ESSENTIAL DIMENSION OF SEPARABLE ALGEBRAS EMBEDDING IN A FIXED CENTRAL SIMPLE ALGEBRA

ROLAND LÖTSCHER

ABSTRACT. One of the key problems in non-commutative algebra is the classification of central simple algebras and more generally of separable algebras over fields, i.e., Azumaya-algebras whose center is étale over the given field. In this paper we fix a central simple F-algebra A of prime power degree and study seperable algebras over extensions K/F, which embed in A_K. The type of such an embedding is a discrete invariant indicating the structure of the image of the embedding and of its centralizer over an algebraic closure. For fixed type we study the minimal number of independent parameters, called essential dimension, needed to define the separable K-algebras embedding in A_K for extensions K/F. We find a remarkable dichotomy between the case where the index of A exceeds a certain bound and the opposite case. In the second case 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 first case, however, we manage to compute the exact value of the essential dimension, except in one special case, where we provide lower and upper bounds on the essential dimension.

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 [Am55, ABGV11] for surveys on these topics, including discussion of open problems.

Essential dimension is a more recent topic, introduced around 1995 by J. Buhler and Z. Reichstein [BR97] and in full generality by A. Merkurjev [BF03]. The essential dimension of a functor $\mathcal{F}\colon \mathrm{Fields}_F \to \mathrm{Sets}$ 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

Date: March 10, 2014.

2000 *Mathematics Subject Classification.* 16W10, 16K20.

Key words and phrases. essential dimension, central simple algebras, separable algebra, étale algebras, non-split algebraic group.

The author acknowledges support from the Deutsche Forschungsgemeinschaft, GI 706/2-1.

$K_0 \to K$. 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

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

It is denoted by $\mathrm{ed}(G)$ and measures the complexity of G-torsors and hence of objects which are in natural bijection with torsors of an algebraic group G like central simple algebras (for projective linear groups), quadratic forms (for orthogonal groups), étale algebras (for symmetric groups) etc. See [Re10, Me13] 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 dL) and étale algebras (of dimension n), respectively. The first problem goes back to C. Procesi [Pr67], who asked for fields of definition of the universal division algebra and discovered, in modern terms, that $\mathrm{ed}(\mathbf{PGL}_d) \le d^2$. This upper bound has been improved after the introduction of essential dimension, but it is still quadratic in d. See Remark 3.1 for details. A recent breakthrough has been made by A. Merkurjev [Me10] for a lower bound on $\mathrm{ed}(\mathbf{PGL}_d)$. Namely, if $d = p^a$ for some prime p different from $\mathrm{char}(F)$, he showed that $\mathrm{ed}(\mathbf{PGL}_d) \ge (a-1)p^a + 1$. This was used to show $\mathrm{ed}(\mathbf{PGL}_{p^2}) = p^2 + 1$ when $\mathrm{char}(F) \ne p$. For exponent $a \ge 3$ the problem is still wide open.

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 [BR97]. In our language Hermite and Joubert showed that $\mathrm{ed}(S_5) \le 2$ and $\mathrm{ed}(S_6) \le 3$ (over a field F of characteristic zero), and Klein proved that $\mathrm{ed}(S_5) > 1$, hence $\mathrm{ed}(S_5) = 2$. The gap between the best lower bound (roughly $\frac{n}{2}$) and the best upper bound $n-3$ on $\mathrm{ed}(S_n)$ for $n \ge 5$ is still quite large in general. See [Du10], where it is also proven that $\mathrm{ed}(S_7) = 4$ in characteristic zero.

In this paper we study *separable* algebras B. An algebra B over a field is called separable, if it is semisimple 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 [Lö12], 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}. 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 $r, d, m \ge 1$. By [Lö12, 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 $\mathbf{Forms}^{\theta}_A(B)$ 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 $\mathrm{ed}(\mathbf{Forms}_A(B))$. By [Lö12, Lemma 4.6] we have a natural isomorphism

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

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.

