ESSENTIAL DIMENSION OF SIMPLE ALGEBRAS WITH INVOLUTIONS

SANGHOON BAEK

Abstract. Let $1 \leq m \leq n$ be integers with $m|n$ and $\mathsf{Alg}_{n,m}$ the class of central simple algebras of degree n and exponent dividing m. In this paper, we find upper bounds for the essential (2)-dimension of $\mathsf{Alg}_{n,2}$. Moreover, we find a stronger upper bound for the essential 2-dimension of $\mathsf{Alg}_{n,2}$ over a field F of $\mathrm{char}(F) \neq 2$. As a result, we show that $\mathrm{ed}_2(\mathsf{Alg}_{16,2}) = 24$ over a field F of $\mathrm{char}(F) \neq 2$.

1. Introduction

Let $\mathcal{T} : \mathsf{Fields}/F \to \mathsf{Sets}$ be a functor from the category Fields/F of field extensions over F to the category Sets of sets. For fields $E, E' \in \mathsf{Fields}/F$, a field homomorphism $f : E \to E'$ over F and $\alpha \in \mathcal{T}(E)$, we write $\alpha_{E'}$ for the image of α under the morphism $\mathcal{T}(f) : \mathcal{T}(E) \to \mathcal{T}(E')$.

Let $E \in \mathsf{Fields}/F$ and $K \subset E$ a subfield over F. An element $\alpha \in \mathcal{T}(E)$ is said to be *defined over* K and K is called a *field of definition of* α if there exists an element $\beta \in \mathcal{T}(K)$ such that $\beta_E = \alpha$. The *essential dimension of* α is $\mathrm{ed}(\alpha) = \min\{\mathrm{tr.deg}_F(K)\}$ over all fields of definition K of α. The *essential dimension of the functor* $\mathcal{T}$ is $\mathrm{ed}(\mathcal{T}) = \sup\{\mathrm{ed}(\alpha)\}$, where the supremum is taken over all fields $E \in \mathsf{Fields}/F$ and all $\alpha \in \mathcal{T}(E)$. Hence, the essential dimension of an algebraic structure $\mathcal{T}$ measures the complexity of the structure in terms of the smallest number of parameters required to define the structure over a field extension of F.

Let p be a prime integer. The *essential p-dimension of* α is $\mathrm{ed}_p(\alpha) = \min\{\mathrm{ed}(\alpha_L)\}$, where L ranges over all field extensions of E of degree prime to p. In other words, $\mathrm{ed}_p(\alpha) = \min\{\mathrm{tr.deg}_F(K)\}$, where the minimum is taken over all field extensions L/E of prime to p and all subextensions K/F of L which are field of definition of α_L. Hence, $\mathrm{ed}(\alpha) \geq \mathrm{ed}_p(\alpha)$ for all p. The *essential p-dimension of* $\mathcal{F}$ is $\mathrm{ed}_p(\mathcal{T}) = \sup\{\mathrm{ed}_p(\alpha)\}$, where the supremum ranges over all fields $E \in \mathsf{Fields}/F$ and all $\alpha \in \mathcal{T}(E)$.

Let G be an algebraic group over F. The *essential dimension* $\mathrm{ed}(G)$ (respectively, *essential p-dimension* $\mathrm{ed}_p(G)$) of G is defined to be $\mathrm{ed}(H^1(-, G))$ (respectively, $\mathrm{ed}_p(H^1(-, G))$), where $H^1(E, G)$ is the Galois cohomology set (equivalently, the set of isomorphism classes of G-torsors) over a field extension E of F.

For every integer $n \geq 1$, a divisor m of n and any field extension E/F, let $\mathsf{Alg}_{n,m}(E)$ denote the set of isomorphism classes of central simple E-algebras of degree n and exponent dividing m. Then, for any field extension E/F, there is

a natural bijection between $H^1(E, \mathbf{GL}_n/\boldsymbol{\mu}_m)$ and $\mathsf{Alg}_{n,m}(E)$ (see [1, Example 1.1]), thus $\mathrm{ed}(\mathsf{Alg}_{n,m}) = \mathrm{ed}(\mathbf{GL}_n/\boldsymbol{\mu}_m)$ and $\mathrm{ed}_p(\mathsf{Alg}_{n,m}) = \mathrm{ed}_p(\mathbf{GL}_n/\boldsymbol{\mu}_m)$.

In this paper, we compute upper bounds for the essential dimension of $\mathsf{Alg}_{n,2}$. By a theorem of Albert, a central simple algebra has exponent dividing 2 if and only if it admits an involution of the first kind (see [3, Theorem 3.1]). Thus, any algebra A in $\mathsf{Alg}_{n,2}(K)$ for any field extension K/F has involutions of the first kind. Moreover, such A has involutions of both symplectic and orthogonal types (see [3, Corollary 2.8(2)]). By the primary decomposition theorem and [2, Section 6], we have $\mathrm{ed}(\mathsf{Alg}_{n,2}) = \mathrm{ed}(\mathsf{Alg}_{2^r,2})$ and $\mathrm{ed}_2(\mathsf{Alg}_{n,2}) = \mathrm{ed}_2(\mathsf{Alg}_{2^r,2})$, where 2^r is the largest power of 2 dividing n. Hence, we may assume that n is a power of 2.

