ESSENTIAL DIMENSION AND LINEAR CODES

by

SHANE CERNELE

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

April 2014

Abstract

The essential dimension of an algebraic group G is a measure of the complexity of G-torsors. One of the central open problems in the theory of essential dimension is to compute the essential dimension of PGL_n, whose torsors correspond to central simple algebras up to isomorphism. In this thesis, we study the essential dimension of groups of the form G/μ, where G is a reductive algebraic group satisfying certain properties, and μ is a central subgroup of G. In particular, we consider the case

$$G = \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$$

where each n_i a power of a single prime p, which is a generalization of the group $\mathrm{PGL}_{p^a} = \mathrm{GL}_{p^a} / \mathbb{G}_m$. We will see that torsors for G/μ correspond to tuples of central simple algebras satisfying certain properties. Surprisingly, computing the essential dimension of G/μ becomes easier when $r \geq 3$.

Using techniques from Galois cohomology, representation theory and the essential dimension of stacks, we give upper and lower bounds for the essential dimension of G/μ. To do this, we first attach a linear 'code' $\overline{C_\mu}$ to the central subgroup μ, and define a weight function on $\overline{C_\mu}$. Our upper and lower bounds are given in terms of a minimal weight generator matrix for $\overline{C_\mu}$. In some cases we can determine the exact value of the essential dimension of G/μ.

Preface

This dissertation is original, unpublished, independent work by the Author, S. Cernele.

Table of Contents

List of Tables

Acknowledgements

First, I would like to thank my supervisor Zinovy Reichstein. His guidance, suggestions and feedback on early versions of this thesis have been invaluable.

I would also like to thank Zinovy Reichstein and Roland Lötscher for suggesting the methods used to prove Corollary B.4, and Zinovy Reichstein for showing me the proof of Theorem 7.9.

I would like to thank my committee members Julia Gordon and Lior Silberman for their helpful questions and conversations. Also, thanks to Athena Nguyen for showing me the results of her Master's thesis, and to my fellow graduate students Mario Garcia Armas and Jerome Lefebvre for the countless mathematical discussions we've had together.

1 Introduction

1.1 Background

Informally, the essential dimension of an object is the minimum number of algebraically independent variables required to define that object. Essential dimension was introduced by Buhler and Reichstein ([BR97]) in 1997, and the definition has since been generalized by Reichstein ([R00]) and Merkurjev ([BF03]). For the definition of essential dimension see §2, and for recent surveys see [R10] and [M13].

Let k be a base field of characteristic zero. The essential dimension of an algebraic group G/k is the maximum essential dimension of an element of the first Galois cohomology set $H^1(K, G)$, over all field extensions K/k. For example, $H^1(K, \mathrm{PGL}_n)$ can be identified with central simple algebras of degree n over K (up to isomorphism), and so $\mathrm{ed}_k(\mathrm{PGL}_n)$ is the minimum number of algebraically independent variables needed to define a central simple algebra of degree n over any field extension of k. For $n \geq 5$ and odd, from [LRRS03] we have

$$\mathrm{ed}_k(\mathrm{PGL}_n) \leq \frac{1}{2}(n-1)(n-2)$$

and if $a^b \mid n$ for some $a > 1$, from [R00, Theorem 9.3 & Proposition 9.8a] we have

$$\mathrm{ed}_k(\mathrm{PGL}_n) \geq 2b$$

Stronger results are known for a 'local version' of essential dimension at a prime p, called essential p-dimension. We denote essential p-dimension by $\mathrm{ed}_k(G; p)$, and by definition $\mathrm{ed}_k(G; p) \leq \mathrm{ed}_k(G)$.

In the case where $G = \mathrm{PGL}_n$, if $n = p^a b$ with $(p, b) = 1$ then

$$\mathrm{ed}_k(\mathrm{PGL}_n; p) = \mathrm{ed}_k(\mathrm{PGL}_{p^a}; p)$$

and so we can reduce to studying only central simple algebras of p-primary

degree.

Every central simple algebra of index p becomes a cyclic algebra after a prime-to-p extension of the base field; from this one can deduce

$$\mathrm{ed}_k(\mathrm{PGL}_p; p) = 2$$

(see [RY00, Lemma 8.5.7]). When $a \geq 2$ we have the following result:

$$(a-1)p^a + 1 \leq \mathrm{ed}_k(\mathrm{PGL}_{p^a}; p) \leq p^{2a-2} + 1$$

The lower bound is from [M10] and the upper bound is from [Ru11].

The set $H^1(K, G)$ where $G = \mathrm{GL}_{p^a}/\mu_{p^s}$ $(s < a)$ corresponds to central simple algebras of degree p^a and exponent dividing p^s. The essential p-dimension of $\mathrm{GL}_{p^a}/\mu_{p^s}$ was studied in [BM12], where the authors show:

$$\begin{aligned} \mathrm{ed}_k(\mathrm{GL}_{p^a}/\mu_{p^s}; p) &\leq 2p^{2a-2} - p^a + p^{a-s} \\ \mathrm{ed}_k(\mathrm{GL}_{p^a}/\mu_{p^s}; p) &\geq \begin{cases} (a-1)2^{a-1} & \text{if } p = 2 \text{ and } s = 1 \\ (a-1)p^a + p^{a-s} & \text{otherwise} \end{cases} \end{aligned}$$

In this paper we will study the essential dimension of a certain class of groups, including the groups G/μ where $G = \mathrm{GL}_{p^{a_1}} \times \ldots \times \mathrm{GL}_{p^{a_r}}$ for some prime p, and $\mu \leq Z(G)$. The Galois cohomology of G/μ is related to r-tuples of central simple algebras; see Section 3. Surprisingly, computing the essential dimension becomes easier when $r \geq 3$.

Let C_μ be the submodule of $\mathbb{Z}^r$ consisting of all r-tuples $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ such that $\lambda_1^{x_1} \cdot \ldots \cdot \lambda_r^{x_r} = 1$ for all $(\lambda_1, \ldots, \lambda_r) \in \mu$. Let $\overline{C_\mu}$ be the (finite) image of C_μ under the natural surjection

$$\mathbb{Z}^r \to \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$$

If $(c_1, \ldots, c_r) \in \overline{C_\mu}$ then write $c = (u_1 p^{k_1}, \ldots, u_r p^{k_r})$ with $u_i \in (\mathbb{Z}/\mathrm{p}^{a_i}\mathbb{Z})^*$

and $0 \leq k_i \leq a_i$, and define the 'weight of c', denoted $\mathrm{w}(c)$, by

$$\mathrm{w}(c) = \sum_{i=1}^{r} (a_i - k_i).$$

The main result of this paper is the following. Let $(Y_1, \ldots, Y_t)$ be a generating set of $\overline{C_\mu}$ such that $\sum_{i=1}^{t} \mathrm{w}(Y_i)$ is minimal. Let $M = \sum_{i=1}^{t} p^{\mathrm{w}(Y_i)}$. Then

$$\mathrm{ed}_k(G/\mu) \geq M + (r-t) - p^{2a_1} - \ldots - p^{2a_r}$$

and for many choices of μ (when $r \geq 3$), equality holds.

1.2 Notation

We will now introduce some notation before stating our main results. The major notation is summarized in the tables throughout this section. We begin by defining some standard notation in the table below.

Table 1: General Notation

Notation	**Definition and Assumptions**
k	Base field of characteristic zero.
p	Positive prime integer.
$Z(B)$	Center of the group B.
$X(A)$	Character lattice of the diagonalizable group A.
$\mathrm{Br}(K)$	Brauer group of the field K.
$H^j(K, B)$	jth Galois cohomology group of B over K. We assume B is abelian for $j > 1$.

Good references for more information on the Brauer group include [GS06] and [BO13]. For the the definition and properties of Galois cohomology, consult [S97].

We now proceed to define the groups and maps we will study in this paper. For $i = 1, \dots, r$, let G_i be a reductive linear algebraic group with $Z(G_i) \leq \mathbb{G}_m$. In other words, we are once and for all identifying $Z(G_i)$ with a subgroup of $\mathbb{G}_m$, so that we may have the *identity character:* $Z(G_i) \hookrightarrow \mathbb{G}_m$.

Denote $\overline{G}_i = G_i/Z(G_i)$ and consider $\delta_K^i : H^1(K, \overline{G}_i) \to H^2(K, Z(G_i)) \leq \mathrm{Br}(K)$ for any K/k. Here δ_K^i is the coboundary map induced from the sequence

$$1 \to Z(G_i) \to G_i \to \overline{G}_i \to 1$$

for any K/k, see [S97, Section I.5].

We will assume that the image of δ_K^i consists of elements of p-primary order for some prime p. Let p^{a_i} be the maximal index of $\delta_K^i(E)$ (over all K/k and $E \in H^1(K, \overline{G}_i)$), and let p^{b_i} be the maximal exponent of $\delta_K^i(E)$ (over all K/k and $E \in H^1(K, \overline{G}_i)$). We make the following additional assumptions:

i) For each i, $b_i \in \{1, a_i\}$.

ii) Either $Z(G_i) = \mathbb{G}_m$ for all i, or $Z(G_i) = \mu_{p^{b_i}}$ for all i. In particular, $Z(G_1) \times \cdots \times Z(G_r)$ is either connected or finite.

Let $n_i = p^{a_i}$.

Example 1.1. Examples of groups G_i satisfying $b_i \in \{1, a_i\}$ and having $Z(G_i) \in \{\mathbb{G}_m, \mu_{p^{b_i}}\}$ include:

a) GL_{n_i} and SL_{n_i} for p arbitrary, $a_i \geq 1$ ($b_i = a_i$). In this case $\overline{G}_i = \mathrm{PGL}_{n_i}$, and $H^1(K, \mathrm{PGL}_{n_i})$ classifies central simple algebras of degree n over K. The coboundary map sends a central simple algebra to its Brauer class in $\mathrm{Br}(K)$.

b) For $p = 2$, GO_{n_i}, O_{n_i}, GSP_{n_i}, and SP_{n_i} when $a_i \geq 1$ ($b_i = 1$), and $\mathrm{GO}_{n_i}^+$ and SO_{n_i} when $a_i \geq 2$ ($b_i = 1$). In these cases $H^1(K, \overline{G}_i)$ classifies

central simple algebras of degree n_i with involution (of the first kind) satisfying certain properties. The coboundary map sends a central simple algebra A with involution to the Brauer class of A in $\mathrm{Br}(K)$ (see [KMRT98, Section 29]). Note that the groups GO_n, O_n and SO_n when $p \neq 2$ have a trivial coboundary map; we discuss these groups further in Appendix C.

c) E_6 (simply connected) for $p = 3$, $a_i = 3$ ($b_i = 1$).

d) Non-abelian finite p-groups G_i where $Z(G_i) \cong \mu_p$ and the dimension of a minimal faithful representation of G_i is n_i (see [KM08, Theorem 4.4]). In this case, $a_i \geq 1$ and $b_i = 1$.

We summarize the notation related to the groups G_i in the table below.

Table 2: Notation for the Groups G_i

Notation	**Definition and Assumptions**
r	Positive integer.
G_i $(i = 1 \dots r)$	Reductive linear algebraic group. $Z(G_i) \leq \mathbb{G}_m$.
$\overline{G}_i$ $(i = 1, \dots, r)$	$G_i/Z(G_i)$.
δ_K^i	The coboundary map $H^1(K, \overline{G}_i) \to H^2(K, Z(G_i))$ induced from the sequence $1 \to Z(G_i) \to G_i \to \overline{G}_i \to 1$. We assume every element of $\mathrm{im}(\delta_K^i)$ has p-primary order.
a_i	Maximum index of an element in $\mathrm{im}(\delta_K^i)$ over all K/k.
	Continued on next page...

Table 2: Notation for the Groups G_i (continued)

Notation	**Definition and Assumptions**
b_i	Maximum exponent of an element in $\mathrm{im}(\delta_K^i)$ over all K/k. We assume $b_i \in \{1, a_i\}$. If $\lvert Z(G_i)\rvert < \infty$ then we assume $Z(G_i) \cong \mu_{p^{b_i}}$.
n_i	p^{a_i}.

We now proceed to define the groups whose essential dimension we are interested in, and some of their related structures. Let

$$G = G_1 \times \cdots \times G_r, \quad \text{and} \quad \overline{G} = G/Z(G) = \prod_{i=1}^{r} \overline{G}_i.$$

Let μ be a subgroup of $Z(G)$ (in particular, $\mu \leq \mathbb{G}_m^r$), and let

$$\delta_K : H^1(K, G) \to H^2(K, Z(G)/\mu)$$

be the coboundary map induced from the sequence $1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1$. We will compute bounds on the essential dimension of G/μ over k.

From $\mu \leq Z(G)$ we get a surjective map $X(Z(G)) \to X(\mu)$ given by restricting a character of $Z(G)$ to μ. We define

$$C_\mu \;=\; \ker\left(X(Z(G)) \twoheadrightarrow X(\mu)\right)$$

and observe that $C_\mu \cong X(Z(G)/\mu)$.

Note that $X(Z(G))$ is a $\mathbb{Z}$-module of rank r, and comes with a canonical coordinate system. This coordinate system is determined by r generators, which are the r maps $Z(G) \to Z(G_i) \hookrightarrow \mathbb{G}_m$. Thus we can think of an

element of C_μ as an r-tuple $(z_1, \ldots, z_r)$, where

$$z_i \in \begin{cases} \mathbb{Z} & \text{if } Z(G_i) \cong \mathbb{G}_m \\ \mathbb{Z} / \mathrm{p}^{b_i} \mathbb{Z} & \text{if } Z(G_i) \cong \mu_{p^{b_i}} \end{cases}$$

and we can write C_μ explicitly as:

$$C_\mu = \{(c_1, \ldots, c_r) \in X(Z(G)) \mid \lambda_1^{c_1} \cdot \ldots \cdot \lambda_r^{c_r} = 1 \text{ for all } (\lambda_1, \ldots, \lambda_r) \in \mu\}.$$

Set $F = \mu_{p^{b_1}} \times \cdots \times \mu_{p^{b_r}} \leq Z(G)$, and for any subgroup τ of $Z(G)$, define $\tau_f = \tau \cap F$. Given $\mu \leq Z(G)$, we define the *code associated to* μ, denoted $\overline{C_\mu}$, to be the image of C_μ under the natural surjection $X(Z(G)) \twoheadrightarrow X(Z(G)_f)$. In other words, $\overline{C_\mu}$ is the code given by reducing the i^{th} coordinate in each element of C_μ modulo p^{b_i}. Note that this construction is trivial in the case where $|Z(G)| < \infty$, since in this case we assumed $Z(G) = F$ and hence $C_\mu = \overline{C_\mu}$.

