

ESSENTIAL DIMENSION

ALEXANDER S. MERKURJEV

1. INTRODUCTION

The essential dimension of an algebraic object is an integer that measures the complexity of the object. For example, let $Q = (a, b)_K$ be a quaternion algebra over a field extension K of a base field F of characteristic not 2. That is, let Q be a 4-dimensional algebra over K with basis $\{1, i, j, ij\}$ and multiplication table $i^2 = a, j^2 = b, ij = -ji$, where a and b are nonzero elements in K . Thus, Q is determined by two parameters a and b . Equivalently, we can say that the algebra Q is defined over the subfield $K' = F(a, b)$ of K , namely, $Q \simeq Q' \otimes_{K'} K$ for the quaternion algebra $Q' = (a, b)_{K'}$ over the field K' of transcendence degree at most 2 over F .

On the other hand, if a and b are two variables over an algebraic closure F_{alg} of F and $K = F_{\text{alg}}(a, b)$, then $Q = (a, b)_K$ is a division algebra over K that cannot be defined over a subfield K' of K of transcendence degree at most 1 over F since by Tsen's theorem, there are no division quaternion algebras over the subfield $K'F_{\text{alg}} \subset K$. We say that the essential dimension of the class of quaternion algebras is equal to 2. Informally speaking, the essential dimension of a class of algebraic objects is the minimal number of algebraically independent parameters one needs to define any object in the class.

The notion of the essential dimension was introduced by J. Buhler and Z. Reichstein in [7] for the class of finite Galois field extensions with a given Galois group G and later in [37], it was extended to the class of principal homogeneous G -spaces for a linear algebraic group G . Many classical algebraic objects, such as simple algebras, quadratic and hermitian forms, algebras with involutions, Cayley algebras, Jordan algebras, etc., are closely related to the principal homogeneous spaces of algebraic groups. For example, to give a quaternion algebra is the same as to give a principal homogeneous space of the group \mathbf{PGL}_2 .

The only property of a class of algebraic objects needed to define the essential dimension is that for every field extension K/F , we have a set $\mathcal{F}(K)$ of isomorphism classes of objects (quaternion algebras, for example), and for every field homomorphism $K \rightarrow L$ over F , a change of field map $\mathcal{F}(K) \rightarrow \mathcal{F}(L)$ (e.g., the change of field operation $Q \mapsto Q \otimes_K L$ for quaternion algebras). In other words, \mathcal{F} is a functor from the category \mathbf{Fields}_F of field extensions of F to the category \mathbf{Sets} of sets. The essential dimension for an arbitrary functor $\mathbf{Fields}_F \rightarrow \mathbf{Sets}$ was defined in [5].

One of the applications of the essential dimension is as follows. Suppose we would like to check whether a classification conjecture for the class of objects given by a functor \mathcal{F} holds. Usually, a classification conjecture assumes another functor \mathcal{L} (a

Date: October 2016.

The work has been supported by the NSF grant DMS #1160206.

conjectural classification list) together with a morphism of functors $\mathcal{L} \rightarrow \mathcal{F}$, and the conjecture asserts that this morphism is surjective, i.e., the map $\mathcal{L}(K) \rightarrow \mathcal{F}(K)$ is surjective for every field extension K/F . In other words, every object of type \mathcal{F} is on the list \mathcal{L} up to isomorphism.

Suppose we can compute the essential dimensions of \mathcal{L} and \mathcal{F} , and it turns out that $\text{ed}(\mathcal{L}) < \text{ed}(\mathcal{F})$, i.e., the functor \mathcal{F} is “more complex” than \mathcal{L} . This means that no morphism between \mathcal{L} and \mathcal{F} can be surjective and the classification conjecture fails. Thus, knowing the essential dimension allows us to predict the complexity of the structure. We have examples of this in the quadratic form theory (Section 9a) and in the theory of simple algebras (Corollaries 10.8 and 10.10).

Typically, the problem of computing the essential dimension of a functor splits into two problems of finding upper and lower bounds. Miraculously, in many cases the upper and lower bounds match.

The essential p -dimension for a prime integer p is the version of the essential dimension that ignores “prime to p effects”. Usually, the essential p -dimension is easier to compute than the ordinary essential dimension.

If the algebraic structures given by a functor \mathcal{F} are classified (parameterized), then the essential dimension of \mathcal{F} can be estimated by counting the number of algebraically independent parameters in the classification. (This is how we determined the essential dimension of the class of quaternion algebras.) But the essential dimension can be computed in many cases where no classification theorem is available! The most impressive example is the structure given by principal homogeneous spaces of the even Clifford group \mathbf{Clif}_n^+ (equivalently, non-degenerate quadratic forms of dimension n with trivial discriminant and Clifford invariant). The classification theorem is available for $n \leq 14$ only, but the exact value of the essential dimension was computed for every n and this value is exponential in n .

The canonical dimension is a special case of the essential dimension. The canonical dimension of a variety measures its compressibility. This can be studied by means of algebraic cycles.

The notion of the essential dimension of a functor can be naturally extended to the categories fibered in groupoids (such as stacks and gerbes). This allows us to unite the definitions of the essential dimension of algebraic varieties and algebraic groups.

Essential dimension, which is defined in elementary terms, has surprising connections with many areas of algebra such as algebraic geometry, algebraic K -theory, Galois cohomology, representation theory of algebraic groups, theory of fibered categories and valuation theory.

2. PRINCIPAL HOMOGENEOUS SPACES AND TORSORS

In this section we provide some basic definitions and facts about principal homogeneous spaces and torsors.

2a. Principal homogeneous spaces. Let G be a (linear) algebraic group, i.e., a smooth affine group scheme of finite type over a field F . We can view G as a (closed) subgroup of the general linear group \mathbf{GL}_n over F for some n .

A G -variety is an algebraic variety E together with an action of G on E . For example, the variety $E = G$ with the left G -action on itself is a G -variety. Every G -variety that is isomorphic to G with the left G -action is called a *trivial principal*

homogeneous G -space. If E is a G -variety over F , then for a field extension K/F , the K -variety $E_K := E \times_F \text{Spec } K$ is a G_K -variety. We will simply call E_K a G -variety over K .

A *principal homogeneous G -space* is a G -variety E such that E_K is a trivial principal homogeneous G -space for some field extension K/F . A principal homogeneous G -space is trivial if and only if E has a point over F , i.e., $E(F) \neq \emptyset$. In particular, all principal homogeneous G -spaces are trivial if the base field F is algebraically closed.

Example 2.1. For every nonzero real number a , let E_a be the circle given by the equation $x^2 + y^2 = a$ on the complex plane. We view E_a as a variety over \mathbb{R} . The complex multiplication makes $G := E_1$ (the unit circle) an algebraic group over \mathbb{R} and every E_a a principal homogeneous G -space. All E_a with $a > 0$ have real points, hence are trivial principal homogeneous G -spaces. If $a < 0$, all E_a are nontrivial (but isomorphic to each other) principal homogeneous G -spaces without real points.

Let G be an algebraic group over F . If K/F is a field extension, we write $G\text{-PHS}(K)$ for the set of isomorphism classes of principal homogeneous G -spaces over K . If L/K are field extensions of F , we have a change of field map

$$G\text{-PHS}(K) \rightarrow G\text{-PHS}(L),$$

taking an E to $E_L = E \times_K \text{Spec } L$.

In other words, the assignment $K \mapsto G\text{-PHS}(K)$ can be viewed as a functor from the category \mathbf{Fields}_F of (not necessarily finite) field extensions of F and field homomorphisms over F to the category \mathbf{Sets} of sets. We write

$$G\text{-PHS} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}.$$

Example 2.2. Let G be a finite group. We can view G as a *constant* algebraic group over a field F . A principal homogeneous G -space over a field extension K/F is of the form $\text{Spec}(M) \rightarrow \text{Spec}(K)$, where M is a *Galois G -algebra* over K . If M is a field, it is a Galois extension of K with Galois group G . The change of field map for a field extension L/K takes an algebra M to the tensor product $M \otimes_K L$ that is a Galois G -algebra over L .

Let A be an “algebraic object” over F “based” on a vector space over F , such as an F -algebra, quadratic form over F , a quasi-projective variety over F , an algebraic group over F , etc. Suppose that the change of field operation is defined and the automorphism group $G = \mathbf{Aut}(A)$ has the structure of an algebraic group such that $G(K) = \text{Aut}_K(A_K)$ for every field extension K/F . We say that an object B is a *twisted form of A* if B is isomorphic to A over a field extension K of F : $B_K \simeq A_K$.

If B is a twisted form of A , there is a natural action of the group G on the variety of isomorphisms $E \simeq \mathbf{Iso}(B, A)$ making E a principal homogeneous G -space over F . Conversely, if E is a principal homogeneous G -space over F , then the “diagonal” action of G on $E \times A$ descends to a twisted form $B = (E \times A)/G$ of A .

Thus, we have a bijection

$$G\text{-PHS}(F) \quad \longleftrightarrow \quad \boxed{\text{Isomorphism classes of twisted forms of } A}$$

Example 2.3. 1. Every automorphism of the matrix algebra $M_n(F)$ is inner. Therefore, $\mathbf{Aut}(M_n(F)) = \mathbf{PGL}_n$, the projective linear group. Twisted forms of $M_n(F)$ are central simple F -algebras of *degree* := square root of the dimension = n .

Also, \mathbf{PGL}_n is the automorphism group of the projective space \mathbb{P}_F^{n-1} . Twisted forms of \mathbb{P}_F^{n-1} are *Severi-Brauer* varieties of dimension $n - 1$. We have bijections

$$\boxed{\text{Central simple algebras of degree } n \text{ over } F} \leftrightarrow \mathbf{PGL}_n\text{-PHS}(F) \leftrightarrow \boxed{\text{Severi-Brauer varieties of dimension } n - 1 \text{ over } F}$$

The Severi-Brauer variety corresponding to a central simple F -algebra A of degree n is the variety of right ideals in A of dimension n .

2. The symmetric group S_n acts by permutation of the components of the F -algebra $F^n := F \times F \times \cdots \times F$ (n times) and moreover, $\mathbf{Aut}_{F\text{-alg}}(F^n) = S_n$. Twisted forms of F^n are *étale* (or, equivalently, commutative *separable*) F -algebras of dimension n . Such algebras are finite products of finite separable field extensions of F . Therefore, we have a bijection

$$S_n\text{-PHS}(F) \longleftrightarrow \boxed{\text{Étale algebras of dimension } n \text{ over } F}$$

3. Let q be a non-degenerate quadratic form of dimension n over a field F of characteristic not 2. The automorphism group of q is the orthogonal group $\mathbf{O}(q)$. A twisted form of q is also a non-degenerate quadratic form over F of the same dimension n . We then have a bijection

$$\mathbf{O}(q)\text{-PHS}(F) \longleftrightarrow \boxed{\text{Non-degenerate quadratic forms of dimension } n \text{ over } F}$$

4. The automorphism group of the (split) 8-dimensional Cayley algebra C is a simple group with Dynkin diagram G_2 . A twisted form of C is a *Cayley-Dickson* algebra. Thus, we have a bijection

$$G_2\text{-PHS}(F) \longleftrightarrow \boxed{\text{Cayley-Dickson algebras over } F}$$

For an algebraic group G over F , there is a bijection between pointed sets

$$G\text{-PHS}(F) \simeq H^1(F, G),$$

where $H^1(F, G)$ is the first cohomology set of the *absolute Galois group* $\text{Gal}(F_{\text{sep}}/F)$ with values in $G(F_{\text{sep}})$ (here F_{sep} is a separable closure of F , see [43]).