By [2, Remark 8.2 and Corollary 8.3], $\mathrm{ed}_2(\mathsf{Alg}_{4,2}) = \mathrm{ed}(\mathsf{Alg}_{4,2}) = 4$ and $\mathrm{ed}_2(\mathsf{Alg}_{8,2}) = \mathrm{ed}(\mathsf{Alg}_{8,2}) = 8$ over a field F of $\mathrm{char}(F) \neq 2$. In general, by [2, Theorem], the following bounds were established over a field F of $\mathrm{char}(F) \neq 2$:

$$2^{r-1}(r-1) \leq \mathrm{ed}_2(\mathsf{Alg}_{2^r,2}) \leq 2^{r-1}(2^{r-1}+1) \text{ for all } r \geq 2.$$

In the present paper, we find an upper bound $n(n-1)/2$ for the essential dimension of $\mathsf{Alg}_{n,2}$ in Corollary 2.2. Moreover, we find an upper bound 2^{2r-2} for the essential 2-dimension of $\mathsf{Alg}_{2^r,2}$ in Corollary 2.4. Both upper bounds are valid over an arbitrary field F. In particular, the bound 2^{2r-2} improves the bound $2^{2r-2} + 2^{r-1}$ as above.

Using involutions of the first kind, we further improve the upper bound 2^{2r-2} as follows:

Theorem. *Let F be a field of characteristic different from 2. Then, for any integers $r \geq 3$,*

$$\mathrm{ed}_2(\mathsf{Alg}_{2^r,2}) \ \leq \ 2^{r-1}(2^{r-3}+1).$$

As a result, we find the essential 2-dimension of $\mathsf{Alg}_{16,2}$:

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

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

Remark 1.1. Recently, V. Chernousov and A. Merkurjev proved that

$$\mathrm{ed}_p(\mathbf{SL}_{p^r}/\boldsymbol{\mu}_{p^s}) = \mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s}) + 1$$

for any $0 \neq s < r$ over a field of $\mathrm{char}(F) \neq p$ (this result is communicated to the author by A. Merkurjev). Therefore, the computation of essential p-dimension of split simple group of type A_{p^r-1} is reduced to the computation of $\mathrm{ed}_p(\mathsf{Alg}_{p^r,p^s})$. In particular, we have $\mathrm{ed}_2(\mathbf{SL}_{16}/\boldsymbol{\mu}_2) = 25$ over a field of $\mathrm{char}(F) \neq 2$.

Acknowledgements: I am grateful to my advisor A. Merkurjev for many useful discussions and support and to Z. Reichstein for helpful comments. Section 2 of this paper is based on the author's doctoral thesis at the University of California at Los Angeles.

2. Upper bounds for the essential dimension of $\mathsf{Alg}_{n,2}$

Let G be a reductive algebraic group over F, let T be a maximal torus of G and let N be the normalizer of T in G. Then the canonical map

$$H^1(K, N) \to H^1(K, G)$$

is surjective for any field extension K/F by Springer's Lemma ([7, III.4 Lemma 6]). Therefore, we have

$$\mathrm{ed}(G) \leq \mathrm{ed}(N) \tag{1}$$

by [4, Proposition 1.3].

For any integer $n \geq 2$, consider a reductive group $\mathbf{GL}_n/\boldsymbol{\mu}_2$ and the maximal torus $T_{n,2} := \mathbb{G}_m^n/\boldsymbol{\mu}_2$ in the group.

Lemma 2.1. *Let F be an arbitrary base field and S_n be the symmetric group on n elements. Then for any $n \geq 3$, we have*

$$\mathrm{ed}(T_{n,2} \rtimes S_n) \leq (n^2 - n)/2.$$

Proof. Note that the character group $(T_{n,2})^*$ is isomorphic to

$$\{(t_1, \cdots, t_n) \in \mathbb{Z}^n |\ t_1 + \cdots + t_n = 0 \text{ in } \mathbb{Z}/2\mathbb{Z}\}.$$

Let $e_{i,j} = (0, \cdots, 1, \cdots, -1, 0)$ be an element of $(T_{n,2})^*$, where 1 and -1 are placed in the ith and jth positions respectively for $1 \leq i \neq j \leq n$ and 0's are placed in other positions. Similarly, let $f_{i,j} = (0, \cdots, 1, \cdots, 1, 0)$, where 1's are placed in the ith and jth positions for $1 \leq i \neq j \leq n$ and 0's are placed in other positions and let $g_k = (0, \cdots, -2, \cdots, 0)$ as an element of $(T_{n,2})^*$, where -2 is placed in the kth position for $1 \leq k \leq n$ and 0's are placed in other positions.

