Essential dimension of simple algebras with involutions

S. Baek

Abstract

Let $1 \leq m \leq n$ be integers with $m|n$ and $\mathrm{Alg}_{n,m}$ the class of central simple algebras of degree n and exponent dividing m. In this paper, we find new, improved upper bounds for the essential dimension and 2-dimension of $\mathrm{Alg}_{n,2}$. In particular, we show that $\mathrm{ed}_2(\mathrm{Alg}_{16,2}) = 24$ over a field F of characteristic different from 2.

1. *Introduction*

Let $\mathcal{T} : \mathrm{Fields}/F \to \mathrm{Sets}$ be a functor (called an *algebraic structure*) from the category Fields/F of field extensions over F to the category Sets of sets. For instance, $\mathcal{T}(E)$ with $E \in \mathrm{Fields}/F$ can be the sets of isomorphism classes of central simple E-algebras of degree n, étale E-algebras of rank n, quadratic forms over E of dimension n, torsors (principal homogeneous spaces) over E under a given algebraic group, etc. For fields $E, E' \in \mathrm{Fields}/F$, 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 $\mathcal{T}(f) : \mathcal{T}(E) \to \mathcal{T}(E')$.

The notion of essential dimension was introduced by J. Buhler and Z. Reichstein in [**5**] and was generalized to algebraic structures by A. Merkurjev in [**4**] and [**11**]. The essential dimension of an algebraic structure is defined to be the smallest number of parameters needed to define the structure.

Let $E \in \mathrm{Fields}/F$ 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 $E \in \mathrm{Fields}/F$ 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 fields of definition of α_L. Hence, $\mathrm{ed}(\alpha) \geq \mathrm{ed}_p(\alpha)$ and

2010 *Mathematics Subject Classification* 16K20 (primary), 16K50, 14L30, 20C10, 20G15 (secondary).

The work has been supported by Beckenbach Dissertation Fellowship at the University of California at Los Angeles, Neher's NSERC Discovery grant 008836-2006, and Zainoulline's NSERC Discovery grant 385795-2010 and Accelerator Supplement grant 396100-2010.

$\mathrm{ed}(\mathcal{T}) \geq \mathrm{ed}_p(\mathcal{T})$ for all p. The *essential p-dimension of $\mathcal{T}$* is

$$\mathrm{ed}_p(\mathcal{T}) = \sup\{\mathrm{ed}_p(\alpha)\},$$

where the supremum ranges over all fields $E \in \mathrm{Fields}/F$ 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 nonabelian cohomology set with respect to the finitely generated faithfully flat topology (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 $\mathrm{Alg}_{n,m}(E)$ denote the set of isomorphism classes of central simple E-algebras of degree n and exponent dividing m. Then, there is a natural bijection between $H^1(E, \mathbf{GL}_n / \boldsymbol{\mu}_m)$ and $\mathrm{Alg}_{n,m}(E)$ (see [**2**, Example 1.1]), thus

$$\mathrm{ed}(\mathrm{Alg}_{n,m}) = \mathrm{ed}(\mathbf{GL}_n / \boldsymbol{\mu}_m) \text{ and } \mathrm{ed}_p(\mathrm{Alg}_{n,m}) = \mathrm{ed}_p(\mathbf{GL}_n / \boldsymbol{\mu}_m).$$

In this paper, we compute upper bounds for the essential dimension and 2-dimension of $\mathrm{Alg}_{n,2}$. 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 [**6**, Theorem 3.1]). Thus, any algebra A in $\mathrm{Alg}_{n,2}(K)$ for any field extension K/F has involutions of the first kind. Moreover, such A has involutions of both symplectic and orthogonal types (see [**6**, Corollary 2.8(2)]). By the primary decomposition theorem and [**3**, Section 6], we have

$$\mathrm{ed}(\mathrm{Alg}_{n,2}) = \mathrm{ed}(\mathrm{Alg}_{2^r,2}) \text{ and } \mathrm{ed}_2(\mathrm{Alg}_{n,2}) = \mathrm{ed}_2(\mathrm{Alg}_{2^r,2}), \tag{1.1}$$

where 2^r is the largest power of 2 dividing n. Hence, we may assume that n is a power of 2.

By [**3**, Remark 8.2 and Corollary 8.3],

$$\mathrm{ed}_2(\mathrm{Alg}_{4,2}) = \mathrm{ed}(\mathrm{Alg}_{4,2}) = 4 \text{ and } \mathrm{ed}_2(\mathrm{Alg}_{8,2}) = \mathrm{ed}(\mathrm{Alg}_{8,2}) = 8$$

over a field F of $\mathrm{char}(F) \neq 2$. By [**1**, Theorem 1.1 and Theorem 1.2],

$$\mathrm{ed}_2(\mathrm{Alg}_{4,2}) = \mathrm{ed}(\mathrm{Alg}_{4,2}) = 3 \text{ and } 3 \leq \mathrm{ed}_2(\mathrm{Alg}_{8,2}) \leq \mathrm{ed}(\mathrm{Alg}_{8,2}) \leq 10$$

over a field F of $\mathrm{char}(F) = 2$. In general, in [**3**, Theorem], the following bounds were established over a field F of $\mathrm{char}(F) \neq 2$:

$$(\log_2(n) - 1)n/2 \leq \mathrm{ed}_2(\mathrm{Alg}_{n,2}) \leq n^2/4 + n/2 \text{ for all } n = 2^r \geq 4. \tag{1.2}$$

On the other hand, no upper bound for $\mathrm{ed}(\mathrm{Alg}_{n,2})$ was known for $n \geq 16$.

