Essential Dimension of Separable Algebras Embedding in a Fixed Central Simple Algebra

To Alexander Merkurjev on His 60th Birthday

Roland Lötscher[1]

Received: March 20, 2014

Abstract. In this paper we fix a central simple F-algebra A of prime power degree and consider separable algebras over extensions K/F, which embed in A_K. We study the minimal number of independent parameters, called essential dimension, needed to define these separable algebras. In case the index of A does not exceed a certain bound, the task is equivalent to the problem of computing the essential dimension of the algebraic groups $(\mathbf{PGL}_d)^m \rtimes S_m$, which is extremely difficult in general. In the other case, however, we manage to compute the exact value of the essential dimension of the given class of separable algebras, except in one case for A of index 2, which we study in greater detail.

2010 Mathematics Subject Classification: 16W10, 16K20
Keywords and Phrases: essential dimension, central simple algebras, separable algebra, étale algebras, non-split algebraic group

1. Introduction

Central simple algebras over fields are at the core of non-commutative algebra. Their history is rooted in the middle of the 19th century, when W. Hamilton discovered the quaternions over the real numbers. In the early 20th century J. Wedderburn gave a classification of finite dimensional semisimple algebras by means of division rings and subsequently R. Brauer introduced the Brauer group of a field, which lead to diverse research in algebra and number theory. Moreover central simple algebras and the Brauer group arise naturally in Galois cohomology and are therefore central for the theory of algebraic groups over fields. We refer to [2, 1] for surveys on these topics, including discussion of open problems.

[1]Partially supported by the Deutsche Forschungsgemeinschaft, GI 706/2-1

Essential dimension is a more recent topic, introduced around 1995 by J. Buhler and Z. Reichstein [4] and in full generality by A. Merkurjev [3]. The essential dimension of a functor $\mathcal{F}\colon \text{Fields}_F \to \text{Sets}$ from the category of field extensions of a fixed base field F to the category of sets is defined as the least integer n, such that every object $a \in \mathcal{F}(K)$ over a field extension K/F is defined over a subextension K_0/F of transcendence degree at most n. Here $a \in \mathcal{F}(K)$ is said to be defined over K_0 if it lies in the image of the map $\mathcal{F}(K_0) \to \mathcal{F}(K)$ induced by the inclusion $K_0 \to K$. The functors $\mathcal{F}$ we are mostly interested in take a field extension K/F to the set of isomorphism classes of algebraic objects over K of some kind. The essential dimension of $\mathcal{F}$ is then roughly the number of independent paramters needed to define these objects.
The essential dimension of an algebraic group G over a field F is defined as the essential dimension of the Galois cohomology functor

$$H^1(-,G)\colon \text{Fields}_F \to \text{Sets}, \quad K \mapsto H^1(K,G).$$

It is denoted by $\text{ed}(G)$ and measures the complexity of G-torsors up to isomorphism, and hence of isomorphism classes of certain objects such as central simple algebras (for projective linear groups), quadratic forms (for orthogonal groups), étale algebras (for symmetric groups) etc. See [21, 17] for recent surveys on the topic.

Two of the motivating problems in essential dimension are the computation of the essential dimension of the projective linear group $\mathbf{PGL}_d$ and the symmetric group S_n, since they provide insight to the structure of central simple algebras (of degree d) and étale algebras (of dimension n), respectively. The first problem goes back to C. Procesi [19], who asked for fields of definition of the universal division algebra and discovered, in modern terms, that $\text{ed}(\mathbf{PGL}_d) \leq d^2$. This upper bound has been improved after the introduction of essential dimension, but it is still quadratic in d. See Remark 4.5 for details. A recent breakthrough has been made by A. Merkurjev [16] for a lower bound on $\text{ed}(\mathbf{PGL}_d)$. Namely, if $d = p^a$ for some prime p different from $\text{char}(F)$, he showed that $\text{ed}(\mathbf{PGL}_d) \geq (a-1)p^a+1$. In fact he established this lower bound for the essential p-dimension of $\mathbf{PGL}_d$, denoted $\text{ed}_p(\mathbf{PGL}_d)$, which measures complexity of degree d central simple algebras up to prime to p field extensions, and showed in particular that $\text{ed}_p(\mathbf{PGL}_{p^2}) = p^2 + 1$ when $\text{char}(F) \neq p$ [15]. For exponent $a \geq 3$ the problem of computing $\text{ed}_p(\mathbf{PGL}_{p^a})$ is still wide open. Moreover even the value of $\text{ed}(\mathbf{PGL}_p)$ is unknown for any prime $p \geq 5$ and related to the long-standing cyclicity-conjecture of degree p division algebras due to Albert.

The second problem is related to classical work of F. Klein, C. Hermite and F. Joubert on simplifying minimal polynomials of generators of separable field extensions (of degree $n = 5$ and 6) by means of Tschirnhaus-transformations, and was the main inspiration of [4]. In our language Hermite and Joubert showed that $\text{ed}(S_5) \leq 2$ and $\text{ed}(S_6) \leq 3$ (over a field F of characteristic zero), and Klein proved that $\text{ed}(S_5) > 1$, hence $\text{ed}(S_5) = 2$. The gap between the best lower bound (roughly $\frac{n}{2}$) and the best upper bound $n-3$ on $\text{ed}(S_n)$ for $n \geq 5$

is still quite large in general. See [7], where it is also proven that $\mathrm{ed}(S_7) = 4$ in characteristic zero.

In this paper we study *separable* algebras B. A (finite-dimensional) algebra B over a field is called separable, if it is semisimple (i.e., its Jacobson radical is trivial) and remains semisimple over every field extension. This includes both the case of central simple algebras and étale algebras. We restrict our attention to those separable K-algebras which embed in $A_K = A \otimes_F K$ for a fixed central simple F-algebra A. Here F is our base field and K/F a field extension. This originates in my earlier paper [13], which covers the case where A is a division algebra. The aim in this paper is to prove results for lower index of A.

Throughout A is a central simple algebra over a field F and $B \subseteq A$ a separable subalgebra. The type of B in A is defined as the multiset $\theta_B = [(r_1, d_1), \ldots, (r_m, d_m)]$ such that the algebra B and its centralizer $C = C_A(B)$ have the form

$$B_{\mathrm{sep}} \simeq M_{d_1}(F_{\mathrm{sep}}) \times \cdots \times M_{d_m}(F_{\mathrm{sep}}), \quad C_{\mathrm{sep}} \simeq M_{r_1}(F_{\mathrm{sep}}) \times \cdots \times M_{r_m}(F_{\mathrm{sep}})$$

over a separable closure F_{sep}. Note that central simple and étale subalgebras are those of type $\theta_B = [(d, r)]$ (with $d = \deg(B)$) and $\theta_B = [(1, r_1), \ldots, (1, r_m)]$ (with $m = \dim(B)$), respectively. We will assume throughout that the type θ_B of B is constant, i.e. $\theta_B = [(d, r), \ldots, (d, r)]$ (m-times) for some $r, d, m \geq 1$. This assumption is automatically satisfied if A is a division algebra. By [13, Lemma 4.2(a)] the product drm is the degree of A.