Let X be a set consisting of $f_{i,j}$ and g_k for all $1 \leq i \neq j \leq n$ and all $1 \leq k \leq n$. Then X is a S_n-invariant subset of $(T_{n,2})^*$ and $|X| = |f_{i,j}| + |g_k| = (n^2 - n)/2 + n$.

It is clear that $e_{i,j}$ and $f_{i,j}$ generate $(T_{n,2})^*$ as an abelian group, as the indices i and j run over 1 to n. Since $f_{i,j} + g_j = e_{i,j}$, X generates $(T_{n,2})^*$ as an abelian group and hence we have a surjective S_n-equivariant homomorphism $\nu : \mathbb{Z}[X] \to (T_{n,2})^*$ taking $f_{i,j}$ and g_k to themselves.

We show that S_n acts faithfully on $\mathrm{Ker}(\nu)$. Let σ be a nontrivial element of S_n. Then there exists $1 \leq i_0 \leq n$ such that $\sigma(i_0) \neq i_0$. Choose a $1 \leq j_0 \leq n$ which is different from $\sigma(i_0)$ and i_0. Then σ does not fix $2f_{i_0,j_0} + g_{i_0} + g_{j_0} \in \mathrm{Ker}(\nu)$. By [5, Lemma 3.3], $\mathrm{ed}(T_{n,2} \rtimes S_n) \leq (n^2 - n)/2 + n - \mathrm{rank}((T_{n,2})^*) = (n^2 - n)/2$.

□

By (1), we have an upper bound for $\mathrm{ed}(\mathsf{Alg}_{n,2})$ as follows:

Corollary 2.2. *Let F be an arbitrary base field. Then for any $n \geq 3$,*

$$\mathrm{ed}(\mathsf{Alg}_{n,2}) \leq (n^2 - n)/2.$$

Let P_n be a Sylow 2-subgroup of the symmetric group S_n on n elements. In the following Lemma, we compute an upper bound for the essential dimension of $T_{2^r,2} \rtimes P_{2^r}$.

Lemma 2.3. *Let F be an arbitrary base field. Then for any $r \geq 2$, we have*

$$\mathrm{ed}(T_{2^r,2} \rtimes P_{2^r}) \leq 2^{2r-2},$$

where P_{2^r} is a Sylow 2-subgroup of S_{2^r}.

Proof. Note that a Sylow 2-subgroup P_{2^r} of S_{2^r} is isomorphic to $(P_{2^{r-1}})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Consider the $e_{i,j}$, $f_{i,j}$ and g_k as in the proof of Lemma 2.1. We divide the set of integers $\{1, 2, \cdots, 2^r\}$ into two subsets $\Lambda_1 := \{1, 2, \cdots, 2^{r-1}\}$ and $\Lambda_2 := \{2^{r-1}+1, 2^{r-1}+2, \cdots, 2^r\}$. Let X be a set consisting of $f_{i,j}$ and g_k for all $1 \leq i \neq j \leq 2^r$ such that i and j are placed in different Λ_l's and all $1 \leq k \leq 2^r$, where l is either 0 or 1. Then X is a P_{2^r}-invariant subset of $(T_{2^r,2})^*$ and $|X| = 2^{2r-2} + 2^r$.

It is clear that $e_{i,j}$ and $f_{i,j}$ generate $(T_{2^r,2})^*$ as an abelian group, as the indices i and j run over 1 to 2^r. Note that $f_{i,j} = f_{i,k} + f_{j,k} + g_k$ for all i and j which are in the same Λ_l's, where l is either 1 or 2. As

$$e_{i,j} = \begin{cases} f_{i,j} + g_j & \text{if } i \text{ and } j \text{ are in different } \Lambda_l\text{'s,} \\ f_{i,k} + f_{j,k} + g_j + g_k & \text{otherwise,} \end{cases}$$

X generates $(T_{2^r,2})^*$ as an abelian group and hence we have a surjective P_{2^r}-equivariant homomorphism $\nu : \mathbb{Z}[X] \to (T_{2^r,2})^*$ taking $f_{i,j}$ and g_k to themselves.

We show that P_{2^r} acts faithfully on $\mathrm{Ker}(\nu)$. Note that the center of P_{2^r}, which is generated by $\sigma := (1,2)(3,4)\cdots(2^r-1, 2^r)$ and it is enough to show that σ acts faithfully on $\mathrm{Ker}(\nu)$. In fact, σ does not fix the non-zero element $2f_{1,2^{r-1}+1} + g_1 + g_{2^{r-1}+1} \in \mathbb{Z}[X]$. By [5, Lemma 3.3], we have

$$\mathrm{ed}(T_{2^r,2} \rtimes P_{2^r}) \leq 2^{2r-2} + 2^r - \mathrm{rank}((T_{2^r,2})^*) = 2^{2r-2}.$$