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 $\theta_B = [(d, r), \dots, (d, r)]$ (m-times). Suppose that $\deg(A) = drm$ is a power of a prime p and that $d \le r$, so that $d|r$. Then exatly one of the following cases occurs:*

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

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

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

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

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

Note that the assumption $r \le d$ 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 [Ja89, 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 $\mathrm{ed}(G)$ in that case.

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 generically 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

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

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 $H_{\mathrm{alg}} := H_{F_{\mathrm{alg}}}$. Generically 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 [Sp98, 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 [BF03, Proposition 4.11].

The main result of this section is the following Theorem:

Theorem 2.1. *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 2.1 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 H-invariant subset U of X such that all points $u \in U(F_{\mathrm{alg}})$ have stabilizers conjugate to $S_{\mathrm{alg}} = S_{F_{\mathrm{alg}}}$. 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/N is an SGP for the (faithful) H/N-action on X.

The following lemma is well known.

Lemma 2.1. *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. See [Ma14, Lemma 1.2], who attributes the Lemma to Popov. □

The following proposition will be the key step to establish the case of Theorem 2.1, where $m = 1$.

Proposition 2.1. *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 $\varphi \in \operatorname{End}(V)$ denote by $\varphi^* \in \operatorname{End}(V^*)$ the dual endomorphism (given by the formula $(\varphi^*(f))(v) = f(\varphi(v))$ for $v \in V$, $f \in V^* = \operatorname{Hom}_K(V, K)$).

(a) The subgroup

$$S = \{((\varphi^*)^{-1}, \varphi) \in H \mid \varphi \in \mathbf{GL}(V)\} \simeq \mathbf{GL}(V)$$

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

(b) Let E be a maximal étale subalgebra of $\operatorname{End}(V)$. Then the subgroup

$$T = \{((\varphi^*)^{-1}, \varphi) \in H \mid \varphi \in \mathbf{GL}_1(E)\} \simeq \mathbf{GL}_1(E)$$

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 $\mathbf{G}_m$ under 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 subgroup

$$S' = \{((\varphi^*)^{-1}, \varphi) \in H' \mid \varphi \in \mathbf{GL}(V_1)\}$$

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

Moreover if $t > 1$, the image of $\mathbf{G}_m$ under 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 the F-vector space $V^* \otimes_F V$ with the underlying F-vector space of the F-algebra $\operatorname{End}(V^*)$, 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) $V^* \otimes_F V = \operatorname{End}_F(V^*)$ 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 F_{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 the subgroup of H from part (a). By Lemma 2.1 it suffices to show that T is an SGP for the S-action on $V^* \otimes_F V$. Let $U \subseteq \mathbb{A}(V^* \otimes_F V) = \mathbb{A}(\mathrm{End}(V^*))$ also 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 consists of those $((\varphi^*)^{-1}, \varphi) \in S$ for which φ^* commutes with ρ, or equivalently, φ commutes with ρ^*, i.e., φ lies in the centralizer $C_{\mathbf{GL}(V)_{\mathrm{alg}}}(\rho^*)$. 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 an (S-invariant) 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. [Lö10, Proposition 3.7(A)]. Now the claim follows with Lemma 2.1.

(d) Note that $(V_1^* \otimes_F V)^{\oplus t}$ is H-equivariantly isomorphic to $V_1^* \otimes_F V_2^* \otimes_F V \simeq V^* \otimes_F V$. Let $U \subseteq \mathbb{A}(V^* \otimes_F V)$ be like in part (a). Then every $\rho \in U(F_{\mathrm{alg}})$ has stabilizer in H' 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 2.1.

□

The next lemma will allow a reduction to the case $m = 1$ in Theorem 2.1 when $d \neq 1$.

Lemma 2.2. *(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 $t \geq 1$ generically freeness of $(\rho_{\mathrm{can}}^G)^{\oplus t}$ only depends on the pair (A, B) through r and d.