Denote by $\mathbf{Forms}(B)\colon \mathrm{Fields}_F \to \mathrm{Sets}$ the functor that takes a field extension K/F to the set of isomorphism classes of K-algebras B' which become isomorphic to B over a separable closure of K and by $\mathbf{Forms}_A^\theta(B)$ the subfunctor of $\mathbf{Forms}(B)$ formed by those isomorphism classes B' of forms of B which admit an embedding in A of type θ_B. We are interested in $\mathrm{ed}(\mathbf{Forms}_A^\theta(B))$. By [13, Lemma 4.6] we have a natural isomorphism

$$\mathbf{Forms}_A^\theta(B) \simeq H^1(-, G),$$

of functors $\mathrm{Fields}_F \to \mathrm{Sets}$, where G is the normalizer

$$G := N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B)).$$

Our main result is the following theorem, which shows an interesting dichotomy between the case where the index of A exceeds the bound $\frac{r}{d}$ and when it does not. The case where A is a division algebra is [13, Theorem 4.10]. As there we get examples of algebraic groups, where $\mathrm{ed}(G)$ is determined explicitly, but $\mathrm{ed}(G_{\mathrm{alg}})$ is unknown. Here we see that the mystery starts exactly once $\mathrm{ind}(A) \leq \frac{r}{d}$.

Theorem 1.1. *Let $G = N_{GL_1(A)}(\mathbf{GL}_1(B))$ with A central simple and $B \subseteq A$ a separable subalgebra of type $\theta_B = [(d, r), \ldots, (d, r)]$ (m-times). Suppose that $\deg(A) = drm$ is a power of a prime p and that $d \leq r$, so that $d|r$. Then exatly one of the following cases occurs:*

(a) $\mathrm{ind}(A) \leq \frac{r}{d}$*: Then* $\mathbf{Forms}_A^\theta(B) = \mathbf{Forms}(B)$ *and the three functors* $H^1(-,G)$*,* $\mathbf{Forms}(B)$ *and* $H^1(-,(\mathbf{PGL}_d)^m \rtimes S_m)$ *are naturally isomorphic. In particular*

$$\mathrm{ed}(G) = \mathrm{ed}(\mathbf{Forms}(B)) = \mathrm{ed}((\mathbf{PGL}_d)^m \rtimes S_m).$$

(b) $\mathrm{ind}(A) > \frac{r}{d}$*: Then*

$$\begin{aligned}\mathrm{ed}(G) = \mathrm{ed}(\mathbf{Forms}_A^\theta(B)) &= \deg(A)\,\mathrm{ind}(A) - \dim(G),\\ &= drm\,\mathrm{ind}(A) - m(r^2 + d^2 - 1).\end{aligned}$$

except possibly when $d = r > 1$ *and* $\mathrm{ind}(A) = 2$*.*

Note that the assumption $r \leq d$ is harmless. Indeed since

$$N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B)) \subseteq N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(C_A(B))) \subseteq N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(C_A(C_A(B))))$$

and $C_A(C_A(B)) = B$ by the double centralizer property of semisimple subalgebras [8, Theorem 4.10] we can always replace B by its centralizer (which amounts to switching r and d) without changing $\mathrm{ed}(G)$.

There is a big contrast between the two cases in Theorem 1.1. In case (a) the computation of $\mathrm{ed}(G) = \mathrm{ed}((\mathbf{PGL}_d)^m \rtimes S_m) = \mathrm{ed}(\mathbf{Forms}(B))$ is very hard in general. For instance when B is central simple (i.e., $m = 1$), we have $\mathrm{ed}(G) = \mathrm{ed}(\mathbf{PGL}_d)$ with $d = \deg(B)$, and in case B is étale (i.e., $d = 1$), $\mathrm{ed}(G) = \mathrm{ed}(S_m)$ where $m = \dim(B)$.
In contrast the above theorem gives the precise value of $\mathrm{ed}(G)$ in case (b) with only a small exception. The exception occurs when $d = r > 1$ and $\mathrm{ind}(A) = 2$, i.e., when $A \simeq M_{d/2}(Q)$ for a non-split quaternion F-algebra Q and B and the centralizer $C = C_A(B)$ become isomorphic to $(M_d(F_{\mathrm{sep}}))^m$ over F_{sep}. Note that we then automatically have $p = 2$, so $r = d$ and m are 2-primary. This special case will be treated separately. We will provide lower bounds and upper bounds on $\mathrm{ed}(G)$. When $m = 1$ the set $H^1(K,G)$ then classifies central simple K-algebras B' of degree d, whose tensor product with a fixed quaternion algebra over F is not division (see Example 4.1). In particular we will prove that $\mathrm{ed}(G)$ is either 2 or 3 when $r = d = 2$ and $m = 1$ (see Corollary 4.6).

The rest of the paper is structured as follows. In section 2 we study representations of $G = N_{GL_1(A)}(GL_1(B))$ with respect to generic freeness. This is used in section 3 to prove that $\mathrm{ed}(G)$ does not exceed the value suggested in Theorem 1.1(b). We will conclude the proof of the whole theorem in that section. It remains to study the case excluded from Theorem 1.1, where A has index 2 and $r = d > 1$. This is finally done in section 4.

2. Results on the Canonical Representation

The group $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$, as every subgroup of $\mathbf{GL}_1(A)$, has a canonical representation defined as follows:

Definition 2.1. Let H be a subgroup of $\mathbf{GL}_1(A)$ for a central simple algebra A. Let D be a division F-algebra representing the Brauer class of A. Fix an isomorphism $A \otimes_F D^{\mathrm{op}} \simeq \mathrm{End}(V)$ for an F-vector space V. We call the representation

$$H \hookrightarrow \mathbf{GL}_1(A) \hookrightarrow \mathbf{GL}_1(A \otimes_F D^{\mathrm{op}}) \simeq \mathbf{GL}(V)$$

the canonical representation of H, denoted $\rho^H_{\mathrm{can}} \colon H \to \mathbf{GL}(V)$.

Clearly ρ^H_{can} is faithful of dimension $\deg(A)\,\mathrm{ind}(A)$ and its equivalence class does not depend on the chosen isomorphism $A \otimes_F D^{\mathrm{op}} \simeq \mathrm{End}(V)$. Strictly speaking ρ^H_{can} depends on the embedding of H in $\mathbf{GL}_1(A)$. However it will always be clear from the context, which embedding is meant.

Recall that a representation $H \to \mathbf{GL}(W)$ of an algebraic group H over F in a F-vector space W is called *generically free*, if the affine space $\mathbb{A}(W)$ contains a non-empty H-invariant open subset U on which H acts freely, i.e., any $u \in U(F_{\mathrm{alg}})$ has trivial stabilizer in $H_{\mathrm{alg}} := H_{F_{\mathrm{alg}}}$. By stabilizer we will always mean the scheme-theoretic stabilizer (whose group of R-rational points for any commutative F_{alg}-algebra R is the subgroup of $H(R) = H_{\mathrm{alg}}(R)$ formed by those $h \in H(R)$ satisfying $hu = u$). Generic freeness of W can be tested over a separable or algebraic closure. In fact if $U \subseteq \mathbb{A}(W)_{F_{\mathrm{alg}}}$ is an H_{alg}-invariant nonempty open subset with free H_{alg}-action then the union of all $\mathrm{Gal}(F_{\mathrm{alg}}/F)$-translates of U descends to a nonempty H-invariant open subset with free H-action, see [23, Prop. 11.2.8].
Every generically free representation is faithful, but the converse need not be true. In particular, every generically free representation V of H has dimension $\dim(V) \geq \dim(H)$ and when $\mathrm{ed}(H) > 0$ this inequality is strict by [3, Proposition 4.11].
The main result of this section is the following Theorem:

Theorem 2.2. *Assume that d divides r. Then the canonical representation of $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ is generically free if and only if the index of A satisfies*

$$\mathrm{ind}(A) \geq \begin{cases} 2, & \text{if } d = r = 1, m > 1, \\ 3, & \text{if } d = r > 1, \\ r, & \text{if } d = m = 1 \\ \frac{r}{d} + 1, & \text{if } d < r \text{ and } (d > 1 \text{ or } m > 1). \end{cases}$$

In order to prove Theorem 2.2 we start with a couple of intermediate results. We will need the notion of *stabilizer in general position*, abbreviated SGP. An SGP for an action of an algebraic group H (over a field F) on a geometrically irreducible F-variety X is a subgroup S of H with the property that there exists a non-empty open subscheme U of X such that all points $u \in U(F_{\mathrm{alg}})$ have (scheme-theoretic) stabilizers conjugate to $S_{\mathrm{alg}} = S_{F_{\mathrm{alg}}}$. We can always make such a subscheme U invariant under H as follows: Consider $U' := \bigcup_{h \in H(F_{\mathrm{alg}})} hU_{\mathrm{alg}}$, which is a nonempty H_{alg}-invariant open subscheme of X_{alg}. By construction the stabilizer of every $u \in U'(F_{\mathrm{alg}})$ is conjugate to S_{alg}.

Now $U'(F_{\mathrm{alg}})$ is also invariant under the action of the absolute Galois group of F. Therefore, by [23, Prop. 11.2.8] it descends to an H-invariant open subset of X with the same properties as U.

Clearly a representation of H is generically free, if and only if it the trivial subgroup of H is an SGP for that action. Moreover if H acts on X with kernel N, then S is an SGP for the H-action on X if and only if S contains N and S/N is an SGP for the (faithful) H/N-action on X.

The following lemma is well known for algebraically closed fields of characteristic 0. We adapt the proof of [18, Proposition 8] to our more general situation, when F is an arbitrary field.

Lemma 2.3. *Let H act on two geometrically irreducible F-varieties X and Y. Suppose that S_1 is an SGP for the H-action on X and S_2 is an SGP for the S_1-action on Y. Then S_2 is an SGP for the H-action on $X \times Y$.*

Proof. First by replacing X with a suitable non-empty H-invariant open subvariety we may assume that every $x \in X(F_{\mathrm{alg}})$ has stabilizer conjugate to $(S_1)_{\mathrm{alg}}$ in H_{alg}. Let U_Y be a non-empty S_1-invariant open subset of Y such that all $u \in U_Y(F_{\mathrm{alg}})$ have stabilizer conjugate to $(S_2)_{\mathrm{alg}}$ in $(S_1)_{\mathrm{alg}}$. Let $C = H \cdot (X^{S_1} \times U_Y^{S_2})$ denote the set-theoretical image of $(X^{S_1} \times U_Y^{S_2})$ in $X \times Y$ under the action map $H \times (X \times Y) \to X \times Y$. Endow the closure $Z := \bar{C}$ with the reduced scheme structure and consider the morphism $p_X \colon Z \to X$ of schemes given by the composition $Z \hookrightarrow X \times Y \stackrel{\pi_X}{\to} X$. The fiber of p_X over any $x \in X(F_{\mathrm{alg}})$ has dimension equal to $\dim Y$. In fact if $h_x \in H(F_{\mathrm{alg}})$ is such that $(H_{\mathrm{alg}})_x = h_x (S_1)_{\mathrm{alg}} h_x^{-1}$ then $p_X^{-1}(x)(F_{\mathrm{alg}})$ contains $\{x\} \times h_x U_Y(F_{\mathrm{alg}})$, as one easily checks. Therefore by the fiber dimension theorem $\dim Z = \dim X + \dim Y$ and it follows that C is dense in $X \times Y$. Since C is constructible (by Chevalley's Theorem) there exists a non-empty open subset $U \subset X \times Y$ contained in C. The stabilizer of every $u \in U(F_{\mathrm{alg}})$ is conjugate to $(S_2)_{\mathrm{alg}}$, since this is obviously true for elements of $(X^{S_1} \times U_Y^{S_2})(F_{\mathrm{alg}})$. Therefore S_2 is an SGP for the H-action on $X \times Y$. □

The following proposition will be the key step in order to establish the case of Theorem 2.2, where $m = 1$.

Proposition 2.4. *Let V be a vector space over a field F, whose dual we denote by V^*, and let*

$$H = \mathbf{GL}(V^*) \times \mathbf{GL}(V).$$

For any commutative F-algebra R and $\varphi \in \mathrm{End}(V_R)$ denote by $\varphi^* \in \mathrm{End}(V_R^*)$ the dual endomorphism (given by the formula $(\varphi^*(f))(v) = f(\varphi(v))$ for $v \in V_R$, $f \in V_R^* = \mathrm{Hom}_R(V_R, R)$).

(a) *The image $S \simeq \mathbf{GL}(V)$ of the homomorphism*

$$\mathbf{GL}(V) \to H,\ \varphi \mapsto ((\varphi^*)^{-1}, \varphi)$$

is an SGP for the natural H-action on $V^* \otimes_F V$.

(b) *Let E be a maximal étale subalgebra of* $\mathrm{End}(V)$*. Then the image* $T \simeq \mathbf{GL}_1(E)$ *of the homomorphism*

$$\mathbf{GL}_1(E) \to H,\ \varphi \mapsto ((\varphi^*)^{-1}, \varphi)$$

is an SGP for the natural H-action on $(V^* \otimes_F V)^{\oplus 2}$.

(c) *Let* $Z(H) \simeq \mathbf{G}_m \times \mathbf{G}_m$ *denote the center of H. The image of the homomorphism*

$$\mathbf{G}_m \to Z(H) \subseteq H, \quad \lambda \mapsto (\lambda^{-1}, \lambda)$$

is an SGP for the natural H-action on $(V^* \otimes_F V)^{\oplus 3}$.

(d) *Suppose* $V = V_1 \otimes_F V_2$ *and consider the subgroup*

$$H' = \mathbf{GL}(V_1^*) \times \mathbf{GL}(V)$$

of $H = \mathbf{GL}(V^*) \times \mathbf{GL}(V)$*. Let* $t = \dim(V_2)$*. Then the image S' of the homomorphism*

$$\mathbf{GL}(V_1) \to H',\ \varphi \mapsto ((\varphi^*)^{-1}, \varphi)$$

is an SGP for the natural H'-action on $(V_1^* \otimes_F V)^{\oplus t}$.

Moreover if $t > 1$, the image of the homomorphism

$$\mathbf{G}_m \to Z(H') \subseteq H', \quad \lambda \mapsto (\lambda^{-1}, \lambda)$$

is an SGP for the natural H'-action on $(V_1^* \otimes_F V)^{\oplus (t+1)}$.

Proof. (a) We use the canonical identification of $V^* \otimes_F V$ with the underlying F-vector space of the F-algebra $\mathrm{End}_F(V^*)$, where a pure tensor $f \otimes v$ corresponds to the endomorphism of V^* defined by $f' \mapsto f'(v)f$. The H-action on (the affine space associated with) $V^* \otimes_F V = \mathrm{End}_F(V^*)$ is then given by the formula

$$(\psi, \varphi) \cdot \rho = \psi \rho \varphi^*.$$

Let $U = \mathbf{GL}(V^*) \subseteq \mathbb{A}(\mathrm{End}(V^*))$, which is a non-empty and H-invariant open subset. The stabilizer of $\rho \in U(F_{\mathrm{alg}})$ in H_{alg} is given by the image of the homomorphism

$$\mathbf{GL}(V)_{\mathrm{alg}} \to H_{\mathrm{alg}}, \quad \varphi \mapsto (\rho(\varphi^*)^{-1}\rho^{-1}, \varphi)$$

which is a conjugate of S_{alg} over F_{alg}. This shows the claim.