□

As $(2, [T_{2^r,2} \rtimes S_{2^r} : T_{2^r,2} \rtimes P_{2^r}]) = 1$, we have $\mathrm{ed}_2(T_{2^r,2} \rtimes S_{2^r}) = \mathrm{ed}_2(T_{2^r,2} \rtimes P_{2^r})$ by [5, Lemma 4.1]. Therefore, by Lemma 2.3, we have the following Corollary:

Corollary 2.4. *Let F be an arbitrary base field. Then for any $r \geq 2$,*

$$\mathrm{ed}_2(\mathsf{Alg}_{2^r,2}) \leq 2^{2r-2}.$$

3. Algebras with involutions

Let A be a central simple algebra over F. For any $a \in A^\times$, we denote the inner automorphism of A by $\mathrm{Int}(a)$: $\mathrm{Int}(a)(x) = axa^{-1}$ for all $x \in A$. For any subalgebra B of A, we write $C_A(B)$ for the centralizer of B in A. The following Lemma characterizes all involutions of the first kind on A.

Lemma 3.1. [3, Proposition 2.7] *Let F be a field of* $\mathrm{char}(F) \neq 2$*, A be a central simple algebra over F and σ be an involution of the first kind on A. Then every involution σ' of the first kind on A is of the form* $\mathrm{Int}(a) \circ \sigma$ *for some $a \in A^\times$ uniquely determined up to a factor in $F^\times$, such that $\sigma(a) = \pm a$. Moreover, σ and σ' are of the same type if and only if $\sigma(a) = a$.*

We use the following Lemma for extension of involutions:

Lemma 3.2. [3, Theorem 4.14] *Let F be a field of* $\mathrm{char}(F) \neq 2$*, A be a central simple algebra over F with an involution σ of the first kind, and B be a simple subalgebra of A with an involution τ such that $\tau|_F = \sigma|_F$. Then A has involutions of both types whose restriction to B is τ, unless τ is of the first kind and* $\deg(C_A(B))$ *is odd.*

From now we assume that the base field F is 2-closed (i.e., every finite extension of F is separable of degree a power of 2) and is of characteristic different from 2.

Proposition 3.3. *Let $r \geq 3$ be an integer, F a 2-closed field such that* $\mathrm{char}(F) \neq 2$ *and D a division F-algebra of degree 2^r and exponent 2. Then for any biquadratic field extension K_1K_2/F in D with quadratic field extensions K_1/F and K_2/F there exists a quadratic extension K_3/F in D such that $K_1K_2K_3/F$ is a triquadratic extension in D.*

Proof. By [3, Theorem 3.1(1)], D has an involution of the first kind σ. Let τ_1 and τ_2 be two distinct nontrivial automorphisms of the field K_1K_2. As $\sigma|_F = \tau_i|_F$ for any $i = 1, 2$, there are two distinct involutions σ_1 and σ_2 of the same type on A such that $\sigma_i|_{K_1K_2} = \tau_i$ by Lemma 3.2.

By Lemma 3.1, there exists $d \in D^\times$ such that $\sigma_1 = \mathrm{Int}(d) \circ \sigma_2$ and $\sigma_i(d) = d$ for all $i = 1, 2$. In particular, d^2 commutes with K_1 and K_2 and $F(d^2) \cap K_1K_2 = F$. If $F(d^2) \neq F$, then $F(d^2)$ contains a quadratic extension K_3 over F by [6, Proposition 1.1]. Hence we a triquadratic extension $K_1K_2K_3$ in D.

Suppose that $d^2 \in F$. Then there exist quaternion subalgebras $Q_1 := (K_1, d^2)$ and $Q_2 := (K_2, d^2)$ of D. As $\mathrm{ind}(C_D(Q_1 \otimes Q_2)) \geq 2$, $C_D(Q_1 \otimes Q_2)$ contains a quadratic extension K_3/F by [6, Proposition 1.1]. Therefore, we have $K_1K_2K_3 = K_1 \otimes K_2 \otimes K_3 \subset Q_1 \otimes Q_2 \otimes C_D(Q_1 \otimes Q_2) = D$. □

Corollary 3.4. *Let $r \geq 3$ be an integer and F be a 2-closed field such that* $\mathrm{char}(F) \neq 2$*. Then for any division F-algebra D of degree 2^r and exponent 2 and an étale subalgebra $K_1K_2 := K_1 \otimes K_2$ of D such that* $\dim_F(K_i) = 2$ *for $i = 1, 2$, there exists a maximal étale subalgebra $K_1K_2K := K_1 \otimes K_2 \otimes K$ of D with* $\dim_F(K) = 2^{r-2}$.