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 [BF03, Theorem 4.7] or [SGA3, 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 non-empty 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 $(\rho^G_{\text{can}})_{F_{\text{alg}}} = \rho^{G_{\text{alg}}}_{\text{can}}$ 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 oder 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 $(\rho^G_{\text{can}})^{\oplus t}$ 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 2.3. *Over F_{sep} the representation ρ^H_{can} decomposes as a direct sum of $\text{ind}(A)$ copies of the canonical representation of $H_{\text{sep}} = H_{F_{\text{sep}}}$.*

Proof. Fix isomorphisms $A_{\text{sep}} \xrightarrow{\sim} \text{End}(V)$, $(D^{\text{op}})_{\text{sep}} \xrightarrow{\sim} \text{End}(W)$ with F_{sep}-vector spaces V and W. Let $w_1, \dots, w_a$ be a basis of W, with $a = \dim(W) = \text{ind}(A)$. Then $(\rho^H_{\text{can}})_{F_{\text{sep}}}$ is equivalent to the composition $H_{\text{sep}} \hookrightarrow \mathbf{GL}(V) \hookrightarrow \mathbf{GL}(V \otimes_{F_{\text{sep}}} W)$, whilst $\rho^{H_{\text{sep}}}_{\text{can}}$ is equivalent to the inclusion $H_{\text{sep}} \hookrightarrow \mathbf{GL}(V)$. Since the subspaces $V \otimes_{F_{\text{sep}}} F_{\text{sep}} w_i$ of $V \otimes_{F_{\text{sep}}} W$ 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 2.1. In view of Lemma 2.3 it suffices to show that the least integer ≥ 1 such that the t-fold direct sum of $\rho^{G_{\text{sep}}}_{\text{can}}$ is generically free, is given by the lower bound on the index given in the theorem to prove.

(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 $u \in U(F_{\text{alg}})$ is conjugate to the stabilizer of $(1, \dots, 1)$ 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 2.1.

(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 2.2, 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 $\text{End}(V^*)$ and its centralizer in A_{sep} with $\text{End}(V)$. 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 2.1(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 2.1(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 reason 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 2.2 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 $V = V_1 \otimes_{F_{\text{sep}}} V_2$, which is of dimension r. Identify B_{sep} with $\text{End}(V_1^*)$ and its centralizer in A_{sep} with $\text{End}(V)$, so that $G_{\text{sep}} = (\mathbf{GL}(V_1^*) \times \mathbf{GL}(V))/\mathbf{G}_m$. Its canonical representation is given by the natural action on $V_1^* \otimes_{F_{\text{sep}}} V$. By Proposition 2.1(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 a 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 [LMMR13, 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 [Lö12, 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 [BF03, 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 2.1 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 when $d = r > 1$ and $\mathrm{ind}(A) = 2$.

Now we show the converse to inequality (1). We follow the approach given in [Lö12]. Let $\mathbf{Aut}_F(A, B)$ denote the group scheme of automorphisms of

B-preserving automorphisms of A. We have an exact sequence

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

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 [Lö12, 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 $D_1, \dots, D_s$ 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 $i \in \{1, \dots, c\}$. 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 $[(d,r), \dots, (d,r)]$ (like B in A). This implies that (A', B') is a K-form of (A,B) by [Lö12, 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 [BRV11, 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 [Me09] or [Re10]. 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 [Ka00, Theorem 2.1] and [Me09, Theorem 4.6].

4. The Special Case

In this section we cosider 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 $2a + c = n + 1$.

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 [BF03, 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 2.1 and Lemma 2.3.

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 4.1. *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 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. [CGR08, Lemma 5.1]. Since ι factors through H, the map ι_* factors through $H^1(-, H)$. By [BF03, Lemma 1.9] this proves the first inequality. The second inequality follows from $\dim(\rho^H_{\mathrm{can}}) = 2\deg(A)$ and [BF03, Proposition 4.11]. □

In order to make use of Lemma 4.1 we will need the following result:

Lemma 4.2. *Let V be a vector space over an algebraically closed field F with $2 \leq \dim(V) < \infty$ and let T be a maximal torus of $\mathbf{GL}(V)$. Then there exists a non-empty open subset $U \subseteq \mathbf{GL}(V)$ such that*

$$N_G(T) \cap T^g = \mathbf{G}_m$$

for every $g \in U(F)$, where $T^g = gTg^{-1}$ and $\mathbf{G}_m$ is the center of $\mathbf{GL}(V)$.