(b) Let S be the subgroup of H from part (a). By Lemma 2.3 it suffices to show that T is an SGP for the S-action on $V^* \otimes_F V$. Let $U \subseteq \mathbb{A}(V^* \otimes_F V) = \mathbb{A}(\mathrm{End}(V^*))$ be as in part (a). Identify $(V^*)^*$ with V in the usual way, so that $\psi^* \in \mathrm{End}(V)$ for $\psi \in \mathrm{End}(V^*)$. For any $\rho \in U(F_{\mathrm{alg}})$ the stabilizer of ρ in S_{alg} is the image of the centralizer $C_{\mathbf{GL}(V)_{\mathrm{alg}}}(\rho^*)$ under the homomorphism $\mathbf{GL}(V)_{\mathrm{alg}} \to S_{\mathrm{alg}}, \varphi \mapsto ((\varphi^*)^{-1}, \varphi)$. When ρ^* is semisimple regular $C_{\mathbf{GL}(V)_{\mathrm{alg}}}(\rho^*)$ is a maximal torus of $\mathbf{GL}(V)_{\mathrm{alg}}$. Now the claim follows from the well known facts that all maximal tori of $\mathbf{GL}(V)_{\mathrm{alg}}$ are conjugate and the semisimple regular elements in $\mathbb{A}(\mathrm{End}(V^*))$ form a non-empty open subset.

(c) By part (b) $T \simeq \mathbf{GL}_1(E)$ is an SGP for the H-action on two copies of $V^* \otimes_F V$. The kernel of the T-action on $V^* \otimes_F V$ is the image of $\mathbf{G}_m$ in H and coincides with the SGP for this action, since T is a torus, see e.g. [12, Proposition 3.7(A)]. Now the claim follows with Lemma 2.3.

(d) Note that $(V_1^* \otimes_F V)^{\oplus t}$ is H-equivariantly isomorphic to $V_1^* \otimes_F V_2^* \otimes_F V \simeq V^* \otimes_F V$. Define the open subset $U \subseteq \mathbb{A}(V^* \otimes_F V)$ like in part (a). Then every $\rho \in U(F_{\mathrm{alg}})$ has stabilizer in $(H')_{\mathrm{alg}}$ given by the image of the homomorphism

$$\mathbf{GL}(V_1)_{\mathrm{alg}} \to (H')_{\mathrm{alg}}, \quad \alpha \mapsto ((\alpha^*)^{-1}, \rho^*\alpha(\rho^*)^{-1})$$

which is conjugate to $(S')_{\mathrm{alg}}$ over F_{alg}. This shows the first claim.

As an S'-representation $V_1^* \otimes_F V$ is isomorphic to the t-fold direct sum of $W = \mathrm{End}(V_1^*)$ where S' acts through the formula

$$((\varphi^*)^{-1}, \varphi) \cdot \rho = (\varphi^*)^{-1} \rho \varphi^*.$$

As in the proof of part (b) and (c) the S'-action on W has SGP isomorphic to $\mathbf{GL}_1(E')$ for a maximal étale subalgebra E' of $\mathbf{GL}(V_1)$ and the S'-action on $W^{\oplus 2}$ and, since $t > 1$, also on $W^{\oplus t} \simeq V_1^* \otimes_F V$, has as SGP the kernel of this action, which is the image of $\mathbf{G}_m$ in H' by the given homomorphism. Now the claim follows from Lemma 2.3.

□

The next lemma will allow a reduction to the case $m = 1$ in Theorem 2.2 when $d \neq 1$.

Lemma 2.5. *(a) Let $m \geq 1$. A representation of an algebraic group H on a vector space V of dimension $\dim(V) > \dim(H)$ is generically free if and only if the associated representation of the wreath product $H^m \rtimes S_m$ on $V^{\oplus m}$ is generically free.*

(b) Suppose A is split and $d \neq 1$. Then for any $t \geq 1$ generic freeness of $(\rho_{\mathrm{can}}^G)^{\oplus t}$ depends only on r and d, not on m.

Proof. (a) If $H^m \rtimes S_m$ acts generically freely on $V^{\oplus m}$ then so does the subgroup H^m. Let

$$U \subseteq \mathbb{A}(V^{\oplus m}) = \underbrace{\mathbb{A}(V) \times \cdots \times \mathbb{A}(V)}_{m \text{ times}}$$

be a non-empty H^m-invariant open subset where H^m acts freely. Then the projection $\pi_1(U) \subseteq \mathbb{A}(V)$ is non-empty open and H-invariant with free H-action. Hence H acts generically freely on V.

Conversely suppose that H acts generically freely on V. Let $U_0 \subseteq \mathbb{A}(V)$ a friendly open subset, i.e., an H-invariant non-empty open subset such that there exists an H-torsor $\pi\colon U_0 \to Y$ for some irreducible F-scheme Y (which we will fix). Existence of U_0 is granted by a Theorem of P. Gabriel, see [3, Theorem 4.7] or [22, Exposé V, Théoréme 10.3.1]. Since $\dim(U_0) = \dim(V) > \dim(H)$ we have $\dim(Y) > 0$. Hence the open subset $Y^{(m)}$ of Y^m where the m coordinates are different, is nonempty open with free natural S_m-action on it. Now the inverse image of $Y^{(m)}$ in U_0^m under the morphism $\pi^m\colon U_0^m \to Y^m$ is $H^m \rtimes S_m$-invariant, nonempty and open with $H^m \rtimes S_m$ acting freely on it.

(b) Since the property of being generically free can be checked over an algebraic closure F_{alg} and $(\rho^G_{\mathrm{can}})_{F_{\mathrm{alg}}} = \rho^{G_{\mathrm{alg}}}_{\mathrm{can}}$ we may assume without loss of generality that F is algebraically closed. Let

$$H = (\mathbf{GL}(V_1) \times \mathbf{GL}(V_2))/\mathbf{G}_m,$$

where V_1 and V_2 are vector spaces of dimension $\dim(V_1) = d$, $\dim(V_2) = r$ and $\mathbf{G}_m$ is embedded in the center of $\mathbf{GL}(V_1) \times \mathbf{GL}(V_2)$ through $\lambda \mapsto (\lambda, \lambda^{-1})$. Then

$$G \simeq H^m \rtimes S_m.$$

In particular for $m = 1$ the two groups H and G are isomorphic. Moreover, in general, ρ^G_{can} is given by the obvious homomorphism

$$G \to \mathbf{GL}((V_1 \otimes_F V_2)^{\oplus m}).$$

In order to establish the claim, it suffices to show that the representation of H on $V := (V_1 \otimes_F V_2)^{\oplus t}$ is generically free if and only if the associated representation $(\rho^G_{\mathrm{can}})^{\oplus t}$ of G on $V^{\oplus m}$ is generically free. When $\dim(V) > \dim(H)$ the claim follows from part (a). On the other hand when $\dim(V) \leq \dim(H)$ or equivalently $\dim(V^{\oplus m}) \leq \dim G$ the two representations of G and H, respectively, are both not generically free, since otherwise the respective group would have essential dimension 0. This is both excluded by the assumption $d \neq 1$, since $B \simeq M_d(F)^m$ and $M_d(F)$ have nontrivial forms over some field extension K/F which embed in $A \otimes_F K \simeq M_{drm}(K)$. Correspondingly there is a non-trivial G-torsor (resp. H-torsor) over K. This torsor cannot be defined over any subfield of transcendence degree 0 over F, since F is algebraically closed.