2b. Torsors. Informally speaking, a G -torsor for an algebraic group G over a field F is a family of principal homogeneous G -spaces with the base a variety over F . That is, let $f : X \rightarrow Y$ be a morphism of G -varieties such that G acts trivially on the base Y . We say that X is a *G -torsor over Y* if there is a faithfully flat base change $Y' \rightarrow Y$ such that the morphism $X \times_Y Y' \rightarrow Y'$ is a *trivial G -torsor*, i.e., it is isomorphic to the projection $G \times Y' \rightarrow Y'$. In particular, f is flat and for every point $y \in Y(K)$ for a field extension K/F , the fiber of f over y is a principal homogeneous G -space over K . Thus, a torsor can be viewed as a flat family of principal homogeneous G -spaces.

A principal homogeneous G -space X over F yields a G -torsor $X \rightarrow \text{Spec}(F)$ over the point $\text{Spec}(F)$ and the converse is also true.

Example 2.4. Let X be the open subvariety of the complex plane given by $x^2 + y^2 \neq 0$ viewed as a variety over \mathbb{R} . The unit circle G acts on X by complex multiplication. Write Y for the affine real line without the origin. The morphism $f : X \rightarrow Y$ taking a point (b, c) to $b^2 + c^2$ is a G -torsor. The scheme-theoretic fiber of f over a point a is the variety E_a defined in Example 2.1. Thus, f provides a family of principal homogeneous G -spaces E_a when a varies in Y .

Example 2.5. If G is a (closed) subgroup of an algebraic group G' , by a theorem of Chevalley, the factor variety G'/G of (left) cosets exists and the natural morphisms $G' \rightarrow G'/G$ is a G -torsor.

A G -variety X is called *generically free* if the scheme-theoretic stabilizer of the generic point of X is trivial. By [10, Exposé V, Théorème 8.1], this is equivalent to saying that there is a nonempty open G -invariant subvariety $U \subset X$ and a G -torsor $U \rightarrow Y$ with Y a variety over F .

A nonempty G -invariant open subvariety of a generically free G -variety is also a generically free G -variety.

A finite dimensional linear representation V of G is called *generically free* if the affine space $\mathbb{A}(V)$ is generically free as a G -variety. If G is finite, a representation is generically free if and only if it is faithful.

Example 2.6. Generically free G -representations exist. Indeed, embed G as a subgroup into a general linear group $U := \mathbf{GL}_n$ for some n . Then U can be viewed as an open subvariety of the affine space $V := M_n(F)$ of all $n \times n$ matrices over F . The group U (and therefore, G) acts linearly on V by left translations. Moreover, G acts on the open set U with trivial stabilizers and the factor variety U/G exists by Example 2.5.

A G -torsor $f : X \rightarrow Y$ is called *versal* if for every field extension K/F with K infinite (this holds automatically if F is infinite), for every principal homogeneous G -space $E \rightarrow \text{Spec}(K)$ and for every nonempty open subvariety $W \subset Y$, there is a point $y \in W(K)$ such that the fiber of f over y is isomorphic to E as a G -variety. In other words, every principal homogeneous G -space is isomorphic to (many) fibers of the versal G -torsor and the union of such fibers is dense in X .

An application of Hilbert Theorem 90 yields the following result.

Proposition 2.7. *Let V be a generically free representation of an algebraic group G , $U \subset V$ a nonempty open G -invariant subvariety and $U \rightarrow Y$ a G -torsor with Y a variety over F . Then the torsor $U \rightarrow Y$ is versal.*

3. EVOLUTION OF THE DEFINITION OF THE ESSENTIAL DIMENSION

In this section, we describe four steps of the evolution of the notion of essential dimension.

Step 1. The definition of the essential dimension of an algebraic group G was given by J. Buhler and Z. Reichstein in [7] when G is finite and by Z. Reichstein in [37] for an arbitrary G . The original approach to the essential dimension of algebraic groups used the language of equivariant compressions of algebraic varieties.

Let X be an irreducible generically free G -variety. A G -compression of X is a G -equivariant dominant rational morphism $X \dashrightarrow X'$ to a generically free G -variety X' . We write $\text{ed}(X, G)$ for the smallest integer

$$\dim(X') - \dim(G)$$

over all generically free G -varieties X' such that there is G -compression $X \dashrightarrow X'$.

The following proposition is a direct consequence of the definition of versality.

Proposition 3.1. *Let X and X' be two irreducible generically free G -varieties such that X' is versal. Then $\text{ed}(X, G) \leq \text{ed}(X', G)$.*

It follows from the proposition that the integer $\text{ed}(X, G)$ is independent of the choice of the generically free versal G -variety X . This integer is called the *essential dimension* $\text{ed}(\text{BG})$ of G . (The notation BG will be explained in Example 3.6.)

If V is a generically free representation of G , then V is versal by Proposition 2.7. Therefore, the essential dimension of G is equal to $\text{ed}(V, G)$.

Step 2. One can define the essential dimension of a group G in terms of principal homogeneous spaces only. Let X be an irreducible generically free G -variety and $U \subset X$ a nonempty open G -invariant subvariety such that there exists a G -torsor $U \rightarrow Y$ over F .

The generic fiber $E := U \times_Y \text{Spec } F(Y)$ of $U \rightarrow Y$, where $F(Y)$ is the function field of Y , is a principal homogeneous G -space over $F(Y)$ independent of the choice of the open set U . We write $F(X)^G$ for the field $F(Y)$. The transcendence degree $\text{tr. deg}_F(F(X)^G)$ of the field $F(X)^G$ over F is equal to $\dim(X) - \dim(G) = \text{ed}(X, G)$.

Conversely, every principal homogeneous G -space over a finitely generated field extension K/F extends to a G -torsor $X \rightarrow Y$ for a variety Y over F with $F(Y) \simeq K$.

Let K/F be a field extension, E a principal homogeneous G -space over K and $K' \subset K$ a subfield containing F . We say that E is *defined over K'* (or that K' is a *field of definition of E*) if there is a principal homogeneous G -space E' over K' such that $E \simeq E' \times_{K'} \text{Spec}(K)$.

A G -compression $X \dashrightarrow X'$ of irreducible generically free G -varieties yields an embedding of fields $F(X')^G \hookrightarrow F(X)^G$. Moreover, the generic fiber E for the G -variety X is obtained via change of field from the generic fiber E' for X' , i.e.,

$$E \simeq E' \times_{F(X')^G} \text{Spec}(F(X)^G).$$

Therefore, the smallest transcendence degree of the field of definition of E is equal to $\text{ed}(X, G)$.

We then have the following definition of the essential dimension of G in terms of principal homogeneous G -spaces. Let K/F be a field extension and E a principal homogeneous G -space over K . Let $\text{ed}(E)$ denote the smallest transcendence degree of a field of definition of E . If E is the generic fiber for a generically free G -variety X , then $\text{ed}(E) = \text{ed}(X, G)$. The essential dimension $\text{ed}(\text{BG})$ of G is the supremum of $\text{ed}(E)$ over all principal homogeneous G -spaces E over all field extensions K/F .

Let X be a generically free versal G -variety. The generic fiber E_{gen} for X is called a *generic principal homogeneous G -space*. We have $\text{ed}(E_{\text{gen}}) = \text{ed}(X, G) = \text{ed}(\text{BG})$, i.e., the essential dimension of G coincides with the essential dimension of a generic principal homogeneous G -space.

Step 3. The only property of principal homogeneous spaces used in the definition of the essential dimension of an algebraic group G in Step 2 was the existence of the

natural change of field operation. We can then define the essential dimension in a much more general abstract situation (see [5]).

Suppose for every field extension K/F , we have a set $\mathcal{F}(K)$ and for every field extension L/K we have a map of sets $\mathcal{F}(K) \rightarrow \mathcal{F}(L)$ natural for towers of field extensions. In other words, we are given a functor

$$\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}.$$

Let K/F be a field extension, $x \in \mathcal{F}(K)$ and $K' \subset K$ a subfield containing F . We say that x is *defined over K'* (or K' is a *field of definition of x*) if x belongs to the image of the map $\mathcal{F}(K') \rightarrow \mathcal{F}(K)$ induced by the inclusion of K' into K .

We define the *essential dimension* $\text{ed}(x)$ of x by

$$\text{ed}(x) := \min \text{tr. deg}_F(K'),$$

where the minimum is taken over all fields of definition K' of x . In other words, the essential dimension of x is the smallest transcendence degree of a field of definition of x .

We also define the *essential dimension* $\text{ed}(\mathcal{F})$ of the functor \mathcal{F} by

$$\text{ed}(\mathcal{F}) := \sup \text{ed}(x),$$

where the supremum is taken over all field extensions K/F and all $x \in \mathcal{F}(K)$.

Remark 3.2. The essential dimension of the class $x \in \mathcal{F}(K)$ of an algebraic object can be viewed as the minimal number of algebraically independent parameters one needs to define the object.

Example 3.3. The essential dimension of the functor G -PHS defined in Section 2a for an algebraic group G coincides with the essential dimension of G as defined in Step 2.

Example 3.4. ([29, Corollary 1.4]) Every variety X over F can be viewed as a functor taking a field extension K/F to the set $X(K)$ of K -points of X . We have $\text{ed}(X) = \dim(X)$.

Step 4. In many examples of functors $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$, the sets $\mathcal{F}(K)$ are isomorphism classes of objects in certain categories. It is convenient to consider these categories which usually form what is called a *category fibered in groupoids*.

Let $\mathbf{Schemes}_F$ be the category of schemes over F , $\pi : \mathcal{X} \rightarrow \mathbf{Schemes}_F$ a functor, a an object of \mathcal{X} and $X = \pi(a)$. We say that a is an *object over X* . For every scheme X over F , all objects over X form the *fiber category* $\mathcal{X}(X)$ with morphisms f satisfying $\pi(f) = 1_X$.

Let $f : a \rightarrow b$ be a morphism in \mathcal{X} and $\alpha := \pi(f) : X \rightarrow Y$, so that a is an object over X and b is over Y . We say that the *morphism f is over α* .

The category \mathcal{X} equipped with a functor π is called a *category fibered in groupoids over F* (CFG) if the following two conditions hold:

- (1) For every morphism $\alpha : X \rightarrow Y$ in $\mathbf{Schemes}_F$ and every object b in \mathcal{X} over Y , there is an object a in \mathcal{X} over X and a morphism $a \rightarrow b$ over α .
- (2) For every pair of morphisms $\alpha : X \rightarrow Y$ and $\beta : Y \rightarrow Z$ in $\mathbf{Schemes}_F$ and morphisms $g : b \rightarrow c$ and $h : a \rightarrow c$ in \mathcal{X} over β and $\beta \circ \alpha$, respectively, there is a unique morphism $f : a \rightarrow b$ over α such that $h = g \circ f$.

It follows from the definition that the object a in (1) is uniquely determined by b and α up to canonical isomorphism. We will write $\alpha^*(b)$ for a . The fiber categories $\mathcal{X}(X)$ are *groupoids* for every X , i.e., every morphism in $\mathcal{X}(X)$ is an isomorphism.

Informally speaking, a *CFG* over F is a collection of groupoids $\mathcal{X}(X)$ for all schemes X over F and a collection of “base change” functors $\mathcal{X}(Y) \rightarrow \mathcal{X}(X)$, $b \mapsto \alpha^*(b)$, for all morphisms $\alpha : X \rightarrow Y$ of schemes over F .

Example 3.5. Every scheme X over F can be viewed as a *CFG* as follows. An object of X (as a *CFG*) is a scheme Y over X , i.e., a morphism $Y \rightarrow X$ over F . A morphism between two objects is a morphism of schemes over X . The functor $\pi : X \rightarrow \mathbf{Schemes}_F$ takes a scheme Y over X to Y and a morphism between two schemes over X to itself. Note that the fiber groupoids $X(Y) = \text{Mor}(Y, X)$ are sets, i.e., every morphism in $X(Y)$ is the identity.