Proof. Let $B \subset V$ be a (unordered) basis of V consisting of eigenvectors of the T-action. Let $U_0 \subset \mathbf{GL}(V)$ denote the (non-empty) open subset on which all matrix entries with respect to B are non-zero.

For every $t \in T(F)$ let U_t denote the preimage of the complement of $N_G(T)$ under the morphism $\mathbf{GL}(V) \to \mathbf{GL}(V)$, $\quad g \mapsto gtg^{-1}$. This is an open subset of $\mathbf{GL}(V)$. Note that $U_{\lambda t} = U_t$ for all scalars $\lambda \in \mathbf{G}_m(F)$. When t is not a scalar U_t is non-empty, since when $b_1, b_2 \in B$ belong to different eigenspaces of t with corresponding eigenvalues λ_1 and λ_2, then the invertible endomorphism of V defined by $gb_1 = b_1, gb_2 = b_1 + b_2$ and $gb = b$ for $b \in B \setminus \{b_1, b_2\}$ has

$$gtg^{-1}(b_2) = (\lambda_2 - \lambda_1)b_1 + \lambda_2 b_2,$$

which implies $gtg^{-1} \notin N_G(T) = T \rtimes \mathrm{Sym}(B)$, whence $g \in U_t(F)$.

Set

$$U = U_0 \cap \bigcap U_t,$$

where the intersection runs over the (finitely many) elements t of the $n!$-torsion subgroup of $T(F)$ which are not contained in $\mathbf{G}_m(F)$. Then U is non-empty open and it remains to show that $N_G(T) \cap T^g = \mathbf{G}_m$ for every $g \in U(F)$.

Let $g \in U(F)$. First we show that $N_G(T) \cap T^g$ is connected. It suffices to show that the F-rational points of $N_G(T) \cap T^g$ are contained (hence are equal to) the F-rational points of $\mathbf{G}_m$. An element of $(N_G(T) \cap T^g)(F) \setminus \mathbf{G}_m(F)$ is of the form

$$gtg^{-1} = t'\sigma,$$

where $t, t' \in T$ and $\sigma \in \mathrm{Sym}(B)$. Moreover $t \notin \mathbf{G}_m(F) \cdot T(F)[n!]$ by construction of U. Hence there exist two eigenvalues of t with different $n!$-th power. Fix an $n!$-th power of an eigenvalue of t and call it μ. For $b \in B$ let $\lambda_b, \mu_b \in F^\times$ denote the eigenvalue of t and t', respectively, for the eigenvector b, and define $\ell_b \in \mathbb{N}$ as the length of the $\langle\sigma\rangle$-orbit of b. Let V' be the subspace of V generated by those $b \in B$ which satisfy $(\lambda_b)^{n!} = \mu$. Then $\{0\} \subsetneq V' \subsetneq V$ and $g(V')$ is the sum of the eigenspaces of $t'\sigma$ corresponding to eigenvalues whose $n!$-power is μ. The eigenvalues of the restriction of $t'\sigma$ to the subspace generated by $\langle\sigma\rangle b$ are given by the different ℓ_b-th roots of the product $\prod_{b' \in \langle\sigma\rangle b} \mu_{b'}$. Let

$$B' = \left\{ b \in B \mid (\prod_{b' \in \langle\sigma\rangle b} \mu_{b'})^{\frac{n!}{\ell_b}} = \mu \right\}$$

which is a $\langle\sigma\rangle$-invariant subset of B. Then $g(V')$ is the subspaces of V generated by B'. This yields a contradiction, since all matrix entries of g with respect to the basis B are nonzero. Therefore $(N_G(T) \cap T^g)(F) \setminus \mathbf{G}_m(F)$ is in fact empty. Hence $N_G(T) \cap T^g$ is connected, as claimed.