□

The following lemma tells us how ρ^H_{can} looks over F_{sep}, for any subgroup H of $\mathbf{GL}_1(A)$.

Lemma 2.6. *Over F_{sep} the representation ρ^H_{can} decomposes as a direct sum of* $\mathrm{ind}(A)$ *copies of the canonical representation of $H_{\mathrm{sep}} = H_{F_{\mathrm{sep}}}$.*

Proof. Fix isomorphisms $A_{\mathrm{sep}} \xrightarrow{\sim} \mathrm{End}(V)$, $(D^{\mathrm{op}})_{\mathrm{sep}} \xrightarrow{\sim} \mathrm{End}(W)$ with F_{sep}-vector spaces V and W. Let $w_1, \ldots, w_a$ be a basis of W, with $a = \dim(W) = \mathrm{ind}(A)$. Then $(\rho^H_{\mathrm{can}})_{F_{\mathrm{sep}}}$ is equivalent to the composition $H_{\mathrm{sep}} \hookrightarrow \mathbf{GL}(V) \hookrightarrow \mathbf{GL}(V \otimes_{F_{\mathrm{sep}}} W)$, whilst $\rho^{H_{\mathrm{sep}}}_{\mathrm{can}}$ is equivalent to the inclusion $H_{\mathrm{sep}} \hookrightarrow \mathbf{GL}(V)$. Since the subspaces $V \otimes_{F_{\mathrm{sep}}} F_{\mathrm{sep}} w_i$ of $V \otimes_{F_{\mathrm{sep}}} W$ are $\mathbf{GL}(V)$-invariant and $\mathbf{GL}(V)$-equivariantly (and therefore H_{sep}-equivariantly) isomorphic to V, the claim follows. □

We are now ready to prove our main result from this section.

Proof of Theorem 2.2. In view of Lemma 2.6 it suffices to show that the least integer $t \geq 1$ such that the t-fold direct sum of $\rho_{\mathrm{can}}^{G_{\mathrm{sep}}}$ is generically free, is given by the lower bound on the index in the statement of the theorem.

(a) Case $d = r = 1, m > 1$: Here B is a maximal étale subalgebra of A of dimension $\deg(A) = m > 1$. The canonical representation of G_{sep} is given by the natural action of $(\mathbf{G}_m)^m \rtimes S_m$ on $V = F^m$. Let $U \subseteq \mathbb{A}(V) = \mathbb{A}^m$ denote the open subset where all coordinates are non-zero. The group G_{sep} operates transitively on U. Therefore the stabilizer of any $u \in U(F_{\mathrm{alg}})$ is conjugate to the stabilizer of $(1, \ldots, 1)$ in G_{sep}, which is S_m. Therefore S_m is an SGP for the canonical representation of G_{sep}. Moreover S_m acts freely on the S_m-invariant open subset of U, where all coordinates are different. Thus the canonical representation of G_{sep} is not generically free, but two copies of it are, by Lemma 2.3.

(b) Case $d = r > 1$: We must show that two copies of the canonical representation of G_{sep} are not generically free, but three copies are. By Lemma 2.5, since $d > 1$, we may assume that $m = 1$. Let V be an F_{sep}-vector space of dimension $d = r$. Identify B_{sep} with $\mathrm{End}(V^*)$ and its centralizer in A_{sep} with $\mathrm{End}(V)$. This identifies G_{sep} with $(\mathbf{GL}(V^*) \times \mathbf{GL}(V))/\mathbf{G}_m$, where $\mathbf{G}_m$ is embedded in the center of $\mathbf{GL}(V^*) \times \mathbf{GL}(V)$ via $\lambda \mapsto (\lambda^{-1}, \lambda)$. Its canonical representation is given by the natural action on $V^* \otimes_F V$. By Proposition 2.4(b) the sum of two copies of this representation has an SGP in general position of the form $\mathbf{G}_m^d/\mathbf{G}_m$, hence it is not generically free. Moreover Proposition 2.4(c) shows that the sum of three copies of that representation is generically free.

(c) Case $d = m = 1$: Here $G = \mathbf{GL}_1(A)$ with A of degree $drm = r$. By dimension reasons we need at least r copies of the canonical representation of G_{sep} (whose dimension is r) in order to get a generically free representation. On the other hand r copies are clearly enough.

(d) Case $d < r$ and ($d > 1$ or $m > 1$):

First assume $d > 1$. This case is similar to case (b). We must show that $\frac{r}{d} + 1$ copies of the canonical representation of G_{sep} are generically free, but $\frac{r}{d}$ copies are not. By Lemma 2.5 we may assume that $m = 1$. Let V_1 and V_2 be F_{sep}-vector spaces of dimension d and $\frac{r}{d}$, respectively, and set $V = V_1 \otimes_{F_{\mathrm{sep}}} V_2$, which is of dimension r. Identify B_{sep} with $\mathrm{End}(V_1^*)$ and its centralizer in A_{sep} with $\mathrm{End}(V)$, so that $G_{\mathrm{sep}} = (\mathbf{GL}(V_1^*) \times \mathbf{GL}(V))/\mathbf{G}_m$. Its canonical representation is given by the natural action on $V_1^* \otimes_{F_{\mathrm{sep}}} V$. By Proposition 2.4(c) exactly $\dim(V_2) + 1 = \frac{r}{d} + 1$ copies of this representation are needed in order to get a generically free representation. This establishes the claim in case $d > 1$.

Now assume $d = 1 < r$ and $m > 1$. Here B is étale of dimension m with $1 < m < rm = \deg(A)$. Let V denote an r-dimensional

F_{sep}-vector space. Then $G_{\mathrm{sep}} \simeq (\mathbf{GL}(V))^m \rtimes S_m$ and its canonical representation is given by the natural action on $V^{\oplus m}$. We have $\dim G = r^2 m = r \cdot \dim(V^{\oplus m})$. Since G_{sep} is not connected it has $\mathrm{ed}(G_{\mathrm{sep}}) > 0$, see [11, Lemma 10.1], hence we need at least $r+1$ copies of $V^{\oplus m}$ in order to get a generically free representation. On the other hand the connected component $G^0_{\mathrm{sep}} \simeq (\mathbf{GL}(V))^m$ acts generically freely on r copies of $V^{\oplus m}$ and S_m acts generically freely on $V^{\oplus m}$, which implies that G_{sep} acts generically freely on $r+1$ copies of $V^{\oplus m}$. This concludes the proof.

□

3. Proof of Theorem 1.1

The purpose of this section consists in proving the results on $\mathrm{ed}(G)$ as formulated in our main theorem.

Proof of Theorem 1.1. (a) The inequality $\mathrm{ind}(A) \leq \frac{r}{d}$ implies that r is divisible by $d\,\mathrm{ind}(A)$, since $\mathrm{ind}\,A$, r and d are powers of p. In this case natural isomorphism between the functors of $H^1(-,G)$ and $\mathbf{Forms}(B)$ was established in [13, Remark 4.8]. In fact when r is divisible by $d\,\mathrm{ind}(A)$ every form B' of B over a field extension K/F can be embedded in $A \otimes_F K$ with type $[(d,r),\dots,(d,r)]$.