Example 3.6. Let G be an algebraic group and let X be a G -variety over F . We define X/G as a *CFG* as follows. An object of X/G is a diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & X, \\ \rho \downarrow & & \\ & & Y \end{array}$$

where ρ is a G -torsor and φ is a G -equivariant morphism. A morphism between two such diagrams is a morphism between the G -torsors satisfying the obvious compatibility condition. The functor $\pi : X/G \rightarrow \mathbf{Schemes}_F$ takes the diagram to Y .

If $E \rightarrow Y$ is a G -torsor, then $E/G \simeq Y$.

If $X = \text{Spec}(F)$, we write BG for X/G . This is the category of all G -torsors over arbitrary bases and the fiber category $\text{BG}(Y)$ for a scheme Y is the category of G -torsors $E \rightarrow Y$ over Y . Sometimes BG is called the *classifying space* of G .

Example 3.7. Let K/F be a finite Galois field extension with Galois group H and $f : G \rightarrow H$ a surjective homomorphism of finite groups with kernel N . Then G acts on $\text{Spec}(K)$ via f . An object of the fiber of the category $\mathcal{X} := \text{Spec}(K)/G$ over $\text{Spec}(F)$ is a principal homogeneous G -space $E \rightarrow \text{Spec}(F)$ together with an isomorphism $E/N \xrightarrow{\sim} \text{Spec}(K)$ of H -spaces. By Example 2.2, $E \simeq \text{Spec}(L)$, where L/F is a Galois extension with Galois group G such that $L^N \simeq K$. In other words, L/F is a solution of the *embedding problem* in Galois theory given by K/F and f (see [17]).

Example 3.8. Let $f : G \rightarrow H$ be a surjective homomorphism such that the subgroup $C := \text{Ker}(f)$ of G is central. Let E be a principal homogeneous H -space over F . The category E/G is called a *gerbe banded by C* . It is uniquely determined by a class in the cohomology group $H^2(F, C)$, the image of the class of E under the connecting map $H^1(F, H) \rightarrow H^2(F, C)$ induced by the exact sequence $1 \rightarrow C \rightarrow G \rightarrow H \rightarrow 1$.

An object of the fiber of the category E/G over $\text{Spec}(F)$ is a principal homogeneous G -space E' over F together with an isomorphism $E \simeq E'/C$ of H -varieties, i.e., the principal homogeneous G -space E' is a *lifting* of E .

The essential dimension of a category fibered in groupoids was defined by R. Löttscher in [28] as follows. Let \mathcal{X} be a *CFG* over F , x an object in the fiber $\mathcal{X}(K)$ of \mathcal{X} over $\text{Spec}(K)$ and $K' \subset K$ a subfield over F . We say that x is *defined over K'* (or

that K' is a field of definition of x) if there exists an object x' in $\mathcal{X}(K')$ such that $x \simeq \alpha^*(x')$, where $\alpha : K' \rightarrow K$ is the inclusion.

Define

$$\text{ed}(x) := \min \text{tr. deg}_F(K'),$$

where the minimum is taken over all fields of definition K' of x .

If the fiber category $\mathcal{X}(X)$ is *essentially small* for every X , i.e, isomorphism classes of objects of $\mathcal{X}(X)$ form a set, we have a functor $\mathcal{F}_{\mathcal{X}} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ taking a field K to the set of isomorphism classes in $\mathcal{F}(K)$ and a field extension $\alpha : K \rightarrow L$ to the map $[x] \mapsto [\alpha^*(x)]$, where $[x]$ denotes the isomorphism class of a . It follows from the definitions that

$$\text{ed}(\mathcal{X}) = \text{ed}(\mathcal{F}_{\mathcal{X}}).$$

Thus, the notion of the essential dimension of a CFG generalizes the one of a functor given in Step 3.

Example 3.9. If G is an algebraic group over F , then $\text{ed}(BG)$, where BG is defined in Example 3.6, coincides with the essential dimension of G as defined in Step 2.

Example 3.10. If X is a variety over X , the essential dimension of X viewed as CFG in Example 3.5, coincides with the essential dimension of X viewed as a functor and thus is equal to $\dim(X)$ by Example 3.4.

Thus, the language of fibered categories unites the two seemingly different cases of the essential dimension of an algebraic variety and an algebraic group.

3a. Simple properties and examples. The following proposition is a straightforward consequence of the definition of the essential dimension of a functor.

Proposition 3.11 ([29], Proposition 1.3). *If $\alpha : \mathcal{F} \rightarrow \mathcal{F}'$ is a surjective morphism of functors from \mathbf{Fields}_F to \mathbf{Sets} , then $\text{ed}(\mathcal{F}) \geq \text{ed}(\mathcal{F}')$.*

The problem of computing the essential dimension of a functor \mathcal{F} very often splits into two problems of finding a lower and an upper bound for $\text{ed}(\mathcal{F})$, and in some cases the bounds match.

Example 3.12. For an integer $n > 0$ and a field extension K/F , let $\mathcal{F}(K)$ be the set of similarity classes of all $n \times n$ matrices over K , or, equivalently, the set of isomorphism classes of linear operators in an n -dimensional vector space over K . The *rational canonical form* of a linear operator suggests that it suffices to give n parameters to define an operator, so $\text{ed}(\mathcal{F}) \leq n$. On the other hand, the coefficients of the characteristic polynomial of an operator yield a surjective morphism of functors $\mathcal{F} \rightarrow \mathbb{A}_F^n$, where \mathbb{A}_F^n is the affine space of dimension n , hence by Example 3.4 and Proposition 3.11, $\text{ed}(\mathcal{F}) \geq \text{ed}(\mathbb{A}_F^n) = \dim(\mathbb{A}_F^n) = n$. Therefore, the upper and lower bounds match and $\text{ed}(\mathcal{F}) = n$.

Let $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ be a functor. A variety X over F is called *classifying* for \mathcal{F} if there is a surjective morphism of functors $X \rightarrow \mathcal{F}$.

Corollary 3.13. *Let $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ be a functor and X a classifying variety for \mathcal{F} . Then $\dim(X) \geq \text{ed}(\mathcal{F})$.*

3b. Essential p -dimension. Let p be a prime integer. The idea of the essential p -dimension is to “ignore field extensions of degree prime to p ” (see [39]).

We say that a field extension L/K is a *prime to p extension* if L/K is finite and the degree $[L : K]$ is prime to p .

Let $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ be a functor, K/F a field extension, $x \in \mathcal{F}(K)$. We define the *essential p -dimension of x* :

$$\mathrm{ed}_p(x) := \min \mathrm{ed}(x_L),$$

where L runs over all prime to p extensions of K and we let the *essential p -dimension of the functor \mathcal{F}* be defined as

$$\mathrm{ed}_p(\mathcal{F}) := \max \mathrm{ed}_p(x),$$

where the maximum is taken over all field extensions K/F and all $x \in \mathcal{F}(K)$.

We have the inequality $\mathrm{ed}_p(\mathcal{F}) \leq \mathrm{ed}(\mathcal{F})$ for every p .

3c. Special groups. The *index n_X* of a variety X is the greatest common divisor of the degrees $[F(x) : F]$ over all closed points $x \in X$.

Let G be an algebraic group over F . The *torsion index t_G* of G is the least common multiple of the indices n_X over all principal homogeneous G -spaces $X \rightarrow \mathrm{Spec}(K)$ as K ranges over the field extensions of F . Prime divisors of t_G are called *torsion primes for G* [42, 2.3].

An algebraic group G over F is called *special* if for any field extension K/F , every principal homogeneous G -space over $\mathrm{Spec} K$ is trivial. Clearly, special groups have no torsion primes. Examples of special groups are \mathbf{GL}_n , \mathbf{SL}_n , \mathbf{Sp}_{2n} and quasi-split tori.

The last statement of the following proposition was proven in [38, Proposition 5.3] in the case when F is algebraically closed.

Proposition 3.14. [29, Proposition 4.4] Let G be an algebraic group over F . Then

- (1) A prime integer p is a torsion prime for G if and only if $\mathrm{ed}_p(\mathrm{BG}) > 0$.
- (2) An algebraic group G is special if and only if $\mathrm{ed}(\mathrm{BG}) = 0$.

4. CANONICAL DIMENSION

The canonical dimension is a special case of the essential dimension. It turns out to be related to the incompressibility property of algebraic varieties and can be studied by means of algebraic cycles.

4a. Definition of the canonical dimension. The notion of canonical dimension of G -varieties was introduced by G. Berhuy and Z. Reichstein in [4]. In this section, we give a more general definition of the canonical dimension of a functor (see [23, §2] and [29, §1.6]). A more general definition of the canonical dimension of a category fibered in groupoids was given in [28].

A functor $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ is called a *detection functor* if the set $\mathcal{F}(K)$ has at most one element for every field extension K/F . Every detection functor \mathcal{F} determines a class $\mathcal{C}_{\mathcal{F}}$ of field extensions of F consisting of all K/F such that $\mathcal{F}(K)$ is non-empty. The class $\mathcal{C}_{\mathcal{F}}$ is *closed under extensions*: if $K \in \mathcal{C}_{\mathcal{F}}$ and L/K is a field extension, then $L \in \mathcal{C}_{\mathcal{F}}$. Conversely, every class \mathcal{C} of field extensions of F closed under extensions determines a unique detection functor \mathcal{F} such that $\mathcal{C} = \mathcal{C}_{\mathcal{F}}$. Thus, to give a detection functor $\mathbf{Fields}_F \rightarrow \mathbf{Sets}$ is the same as to give a class of field extensions of F closed under extensions.

Let $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ be an arbitrary functor. We can associate with \mathcal{F} a detection functor $\widehat{\mathcal{F}}$ defined by

$$\widehat{\mathcal{F}}(K) = \begin{cases} \{K\}, & \text{if } \mathcal{F}(K) \neq \emptyset; \\ \emptyset, & \text{otherwise.} \end{cases}$$

The corresponding class $\mathcal{C}_{\mathcal{F}} := \mathcal{C}_{\widehat{\mathcal{F}}}$ of field extensions of F consists of all K/F such that $\mathcal{F}(K)$ is not empty.

We define the *canonical dimension* $\text{cdim}(\mathcal{F})$ of the functor \mathcal{F} by

$$\text{cdim}(\mathcal{F}) := \text{ed}(\widehat{\mathcal{F}}).$$

If \mathcal{C} is a class of field extensions of F closed under extensions, we write

$$\text{cdim}(\mathcal{C}) := \text{ed}(\mathcal{F}),$$

where \mathcal{F} is the detection functor associated with \mathcal{C} .

By definition, the integer $\text{cdim}(\mathcal{C})$ is the supremum of the integers $\text{cdim}(K)$ over all fields $K \in \mathcal{C}$, where

$$\text{cdim}(K) := \min \text{tr. deg}_F(K'),$$

where the minimum is taken over all subfield $K' \subset K$ containing F such that $K' \in \mathcal{C}$.

Since there is a natural surjection $\mathcal{F} \rightarrow \widehat{\mathcal{F}}$, we have

$$\text{cdim}(\mathcal{F}) \leq \text{ed}(\mathcal{F})$$

by Proposition 3.11.

As in the case of the essential dimension, we can define the *p-canonical dimension* of a functor for a prime integer p by

$$\text{cdim}_p(\mathcal{F}) := \text{ed}_p(\widehat{\mathcal{F}}).$$

4b. Canonical dimension and incompressibility of a variety. Let X be a variety over F . Viewing X as a functor from \mathbf{Fields}_F to \mathbf{Sets} , we have the *canonical dimension* $\text{cdim}(X)$ and the *canonical p-dimension* $\text{cdim}_p(X)$ of X defined. In other words, $\text{cdim}(X)$ is the canonical dimension of the class of fields

$$\mathcal{C}_X = \{K \in \mathbf{Fields}_F \text{ such that } X(K) \neq \emptyset\}.$$

We have $\text{cdim}(X) \leq \text{ed}(X) = \dim(X)$.

