C. R. Acad. Sci. Paris, Ser. I 349 (2011) 375–378

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Algebra

Essential dimension of simple algebras in positive characteristic

Dimension essentielle des algèbres simples en caractéristique positive

Sanghoon Baek

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

ARTICLE INFO

Article history:
Received 18 January 2011
Accepted after revision 15 March 2011
Available online 1 April 2011

Presented by the Editorial Board

ABSTRACT

Let p be a prime integer. For any integers $1 \leqslant s \leqslant r$, Alg_{p^r,p^s} denotes the class of central simple algebras of degree p^r and exponent dividing p^s. For any $s < r$, we find a lower bound for the essential p-dimension of Alg_{p^r,p^s}. Furthermore, we compute an upper bound for $Alg_{8,2}$ over a field of characteristic 2. As a result, we show $\mathrm{ed}_2(Alg_{4,2}) = \mathrm{ed}(Alg_{4,2}) = 3$ and $3 \leqslant \mathrm{ed}(Alg_{8,2}) \leqslant 10$ over a field of characteristic 2.

RÉSUMÉ

Soit p un nombre premier. Pour toutes nombres entiers $1 \leqslant s \leqslant r$, on note Alg_{p^r,p^s} la classe des algèbres simples centrales de degré p^r et d'exposant au plus p^s. Pour tous $s < r$, nous trouvons une borne inférieure pour la p-dimension essentielle de Alg_{p^r,p^s}. De plus, nous calculons une borne supérieure pour $Alg_{8,2}$ sur un corps de caractéristique 2. En conséquence, on montre que $\mathrm{ed}_2(Alg_{4,2}) = \mathrm{ed}(Alg_{4,2}) = 3$ et $3 \leqslant \mathrm{ed}(Alg_{8,2}) \leqslant 10$ sur un corps de caractéristique 2.

1. Introduction

A numerical invariant of an algebraic group, called the essential dimension, was introduced by Reichstein and was generalized to an algebraic structure by Merkurjev. We refer to [10] for the definition of essential dimension. For a given prime p, we denote by ed and ed_p the essential dimension and essential p-dimension, respectively.

Let F be a field and p a prime integer. For any integers $1 \leqslant s \leqslant r$, let $Alg_{p^r,p^s} : Fields/F \to Sets$ be the functor from the category $Fields/F$ of field extensions over F to the category $Sets$ of sets, taking a field extension E/F to the set of isomorphism classes of central simple E-algebras of degree p^r and exponent dividing p^s. Then, there is a natural bijection between $H^1(E, \mathbf{GL}_{p^r}/\boldsymbol{\mu}_{p^s})$ and $Alg_{p^r,p^s}(E)$ (see [2, Example 1.1]), thus we have $\mathrm{ed}(Alg_{p^r,p^s}) = \mathrm{ed}(\mathbf{GL}_{p^r}/\boldsymbol{\mu}_{p^s})$ and $\mathrm{ed}_p(Alg_{p^r,p^s}) = \mathrm{ed}_p(\mathbf{GL}_{p^r}/\boldsymbol{\mu}_{p^s})$.

Let F be a field of characteristic p. For $a \in F$ and $b \in F^\times$, the *p-symbol* $[a,b)$ is a central simple F-algebra generated by u and v satisfying $u^p - u = a$, $v^p = b$ and $vu = uv + v$. Let $Dec_{p^r} : Fields/F \to Sets$ be the functor taking a field extension E/F to the set of isomorphism classes of the tensor product of r p-symbols over E.

Some exact values of $\mathrm{ed}(Alg_{p^r,p^s})$ and $\mathrm{ed}_p(Alg_{p^r,p^s})$ have been computed (see [11,3,14], and [1]). However, all of them were calculated over a field F of $\mathrm{char}(F) \neq p$. In Section 2, for any integers $r > s$, we find a new lower bound for

E-mail address: sbaek@uottawa.ca.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2011.03.014

$\mathrm{ed}_p(Alg_{p^r,p^s})$ in $\mathrm{char}(F)=p$. In Section 3, we compute upper bounds for Dec_{p^r} and $Alg_{8,2}$ in $\mathrm{char}(F)=p$ and $\mathrm{char}(F)=2$, respectively. As a result, we get:

Theorem 1.1. *Let F be a field containing the field with 4 elements. Then*

$$\mathrm{ed}_2(Alg_{4,2})=\mathrm{ed}(Alg_{4,2})=\mathrm{ed}_2(\mathbf{GL}_4/\boldsymbol{\mu}_2)=\mathrm{ed}(\mathbf{GL}_4/\boldsymbol{\mu}_2)=3.$$

Proof. It follows from Corollary 2.2 that $3\leqslant \mathrm{ed}_2(Alg_{4,2})\leqslant \mathrm{ed}(Alg_{4,2})$. By a Theorem of Albert, we have $Dec_4=Alg_{4,2}$ for $p=2$, thus we obtain $\mathrm{ed}(Alg_{4,2})\leqslant 3$ by Proposition 3.2. □

Corollary 2.2 and Proposition 3.4 give the following:

Theorem 1.2. *Let F be a field of characteristic 2. Then $3\leqslant \mathrm{ed}(Alg_{8,2})=\mathrm{ed}(\mathbf{GL}_8/\boldsymbol{\mu}_2)\leqslant 10$.*

2. Lower bound

Initially, the following theorem is proved under the additional condition that $\mathrm{char}(F)$ does not divide $\exp(A)$ in [5]. In a subsequent paper [9, Theorem 4.2.2.3], this condition is removed:

Theorem 2.1 *(de Jong). Let E be a field of transcendental degree 2 over an algebraically closed field F. Then, for any central simple algebra A over E, $\mathrm{ind}(A)=\exp(A)$.*

As an application of Theorem 2.1, we have the following result:

Corollary 2.2. *Let F be a field and p a prime. For any integers $1\leqslant s<r$, $\mathrm{ed}_p(Alg_{p^r,p^s})\geqslant 3$.*

Proof. By [10, Proposition 1.5], we may assume that F is algebraically closed. It follows from [13, Lemma 9.4(a)] that $\mathrm{ed}_p(Alg_{p^r,p^s})\geqslant 2$ for any integers r, s, and any prime p. Note that for any integers $1\leqslant s<r$ there exist a field extension L/F and a division L-algebra D of $\mathrm{ind}(D)=p^r$ and $\exp(D)=p^s$ by the proof of [12, §19.6, Theorem] together with Artin–Schreier theory. Let K be a field extension of F and A a central simple algebra over K of $\mathrm{ind}(A)=p^r$ and $\exp(A)|p^s$. Let E be a field extension of K of degree prime to p. As $\mathrm{ind}(A)$ is relatively prime to $[E:K]$, we have $\mathrm{ind}(A_E)=\mathrm{ind}(A)=p^r$. Suppose that $A_E\simeq B\otimes E$ for some $B\in Alg_{p^r,p^s}(L)$ and $\mathrm{tr.deg}_F(L)=2$. Then, by Theorem 2.1, we have $\mathrm{ind}(B)=\exp(B)$. As $p^r=\mathrm{ind}(A_E)|\,\mathrm{ind}(B)=\exp(B)$, we get $p^r|\exp(B)$. But this contradicts to $\exp(B)|p^s$. □

Remark. The above lower bound 3 is much less than the best known lower bounds (see [3, Theorem]), but these lower bounds are valid only for $\mathrm{char}(F)\neq p$. Hence, our main application of Corollary 2.2 is for the case of $\mathrm{char}(F)=p$.

3. Upper bounds

Lemma 3.1. *(See [4, Example 2.3 and p. 298].) Let $r\geqslant 1$ be an integer and F a field containing the field with p^r elements. Then $\mathrm{ed}((\mathbb{Z}/p\mathbb{Z})^r)=1$.*

Proposition 3.2. *Let F be a field containing the field with p^r elements. Then $\mathrm{ed}(Dec_{p^r})\leqslant r+1$.*

Proof. Let $A=\bigotimes_{i=1}^r[a_i,b_i)\in Dec_{p^r}(E)$ for a field extension E/F. As $\mathrm{ed}((\mathbb{Z}/p\mathbb{Z})^r)=1$ by Lemma 3.1, there exists a sub-extension E_0/F of E/F and $c_i\in E_0$ for all $1\leqslant i\leqslant r$ such that $c_i\equiv a_i \bmod \wp(E)$ and $\mathrm{tr.deg}_F(E_0)\leqslant 1$. Therefore, A is defined over $L=E_0(b_1,\dots,b_r)$ and $\mathrm{tr.deg}_F(L)\leqslant r+1$. Hence, $\mathrm{ed}(A)\leqslant r+1$ and $\mathrm{ed}(Dec_{p^r})\leqslant r+1$. □

The upper bound 8 (indeed, the exact value by [3, Corollary 8.3]) for $\mathrm{ed}(Alg_{8,2})$ over a field F of characteristic different from 2 was determined in [2, Theorem 2.12]. We use a similar method to find an upper bound for $\mathrm{ed}(Alg_{8,2})$ over a field F of characteristic 2. From now on we assume that $\mathrm{char}(F)=2$.