Now for every F-form B' of B the functors $\mathbf{Forms}(B)$ and $\mathbf{Forms}(B')$ are equivalent as functors to the category of sets. The split form of B over F is $M_d(F)^m$ and its automorphism group scheme is $(\mathbf{PGL}_d)^m \rtimes S_m$. This shows that $\mathbf{Forms}(B)$ is naturally isomorphic to the Galois cohomology functor $H^1(-,(\mathbf{PGL}_d)^m \rtimes S_m)$.

(b) Assume $\mathrm{ind}(A) > \frac{r}{d}$. For any algebraic group H over F we have the standard inequality

$$\mathrm{ed}(H) \leq \dim(\rho) - \dim(H)$$

for any generically free representation ρ of H, see [3, Proposition 4.11]. The canonical representation of the group $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$ has dimension $\deg(A)\,\mathrm{ind}(A)$. Therefore Theorem 2.2 yields the inequality

$$\mathrm{ed}(G) \leq \deg(A)\,\mathrm{ind}(A) - \dim(G) \tag{1}$$

in case

$$\mathrm{ind}(A) \geq \begin{cases} 2, & \text{if } d = r = 1, m > 1,\\ 3, & \text{if } d = r > 1,\\ r, & \text{if } d = m = 1\\ \frac{r}{d}+1, & \text{if } d < r \text{ and } (d > 1 \text{ or } m > 1).\end{cases}$$

Combining this with the assumption $\mathrm{ind}(A) > \frac{r}{d}$ shows that inequality (1) is always satisfied, except possibly when $d = r > 1$ and $\mathrm{ind}(A) = 2$.

Now we show the converse to inequality (1). We follow the approach given in [13]. Let $\mathbf{Aut}_F(A,B)$ denote the group scheme of automorphisms of B-preserving automorphisms of A. We have an exact sequence

$$1 \to \mathbf{G}_m \to G \overset{\mathrm{Int}}{\to} \mathbf{Aut}_F(A,B) \to 1,$$

where $\mathrm{Int}\colon G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B)) \to \mathbf{Aut}_F(A,B)$ takes, for every commutative F-algebra R, the element $g \in G(R) \subseteq (A \otimes_F R)^\times$ to the inner automorphism of $A \otimes_F R$ given by conjugation by g. The connection map

$$H^1(K, \mathbf{Aut}_F(A,B)) \to H^2(K, \mathbf{G}_m) = \mathrm{Br}(K)$$

sends the isomorphism class of a K-form (A', B') of (A,B) to the Brauer class $[A'] - [A \otimes_F K] = [A' \otimes_F A^{\mathrm{op}}]$. Write $\deg(A) = p^s$. By [13, Lemma 2.3] there exists a field extension K/F and a central simple K-algebra A' of the form $A' = D_1 \otimes_K \cdots \otimes_K D_s$ for division K-algebras $D_1, \ldots, D_s$ of degree p, such that

$$\mathrm{ind}(A' \otimes_F A^{\mathrm{op}}) = p^s \,\mathrm{ind}(A) = \deg(A)\,\mathrm{ind}(A).$$

Write $d = p^a$, $r = p^b$, $m = p^c$, so that $a + b + c = s$. Choose a maximal étale K-subalgebra L_i of D_{a+i} for $i \in \{1, \ldots, c\}$. Then

$$B' := D_1 \otimes_K \cdots \otimes_K D_a \otimes_K L_1 \otimes_K \cdots \otimes_K L_c$$

is a separable K-subalgebra of A' of type $[(d,r), \ldots, (d,r)]$ (like B in A). This implies that (A', B') is a K-form of (A,B) by [13, Lemma 4.2(d)]. Therefore the maximal index of a Brauer class contained in the image of a connection map $H^1(K, \mathbf{Aut}_F(A,B)) \to \mathrm{Br}(K)$ for a field extension K/F is precisely $\deg(A)\,\mathrm{ind}(A)$. Now the inequality

$$\mathrm{ed}(G) \geq \deg(A)\,\mathrm{ind}(A) - \dim(G)$$

follows from [5, Corollary 4.2].

□

Remark 3.1. Theorem 1.1 holds with essential dimension replaced by essential p-dimension. For definition of $\mathrm{ed}_p(G)$ see [14] or [21]. In fact part (a) follows from the description of the Galois cohomology functor $H^1(-, G)$ like for essential dimension. Moreover we always have $\mathrm{ed}_p(G) \leq \mathrm{ed}(G)$ and the lower bounds given in part (b) are actually lower bounds on $\mathrm{ed}_p(G)$. This follows from the p-incompressibility of Severi-Brauer varieties of division algebras of p-power degree [9, Theorem 2.1] and [14, Theorem 4.6].

4. The Special Case

In this section we consider the case, which was not resolved by Theorem 1.1. Hence we assume throughout this section that

$$A = M_{2^n}(Q)$$

for some integer $n \geq 0$ and a non-split quaternion F-algebra Q, and $B \subseteq A$ is a separable subalgebra with

$$B_{\mathrm{sep}} \simeq (M_{2^a}(F_{\mathrm{sep}}))^{2^c} \simeq C_{\mathrm{sep}},$$

where $C \subseteq A$ is the centralizer of B in A and a, c are integers with $a \geq 1, c \geq 0$. Note that the relation $drm = \deg(A)$ implies $2a + c = n + 1$. Recall that $G = N_{\mathbf{GL}_1(A)}(\mathbf{GL}_1(B))$.

Example 4.1. Suppose $m = 1$, which means that B is central simple of degree $d = 2^a$. Then the functor $H^1(-, G) \simeq \mathbf{Forms}^{\theta}_A(B)$ (with $\theta_B = [(d,d)]$) classifies central simple algebras B' of degree d over field extensions K/F such that $B' \otimes_F Q$ is not a division algebra. This is shown as follows: B' embeds in A_K if and only if $B' \otimes_F Q$ embeds in $A_K \otimes_F Q \simeq M_{2d^2}(K)$. If this is the case, the centralizer of $B' \otimes_F Q$ in $M_{2d^2}(K)$ has degree d and has opposite Brauer class to $B' \otimes_F Q$. Therefore the index of $B' \otimes_F Q$ divides d, i.e. $B' \otimes_F Q$ is not a division algebra. Conversely, if the index of $B' \otimes_F Q$ divides d, then the opposite algebra is Brauer equivalent to a degree d algebra, so $B' \otimes_F Q$ embeds in $M_{2d^2}(K)$.

Let L/F be a maximal separable subfield of Q (of dimension 2 over F). The algebra A splits over L. In particular we get the lower bound

$$\mathrm{ed}(\mathbf{Forms}(M_d(L)^m)) = \mathrm{ed}(\mathbf{Forms}(B_L)) = \mathrm{ed}(G_L) \leq \mathrm{ed}(G)$$

on $\mathrm{ed}(G)$ by Theorem 1.1(a) and [3, Proposition 1.5].
Moroever we have the upper bound

$$\begin{aligned}\mathrm{ed}(G) \leq 4\deg(A) - \dim(G) &= 4 \cdot 2^{2a+c} - 2^c((2^a)^2 + (2^a)^2 - 1) \\ &= 2^{2a+c+2} - 2^{2a+c+1} + 2^c \\ &= 2^c(2^{2a+1} + 1),\end{aligned}$$

since 2 copies of ρ^G_{can} are generically free by Theorem 2.2 and Lemma 2.6.
The main effort in this section will go into proving a better upper bound on $\mathrm{ed}(G)$.