Proof. By Proposition 3.3, there exists a triquadratic field extension $K_1K_2K_3$ over F. Induction on r. If $r = 3$, then $K = K_3$ satisfies the conclusion of Corollary. For $r \geq 3$, the centralizer $C_D(K_3)$ is a division K_3-algebra of degree 2^{r-1}. By the induction hypothesis with K_1K_3/K_3 and K_2K_3/K_3, $C_D(K_3)$ contains a subfield K/F with $[K : K_3] = 2^{r-3}$. Hence D contains a field extension K_1K_2K over F such that $\dim_F(K) = 2^{r-3} \cdot 2$. □

4. Essential 2-dimension of $\mathsf{Alg}_{n,2}$

Let $n \geq 2$ be an integer, G be a subgroup of S_n and X be a G-set of n elements (G acts on X by permutation). For any divisor m of n, we consider the surjective G-modules homomorphism $\bar{\varepsilon} : \mathbb{Z}[X] \to \mathbb{Z}/m\mathbb{Z}$, defined by $\bar{\varepsilon}(x) = \varepsilon(x) + m\mathbb{Z}$, where $\varepsilon : \mathbb{Z}[X] \to \mathbb{Z}$ is the *augmentation homomorphism* given by $\varepsilon(x) = 1$ for all $x \in X$. Set $J = \mathrm{Ker}(\bar{\varepsilon})$. Then we have an exact sequence

$$0 \to J \to \mathbb{Z}[X] \xrightarrow{\bar{\varepsilon}} \mathbb{Z}/m\mathbb{Z} \to 0. \tag{2}$$

We shall need the following lemma (see also the proof of [2, Theorem 8.1]):

Lemma 4.1. *Let F be a field of $\mathrm{char}(F) \not| \, n$ and $T = \mathrm{Spec}\, F[J]$ be the split torus with the character group J. Then*

$$H^1(F, T \rtimes G) = \coprod_{\mathrm{Gal}(E/F)=G} \mathrm{Br}_m(E/F),$$

where the disjoint union is taken over all isomorphism classes of Galois G-algebras E/F.

Proof. Let T_γ (respectively, G_γ) be the twist of T (respectively, G) by the 1-cocycle $\gamma \in Z^1(F, G)$. Then by [3, Proposition 28.11], there is a natural bijection between the fiber of $H^1(F, T \rtimes G) \to H^1(F, G)$ over $[\gamma]$ and the orbit set of the group $G_\gamma(F)$ in $H^1(F, T_\gamma)$, i.e.,

$$H^1(F, T \rtimes G) \simeq \coprod H^1(F, T_\gamma)/G_\gamma(F), \tag{3}$$

where the coproduct is taken over all $[\gamma] \in H^1(F, G)$.

Let E be the corresponding Galois G-algebra over F to γ. From (2), we have the corresponding exact sequence of algebraic groups

$$1 \to \boldsymbol{\mu}_m \to \mathbb{G}_m^n \to T \to 1$$

and then the exact sequence

$$1 \to \boldsymbol{\mu}_m \to R_{E/F}(\mathbb{G}_{m,E}) \to T_\gamma \to 1, \tag{4}$$

each term of which is twisted by γ. The exact sequence (4) induces an exact sequence of Galois cohomology

$$1 \to H^1(F, T_\gamma) \to H^2(F, \boldsymbol{\mu}_m) = \mathrm{Br}_m(F) \to H^2(E, \mathbb{G}_{m,E}) = \mathrm{Br}(E) \tag{5}$$

by Eckmann-Faddeev-Shapiro's Lemma and Hilbert's 90. The G-action on $R_{E/F}(\mathbb{G}_{m,E})$ restricts to the trivial action on the subgroup $\boldsymbol{\mu}_m$. Let $\sigma \in G_\gamma(F)$ acts on $T_\gamma = R_{E/F}(\mathbb{G}_{m,E})/\boldsymbol{\mu}_m$. The action of σ and (5) induce the following diagram

$$\begin{array}{ccc} H^1(F, T_\gamma) & \hookrightarrow & H^2(F, \boldsymbol{\mu}_m) \\ \downarrow{\scriptstyle \sigma^*} & & \| \\ H^1(F, T_\gamma) & \hookrightarrow & H^2(F, \boldsymbol{\mu}_m). \end{array}$$

Therefore, $G_\gamma(F)$ acts trivially on $H^1(F, T_\gamma)$, hence the result follows by (3). □

Let $r \geq 3$ be an integer. Let $G_r = S_2 \times S_2 \times S_{2^{r-2}}$ be a subgroup of the symmetric group S_{2^r} on 2^r elements and let $H_r = S_2 \times S_2 \times P_{2^{r-2}}$ be a Sylow 2-subgroup of G_r, where $P_{2^{r-2}}$ is a Sylow 2-subgroup of $S_{2^{r-2}}$. Let X_r be a G_r-set of 2^r elements (G_r acts on X_r by permutations). The action of H_r may be described as follows: we subdivide the integers $1, 2, \cdots, 2^r$ into four blocks B_1, B_2, B_3, B_4 such that each block consists of 2^{r-2} consecutive integers. The $P_{2^{r-2}}$ permutes the elements of B_i for all $1 \leq i \leq 4$, S_2 interchanges B_{2i-1} and B_{2i} for all $i = 1, 2$, and another S_2 interchanges $B_1 \cup B_2$ and $B_3 \cup B_4$.

