := Q_d \cap A$.

We will prove that $\mathrm{ed}(\mathcal{X}) \geq \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A')$ and $\mathrm{ed}(A') \geq \mathrm{ed}(A)$. From this the claims follow readily.

For the assertion $\mathrm{ed}(A') \geq \mathrm{ed}(A)$ consider the following diagram with exact rows:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & A' & \longrightarrow & Q_d & \longrightarrow & S & \longrightarrow & 1 \\
& & \cap \downarrow & & \cap \downarrow & & \| & & \\
1 & \longrightarrow & A & \longrightarrow & Q & \longrightarrow & S & \longrightarrow & 1
\end{array}
$$

Since Q (which is invertible) and Q_d (which is a split torus) are special, we get a surjection in Galois-cohomology $H^1(-, A') \to H^1(-, A)$ as functors from the category of field extensions of F to the category of sets. Hence the claim follows from [BF03, Lemma 1.9].

Now we will prove the assertion $\mathrm{ed}(\mathcal{X}) \geq \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A')$, for which we use the addition $BA \times \mathcal{X} \to \mathcal{X}, (t, x) \mapsto t + x$ and subtraction $\mathcal{X} \times \mathcal{X} \to BA, (x, x') \mapsto x - x'$ as in [Me09]. By Lemma 2.2 we can choose a field extension K/F linearly disjoint from F_{alg} and $x \in \mathcal{X}(K)$ such that $\mathrm{cdim}(x) = \mathrm{cdim}(\mathcal{X})$.

Let $M := K(t_1, \ldots, t_s)$, where $s := \dim S$. We will identify S with $\mathbf{G}_m^s$. We write $\langle t \rangle$ for the A-torsor over M given by $f^{-1}(t_1, \ldots, t_s)$. Let $x' := \langle t \rangle + x_M \in \mathcal{X}(M)$. We will prove that $\mathrm{ed}(x') \geq \mathrm{cdim}(x) + \mathrm{ed}(A')$.

Let M_0 be an intermediate field of M/F and $y \in \mathcal{X}(M_0)$ such that $y_M \simeq x'$ and $\mathrm{tdeg}_F(M_0) = \mathrm{ed}(x')$. Let ν be the canonical $\mathbb{Z}^r$-valued valuation of $K_{\mathrm{alg}}(t_1, \ldots, t_s)$, so that $\nu(t_i) = e_i := (0, \ldots, 1, \ldots, 0) \in \mathbb{Z}^s$ (with 1 on place i) and $\nu|_{K_{\mathrm{alg}}}$ is trivial. Let $\nu_0 = \nu|_{M_0}$ and $R_0 \subseteq M_0$ the valuation ring of ν_0 and R the valuation ring of $\nu|_M$, whose residue field is K.

Claim: $\mathrm{rk}(\nu_0) \geq \mathrm{ed}(A')$.

The residue field of R_0 embeds in K over F, hence it is linearly disjoint from the finite extension L/F. Since $y \in \mathcal{X}(M_0)$ we get $\mathcal{X}(R_0) \neq \emptyset$ by Corollary 2.1. Choose $x_0 \in \mathcal{X}(R_0)$. By Lemma 2.3 there exists $z = (z_1, \ldots, z_s) \in S(M_0) = (M_0^\times)^s$ such that $y - (x_0)_{M_0} \simeq \langle z \rangle \in BA(M_0)$, where $\langle z \rangle$ denotes the fiber $f^{-1}(z)$. Since $z_i \in M_0^\times$ it suffices to show that the subgroup of $\mathbb{Z}^s$ generated by $\nu(z_1), \ldots, \nu(z_r)$ has rank $\geq \mathrm{ed}(A')$. We have

$$\langle z \rangle_M \simeq y_M - (x_0)_M \simeq x' - (x_0)_M = (\langle t \rangle + x_M) - (x_0)_M \simeq \langle t \rangle + (x_M - (x_0)_M).$$

Note that $x_M - (x_0)_M$ is defined over R (since R contains K and R_0). By Lemma 2.3 there exists $r = (r_1, \ldots, r_s) \in S(R) = (R^\times)^s \subseteq (M^\times)^s$ with $x_M - (x_0)_M \simeq \langle r \rangle_M$. Therefore

$$\langle z \rangle_M \simeq \langle t \rangle + \langle r \rangle_M \simeq \langle tr \rangle.$$