In the present paper, we find upper bounds for the essential dimension and 2-dimension of $\mathrm{Alg}_{n,2}$ over an arbitrary field as follows:

THEOREM 1.1. *Let F be an arbitrary field. Then, for any integers $n = 2^r \geq 8$,*

(i) $\mathrm{ed}(\mathbf{GL}_n / \boldsymbol{\mu}_2) = \mathrm{ed}(\mathrm{Alg}_{n,2}) \leq (n-1)(n-2)/2$ *if* $\mathrm{char}\, F \neq 2$,

(ii) $\mathrm{ed}_2(\mathbf{GL}_n / \boldsymbol{\mu}_2) = \mathrm{ed}_2(\mathrm{Alg}_{n,2}) \leq \begin{cases} n^2/4 & \textit{if } \mathrm{char}\, F = 2, \\ n^2/16 + n/2 & \textit{if } \mathrm{char}\, F \neq 2. \end{cases}$

We remark that our proof of the first inequality of (ii) in Theorem 1.1 holds for an arbitrary field.

COROLLARY 1.2. *Let F be a field of characteristic different from 2. Then*

$$\mathrm{ed}_2(\mathbf{GL}_{16} / \boldsymbol{\mu}_2) = \mathrm{ed}_2(\mathrm{Alg}_{16,2}) = 24.$$

Proof. The lower bound $24 \leq \mathrm{ed}_2(\mathrm{Alg}_{16,2})$ follows from (1.2). On the other hand, the upper bound $\mathrm{ed}_2(\mathrm{Alg}_{16,2}) \leq 24$ follows from Theorem 1.1(ii). □

The paper is organized as follows. In Section 2, we introduce a general strategy to find an upper bound for the essential dimension. In Section 3, we construct generically free representations for normalizers of maximal tori in $\mathbf{GL}_n / \boldsymbol{\mu}_2$ and $\mathbf{SL}_n / \boldsymbol{\mu}_2$, and a subgroup of the normalizer in $\mathbf{GL}_n / \boldsymbol{\mu}_2$ to prove Theorem 1.1(i) and the first part of (ii). The proof of the second part of (ii) in the main theorem is divided into two parts. In the first part, we study the structure of division algebras of exponent 2 using involutions and then construct a certain surjective morphism Θ. In the second part, we construct a generically free representation for a subgroup of the normalizer of the maximal torus of $\mathbf{GL}_n / \boldsymbol{\mu}_2$ to obtain the upper bound in the main theorem. In the last section, we relate the essential dimensions of $\mathrm{Alg}_{n,m}$ and of the split simple groups of type A_{n-1}.

To prove Theorem 1.1(i) we use Lemmas 6.1 and 3.1(ii). In fact, both Lemma 3.1(i) and (ii) give upper bounds for the essential dimension of $\mathbf{GL}_n / \boldsymbol{\mu}_2$, but the latter provides a better bound combined with Lemma 6.1. Before we compute both (i) and (ii) in Lemma 3.1, it is not clear which one gives a better bound. In particular, Lemma 3.1(ii) was obtained by N. Lemire in [**9**] under the assumption that the base field F is an algebraically closed of characteristic 0. Here we provide a different proof without the assumption on the base field F.

The general strategy (see Section 2) was first used by A. Meyer and Z. Reichstein in [**13**] and [**14**] to obtain an upper bound for the essential p-dimension of $\mathbf{SL}_{p^r} / \boldsymbol{\mu}_{p^r}$. In a subsequent paper [**17**] using a similar general method, A. Ruozzi obtained an improved upper bound. Based on his result, the upper bound in (1.2) was obtained. Here, the general strategy is further refined by methods of algebraic tori (Lemmas 5.1 and 5.2), combined with the structure of simple algebras of exponent 2 (Corollary 4.4), and the results provide a sharper upper bound for the essential dimension (Theorem 1.1(ii)).

2. *Preliminaries*

A morphism of functors $\mathcal{S} \to \mathcal{T}$ from Fields/F to Sets is called *surjective* if for any $E \in$ Fields/F, $\mathcal{S}(E) \to \mathcal{T}(E)$ is surjective. Such a surjective morphism gives an upper bound for the essential dimension of $\mathcal{T}$,

$$\mathrm{ed}(\mathcal{T}) \leq \mathrm{ed}(\mathcal{S}); \tag{2.1}$$

see [**4**, Lemma 1.9]. Similarly, a morphism $\mathcal{S} \to \mathcal{T}$ from Fields/F to Sets is called *p-surjective* if for any $E \in$ Fields/F and any $\alpha \in \mathcal{T}(E)$, there is a finite field extension L/E of degree prime to p such that $\alpha_L \in \mathrm{Im}(\mathcal{S}(L) \to \mathcal{T}(L))$. Then

$$\mathrm{ed}_p(\mathcal{T}) \leq \mathrm{ed}_p(\mathcal{S}); \tag{2.2}$$

see [**11**, Proposition 1.3]. Obviously, any surjective morphism is p-surjective for any prime p.

A field extension K/F is called *p-closed* (or *p-special*) if every finite extension of K is separable of degree a power of p. For a limit-preserving functor $\mathcal{T}$ (e.g. the Galois cohomology functor $H^1(-, G)$ for an algebraic group G over F), by [**10**, Lemma 3.3], we have

$$\mathrm{ed}_p(\mathcal{T}) = \mathrm{ed}_p(\mathcal{T}_K), \tag{2.3}$$

where K/F is a p-closed field and $\mathcal{T}_K$ is the restriction of $\mathcal{T}$ to Fields/K.