We set $J_r = \mathrm{Ker}(\mathbb{Z}[X_r] \xrightarrow{\bar{\varepsilon}} \mathbb{Z}/2\mathbb{Z})$, where $\bar{\varepsilon}$ is the map with $m = 2$ as in (2). Applying Lemma 4.1 with $n = 2^r$, $m = 2$, $G = G_r$, $X = X_r$, $J = J_r$, and $T = T_r := \mathrm{Spec}(F[J_r])$, we have a morphism

$$\theta : H^1(-, T_r \rtimes G_r) \to \mathsf{Alg}_{2^r,2}$$

defined by $\theta(N)([A]) = B$ for a field extension N over F, where $[A] \in \mathrm{Br}_2(L/N)$ for some field extension L/N with $\mathrm{Gal}(L/N) = G_r$ and B is the central simple N-algebra of degree 2^r such that $[A] = [B]$ in $\mathrm{Br}_2(L/N)$.

We also have a morphism

$$\Theta : H^1(-, T_r \rtimes G_r) \coprod \Big(\coprod_{1 \leq i \leq r-1} \mathsf{Alg}_{2^i,2} \Big) \to \mathsf{Alg}_{2^r,2} \tag{6}$$

defined by

$$[A] \mapsto \theta(N)([A]), \quad A_i \mapsto M_{2^{r-i}}(A_i)$$

over a field extension N over F, where $A_i \in \mathsf{Alg}_{2^i,2}(N)$ for $1 \leq i \leq r-1$.

Lemma 4.2. *If the base field F is 2-closed and is of characteristic different 2, then Θ is surjective.*

Proof. We show that $\Theta(N)$ is surjective for a field extension N/F. By the definition of Θ, we only need to check the surjectivity for a division N-algebra D of degree 2^r and exponent 2. By [6, Theorem 1.2], there exists an étale subalgebra K_1K_2 in D such that $\dim_N(K_i) = 2$ for $i = 1, 2$. By Corollary 3.4, there exists a maximal étale subalgebra K_1K_2K in D such that $\dim_N(K) = 2^{r-2}$. Hence θ is surjective, so is Θ. □

Example 4.3. (see [2, Remark 3.10]) Let $r = 3$. Then $G_3 = H_3 = S_2 \times S_2 \times S_2 := \langle \tau_1 \rangle \times \langle \tau_2 \rangle \times \langle \tau_3 \rangle$. As the action of H_3 on X_3 is simply transitive, $X_3 \simeq H_3$ as H_3-sets, hence J_3 is generated by 2 and $\tau_i - 1$ for $i = 1, 2, 3$. Set $\Lambda_3 := \mathbb{Z}[H_3/\langle \tau_1 \rangle] \oplus \mathbb{Z}[H_3/\langle \tau_2 \rangle] \oplus \mathbb{Z}[H_3/\langle \tau_3 \rangle] \oplus \mathbb{Z}[H_3/\langle \tau_1\tau_2 \rangle]$. Define a map $\rho : \Lambda_3 \to J_3$ by

$$\rho(\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_4}) = \sum_{i=1}^{3} (\tau_i + 1)x_i + (\tau_1\tau_2 + 1)x_4.$$

As $2 = (\tau_1\tau_2 + 1) - \tau_1(\tau_2 + 1) + (\tau_1 + 1)$, ρ is surjective. It is easy to check that H_3 acts on $\mathrm{Ker}(\rho)$ faithfully. Therefore, by [5, Lemma 3.3] and [4, Corollary 4.2], $\mathrm{ed}_2(\mathsf{Alg}_{8,2}) \leq 4 + 4 + 4 + 4 - 2^3 = 8$.

For an $x \in X_r$, let $H_{r,x}$ be the stabilizer of x in $H_r = S_2 \times S_2 \times P_{2^{r-2}} := \langle \tau_1 \rangle \times \langle \tau_2 \rangle \times P_{2^{r-2}}$. We set $P_{2^{r-2}} = (P_{2^{r-3}})^2 \rtimes \langle \tau_r \rangle$.

Lemma 4.4. *For any $r \geq 3$ and any $x \in X_r$, we have*

(1) $H_{r,x} = H_{r-1,x} \times P_{2^{r-3}}$.
(2) $H_r = \langle \tau_1, \tau_2, \tau_r, H_{r,x} \rangle$.
(3) $J_r = \langle 2x, \tau_1 x - x, \tau_2 x - x, \tau_r x - x \rangle$.
(4) $\tau_r H_{r,x} \tau_r \cap H_{r,x} = H_{r-1,x} \times H_{r-1,x}$.

Proof. (1) The stabilizer of x in H_r is the stabilizer of x under the action of $P_{2^{r-2}}$ on the block B_i containing x for some i. As $P_{2^{r-2}} = (P_{2^{r-3}})^2 \rtimes \langle \tau_r \rangle$, the stabilizer of x in $P_{2^{r-2}}$ is $H_{r-1,x} \times P_{2^{r-3}}$.