Remark 1.2. $\overline{C_\mu}$ can be identified with $X(Z(G)_f/\mu_f)$, and thus if α and β are subgroups of $Z(G)$, then $\alpha_f = \beta_f$ if and only if $\overline{C_\alpha} = \overline{C_\beta}$.

We will now assign 'weights' to the elements of our code. Let $\mu \leq Z(G)$ with associated code $\overline{C_\mu}$. Define a map $v_i : \mathbb{Z}/p^{b_i}\mathbb{Z} \to \mathbb{Z}$ as follows. For $z \in \mathbb{Z}/p^{b_i}\mathbb{Z}$, if $z = 0$ then define $v_i(z) = a_i$. Otherwise, write $z = up^k$ with u invertible in $\mathbb{Z}/p^{b_i}\mathbb{Z}$ and $0 \leq k < b_i$, and define $v_i(z) = k$.

For an element $z = (z_1, \ldots, z_r) \in \overline{C_\mu}$, we define the **weight of** z, denoted $\mathrm{w}(z)$ to be:

$$\mathrm{w}(z) = \sum_{i=1}^{r} (a_i - v_i(z_i))$$

Remark 1.3. In the case where $a_i = b_i = 1$ for all i, $\mathrm{w}(z)$ is the usual Hamming weight of z.

Remark 1.4. Since we assumed $b_i \in \{1, a_i\}$, our weight function has the following important property. Suppose that for $i = 1, \ldots, r$, E_i is a central

simple algebra with index p^{a_i} and exponent p^{b_i}, and $z_i \in \mathbb{Z}/p^{b_i}\mathbb{Z}$. Then $\mathrm{ind}(E_i^{\otimes z_i}) = p^{a_i - v_i(z_i)}$, and further if $z = (z_1, \ldots, z_r) \in \overline{C_\mu}$ then

$$\mathrm{ind}(E_1^{\otimes z_1} \otimes \cdots \otimes E_r^{\otimes z_r}) \leq \prod_{i=1}^{r} \mathrm{ind}(E_i^{\otimes z_i}) = p^{\mathrm{w}(z)}$$

We summarize the notation related to the group G/μ and the code associated to μ in the following table.

Table 3: Notation Related to G and μ

Notation	**Definition and Assumptions**
G	$G_1 \times \cdots \times G_r$. We assume $Z(G)$ is finite or connected.
$\overline{G}$	G/Z(G).
μ	Subgroup of $Z(G)$.
C_μ	The $\mathbb{Z}$-module given by $\ker\left(X(Z(G)) \to X(\mu)\right)$. Explicitly, C_μ is given by: $\left\{ \begin{array}{c} (c_1, \ldots, c_r) \in X(Z(G)) \mid \lambda_1^{c_1} \cdot \ldots \cdot \lambda_r^{c_r} = 1, \\ \forall\, (\lambda_1, \ldots, \lambda_r) \in \mu \end{array} \right\}$
	Continued on next page...

Table 3: Notation Related to G and μ (continued)

Notation	**Definition and Assumptions**
$\overline{C_\mu}$	Image of C_μ under the map $$X(Z(G)) \to X(\mu_{p^{b_1}} \times \cdots \times \mu_{p^{b_r}})$$ induced from $\mu_{p^{b_1}} \times \cdots \times \mu_{p^{b_r}} \hookrightarrow Z(G)$. Equivalently, $\overline{C_\mu}$ is the $\mathbb{Z}$-module given by reducing the i^{th} coordinate of C_μ modulo p^{b_i}, for $i = 1, \ldots, r$. $\overline{C_\mu}$ is called the *code associated to* μ.
w	$$\begin{aligned} \mathrm{w} : \overline{C_\mu} &\to \mathbb{Z} \\ (u_1 p^{k_1}, \ldots, u_r p^{k_r}) &\mapsto \sum_{u_i p^{k_i} \neq 0} (a_i - k_i) \end{aligned}$$ Here, $u_i \in (\mathbb{Z} \,/\, \mathrm{p}^{b_i}\, \mathbb{Z})^*$ and $0 \leq k_i \leq b_i$.
δ_K	The coboundary map $$H^1(K, G) \to H^2(K, Z(G)/\mu)$$ induced from the sequence $$1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1.$$

1.3 Main Results

We will now state the main results of this paper. We begin with a result explaining the significance of the code associated to μ.

Theorem 1.5. *Let $\mu, \tau \leq Z(G)$ and K/k. If $\overline{C_\mu} = \overline{C_\tau}$ (or equivalently, if $\mu_f = \tau_f$) then there is an isomorphism of functors $H^1(-, G/\mu) \to H^1(-, G/\tau)$. In particular, the essential dimension and essential p-dimension of G/μ depend only on the code $\overline{C_\mu}$.*

A *generator matrix* Y of a code is a matrix whose rows generate the code, and if Y is a generator matrix, then Y_i denotes the i^{th} row of the matrix and y_{ij} denotes the entry in the i^{th} row and j^{th} column.

Definition 1.6. Let Y be a generator matrix for $\overline{C_\mu}$, with rows $Y_1, \ldots, Y_t$. We say that Y is **minimal** if, for any other generator matrix Z of $\overline{C_\mu}$ with rows $Z_1, \ldots, Z_l$,

$$\sum_{i=1}^{t} \mathrm{w}(Y_i) \leq \sum_{i=1}^{l} \mathrm{w}(Z_i).$$

We can now state upper and lower bounds on the essential dimension of G/μ, where $\mu \leq Z(G)$. Recall that, by Theorem 1.5, we are free to replace μ with any $\tau \leq Z(G)$ such that $\overline{C_\mu} = \overline{C_\tau}$.

Theorem 1.7. *Let $\mu \leq Z(G)$ and let Y be a minimal generator matrix for $\overline{C_\mu}$ with rows $Y_1, \ldots, Y_t$.*

1. $\mathrm{ed}_k(G/\mu; p) \geq \left(\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)} \right) - d - \dim(\overline{G})$
2. $\mathrm{ed}_k(G/\mu) \leq \left(\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)} \right) - d + \mathrm{ed}_k(\overline{G})$

where $d = \begin{cases} t, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}$

Although the upper and lower bounds in Theorem 1.7 never meet, for many families of subgroups μ the term $\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)}$ appearing in both the upper and lower bound is much larger than any of the other terms in either formula.

Definition 1.8. Let Y be a generator matrix for $\overline{C_\mu}$. We say that Y is *very acceptable* if:

1. Each y_{ij} equals $-1, 0$ or 1 in $\mathbb{Z}/p^{b_i}\mathbb{Z}$.
2. Y contains no column of all zeroes.
3. For each i, the Hamming weight of Y_i is at least $f(p)$, where

$$f(p) = \begin{cases} 5, \text{ if } p = 2 \\ 4, \text{ if } p = 3 \\ 3, \text{ otherwise} \end{cases}$$

When G_i has a faithful representation of dimension n_i such that $Z(G_i)$ acts by the identity character (for example, every G_i in Example 1.1), we can sometimes use very acceptable generator matrices to find a stronger upper bound.

Theorem 1.9. *Suppose that G_i has a faithful representation of dimension n_i such that $Z(G_i)$ acts by the identity character, for all i. Let $\mu \leq Z(G)$ and let Y be a very acceptable minimal generator matrix for $\overline{C_\mu}$ with rows $Y_1, \ldots, Y_t$. Suppose additionally that for all $1 \leq i, j, k \leq r$, we have $a_i < a_j + a_k$ (or equivalently, $n_i < n_j \cdot n_k$). Then*

$$\mathrm{ed}_k(G/\mu) = \mathrm{ed}_k(G/\mu; p) = \left(\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)} \right) - d - \dim(\overline{G})$$

where $d = \begin{cases} t, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}$

Remark 1.10. The conditions in Theorem 1.9 that for all $1 \leq i, j, k \leq r$, $a_i < a_j + a_k$, and that Y is very acceptable can be replaced by assuming Y is an *acceptable* generator matrix. The definition of an acceptable generator matrix is more complicated to describe; see Section 6.

Example 1.11. A motivating example to keep in mind is the following. Let $n_1 = n_2 = \cdots = n_r = p^a$ for $r \geq 5$ and $a \geq 1$, and let $G_i \cong \mathrm{GL}_{n_i}$ for $1 \leq i \leq r$. Let $\mu < Z(G)$ be defined by:

$$\mu := \{(\lambda_1, \ldots, \lambda_r) \in Z(G) \mid \lambda_1 \cdot \ldots \cdot \lambda_r = 1\}$$

Thus $C_\mu = \langle (1, 1, \ldots, 1) \rangle \leq X(Z(G)) = \mathbb{Z}^r$. By Theorem 1.9, we have

$$\mathrm{ed}(G/\mu) = \mathrm{ed}(G/\mu; p) = p^{ra} - rp^2 + r - 1$$

See Section 7 for a generalization of this example.

The rest of this report is structured as follows. In §2 we discuss some preliminaries on essential dimension, including the definition. Then in §3 we study the Galois cohomology of G/μ and prove Theorem 1.5. In §4, we will discuss codes and minimal generator matrices, and in §5 we discuss the relationship between codes and subgroups of the Brauer group and prove Theorem 1.7. In §6 we prove Theorem 1.9. In §7 we discuss an interesting example, and in §8 we look at a class of codes where we can find acceptable minimal generator matrices. Throughout, all diagrams are commutative, G and $\overline{G}$ are groups of the form described in this section, and μ denotes a subgroup of $Z(G)$.

2 Preliminaries

2.1 Essential Dimension and Canonical Dimension

In this section we will give the definition of essential dimension and essential p-dimension. All fields are assumed to contain our base field k. Let $\mathcal{F}$ be a covariant functor from $\mathbf{Fields}_k$ to $\mathbf{Sets}$. If we have a field extension given by $L \overset{i}{\hookrightarrow} K$ and $\alpha \in \mathcal{F}(L)$, then we write $(\alpha)_K$ for $\mathcal{F}(i)(\alpha) \in \mathcal{F}(K)$.

Let K/k be a field extension and $\alpha \in \mathcal{F}(K)$. If K/L is a field extension, then we say α *descends* to L if there exists $\alpha_0 \in \mathcal{F}(L)$ that that $(\alpha_0)_K = \alpha$. The essential dimension of α (over k), denoted $\mathrm{ed}_k(\alpha)$, is defined to be the minimum value of $\mathrm{trdeg}_k(L)$ over all fields L such that such that α descends to L.

The essential dimension of $\mathcal{F}$ (over k), denoted $\mathrm{ed}_k(\mathcal{F})$ is defined to be the maximum value of $\mathrm{ed}_k(\alpha)$, where K runs over all field extensions of k and $\alpha \in \mathcal{F}(K)$.

Essential p-dimension is defined similarly, for a covariant functor $\mathcal{F}$ from $\mathbf{Fields}_k$ to $\mathbf{Sets}$. If K/L and $\alpha \in \mathcal{F}(K)$ then we say α *p-descends* to L if there exists $\alpha_0 \in \mathcal{F}(L)$ and a finite exenstion K'/K of degree prime-to-p, such that $(\alpha_0)_{K'} = (\alpha)_{K'}$. The essential p-dimension of α (over k), denoted $\mathrm{ed}_k(\alpha; p)$, is defined to be the minimum value of $\mathrm{trdeg}_k(L)$ over all fields L such that such that α p-descends to L. The essential p-dimension of $\mathcal{F}$, denoted $\mathrm{ed}_k(\mathcal{F}; p)$, is defined to be the maximum value of $\mathrm{ed}_k(\alpha; p)$, where K runs over all field extensions of k and $\alpha \in \mathcal{F}(K)$. We have from the definitions that $\mathrm{ed}_k(\mathcal{F}) \geq \mathrm{ed}_k(\mathcal{F}; p)$.

For an algebraic group G, the essential dimension (resp. p-dimension) of G is defined to be the essential dimension (resp. p-dimension) of the Galois cohomology functor $\mathrm{ed}_k(H^1(-, G))$. For example, by Hilbert's Theorem 90 $H^1(K, \mathrm{GL}_n) = 0$ for all K, and hence $\mathrm{ed}_k(\mathrm{GL}_n) = \mathrm{ed}_k(\mathrm{GL}_n; p) = 0$ (for any p).

It is clear from the definitions that for any group G, $\mathrm{ed}_k(G) \geq \mathrm{ed}_k(G; p)$.

However, for some groups $\mathrm{ed}_k(G)$ is strictly greater than $\mathrm{ed}_k(G;p)$ for any prime p; for an example, see [D10].

We now recall some results from the theory of essential dimension.

Theorem 2.1. *[BF03, Lemma 1.9] Let $\mathcal{F}$, $\mathcal{T}$ be functors from* $\mathbf{Fields}_k$ *to* **Sets**. *If there is a surjective morphism of functors $\mathcal{F} \twoheadrightarrow \mathcal{T}$ then*

$$ed_k(\mathcal{T}) \leq \mathrm{ed}_k(\mathcal{F}).$$

Theorem 2.2. *[S97, III.4.3, Lemma 6] Let G be a reductive linear algebraic group, and N be the normalizer of the maximal torus in G. Then the induced map in cohomolgy $H^1(-,N) \to H^1(-,G)$ is surjective. In particular, by Theorem 2.1,*

$$\mathrm{ed}_k(G) \leq \mathrm{ed}_k(N).$$

Let G be a linear algebraic group.

Definition 2.3. A representation $\rho : G \to \mathrm{GL}(V)$ is called *generically free* if there exists a dense open subset $U \subset V$ such that the geometric stabilizer of every point x of U is trivial.

Remark 2.4. Note that if V is a faithful representation of G, then G acts generically freely on the vector space $\mathrm{End}(V)$. This is because, with $U = \mathrm{Aut}(V) \subset \mathrm{End}(V)$, it is easy to see that the geometric stabilizer of every point in U is trivial. In particular, generically free representations always exist for linear algebraic groups.