For this purpose we will show that the canonical representation of the normalizer of a maximal torus (and even of some larger subgroup) of G is generically free. The following lemma reveals that this will improve the above upper bound on $\mathrm{ed}(G)$.

Lemma 4.2. *Let T be a maximal torus of G and H a subgroup of G containing the normalizer $N_G(T)$. Suppose that ρ^H_{can} is generically free. Then*

$$\begin{aligned}\mathrm{ed}(G) \leq \mathrm{ed}(H) &\leq 2\deg(A) - \dim H \\ &= 2^{c+2a+1} - \dim H.\end{aligned}$$

Proof. The connected component $G^0_{\mathrm{alg}} \simeq ((\mathbf{GL}_{2^a} \times \mathbf{GL}_{2^a})/\mathbf{G}_m)^{2^c}$ of G_{alg} is reductive. Therefore the inclusion $\iota\colon N_G(T) \hookrightarrow G$ induces a surjection of functors

$$\iota_*\colon H^1(-, N_G(T)) \twoheadrightarrow H^1(-, G),$$

see e.g. [6, Corollary 5.3]. Note that G is supposed to be connected reductive there, but the proof goes through if only G^0 is reductive (over F_{alg}).
Since ι factors through H, the map ι_* factors through $H^1(-,H)$. By [3, Lemma 1.9] this proves the first inequality. The second inequality follows from $\dim(\rho^H_{\mathrm{can}}) = 2\deg(A)$ and [3, Proposition 4.11]. □

In order to make use of Lemma 4.2 we will need the following result:

Lemma 4.3. *Let R be a connected reductive algebraic group over F. Let T be a maximal torus of R and let $\mathcal{T}_R \simeq R/N_R(T)$ denote the variety of maximal tori in R. Assume that $R/Z(R)$ is simple, i.e., has no nontrivial normal subgroups. Then there exists a non-empty open subscheme U of $\mathcal{T}_R$ such that every maximal torus of R_{alg} contained in $U(F_{\mathrm{alg}})$ intersects $(N_R(T))_{\mathrm{alg}}$ exactly in $Z(R)_{\mathrm{alg}}$.*

Proof. First note that T contains $Z(R)$, since R is reductive. If T is central in R, then $T = Z(R)$, and the claim easily follows. Hence we may assume that T is non-central. We let R act on $\mathcal{T}_R$ through conjugation. The kernel of this action is a proper normal subgroup of R containing $Z(R)$. Hence it is equal to $Z(R)$. Therefore the kernel of the T-action on $\mathcal{T}_R$ obtained by restriction is also $Z(R)$. By [12, Proposition 3.7] the induced $T/Z(R)$-action on $\mathcal{T}_R$ is generically free. Hence there exists a non-empty open subscheme $\tilde{U}$ of $\mathcal{T}_R$ such that every $S \in \tilde{U}(F_{\mathrm{alg}})$ has stabilizer in T_{alg} equal to $Z(R)_{\mathrm{alg}}$, i.e. $N_{R_{\mathrm{alg}}}(S) \cap T_{\mathrm{alg}} = Z(R)_{\mathrm{alg}}$. For $a \in R(F_{\mathrm{alg}})$ with $S = aT_{\mathrm{alg}}a^{-1}$ this is equivalent to $(N_R(T))_{\mathrm{alg}} \cap (a^{-1}T_{\mathrm{alg}}a) = Z(R)_{\mathrm{alg}}$.
Denote by $\pi\colon R \to \mathcal{T}_R,\ a \mapsto aTa^{-1}$ the projection map and by $\iota\colon R \to R,\ a \mapsto a^{-1}$ the inversion map. Then $U := (\pi\circ\iota)(\pi^{-1}(\tilde{U}))$ has the desired property. □

Proposition 4.4. *With the standing assumptions $r = d = 2^a > 1$, $m = 2^c \geq 1$ and $\mathrm{ind}(A) = 2$:*

$$\begin{aligned}\mathrm{ed}(G) &\leq 2^{c+2a+1} - 2^c(2^{2a} + 2^a - 1)\\ &= 2^c(2^{2a} - 2^a + 1).\end{aligned}$$

Proof. We first consider the case $m = 1$ (i.e., $c = 0$): Let E be a maximal étale subalgebra of the centralizer $C = C_A(B)$ and let

$$H = (\mathbf{GL}_1(B) \times N_{\mathbf{GL}_1(C)}(\mathbf{GL}_1(E)))/\mathbf{G}_m \subseteq G.$$

We will show that ρ^H_{can} is generically free. Since $\dim(H) = 2^{2a} + 2^a - 1$ this would establish the claim in case $m = 1$ in view of Lemma 4.2. Over F_{alg} we may identify H_{alg} with $(\mathbf{GL}(V^*) \times N_{\mathbf{GL}(V)}(T))/\mathbf{G}_m$ where V is an F_{alg}-vector space of dimension $d = 2^a$ and T is a maximal torus of $\mathbf{GL}(V)$. Moreover ρ^H_{can} becomes a direct sum of two copies of the natural representation

$$H_{\mathrm{alg}} \to \mathbf{GL}(V^* \otimes_{F_{\mathrm{alg}}} V) = \mathbf{GL}(\mathrm{End}(V^*))$$

over F_{alg}. Hence it suffices to show that $\mathbf{G}_m$ is an SGP for the natural action of $H' := \mathbf{GL}(V^*) \times N_{\mathbf{GL}(V)}(T)$ on two copies of $W := \mathrm{End}(V^*)$. Identify $N := N_{\mathbf{GL}(V)}(T)$ with its image in H' under the map $\varphi \mapsto ((\varphi^*)^{-1}, \varphi)$. The proof of Proposition 2.4(b) shows that N is an SGP for the H' action on one copy of W. Moreover the stabilizer of any $\rho \in \mathrm{End}(V^*)$ in N is given by the intersection of N with the centralizer $C_{\mathbf{GL}(V)}(\rho^*)$. When ρ is semisimple regular, $C_{\mathbf{GL}(V)}(\rho^*)$ is a maximal torus of $\mathbf{GL}(V)$. It can be considered as a rational point of the variety of maximal tori $\mathcal{T}_{\mathbf{GL}(V)}$ of $\mathbf{GL}(V)$. By Lemma 4.3 there exists a non-empty open subscheme U of $\mathcal{T}_{\mathbf{GL}(V)}$ such that $N \cap S = \mathbf{G}_m$ for every $S \in U(F_{\mathrm{alg}})$. Let $\mathbf{GL}(V^*)^{\mathrm{ss,reg}} \subset \mathbb{A}(W)$ denote the open subset given by the regular semisimple elements. We have a morphism $\mathbf{GL}(V^*)^{\mathrm{ss,reg}} \to \mathcal{T}_{\mathbf{GL}(V)}$, sending a semisimple regular element ρ to the centralizer $C_{\mathbf{GL}(V)}(\rho^*)$. The preimage P of U in $\mathbf{GL}(V^*)^{\mathrm{ss,reg}}$ is a non-empty open subset of $\mathbb{A}(W)$ such that every $\rho \in P(F_{\mathrm{alg}})$ has stabilizer in N equal to $\mathbf{G}_m$. By Lemma 2.3 this implies the claim.