The canonical dimension of X can be much smaller than $\dim(X)$. For example, if X has a rational point, i.e., $X(F) \neq \emptyset$, then \mathcal{C}_X coincides with the class of all field extensions of F . Therefore, $\text{cdim}(X) = 0$.

We say that an irreducible variety X is *incompressible* if every rational morphism $X \dashrightarrow X$ is dominant, i.e, X cannot be ‘‘compressed’’ rationally to a proper closed subvariety.

A relation between the canonical dimension and the incompressibility property of an irreducible variety X can be seen as follows. Let $x_{\text{gen}} \in X(F(X))$ be the generic point (over the function field $F(X)$) and let $f : X \dashrightarrow X$ be a rational morphism with closure of the image being a closed irreducible subvariety $Z \subset X$. The morphism f identifies the function field $F(Z)$ with a subfield of $F(X)$, and X has a point over $F(Z)$, the generic point of Z , i.e., $X(F(Z)) \neq \emptyset$. If one can choose a non-dominant rational map f , then Z is smaller than X and by the definition of the canonical dimension,

$$\text{cdim}(x_{\text{gen}}) \leq \text{tr. deg}_F(F(Z)) = \dim(Z) < \dim(X).$$

In fact, one can prove that $\text{cdim}(X) < \dim(X)$. A more precise statement is the following proposition.

Proposition 4.1 ([32], Proposition 4.3). *Let X be an irreducible variety over F . Then X is incompressible if and only if $\text{cdim}(X) = \dim(X)$.*

We say that an irreducible variety X over F is *p -incompressible* if for any variety X' over F , admitting a dominant morphism $X' \rightarrow X$ of degree prime to p , every morphism $X' \rightarrow X$ is dominant or, equivalently, $\text{cdim}_p(X) = \dim(X)$. Every p -incompressible variety is incompressible.

The canonical dimension and p -dimension of regular complete varieties can be determined as follows.

Proposition 4.2 ([22], Corollary 4.11). *Let X be an irreducible regular complete variety over F . Then $\text{cdim}_p(X)$ is the least dimension of the image of a morphism $X' \rightarrow X$, where X' is a variety over F admitting a dominant morphism $X' \rightarrow X$ of degree prime to p . Similarly, $\text{cdim}(X)$ is the smallest dimension of the image of a rational morphism $X \dashrightarrow X$.*

The study of algebraic cycles proved to be very useful while studying the incompressibility property of algebraic varieties.

Let X and Y be varieties over F and $d = \dim(X)$. A *correspondence* from X to Y , denoted $\alpha: X \rightsquigarrow Y$, is an element $\alpha \in \text{CH}_d(X \times Y)$ of the *Chow group* of classes of algebraic cycles of dimension d on $X \times Y$. If $\dim(Y) = d$, we write $\alpha^t: Y \rightsquigarrow X$ for the image of α under the exchange isomorphism $\text{CH}_d(X \times Y) \simeq \text{CH}_d(Y \times X)$.

Let $\alpha: X \rightsquigarrow Y$ be a correspondence. Assume that Y is complete. The projection morphism $p: X \times Y \rightarrow X$ is proper and hence the push-forward homomorphism

$$p_*: \text{CH}_d(X \times Y) \rightarrow \text{CH}_d(X) = \mathbb{Z} \cdot [X]$$

is defined [13, § 1.4]. The integer $\text{mult}(\alpha) \in \mathbb{Z}$ such that $p_*(\alpha) = \text{mult}(\alpha) \cdot [X]$ is called the *multiplicity* of α . For example, if α is the class of the closure of the graph of a rational morphism $X \dashrightarrow Y$ of varieties of the same dimension, then $\text{mult}(\alpha) = 1$ and $\text{mult}(\alpha^t) := \deg(f)$, where $\deg(f)$ indicates the *degree* of f .

Proposition 4.3 ([21], Lemma 2.7). *Let p be a prime integer and X an irreducible complete variety. Suppose that for every correspondence $\alpha: X \rightsquigarrow X$ such that $\text{mult}(\alpha)$ is not divisible by p , the integer $\text{mult}(\alpha^t)$ is also not divisible by p . Then X is p -incompressible.*

Example 4.4. Proposition 4.3 can be used to prove the following (see [18] or [19]). Let A be a central simple F -algebra of degree p^n , where p is a prime integer. Let $X = \text{SB}(A)$ be the Severi-Brauer variety of right ideals in A of dimension p^n (see Example 2.3.1). The variety X has a point over a field extension K/F if and only if the algebra $A \otimes_F K$ is split, i.e., isomorphic to the matrix algebra $M_{p^n}(K)$. Then $\text{cdim}(X) = \text{cdim}_p(X) = p^m - 1$, where $p^m \leq p^n$ is the *index* of A , i.e., the smallest degree of a splitting field of A . In particular, X is p -incompressible if and only if $\text{ind}(A) = p^n = \deg(A)$ if and only if A is a division algebra.

In general, the product of incompressible varieties may not be incompressible.

The following generalization of the previous example has been used in the proof of Theorem 6.3.

Example 4.5. Let p be a prime integer and $B \subset \text{Br}(F)$ a p -elementary finite subgroup. Let A_1, A_2, \dots, A_n be central division algebras such that the classes $[A_i]$ form a basis of B over $\mathbb{Z}/p\mathbb{Z}$. Let X_i be the Severi-Brauer variety of A_i . Then the product $X := X_1 \times X_2 \times \dots \times X_n$ is p -incompressible if and only if the sum $\sum_i \deg(A_i)$ is the smallest possible over all choices of a basis $[A_1], [A_2], \dots, [A_n]$ for B . This was originally shown in [23, Theorem 2.1] with the help of algebraic K -theory. For the proof in the context of algebraic cycles, see [20].

The algebras A_i providing a p -incompressible X can be constructed by induction as follows. Let $[A_1]$ be a nonzero class in B of the smallest index. If the classes $[A_1], \dots, [A_{i-1}]$ are already chosen for some i , we take $[A_i]$ to be the class of the smallest index among the classes in $B \setminus \text{span}([A_1], \dots, [A_{i-1}])$.

Surprisingly, the incompressibility of Severi-Brauer varieties of algebras of relatively prime degrees is a more difficult problem. The following conjecture is still wide open.

Conjecture 4.6. *Let A_1, A_2, \dots, A_r be central division F -algebras of degree q_1, q_2, \dots, q_r , respectively, where q_i are powers of distinct primes. Let X_i be the Severi-Brauer variety of A_i . Then the product $X = X_1 \times X_2 \times \dots \times X_r$ is incompressible.*

This conjecture was proved in the case when $r = 1$, i.e., when $\deg(A)$ is a power of a prime integer (Example 4.4) and in the case $n = 6$ if $\text{char}(F) = 0$ (see [9, Theorem 1.3]). The proof uses the classification of rational surfaces. In particular, del Pezzo surfaces of degree 6 were used.

If the conjecture were true, we would know the canonical dimension of an arbitrary Severi-Brauer variety. That is, if A is a central simple F -algebra, we can write the class of A in the Brauer group of F as the sum of classes of central division F -algebras A_1, A_2, \dots, A_r of degree q_1, q_2, \dots, q_r , respectively, where q_i are powers of distinct primes. Then, Conjecture 4.6 would imply that

$$\text{cdim}(\text{SB}(A)) = \sum_{i=1}^r (q_i - 1).$$

5. ESSENTIAL DIMENSION OF ALGEBRAIC GROUPS

Let G be an algebraic group over a field F . The essential dimension $\text{ed}(\text{BG})$ of the group G is defined as the essential dimension of the category fibered in groupoids BG of G -torsors (see Example 3.9), or equivalently, as the essential dimension of the functor $G\text{-PHS} : \text{Fields}_F \rightarrow \text{Sets}$ (Example 3.3). Thus, the integer $\text{ed}(\text{BG})$ measures the complexity of the class of principal homogeneous G -spaces.

Let V be a generically free representation of G . By Step 1 in Section 2, $\text{ed}(\text{BG}) = \text{ed}(V, G) \leq \dim(V) - \dim(G)$. Therefore, we have the following upper bound for $\text{ed}(\text{BG})$.

Proposition 5.1. *Let G be an algebraic group over a field F . Then*

$$\text{ed}(\text{BG}) \leq \min \dim(V) - \dim(G),$$

where the minimum is taken over all generically free representation V of G over F .

Example 5.2. Let G be an adjoint semisimple group (a semisimple group with a trivial center). Then the adjoint representation of G on the direct sum of two copies

of the Lie algebra $\mathrm{Lie}(G)$ of G is generically free. Hence,

$$\mathrm{ed}(\mathrm{BG}) \leq 2 \dim \mathrm{Lie}(G) - \dim(G) = \dim(G).$$

Note that, in contrast, the essential dimension of the spinor group \mathbf{Spin}_n is exponential in n (see Section 9).

5a. Cohomological invariants. Cohomological invariants provide lower bounds for the essential dimension (see [37]). Let M be a *Galois module over F* , i.e., M is a (discrete) abelian group equipped with a continuous action of the absolute Galois group $\Gamma_F := \mathrm{Gal}(F_{\mathrm{sep}}/F)$ of F . For a field extension K/F , M can be viewed as a Galois module over K via the restriction homomorphism $\Gamma_K \rightarrow \Gamma_F$. For every $d \geq 0$, we have a *degree d cohomological functor*

$$\begin{aligned} H : \mathbf{Fields}_F &\rightarrow \mathbf{AbelianGroups} \\ K &\mapsto H^d(K, M). \end{aligned}$$

A *degree d cohomological invariant with values in M of a functor $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$* is a morphism of functors $u : \mathcal{F} \rightarrow H$, where we view H as a functor to \mathbf{Sets} . In other words, an invariant is a collection of maps of sets

$$\mathcal{F}(K) \rightarrow H^d(K, M) := H^d(\Gamma_K, M)$$

for all field extensions K/F , natural in K .

An invariant u is called *nontrivial* if there is a field extension K/F containing an algebraic closure of F and an element $x \in \mathcal{F}(K)$ such that $u_K(x) \neq 0$ in $H^d(K, M)$.

A theorem of J.-P. Serre on vanishing of degree d Galois cohomology group of a field extension of an algebraically closed field of transcendence degree less than d yields the following statement that provides a lower bound for the essential p -dimension of a functor.

Theorem 5.3 ([32], Theorem 3.4). *Let $\mathcal{F} : \mathbf{Fields}_F \rightarrow \mathbf{Sets}$ be a functor, M a torsion p -primary Galois module over F , where p a prime integer. If \mathcal{F} admits a nontrivial degree d cohomological invariant with values in M , then $\mathrm{ed}(\mathcal{F}) \geq \mathrm{ed}_p(\mathcal{F}) \geq d$.*

In the following two examples the upper and lower bounds for the essential dimension match.

Example 5.4. Denote by μ_n the group of n th roots of unity over a field F such that n is not divisible by $\mathrm{char}(F)$. For a field extension K/F , we have the *Kummer isomorphism*

$$K^\times / K^{\times n} \xrightarrow{\sim} H^1(K, \mu_n), \quad aK^n \mapsto (a).$$

It follows that

$$(\mu_n)^s\text{-PHS}(K) = (K^\times / K^{\times n})^s.$$

Therefore, $(\mathbb{A}_F^1 \setminus \{0\})^s$ is a classifying variety for $(\mu_n)^s$. It follows that $\mathrm{ed}(\mu_n)^s \leq s$ by Corollary 3.13. On the other hand, if p is a prime divisor of n , then the cohomological degree s invariant

$$(a_1, a_2, \dots, a_s) \mapsto (a_1) \cup (a_2) \cup \dots \cup (a_s) \in H^s(K, \mu_p^{\otimes s})$$

is not trivial [5, Corollary 4.9], hence $\mathrm{ed}_p(\mathrm{B}\mu_n^s) = \mathrm{ed}(\mathrm{B}\mu_n^s) = s$ by Theorem 5.3.