Theorem 2.5. *[BF03, Proposition 4.11] Suppose G has a generically free repesentation $\rho : G \to \mathrm{GL}(V)$. Then*

$$\mathrm{ed}_k(G) \leq \dim(V) - \dim(G).$$

A special case of essential dimension is *canonical dimension*. For a functor $\mathcal{F} : \mathbf{Fields}_k \to \mathbf{Sets}$, we define the detection functor $\mathcal{D}_\mathcal{F} : \mathbf{Fields}_k \to \mathbf{Sets}$ as follows. For a field K,

$$\mathcal{D}_{\mathcal{F}}(K) = \begin{cases} \{*\}, & \text{if } \mathcal{F}(K) \neq \emptyset; \\ \emptyset, & \text{if } \mathcal{F}(K) = \emptyset. \end{cases}$$

We define the canonical dimension (resp. p-dimension) of $\mathcal{F}$ to be the essential dimension (resp. p-dimension) of $\mathcal{D}_{\mathcal{F}}$, and denote it by $\mathrm{cdim}_k(\mathcal{F})$ (resp. $\mathrm{cdim}_k(\mathcal{F}; p)$). For more on canonical dimension, including the definition of the canonical dimension of an algebraic group (which will not be used in this paper), see [M13, Section 4].

2.2 Quotient Stacks

A good reference for background on quotient stacks is [M13, Section 5].

Let $1 \to D \to H \to \overline{H} \to 1$ be an exact sequence of algebraic groups over k, where D is diagonalizable and central in H. For any K/k, let $d_K : H^1(K, \overline{H}) \to H^2(K, D)$ be the coboundary map. Let K/k and $E \in H^1(K, \overline{H})$, and view E as an $\overline{H}$-torsor over K. In particular, E is an H-scheme via the map $H \to \overline{H}$. We define a fibered category over the category of schemes over K (called the quotient stack for the action of H on E) and denote it by $[E/H]$. The objects over a scheme X are diagrams (T, π, ϕ) given by:

$$\begin{array}{ccc} T & \xrightarrow{\phi} & E \\ {\scriptstyle \pi}\downarrow & & \\ X & & \end{array}$$

where ϕ is H-equivariant and π is an H-torsor. A morphism between objects (T, π, ϕ) and (T', π', ϕ') over X is a G-equivariant morphism from T to T' satisfying the obvious commuting relationships over E and X.

Remark 2.6. (See [M13, Section 5c]) If L/K is a field extension, then an object (T, π, ϕ) of $[E/H](L)$ induces an H-equivariant map from T to E_L over L, which in particular implies that E_L is the image of T under the

induced map in cohomology $H^1(L,H) \to H^1(L,\overline{H})$. It follows that for any field L/K,

$$\begin{aligned} [E/H](L) \neq \emptyset &\iff E_L \text{ is in the image of } H^1(L,H) \to H^1(L,\overline{H}) \\ &\iff d_L(E_L) = 0 \in H^2(L,D) \end{aligned}$$

We now have a functor $\mathcal{F} : \mathbf{Fields}_K \to \mathbf{Sets}$ given by

$$\mathcal{F}(L) = ([E/H](L)) \,/ \approx$$

for any L/K. This allows us to define $\mathrm{ed}_K([E/H]) = \mathrm{ed}_K(\mathcal{F})$, $\mathrm{ed}_K([E/H];p) = \mathrm{ed}_K(\mathcal{F};p)$, $\mathrm{cdim}_K([E/H]) = \mathrm{cdim}_K(\mathcal{F})$, and $\mathrm{cdim}_K([E/H];p) = \mathrm{cdim}_K(\mathcal{F};p)$.

The following theorem provides a relationship between the essential dimension of an algebraic group and the essential dimension of certain quotient stacks.

Theorem 2.7. *(See [M13, Section 5]) Let $1 \to D \to H \to \overline{H} \to 1$ be an exact sequence of algebraic groups, with D central and diagonalizable. Then*

1. $\mathrm{ed}_k(H;p) \geq \max_{A,L} (\mathrm{cdim}_L([A/H];p)) + \mathrm{ed}_k(D;p) - \dim(\overline{H})$
2. $\mathrm{ed}_k(H) \leq \max_{A,L} (\mathrm{cdim}_L([A/H])) + \mathrm{ed}_k(D) + \mathrm{ed}_k(\overline{H})$

Here, L runs over all field extensions of k, $A \in H^1(L,\overline{H})$.

Proof. Choose K/k and $E \in H^1(K,\overline{H})$. Then $\mathrm{ed}_k(H;p) \geq \mathrm{ed}_K(H;p)$ and from [BRV11, Corollary 3.3] (see also [M13, Corollary 5.7]), we have:

$$\mathrm{ed}_K(H;p) \geq \mathrm{ed}_K([E/H];p) - \dim(\overline{H}).$$

To complete the proof of the lower bound, we must show $\mathrm{ed}_K([E/H];p) = \mathrm{cdim}_K([E/H];p) + \mathrm{ed}_k(D;p)$. If $D \cong (\mu_p)^t$ for some t then the result follows from [M13, Theorem 5.11]. One can check that their proof holds with only

trivial modifications in the general case when D is only assumed to be central and diagonalizable. Alternatively, if we assume the image of $H^1(-, \overline{H}) \to H^2(-, D)$ consists only of elements of p-primary order (which is true in all of our applications), then using [M13, Theorem 5.11] and [KM08, Theorem 4.4 & Remark 4.5] we can deduce the result for a particular (E, K) with $\mathrm{cdim}_K([E/H]; p) = \max_{A,L}(\mathrm{cdim}_L([A/H]; p))$; see Corollary B.4 in Appendix B.

The upper bound can be deduced from [M13, Corollary 5.8 & Proposition 5.10]. For completeness we provide a direct proof in Appendix B. □

3 Galois Cohomology of G/μ

In this section we will discuss the Galois Cohomology of G/μ, and prove a stronger version of Theorem 1.5. The following theorem is a more general version of [N11, Theorem 5.1.3].

Theorem 3.1. *Suppose $Z(G)$ is a torus and let $\mu \leq Z(G)$. From $\mu \hookrightarrow Z(G)$ we get $G/\mu \twoheadrightarrow \overline{G}$, and hence an induced map in cohomology $H^1(K, G/\mu) \to H^1(K, \overline{G})$ for any K/k. Then*

$$H^1(K, G/\mu) \to H^1(K, \overline{G})$$

is injective, and identifies $H^1(K, G/\mu)$ with r-tuples $(E_1, \ldots, E_r)$, with $E_i \in H^1(K, \overline{G}_i)$, such that for all $\chi = (c_1, \ldots, c_r) \in \overline{C_\mu}$,

$$\delta_K^1(E_1)^{\otimes c_1} \otimes \cdots \otimes \delta_K^r(E_r)^{\otimes c_r} = 0 \ \in \mathrm{Br}(K)$$

Note that $\delta_K^i(E_i)^{\otimes c_i}$ is always well-defined since $\exp(\delta_K^i(E_i)) \mid p^{b_i}$.

Corollary 3.2. *From $\mu_f \hookrightarrow \mu$ we get $G/\mu_f \twoheadrightarrow G/\mu$, and hence an induced map in cohomology $\gamma : H^1(K, G/\mu_f) \to H^1(K, G/\mu)$ for any K/k. The map γ is a bijection.*

We can use these two results to prove Theorem 3.4, which is a stronger version of Theorem 1.5.

Definition 3.3. Two codes are called (linearly) **equivalent** if one can be obtained from the other by repeatedly performing the following operations:

1. Permuting entries i and j in every vector of the code, for any i, j with $G_{n_i} \cong G_{n_j}$.

2. Multiplying the i^{th} entry in every vector of the code by any $\lambda \in (\mathbb{Z}/p^{b_i}\mathbb{Z})^*$, for any i with $G_i \cong \mathrm{GL}_{n_i}$.

Theorem 3.4. *Let $\mu, \tau \leq Z(G)$ and K/k. If $\overline{C_\mu}$ is equivalent to $\overline{C_\tau}$, then there is an isomorphism of functors $H^1(-, G/\mu) \to H^1(-, G/\tau)$. In particular, the essential dimension and essential p-dimension of G/μ depend only on $\overline{C_\mu}$ up to equivalence.*

Proof of Theorem 3.4. In the case where $\overline{C_\mu} = \overline{C_\tau}$, the result is immediate from Corollary 3.2 and Remark 1.2. Now using the definition of equivalence and induction, we may assume $\overline{C_\mu}$ is obtained from $\overline{C_\tau}$ by either permuting entries i and j where $G_i \cong G_j$, or by multiplying the i^{th} entry in every vector of $\overline{C_\tau}$ by some $\lambda \in (\mathbb{Z}/p^{b_i}\mathbb{Z})^*$, for some i with $G_i \cong \mathrm{GL}_{n_i}$. In the former case, the automorphism of G which swaps G_i with G_j sets up an isomorphism $G/\mu \cong G/\tau$ and the result follows. In the latter case we must have that $Z(G)$ is a torus, and using the description of $H^1(K, G/\mu)$ given by Theorem 3.1, it is easy to check that

$$\begin{array}{rcl} H^1(K, G/\mu) & \to & H^1(K, G/\tau) \\ (E_1, \ldots, E_r) & \mapsto & (E_1, \ldots, E_{i-1}, [E_i^{\otimes\lambda}], E_{i+1}, \ldots, E_r) \end{array}$$

is an isomorphism. Here, $[E_i^{\otimes\lambda}]$ means the algebra of degree n_i which is Brauer equivalent to $E_i^{\otimes\lambda}$ (such an algebra is unique up to isomorphism). $\square$

We will now prove Theorem 3.1 and Corollary 3.2, beginning with a number of elementary results from Galois cohomology. Throughout, we will identify $H^2(K, \mathbb{G}_m^r)$ with $\prod_{i=1}^{r} H^2(K, \mathbb{G}_m)$ in the usual way.

Remark 3.5. Let $a = (a_1, \ldots, a_r) \in X(\mathbb{G}_m^r)$. Then the induced map in cohomology is easily seen to be given by:

$$\begin{aligned} a_* : \prod_{i=1}^{r} H^2(K, \mathbb{G}_m) &\to H^2(K, \mathbb{G}_m) \\ (x_1, \ldots, x_r) &\mapsto x_1^{a_1} \cdot x_2^{a_2} \cdot \ldots \cdot x_r^{a_r} \end{aligned}$$

Proposition 3.6. *(See [N11, Lemma 5.1.2]) Let K/k be a field extension.*

1. *If $i : A \hookrightarrow B$ is injective, where A and B are diagonalizable groups, then $i_* : H^2(K, A) \to H^2(K, B)$ is injective. In particular, we can identify $H^2(K, A)$ as a subgroup of $H^2(K, B)$.*

2. *Suppose $A \leq \mathbb{G}_m^r$, thus giving $X(G_m^r/A)$ a coordinate system. Then the image of the map $H^2(K, A) \to H^2(K, \mathbb{G}_m^r)$ identifies $H^2(K, A)$ with the subgroup of $H^2(K, \mathbb{G}_m)^r$ consisting of r-tuples $(A_1, \dots A_r)$ such that for all $\chi = (c_1, \dots, c_r) \in X(G_m^r/A)$,*

$$A_1^{c_1} \otimes \cdots \otimes A_r^{c_r} = 0 \in H^2(K, \mathbb{G}_m)$$

Proof. 1. Put A into any exact sequence $1 \to A \to \mathbb{G}_m^l \to \mathbb{G}_m^l/A \to 1$. Then since $\mathbb{G}_m^l/A$ is a split torus, we use the long exact sequence in cohomology and Hilbert's Theorem 90 to get:

$$0 \to H^2(K, A) \to H^2(K, \mathbb{G}_m^l)$$

It follows that $H^2(K, A) \to H^2(K, \mathbb{G}_m^r)$ is injective. Now, choose any embedding $j : B \hookrightarrow \mathbb{G}_m^q$. Then $A \overset{i}{\hookrightarrow} B \overset{j}{\hookrightarrow} \mathbb{G}_m^q$ and we get the following diagram:

$$\begin{array}{ccc} H^2(K, A) & \xrightarrow{i_*} & H^2(K, B) \\ {\scriptstyle (j\circ i)_*}\downarrow & \swarrow{\scriptstyle j_*} & \\ H^2(K, \mathbb{G}_m^q) & & \end{array}$$

From our previous argument we know that $(j \circ i)_*$ is injective, and hence so is i_*.

2. From $1 \to A \to \mathbb{G}_m^r \overset{\mathrm{p}}{\to} \mathbb{G}_m^r/A \to 1$ we get the induced sequence in cohomology

$$H^2(K, A) \to H^2(K, \mathbb{G}_m^r) \overset{\mathrm{p}_*}{\to} H^2(K, \mathbb{G}_m^r/A)$$

By part (1), we can identify $H^2(K,A)$ with its image in $H^1(K,\mathbb{G}_m^r)$, and by exactness this image equals $\ker(\mathrm{p}_*)$. Let $Y=(Y_1,\dots,Y_r)\in H^2(K,\mathbb{G}_m^r)$. Since $\mathbb{G}_m^r/A$ is diagonalizable, $\mathrm{p}_*(Y)=0$ if and only if $\chi_*(\mathrm{p}_*(Y))=0$ for all $\chi\in X(\mathbb{G}_m^r/A)\leq X(\mathbb{G}_m^r)$. If $\chi=(a_1,\dots,a_r)\in X(G_m^r/A)$ then by Remark 3.5, $\chi_*(\mathrm{p}_*(Y))=Y_1^{\otimes a_1}\otimes\cdots\otimes Y_r^{\otimes a_r}$, and the result follows.

□

Proof of Theorem 3.1. We argue as in [N11, §5.1]. Consider the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & \prod_{i=1}^r \overline{G_i} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \tau} & & \downarrow & & \| & & \\ 1 & \longrightarrow & Z(G)/\mu & \longrightarrow & G/\mu & \xrightarrow{\pi} & \prod_{i=1}^r \overline{G_i} & \longrightarrow & 1 \end{array}$$

Since $Z(G)/\mu$ is a split torus, we can use the long exact sequences in cohomology and Hilbert's Theorem 90 to get the following diagram with exact rows:

$$\begin{array}{ccccccc} & & & & H^1(K,\prod_{i=1}^r \overline{G_i}) & \xrightarrow{(\delta_K^1,\dots,\delta_K^r)} & H^2(K,Z(G)) \\ & & & & \| & & \downarrow{\scriptstyle \tau_*} \\ 0 & \longrightarrow & H^1(K,G/\mu) & \xrightarrow{\pi_*} & H^1(K,\prod_{i=1}^r \overline{G_i}) & \xrightarrow{\delta_K} & H^2(K,Z(G)/\mu) \end{array}$$

By [S97, I.5, Proposition 42], π_* is injective. Thus we may identify $H^1(K,G/\mu)$ with the set of r-tuples $(E_1,\dots,E_r)$, $E_i\in H^1(K,\overline{G_i})$, such that $(\delta_K^1(E_1),\dots,\delta_K^r(E_r))\in\ker\tau_*$. From the exact sequence

$$1\to\mu\to Z(G)\xrightarrow{\tau}Z(G)/\mu\to 1$$

$\ker(\tau_*)$ equals

$$\operatorname{im}\left(H^2(K,\mu) \to H^2(K, Z(G))\right)$$

Viewed inside $\mathrm{Br}(K)^r$, this is the same as the image of the map $H^2(K,\mu) \to H^2(K, \mathbb{G}_m^r)$. Since the exponent of $\delta_K^i(E_i)$ divides p^{b_i} and $\overline{C_\mu}$ is obtained from C_μ by reducing the i^{th} coordinate modulo p^{b_i}, the result follows from Proposition 3.6.2.