By (2.3), a surjective morphism $\mathcal{S} \to \mathcal{T}$ of limit-preserving functors over a p-closed field gives an upper bound for the essential p-dimension of $\mathcal{T}$,

$$\mathrm{ed}_p(\mathcal{T}) \leq \mathrm{ed}_p(\mathcal{S}).$$

In particular, if $\mathcal{T} = H^1(-, G)$ for an algebraic group G over F, then any *generically free* representation, i.e., a finite dimensional vector space V with G-action such that there exist a nonempty G-invariant open subset of V on which G acts freely, gives an upper bound for $\mathcal{T}$,

$$\operatorname{ed}_p(G) \leq \operatorname{ed}(G) \leq \dim(V) - \dim(G); \tag{2.4}$$

see [**15**, Theorem 3.4] and [**11**, Corollary 4.2]. Moreover, if G' is a closed subgroup of G such that $([G : G'], p) = 1$, then by [**13**, Lemma 4.1],

$$\operatorname{ed}_p(G) = \operatorname{ed}_p(G'). \tag{2.5}$$

Let T be a split torus over F and X be a finite set. Suppose that a finite group H acts on the character group T^* and X, and there is a H-equivariant homomorphism $\nu : \mathbb{Z}[X] \to T^*$. Then one can construct a generically free representation V_X for $T \rtimes H$ as follows: let

$$V_X = \coprod_{x \in X} F \cdot x$$

be a vector space over F generated by X. The action of H on X induces a natural H-action on V_X. The split torus T acts on V_X by $t \cdot x = \nu(x)(t) \cdot x$ for $t \in T$. Therefore, the semidirect product $T \rtimes H$ acts linearly on V_X.

Lemma 2.1 [**13**, Lemma 3.3]. *The vector space V_X gives a generically free representation for $T \rtimes H$ if and only if*

(i) *ν is surjective and*

(ii) *H acts faithfully on* $\operatorname{Ker}(\nu)$.

Moreover, if these conditions are satisfied, then $\operatorname{ed}(T \rtimes H) \leq |X| - \operatorname{rank}(T^*)$.

The last statement in Lemma 2.1 follows from (2.4).

3. *Proofs of* (i) *and the first part of* (ii) *in Theorem* 1.1

Let G be a smooth reductive algebraic group over F. Let T be a maximal torus of G and N 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 [**7**, Corollary 5.3], i.e., the morphism $H^1(-, N) \to H^1(-, G)$ is surjective and p-surjective for any prime p. Therefore, by (2.1) and (2.2), we have

$$\operatorname{ed}(G) \leq \operatorname{ed}(N) \text{ and } \operatorname{ed}_p(G) \leq \operatorname{ed}_p(N). \tag{3.1}$$

For any integer n with $2|n$, consider the 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. Similarly, we let $T'_{n,2}$ be the maximal torus in $\mathbf{SL}_n / \boldsymbol{\mu}_2$, i.e., $T'_{n,2} = T_{n,2} \cap (\mathbf{SL}_n / \boldsymbol{\mu}_2)$. In the following lemma we compute upper bounds for the essential dimension of normalizers of maximal tori in $\mathbf{GL}_n / \boldsymbol{\mu}_2$ and $\mathbf{SL}_n / \boldsymbol{\mu}_2$. We note that a different proof of Lemma 3.1(ii) is given in [**9**, Proposition 5.6] under the assumption that the base field F is an algebraically closed of characteristic 0.

Lemma 3.1. *Let F be an arbitrary field and S_n the symmetric group on n elements. Then we have*

(i) $\operatorname{ed}(T_{n,2} \rtimes S_n) \leq (n^2 - n)/2$ *for* $n \geq 3$,

(ii) $\operatorname{ed}(T'_{n,2} \rtimes S_n) \leq (n^2 - 3n + 2)/2$ *for* $n \geq 6$.

Proof. (i) 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 $1 \le i \ne j \le n$ 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 $1 \le i \ne j \le n$ 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 $1 \le k \le n$ and 0's are placed in other positions.

Let X be a set consisting of $f_{i,j}$ and g_k for all $1 \le i < j \le n$ and all $1 \le k \le n$. 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 $1 \le i_0 \le n$ such that $\sigma(i_0) \ne i_0$. Choose a $1 \le j_0 \le n$ which is different from $\sigma(i_0)$ and i_0. Then σ does not fix $2f_{i_0,j_0} + g_{i_0} + g_{j_0} \in \mathrm{Ker}(\nu)$. Hence, by Lemma 2.1, there exists a generically free representation for $T_{n,2} \rtimes S_n$, therefore,

$$\mathrm{ed}(T_{n,2} \rtimes S_n) \le (n^2 - n)/2 + n - \mathrm{rank}((T_{n,2})^*) = (n^2 - n)/2.$$

(ii) Note that the exact sequence

$$0 \to \mathbf{SL}_n / \boldsymbol{\mu}_2 \to \mathbf{GL}_n / \boldsymbol{\mu}_2 \to \mathbb{G}_m \to 0$$

implies that

$$0 \to T'_{n,2} \to T_{n,2} \to \mathbb{G}_m \to 0$$

is exact. By taking character lattices, we have

$$0 \to \mathbb{Z} \to (T_{n,2})^* \to (T'_{n,2})^* \to 0$$

and hence $(T'_{n,2})^* \simeq (T_{n,2})^*/\mathbb{Z}$.