Example 5.5. Let \mathbf{O}_n be the orthogonal group of a non-degenerate quadratic form of dimension n over a field F with $\text{char}(F) \neq 2$. By Example 2.3.3, the set $\mathbf{O}_n\text{-PHS}(K)$ is in bijection with the set of isomorphism classes of non-degenerate quadratic forms of dimension n for a field extension K/F . Every such form q is diagonalizable, i.e. $q \simeq \langle a_1, a_2, \dots, a_n \rangle$ with $a_i \in K^\times$. It follows that $(\mathbb{A}_F^1 \setminus \{0\})^n$ is a classifying variety for \mathbf{O}_n , hence $\text{ed}(\mathbf{BO}_n) \leq n$ by Corollary 3.13. On the other hand, the cohomological degree n invariant (the n th Stiefel-Whitney class)

$$\langle a_1, a_2, \dots, a_n \rangle \mapsto (a_1) \cup (a_2) \cup \dots \cup (a_n) \in H^n(K, \mathbb{Z}/2\mathbb{Z})$$

is well defined and nontrivial [14, §17], hence $\text{ed}_2(\mathbf{BO}_n) = \text{ed}(\mathbf{BO}_n) = n$ by Theorem 5.3.

Let H be a subgroup of an algebraic group G . Then every generically free G -representation is also a generically free H -representation. This yields the following statement which can be viewed as a lower bound for $\text{ed}(BG)$ and an upper bound for $\text{ed}(BH)$.

Proposition 5.6 ([6], Lemma 2.2). *Let H be a subgroup of an algebraic group G . Then*

$$\text{ed}(BG) + \dim(G) \geq \text{ed}(BH) + \dim(H).$$

In particular, if G is a finite group, then $\text{ed}(BG) \geq \text{ed}(BH)$.

6. ESSENTIAL DIMENSION OF FINITE GROUPS

By Example 2.2, to give a principal homogeneous G -space for a finite group G is the same as to give a Galois G -algebra. Thus, the essential dimension of G measures the complexity of the class of Galois extensions with Galois group G .

By Proposition 5.1, $\text{ed}(G) \leq \min \dim(V)$ over all faithful (= generically free) representation of G . When does the equality hold?

Example 6.1. We will see in Section 8 that the essential dimension of the symmetric group S_3 is equal to 1, but S_3 has no 1-dimensional faithful representation, hence the equality does not hold.

Example 6.2. Let G be a cyclic group of order 3. Since $G \subset S_3$, we have $\text{ed}(G) \leq \text{ed}(S_3) = 1$ by Proposition 5.6. But G has no 1-dimensional faithful representation over \mathbb{Q} since there are no primitive cubic roots of unity in \mathbb{Q} .

It turns out that if G is a p -group and the base field has p th roots of unity, then equality holds. Equivalently, if V is a faithful representation of G of the smallest dimension, then V is G -incompressible as a variety.

Theorem 6.3 ([23], Theorem 4.1). *Let p be a prime integer, G be a p -group and F a field of characteristic different from p containing a primitive p th root of unity. Then*

$$\text{ed}_p(BG) = \text{ed}(BG) = \min \dim(V),$$

where the minimum is taken over all faithful representations V of G over F .

The proof of this theorem involves a lot of the machinery discussed in this paper, in particular, categories fibered in groupoids (gerbes), canonical dimension, algebraic cycles, algebraic K -theory, representation theory. The main steps of the proof are the following:

1. It suffices to construct a faithful representation V of G such that $\text{ed}_p(\text{BG}) \geq \dim(V)$. Let C be the p -socle of G , i.e., the subgroup of all central elements of exponent p . By the assumption on the roots of unity, C is isomorphic to $(\mu_p)^s$ for some s . Set $H := G/C$.

2. Choose a principle homogeneous H -space E over a field extension L of F . Then the category E/G is a gerbe banded by C (see Example 3.8). An object of this category is a lift of E to a principal homogeneous G -space. One readily deduces the inequality $\text{ed}_p(\text{BG}) \geq \text{ed}_p(E/G)$.

3. There is a simple formula relating the essential and canonical p -dimensions of the gerbe E/G , so we can switch to the canonical p -dimension of E/G . This integer is easier to calculate since it depends only on the class \mathcal{C} of field extensions K/L such that the fiber of E/G over K has an object, i.e., E has a lift to a principal homogeneous G -space over K . We have $\text{cdim}_p(E/G) = \text{cdim}_p(\mathcal{C})$.

4. The gerbe E/G is determined by a class α in $H^2(C) = H^2(L, \mu_p)^s$ (see Example 3.8). The group $H^2(L, \mu_p)$ is identified with the subgroup $\text{Br}(L)$ of classes of exponent dividing p in the Brauer group $\text{Br}(L)$ of L . Therefore, the element α determines a finite p -elementary subgroup $B \subset \text{Br}(L)$ generated by the images of α under the homomorphisms $H^2(L, C) \rightarrow H^2(L, \mathbf{G}_m) = \text{Br}(L)$ over all characters $C \rightarrow \mathbf{G}_m$ over L . Therefore, a field K/L belongs to the class \mathcal{C} if and only if B is split over K .

5. If we choose the principal homogeneous H -space in the step 2 to be trivial, then D is split and we get $\text{cdim}_p(\mathcal{C}) = 0$. Since we are proving the lower bound for $\text{ed}(G)$, we need to pursue the opposite strategy and start with the “most generic” E hoping to get largest possible dimensions of the algebras A_i . Each algebra A_i arises from a character $\chi_i : C \rightarrow \mathbf{G}_m$. An application of the equivariant K -theory shows that for every i , the maximal value of the index of A_i over all L and E is attained for the same choice of generic L and E . This maximal value is determined by the representation theory of G . That is, $\max \text{ind}(A_i)$ is the smallest dimension of a representation V_i of G such that the restriction to C is given by multiplication by the character χ_i .

6. Choose generic L and E . Now we are in the setup of Example 4.5. Choose central division algebras A_1, A_2, \dots, A_r such that the classes $[A_i]$ form a basis of B and the sum $\sum_i \text{deg}(A_i)$ is the smallest possible over all choices of a basis $[A_1], [A_2], \dots, [A_n]$ for B . Then the product $X = X_1 \times X_2 \times \dots \times X_r$ is p -incompressible and $\text{cdim}_p(\mathcal{C}) = \dim(X) = \min \sum_i (\text{deg}(A_i) - 1)$.

7. We end up in the following problem: choose a basis (χ_i) of the character group of C and representations V_i of G as above with the smallest $\sum \dim(V_i)$. Then the direct sum V of all the V_i satisfies $\text{ed}_p(\text{BG}) \geq \dim(V)$, and, by construction, the restriction of V to the p -socle C is faithful. Elementary group theory shows that the G -representation V is faithful. Thus, we have found a faithful representation V of G of the smallest dimension and $\text{ed}(\text{BG}) = \text{ed}_p(\text{BG}) = \dim(V)$.

Remark 6.4. In the proof, we don’t show directly that a faithful representation of the smallest dimension is G -incompressible. Instead, we construct a representation V such that $\text{ed}_p(\text{BG}) \geq \dim(V)$. It follows that V is a faithful representation of the smallest dimension.

The proof of Theorem 6.3 (see also Example 4.5) shows how to find a faithful representation of G of the smallest dimension and compute the essential dimension of G over F . For every character $\chi \in C^* := \text{Hom}(C, \mathbf{G}_m)$, choose a nonzero representation V_χ of the smallest dimension such that the restriction to the p -socle C is multiplication by the character χ . It appears as an irreducible component of the smallest dimension of the induced representation $\text{Ind}_C^G(\chi)$. We construct a basis χ_1, \dots, χ_s of C^* by induction as follows. Let χ_1 be a nonzero character with the smallest $\dim(V_{\chi_1})$. If the characters $\chi_1, \dots, \chi_{i-1}$ are already constructed for some i , then we take χ_i to be a character with minimal $\dim(V_{\chi_i})$ among all characters outside of the subgroup generated by $\chi_1, \dots, \chi_{i-1}$. Then V is a faithful representation of the smallest dimension and $\text{ed}(BG) = \sum_{i=1}^s \dim(V_{\chi_i})$.

As an example, the following corollary computes the essential dimension of a finite abelian p -group.

Corollary 6.5 ([23], Corollary 5.2). *Let F be a field as in Theorem 6.3 and G a finite abelian group that is a direct sum of cyclic groups with orders $p^{n_1}, p^{n_2}, \dots, p^{n_s}$. Then*

$$\text{ed}(BG) = \sum_{i=1}^s [F(\xi_{p^{n_i}}) : F],$$

where ξ_{p^m} is a primitive p^m th root of unity.

For cyclic groups Corollary 6.5 was proved earlier by M. Florence in [12].

7. ESSENTIAL DIMENSION OF GROUPS OF MULTIPLICATIVE TYPE

The essential dimension of groups of multiplicative type was considered in [27].

An algebraic group G over F is said to be of *multiplicative type* if over a separable closure F_{sep} of F , G_{sep} is a subgroup of the group of diagonal matrices. If G is a group of multiplicative type, the assignment

$$G \mapsto G_{\text{sep}}^* := \text{Hom}_{F_{\text{sep}}}(G_{\text{sep}}, \mathbf{G}_m)$$

yields an anti-equivalence between the category of groups of multiplicative type and the category of finitely generated Γ_F -modules, where $\Gamma_F = \text{Gal}(F_{\text{sep}}/F)$ (see [24, 20.17]).

Example 7.1. An *algebraic torus* is a group G of multiplicative type such that the character group G_{sep}^* is a free abelian group of finite rank.

Let A be an étale F -algebra and T^A be the torus of invertible elements in A . Then the character Γ_F -module of T_{sep}^A is a *permutation module*, i.e., it has a Γ_F -invariant \mathbb{Z} -basis. Conversely, every permutation module is the character Γ_F -module of a torus T^A for an étale F -algebra A . The torus T^A acts linearly on the affine space of A and T^A is equal to the open orbit of 1.

Let G be a group of multiplicative type. A *presentation* of G is a surjective Γ_F -homomorphism $f : P \rightarrow G_{\text{sep}}^*$ with P a permutation Γ_F -module. Such a presentation of G identifies G with a subgroup of T^A with the character module P for an étale F -algebra A . Therefore, the affine space of A is a generically free representation of G . By Proposition 5.1,

$$\text{ed}(BG) \leq \dim(A) - \dim(G) = \text{rank}(\text{Ker}(f)).$$

Does the equality hold for a presentation f of G with the smallest $\text{rank}(P)$? In general, the answer is not known. But, as in the case of finite p -groups, the p -variant of the question has a positive answer.

A representations V of G over F is called p -faithful if the kernel of V is a finite group of order prime to p . The image of the natural homomorphism $\Gamma_F \rightarrow \text{Aut}(G_{\text{sep}}^*)$ is called the *splitting group* of G .

Theorem 7.2. [27, Theorem 1.1] *Let F be a field and p an integer different from $\text{char}(F)$. Let G be a group of multiplicative type over F such that the splitting group of G and the factor group G/T by the maximal sub-torus T in G are p -groups. Then*

$$\text{ed}_p(G) = \text{ed}(G) = \min \dim(V),$$

where the minimum is taken over all p -faithful representations V of G over F .