□

Proof of Corollary 3.2. The result is trivial if $Z(G)$ is finite since in this case we assumed $\mu = \mu_f$. Thus assume $Z(G)$ is a torus. Consider the following diagram:

$$\begin{array}{ccc} H^1(K, G/\mu) & \xrightarrow{\gamma} & H^1(K, G/\mu_f) \\ \downarrow{\scriptstyle \pi_*} & \swarrow{\scriptstyle \pi_{f*}} & \\ H^1(K, \overline{G}) & & \end{array}$$

By Theorem 3.1, π_* and π_{f*} are injective. Since $\exp(\delta_K^i(E_i)) \mid p^{b_i}$, then also by Theorem 3.1 π_* and π_{f*} have the same image. It follows that γ is a bijection. □

In the sequel, δ_K will continue to denote the coboundary map $H^1(K, \overline{G}) \to H^2(K, Z(G)/\mu)$.

Definition 3.7. For any K/k and $E \in H^1(K, \overline{G})$ we have a map

$$\begin{aligned} \Psi_{E,K} : C_\mu &\to \mathrm{Br}(K) \\ \chi &\mapsto \chi_* \circ \delta_K(E) \end{aligned}$$

Clearly $\Psi_{E,K}$ factors through $\overline{\Psi}_{E,K} : \overline{C_\mu} \to \mathrm{Br}(K)$ by definition of $\overline{C_\mu}$. In the sequel, if $(c_1, \ldots, c_r) \in \overline{C_\mu}$ (or C_μ) and $E_i \in H^1(K, G_i)$ for all i, then we will write

$$[\delta_K^1(E_1)^{\otimes c_1} \otimes \cdots \otimes \delta_K^r(E_r)^{\otimes c_r}]$$

to mean the Brauer class of

$$[\delta_K^1(E_1)^{\otimes c_1'} \otimes \cdots \otimes \delta_K^r(E_r)^{\otimes c_r'}]$$

where $(c_1', \ldots, c_r')$ is any set of integer representatives for $(c_1, \ldots, c_r)$ respectively.

We end this section with the following result, which follows easily from the proof of Theorem 3.1.

Lemma 3.8. *Let K/k and $c = (c_1, \ldots, c_r) \in \overline{C_\mu}$. Let $\delta_K^i : H^1(K, \overline{G}_i) \to H^2(K, Z(G_i))$, and view $H^2(K, Z(G_i)) \leq \mathrm{Br}(K)$ via the inclusion $Z(G_i) \hookrightarrow \mathbb{G}_m$. If $E = (E_1, \ldots, E_r) \in H^1(K, \overline{G})$ with each $E_i \in H^1(K, \overline{G_i})$, then*

$$\overline{\Psi}_{E,K}(c) = [\delta_K^1(E_1)^{\otimes c_1} \otimes \cdots \otimes \delta_K^r(E_r)^{\otimes c_r}]$$

4 On Minimal Generator Matrices

The $\mathbb{Z}$-module $\overline{C_\mu}$ can be thought of as a $\mathbb{Z}/p^b\mathbb{Z}$-module, where $b := \max\{b_1, \ldots, b_r\}$. In this section we will develop some preliminary algebraic results for this context. In particular, we show in Example 4.8 that if we replaced our weight function w with the weight function p^{w}, then the set of minimal generator matrices would remain unchanged. We assume for simplicity that generating sets are ordered and do not contain 0.

Let R be a local ring, I the unique maximal ideal of R, and let M be a finitely generated R-module. For $m \in M$, let $\overline{m}$ denote the image of m in M/IM. The following lemma can be deduced from Nakayama's Lemma, and is an immediate consequence of [AM69, Proposition 2.8].

Lemma 4.1. *The set $\{m_1, \ldots, m_t\}$ is a generating set of minimal size for M as an R-module if and only if $\{\overline{m_1}, \ldots, \overline{m_t}\}$ is a basis for M/IM as an R/I-vector space.*

Let $w : M \to \mathbb{Z}_{\geq 0}$ be a function with $w(m) \neq 0$ if $m \neq 0$. For each generating set $B = \{m_1, \ldots, m_t\}$ of M, we define

$$w(B) := (w(m_1), \ldots, w(m_t), 0, 0, \ldots) \in \mathbb{Z}^{\mathbb{N}}$$

We define $w_{ord}(B)$ to be the element of $\mathbb{Z}^{\mathbb{N}}$ obtained by rearranging the entries of $w(B)$ in decreasing order, and we call $w_{ord}(B)$ the w-profile of B.

Remark 4.2. If B is arranged in weight-decreasing order, then $w_{ord}(B) = w(B)$.

If γ is a w-profile of M, we call a generating set $B_\gamma = \{\beta_1, \ldots, \beta_l\}$ a *representative generating set for* γ if the w-profile of B_γ equals γ.

We put a partial order $\leq$ on $\mathbb{Z}^{\mathbb{N}}$ as follows. For $\gamma, \beta \in \mathbb{Z}^{\mathbb{N}}$, $\gamma \leq \beta$ if $\gamma_i \leq \beta_i$ for all $i \geq 1$, where γ_i denotes the i^{th} component of $\gamma \in \mathbb{Z}^{\mathbb{N}}$. Let $\mathrm{Prof}(M)$ (or, $\mathrm{Prof}_w(M)$) denote the set of w-profiles of generating sets of M.

Theorem 4.3. $(\mathrm{Prof}(M), \leq)$ *has a unique minimal element, and this element is comparable to every other element.*

Proof. $\mathrm{Prof}(M)$ has no infinite descending totally ordered chain, so it suffices to show that there is a unique minimal element. Towards a contradiction, suppose X and Y are representative generating sets for distinct minimal elements of $\mathrm{Prof}(M)$. By Lemma 4.1, both X and Y must have the same size, say t. Thus write $X = \{x_1, \ldots, x_t\}$ and $Y = \{y_1, \ldots, y_t\}$ with $w(x_1) \geq \cdots \geq w(x_t)$ and $w(y_1) \geq \cdots \geq w(y_t)$. Suppose s is minimal such that $w(x_i) = w(y_i)$ for all $i > s$. Since by assumption the w-profiles of X and Y are distinct, $s \geq 1$. Without loss of generality, assume $w(x_s) < w(y_s)$.

We can extend the set $\{x_s, \ldots, x_t\}$ to a minimal generating set of M by adding elements of Y. That is, for some $J = \{j_1, \ldots, j_{s-1}\} \subset Y$ with $w(j_1) \geq w(j_2) \geq \cdots \geq w(j_{s-1})$, we have that

$$\{\overline{j_1}, \ldots, \overline{j_{s-1}}, \overline{x_s}, \ldots, \overline{x_t}\}$$

is a basis for M/IM as an R/I-vector space. By Lemma 4.1,

$$\Gamma := \{j_1, \ldots, j_{s-1}, x_s, \ldots, x_t\}$$

generates M as an R-module.

We will now compare the weights of the elements of Γ with the weights of the elements of Y. By construction, $w(x_i) = w(y_i)$ for $s+1 \leq i \leq t$, and $w(x_s) < w(y_s)$ by assumption. Since J is an ordered subset of Y and $w(y_1), \ldots, w(y_{s-1})$ are the largest $s-1$ weights of elements in Y, we have $w(j_i) \leq w(y_i)$ for $1 \leq i \leq s-1$. Thus we have $w(\Gamma) < w(Y) = w_{ord}(Y)$. It remains to show that $w_{ord}(\Gamma) < w_{ord}(Y)$, since this would contradict the minimality of Y.

Let $j_i = x_i$ for $s \leq i \leq t$ so that we may write

$$\Gamma := \{j_1, \ldots, j_{s-1}, j_s, \ldots, j_t\}.$$

If there exists a, b with $a < b$ such that $w(j_a) < w(j_b)$, then we swap these two elements to get a new generating set Γ'. We must show that $w(\Gamma') < w_{ord}(Y)$, since then after finitely many such swaps we obtain a generating set Γ'', which is just Γ rearranged into weight-decreasing order. Thus inductively we would have $w(\Gamma'') < w_{ord}(Y)$, and hence:

$$w_{ord}(\Gamma) = w_{ord}(\Gamma'') = w(\Gamma'') < w_{ord}(Y).$$

Note that the first inequality is true because Γ and Γ'' contain the same elements, and the second equality follows from Remark 4.2.

Since Γ only changes in positions a and b, it is enough to show that $w(j_b) \leq w(y_a)$ and $w(j_a) < w(y_b)$ (note that the second inquality is automatically strict). Since $w(\Gamma) < w(Y)$, we have $w(j_a) \leq w(y_a)$ and $w(j_b) \leq w(y_b)$, and since Y is in decreasing order, we have $w(y_b) \leq w(y_a)$. Thus the first inequality follows from $w(j_b) \leq w(y_b) \leq w(y_a)$, and the second inequality follows from $w(j_a) < w(j_b) \leq w(y_b)$. □

Corollary 4.4. *A generating set $B = \{m_1, \ldots, m_l\}$ of M minimizes $\sum_{i=1}^{l} w(m_i)$ if and only if $w_{ord}(B)$ is the minimal element of* $\mathrm{Prof}(M)$.

Corollary 4.5. *Suppose we form a generating set of M inductively as follows: Select $m_1 \in M$ with $\overline{m_1} \neq 0$ such that $w(m_1)$ is minimal. Suppose $m_1, \ldots, m_i$ have been selected. Then select m_{i+1} such that $w(m_{i+1})$ is minimal among all elements $m \in M$ such that $\overline{m} \notin \langle \overline{m_1}, \ldots, \overline{m_i} \rangle$. Continue until it is not possible to select another element. Then the w-profile of the resulting generating set is the minimal element of* $\mathrm{Prof}(M)$.

Example 4.6. [KM08, Remark 4.7] Take $R = \mathbb{F}_p$, G a finite p-group, D to be the elements of exponent at most p in $Z(G)$ and $M = X(D)$, where $X(D)$ is the group of characters of D. For $x \in M$, define $w(x)$ to be the least dimension of a representation of G, say V_x, such that D acts by x. Then if

$\{x_1, \ldots, x_t\}$ is the basis provided by the greedy algorithm in Corollary 4.5, then $V_{x_1} \oplus \cdots \oplus V_{x_t}$ is a faithful representation of G of minimal dimension.

Corollary 4.7. *Suppose $\tau : M \to \mathbb{Z}$ is a function such that $\tau(m_1) \geq \tau(m_2)$ iff $w(m_1) \geq w(m_2)$. Then the generating sets $\{b_1, \ldots, b_t\}$ that minimize $\sum_{i=1}^{t} \tau(b_t)$ are precisely those whose w-profile is the minimal element of* $\mathrm{Prof}(M)$.

Example 4.8. Take $R = \mathbb{Z}/p^b\mathbb{Z}$, with M and w to be arbitrary. Taking τ to be the function p^w and applying Corollary 4.4 and Corollary 4.7 shows that choosing a generating set $\{m_1, \ldots, m_t\}$ of M that minimizes $\sum_{i=1}^{t} w(m_i)$ is the same as choosing a generating set $\{m'_1, \ldots, m'_l\}$ of M that minimizes $\sum_{i=1}^{l} p^{w(m'_i)}$.

5 Codes and the Brauer Group

In this section we will prove Theorem 1.7, which gives formulas for bounds on the essential dimension of G/μ involving the weights of elements of the associated code $\overline{C_\mu}$. We do this by establishing a relationship between $\overline{C_\mu}$ and the image of the coboundary map δ_K: $H^1(k,\overline{G}) \to H^2(K, Z(G)/\mu)$, and using this relationship to construct our bounds.

Recall from Definition 3.7 that for any K/k and $E \in H^1(K,\overline{G})$ we have a map $\Psi_{E,K} : C_\mu \to \mathrm{Br}(K)$ given by

$$\begin{aligned} \Psi_{E,K} : C_\mu &\to \mathrm{Br}(K) \\ \chi &\mapsto \chi_* \circ \delta_K(E) \end{aligned}$$

where δ_K denotes the coboundary map $H^1(k,\overline{G}) \to H^2(K, Z(G)/\mu)$. Define $T_{E,K} \leq \mathrm{Br}(K)$ to be the (finite) image of $\Psi_{E,K}$. Let $\{t_1, \ldots, t_l\}$ be a generating set of $T_{E,K}$ with $\sum_{i=1}^{l} \mathrm{ind}(t_i)$ minimal, and define

$$\mathrm{ind}(E,K) = \sum_{i=1}^{l} (\mathrm{ind}(t_i) - 1)$$

We will prove the following theorem.

Theorem 5.1. *Let $\mu \leq Z(G)$, and let Y be a minimal generator matrix for $\overline{C_\mu}$ with t rows. Then*

$$\max_{E,K}(\mathrm{ind}(E,K)) = \left(\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)}\right) - t$$

We can use this to prove Theorem 1.7 as follows. Since $T_{E,K}$ is a p-group for any K/k and $E \in H^1(K,\overline{G})$, by [KM08, Theorem 2.1 & Remark 2.9]

(and applying Remark 2.6 and Corollary 4.5) we have:

$$\mathrm{cdim}_K([E/G];p) = \mathrm{cdim}_K([E/G]) = \mathrm{ind}(E,K).$$

If $\mathrm{rank}(\overline{C_\mu}) = t$ then we can find a subgroup $\tau \leq Z(G)$ with $\mathrm{rank}(C_\tau) = t$ and $\overline{C_\tau} = \overline{C_\mu}$. Thus by Theorem 1.5 we may assume $\mathrm{rank}(C_\mu) = t$, and hence $\mathrm{ed}_k(Z(G)/\mu) = \mathrm{ed}_k(Z(G)/\mu;p) = t - d$, where

$$d = \begin{cases} t, & \text{if Z(G) is connected;} \\ 0, & \text{if Z(G) is finite.} \end{cases}$$

Theorem 1.7 is now an immediate consequence of Theorem 5.1 and Theorem 2.7. Thus, it suffices to prove Theorem 5.1, which is the content of the remainder of this section.