It follows that the classes of z and tr are equal in $(M^\times)^s / f_M(Q(M))$. Hence there exists $w \in Q(M)$ such that $z = tr f_M(w)$. That yields the relations

$$\nu(z_j) = \nu(t_j) + \nu(r_j) + \nu(f_M(w)_j) = e_j + \nu(f_M(w)_j)$$

for $j = 1, \ldots, s$. Hence it suffices to show that

$$\mathrm{rk}(\mathbb{Z}^s / \langle \nu(f_M(w)_1), \ldots, \nu(f_M(w)_s) \rangle) \geq \mathrm{ed}(A').$$

We first reduce to the case when Q is quasi-split. Let Q' be an F-torus such that $\tilde{Q} := Q \times Q'$ is quasi-split and let $\tilde{A} = A \times Q'$ and $\tilde{A}' = \tilde{A} \cap \tilde{Q}_d = A' \times Q'_d$. Then $\mathrm{ed}(A') = \mathrm{ed}(\tilde{A}')$, since Q'_d is special. We may replace A by $\tilde{A}$ and Q by $\tilde{Q}$ and hence assume that Q is quasi-split, $Q = \prod_{i=1}^m R_{L_i/F}(\mathbf{G}_m)$ for some separable field extensions $L_1/F, \ldots, L_m/F$.

Let $C \in M_{m,s}(\mathbb{Z})$ be the matrix corresponding to the homomorphism $f|_{Q_d} \colon Q_d \to S$. on character groups. Let U denote the span of the rows of C. Then A' has character lattice $\mathbb{Z}^m / U$. Hence as observed above

$$\mathrm{ed}(A') = \mathrm{rk}(\mathbb{Z}^m / U)_{tors}.$$

There exists $B \in M_{s,m}(\mathbb{Z})$ such that for every field extension F'/F the group homomorphism $f_{F'} \colon \prod_{i=1}^{m}(L_i \otimes_F F')^{\times} \to (F'^{\times})^s$ is given by

$$f_{F'}(x_1, \ldots, x_m) = \left(\prod_{i=1}^{m} N_{L_i \otimes_F F'/F'}(x_i)^{b_{ij}} \right)_{1 \leq j \leq s}.$$

Then $c_{ij} = b_{ij}[L_i : F]$ for all i and j.

Since F_{sep} and $M = K(t_1, \cdots, t_s)$ are linearly disjoint over F we may view $F_{\mathrm{sep}} \otimes_F M$ as a subfield of $K_{\mathrm{alg}}(t_1, \cdots, t_s)$.

Write $w = (w_1, \ldots, w_m) \in Q(M) = \prod_{i=1}^{m}(L_i \otimes_F M)^{\times}$. Note that the value $\nu((\sigma \otimes \mathrm{id}_M)(w_i)) \in \mathbb{Z}^s$ for a F-homomorphism $\sigma \colon L_i \to F_{\mathrm{sep}}$ is independent of the particular choice of σ. The product $\prod(\sigma \otimes \mathrm{id}_M)(w_i)$ taken over all $[L_i : F]$ homomorphisms σ is equal to $N_{L_i \otimes_F M/M}(w_i)$. Writing $\nu_i := \nu((\sigma \otimes \mathrm{id}_M)(w_i))$ we get

$$\nu(f_M(w)_j) = \sum_{i=1}^{m} b_{ij} \nu(N_{L_i \otimes_F M/M}(w_i)) = \sum_{i=1}^{m} b_{ij}[L_i : F]\nu_i = \sum_{i=1}^{m} c_{ij}\nu_i.$$

Let $g \colon \mathbb{Z}^m \to \mathbb{Z}^s$ the group homomorphism, which takes the i-th standard basis vector of $\mathbb{Z}^m$ to ν_i for all i. Then $\langle \nu(f_M(w)_1), \ldots, \nu(f_M(w)_m) \rangle = g(U)$. Note that $\mathrm{rk}(U) = s$, since $f|_{Q_d}$ is surjective. Hence Lemma 3.1 yields:

$$\mathrm{rk}(\mathbb{Z}^s/\langle \nu(f_M(w)_1), \ldots, \nu(f_M(w)_m) \rangle) = \mathrm{rk}(\mathbb{Z}^s/g(U)) \geq \mathrm{rk}((\mathbb{Z}^m/U)_{tors}) = \mathrm{ed}(A').$$

Therefore $\mathrm{rk}(\nu_0) \geq \mathrm{ed}(A')$, proving the claim.