The proof of this theorem is parallel to the one of Theorem 6.3. One considers restrictions of representations to the p -socle of G , the maximal subgroup of G isomorphic to $(\mu_p)^s$ for some s .

Theorem 7.2 can be restated in terms of Γ_F -modules. A homomorphism of Γ_F -modules $P \rightarrow G_{\text{sep}}^*$ with P a permutation Γ_F -module and the finite cokernel of order prime to p is called a p -presentation of G_{sep}^* .

Corollary 7.3. [27, Corollary 5.1] *In the conditions of Theorem 7.2, let $f : P \rightarrow G_{\text{sep}}^*$ be a p -presentation with the smallest $\text{rank}(P)$. Then $\text{ed}_p(G) = \text{ed}(G) = \text{rank}(\text{Ker}(f))$.*

Example 7.4. Let p be a prime integer and L/F be a Galois field extension with Galois p -elementary group Γ of order p^r for some $r > 0$. Fix a basis $\gamma_1, \dots, \gamma_r$ of Γ as a $\mathbb{Z}/p\mathbb{Z}$ -space. Consider the torus T over F given by

$$T(K) = (L \otimes_F K)^\times / K^\times$$

for a field extension K/F . Hilbert's Theorem 90 yields an isomorphism

$$T\text{-PHS}(K) \simeq \text{Br}(L \otimes_F K/K) := \text{Ker}(\text{Br}(K) \rightarrow \text{Br}(L \otimes_F K)).$$

The character Galois module of T is the *augmentation ideal* I in the group ring $\mathbb{Z}[\Gamma]$, i.e., $I = \text{Ker}(\mathbb{Z}[\Gamma] \xrightarrow{\varepsilon} \mathbb{Z})$, where $\varepsilon(\gamma) = 1$ for every $\gamma \in \Gamma$. The surjective homomorphism $f : \mathbb{Z}[\Gamma]^r \rightarrow I$, taking an r -tuple (x_i) to $\sum_r x_i(\gamma_i - 1)$, is a presentation of $I = G_{\text{sep}}^*$. By [31, Example 4.5], f is also a p -presentation of the smallest rank. It follows that

$$\text{ed}(BT) = \text{ed}_p(BT) = \text{rank}(\mathbb{Z}[\Gamma]^r) - \dim(T) = (r-1)p^r + 1.$$

8. ESSENTIAL DIMENSION OF SYMMETRIC GROUPS

In this section, F is a field of characteristic zero.

The essential dimension of the symmetric group S_n for $n \leq 6$ was computed in [7, Theorem 6.5]. By Example 2.3.2, to give a principal homogeneous S_n -space over a field extension K/F is to give a degree n étale K -algebra. Every such an algebra A is generated by one element a , and the choice of a generator yields an algebra isomorphism $A \simeq K[X]/(f_a)$, where $f_a \in K[X]$ is a monic separable polynomial. The algebra A is defined over a subfield $K' \subset K$ if and only if the generator a can be chosen so that $f_a \in K'[X]$. Thus, the essential dimension of A is the smallest transcendence degree of the field generated by the coefficients of f_a over all generators a of A .

Remark 8.1. The problem of simplifying polynomials of degree n in one variable may be viewed as an algebraic variant of Hilbert's 13th problem.

Define a *generic* degree n étale algebra A_{gen} as the factor algebra $K[X]/(f)$, where $K = F(T_1, T_2, \dots, T_n)$ is the rational function field in n variables and $f = X^n + T_1 X^{n-1} + \dots + T_{n-1} X + T_n$ is the “generic polynomial” over K . The algebra A_{gen} corresponds to the generic principal homogeneous S_n -space given by standard n -dimensional permutation representation of S_n (see Step 2 in Section 2). Therefore, the essential dimension of S_n coincides with $\text{ed}(A_{\text{gen}})$.

Upper bounds for the essential dimension of S_n can be obtained as follows. If $f_a = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n$ for a generator a of an étale algebra A of degree n , replacing a by $a + a_1/n$ eliminates the term a_1 , hence $\text{ed}(\text{BS}_n) \leq n - 1$ if $n \geq 2$. Scaling a , we can get the equality $a_{n-1} = a_n$. Therefore $\text{ed}(\text{BS}_n) \leq n - 2$ if $n \geq 3$.

The permutation S_n -action on the product X of n copies of the projective line \mathbb{P}_F^1 commutes element-wise with the diagonal action of the automorphism group $H := \mathbf{PGL}_2$ of \mathbb{P}_F^1 . The variety X is birationally S_n -isomorphic to the affine space \mathbb{A}_F^n with the standard linear action of S_n . By Proposition 2.7, the S_n -variety X is versal. If $n \geq 5$, the induced action of S_n on X/H is faithful, hence

$$\text{ed}(\text{BS}_n) \leq \dim(X/H) = \dim(X) - \dim(H) = n - 3$$

for $n \geq 5$.

The lower bound $\text{ed}(\text{BS}_n) \geq \left\lfloor \frac{n}{2} \right\rfloor$ follows from Proposition 5.6 applied to a maximal 2-elementary subgroup $(\mathbb{Z}/2\mathbb{Z})^k \subset S_n$, where $k = \left\lfloor \frac{n}{2} \right\rfloor$, see Example 5.4. Equivalently, one can see that the k th Stiefel-Whitney class of the trace form of an étale dimension n algebra yields a non-trivial degree k cohomological invariant of S_n .

Note that the upper and lower bound match for $n \leq 6$ and yield an inequality $3 \leq \text{ed}(\text{BS}_7) \leq 4$.

The lower bound $\text{ed}(\text{BS}_7) \geq 4$ was proved by A. Duncan in [11] using the classification of rationally connected 3-folds with a faithful A_7 -action given in [36, Theorem 1.5].

We put all the facts together in the following theorem. The values of $\text{ed}(\text{BS}_n)$ for $n \geq 8$ are not known.

Theorem 8.2. *All known values of the essential dimension of S_n are collected in the following table:*

n	1	2	3	4	5	6	7
$\text{ed}(\text{BS}_n)$	0	1	1	2	2	3	4

Moreover, we have the following inequalities (for $n \geq 7$):

$$n - 3 \geq \text{ed}(\text{BS}_n) \geq \left\lfloor \frac{n+1}{2} \right\rfloor.$$

The values of the essential p -dimension for $p > 0$ were computed in [33, Corollary 4.2]:

$$\text{ed}_p(\text{BS}_n) = \left\lfloor \frac{n}{p} \right\rfloor.$$

9. ESSENTIAL DIMENSION OF SPINOR GROUPS

Let F be a field of characteristic different from 2. Let $\mathcal{Q}_n(F)$ be the set of isomorphism classes of non-degenerate quadratic forms of dimension n over F . By Example 2.3.3, $\mathcal{Q}_n(F) \simeq \mathbf{O}(q_n)\text{-PHS}(F)$ for a non-degenerate quadratic form q_n over F . Every form in $\mathcal{Q}_n(F)$ is isomorphic to the *diagonal* quadratic form $\langle a_1, a_2, \dots, a_n \rangle$ with $a_i \in F^\times$, i.e., every quadratic form in $\mathcal{Q}_n(F)$ up to isomorphism can be given by n parameters. Moreover, by Example 5.5, $\text{ed}(\mathcal{Q}_n) = \text{ed}(\mathbf{BO}(q_n)) = n$.

If n is even, the *discriminant* of the quadratic form $\langle a_1, a_2, \dots, a_n \rangle$ is equal to the class of $(-1)^{n/2}a_1a_2 \dots a_n$ in $F^\times/F^{\times 2}$. Write $\mathcal{Q}_n^1(F) = \mathcal{Q}_n(F)$ (only for even n) and $\mathcal{Q}_n^2(F)$ for the subset in $\mathcal{Q}_n^1(F)$ of all forms with trivial discriminant. Clearly, every form in $\mathcal{Q}_n^2(F)$ can be given by $n - 1$ parameters. Moreover, $\text{ed}(\mathcal{Q}_n^2) = \text{ed}(\mathbf{BO}^+(q_n)) = n - 1$ for $n \geq 3$, where $\mathbf{O}^+(q_n)$ is the *special* orthogonal group, the connected component of the identity in $\mathbf{O}(q_n)$.

The *Clifford algebra* $\text{Cl}(q)$ of a quadratic form q in $\mathcal{Q}_n^1(F)$ is a central simple algebra of degree 2^n over F . The *Clifford invariant* of q is the class of $\text{Cl}(q)$ in the Brauer group $\text{Br}(F)$. Let $\mathcal{Q}_n^3(F)$ be the subset of $\mathcal{Q}_n^2(F)$ of all forms with trivial Clifford invariant. Thus, $\mathcal{Q}_n^3(F)$ is the set of isomorphism classes of non-degenerate quadratic forms of even dimension n over F with trivial discriminant and trivial Clifford invariant.

For an even n write \mathbf{Spin}_n for the *spinor group* of a (unique up to isomorphism) hyperbolic quadratic form of dimension n over F . The spinor group is the kernel of the *spinor norm homomorphism* from the *even Clifford group* \mathbf{Clif}_n^+ to \mathbf{G}_m . It turns out that there is a bijection $\mathcal{Q}_n^3(F) \simeq \mathbf{Clif}_n^+\text{-PHS}(F)$.

The exact sequence

$$1 \rightarrow \mathbf{Spin}_n \rightarrow \mathbf{Clif}_n^+ \rightarrow \mathbf{G}_m \rightarrow 1$$

yield a surjection

$$\mathbf{Spin}_n\text{-PHS}(K) \rightarrow \mathcal{Q}_n^3(K)$$

for every field extension K/F with a transitive action of K^\times on all the fibers of the surjection. It follows that the integers $\text{ed}(\mathbf{BSpin}_n)$ and $\text{ed}(\mathcal{Q}_n^3)$ differ by at most 1. That is,

$$\text{ed}(\mathbf{BSpin}_n) + 1 \geq \text{ed}(\mathcal{Q}_n^3) \geq \text{ed}(\mathbf{BSpin}_n).$$

There is a classification of quadratic forms in $\mathcal{Q}_n^3(F)$ for even $n \leq 14$:

1. Every form in $\mathcal{Q}_n^3(K)$ is hyperbolic for $n \leq 6$, hence $\text{ed}(\mathcal{Q}_n^3) = 0$ for such n .
2. The forms q in $\mathcal{Q}_8^3(K)$ are multiples of *3-fold Pfister forms*

$$\langle\langle a, b, c \rangle\rangle := \langle 1, -a \rangle \otimes \langle 1, -b \rangle \otimes \langle 1, -c \rangle,$$

i.e., $q = d\langle\langle a, b, c \rangle\rangle$ is given by 4 parameters. On the other hand, the degree 4 cohomological invariant $(a) \cup (b) \cup (c) \cup (d) \in H^4(K, \mathbb{Z}/2\mathbb{Z})$ is well defined and non-trivial. It follows that $\text{ed}(\mathcal{Q}_8^3) = 4$.

3. Every form in $\mathcal{Q}_{10}^3(K)$ is isomorphic to $q \perp \mathbb{H}$, where \mathbb{H} is a hyperbolic plane and $q \in \mathcal{Q}_8^3(K)$. Hence $\text{ed}(\mathcal{Q}_{10}^3) = 4$.

4. By a theorem of A. Pfister, every form in $\mathcal{Q}_{12}^3(K)$ is isomorphic to

$$\langle a, b \rangle \otimes \langle c, d, -cd, -e, -f, ef \rangle$$

for arbitrary 6 values of the parameters in K . Observing that the obvious degree 6 cohomological invariant $(a) \cup (b) \cup (c) \cup (d) \cup (e) \cup (f) \in H^6(K, \mathbb{Z}/2\mathbb{Z})$ is well defined and non-trivial, we deduce that $\text{ed}(\mathbf{Q}_{12}^3) = 6$.