As in [KM08], if $1 \to D \to H \to \overline{H} \to 1$ is an exact sequence of algebraic groups with D central and diagonalizable, and $\chi \in X(D)$, let $\mathrm{Rep}^{(\chi)}(H)$ denote the category of all finite dimensional representations ρ of H such that $\rho(z)$ is scalar multiplication by $\chi(z)$ for all $z \in D$. In particular, we have the categories:

1. $\mathrm{Rep}^{\chi}(G)$ corresponding to the exact sequence $1 \to Z(G) \to G \to \overline{G} \to 1$, where $\chi \in X(Z(G))$.

2. $\mathrm{Rep}^{\chi}(G_i)$ corresponding to the exact sequence $1 \to Z(G_i) \to G_i \to \overline{G}_i \to 1$, where $\chi \in X(Z(G_i))$.

3. $\mathrm{Rep}^{\chi}(G/\mu)$ corresponding to the exact sequence $1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1$, where $\chi \in X(Z(G)/\mu) \cong C_\mu$.

Let $d_K : H^1(K, \overline{H}) \to H^2(K, D)$ be the coboundary map. If K/k is a field extension and $E \in H^1(K, \overline{H})$ then for any $\chi \in X(D)$ and $V \in \mathrm{Rep}^{(\chi)}(H)$ we have that $\mathrm{ind}(\chi_* \circ d_K(E))$ divides $\dim(V)$ (see [M13, Theorem 6.1.1]). Indeed, we have the diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}(V) & \longrightarrow & \mathrm{PGL}(V) & \longrightarrow & 1 \\ & & {\scriptstyle\chi}\uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & D & \longrightarrow & H & \longrightarrow & \overline{H} & \longrightarrow & 1 \end{array}$$

which gives the following in cohomology:

$$\begin{array}{ccc} H^1(K, \mathrm{PGL}(V)) & \longrightarrow & \mathrm{Br}(K) \\ \uparrow & & {\scriptstyle\chi_*}\uparrow \\ H^1(K, \overline{H}) & \xrightarrow{d_K} & H^2(K, D) \end{array}$$

Since the image of $H^1(K, \mathrm{PGL}(V)) \to \mathrm{Br}(K)$ consists of classes of algebras of index dividing $\dim(V)$, we see $\mathrm{ind}(\chi_* \circ d_K(E)) \mid \dim(V)$. Thus for any $\chi \in X(D)$,

$$\mathrm{ind}(\chi_* \circ d_K(E)) \mid \gcd\left\{\dim(V) \mid V \in \mathrm{Rep}^{(\chi)}(H)\right\}$$

Theorem 5.2. *[KM08, Theorem 4.4 & Remark 4.5] Let $1 \to D \to H \to \overline{H} \to 1$ as above. Then there exists a field K/k and $E \in H^1(K, \overline{H})$ such that for any $\chi \in X(D)$ we have*

$$\mathrm{ind}(\chi_* \circ d_K(E)) = \gcd\left\{\dim(V) \mid V \in \mathrm{Rep}^{(\chi)}(H)\right\}$$

Since we are studying only reductive groups in characteristic zero, this can be reduced to

$$\mathrm{ind}(\chi_* \circ d_K(E)) = \gcd\left\{\dim(V) \mid V \text{ irreducible}, \ V \in \mathrm{Rep}^{(\chi)}(H)\right\}$$

Before using this to prove Theorem 5.1, we need one more preliminary result. Recall that p^{a_i} and p^{b_i} were defined to be the maximum index and exponent respectively of $\delta_K^i(E)$ over all $E \in H^1(K, \overline{G}_i)$ and K/k. We now prove a lemma which says that they can both be attained by the same torsor.

Lemma 5.3. *For each i, there exists K/k and $E \in H^1(K, \overline{G}_i)$ such* $\operatorname{ind}(\delta^i_K(E)) = p^{a_i}$ *and* $\exp(\delta^i_K(E)) = p^{b_i}$.

Proof. Let V be a generically free representation of $\overline{G}_i$. Then there exists a 'friendly' subset $U \subset V$ (see [BF03, Theorem 4.7]), ie a dense open $\overline{G}_i$-invariant subset $U \subset V$ such that the categorical quotient $U/\overline{G}_i$ exists and $U \to U/\overline{G}_i$ is a $\overline{G}_i$-torsor. Then the generic fiber of this $\overline{G}_i$-torsor gives a $\overline{G}_i$ torsor E with base $K = k(U/\overline{G}_i)$ (ie $E \in H^1(K, \overline{G}_i)$). By [GMS03, Example 5.4], E is versal. By [KM08, Theorem 4.4 & Remark 4.5] and the discussion preceding Theorem 5.2 above, $\operatorname{ind}(\delta^i_K(E))$ is the maximum value of $\operatorname{ind}(\delta^i_L(A))$ over all L/k and $A \in H^1(L, \overline{G}_i)$, ie. $\operatorname{ind}(\delta^i_K(E)) = p^{a_i}$.

Let p^{c_i} be the exponent of $\delta^i_K(E) \in \operatorname{Br}(K)$. Consider the natural transformation

$$H^1(-, \overline{G}_i) \xrightarrow{\delta^i_-} H^2(-, Z(G_i)) \xrightarrow{P} H^2(-, Z(G_i))$$

where P is the map sending A to $A^{\otimes p^{c_i}}$ for any $A \in H^2(L, Z(G_i))$ and any L/k. This natural transformation is a cohomological invariant of $\overline{G}_i$, and in fact lands in $H^2(-, \mu_{p^{b_i}}) \subset H^2(-, Z(G_i))$. By construction, this invariant evaluates to the class of zero when applied to the versal torsor $E \in H^1(K, \overline{G}_i)$ and hence by [GMS03, Theorem 12.3], the invariant is identically zero. In particular, $\delta^i_L(E)$ has maximal exponent over all L/k and $A \in H^1(L, \overline{G}_i)$, and hence $b_i = c_i$ as required. □

Recall that for the exact sequence $1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1$, we have the notation $d = \delta$ and $\chi_* \circ d_K(E) = \Psi_{E,K}(\chi)$.

Proof of Theorem 5.1. Recall that $\{Y_1, \ldots, Y_r\}$ is assumed to be a minimal generating set of $\overline{C_\mu}$. If K/k, $E = (E_1, \ldots, E_r) \in H^1(K, \overline{G})$, and $\chi = (c_1, \ldots, c_r) \in \overline{C_\mu}$, then it follows from Remark 1.4 and Lemma 3.8 that $\operatorname{ind}(\overline{\Psi}_{E,K}(\chi)) = \operatorname{ind}([E_1^{\otimes c_1} \otimes \cdots \otimes E_r^{\otimes c_r}]) \leq p^{\mathrm{w}(\chi)}$. Since $\{\overline{\Psi}_{E,K}(Y_1), \ldots,$

$\overline{\Psi}_{E,K}(Y_r)\}$ generate $T_{E,K}$, the inequality

$$\max_{E,K}(\mathrm{ind}(E,K)) \leq \left(\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)}\right) - t$$

follows immediately.

It remains to prove

$$\max_{E,K}(\mathrm{ind}(E,K)) \geq \left(\sum_{i=1}^{t} p^{\mathrm{w}(Y_i)}\right) - t$$

We may assume that k is algebraically closed. It suffices to find K/k and $E \in H^1(K, \overline{H})$ such that $\mathrm{ind}(\Psi_{E,K}(\chi)) \geq p^{\mathrm{w}(\overline{\chi})}$ for all $\chi \in C_\mu$, or equivalently that $\mathrm{ind}(\Psi_{E,K}(\chi)) = p^{\mathrm{w}(\overline{\chi})}$ for all $\chi \in C_\mu$ (here $\overline{\chi}$ means the image of χ in $\overline{C_\mu}$). Indeed, then

$$\overline{\Psi}_{E,K} : \overline{C_\mu} \to T_{E,K}$$

will be an isomorphism, and $\mathrm{ind}(E,K)$ will be the minimum value of

$$\sum_{i=1}^{l} \left(p^{\mathrm{w}(\chi_i)}\right) - l$$

over all generating sets $\chi_1, \ldots, \chi_l$ of $\overline{C_\mu}$. By Example 4.8 this value is

$$\sum_{i=1}^{t} \left(p^{\mathrm{w}(Y_i)}\right) - t.$$

By Theorem 5.2, we can find K/k and $E \in H^1(K, \overline{G})$ such that for all $\chi \in C_\mu$,

$$\mathrm{ind}(\Psi_{E,K}(\chi)) = \gcd\left(\dim(V) \mid V \text{ irreducible}, \ V \in \mathrm{Rep}^{(\chi)}(G/\mu)\right)$$

If $\chi \in C_\mu$, then via the inclusion $C_\mu \hookrightarrow X(Z(G))$ we can view $\chi \in$

$X(Z(G))$. We can view a representation of G/μ as a representation of G via the morphism $G \twoheadrightarrow G/\mu$. If V is a representation of G such that $Z(G)$ acts by $\tau \in X(Z(G))$, then it is easy to see that V is a well-defined representation of G/μ precisely when $\tau \in C_\mu$. It follows that for any $\chi \in C_\mu$, the functor

$$\begin{aligned} F : \mathrm{Rep}^{(\chi)}(G/\mu) &\to \mathrm{Rep}^{(\chi)}(G) \\ V &\mapsto V \end{aligned}$$

is an isomorphism of categories. Thus

$$\mathrm{ind}(\Psi_{E,K}(\chi)) = \gcd\left\{\dim(V) \mid V \text{ irreducible},\ V \in \mathrm{Rep}^{(\chi)}(G)\right\} \qquad (1)$$

Since k is algebraically closed, a representation V of G decomposes as $V = V_1 \otimes \cdots \otimes V_r$, where V_i is an irreducible representation of G_i for $i = 1, \ldots, r$. If $\chi = (c_1, \ldots, c_r) \in C_\mu$ then $Z(G_i)$ acts on V_i by the character $(c_i) \in X(Z(G_i))$.

If J_i is any set of integers for $1 \leq i \leq r$, then one can easily check the following gcd result:

$$\gcd_{j_i \in J_i, i=1,\ldots,r} \{j_1 \cdot \ldots \cdot j_r\} = \gcd_{j_1 \in J_1} \{j_1\} \cdot \ldots \cdot \gcd_{j_r \in J_r} \{j_r\}$$

Applying this result with $J_i = \{\dim(W) \mid W \in \mathrm{Rep}^{(c_i)}(G)\}$, (1) reduces to:

$$\mathrm{ind}(\Psi_{E,K}(\chi)) = \prod_{i=1}^{r} \left(\gcd\left\{\dim(V_i) \mid V_i \text{ irreducible},\ V_i \in \mathrm{Rep}^{(c_i)}(G_i)\right\}\right).$$

By Lemma 5.3, there exists K/k and $T_i \in H^1(K, \overline{G}_i)$ such that $\mathrm{ind}(\delta^i_K(T_i)) = p^{a_i}$ and $\exp(\delta^i_K(T_i)) = p^{b_i}$. By Remark 1.4, if $\overline{c}_i$ is the reduction of c_i mod p^{b_i}, then $\mathrm{ind}(\delta^i_K(T_i)^{\otimes c_i}) = p^{a_i - v_i(\overline{c}_i)}$. Note that, by Remark 3.5, $\delta^i_K(T_i)^{\otimes c_i} = c_{i*} \circ \delta^i_K(T_i)$, and so by the discussion preceding Theorem 5.2 applied to the

exact sequence $1 \to Z(G_i) \to G_i \to \overline{G}_i \to 1$,

$$\gcd\left\{\dim(V_i) \mid V_i \text{ irreducible, } V_i \in \mathrm{Rep}^{(c_i)}(G_i)\right\}$$

is at least as large as $\mathrm{ind}(\delta_K^i(T_i)^{\otimes c_i})$. Thus we have

$$\gcd\left\{\dim(V_i) \mid V_i \text{ irreducible, } V_i \in \mathrm{Rep}^{(c_i)}(G_i)\right\} \geq p^{a_i - v_i(\overline{c}_i)}$$

and hence,

$$\mathrm{ind}(\Psi_{E,K}(\chi)) \geq \prod_{i=1}^{r} p^{a_i - v_i(\overline{c}_i)} = p^{\sum_{i=1}^{r}(a_i - v_i(\overline{c}_i))} = p^{\mathrm{w}(\overline{\chi})}$$

as required. □

Remark 5.4. In the case where the image of the coboundary map δ_K is well understood, one can prove Theorem 5.1 using the theory of central simple algebras; see Appendix A.

Remark 5.5. An alternate method to prove the lower bound on $\mathrm{ed}(G/\mu; p)$ in Theorem 1.7 would be to find a finite p-subgroup Y of G/μ and apply the bound

$$\mathrm{ed}(G/\mu; p) \geq \mathrm{ed}(Y; p) - \dim(G/\mu).$$

Suppose that for $1 \leq i \leq r$, one can find a finite p-subgroup $H_i \leq G_i$ with $Z(H_i) = \mu_{p^{b_i}} \leq Z(G_i)$, and such that the maximal index and exponent of the coboundary map $H^1(-, H_i/Z(H_i)) \to H^2(-, Z(H_i))$ are p^{a_i} and p^{b_i} respectively. Then set $H = H_1 \times \cdots \times H_r$, so that we have $H/\mu_f \leq G/\mu$. Theorem 1.7 applies, and gives $\mathrm{ed}(H/\mu_f; p) \geq \sum_{i=1}^{t} p^{w(Y_i)}$. Combining this with the bound for the essential dimension of a subgroup above yields:

$$\begin{aligned} \operatorname{ed}(G/\mu; p) &\geq \operatorname{ed}(H/\mu_f; p) - \dim(G/\mu) \\ &\geq \sum_{i=1}^{t} p^{w(Y_i)} - d - \dim(\overline{G}) \end{aligned}$$

where $d = \begin{cases} t, & \text{if Z(G) is connected;} \\ 0, & \text{if Z(G) is finite.} \end{cases}$

This shows that, if one found such subgroups $H_i \leq G_i$, then the lower bound on $\operatorname{ed}(G/\mu; p)$ provided by computing the essential p-dimension of H/μ_f would be the same as the lower bound in Theorem 1.7.

Computing the essential p-dimension of H/μ_f can be done using [KM08, Theorem 4.1], which says that the essential p-dimension of a finite p-group over k equals the minimal dimension of a faithful representation of that group. This is used in [MR10, Theorem 1.2] to give a formula for the essential p-dimension of a finite p-group purely in terms of its group structure. For example, in the case $G_i = \mathrm{GL}_p$, one can take the group H_i to be any finite non-abelian group of order p^3, and the inclusion $H_i \hookrightarrow G_i$ given by any faithful irreducible representation of H_i; see the group Γ defined in the proof of [MR10, Theorem 1.5].