(2) Induction on r. The case $r = 3$ comes from Example 4.3. By induction hypothesis we have $P_{2^{r-3}} = \langle \tau_{r-1}, H_{r-1,x} \rangle$. As τ_{r-1} is generated by τ_r and $P_{2^{r-3}}$, the result follows immediately.

(3) As H_r acts on X_r transitively, the result follows from Lemma 4.4 (2) and the sequence (2).

(4) As $\tau_r H_{r,x} \tau_r = H_{r,\tau_r(x)}$, the result follows from (1). □

Theorem 4.5. *For any $r \geq 3$, there exists a $2^{r-1}(2^{r-3}+3)$-dimensional generically free representation for $T_r \rtimes H_r$. Hence* $\mathrm{ed}_2(\mathsf{Alg}_{2^r,2}) \leq 2^{r-1}(2^{r-3}+1)$.

Proof. For $r \geq 3$ and $x \in X_r$, we set

$$\begin{aligned}\Lambda_r := {} & \mathbb{Z}[H_r/\langle \tau_1 \rangle \times H_{r,x}] \oplus \mathbb{Z}[H_r/\langle \tau_2 \rangle \times H_{r,x}] \oplus \mathbb{Z}[H_r/\langle \tau_1\tau_2 \rangle \times H_{r,x}] \\ & \oplus \mathbb{Z}[H_r/(\tau_r H_{r,x} \tau_r \cap H_{r,x}) \rtimes \langle \tau_r \rangle].\end{aligned}$$

Define a map $\rho : \Lambda_r \to J_r$ by taking a generator of the first component (respectively, the second component) of Λ_r to $\tau_1 x + x$ (respectively, $\tau_2 x + x$), a generator of the third component of Λ_r to $\tau_1\tau_2 x + x$, and a generator of the last component of Λ_r to $\tau_r x + x$. By construction, this map is well defined. As $2x = (\tau_1\tau_2 x + x) - \tau_1(\tau_2 x + x) + (\tau_1 x + x)$, ρ is surjective by Lemma 4.4 (3).

As H_r acts faithfully on $\mathrm{Ker}(\rho)$ by Lemma 4.6, there exists a generically free representation for $T_r \rtimes H_r$ by [5, Lemma 3.3]. Therefore, by [4, Corollary 4.2], we have

$$\begin{aligned}\mathrm{ed}_2(T_r \rtimes H_r) \leq {} & \mathrm{rank}(\mathbb{Z}[H_r/\langle \tau_1 \rangle \times H_{r,x}]) + \mathrm{rank}(\mathbb{Z}[H_r/\langle \tau_2 \rangle \times H_{r,x}]) \\ & + \mathrm{rank}(\mathbb{Z}[H_r/\langle \tau_1\tau_2 \rangle \times H_{r,x}]) + \mathrm{rank}(\mathbb{Z}[H_r/(\tau_r H_{r,x} \tau_r \cap H_{r,x}) \rtimes \langle \tau_r \rangle]) \\ & - \mathrm{rank}(J_r) \\ = {} & 2^{r-1} + 2^{r-1} + 2^{r-1} + 2^{r+(r-1)-2-1} - 2^r \text{ (by Lemma 4.4(1),(4))} \\ = {} & 2^{r-1} + 2^{2r-4}.\end{aligned}$$

By [5, Lemma 4.1], $\mathrm{ed}_2(T_r \rtimes G_r) = \mathrm{ed}_2(T_r \rtimes H_r)$. As the morphism Θ in (6) is surjective by Lemma 4.2, we get

$$\mathrm{ed}_2(\mathsf{Alg}_{2^r,2}) \leq \max\{\mathrm{ed}_2(T_r \rtimes G_r), \mathrm{ed}_2(\mathsf{Alg}_{2,2}), \cdots, \mathrm{ed}_2(\mathsf{Alg}_{2^{r-1},2})\}.$$

By induction on r, we finally have $\mathrm{ed}_2(\mathsf{Alg}_{2^r,2}) \leq \mathrm{ed}_2(T_r \rtimes G_r) \leq 2^{r-1} + 2^{2r-4}$.

□

Lemma 4.6. *Let $\rho : \Lambda_r \to J_r$ be the morphism in proof of Theorem 4.5. The action of H_r on* $\mathrm{Ker}(\rho)$ *is faithful.*

Proof. Note that $J_r \otimes \mathbb{Q} = \mathbb{Q}[X_r]$ by the exact sequence (2). Hence, by the exact sequence

$$\mathrm{Ker}(\rho) \to \Lambda_r \xrightarrow{\rho} J_r,$$

we have

$$\mathbb{Q}[X_r] \oplus (\mathrm{Ker}(\rho))_{\mathbb{Q}} = \mathbb{Q}[H_r/\langle\tau_1\rangle \times H_{r,x}] \oplus \mathbb{Q}[H_r/\langle\tau_2\rangle \times H_{r,x}] \oplus \mathbb{Q}[H_r/\langle\tau_1\tau_2\rangle \times H_{r,x}]$$
$$\oplus \mathbb{Q}[H_r/(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle]. \tag{7}$$