5. By a theorem of M. Rost, every form in $\mathbf{Q}_{14}^3(K)$ is isomorphic to the transfer from a quadratic extension L/K of a 7-dimensional form q such that $q \perp \langle 1 \rangle$ is a 3-fold Pfister form over L . The quadratic extension L/F is given by one parameter and the 3-fold Pfister form over L is given by $3 \cdot 2 = 6$ parameters over K . There is a nontrivial invariant of degree 7 of \mathbf{Q}_{14}^3 (see [40]). Counting the parameters, we get $\text{ed}(\mathbf{Q}_{14}^3) = 7$.

Note that for all even $n \leq 14$, the forms in \mathbf{Q}_n^3 can be parameterized by algebraically independent parameters. Equivalently, the classifying spaces \mathbf{BSpin}_n and \mathbf{BClif}_n^+ are retract rational for $n \leq 14$.

The essential dimension of the spinor groups \mathbf{Spin}_n for $n \leq 14$ was computed by S. Garibaldi in [15].

A classification of forms in \mathbf{Q}_n^3 for $n > 14$ is not known (and cannot be simple if there is one, see Remark 9.2). It is amazing that nevertheless, one can compute the essential dimension of \mathbf{Spin}_n and it is exponential in n . P. Brosnan, Z. Reichstein, and A. Vistoli computed $\text{ed}(\mathbf{BSpin}_n)$ in the case $n \geq 15$ and n is not divisible by 4. In these cases, an upper and a lower bounds match!

For example, consider the case $n > 14$ and $n \equiv 2$ modulo 4. The Clifford algebra of a hyperbolic form q_n of dimension n is $\mathbb{Z}/2\mathbb{Z}$ -graded. Its even component $C_0(q_n)$ (the *even Clifford algebra*) is a product of two matrix algebras $M_k(F) \times M_k(F)$, where $k = 2^{(n-2)/2}$. The inclusion of the spinor group into the group of invertible elements in the even Clifford algebra $C_0(q_n)$ gives then two *half-spin* representations V^\pm of \mathbf{Spin}_n of dimension $2^{(n-2)/2}$ each. Since $n > 14$, both representations V^\pm are generically free (see [35] in the case $\text{char}(F) = 0$ and [16] in general). Then by Proposition 5.1,

$$\text{ed}(\mathbf{BSpin}_n) \leq \dim(V^\pm) - \dim(\mathbf{Spin}_n) = 2^{(n-2)/2} - \frac{n(n-1)}{2}.$$

To get a lower bound one finds a finite 2-subgroup $H \subset \mathbf{Spin}_n$ such that the restriction of a half-spin representation of \mathbf{Spin}_n to H is a faithful representation of H of the smallest dimension. By Proposition 5.6 and Theorem 6.3,

$$\text{ed}(\mathbf{BSpin}_n) \geq \text{ed}(BH) - \dim(\mathbf{Spin}_n) = \dim(V^\pm) - \dim(\mathbf{Spin}_n) = 2^{(n-2)/2} - \frac{n(n-1)}{2}.$$

The case $n \geq 15$ and n is not divisible by 4 required additional considerations and it was completed in [29] and [8].

Theorem 9.1. *Let F be a field of characteristic not 2. Then, for every integer $n \geq 15$ we have:*

$$\text{ed}_2(\mathbf{BSpin}_n) = \text{ed}(\mathbf{BSpin}_n) = \begin{cases} 2^{(n-1)/2} - \frac{n(n-1)}{2}, & \text{if } n \text{ is odd;} \\ 2^{(n-2)/2} - \frac{n(n-1)}{2}, & \text{if } n \equiv 2 \pmod{4}; \\ 2^{(n-2)/2} + 2^m - \frac{n(n-1)}{2}, & \text{if } n \equiv 0 \pmod{4}, \end{cases}$$

where 2^m is the largest power of 2 dividing n .

Below is the table of values of $\text{ed}(\mathbf{BSpin}_n)$ for small n :

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\text{ed}(\mathbf{BSpin}_n)$	0	0	0	0	4	5	5	4	5	6	6	7	23	24	120	103	341

The essential dimension of \mathbf{Q}_n^3 was computed in [8] (if $\text{char}(F) = 0$). For even $n \geq 16$, we have $\text{ed}(\mathbf{Q}_n^3) = \text{ed}(\mathbf{Spin}_n)$ is $n \equiv 2$ modulo 4 and $\text{ed}(\mathbf{Q}_n^3) = \text{ed}(\mathbf{Spin}_n) - 1$ if n is divisible by 4.

Below is the table of values of $\text{ed}(\mathbf{Q}_n^3)$ for small even n :

n	4	6	8	10	12	14	16	18	20	22
$\text{ed}(\mathbf{Q}_n^3)$	0	0	4	4	6	7	23	103	326	793

The integers $\text{ed}(\mathbf{Spin}_n)$ and $\text{ed}(\mathbf{Q}_n^3)$ grow exponentially when n goes to infinity. This behavior is not predicted by the tables for small values of n .

Remark 9.2. We have $\text{ed}(\mathbf{Q}_{14}^3) = 7$, $\text{ed}(\mathbf{Q}_{16}^3) = 23$, $\text{ed}(\mathbf{Q}_{18}^3) = 103$. A jump of the value of $\text{ed}(\mathbf{Q}_n^3)$ when $n > 14$ is probably related to the fact that there is no simple classification of quadratic forms with trivial discriminant and Clifford invariant of dimension greater than 14. Another possible reason is that the forms in \mathbf{Q}_n^3 for $n > 14$ cannot be parameterized by algebraically independent parameters, or, equivalently, that the classifying space of \mathbf{Spin}_n and \mathbf{Clif}_n^+ are (conjecturally) not retract rational.

9a. Pfister numbers. Consider the following application in the algebraic theory of quadratic forms over a field F of characteristic different from 2 (see [6, §4]). Let $W(F)$ be the *Witt ring* of classes of non-degenerate quadratic forms over F and $I(F)$ to be the *fundamental ideal* in $W(F)$ of classes of even dimensional forms.

A quadratic form is called a *general m -fold Pfister form* over F if it is a multiple of an m -fold Pfister form $\langle\langle a_1, a_2, \dots, a_m \rangle\rangle$ with $a_i \in F^\times$. Every form q in the m th power $I^m(F)$ of the fundamental ideal $I(F)$ is the sum of several m -fold Pfister forms. The *m -Pfister number* of q is the smallest number of m -fold Pfister forms appearing in such sum. The *Pfister number* $\text{Pf}_m(n)$ is the supremum of the m -Pfister number of q , taken over all field extensions K/F and all n -dimensional forms $q \in I^m(K)$.

One can check that $\text{Pf}_1(n) = \frac{n}{2}$ and $\text{Pf}_2(n) = \frac{n}{2} - 1$, i.e., these values of the Pfister numbers are linear in n . The exponential lower bound for the essential dimension of spinor groups implies that the value $\text{Pf}_3(n)$ is at least exponential in n . It is not known whether $\text{Pf}_m(n)$ is finite for $m \geq 4$.

10. ESSENTIAL DIMENSION OF SIMPLE ALGEBRAS

Let \mathbf{CSA}_n be the functor taking a field extension K/F to the set of isomorphism classes $\mathbf{CSA}_n(K)$ of central simple K -algebras of degree $n > 1$. By Example 2.3.1, the functors \mathbf{CSA}_n and \mathbf{PGL}_n -*PHS* are isomorphic. In particular, $\text{ed}(\mathbf{CSA}_n) = \text{ed}(\mathbf{BPGl}_n)$.

The tautological degree 2 cohomological invariant with values in the Brauer group yields a lower bound $\text{ed}(\mathbf{CSA}_n) \geq 2$.

By Example 5.2, since G is an adjoint group,

$$\text{ed}(\mathbf{CSA}_n) \leq \dim(G) = n^2 - 1.$$

This upper bound was improved in [25, Proposition 1.6] and [26, Theorem 1.1]:

$$\mathrm{ed}(\mathrm{CSA}_n) \leq \begin{cases} n^2 - 3n + 1, & \text{if } n \geq 4; \\ \frac{(n-1)(n-2)}{2}, & \text{if } n \geq 5 \text{ is odd.} \end{cases}$$

Let L/F be a cyclic field extension of degree n , σ be a generator of the Galois group of L/F . Consider the *twisted polynomial ring* $L_\sigma[X]$ in which $tx = \sigma(x)t$ for all $x \in L$. For every $a \in F^\times$, the factor algebra $L_\sigma[X]/(t^n - a)$ is a central simple F -algebra of degree n called a *cyclic algebra* and it is denoted by $(L/F, \sigma, a)$.

If F contains a primitive root ξ of degree n , then $L = F(b^{1/n})$ for some $b \in F^\times$ and we write $(a, b)_n$ for $(L/F, \sigma, a)$. For example, $(a, b)_2$ is a quaternion algebra. The cyclic algebra $(a, b)_n$ is given by two parameters. Therefore, $\mathrm{ed}(a, b)_n \leq 2$.

Example 10.1. 1. $n = 2$. Every algebra in CSA_2 is cyclic (*quaternion algebra*). The lower and upper bounds match, hence $\mathrm{ed}(\mathrm{CSA}_2) = 2$.

2. $n = 3$. Every central simple algebra is also cyclic. Since a cyclic group C_3 of order 3 is a subgroup of the symmetric group S_3 , we have $\mathrm{ed}(C_3) \leq \mathrm{ed}(S_3) = 1$ and hence $\mathrm{ed}(\mathrm{CSA}_3) = 2$.

3. $n = 4$. M. Rost proved that $\mathrm{ed}(\mathrm{CSA}_4) = 5$.

The value of $\mathrm{ed}(\mathrm{CSA}_5)$ is not known. It is still an open question whether every central simple algebra of prime degree $p \geq 5$ is cyclic even if F contains a primitive p th roots of unity. A positive answer to this question would imply that $\mathrm{ed}(\mathrm{CSA}_p) = 2$ for a prime p over such fields. One could try to show that $\mathrm{ed}(\mathrm{CSA}_p) > 2$ for a prime $p \geq 5$ to answer the question in the negative.

On the other hand, every central simple algebra of prime degree p is cyclic over a finite field extension of degree prime to p . It follows that $\mathrm{ed}_p(\mathrm{CSA}_p) = 2$ [39, Lemma 8.5.7].

Upper bounds for $\mathrm{ed}_p(\mathrm{CSA}_{p^r})$ with $r \geq 2$ were obtained in [33], [34] and then improved in [41].

Theorem 10.2 ([41], Theorem 1.2). *For every prime p and $r \geq 2$, we have*

$$\mathrm{ed}_p(\mathrm{CSA}_{p^r}) \leq p^{2r-2} + 1.$$

In order to get a lower bound for $\mathrm{ed}_p(\mathrm{CSA}_{p^r})$, one can use the valuation method. We “degenerate” the group \mathbf{PGL}_{p^r} to a torus as follows.

Let F be a field and p a prime integer different from $\mathrm{char}(F)$. Over a field extension L/F containing a primitive p th root of unity, let $L' = L(a_1^{1/p}, a_2^{1/p}, \dots, a_r^{1/p})$ for some $a_i \in L^\times$ and choose a central simple L -algebra A of degree p^r that is split by L' . Over the rational function field $L(t) := L(t_1, t_2, \dots, t_r)$, the algebra

$$B := A_{L(t)} \otimes (a_1, t_1)_p \otimes (a_2, t_2)_p \otimes \cdots \otimes (a_r, t_r)_p,$$

is split by $L'(t)$, hence there is a central simple algebra D of degree p^r over $L(t)$ Brauer equivalent to B .