Let $\overline{e}_{i,j}$ and $\overline{f}_{i,j}$ denote the classes of $e_{i,j}$ and $f_{i,j}$ in $\mathbb{Z}^n/\mathbb{Z}$. Let X' be a set consisting of $\overline{f}_{i,j}$ for all $1 \le i \ne j \le n$. Then X' is a S_n-invariant subset of $(T'_{n,2})^*$ and $|X'| = |\overline{f}_{i,j}| = (n^2 - n)/2$. Note that

$$\overline{e}_{i,j} = \overline{f}_{i,k} + \sum_{p,q \ne j,k} \overline{f}_{p,q}$$

for any $i \ne j$ and any $k \ne i, j$. Therefore, X' generates $(T'_{n,2})^*$ as an abelian group as $\overline{e}_{i,j}$ and $\overline{f}_{i,j}$ generate $(T'_{n,2})^*$. Hence we have a surjective S_n-equivariant homomorphism $\nu' : \mathbb{Z}[X'] \to (T'_{n,2})^*$ taking $\overline{f}_{i,j}$ to itself.

Suppose that $\mathrm{Ker}(\nu')$ is not a faithful S_n-lattice. Then the kernel of the action of S_n on $\mathrm{Ker}(\nu')$, denoted by N, is a non-trivial normal subgroup of S_n. As $n \ge 6$, $N = A_n$ or S_n, where A_n is the alternating group on n letters. As the S_n-lattice X' restricted to N is still transitive, $(X')^N$ has rank 1. On the other hand, the rank of $\mathrm{Ker}(\nu')$ is $(n^2 - 3n + 2)/2 > 1$. This contradicts $\mathrm{Ker}(\nu') = \mathrm{Ker}(\nu')^N \subset (X')^N$. Therefore, S_n acts faithfully on $\mathrm{Ker}(\nu')$. Hence, by Lemma 2.1, there exists a generically free representation for $T'_{n,2} \rtimes S_n$, therefore,

$$\mathrm{ed}(T'_{n,2} \rtimes S_n) \le (n^2 - n)/2 - \mathrm{rank}((T'_{n,2})^*) = (n^2 - 3n + 2)/2.$$

□

Proof of Theorem 1.1(i). By (3.1), Lemma 3.1(ii) and Lemma 6.1, we have

$$\mathrm{ed}(\mathrm{Alg}_{n,2}) \le \mathrm{ed}(\mathbf{SL}_n / \boldsymbol{\mu}_2) \le \mathrm{ed}(T'_{n,2} \rtimes S_n) \le (n^2 - 3n + 2)/2.$$

□

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

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

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 3.1. 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 $f_{i,j}$, where $i \in \Lambda_1$, $j \in \Lambda_2$ and g_k, $1 \leq k \leq 2^r$. 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 $\operatorname{Ker}(\nu)$. Note that the center of P_{2^r} is generated by $\sigma := (1,2)(3,4)\cdots(2^r-1, 2^r)$. It is enough to show that σ acts faithfully on $\operatorname{Ker}(\nu)$. In fact, σ does not fix the non-zero element $2f_{1,2^{r-1}+1} + g_1 + g_{2^{r-1}+1} \in \mathbb{Z}[X]$. Hence, by Lemma 2.1, there exists a generically free representation for $T_{2^r,2} \rtimes P_{2^r}$, therefore,

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

□

Proof of the first part in Theorem 1.1(ii). As $(2, [T_{2^r,2} \rtimes S_{2^r} : T_{2^r,2} \rtimes P_{2^r}]) = 1$, we have $\operatorname{ed}_2(T_{2^r,2} \rtimes S_{2^r}) = \operatorname{ed}_2(T_{2^r,2} \rtimes P_{2^r})$ by (2.5). Therefore, by Lemma 3.2 and (3.1),

$$\operatorname{ed}_2(\operatorname{Alg}_{2^r,2}) = \operatorname{ed}_2(\mathbf{GL}_{2^r} / \boldsymbol{\mu}_2) \leq \operatorname{ed}_2(T_{2^r,2} \rtimes S_{2^r}) = \operatorname{ed}_2(T_{2^r,2} \rtimes P_{2^r}) \leq \operatorname{ed}(T_{2^r,2} \rtimes P_{2^r}) \leq 2^{2r-2}.$$

□

4. *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 $\operatorname{Int}(a)$: $\operatorname{Int}(a)(x) = axa^{-1}$ 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 4.1 [**6**, Proposition 2.7]. *Let F be a field of $\operatorname{char}(F) \neq 2$, 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 $\operatorname{Int}(a) \circ \sigma$ 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 4.2 [**6**, Theorem 4.14]. *Let F be a field of $\operatorname{char}(F) \neq 2$, 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 the degree $\deg(C_A(B))$ is odd.*

From now on until the end of this section, 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 4.3. *Let $r \geq 3$ be an integer, F a 2-closed field such that $\operatorname{char}(F) \neq 2$ 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 [**6**, 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 D such that $\sigma_i|_{K_1K_2} = \tau_i$ by Lemma 4.2.