6 An Upper Bound

In this section we will prove Theorem 1.9. Let $H = \mathrm{GL}(V_1) \times \cdots \times \mathrm{GL}(V_r)$ and $H' = \mathrm{SL}(V_1) \times \cdots \times \mathrm{SL}(V_r)$ where $V_i = k^{n_i}$. Then both H and H' act naturally on the vector space

$$V_{c_1,\ldots,c_r} = V_1^{\otimes c_1} \otimes \cdots \otimes V_r^{\otimes c_r}$$

where $c_1, \ldots, c_r \in \{\pm 1\}$ (here, V^{-1} denotes the dual of V). We denote such a representation by $\rho_{(c_1,\ldots,c_r)} : H \to \mathrm{GL}(V_{c_1,\ldots,c_r})$.

Theorem 6.1. *Suppose $r \geq 3$, $2 \leq n_1 \leq \ldots \leq n_r$ and $n_r \leq \frac{n_1 \cdot \ldots \cdot n_{r-1}}{2}$. Then the kernel of $\rho_{(c_1,\ldots,c_r)}$ is central in H, and the action of $H/\ker(\rho_{(c_1,\ldots,c_r)})$ on $V_{c_1,\ldots,c_r}$ is generically free in all but the following exceptional cases:*

1. *$r = 3$, $n_1 = 2$, $n_2 = n_3$.*
2. *$r = 4$, $n_1 = n_2 = n_3 = n_4 = 2$.*
3. *$r = 3$, $n_1 = n_2 = n_3 = 3$.*

Proof. We first reduce to the case where $(c_1, \ldots, c_r) = (1, \ldots, 1)$. Suppose the theorem is true in this case, and let $(c_1, \ldots, c_r) \in \{\pm 1\}^r$. By choosing bases of $V_1, \ldots, V_r$ we can identify V_i with $V_i^{\otimes c_i}$ (we can take the identity map if $c_i = 1$). Define an automorphism:

$$\begin{array}{rcl} \sigma : H & \to & H \\ (h_1, \ldots, h_r) & \mapsto & (h_1^*, \ldots, h_r^*) \end{array}$$

where

$$h_i^* = \begin{cases} h_i & \text{if } c_i = 1; \\ (h_i^{-1})^T & \text{if } c_i = -1 \end{cases}.$$

Now $\rho_{(c_1,\ldots,c_r)}$ is isomorphic to the representation $\rho_{(1,\ldots,1)} \circ \sigma$. Since $Z(H)$ is a characteristic subgroup, we see that the theorem holds for $\rho_{(c_1,\ldots,c_r)}$ as well.

Denote $\rho_{(1,\ldots,1)}$ and $V_{(1,\ldots,1)}$ by ρ and V repectively. It remains to prove the theorem is true for the representation ρ.

By [P87, Theorem 2], with the conditions in our theorem, the $H'/Z(H')$ action on $\mathbb{P}(V)$ is generically free. Thus the stabilizer in general position for the H'-action on V is central. Since a central element of H' either acts trivially on V or non-trivially on all non-zero elements of V, we see that the stabilizer in general position for the H'-action on V is equal to the (central) kernel of this action. It remains to extend this result to the H-action on V.

We may assume $k = \overline{k}$ for the purposes of checking whether a representation is generically free. Suppose $v \in V$ is in general position and $h \in H$ stabilizes v. Write $h = \lambda \cdot h'$ with $\lambda \in (k^*)^r$ and $h' \in H'$. Then we must have h' acting by scalar multiplication on v, and hence h' (mod $Z(H')$)stabilizes the image of v in $\mathbb{P}(V)$. Thus $h' \in Z(H')$, and hence $h \in Z(H)$. As before, a central element of H either acts trivially on V or acts non-trivially on every non-zero element of V, and so the stabilizer of a point $v \in V$ in general position equals the (central) kernel of ρ. Thus the $H/\ker(\rho)$-action on V is generically free, as required.

□

We can now apply this to the essential dimension of G/μ, where μ is a subgroup of $Z(G)$ and $G_i \leq \mathrm{GL}(V_i)$ is a faithful representation of dimension n_i whose central character is the identity character. In other words, with H as above we have $G \leq H$.

Let $\chi = (c_1, \ldots, c_r) \in \overline{C_\mu}$. For $1 \leq j \leq r$, define $\hat{c_j}$ to be the unique integer such that $\hat{c_j} \equiv c_j \mod p^{b_j}$ and $-p^{b_j}/2 < \hat{c_j} \leq p^{b_j}/2$. Define a representation ρ_χ of G by

$$V_\chi = \bigotimes_{i=0}^{r} V_i^{\otimes \hat{c_j}}$$

where $V_i^{\otimes 1}$ is the standard representation, $V_i^{\otimes 0}$ is the trivial representation,

and $V_i^{\otimes -1}$ is the dual of V_i.

We define the set $m(\chi)$ by

$$m(\chi) = \{i \mid c_i \neq 0\}$$

Definition 6.2. We say that $\chi = (c_1, \ldots, c_r) \in \overline{C_\mu}$ is *acceptable* if the following conditions hold:

1. $-1 \leq \hat{c_j} \leq 1$ for $1 \leq j \leq r$.
2. $\max\limits_{i \in m(\chi)} \{a_i\} < \dfrac{1}{2} \left(\sum\limits_{j \in m(\chi)} a_j \right)$ (note this implies $|m(\chi)| \geq 3$).
3. $\{n_i\}_{i \in m(\chi)} \neq \{2, n, n\}, \{2, 2, 2, 2\}$ or $\{3, 3, 3\}$, for any positive integer n.

By Theorem 6.1, if χ is acceptable then the stabilizer in general position for ρ_χ equals $\ker \rho_\chi$, and if $(g_1, \ldots, g_r) \in \ker \rho_\chi$ then $g_i \in Z(G_i)$ for all $i \in m(\chi)$.

Remark 6.3. The first condition in the definition of acceptable implies $\dim(V_\chi) = p^{\mathrm{w}(\chi)}$ for any acceptable χ.

Definition 6.4. Let Y be a generator matrix for $\overline{C_\mu}$ with rows $Y_1, \ldots, Y_m$. We say that Y is *acceptable* if for each j, $1 \leq j \leq r$, there exists i such that $y_{ij} \neq 0$ and Y_i is acceptable.

Theorem 6.5. *Suppose $\mu \leq Z(G)$ and $\overline{C_\mu}$ has an acceptable generator matrix Y with rows $Y_1, \ldots, Y_t$. Then*

$$\mathrm{ed}(G/\mu) \leq \sum_{i=1}^{t} \dim(V_{Y_i}) - \dim(\overline{G}) - d$$

where $d = \begin{cases} t, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}$

Proof. Let $z_i = (\hat{y_{i1}}, \ldots, \hat{y_{ir}}) \in X(Z(G))$ for $1 \leq i \leq t$ and let τ be the subgroup of $Z(G)$ such that C_τ is generated by $z_1, \ldots, z_t$. Then by construction $\overline{C_\mu} = \overline{C_\tau}$.

To each Y_i, we have the associated representation $\rho_{Y_i} : G \to \mathrm{GL}(V_{Y_i})$. If Y_i is acceptable we have that the stabilizer in general position for ρ_{Y_i} is $\ker \rho_{Y_i}$. Let $\rho = \bigoplus_i \rho_{Y_i}$ and let $(v_1, \ldots, v_t)$ be in general position in $V = \bigoplus_i V_{Y_i}$. In particular, v_i is in general position in V_{Y_i} for all i. Then it follows from the comments after Definition 6.2 that

$$\begin{aligned}
\mathrm{Stab}_\rho(v) &= \bigcap_{i=1}^{r} \mathrm{Stab}_{\rho_{Y_i}} v_i \\
&\leq \bigcap_{i \mid Y_i \text{ acceptable}} \mathrm{Stab}_{\rho_{Y_i}} v_i \\
&= \bigcap_{i \mid Y_i \text{ acceptable}} \ker \rho_{Y_i} \\
&\leq Z(G)
\end{aligned}$$

where for the last containment we use the property that for each j there exists i such that $y_{ij} \neq 0$ and Y_i is acceptable. In particular, $\ker \rho \leq Z(G)$. Thus by construction we have $\ker \rho = \tau$, and hence the stabilizer in general position for $\rho : G \to \mathrm{GL}(W)$ equals τ. It follows that ρ is a generically free representation of G/τ, and hence

$$\mathrm{ed}(G/\tau) \leq \sum_{i=1}^{t} \dim(V_{Y_i}) - \dim(G/\tau)$$

By observing $\dim(G/\tau) = \dim(\overline{G}) + d$ and applying Theorem 1.5 we get the desired result. □

Notice that a very acceptable generator matrix is acceptable. Theorem 1.9 follows from Theorem 6.5 by applying Remark 6.3 and the lower bound

in Theorem 1.7.

7 Central Simple Algebras with Tensor Product of Bounded Index.

7.1 General Results

Suppose p is a prime, $r \geq 1$, $a_1, \ldots, a_r \in \mathbb{Z}_{\geq 1}$, and $z \in \mathbb{Z}_{\geq 0}$. Consider the functor $\mathcal{F}_{(a_1,\ldots,a_r);z} : \mathbf{Fields}_k \to \mathbf{Sets}$ given by

$$\mathcal{F}_{(a_1,\ldots,a_r);z}(K) = \left\{ \begin{array}{l} r\text{-tuples } (A_1, \ldots, A_r) \text{ of central simple } K\text{-algebras} \\ \text{up to isomorphism, such that } \deg(A_i) = p^{a_i} \ \forall i, \\ \text{and } \mathrm{ind}(A_1 \otimes \ldots \otimes A_r) \mid p^z. \end{array} \right\}$$

This functor places a restriction on the index of a certain algebra, and is reminiscent of the functor $H^1(-, \mathrm{GL}_{p^a}/\mu_{p^s})$ discussed in the Introduction, which places a restriction on the exponent of a certain algebra:

$$H^1(K, \mathrm{GL}_{p^a}/\mu_{p^s}) = \left\{ \begin{array}{l} \text{central simple } K\text{-algebras A up to isomorphism} \\ \text{such that } \deg(A) = p^a \text{ and } \exp(A) \mid p^s \end{array} \right\}$$

Projection to the first r algebras sets up an isomorphism of functors:

$$\mathcal{F}_{(a_1,\ldots,a_r,z);0} \to \mathcal{F}_{(a_1,\ldots,a_r);z}$$

and thus we may assume $z = 0$. We will also assume $a_1 \leq a_2 \leq \cdots \leq a_r$.

The functor $\mathcal{F}_{(a_1,\ldots,a_r);0}$ classifies r-tuples $(A_1, \ldots, A_r)$ of central simple algebras of specified degrees satisfying the splitting condition $A_1 \otimes \cdots \otimes A_r = 1$ in $\mathrm{Br}(K)$. If we ignored the condition that the tensor product is split, we would be left with the functor $\mathcal{T} = H^1(-, \mathrm{PGL}_{a_1}) \times \cdots \times H^1(-, \mathrm{PGL}_{p^{a_r}})$. The essential dimension of this function is at most quadratic in the p^{a_i}, that is

$$\mathrm{ed}_k(\mathcal{T}) < p^{2a_1} + \ldots + p^{2a_r}$$

We will see in Theorem 7.2 below that, unless $a_r \geq a_1 + \cdots + a_{r-1}$ or $r \leq 2$, the

leading term in the essential dimension of $\mathcal{F}_{(a_1,\dots,a_r);0}$ is $p^{a_1+\cdots+a_r}$. In other words, when trying to descend a tuple of algebras satisfying the splitting condition, enforcing the splitting condition may require significantly more variables than would be needed to just define the algebras individually.

If we set $G_i = \mathrm{GL}_{n_i}$ $(n_i = p^{a_i})$, $G = G_1 \times \cdots \times G_r$, and

$$\mu = \{(\lambda_1, \dots, \lambda_r) \in Z(G) \mid \lambda_1 \cdot \ldots \cdot \lambda_r = 1\}$$

then $C_\mu = [1, \dots, 1]$ and by Theorem 3.1 we have

$$\mathcal{F}_{(a_1,\dots,a_r);0} \cong H^1(-, G/\mu).$$

Lemma 7.1. *Let K/k be a field extension.*
a) If $r = 1$ then $\mathcal{F}_{a_1;0}(K) = \{pt\}$.
b) If $r \geq 2$ and $a_r \geq \sum_{i=1}^{r-1} a_i$ (which is automatic if $r = 2$), then projection to the first $r-1$ algebras gives an isomorphism

$$\gamma : \mathcal{F}_{(a_1,\dots,a_r);0} \to \prod_{i=1}^{r-1} H^1(-, \mathrm{PGL}_{p^{a_i}}).$$

Proof. Part a) is obvious. For part b), a tuple $(A_1, \dots, A_r)$ in $\mathcal{F}_{(a_1,\dots,a_r);0}(K)$ for some field K is uniquely determined by $A_1, \dots, A_{r-1}$, since A_r is the unique central simple algebra of degree p^{a_r} whose Brauer class is

$$(A_1 \otimes \cdots \otimes A_{r-1})^{op}$$

It follows that γ is injective. To see that γ is surjective, observe that for an

arbitrary tuple $(A_1, \ldots, A_{r-1})$ in $\prod_{i=1}^{r-1} H^1(-, \mathrm{PGL}_{p^{a_i}})$, we have

$$\mathrm{ind}(A_1 \otimes \cdots \otimes A_{r-1})^{op} \leq \prod_{i=1}^{r-1} \mathrm{ind}(A_i) \leq p^{a_1+\cdots+a_{r-1}}.$$

Thus the condition on the a_i's guarantees that the Brauer class

$$(A_1 \otimes \cdots \otimes A_{r-1})^{op}$$

will in fact have a representative central simple algebra A_r of degree p^{a_r}, and thus $(A_1, \ldots, A_{r-1})$ is equal to $\gamma(A_1, \ldots, A_r)$. □

Theorem 7.2. *If* $r \geq 3$, $a_r < \sum_{i=1}^{r-1} a_i$, *and* $(p^{a_1}, \ldots, p^{a_r}) \notin \{(2, n, n)_{n\in\mathbb{Z}}, (2, 2, 2, 2), (3, 3, 3)\}$, *then*

$$\mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_r);0}) = \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_r);0}; p) = p^{\sum_{i=1}^{r} a_i} - \sum_{i=1}^{r} p^{2a_i} + r - 1$$