Let $\overline{M_0}$ denote the residue field of ν_0. Note that $\overline{M_0}$ can be considered as a subfield of the residue field of $\nu|_M$, which is F-isomorphic to K. Since $\mathcal{X}(R_0) \neq \emptyset$ we have $\mathcal{X}(\overline{M_0}) \neq \emptyset$, hence

$$\mathrm{ed}(x') = \mathrm{tdeg}_F M_0 \geq \mathrm{tdeg}_F \overline{M_0} + \mathrm{rk}(\nu_0) \geq \mathrm{tdeg}_F \overline{M_0} + \mathrm{ed}(A')$$
$$\geq \mathrm{cdim}(x) + \mathrm{ed}(A').$$

Therefore $\mathrm{ed}(\mathcal{X}) \geq \mathrm{cdim}(x) + \mathrm{ed}(A') = \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(A')$. This concludes the proof. $\qquad\square$

4. Applications

We will discuss three kinds of applications in the following subsections. The first two concern extensions of algebraic groups by abelian algebraic groups. In other words we have a short exact sequence

$$1 \to A \to G \to H \to 1$$

with A abelian (not necessarily central). We want to use such a sequence to get a lower bound on $\mathrm{ed}(G)$, using the inequality (1) for an H-torsor X over a field extension K of F. Note that in general $[X/G]$ is a gerbe banded by the twisted group $^X A$, but (1) holds regardless of whether A is central in G or not. The twist is isomorphic to A_K if A is central in G. When A is not central it may easily happen that A is split and the twist is not split.

Our results on essential dimension of gerbes yield new applications in the following cases

 (a) A itself is a (non-split) group of multiplicative type that lies between an invertible torus and its anisotropic part and A is central in G

(b) A is (possibly split, but) non-central and the twist ^{X}A lies between an invertible torus and its anisotropic part.

The third application concerns an example of splitting a global problem (i.e. depending on several primes) into two local problems (depending on a single prime).

4.1. **Central extensions by non-split groups.** A simple example of a torus T for which we can apply Theorem 1.1 is a non-split one-dimensional torus, i.e. $T = R_{L/F}^{(1)}(\mathbf{G}_m)$, where L/F is a quadratic separable field extension. This group is the center of the unitary group $U(B,\tau)$ where B is a central simple L-algebra with F-linear unitary involution τ.

Proposition 4.1. *If B is a division algebra and $n := \deg(B) = 2^r$ for some $r \geq 0$ then*
$$\mathrm{ed}(U(B,\tau)) = n^2.$$

Proof. The inequality $\mathrm{ed}(U(B,\tau)) \leq n^2$ follows from the fact that $U(B,\tau)$ is contained in the special algebraic group $R_{L/F}(\mathbf{GL}_1(B))$ with codimension n^2.

For the reverse inequality we consider the following commutative diagram with exact rows:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & R_{L/F}^{(1)}(\mathbf{G}_m) & \longrightarrow & U(B,\tau) & \longrightarrow & \mathbf{PGU}(B,\tau) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & R_{L/F}(\mathbf{G}_m) & \longrightarrow & \mathbf{GU}(B,\tau) & \longrightarrow & \mathbf{PGU}(B,\tau) & \longrightarrow & 1
\end{array}
$$

By [Lö11, Theorem 3.2] (and its proof) there exists a field extension K/F linearly disjoint from L/F and a $\mathbf{PGU}(B,\tau)$-torsor X over K whose image under the connecting map

$$H^1(K, \mathbf{PGU}(B,\tau)) \to H^2(K, R_{L/F}(\mathbf{G}_m)) = \mathrm{Br}(L \otimes_F K)$$

is the Brauer class of a central simple $L \otimes_F K$-algebra A of index n^2 whose norm $N_{L\otimes_F K/K}(A)$ is split. The gerbe $[X/U(B,\tau)]$ banded by $R_{L/F}^{(1)}(\mathbf{G}_m)$ has the same splitting fields as the K-variety $R_{L\otimes_F K/K}(\mathrm{SB}(A))$. Therefore by (1) and Theorem 1.1,