By the actions of τ_1 and τ_2, the natural map

$$i : \mathbb{Z}[X_r] \to \mathbb{Z}[X_r/\langle\tau_1\rangle] \oplus \mathbb{Z}[X_r/\langle\tau_2\rangle] \oplus \mathbb{Z}[X_r/\langle\tau_1\tau_2\rangle]$$

is injective, hence we get the exact sequence

$$0 \to \mathbb{Z}[X_r] \xrightarrow{i} \mathbb{Z}[X_r/\langle\tau_1\rangle] \oplus \mathbb{Z}[X_r/\langle\tau_2\rangle] \oplus \mathbb{Z}[X_r/\langle\tau_1\tau_2\rangle] \to \mathrm{Coker}(i) \to 0$$

and

$$\mathbb{Q}[X_r] \oplus (\mathrm{Coker}(i))_{\mathbb{Q}} = \mathbb{Q}[X_r/\langle\tau_1\rangle] \oplus \mathbb{Q}[X_r/\langle\tau_2\rangle] \oplus \mathbb{Q}[X_r/\langle\tau_1\tau_2\rangle]. \tag{8}$$

By (7) and (8), we have

$$(\mathrm{Ker}(\rho))_{\mathbb{Q}} = (\mathrm{Coker}(i))_{\mathbb{Q}} \oplus \mathbb{Q}[H_r/(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle],$$

thus it is enough to show that $H_r = \langle\tau_1\rangle \times \langle\tau_2\rangle \times [(P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle]$ acts faithfully on $Y_r := \mathbb{Q}[H_r/(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle]$:

Case 1: $h = \tau_i h'$ or $\tau_1\tau_2 h'' \in H_r$ for $i = 1, 2$ and $h', h'' \in (P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle$.

If $h = \tau_i h' \in H_r$ for some $h' \in (P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle$ and $i = 1, 2$, then $h\overline{\tau_i} = \overline{h'} \neq \overline{\tau_i}$ in Y_r. Similarly, if $h = \tau_1\tau_2 h'' \in H_r$ for some $h'' \in (P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle$, then $h\overline{\tau_1\tau_2} = \overline{h''} \neq \overline{\tau_1\tau_2}$ in Y_r.

Case 2: $h \in (P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle \backslash (\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle$.

If $h \in (P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle \backslash (\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle$, then $h\overline{1} = \overline{h} \neq \overline{1}$ in Y_r.

Case 3: $h \in (\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle \backslash (\tau_r H_{r,x}\tau_r \cap H_{r,x})$.

Let $h = h_1 h_2 \tau_r \in (H_{r-1,x} \times H_{r-1,x}) \rtimes \langle\tau_r\rangle$. We may assume that $h_1 \neq 1$. Choose a transposition $\delta \in P_{2^{r-3}}$ which does not fix x. Then $h\overline{\delta} = \overline{h_1 h_2 \tau_r \delta} = \overline{h_1 h_2 \delta' \tau_r} = \overline{\delta' h_1 h_2 \tau_r} = \overline{\delta'} \neq \overline{\delta}$, where δ' is the transposition such that $\tau_r\delta = \delta'\tau_r$.

Case 4: $h \in \tau_r H_{r,x}\tau_r \cap H_{r,x}$.

Let $h = h_1 h_2 \in H_{r-1,x} \times H_{r-1,x} = \tau_r H_{r,x}\tau_r \cap H_{r,x}$. We may assume that $h_1 \neq 1$. Let τ_{r-1} be the permutation which acts on the same block with h_1. Then $h\overline{\tau_{r-1}} = \overline{h_1\tau_{r-1}} \neq \overline{\tau_{r-1}}$ in Y_r.

This completes the proof of faithfulness.

□

Corollary 4.7. *Let F be a field of characteristic different* 2*. Then*

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

Proof. The lower bound $24 \leq \mathrm{ed}_2(\mathcal{A}lg_{16,2})$ follows from [2, Theorem 6.1]. Therefore, the statement follows from Theorem 4.5. □

References

[1] S. Baek and A. Merkurjev, *Invariants of simple algebras*, Manuscripta Math, Vol. 129, No. 4 (2009), 409–421.

[2] S. Baek and A. Merkurjev, *Essential dimension of central simple algebras*, to appear in Acta Math.

[3] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society, Providence, RI, 1998, With a preface in French by J. Tits.

[4] A. S. Merkurjev, *Essential dimension*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 299–325.

[5] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra and Number Theory **3** (2009), no. 4, 467–487.

[6] L. H. Rowen and D. J. Saltman, *Prime to p extensions of division algebra*, Israel J. Math. **78** (1992), no. 2-3, 197–207.

[7] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.

Department of Mathematics and Statistics, University of Ottawa, Canada
E-mail address: sbaek@uottawa.ca