Now let $m = 2^c$ be arbitrary. Since the functor $H^1(-, G)\colon \mathrm{Fields}_F \to \mathrm{Sets}$ depends only on the type of B, we may replace B by any subalgebra of A of the same type as B without changing $\mathrm{ed}(G)$. As

$$A = M_{2^n}(Q) = M_m(B_0 \otimes_F C_0),$$

with $B_0 = M_{2^a}(F)$ and $C_0 = M_{2^{a-1}}(Q)$, we may take for B the m×m diagonal-matrices with entries in B_0. Its centralizer C is the set of m×m diagonal-matrices with entries in C_0. Therefore

$$G = (G_0)^m \rtimes S_m$$

where

$$G_0 = (\mathbf{GL}_1(B_0) \times \mathbf{GL}_1(C_0))\,/\mathbf{G}_m = N_{\mathbf{GL}_1(B_0 \otimes_F C_0)}(\mathbf{GL}_1(B_0))$$

has $\mathrm{ed}(G_0) \leq 2^{2a} - 2^a + 1$ by the case $m = 1$. By [13, Lemma 4.13] we have $\mathrm{ed}(G) \leq m\,\mathrm{ed}(G_0)$ and the claim follows. □

Remark 4.5. Consider the case $m = 1$. Since $\mathrm{ed}((\mathbf{PGL}_{2^a})_{\mathrm{sep}}) = \mathrm{ed}(G_{\mathrm{sep}}) \leq \mathrm{ed}(G)$ the upper bound

$$\mathrm{ed}(G) \leq 2^{2a} - 2^a + 1$$

should be compared with the best existing upper bound on the essential dimension of $(\mathbf{PGL}_{2^a})_{\mathrm{sep}}$, namely

$$\mathrm{ed}((\mathbf{PGL}_{2^a})_{\mathrm{sep}}) \leq 2^{2a} - 3 \cdot 2^a + 1$$

by [10, Proposition 1.6] (which assumes $\mathrm{char}(F) = 0$).

Corollary 4.6. *Suppose B is central simple (i.e., $m = 1$) and* $\mathrm{char}(F) \neq 2$. *Then*

$$\max\{2, (a-1)2^a + 1\} \leq \mathrm{ed}(G) \leq 2^{2a} - 2^a + 1.$$

In particular when B has degree 2 we have

$$\mathrm{ed}(G) \in \{2, 3\}$$

and when B has degree 4 we have

$$\mathrm{ed}(G) \in \{5, 6, \ldots, 13\}.$$

If B is central simple of degree 2 and $\mathrm{char}(F) = 2$ *we still have* $\mathrm{ed}(G) \in \{2, 3\}$.

Proof. The upper bound on $\mathrm{ed}(G)$ is contained in Proposition 4.4.
By Theorem 1.1(a) we have $\mathrm{ed}(\mathbf{Forms}(M_{2^a}(F_{\mathrm{sep}}))) = \mathrm{ed}(G_{\mathrm{sep}}) \leq \mathrm{ed}(G)$. Hence the lower bound

$$(a-1)2^a + 1 \leq \mathrm{ed}(G)$$

follows from [16, Theorem 6.1] (which assumes $\mathrm{char}(F) \neq 2$) and the lower bound $2 \leq \mathrm{ed}(G)$ follows from [20, Lemma 9.4(a)] (the paper assumes characteristic 0, but the proof works in arbitrary characteristic). □

References

[1] Auel, A., E. Brussel, S. Garibaldi and U. Vishne. "Open problems on Central Simple Algebras." *Transformation Groups* 16, no. 1, (2011): 219–264.
[2] Amitsur, S.A. "Division algebras. A survey." Algebraists homage: papers in ring theory and related topics (New Haven, Conn., 1981), *Contemporary Mathematics* 13, Amer. Math. Soc., Providence, R.I., (1982): 3–26.
[3] Berhuy, G., and G. Favi. "Essential Dimension: A Functorial Point of View (after A. Merkurjev)." *Documenta Mathematica* 8 (electronic) (2003): 279–330.
[4] Buhler, J., and Z. Reichstein. "On the essential dimension of a finite group." *Compositio Mathematica* 106 (1997): 159–179.
[5] Brosnan, P., Z. Reichstein, and A. Vistoli. "Essential dimension of moduli of curves and other algebraic stacks." *Journal of the European Mathematical Society* 13, no. 4, (2011): 1079–1112. With an appendix by N. Fakhruddin.
[6] Chernousov, V., Ph. Gille, and Z. Reichstein. "Reduction of structure for torsors over semilocal rings." *Manuscripta Mathematica* 126 (2008): 465–480.
[7] Duncan, A. "Essential dimensions of A_7 and S_7." *Mathematical Research Letters* 17, no. 2 (2010): 263–266.
[8] Jacobson, J. *Basic algebra II*, 2nd ed., New York, NY: W. H. Freeman and Company. xvii, 686 p. (1989).
[9] Karpenko, N. "On anisotropy of orthogonal involutions." Journal of the Ramanujan Mathematical Society 15, no. 1, (2000): 1–22.
[10] Lemire, N. "Essential dimension of algebraic groups and integral representations of Weyl groups", *Transformation Groups* 9, no. 4, (2004): 337–379.
[11] Lötscher R., M. MacDonald, A. Meyer, and Z. Reichstein. "Essential p-dimension of algebraic groups whose connected component is a torus." *Algebra & Number Theory* 7, no. 8 (2013): 1817–1840.
[12] R. Lötscher. "Contributions to the essential dimension of finite and algebraic groups." (PhD diss., University of Basel, 2010). Electronic: http://edoc.unibas.ch/1147/1/DissertationEdocCC.pdf.
[13] Lötscher, R. "Essential dimension of involutions and subalgebras." *Israel Journal of Mathematics* 192, Part A, (2012): 325–346.

[14] Merkurjev, A.S. "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.

[15] Merkurjev, A.S. "Essential p-dimension of $\mathbf{PGL}(p^2)$", *J. Amer. Math. Soc.* 23 (2010): 693–712.

[16] Merkurjev, A.S. "A lower bound on the essential dimension of simple algebras." *Algebra & Number Theory* 4, no.8, (2010): 1055–1076.

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

[18] Popov, V.L. "Closed orbits of Borel subgroups." *Matematicheskii Sbornik. Novaya Seriya* 135, no. 3, (1988): 385–402. English transl.: Math. USSR, Sb. 63, 375–392 (1989).

[19] Procesi, C. "Non-commutative affine rings." *Atti della Accademia Nazionale dei Lincei. Memorie. Classe di Scienze Fisiche, Matematiche e Naturali. Serie VIII. Sezione I* 8 (1967): 237–255.

[20] Reichstein, Z. "On the notion of essential dimension for algebraic groups." *Transformation Groups* 5, no. 3, (2000): 265–304.

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

[22] Gabriel, P. "Construction de schémas quotients", pp. 249–289 in *Schémas en groupes* (SGA 3), tome I: Propriétés générales des schémas en groupes, edited by P. Gille and P. Polo, Documents Mathématiques 7, Société Mathématique de France, Paris, 2011.

[23] Springer, T.A. *Linear algebraic groups*, 2nd ed., Progress in Mathematics (Boston, MA, 1998), Birkhäuser, Boston, 1998.

Roland Lötscher
Mathematisches Institut
Ludwig-Maximilians-Universität
Theresienstraße 39
D-80333 München
Germany
roland.loetscher@math.lmu.de