$$
\begin{aligned}
\mathrm{ed}(U(B,\tau)) &\geq \mathrm{ed}([X/U(B,\tau)]) - \dim \mathbf{PGU}(B,\tau) \\
&= \mathrm{cdim}(R_{L\otimes_F K/K}(\mathrm{SB}(A))) + \mathrm{ed}\left(R_{L/F}^{(1)}(\mathbf{G}_m)\right) - \dim \mathbf{PGU}(B,\tau) \\
&= \mathrm{cdim}(R_{L\otimes_F K/K}(\mathrm{SB}(A))) + 1 - (n^2 - 1).
\end{aligned}
$$

By [Ka12, Theorem 1.1]

$$\mathrm{cdim}(R_{L\otimes_F K/K}(\mathrm{SB}(A))) = \dim(R_{L\otimes_F K/K}(\mathrm{SB}(A))) = 2(n^2 - 1),$$

hence the inequality $\mathrm{ed}(U(B,\tau)) \geq n^2$ follows. $\qquad\square$

4.2. **Non-central extensions by abelian groups.** Let A be a central simple F-algebra of degree d and let $n \geq 1$. A simple example of a non-central extension by an abelian group is given by the exact sequence

$$1 \to \mathbf{G}_m^n \to \mathbf{GL}_1(A)^n \rtimes S_n \to \mathbf{PGL}_1(A)^n \rtimes S_n \to 1,$$

where the semidirect products are understood with respect to the natural permutation action. The group $\mathbf{PGL}_1(A)^n \rtimes S_n$ can be considered as automorphism

group scheme of the F-algebra A^n. From this observation we get a natural bijection between isomorphism classes of $\mathbf{PGL}_1(A)^n \rtimes S_n$-torsors over a field extension K/F and isomorphism classes of Azumaya algebras of (constant) degree d over n-dimensional étale extensions E/K.

Similarly isomorphism classes of $\mathbf{GL}_1(A)^n \rtimes S_n$-torsors over K can be identified with isomorphism classes of pairs (E, M) consisting of an n-dimensional étale K-algebra E and an $A_E := A \otimes_F E$-module M of reduced dimension d, where a morphism between two pairs (E, M) and (E', M') is a pair (ι, φ) consisting of a K-algebra isomorphism $\iota \colon E \to E'$ and an A-linear isomorphism $\varphi \colon M \to M'$ satisfying $\varphi(em) = \iota(e)\varphi(m)$ for all $e \in E, m \in M$. In these terms the map

$$H^1(K, \mathbf{GL}_1(A)^n \rtimes S_n) \to H^1(K, \mathbf{PGL}_1(A)^n \rtimes S_n)$$

takes the isomorphism class of (E, M) to the isomorphism class of $\mathrm{End}_{A_E}(M)$.

For a $\mathbf{PGL}_1(A)^n \rtimes S_n$-torsor X over K corresponding to an Azumaya algebra B over the n-dimensional étale K-algebra E the gerbe $[X/\mathbf{GL}_1(A)^n \rtimes S_n]$ is banded by $R_{E/K}(\mathbf{G}_m)$ and its class in $H^2(K, R_{E/K}(\mathbf{G}_m)) = \mathrm{Br}(E)$ is the class of $[B] - [A_E]$.

Now let $n = 2$ and suppose that A carries an involution σ of the first kind. Let

$$G := \mathbf{GL}_1(A) \rtimes S_2,$$

where the non-trivial element of S_2 acts via $a \mapsto \sigma(a^{-1})$. We have a commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & R^{(1)}_{F^2/F}(\mathbf{G}_m) & \longrightarrow & G & \longrightarrow & \mathbf{PGL}_1(A) \rtimes S_2 & \longrightarrow & 1 \ , \\
& & \Big\uparrow & & \Big\downarrow & & \Big\downarrow & & \\
1 & \longrightarrow & R_{F^2/F}(\mathbf{G}_m) & \longrightarrow & \mathbf{GL}_1(A)^2 \rtimes S_2 & \longrightarrow & \mathbf{PGL}_1(A)^2 \rtimes S_2 & \longrightarrow & 1
\end{array}
$$

where the second and third vertical arrows are induced by the inclusion

$$\mathbf{GL}_1(A) \to \mathbf{GL}_1(A)^2, \quad a \mapsto (a, \sigma(a^{-1})).$$