Consider the functor $\mathcal{F} : \mathbf{Fields}_L \rightarrow \mathbf{Sets}$ that takes a field extension K/L to the factor group of the relative Brauer group $\mathrm{Br}(L' \otimes_L K/K)$ modulo the subgroup of decomposable elements of the form $(a_1, b_1)_p \otimes \cdots \otimes (a_r, b_r)_p$ with $b_i \in K^\times$. We can view the algebra A as an element of $\mathcal{F}(L)$, denoted \tilde{A} . Using the theory of simple algebras over complete discrete valued fields, one obtains the key inequality

$$\mathrm{ed}_p(\mathrm{CSA}_{p^r}) \geq \mathrm{ed}_p(D) \geq \mathrm{ed}_p(\tilde{A}) + r.$$

Note that the values of \mathcal{F} are abelian groups. Moreover, there is a torus S over L such that $\mathcal{F} \simeq S$ -PHS. For a generic choice of A , one has $\text{ed}_p(\tilde{A}) = \text{ed}_p(S)$. The value of $\text{ed}_p(S)$ can be computed using Theorem 7.2 or Corollary 7.3.

Theorem 10.3 ([31], Theorem 6.1). *Let F be a field and p a prime integer different from $\text{char}(F)$. Then*

$$\text{ed}_p(\text{CSA}_{p^r}) \geq (r-1)p^r + 1.$$

Remark 10.4. The torus T in Example 7.4 is a maximal torus in \mathbf{PGL}_{p^r} . The inclusion of T into \mathbf{PGL}_{p^r} yields

$$T\text{-PHS}(K) = \text{Br}(L \otimes_F K/K) \subset \text{CSA}_{p^r}(K) = \mathbf{PGL}_n\text{-PHS}(K)$$

for every extension K/F , i.e., T -PHS is a sub-functor of \mathbf{PGL}_n -PHS. By Example 7.4, $\text{ed}_p(\text{BT}) = (r-1)p^r + 1$. Note that the essential dimension of a sub-functor can be larger than the essential dimension of the functor (see Remark 10.9).

Combining Theorem 10.3 with the upper bound in Theorem 10.2, we see that in certain cases the upper and lower bound match.

Corollary 10.5 ([30], Theorem 1.1). *Let F be a field and p a prime integer different from $\text{char}(F)$. Then, $\text{ed}_p(\text{CSA}_{p^2}) = p^2 + 1$.*

Recall that M. Rost proved earlier that $\text{ed}(\text{CSA}_4) = 5$.

Corollary 10.6 ([41]). *Let F be a field of characteristic different from 2. Then, $\text{ed}_2(\text{CSA}_8) = 17$.*

For every integers $n, m \geq 1$, m dividing n , and a field extension K/F , let $\text{CSA}_{n,m}(K)$ denote the set of isomorphism classes of central simple K -algebras of degree n and exponent in the Brauer group dividing m . In fact, $\text{CSA}_{n,m} \simeq G$ -PHS, where $G = \mathbf{GL}_n / \mu_m$.

Below we state upper and lower bounds for $\text{ed}_p(\text{CSA}_{p^r, p^s})$ with $s \leq r$ for a prime integer p obtained by the method of degeneration.

Theorem 10.7 ([3], Theorem 6.1). *Let F be a field and p a prime integer different from $\text{char}(F)$. Then, for any integers $r \geq 2$ and s with $1 \leq s \leq r$,*

$$p^{2r-2} + p^{r-s} \geq \text{ed}_p(\text{CSA}_{p^r, p^s}) \geq \begin{cases} (r-1)2^{r-1} & \text{if } p=2 \text{ and } s=1, \\ (r-1)p^r + p^{r-s} & \text{otherwise.} \end{cases}$$

Corollary 10.8. *Let p be an odd prime integer and F a field of characteristic different from p . Then,*

$$\text{ed}_p(\text{CSA}_{p^2, p}) = p^2 + p.$$

By a theorem of A. Albert, every central simple algebra of degree 4 and exponent 2 is the tensor product $(a_1, b_1)_2 \otimes (a_2, b_2)_2$ of two quaternion algebras. It follows that $\text{ed}(\text{CSA}_{4,2}) = \text{ed}_2(\text{CSA}_{4,2}) = 4$.

Corollary 10.8 recovers a result in [44] that for p odd, there exists a central simple algebra of degree p^2 and exponent p over a field K which is not decomposable as a tensor product of two algebras of degree p over any finite extension of K of degree prime to p . Indeed, if every central simple algebra of degree p^2 and exponent p were decomposable, then the essential p -dimension of $\text{CSA}_{p^2, p}$ would be at most 4.

Remark 10.9. Interestingly, for an odd prime p , the essential dimension $p^2 + p$ of central simple algebras of degree p^2 of exponent p is larger than the essential dimension $p^2 + 1$ of all algebras of degree p^2 .

Corollary 10.10. *Let F be a field of characteristic different from 2. Then,*

$$\mathrm{ed}_2(\mathrm{CSA}_{8,2}) = \mathrm{ed}(\mathrm{CSA}_{8,2}) = 8.$$

The corollary recovers a result in [1] that there is a central simple algebra of degree 8 and exponent 2 over a field F which is not decomposable as a tensor product of three quaternion algebras over any finite extension of F of odd degree. Indeed, if every central simple algebra of degree 8 and exponent 2 were decomposable, then the essential 2-dimension of $\mathrm{CSA}_{8,2}$ would be at most 6.

In the case $p = 2$, one can get a better upper bound.

Theorem 10.11 ([2], Theorem 1.1). *Let F be a field of characteristic different from 2. Then, for any integer $n \geq 3$,*

$$\mathrm{ed}_p(\mathrm{CSA}_{2^n,2}) \leq 2^{2n-4} + 2^{n-1}.$$

Corollary 10.12. *Let F be a field of characteristic different from 2. Then,*

$$\mathrm{ed}_2(\mathrm{CSA}_{16,2}) = 24.$$

REFERENCES

- [1] S. A. Amitsur, L. H. Rowen, and J.-P. Tignol, *Division algebras of degree 4 and 8 with involution*, Israel J. Math. **33** (1979), no. 2, 133–148.
- [2] S. Baek, *Essential dimension of simple algebras with involutions*, Bull. Lond. Math. Soc. **44** (2012), no. 3, 578–590.
- [3] S. Baek and A.S. Merkurjev, *Essential dimension of central simple algebras*, Acta Math. **209** (2012), no. 1, 1–27.
- [4] G. Berhuy and Z. Reichstein, *On the notion of canonical dimension for algebraic groups*, Adv. Math. **198** (2005), no. 1, 128–171.
- [5] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330 (electronic).
- [6] P. Brosnan, Z. Reichstein, and Angelo Vistoli, *Essential dimension, spinor groups, and quadratic forms*, Ann. of Math. (2) **171** (2010), no. 1, 533–544.
- [7] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.
- [8] V. Chernousov and A. Merkurjev, *Essential dimension of spinor and Clifford groups*, Algebra Number Theory **8** (2014), no. 2, 457–472.
- [9] J.-L. Colliot-Thélène, N. A. Karpenko, and A. S. Merkurjev, *Rational surfaces and the canonical dimension of the group PGL_6* , Algebra i Analiz **19** (2007), no. 5, 159–178.
- [10] M. Demazure and A. Grothendieck, *Schémas en groupes*, SGA 3, vol. 1, Springer-Verlag, Berlin, 1970.
- [11] A. Duncan, *Essential dimensions of A_7 and S_7* , Math. Res. Lett. **17** (2010), no. 2, 263–266.
- [12] M. Florence, *On the essential dimension of cyclic p -groups*, Invent. Math. **171** (2008), no. 1, 175–189.
- [13] W. Fulton, *Intersection theory*, Springer-Verlag, Berlin, 1984.
- [14] R. Garibaldi, A. Merkurjev, and Serre J.-P., *Cohomological invariants in galois cohomology*, American Mathematical Society, Providence, RI, 2003.
- [15] S. Garibaldi, *Cohomological invariants: exceptional groups and spin groups*, Mem. Amer. Math. Soc. **200** (2009), no. 937, xii+81, With an appendix by Detlev W. Hoffmann.
- [16] S. Garibaldi and R. Guralnick, *Spinors and essential dimension*, arXiv:1601.00590v2 [math.GR] (17 Mar 2016), 20 pages.

- [17] V. V. Ishkhanov, B. B. Lur'e, and D. K. Faddeev, *The embedding problem in Galois theory*, Translations of Mathematical Monographs, vol. 165, American Mathematical Society, Providence, RI, 1997, Translated from the 1990 Russian original by N. B. Lebedinskaya.
- [18] N.A. Karpenko, *Grothendieck Chow motives of Severi-Brauer varieties*, Algebra i Analiz **7** (1995), no. 4, 196–213.
- [19] N.A. Karpenko, *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. **15** (2000), no. 1, 1–22.
- [20] N.A. Karpenko, *Incompressibility of products of pseudo-homogeneous varieties*, Canad. Math. Bull. (published electronically on May 25, 2016).
- [21] N.A. Karpenko, *Canonical dimension*, Proceedings of the International Congress of Mathematicians. Volume II (New Delhi), Hindustan Book Agency, 2010, pp. 146–161.
- [22] N.A. Karpenko and A.S. Merkurjev, *Canonical p -dimension of algebraic groups*, Adv. Math. **205** (2006), no. 2, 410–433.
- [23] N.A. Karpenko and A.S. Merkurjev, *Essential dimension of finite p -groups*, Invent. Math. **172** (2008), no. 3, 491–508.
- [24] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits.
- [25] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379.
- [26] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.
- [27] R. Löttscher, M. MacDonald, A. Meyer, and Z. Reichstein, *Essential dimension of algebraic tori*, J. Reine Angew. Math. **677** (2013), 1–13.
- [28] R. Löttscher, *A fiber dimension theorem for essential and canonical dimension*, Compos. Math. **149** (2013), no. 1, 148–174.
- [29] A.S. Merkurjev, *Essential dimension*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 299–325.
- [30] A.S. Merkurjev, *Essential p -dimension of $\mathrm{PGL}(p^2)$* , J. Amer. Math. Soc. **23** (2010), no. 3, 693–712.
- [31] A.S. Merkurjev, *A lower bound on the essential dimension of simple algebras*, Algebra Number Theory **4** (2010), no. 8, 1055–1076.
- [32] A.S. Merkurjev, *Essential dimension: a survey*, Transform. Groups **18** (2013), no. 2, 415–481.
- [33] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory **3** (2009), no. 4, 467–487.
- [34] A. Meyer and Z. Reichstein, *An upper bound on the essential dimension of a central simple algebra*, J. Algebra **329** (2011), 213–221.
- [35] A. M. Popov, *Finite stationary subgroups in general position of simple linear Lie groups*, Trudy Moskov. Mat. Obshch. **48** (1985), 7–59, 263.
- [36] Yu Prokhorov, *Simple finite subgroups of the cremona group of rank 3*, J. Algebraic Geom. **21** (2012), 563–600.
- [37] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.
- [38] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5** (2000), no. 3, 265–304.
- [39] 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.
- [40] M. Rost, *On the galois cohomology of $\mathrm{spin}(14)$* , <https://www.math.uni-bielefeld.de/~rost/data/spin-14.pdf> (2006).
- [41] A. Ruzozzi, *Essential p -dimension of PGL_n* , J. Algebra **328** (2011), 488–494.
- [42] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, Astérisque (1995), no. 227, Exp. No. 783, 4, 229–257, Séminaire Bourbaki, Vol. 1993/94.
- [43] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.
- [44] J.-P. Tignol, *Algèbres indécomposables d'exposant premier*, Adv. in Math. **65** (1987), no. 3, 205–228.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT LOS ANGELES, LOS ANGELES,
CALIFORNIA, 90095-1555, U.S.A.

E-mail address: merkurev@math.ucla.edu