Proof. The matrix $[1, \ldots, 1]$ is an acceptable and minimal generator matrix for $\overline{C_\mu}$. Since $\mathcal{F}_{(a_1,\ldots,a_r);0} \cong H^1(-, G/\mu)$ we have

$$\begin{aligned} \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_r);0}) &= \mathrm{ed}_k(G/\mu) \\ \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_r);0}; p) &= \mathrm{ed}_k(G/\mu; p) \end{aligned}$$

and so the result follows from Theorem 1.9. □

Now let $r \geq 3$, and $a_1 \leq a_2 \leq \cdots \leq a_{r-1}$ such that $(p^{a_1}, \ldots, p^{a_{r-1}}) \notin \{(2, n)_{n\in\mathbb{Z}}, (3, 3)\}$. Let $a_r = \left(\sum_{i=1}^{r-1} a_i\right) - 1$. Then by Theorem 3.1

$$\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}(K) = \left\{ \begin{array}{l} m\text{-tuples } (A_1,\ldots,A_{r-1}) \text{ of central simple } k\text{-algebras} \\ \text{up to isomorphism, such that } \deg(A_i) = p^{a_i}\ \forall i \text{ and} \\ A_1 \otimes \ldots \otimes A_{r-1} \text{ is not a division algebra.} \end{array} \right\}$$

Corollary 7.3. *Let $r \geq 3$, and $a_1 \leq a_2 \leq \cdots \leq a_{r-1}$ such that $(p^{a_1},\ldots,p^{a_{r-1}}) \notin \{(2,n)_{n\in\mathbb{Z}},(3,3)\}$. Let $a_r = \left(\sum_{i=1}^{r-1} a_i\right) - 1$. Then*

$$\mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}) = \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r};p) = p^{2a_r+1} - \sum_{i=1}^{r} p^{2a_i} + r - 1$$

Proof. Theorem 7.2 applies, and gives:

$$\begin{aligned} \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}) &= \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r};p) \\ &= \mathrm{ed}_k(\mathcal{F}_{(a_1,\ldots,a_r);0};p) \\ &= p^{a_1+\cdots+a_r} - \sum_{i=1}^{r} p^{2a_i} + r - 1 \\ &= p^{2a_r+1} - \sum_{i=1}^{r} p^{2a_i} + r - 1 \end{aligned}$$

□

7.2 Small Cases in Theorem 7.2

We now turn to the special cases from Theorem 7.2. Recall that $r \geq 3$, $a_1 \leq a_2 \leq \cdots \leq a_r$. If we set $G_i = \mathrm{GL}_{n_i}$ $(n_i = p^{a_i})$ for $1 \leq i \leq r$ then this functor is isomorphic to $H^1(-, G/\mu)$, where $\overline{C_\mu} = [1,1,\ldots,1]$.

Remark 7.4. Note that in all cases, projection to the $(r-1)^{st}$ algebra gives a surjective morphism of functors from $\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r}$ to $H^1(-,\mathrm{PGL}_{p^{a_{r-1}}})$.

By Theorem 2.1, we get the lower bound

$$\mathrm{ed}(\mathcal{F}_{(a_1,\ldots,a_{r-1});a_r};p) \geq \mathrm{ed}_k(\mathrm{PGL}_{p^{a_{r-1}}};p)$$

We have a natural representation of G/μ given by $W = V_1 \otimes \cdots \otimes V_r$, where each V_i is a vector space of dimension n_i, and G_i acts on V_i. Outside of the exceptional cases $(p^{a_1},\ldots,p^{a_r}) \in \{(2,n,n)_{n\in\mathbb{Z}},(2,2,2,2),(3,3,3)\}$, this representation is generically free. For the exceptional cases, one could try replacing the representation $W := V_1 \otimes \cdots \otimes V_r$ with $W \oplus W$ and checking if it is generically free. However, we can find a better upper bound using normalizers of maximal tori, by instead finding an upper bound on this normalizer and applying Theorem 2.2.

A maximal torus M in GL_n is the set of diagonal matrices, and the normalizer of M is $M \rtimes S_n$ where S_n acts by permutation. Let T be a maximal torus in $\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$. Then T/μ is a maximal torus of G/μ. One can check that the normalizer of T/μ has the form $T/\mu \rtimes S$, where $S = S_{n_1} \times \cdots \times S_{n_r}$ and each S_{n_i} acts by permutation on $G_i \bigcap T/\mu$.

Since $T \twoheadrightarrow T/\mu$ we can identify $X(T/\mu)$ with a subgroup of $X(T)$. Recall $X(T) = \mathbb{Z}^{n_1} \times \ldots \times \mathbb{Z}^{n_r}$. Then $X(T/\mu)$ is the set of characters in $X(T)$ which are trivial on μ. Let $C_i = \mathbb{Z}^{n_i}$ so that $X(T) = C_1 \times \ldots \times C_r$, and let $\gamma_i : C_i \to \mathbb{Z}$ be the augmentation map. Take $t = (t_1,\ldots,t_r) \in \mu$, so that $t_i \in Z(G_i)$ and $t_1 \cdot \ldots \cdot t_r = 1$. For $\chi = (c_1,\ldots,c_r) \in X(T)$ with $c_i \in C_i$, we have:

$$\chi(t) = t_1^{\gamma_1(c_1)} \cdot \ldots \cdot t_r^{\gamma_r(c_r)}$$

It is now easy to see (for example, by writing $t_r = (t_1 \cdot \ldots \cdot t_{r-1})^{-1}$) that $\chi(t) = 1$ for all $t \in \mu$ precisely when

$$\gamma_1(c_1) = \gamma_2(c_2) = \ldots = \gamma_r(c_r)$$

and this is the condition that describes $X(T/\mu)$ as a submodule of $X(T)$.

We have the induced action of S on $X(T)$, where each S_{n_i} acts by permutation on C_i. To any S-invariant generating set $\Lambda \subset X(T)$, [MR09, Section 3] describes a method to construct a representation V_Λ of $T/\mu \rtimes S$, of dimension $|\Lambda|$. To use this to give an upper bound on essential dimension, we require this representation V_Λ to be generically free, and the following lemma tells us how to check this.

Lemma 7.5. *([MR09, Lemma 3.3]) Let R be the kernel of the natural map of $Z[S]$-modules $Z[\Lambda] \to X(T)$. Then the representation V_Λ is generically free precisely when the S-action on R is faithful.*

We construct an S-invariant generating set Λ of $X(T/\mu)$ as follows. Let $c^i_{m_i}$, where $1 \leq i \leq r$ and $1 \leq m_i \leq n_i$ be the vector in C_i which has a 1 in the m_i^{th} position and a zero in all other positions. Then define

$$\Lambda = \{(c^1_{m_1}, \ldots, c^r_{m_r}) \mid 1 \leq m_i \leq n_i \ (1 \leq i \leq r)\}$$

Then Λ clearly generates $X(T/\mu)$ and is S-invariant. It remains to verify the condition in the lemma that S acts faithfully on R. Suppose $1 \neq (\sigma_1, \ldots, \sigma_r) \in S$. Without loss of generality, we may assume $\sigma_1 \neq 1$ and $\sigma_1(1) = j \neq 1$. Consider the elements $r_1, r_2, r_3, r_4 \in R$:

$$\begin{aligned}
r_1 &= (c^1_1, c^2_1, \ldots, c^r_1) \\
r_2 &= (c^1_1, c^2_2, c^3_1, c^4_1, \ldots, c^r_1) \\
r_3 &= (c^1_1, c^2_1, c^3_2, c^4_1, c^5_1, \ldots, c^r_1) \\
r_4 &= (c^1_1, c^2_2, c^3_2, c^4_1, c^5_1, \ldots, c^r_1)
\end{aligned}$$

Setting $r = r_1 - r_2 - r_3 + r_4 \in Z[\Lambda]$ we see $r \in R$, but each $\sigma_1(r_i)$ will have the form $(c^1_j, \ldots)$. Thus $\sigma(r) \neq r$, and the result follows.

Remark 7.6. Note that this argument depended crucially on $r \geq 3$, but not on p or $n_1, \ldots, n_r$.

Since $|\Lambda| = \prod_{i=1}^{r} n_i$, and $\dim(T/\mu \rtimes S) = \dim(T/\mu) = \left(\sum_{i=1}^{r} n_i\right) - r + 1$, we get the following corollary by Theorem 2.5.

Corollary 7.7. *We have* $\operatorname{ed}(T/\mu \rtimes S) \leq \prod_{i=1}^{r} n_i - \left(\sum_{i=1}^{r} n_i\right) + r - 1$. *In particular, by Theorem 2.2:*

$$\operatorname{ed}(G/\mu) \leq \prod_{i=1}^{r} n_i - \left(\sum_{i=1}^{r} n_i\right) + r - 1.$$

Theorem 7.8. *1.* $p = 2$, $a > 1$*:*

$$(a-1)2^a + 1 \leq \operatorname{ed}_k(\mathcal{F}_{(1,a,a);0}) \leq 2^{2a+1} - 2^{a+1}$$

2. $p = 2$*:* $4 \leq \operatorname{ed}_k(\mathcal{F}_{(1,1,1,1);0}) \leq 11$

3. $p = 3$*:* $2 \leq \operatorname{ed}_k(\mathcal{F}_{(1,1,1);0}) \leq 20$

The bounds are also valid for essential p-dimension in all four cases.

Proof. The upper bounds all follow from Corollary 7.7. The lower bounds in (1) and (3) follow from Remark 7.4 and [R00, Theorem 9.3 & Proposition 9.8a]. For the lower bound in part (2), observe that projection the the first 2 algebras gives a surjective morphism of functors

$$\mathcal{F}_{(1,1,1,1);0} \to H^1(-, \mathrm{PGL}_2) \times H^1(-, \mathrm{PGL}_2).$$

It follows from [RY00, Section 8] that $\mathrm{PGL}_2 \times \mathrm{PGL}_2$ has a self-centralizing finite 2-subgroup of rank 4, and hence by [RY00, Theorem 7.8.1] and [RY00,

Lemma 8.5.7]

$$\mathrm{ed}_k(\mathrm{PGL}_2 \times \mathrm{PGL}_2; p) = 4.$$

Thus the lower bound follows from Theorem 2.1. □

We could use the methods of the above theorem to prove that for $p = 2$ we have

$$2 \leq \mathrm{ed}_k(\mathcal{F}_{(1,1,1);0}) \leq 4$$

but in this case we can determine the essential dimension exactly.

Theorem 7.9. *For $p = 2$,*

$$\mathrm{ed}_k(\mathcal{F}_{(1,1,1);0}) = \mathrm{ed}_k(\mathcal{F}_{(1,1,1);0}; 2) = 3.$$

Proof. We begin with the upper bound. Recall that $\mathcal{F}_{(1,1,1);0}(L)$ classifies triples of quaternion algebras (Q_1, Q_2, Q_3) (up to isomorphism over L) such that $Q_1 \otimes Q_2 \otimes Q_3$ is split. By a theorem of Albert [L05, Theorem III.4.8], since $Q_1 \otimes Q_2$ is not a division algebra, we may write $Q_1 = (a, b)$ and $Q_2 = (a, c)$. Thus $Q_3 \cong Q_1 \otimes Q_2 \cong (a, bc)$. Hence the triple (Q_1, Q_2, Q_3) descends to the field $K = k(a, b, c)$ while still satisfying the splitting property. Thus $\mathrm{ed}_k(\mathcal{F}_{(1,1,1);0}) \leq 3$.

To prove the lower bound, consider the map

$$\begin{array}{rcl} \Gamma : \mathcal{F}_{(1,1,1);0} & \to & H^1(-, \mathrm{SO}_4) \\ (Q_1, Q_2, Q_3) & \mapsto & \alpha \end{array}$$

Here α is defined to be the quadratic form such that $\alpha \oplus \mathbb{H} \oplus \mathbb{H} \cong N(Q_1) \oplus -N(Q_2)$ where $\mathbb{H} = \langle 1, -1 \rangle$ is the 2-dimensionsal hyperbolic form. (Equivalently, using the definition of the Albert form given in [L05, p.69], α is the quadratic form such that $\alpha \oplus \mathbb{H} \cong A_{Q_1.Q_2}$ where A_{Q_1,Q_2} is the Albert form of Q_1 and Q_2.) By the Witt cancellation theorem, α is unique up to

isomorphism. We can explicitly compute α as follows, for arbitrary K/k. Suppose $Q_1 = (a, b)$ and $Q_2 = (a, c)$ as above. Then

$$N(Q_1) = \langle\langle -a, -b\rangle\rangle = \langle 1, -a, -b, ab\rangle$$

$$N(Q_2) = \langle 1, -a, -c, ac\rangle$$

and so

$$N(Q_1) \oplus -N(Q_2) = \langle 1, -1, -a, a, -b, c, ab, -ac\rangle.$$

This is isomorphic to

$$\langle -b, c, ab, -ac\rangle \oplus \mathbb{H} \oplus \mathbb{H}\,.$$

Thus $\alpha \cong \langle -b, c, ab, -ac\rangle$. Since $H^1(K, \mathrm{SO}_4)$ classifies 4-dimensional quadratic forms over K of discriminant 1, it is clear from specializing the values a, b and c in our expression for α that Γ is surjective. Since $\mathrm{ed}_k(\mathrm{SO}_4; 2) = 3$ (see [RY00, Theorem 8.1 & Remark 8.2]), by Theorem 2.1 we have

$$\mathrm{ed}_k(\mathcal{F}_{(1,1,1);0}; 2) \geq 3.$$

□

8 Examples of Linear Error-Correcting Codes

Given a code $\overline{C_\mu}$, the two questions we must determine are:

1. What does a minimal generator matrix look like?

2. Can a minimal generator matrix be chosen such that all the coefficients are $0, -1$ or 1?

Example 4.8 and Corollary 4.5 provide a partial answer to the first question: the greedy algorithm will always result in a minimal generator matrix. In the case $b_i = 1$ for all i, the code $\overline{C_\mu}$ is a linear error-correcting code over $\mathbb{F}_p$ in the traditional sense. If $a_1 = a_2 = \cdots = a_r$ then the weight on $\overline{C_\mu}$ will just be a_1 times the usual Hamming weight. Of note though is that unless $G_i = \mathrm{GL}_p$ for all i, our notion of equivalence of codes does not coincide with the usual notion of linear equivalence of linear error-correcting codes.

Example 8.1. $\overline{C_\mu}$ is a traditional code, and the weight is a scaling of the Hamming weight, when:

1. p arbitrary: $G_i \in \{\mathrm{GL}_p, \mathrm{SL}_p\}$, for all i.