A $\mathbf{PGL}_1(A) \rtimes S_2$-torsor X over a field extension K/F corresponds to a pair (B, τ) of a central simple K-algebra of degree d with unitary involution, where the trivial torsor corresponds to the pair $(A \times A, \varepsilon)$ with $\varepsilon(a, b) = (\sigma(b), \sigma(a))$. The induced $\mathbf{PGL}_1(A)^2 \rtimes S_2$-torsor corresponds to the algebra B. The gerbe $[X/G]$ is then banded by $R^{(1)}_{E/K}(\mathbf{G}_m)$, where $E := Z(B)$, and its class in

$$H^2(K, R^{(1)}_{E/K}(\mathbf{G}_m)) = \ker(\mathrm{cor}_{E/K} \colon \mathrm{Br}(E) \to \mathrm{Br}(K)) \subseteq \mathrm{Br}(E)$$

is again the class of $[B] - [A_E]$.

Proposition 4.2. *With notations as above:*

(a) *For any field extension K/F and any pair (B, τ) of a central simple K-algebra B of degree d with unitary involution τ we have*

$$\mathrm{ed}(G) \geq \mathrm{cdim}(R_{E/K}(\mathrm{SB}(B \otimes_F A^{\mathrm{op}}))) + \delta_E - (d^2 - 1),$$

where $\delta_E := \mathrm{ed}(R^{(1)}_{E/K}(\mathbf{G}_m)) \in \{0, 1\}$ is 0 if E is split (i.e., $E \simeq K \times K$) and 1 otherwise (i.e., if E is a field).

(b) *Suppose $d > 1$. Then we have $\mathrm{ed}(G) \leq d^2$.*

(c) *Suppose that A is a division algebra of index $d = 2^m$ with $m \geq 1$. Then*

$$\mathrm{ed}(G) = d^2.$$

Proof.   (a) Let X be the $\mathbf{PGL}_1(A) \rtimes S_2$-torsor corresponding to (B, τ). Then the gerbe $[X/G]$ has the same splitting fields as $R_{E/K}(\mathrm{SB}(B \otimes_F A^{\mathrm{op}}))$, hence the desired inequality follows from inequality (1) and Theorem 1.1.

(b) Define a representation of G on the F-vector space $V = A \oplus A$ by letting $\mathbf{GL}_1(A)$ act on V through $a \cdot (a_1, a_2) = (aa_1, \sigma(a^{-1})a_2)$ and S_2 through permuting coordinates. Clearly $\dim V = 2d^2$, hence $\dim V - \dim G = d^2$. In view of [BF03, Proposition 4.11] it suffices to prove that V is generically free in case $d > 1$. Let U denote the open subset of the affine space $\mathbb{A}(V)$ consisting of those pairs (a_1, a_2) where a_1 and a_2 are invertible and $a_1 a_2^{-1}$ is not symmetric with respect to σ. It is easy to check that U is G-stable and G acts freely on U. Moreover the symmetric elements $\mathrm{Sym}(A, \sigma)$ form a proper subspace of A in case $d > 1$, hence U is non-empty. This proves the claim.

(c) By part (b) $\mathrm{ed}(G) \leq d^2$. We will prove $\mathrm{ed}(G) \geq d^2$ using part (a). Since $\dim(R_{E/K}(\mathrm{SB}(B \otimes_F A^{\mathrm{op}}))) = 2(d^2 - 1)$ it suffices to construct a field extension K/F and a pair (B, τ) of a central simple K-algebra with unitary involution such that E is a field (so $\delta_E = 1$) and

$$Y := R_{E/K}(\mathrm{SB}(B \otimes_F A^{\mathrm{op}}))$$

is incompressible, i.e., $\mathrm{cdim}(Y) = \dim(Y)$. For this by N. Karpenko's incompressibility result [Ka12, Theorem 1.1] it suffices that $B \otimes_F A^{\mathrm{op}}$ is a division algebra (note that B and A_E both carry unitary involutions, hence $N_{E/K}(B \otimes_F A^{\mathrm{op}})$ is split as required). The existence of such a pair (B, τ) was proven in [Lö11, Lemma 2.3].