By Lemma 4.1, there exists $d \in D^\times$ such that $\sigma_1 = \operatorname{Int}(d) \circ \sigma_2$ 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 [**18**, Proposition 1.1]. Hence we have 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 the index $\operatorname{ind}(C_D(Q_1 \otimes Q_2))$ is bigger than or equal to 2, $C_D(Q_1 \otimes Q_2)$ contains a quadratic extension K_3/F by [**18**, 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 4.4. *Let $r \geq 3$ be an integer and F be a 2-closed field such that $\operatorname{char}(F) \neq 2$. 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 4.3, 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/K_3 with $[K : K_3] = 2^{r-3}$. Hence D contains a field extension K_1K_2K over F such that $\dim_F(K) = 2^{r-3} \cdot 2$. □

5. *Proof of the second part in Theorem* 1.1(ii)

Let $n \geq 2$ be an integer, G a subgroup of S_n and X a G-set of n elements (G acts on X by permutations). For any divisor m of n, we consider the surjective G-module 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 $J = \operatorname{Ker}(\bar{\varepsilon})$. Then we have an exact sequence

$$0 \to J \to \mathbb{Z}[X] \overset{\bar{\varepsilon}}{\to} \mathbb{Z}/m\mathbb{Z} \to 0. \tag{5.1}$$

We shall need the following lemma (see also the proof of [**3**, Theorem 8.1]):

Lemma 5.1. *Let F be a field of* $\operatorname{char}(F) \not| n$ *and* $T = \operatorname{Spec} F[J]$ *be the split torus with the character group J. Then*

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

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 [**6**, 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.,

$$H^1(F, T \rtimes G) \simeq \coprod H^1(F, T_\gamma)/G_\gamma(F), \tag{5.2}$$

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

Let E be the Galois G-algebra over F associated to γ. From (5.1), 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

$$1 \to \boldsymbol{\mu}_m \to R_{E/F}(\mathbb{G}_{m,E}) \to T_\gamma \to 1, \tag{5.3}$$

each term of which is twisted by γ. The exact sequence (5.3) induces an exact sequence of Galois cohomology

$$1 \to H^1(F, T_\gamma) \to H^2(F, \boldsymbol{\mu}_m) = \operatorname{Br}_m(F) \to H^2(E, \mathbb{G}_{m,E}) = \operatorname{Br}(E) \tag{5.4}$$

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 $\sigma \in G_\gamma(F)$ act on $T_\gamma = R_{E/F}(\mathbb{G}_{m,E})/\boldsymbol{\mu}_m$. The action of σ and (5.4) induce the following diagram

$$\begin{tikzcd} H^1(F, T_\gamma) \arrow[r, hook] \arrow[d, "\sigma^*"] & H^2(F, \boldsymbol{\mu}_m) \arrow[d, equal] \\ H^1(F, T_\gamma) \arrow[r, hook] & H^2(F, \boldsymbol{\mu}_m). \end{tikzcd}$$

Therefore, $G_\gamma(F)$ acts trivially on $H^1(F, T_\gamma)$, hence the result follows from (5.2). □

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 $J_r = \operatorname{Ker}(\mathbb{Z}[X_r] \overset{\bar{\varepsilon}}{\to} \mathbb{Z}/2\mathbb{Z})$, where $\bar{\varepsilon}$ is the map with $m = 2$ as in (5.1). Applying Lemma 5.1 with $n = 2^r$, $m = 2$, $G = G_r$, $X = X_r$, $J = J_r$, and $T = T_r := \operatorname{Spec}(F[J_r])$, we have a morphism

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

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 $\mathrm{Br}_2(L/N)$.

Consider the morphism

$$\Theta : H^1(-, T_r \rtimes G_r) \coprod \Big(\coprod_{1 \le i \le r-1} \mathrm{Alg}_{2^i,2} \Big) \to \mathrm{Alg}_{2^r,2} \tag{5.5}$$

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 $A_i \in \mathrm{Alg}_{2^i,2}(N)$ for $1 \le i \le r-1$.

Lemma 5.2. *If the base field F is 2-closed and is of characteristic different from 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 [**18**, 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 4.4, there exists a maximal étale subalgebra K_1K_2K in D such that $\dim_N(K) = 2^{r-2}$. Hence θ is surjective and so is Θ. □

Example 1 (see [**3**, 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. For any $1 \le i \ne j \le 3$ and any $\tau \in H_3 \backslash < \tau_i, \tau_j >$, an element $(\tau_i + 1)e_j - (\tau_j + 1)e_i$ of $\mathrm{Ker}(\rho)$ is not fixed by τ. Hence, H_3 acts on $\mathrm{Ker}(\rho)$ faithfully. Therefore, by Lemma 2.1, $\mathrm{ed}_2(\mathrm{Alg}_{8,2}) \le 4 + 4 + 4 + 4 - 2^3 = 8$.

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 5.3. *For any $r \ge 3$ and any $x \in X_r$, we have*

(i) $H_{r,x} \simeq H_{r-1,x} \times P_{2^{r-3}}$.
(ii) *The group H_r is generated by τ_1, τ_2, τ_r and $H_{r,x}$.*
(iii) *The $\mathbb{Z}[H_r]$-module J_r is generated by $2x, \tau_1 x - x, \tau_2 x - x$ and $\tau_r x - x$.*
(iv) $\tau_r H_{r,x} \tau_r \cap H_{r,x} \simeq H_{r-1,x} \times H_{r-1,x}$.

Proof. (i) By the action of H_r (see page 8), the stabilizer of x in H_r is the stabilizer of x under the action of $1 \times 1 \times P_{2^{r-2}} \simeq P_{2^{r-2}}$ 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 $H_{r-1,x} \times P_{2^{r-3}}$.

(ii) Induction on r. The case $r = 3$ comes from Example 1. By induction hypothesis we have $P_{2^{r-3}} = \langle \tau_{r-1}, H_{r-1,x}\rangle$. By Lemma 5.3(i), we have

$$P_{2^{r-2}} =< \tau_r, P_{2^{r-3}} >\subseteq< \tau_r, H_{r-1,x} \times P_{2^{r-3}} >=< \tau_r, H_{r,x} > .$$

Hence, the result follows immediately.