For a commutative F-algebra R, $a\in R$ and $b\in R^\times$ we write $[a,b)_R$ for the quaternion algebra $R\oplus Ru\oplus Rv\oplus Rw$ with the multiplication table $u^2+u=a$, $v^2=b$, $uv=w=vu+v$. The class of $[a,b)_R$ in the Brauer group $\mathrm{Br}(R)$ will be denoted by $\{a,b\}=\{a,b\}_R$. Let $a\in R$ and $T=R[\alpha]:=R[t]/(t^2+t+a)$ with $\alpha^2=\alpha+a$ the quadratic extension of R, i.e., T/R is a $\mathbb{Z}/2\mathbb{Z}$-Galois algebra. We write $N_R(a)$ for the subgroup of $R^\times$ of all elements of the form $x^2+xy+ay^2$ with $x,y\in R$. If $b\in N_R(a)$, then the quaternion algebra $[a,b)_R$ is isomorphic to the matrix algebra $M_2(R)$ by the proof of [8, Theorem 6]. We shall need the following result:

Lemma 3.3. *Let R be a commutative F-algebra, $a,b\in R$, $T=R[\alpha]:=R[t]/(t^2+t+a)$ and $x+y\alpha\in T^\times$ such that $x^2+xy+ay^2=u^2+uv+bv^2$ for some $u,v\in R$. If $v+y\in R^\times$, then $(v+y)(x+y\alpha)\in N_T(b)$. In particular, $\{b,x+y\alpha\}_T=\{b,v+y\}_T$.*

Proof. The result comes from the following equality $(x+y\alpha+u)^2+(x+y\alpha+u)v+bv^2=(x+y\alpha)^2+(x+y\alpha)v+u^2+uv+bv^2=(x+y\alpha)^2+(x+y\alpha)v+x^2+xy+ay^2=(x+y\alpha)(v+y)$. $\square$

Rowen extended Tignol's result [17] to a field of characteristic 2. Following Rowen's construction [15], we find a versal Azumaya algebra for $Alg_{8,2}$, i.e., the corresponding $\mathbf{GL}_8/\boldsymbol{\mu}_2$-torsor is versal (see [6, Definition 5.1 and Remark 5.8] or [2, Section 1.4]). Consider the affine space $\mathbb{A}^{13}_F$ with coordinates $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{m}, \mathbf{n}$ and define the following functions:

$$\begin{aligned}
&\mathbf{f}=\mathbf{xz}+\mathbf{wz}+\mathbf{xy},\\
&\mathbf{g}=\mathbf{wy}+\mathbf{xza},\\
&\mathbf{r}=\left(\mathbf{g}^2+\mathbf{gf}+\mathbf{f}^2\mathbf{a}+\mathbf{m}^2+\mathbf{mn}\right),\\
&\mathbf{h}=\left(\mathbf{w}^2+\mathbf{wx}+\mathbf{x}^2\mathbf{a}+1+\mathbf{u}+\mathbf{u}^2\mathbf{d}\right),\\
&\mathbf{l}=\left(\mathbf{y}^2+\mathbf{yz}+\mathbf{z}^2\mathbf{a}+1+\mathbf{v}+\mathbf{v}^2\mathbf{d}\right),\\
&\mathbf{p}=(\mathbf{u}+\mathbf{x})(\mathbf{v}+\mathbf{z})(\mathbf{n}+\mathbf{f}),\\
&\mathbf{q}=\mathbf{abcdep}\left(\mathbf{w}^2+\mathbf{wx}+\mathbf{x}^2\mathbf{a}\right)\left(\mathbf{y}^2+\mathbf{yz}+\mathbf{z}^2\mathbf{a}\right)\left(\mathbf{g}^2+\mathbf{gf}+\mathbf{f}^2\mathbf{a}\right).
\end{aligned}$$