□

Remark 4.1.   (a) In order to prove the correct lower bound on $\mathrm{ed}(G)$ in Proposition 4.2 using part (a) we really must choose the pair (B, τ) over a field K such that the center $E = Z(B)$ is non-split. Otherwise $B \simeq B_0 \times B_0^{\mathrm{op}}$ for some central simple K-algebra B_0 of degree d and the variety $R_{E/K}(\mathrm{SB}(B \otimes_F A^{\mathrm{op}}))$ has the same splitting fields as $\mathrm{SB}(B_0 \otimes_F A^{\mathrm{op}})$, which has strictly smaller dimension. Moreover δ_E would be 0 instead of 1.

(b) For $m = 0$, $d = 2^m = 1$, it is not true that $\mathrm{ed}(G) = d^2 = 1$, since then $G \simeq O_2$ and this group has $\mathrm{ed}(G) = 2$ by [Re99, Theorem 10.3].

4.3. Splitting a global problem into two local problems.

In almost all situations, when the (absolute) essential dimension of an algebraic group or algebraic stack is known, it is equal to its essential p-dimension for some prime p. This is a limitation of most methods we have in Galois cohomology and related algebraic areas. For a broad discussion of this phenomenon, see [Re10, §5]. As an example it is well known that $\mathrm{ed}_p(\mathbf{PGL}_p) = 2$ for all primes p, but the question if $\mathrm{ed}(\mathbf{PGL}_p) = 2$ for all primes p is widely open and a negative answer to this question would disprove the cyclicity conjecture of Albert for central simple algebras of degree p.

When the absolute essential dimension differs from essential p-dimension for all primes p (or is not known to coincide with essential p-dimension for some prime p) it often becomes significantly more difficult to compute it. This usually happens

when several primes are immediately tied to the problem. We call such a problem a global problem. A local problem is one, which depends only on one prime.

Theorem 1.1 allows us to attack some of these global problems by decomposing a global problem into two local problems.

We construct the following example: Let K/F be a quadratic separable extension and L/F a qubic separable extension. Let B be a central simple K-algebra of degree 3. Assume that $N_{K/F}(B)$ and $B \otimes_K (K \otimes_F L) \simeq B \otimes_F L$ are split, but B is non-split. Let $\mathcal{X}_B$ be the $R_{K/F}^{(1)}(\mathbf{G}_m)$-gerbe over F corresponding to the class of B in $H^2(F, R_{K/F}^{(1)}(\mathbf{G}_m)) = \ker(\mathrm{Br}(K) \overset{\mathrm{cor}}{\to} \mathrm{Br}(F))$.

Proposition 4.3. $\mathrm{ed}(\mathcal{X}_B) = 3$, $\mathrm{ed}_2(\mathcal{X}_B) = 1$, $\mathrm{ed}_3(\mathcal{X}_B) = 2$ and $\mathrm{ed}_p(\mathcal{X}_B) = 0$ for every prime $p \neq 2, 3$.

Proof. By Theorem 1.1

$$\mathrm{ed}(\mathcal{X}_B) = \mathrm{cdim}(\mathcal{X}) + \mathrm{ed}(R_{K/F}^{(1)}(\mathbf{G}_m)) = \mathrm{cdim}(\mathcal{X}_B) + 1.$$

Since $\mathcal{X}_B$ splits over L, which is of degree 3 over F, we have $\mathrm{cdim}_p(\mathcal{X}_B) = 0$ for every prime $p \neq 3$, hence for these primes $\mathrm{ed}_p(\mathcal{X}_B) = \mathrm{ed}_p(R_{K/F}^{(1)}(\mathbf{G}_m))$, which is 1 if $p = 2$ and 0 if $p \neq 2, 3$.