(iii) As H_r acts on X_r transitively, the result follows from Lemma 5.3(ii) and the sequence (5.1).

(iv) As $\tau_r H_{r,x}\tau_r = H_{r,\tau_r(x)}$, the result follows from Lemma 5.3(i). □

Proof of the second part in Theorem 1.1(ii). 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 the 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 5.3(iii).

As H_r acts faithfully on $\mathrm{Ker}(\rho)$ by Lemma 5.4, there exists a generically free representation for $T_r \rtimes H_r$ by Lemma 2.1. Therefore, by Lemma 2.1 and (2.3), we have

$$\begin{aligned}\mathrm{ed}_2(T_r \rtimes H_r) \leq\ &\mathrm{rank}(\mathbb{Z}[H_r/\langle\tau_1\rangle \times H_{r,x}]) + \mathrm{rank}(\mathbb{Z}[H_r/\langle\tau_2\rangle \times H_{r,x}])\\ &+ \mathrm{rank}(\mathbb{Z}[H_r/\langle\tau_1\tau_2\rangle \times H_{r,x}]) + \mathrm{rank}(\mathbb{Z}[H_r/(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle])\\ &- \mathrm{rank}(J_r)\\ &= 2^{r-1} + 2^{r-1} + 2^{r-1} + 2^{r+(r-1)-2-1} - 2^r \text{ (by Lemma 5.3(i),(iv))}\\ &= 2^{r-1} + 2^{2r-4}.\end{aligned}$$

By (2.5), $\mathrm{ed}_2(T_r \rtimes G_r) = \mathrm{ed}_2(T_r \rtimes H_r)$. As the morphism Θ in (5.5) is surjective by Lemma 5.2, it follows from [**4**, Lemma 1.10] and (2.3) that

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

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

Lemma 5.4. *Let $\rho : \Lambda_r \to J_r$ be the morphism in the proof of the second part in Theorem* 1.1(ii). *Then, the action of H_r on* $\mathrm{Ker}(\rho)$ *is faithful.*

Proof. For $r = 3$, it is shown in Example 1. We assume $r \geq 4$. It follows from the exact sequence (5.1) that $J_r \otimes \mathbb{Q} = \mathbb{Q}[X_r]$. Hence, by the exact sequence

$$0 \to \mathrm{Ker}(\rho) \to \Lambda_r \xrightarrow{\rho} J_r \to 0,$$

we have

$$\begin{aligned}\mathbb{Q}[X_r] \oplus (\mathrm{Ker}(\rho))_{\mathbb{Q}} = &\mathbb{Q}[H_r/\langle\tau_1\rangle \times H_{r,x}] \oplus \mathbb{Q}[H_r/\langle\tau_2\rangle \times H_{r,x}] \oplus \mathbb{Q}[H_r/\langle\tau_1\tau_2\rangle \times H_{r,x}]\\ &\oplus \mathbb{Q}[H_r/(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle]. \qquad (5.6)\end{aligned}$$

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

$$\mathbb{Q}[X_r] \oplus (\mathrm{Coker}(i))_{\mathbb{Q}} = \mathbb{Q}[X_r/\langle\tau_1\rangle] \oplus \mathbb{Q}[X_r/\langle\tau_2\rangle] \oplus \mathbb{Q}[X_r/\langle\tau_1\tau_2\rangle]. \tag{5.7}$$

By (5.6) and (5.7), 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 $Y_r := \mathbb{Q}[H_r/(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle]$. We prove this using case by case analysis.

Case 1: Suppose that $h \notin 1 \times 1 \times [(P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle] \subset H_r$.

(i) 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.

(ii) 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: Suppose now that $h \in 1 \times 1 \times [(P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle] \subset H_r$. Recall from Lemma 5.3(iv) that $\tau_r H_{r,x}\tau_r \cap H_{r,x} \simeq H_{r-1,x} \times H_{r-1,x}$. We view $(\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle$ as a subgroup of $(P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle$.

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

(ii) Suppose that $h = h_1h_2\tau_r \in (H_{r-1,x} \times H_{r-1,x}) \rtimes \langle\tau_r\rangle \simeq (\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle$, where h_1 and h_2 are elements in the first and the second $H_{r-1,x}$, respectively. We may assume that $x = 1$. Choose a transposition $\delta = (1, 2) \in H_r$. Then $\delta h\delta = (1, 2)h(1, 2) = (1, 2)h_1h_2\tau_r(1, 2) = (1, \tau_r(2))\delta' \notin (\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle$ for some disjoint cycle δ'. Hence, $h\overline{\delta} \neq \overline{\delta}$ in Y_r.