Now, for any $g \in U(F)$:

$$\mathbf{G}_m \subseteq N_G(T) \cap T^g = (N_G(T) \cap T^g)^0 \subseteq N_G(T)^0 \cap T^g = T \cap T^g.$$

It remains to show that $T \cap T^g \subseteq \mathbf{G}_m$. Let R be a commutative F-algebra and $t' \in (T \cap T^g)(R) = T(R) \cap gT(R)g^{-1}$. Choose $t \in T(R)$ with $t' = gtg^{-1}$, or equivalently $t'g = gt$. Since all matrix entries of g with respect to the basis B are non-zero in F, hence invertible in R, this implies that $t' \in \mathbf{G}_m(R)$. Thus $T \cap T^g \subseteq \mathbf{G}_m$, finishing the proof. □

Proposition 4.1. *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 4.1. 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

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

over F_{alg}. Hence it suffices to show that $\mathbf{G}_m$ is an SGP for the natural action of the group $H' := \mathbf{GL}(V^*) \times N_{\mathbf{GL}(V)}(T)$ on two copies of $W = \text{End}(V^*)$. Identify $S = N_{\mathbf{GL}(V)}(T)$ with its image in H' under the map $\varphi \mapsto ((\varphi^*)^{-1}, \varphi)$. The proof of Proposition 2.1(b) shows that S is an SGP for the H' action on one copy of W. Moreover the stabilizer of any $\rho \in \text{End}(V^*)$ in S is given by the intersection of S 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 $\mathbf{GL}(V)$, which is isomorphic to $\mathbf{GL}(V)/N_G(T)$ through the morphism

$$\mathbf{GL}(V)/N_G(T) \to \mathcal{T}_{\mathbf{GL}(V)}, \quad \bar{g} \mapsto T^g.$$

By 4.2 there exists a non-empty open subset U of $\mathbf{GL}(V)$ such that

$$N_{\mathbf{GL}(V)}(T) \cap T^g = \mathbf{G}_m$$

for every $g \in \mathbf{GL}(V)(F_{\text{alg}})$. Its image in $\mathcal{T}_{\mathbf{GL}(V)}$ is again non-empty open, call it U'. Let $\mathbf{GL}(V^*)^{\text{ss,reg}} \subset \mathbb{A}(W)$ denote the open subset given by the regular semisimple elements. We have a morphism $\mathbf{GL}(V^*)^{\text{ss,reg}} \to \mathcal{T}_{\mathbf{GL}(V)}$, sending a semisimple regular element ρ to the centralizer $C_{\mathbf{GL}(V)}(\rho^*)$. The preimage P of U' in $\mathbf{GL}(V^*)^{\text{ss,reg}}$ is a non-empty open subset of $\mathbb{A}(W)$ such that every $\rho \in P(F_{\text{alg}})$ has stabilizer in S equal to $\mathbf{G}_m$. Replacing P by the union of its $S(F_{\text{alg}})$-translates we make it S-invariant without changing stabilizers. By Lemma 2.1 this implies that $\mathbf{G}_m$ is an SGP for the $H' = \mathbf{GL}(V^*) \times N_{\mathbf{GL}(V)}(T)$-action on two copies of W. Hence the claim follows.

Now let $m = 2^c$ be arbitrary. Since the functor $H^1(-, G)\colon \text{Fields}_F \to \text{Sets}$ depends only on the type of B, we may replace B by any subalgebra of A of the same type as B without changing $\text{ed}(G)$. 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 $m \times m$ diagonal-matrices with entries in B_0. Its centralizer C are given by the $m \times m$ 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 $\text{ed}(G_0) \leq 2^{2a} - 2^a + 1$ by the case $m = 1$. By [Lö12, Lemma 4.13] we have $\text{ed}(G) \leq m\,\text{ed}(G_0)$ and the claim follows. □

Remark 4.1. Consider the case $m = 1$. Since $\text{ed}((\mathbf{PGL}_{2^a})_{\text{sep}}) = \text{ed}(G_{\text{sep}}) \leq \text{ed}(G)$ the upper bound

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

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

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

by [Le04, Proposition 1.6] and [LRRS03, Theorem 1.1].