Moreover $\mathrm{ed}_3(\mathcal{X}_B) \leq \mathrm{cdim}_3(\mathcal{X}_B) + \mathrm{ed}_3(\mathcal{X}_B) = \mathrm{cdim}_3(\mathcal{X}_B)$. Since $\mathrm{cdim}_3(\mathcal{X}_B) \leq \mathrm{cdim}(\mathcal{X}_B)$ it remains to show that $\mathrm{cdim}(\mathcal{X}_B) \leq 2$ and $\mathrm{cdim}_3(\mathcal{X}_B) \geq 2$. Note that $\mathcal{X}_B$ becomes a $\mathbf{G}_m$-gerbe over K corresponding to the class of B in $\mathrm{Br}(K)$. Since B is non-split of degree 3 we have $\mathrm{cdim}_3(\mathcal{X}_B) = \mathrm{cdim}_3((\mathcal{X}_B)_K) = 2$. To show $\mathrm{cdim}(\mathcal{X}_B) \leq 2$ first note that a field extension M/F is a splitting field of $\mathcal{X}_B$ if and only if $B \otimes_F M$ is split. Hence it follows from [Bl10, Corollary 3.6] that $\mathcal{X}_B$ has the same splitting fields as a Del Pezzo surface S of degree 6 (the one associated to the triple $(B, M_2(L), KL)$). Therefore $\mathrm{cdim}(\mathcal{X}_B) \leq \dim S = 2$. $\qquad\square$

ACKNOWLEDGMENTS

REFERENCES

[BF03]   G. Berhuy, G. Favi, *Essential Dimension: A Functorial Point of View (after A. Merkurjev)*, Doc. Math. **8** (electronic) (2003), 279–330.

[Bl10]   M. Blunk, *Del Pezzo surfaces of degree 6 over an arbitrary field*, J. Algebra **323** (2010), no. 1, 42–58.

[BR97]   J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica **106** (1997), 159–179.

[BRV11]   P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*. With an appendix by Najmuddin Fakhruddin. J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1079-1112.

[Gi04]   Ph. Gille, *Spécialisation de la R-équivalence pour les groupes réductifs*, Trans. Amer. Math. Soc. **356** (2004), 4465–4474.

[Gir71]   J. Giraud, *Cohomologie non abélienne*, Springer-Verlag, Berlin, 1971, Die Grundlehren der mathematischen Wissenschaften, Band **179**.

[Ka00]   N. Karpenko, *On anisotropy of orthogonal involutions*. J. Ramanujan Math. Soc. **15**(1), (2000), 1–22.

[Ka12]   N. Karpenko, *Incompressibility of quadratic Weil transfer of generalized Severi- Brauer varieties.*, J. Inst. Math. Jussieu **11** (2012), no. 1, 119–131.

[KM06]   N. Karpenko, A. Merkurjev, *Canonical p-dimension of algebraic groups.* Adv. Math. **205**, 2 (2006), 410–433.

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

[KV84]   A. Klyachko, V. Voskresenskii, *Toric Fano varieties and systems of roots.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), no.2, 237–263.

[Lö10]   R. Lötscher, *Contributions to the essential dimension of finite and algebraic groups*, Ph.D. thesis (2010), available at `edoc.unibas.ch/1147/1/DissertationEdocCC.pdf`.

[Lö11]   R. Lötscher, *Essential dimension of involutions and subalgebras.* Israel J. Math. **192**(1), (2012), 325–346.

[Lö12]   R. Lötscher, *A fiber dimension theorem for essential and canonical dimension*, Compos. Math. **149**(1), (2013), 148–174.

[LMMR13] R. Lötscher, M. MacDonald, A. Meyer, Z. Reichstein, *Essential dimension of algebraic tori.* Crelle **677** (2013), 1–13.

[Me08]   A. Merkurjev, *Essential p-dimension of finite groups, Mini Course Lens 2008*, (2008), http://www.math.ucla.edu/˜merkurev/publicat.htm.

[Me09]   A. Merkurjev, *Essential dimension*, in Quadratic forms – algebra, arithmetic, and geometry (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemporary Mathematics **493** (2009), 299–326.

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

[Re99]   Z. Reichstein, *On the Notion of Essential Dimension for Algebraic Groups*, Transf. Groups **5**, no. 3 (2000), 265–304.

[Re10]   Z. Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians, Vol. II, Hindustan Book Agency, New Delhi, 2010, pp. 162–188.

[Stacks]   The Stacks Project Authors, *Stacks Project*, http://math.columbia.edu/algebraic_geometry/stacks-git.

Roland Lötscher

Mathematisches Institut der Ludwig-Maximilians-Universität München, Theresienstrasse 39, D-80333 München, Germany

E-mail address: `Roland.Loetscher@mathematik.uni-muenchen.de`