(iii) Suppose that $h = h_1h_2 \in H_{r-1,x} \times H_{r-1,x} \simeq \tau_r H_{r,x}\tau_r \cap H_{r,x}$, where h_1 and h_2 are elements in the first and the second $H_{r-1,x}$, respectively. We may assume that $h_1 \neq 1$ and $x = 1$. For any integer $y \in \{2, \cdots, 2^{r-3}\}$, we claim that there exists $\delta_r \in 1 \times 1 \times [(P_{2^{r-3}})^2 \rtimes \langle\tau_r\rangle]$ such that δ moves 1 to y and $\overline{\delta} \neq \overline{1}$ in Y_r. We show the claim by induction on r. If $r = 5$, then the claim is true as $P_4 = (P_2)^2 \rtimes \langle\tau_4\rangle = \langle(1, 2), (3, 4)\rangle \rtimes \langle(1, 3)(2, 4)\rangle$. By the induction hypothesis, $\delta_r = \delta_{r-1}$ or $\tau_{r-1}\delta_{r-1}$ satisfies the claim. Suppose that h_1 moves y to z, where $y, z \in \{2, \cdots, 2^{r-3}\}$ and $y \neq z$. Then, by the claim, $\delta_r h_1h_2\delta_r$ moves 1 to $\delta_r(z) \neq 1$, i.e., $\delta_r h_1h_2\delta_r \notin (\tau_r H_{r,x}\tau_r \cap H_{r,x}) \rtimes \langle\tau_r\rangle$. Hence, $h\overline{\delta_r} \neq \overline{\delta_r}$ in Y_r.

This completes the proof of faithfulness. □

6. *Essential dimension of split simple groups of type A_{n-1}*

Computing the essential dimension of split simple groups of type A_{n-1}, especially of their adjoint cases, is a long-standing open problem. It is wide open in general and the only completely known cases are the following:

Example 2. Let F be an arbitrary base field.

(i) (A_1 and A_2) By [**16**, Lemma 8.5.7] and [**15**, Lemma 9.4(c)],

$$\mathrm{ed}_2(\mathbf{SL}_2 / \boldsymbol{\mu}_2) = \mathrm{ed}(\mathbf{SL}_2 / \boldsymbol{\mu}_2) = \mathrm{ed}_3(\mathbf{SL}_3 / \boldsymbol{\mu}_3) = \mathrm{ed}(\mathbf{SL}_3 / \boldsymbol{\mu}_3) = 2.$$

(ii) (A_3) In [**12**, Corollary 1.2], the adjoint case was obtained as

$$\mathrm{ed}_2(\mathbf{SL}_4 / \boldsymbol{\mu}_4) = \mathrm{ed}(\mathbf{SL}_4 / \boldsymbol{\mu}_4) = 5$$

over a field F of $\operatorname{char}(F) \neq 2$. As $A_3 = D_3$, we have $\mathbf{SL}_4 / \boldsymbol{\mu}_2 \simeq \mathbf{SO}_6$. Therefore, by [**15**, Theorem 10.4 and Example 12.7],

$$\operatorname{ed}_2(\mathbf{SL}_4 / \boldsymbol{\mu}_2) = \operatorname{ed}(\mathbf{SL}_4 / \boldsymbol{\mu}_2) = 5.$$

over a field F of $\operatorname{char}(F) \neq 2$. Alternatively, one may use [**16**, Theorem 8.13] and Lemma 6.1 for lower and upper bounds, respectively.

In this section we relate the essential dimensions of $\operatorname{Alg}_{n,m}$ and of the split simple groups of type A_{n-1} ($\simeq \mathbf{SL}_n / \boldsymbol{\mu}_m$). As $\operatorname{ed}(\mathbf{SL}_n / \boldsymbol{\mu}_n) = \operatorname{ed}(\operatorname{Alg}_{n,n})$, the main purpose of the following lemma is the case where $m \neq n$.

Lemma 6.1. *Let F be a field, $n \geq 1$ a integer not divisible by* $\operatorname{char}(F)$ *and m a divisor of n. Then*

$$\operatorname{ed}(\operatorname{Alg}_{n,m}) \leq \operatorname{ed}(\mathbf{SL}_n / \boldsymbol{\mu}_m) \leq \operatorname{ed}(\operatorname{Alg}_{n,m}) + 1.$$

Proof. Consider the exact sequence

$$1 \to \boldsymbol{\mu}_{n/m} \xrightarrow{\alpha} \mathbf{SL}_n / \boldsymbol{\mu}_m \to \mathbf{PGL}_n \to 1. \tag{6.1}$$

For a field extension K/F, the sequence (6.1) induces an exact sequence

$$H^1(K, \boldsymbol{\mu}_{n/m}) \to H^1(K, \mathbf{SL}_n / \boldsymbol{\mu}_m) \to H^1(K, \mathbf{PGL}_n) \xrightarrow{\partial} H^2(K, \boldsymbol{\mu}_{n/m}),$$

where $\partial : H^1(K, \mathbf{PGL}_n) \to H^2(K, \boldsymbol{\mu}_{n/m}) = \operatorname{Br}_{n/m}(K)$ takes the isomorphism class of a central simple K-algebra A of degree n to the class $m[A]$. Therefore, we have the following sequence

$$H^1(K, \boldsymbol{\mu}_{n/m}) \xrightarrow{\alpha_*} H^1(K, \mathbf{SL}_n / \boldsymbol{\mu}_m) \twoheadrightarrow \operatorname{Alg}_{n,m}(K). \tag{6.2}$$

As $H^1(K, \mathbf{SL}_n)$ is trivial and the first vertical map of the following diagram

$$\begin{tikzcd} H^1(K, \boldsymbol{\mu}_n) \arrow[r] \arrow[d] & H^1(K, \mathbf{SL}_n) \arrow[d] \\ H^1(K, \boldsymbol{\mu}_{n/m}) \arrow[r, "\alpha_*"] & H^1(K, \mathbf{SL}_n / \boldsymbol{\mu}_m). \end{tikzcd}$$

is surjective, the image of α_* is trivial. Therefore, from (6.2), we get a fibration of functors (see [**4**, Definition 1.12])

$$H^1(-, \boldsymbol{\mu}_{n/m}) \rightsquigarrow H^1(-, \mathbf{SL}_n / \boldsymbol{\mu}_m) \twoheadrightarrow \operatorname{Alg}_{n,m}.$$

As $\operatorname{ed}(\boldsymbol{\mu}_{n/m}) = 1$, we get $\operatorname{ed}_F(\mathbf{SL}_n / \boldsymbol{\mu}_m) \leq \operatorname{ed}_F(\operatorname{Alg}_{n,m}) + 1$ by [**4**, Proposition 1.13]. The lower bound follows from (2.1). □

Remark 1. Let F be an arbitrary base field.