Let $X=\operatorname{Spec}(R)$ be the affine scheme, where

$$R=F\left[\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d},\mathbf{e},\mathbf{u},\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{m},\mathbf{n},\mathbf{q}^{-1}\right]/\left\langle\mathbf{bu}^2+\mathbf{h},\mathbf{cv}^2+\mathbf{l},\mathbf{dn}^2+\mathbf{r}\right\rangle.$$

Let $T=R[\alpha]$ and $S=R[\alpha,\beta,\gamma]$ with $\alpha^2=\alpha+\mathbf{a}$, $\beta^2=\beta+\mathbf{b}$, $\gamma^2=\gamma+\mathbf{c}$. Consider the Azumaya R-algebra

$$\mathcal{B}'=[\mathbf{a},\mathbf{e})_R\otimes[\mathbf{b},\mathbf{x}+\mathbf{u})_R\otimes[\mathbf{c},\mathbf{z}+\mathbf{v})_R\otimes[\mathbf{d},\mathbf{p})_R. \tag{1}$$

By Lemma 3.3, we get $(\mathbf{x}+\mathbf{u})(\mathbf{w}+\mathbf{x}\alpha)\in N_T(\mathbf{b}+\mathbf{d})\subset N_S(\mathbf{d})$, $(\mathbf{z}+\mathbf{v})(\mathbf{y}+\mathbf{z}\alpha)\in N_T(\mathbf{c}+\mathbf{d})\subset N_S(\mathbf{d})$, and $(\mathbf{n}+\mathbf{f})(\mathbf{w}+\mathbf{x}\alpha)(\mathbf{y}+\mathbf{z}\alpha)\in N_T(\mathbf{d})\subset N_S(\mathbf{d})$. It follows from (1) that $\{\mathcal{B}'\}_T=\{\mathbf{b},\mathbf{w}+\mathbf{x}\alpha\}+\{\mathbf{c},\mathbf{y}+\mathbf{z}\alpha\}$ in $\operatorname{Br}(T)$. Since $\mathbf{p}\in N_S(\mathbf{d})$, $[\mathbf{d},\mathbf{p})_S$ is isomorphic to the matrix algebra $M_2(S)$. In particular,

$$M_2(R)\subset M_2(S)\simeq[\mathbf{d},\mathbf{p})_S\subset\mathcal{B}'$$

and hence $\mathcal{B}'\simeq M_2(\mathcal{B})$ for the centralizer $\mathcal{B}$ of $M_2(R)$ in $\mathcal{B}'$ by the proof of [7, Theorem 4.4.2]. Then $\mathcal{B}$ is an Azumaya R-algebra of degree 8 that is Brauer equivalent to $\mathcal{B}'$ by [16, Theorem 3.10].

Proposition 3.4. *The Azumaya algebra $\mathcal{B}$ is versal for $Alg_{8,2}$. In particular,* $\operatorname{ed}(Alg_{8,2})\leqslant 10$.

Proof. Let $A\in Alg_{8,2}(K)$, where K is a field extension of F. We shall find a point $p\in X(K)$ such that $A\simeq\mathcal{B}(p)$, where $\mathcal{B}(p):=\mathcal{B}\otimes_R K$ with the F-algebra homomorphism $R\to K$ given by the point p.

Following Rowen's construction, there is a triquadratic splitting extension $K(\alpha,\beta,\gamma)/K$ of A such that $\alpha^2+\alpha=a$, $\beta^2+\beta=b$, and $\gamma^2+\gamma=c$ for some $a,b,c\in K$. Let $L=K(\alpha)$, so $\{A\}_L=\{b,s\}+\{c,t\}$ in $\operatorname{Br}(L)$ for some $s=w+x\alpha$, and $t=y+z\alpha\in L^\times$. We have

$$\left\{b,w^2+wx+x^2a\right\}_K=\left\{d,w^2+wx+x^2a\right\}_K=\left\{d,y^2+yz+z^2a\right\}_K=\left\{c,y^2+yz+z^2a\right\}_K\quad\text{for some } d\in K,$$

so $\{b+d,w^2+wx+x^2a\}=\{c+d,y^2+yz+z^2a\}=\{d,(w^2+wx+x^2a)(y^2+yz+z^2a)\}=0$. Hence $w^2+wx+x^2a=u'^2+u'u+u^2(b+d)$, $y^2+yz+z^2a=v'^2+v'u+v^2(c+d)$, and $(w^2+wx+x^2a)(y^2+yz+z^2a)=m^2+mn+n^2d$ for some u,u',v,v',m,n in K. Moreover, we may assume that $u'\neq 0$. Replacing w, x and u by wu', xu' and $u'u$ respectively, we may assume that $u'=1$. Similarly, we can assume that $v'=1$.