Corollary 4.1. *When B is central simple (i.e., $m = 1$) we have*

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

where the lower bound $(a-1)p^a+1$ assumes characteristic not 2. In particular when B has degree 2 we have

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

(in arbitrary characteristic) and when B has degree 4 we have

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

in characteristic $\neq 2$.

Proof. The upper bound on $\mathrm{ed}(G)$ is contained in Proposition 4.1.

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 $(a-1)p^a + 1 \leq \mathrm{ed}(G)$ follows from [Me10, Theorem 6.1] (which assumes $\mathrm{char}(F) \neq 2$) and the lower bound $2 \leq \mathrm{ed}(G)$ follows from [Re00, Lemma 9.4(a)] (the paper assumes characteristic 0, but the proof works in arbitrary characteristic). □

References

[ABGV11] A. Auel, E. Brussel, S. Garibaldi and U. Vishne, *Open problems on Central Simple Algebras*, Transformation Groups, Vol. **16**(1), 219-264, (2011).

[Am55] S.A. Amitsur, *Division algebras. A survey*, Algebraistsf homage: papers in ring theory and related topics (New Haven, Conn., 1981), Contemp. Math., vol. **13**, Amer. Math. Soc., Providence, R.I., 1982, pp. 3–26.

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

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

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

[CGR08] V. Chernousov, Ph. Gille, Z. Reichstein, *Reduction of structure for torsors over semilocal rings*, Manuscripta. Math **126** (2008), 465–480.

[Du10] A. Duncan, *Essential dimensions of A_7 and S_7*. Math. Res. Lett. **17**, no. 2 (2010), 263–266.

[Ja89] J. Jacobson, *Basic algebra II*, 2nd ed., New York, NY: W. H. Freeman and Company. xvii, 686 p. (1989).

[Ka00] N. Karpenko, *On anisotropy of orthogonal involutions*, J. Ramanujan Math. Soc. **15**, no. 1 (2000), 1–22.

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

[Le04] N. Lemire, *Essential dimension of algebraic groups and integral representations of Weyl groups*, Transform. Groups **9** (2004), no. 4, 337–379.

[LRRS03] M. Lorenz, Z. Reichstein, L. Rowen, and D. Saltman, *Fields of definition for division algebras*, J. London Math. Soc. (2) **68** (2003), no. 3, 651–670.

[Lö10] R. Lötscher, *Contributions to the essential dimension of finite and algebraic groups*, Ph.D. thesis, Universität Basel, 2010
Electronic: http://edoc.unibas.ch/1147/1/DissertationEdocCC.pdf.

[Lö12] R. Lötscher, *Essential dimension of involutions and subalgebras*, Isr. J. Math. **192**, Part A, 325–346 (2012).

[Ma14] M. MacDonald, *Upper bounds for the essential dimension of E_7*, preprint (2014).

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

[Me10] A. Merkurjev, *A lower bound on the essential dimension of simple algebras*, Algebra Number Theory **4**, no.8, (2010), 1055–1076.

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

[Pr67] C. Procesi, *Non-commutative affine rings*, Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I (8) **8** (1967), 237–255.

[Re00] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transform. Groups **5**, no. 3, (2000), 265–304.

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

[SGA3] P. Gabriel, *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.

[Sp98] T. A. Springer, Linear algebraic groups, 2nd ed., Progress in Mathematics (Boston, MA, 1998), Birkhäuser, Boston, 1998.

Roland Lötscher
Mathematisches Institut der Ludwig-Maximilians-Universität München,
Theresienstrasse 39, D-80333 München, Germany
E-mail address: Roland.Loetscher@mathematik.uni-muenchen.de