(i) As $\mathbf{SL}_n / \boldsymbol{\mu}_m$ is a subgroup of $\mathbf{GL}_n / \boldsymbol{\mu}_m$ of codimension 1, the second inequality of Lemma 6.1 can be obtained by [**4**, Theorem 6.19].

(ii) Recently, V. Chernousov and A. Merkurjev proved that

$$\operatorname{ed}_p(\mathbf{SL}_{p^r} / \boldsymbol{\mu}_{p^s}) = \operatorname{ed}_p(\operatorname{Alg}_{p^r,p^s}) + 1 \tag{6.3}$$

for any $0 \neq s < r$ over a field of $\operatorname{char}(F) \neq p$ in [**8**]. Therefore, the computation of essential p-dimension of split simple group of type A_{p^r-1} is reduced to the computation of $\operatorname{ed}_p(\operatorname{Alg}_{p^r,p^s})$. In particular, [**3**, Corollary 8.3], we have $\operatorname{ed}_2(\operatorname{Alg}_{8,2}) = \operatorname{ed}(\operatorname{Alg}_{8,2}) = 8$

over a field F of $\mathrm{char}(F) \neq 2$. Hence, by (6.3) and Lemma 6.1, one can find

$$\mathrm{ed}_2(\mathbf{SL}_8 \,/\, \boldsymbol{\mu}_2) = \mathrm{ed}(\mathbf{SL}_8 \,/\, \boldsymbol{\mu}_2) = 9$$

over a field F of $\mathrm{char}(F) \neq 2$. Moreover, by (6.3) and Corollary 1.2, one can conclude that

$$\mathrm{ed}_2(\mathbf{SL}_{16} \,/\, \boldsymbol{\mu}_2) = 25$$

over a field F of $\mathrm{char}(F) \neq 2$; see [**8**, Corollary 1.2].

Acknowledgements. I am grateful to my advisor A. Merkurjev for many useful discussions and support and to Z. Reichstein for helpful comments. I am also grateful to the referee for helpful suggestions. Finally, I wish to thank E. Neher and K. Zainoulline for their reading of the manuscript. Section 3 of this paper is based on the author's doctoral thesis at the University of California at Los Angeles.

References

1. S. Baek, 'Essential dimension of simple algebras in positive characteristic', *C. R. Math. Acad. Sci. Paris* 349 (2011) 375–378.

2. S. Baek and A. Merkurjev, 'Invariants of simple algebras', *Manuscripta Math.* 129 (2009) 409–421.

3. S. Baek and A. Merkurjev, 'Essential dimension of central simple algebras', *To appear in Acta Math.*

4. G. Berhuy and G. Favi, 'Essential dimension: a functorial point of view after (A. Merkurjev)', *Doc. Math.* 8 (2003) 279–330.

5. J. Buhler and Z. Reichstein, 'On the essential dimension of a finite group', *Compositio Math.* 106 (1997) 159–179.

6. M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions* (American Mathematical Society, Providence, RI, 1998).

7. V. Chernousov, P. Gille, and Z. Reichstein, 'Reduction of structure for torsors over semilocal rings', *Manuscripta Math.* 126 (2008) 465–480.

8. V. Chernousov and A. Merkurjev, 'Essential p-dimension of split simple groups of type A_n', *Preprint,* http://www.math.uni-bielefeld.de/LAG/man/429.html.

9. N. Lemire, 'Essential dimension of algebraic groups and integral representations of Weyl groups', *Transform. Groups* 9 (2004) 337–379.

10. R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein, 'Essential p-dimension of algebraic tori', *Preprint,* http://www.mathematik.uni-bielefeld.de/LAG/man/363.html.

11. A. S. Merkurjev, 'Essential dimension', Quadratic forms—algebra, arithmetic, and geometry, *Contemp. Math.* 493 (Amer. Math. Soc., Providence, RI, 2009) 299–325.

12. A. S. Merkurjev, 'Essential p-dimension of $\mathrm{PGL}(p^2)$', *J. Amer. Math. Soc.* 23 (2010) 693–712.

13. 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) 467–487.

14. A. Meyer and Z. Reichstein, 'An upper bound on the essential dimension of a central simple algebra', *J. Algebra* 329 (2011) 213–221.

15. Z. Reichstein, 'On the notion of essential dimension for algebraic groups', *Transform. Groups* 5 (2000) 265-304.

16. Z. Reichstein and B. Youssin, 'Essential dimensions of algebraic groups and a resolution theorem for G-varieties', *Canad. J. Math.* 52 (2000) 1018–1056, with an appendix by János Kollár and Endre Szabó.

17. A. Rouzzi, 'Essential p-dimension of PGL_n', *J. Algebra* 328 (2011) 488–494.

18. L. H. Rowen and D. J. Saltman, 'Prime to p extensions of division algebra', *Israel J. Math.* 78 (1992) 197–207.

Sanghoon Baek
Department of Mathematics and Statistics
University of Ottawa
585 King Edward, Ottawa, ON K1N6N5
Canada

sbaek@uottawa.ca