We also may assume that $u\neq x$ by replacing u by $u/(b+d)$. Similarly, we can assume that $v\neq z$ and $n+xz+wz+xy\neq 0$. It follows from Lemma 3.3 that $\{b+d,w+x\alpha\}=\{b+d,u+x\}$, $\{c+d,y+z\alpha\}=\{c+d,z+v\}$, and $\{d,(w+x\alpha)(y+z\alpha)\}=\{d,n+xz+wz+xy\}$ in $\operatorname{Br}(L)$. Hence, $\{A\}=\{a,e\}+\{b,u+x\}+\{c,z+v\}+\{d,(u+x)(z+v)(n+xz+wz+xy)\}$ in $\operatorname{Br}(K)$ for some $e\in K^\times$. Let p be the point $(a,b,c,d,e,u,v,w,x,y,z,m,n)$ in $X(K)$. We have $\{\mathcal{B}(p)\}=\{A\}$ and hence $\mathcal{B}(p)\simeq A$ as $\mathcal{B}(p)$ and A have the same dimension.

Thus, there is surjective morphism $X\to Alg_{8,2}$. By [10, Proposition 1.3], $\operatorname{ed}(Alg_{8,2})\leqslant\dim(X)=10$. $\square$

Acknowledgements

I would like to thank Prof. A. Merkurjev for advice and useful discussions. I also would like to thank J. Malagón-López, E. Neher, and K. Zainoulline. The work has been supported by Neher's NSERC Discovery grant 008836-2006, and Zainoulline's NSERC Discovery grant 385795-2010 and Accelerator Supplement grant 396100-2010.

References

[1] S. Baek, Essential dimension of simple algebras with involutions, preprint, http://arxiv.org/abs/1008.2406.
[2] S. Baek, A. Merkurjev, Invariants of simple algebras, Manuscripta Math. 129 (4) (2009) 409–421.
[3] S. Baek, A. Merkurjev, Essential dimension of central simple algebras, Acta Math., in press.
[4] G. Berhuy, G. Favi, Essential dimension: a functorial point of view (after A. Merkurjev), Doc. Math. 8 (2003) 279–330.
[5] A.J. de Jong, The period-index problem for the Brauer group of an algebraic surface, Duke Math. J. 123 (2004) 71–94.
[6] R. Garibaldi, A. Merkurjev, J.-P. Serre, Cohomological Invariants in Galois Cohomology, American Mathematical Society, Providence, RI, 2003.
[7] I.N. Herstein, Noncommutative Rings, Mathematical Association of America, Washington, DC, 1994.
[8] T. Kanzaki, Note on quaternion algebras over a commutative ring, Osaka J. Math. 13 (3) (1976) 503–512.
[9] M. Lieblich, Twisted sheaves and the period-index problem, Compos. Math. 144 (1) (2008) 1–31.
[10] A.S. Merkurjev, Essential dimension, in: Quadratic Forms—Algebra, Arithmetic, and Geometry, in: Contemp. Math., vol. 493, American Mathematical Society, Providence, RI, 2009, pp. 299–325.
[11] A.S. Merkurjev, Essential p-dimension of $\mathrm{PGL}(p^2)$, J. Amer. Math. Soc. 23 (2010) 693–712.
[12] R.S. Pierce, Associative Algebras, Springer-Verlag, New York, 1982.
[13] Z. Reichstein, On the notion of essential dimension for algebraic groups, Transform. Groups 5 (3) (2000) 265–304.
[14] A. Rouzzi, Essential p-dimension of PGL_n, J. Algebra 328 (1) (2011) 488–494.
[15] L. Rowen, Division algebras of exponent 2 and characteristic 2, J. Algebra 90 (1) (1984) 71–83.
[16] D.J. Saltman, Lectures on Division Algebras, American Mathematical Society, Providence, RI, 1999.
[17] J.-P. Tignol, Sur les classes de similitude de corps à involution de degré 8, C. R. Acad. Sci. Paris Sér. A–B 286 (20) (1978) A875–A876.