2. $p = 2$: $G_i \in \{\mathrm{GL}_2, \mathrm{GO}_2, \mathrm{GSP}_2, \mathrm{SL}_2 = \mathrm{SP}_2, \mathrm{O}_2\}$, for all i.

3. $p = 2$: $G_i \in \{\mathrm{GO}_n, \mathrm{GSP}_n, \mathrm{SP}_n, \mathrm{O}_n, \mathrm{GO}_n^+, \mathrm{SO}_n\}$ where $n = 2^a > 2$, for all i.

4. $p = 3$: $G_i = E_6 \leq \mathrm{GL}_{27}$ for all i.

In this case, if a code can be generated by its minimum (Hamming) weight vectors then this completely answers the first question above. In this section

we recall a class of traditional codes (called generalized Reed-Muller codes) that are generated by their minimum weight vectors, and where the second question sometimes has an affirmative answer. The primary references are [DK00] and [AK92, Section 5].

Generalized Reed-Muller codes are a family of codes that is closed under taking dual codes and contains, for example, all extended Hamming codes. We recall the definition. Let q be a power of a prime p, $m \geq 1$, $r \geq 1$ such that $r \leq m(q-1)$, and $V = \mathbb{F}_q^m$ with standard basis $e_1, \ldots, e_m$. The underlying vector space for the generalized Reed-Muller code $R_{\mathbb{F}_q}(r, m)$ is the vector space W of all functions from V to $\mathbb{F}_q$. We have $\dim(W) = q^m$, and our distinguished basis for W is the set of characteristic functions of vectors in V.

Any monomial $n(x_1, \ldots, x_m)$ defines an element of W, since we can evaluate $n(v)$ by writing $v = \sum_{i=1}^m z_i e_i$, with $z_i \in \mathbb{F}_q$, and defining $n(v) = n(z_1, \ldots, z_m)$. Of course, $x_i^q = x_i$ as elements of W by Fermat's little theorem, and it follows that we can identify W with the underlying vector space of the ring

$$\mathbb{F}_q[x_1, \ldots, x_m]/(x_1^q - x_1, \ldots, x_m^q - x_m)$$

For any monomial $n = x_1^{i_1} \cdot \ldots \cdot x_m^{i_m}$, we define $\deg_{x_j}(n) = i_j$ and $\deg(n) = i_1 + \cdots + i_m$. The reduced monic monomials (that is, monic monomials n with $\deg_{x_i} n < q \ \forall i$) give us a new basis of W. We now define $R_{\mathbb{F}_q}(r, m)$ to be the span in W of all reduced monic monomials n with $\deg(n) \leq r$.

Theorem 8.2. *Write $r = t(q-1) + s$ with $0 \leq s < q-1$.*

1. *[AK92, Theorem 5.5.3] The minimum weight codewords of $R_{\mathbb{F}_q}(r, m)$ have weight $(q-s)q^{m-t-1}$.*

2. *[DK00, Theorem 1] If $q = p$ then $R_{\mathbb{F}_q}(r, m)$ is generated by its minimum weight codewords.*

3. *[DGM70, Theorem 2.6.3] If $s = 0$ and $q = p$ then $R_{\mathbb{F}_q}(r, m)$ is generated by minimum weight codewords whose entries are all 0 or 1.*

Using this theorem and Theorems 1.7 and 1.9, we conclude the following.

Corollary 8.3. *Suppose* $\overline{C_\mu} = R_{\mathbb{F}_p}(r,m)$ *(up to equivalence). Write* $r = t(p-1)+s$ *with* $0 \le s < p-1$. *Let* $D = \dim R_{\mathbb{F}_p}(r,m)$.

1.

$$\begin{aligned} \mathrm{ed}_k(G/\mu;p) &\geq Dp^{(p-s)p^{m-t-1}} - d - \dim(\overline{G}) \\ \mathrm{ed}_k(G/\mu) &\leq Dp^{(p-s)p^{m-t-1}} - d + \mathrm{ed}_k(\overline{G}) \end{aligned}$$

2. Suppose $(p-1) \mid r$.

$$\mathrm{ed}_k(G/\mu;p) = Dp^{(p-s)p^{m-t-1}} - d - \dim(\overline{G})$$

where $d = \begin{cases} D, & \text{if } Z(G) \text{ is connected;} \\ 0, & \text{if } Z(G) \text{ is finite.} \end{cases}$

Remark 8.4. [AK92, Theorem 5.4.1] The dimension of $R_{\mathbb{F}_q}(r,m)$ is given by:

$$\dim R_{\mathbb{F}_q}(r,m) = \sum_{i=0}^{r}\sum_{k=0}^{m}(-1)^k\binom{m}{k}\binom{i-kq+m-1}{i-kq}$$

[DGM70, Theorem 2.6.3] gives us an explicit description of the minimum weight codewords, which we recall here in the $s=0$ case. Let $w_1,\ldots,w_t \in \mathbb{F}_q$. Consider the codeword:

$$P(x_1,\ldots,x_m) = \prod_{i=1}^{t}(1-(x_i-w_i)^{q-1})$$

We see that the degree of P is precisely $t(q-1)=r$, which is the maximum allowable degree of a polynomial defining an element of $R_{\mathbb{F}_q}(r,m)$. It is also clear the codeword corresponding to P contains entries 0 and 1. The entry in the codeword associated to the vector $v \in V$ is equal to 1 precisely when $x_i(v) = w_i$ for $1 \le i \le t$. Recall that a k-flat in V is a subset of V of the

form $v_0 + U$ where $v_o \in V$ and U is a k-dimensional subspace of V. Then we have that the codeword corresponding to P is the incidence vector of the $(m-t)$-flat given by $(w_1, \ldots, w_t, *, \ldots, *)$. Thus the weight of P is q^{m-t}, and P corresponds to a minimum weight vector. From [DGM70, Theorem 2.6.3], all minimal weight codewords in W can be obtained from codewords of the form P, along with scalar multiplication and replacing $x_1, \ldots, x_t$ with any other set of t linearly independent linear polynomials. In particular, all minimal weight codewords lie in the subspace generated by the minimal weight codewords whose entries are all 0 and 1.

Remark 8.5. The question of whether a code has a generator matrix where each element has minimal weight has been studied for other classes of codes as well, see [KL06, Section 1] for an overview. In particular, the authors show that certain extended binary BCH codes are always generated by their minimum weight vectors.

9 Conclusion

In this report we have computed bounds on the essential dimension of certain families of reductive algebraic groups. One of the motivating examples was the group G/μ, where

$$G = \mathrm{GL}_{p^{a_1}} \times \cdots \times \mathrm{GL}_{p^{a_r}},$$

p is a prime and μ is a central subgroup of G. This example was particularly interesting because we interepreted the Galois cohomology of this group as tuples of central simple algebras satisfying relations in the Brauer group.

Surprisingly, this problem became easier for $r \geq 3$, and we were able to give asymptotically sharp bounds (or even exact values) for many families of central subgroups. We also looked at one particular family of central subgroups where $\mathrm{ed}(G/\mu)$ grew 'exponentially in r', or informally:

$$\mathrm{ed}(G/\mu) = p^{a_1+\cdots+a_r} - \text{smaller order terms.}$$

This is in contrast to the group $\mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_r}}$, whose cohomology classifies tuples of central simple algebras without any additional conditions. In this case, the essential dimension grows much more slowly in r:

$$\mathrm{ed}(\mathrm{PGL}_{p^{a_1}} \times \cdots \times \mathrm{PGL}_{p^{a_r}}) < p^{2a_1} + \cdots + p^{2a_r}.$$

Our bounds for the essential dimension of G/μ were given in terms of a 'code' $\overline{C_\mu}$ and a weight function on this code. Specifically, computing the upper and lower bounds depend on finding a minimal weight generator matrix for $\overline{C_\mu}$. For some families of codes (for example, see Sections 7 and 8) we could determine a minimal weight generator matrix. For other, more complicated codes, it may be more difficult to determine the structure of a minimal weight generator matrix. This is related to the general notion of weight distribution in codes.

In section 7 we studied an interesting family of groups where $\overline{C_\mu}$ was particularly simple, and the cohomology could be interpreted as tuples of central simple algebras satisfying certain index conditions. One example of this was the functor of pairs of central simple algebras (A, B) of degree p^a, where $A \otimes B$ is not a division algebra. This functor was of particular interest both because of its connection to linkages of cyclic algebras (Theorem 7.9), and because the problem of determining a structural condition for when the tensor product of two central simple algebras is not a division algebra is an open problem ([ABGV12, Problem 9.1]). Both of these connections could be areas for future research.

One of the primary limitations of this research was the requirement that each n_i be a power of the same prime. This requirement was not needed to conclude that the essential dimension of G/μ depended only on $\overline{C_\mu}$ (Theorem 1.5), and the upper bound (Theorem 6.5) can also be formulated without this assumption. However, it was needed to deduce the lower bound. Specifically, we appealed to [KM08] regarding a formula for the canonical dimension of a finite p-subgroup of the Brauer group. Although one can find a formula for the canonical p-dimension of a finite subgroup of the Brauer group (see [KM08, Remark 2.10]), it is unclear what the formula for absolute canonical dimension might look like when the finite subgroup is not a p-group (see [M13, Conjecture 4.23] for a related conjecture), and this could also be the subject of future research.

Bibliography

[ABGV12] Auel, Asher; Brussel, Eric; Garibaldi, Skip; Vishne, Uzi. *Open problems on central simple algebras.* Transform. Groups 16 (2011), no. 1, 219-264.

[AK92] Assmus, E. F., Jr.; Key, J. D. *Designs and their codes.* Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.

[AM69] Atiyah, M. F.; Macdonald, I. G. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[BF03] Berhuy, Grégory; Favi, Giordano. *Essential dimension: a functorial point of view (after A. Merkurjev)* Doc. Math. 8 (2003), 279-330.

[BM12] Baek, Sanghoon; Merkurjev, Alexander S. *Essential dimension of central simple algebras.* Acta Math. 209 (2012), no. 1, 1-27.

[BR97] Buhler, J.; Reichstein, Z. *On the essential dimension of a finite group.* Compositio Math. 106 (1997), no. 2, 159-179.

[BO13] Berhuy, Grégory; Oggier, Frédérique. *An introduction to central simple algebras and their applications to wireless communication.* With a foreword by B. A. Sethuraman. Mathematical Surveys and Monographs, 191. American Mathematical Society, Providence, RI, 2013.

[BR05] Berhuy, G.; Reichstein, Z. *On the notion of canonical dimension for algebraic groups.* Adv. Math. 198 (2005), no. 1, 128-171.

[BRV11] Brosnan, Patrick; Reichstein, Zinovy; Vistoli, Angelo. *Essential dimension of moduli of curves and other algebraic stacks.* With an appendix by Najmuddin Fakhruddin. J. Eur. Math. Soc. (JEMS) 13 (2011), no. 4, 1079-1112.

[D83] Draxl, P. K. *Skew fields.* London Mathematical Society Lecture Note Series, 81. Cambridge University Press, Cambridge, 1983

[D10] A. Duncan. *Essential dimensions of A7 and S7.* Math. Res. Lett. 17 (2010), no. 2, 263-266.

[DK00] Ding, Peng; Key, Jennifer D. *Minimum-weight codewords as generators of generalized Reed-Muller codes.* IEEE Trans. Inform. Theory 46 (2000), no. 6, 2152-2158.

[DGM70] Delsarte, P.; Goethals, J.-M.; MacWilliams, F. J. *On generalized Reed-Muller codes and their relatives.* Information and Control 16 1970 403-442.

[GMS03] Garibaldi, Skip; Merkurjev, Alexander; Serre, Jean-Pierre. *Cohomological invariants in Galois cohomology.* University Lecture Series, 28. American Mathematical Society, Providence, RI, 2003.

[GS06] Gille, Philippe; Szamuely, Tamás. *Central simple algebras and Galois cohomology.* Cambridge Studies in Advanced Mathematics, 101. Cambridge University Press, Cambridge, 2006.

[GR09] Gille, Phillippe; Reichstein, Zinovy. *A lower bound on the essential dimension of a connected linear group.* Comment. Math. Helv. 84, No. 1, 189-212 (2009).

[IK99] Izhboldin, Oleg T.; Karpenko, Nikita A. *Generic splitting fields of central simple algebras: Galois cohomology and nonexcellence.* Algebr. Represent. Theory 2 (1999), no. 1, 19-59.

[KL06] Kaufman, Tali; Litsyn, Simon. *Long extended BCH codes are spanned by minimum weight words.* Applied algebra, algebraic algorithms and error-correcting codes. 285-294, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006.

[KMRT98] Knus, Max-Albert; Merkurjev, Alexander; Rost, Markus; Tignol, Jean-Pierre. *The book of involutions*. With a preface in French by J. Tits. American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998. xxii+593 pp.

[KM08] Karpenko, Nikita A.; Merkurjev, Alexander S. *Essential dimension of finite p-groups.* Invent. Math. 172 (2008), no. 3, 491-508.

[L05] Lam, T. Y. *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

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

[M09] Merkurjev, Alexander S. *Essential dimension*. Quadratic forms−algebra, arithmetic, and geometry, 299-325, Contemp. Math., 493, Amer. Math. Soc., Providence, RI, 2009.

[M10] Merkurjev, Alexander S. *A lower bound on the essential dimension of simple algebras*, Algebra & Number Theory, 4 (2010), no. 8, 1055-1076.

[MR09] Meyer, Aurel; Reichstein, Zinovy. *The essential dimension of the normalizer of a maximal torus in the projective linear group*. Algebra Number Theory 3 (2009), no. 4, 467-487.

[MR10] Meyer, Aurel; Reichstein, Zinovy. *Some consequences of the Karpenko-Merkurjev theorem*. Doc. Math. 2010, Extra volume: Andrei A. Suslin sixtieth birthday, 445-457.

[M13] Merkurjev, Alexander S. *Essential dimension: a survey.* Transform. Groups 18 (2013), no. 2, 415-481.

[N11] Nguyen, Athena. *Master's Thesis*. UBC, 2011.

[P87] Popov, A.M. *Finite isotropy subgroups in general position of irreducible semisimple linear Lie groups.* (Russian) Trudy Moskov. Mat. Obshch. 50 (1987), 209–248, 262; translation in Trans. Moscow Math. Soc. 1988, 205-249.

[R88] Rowen, Louis H. *Ring theory. Vol. II.* Pure and Applied Mathematics, 128. Academic Press, Inc., Boston, MA, 1988.

[R00] Reichstein, Z. *On the notion of essential dimension for algebraic groups.* Transform. Groups 5 (2000), no. 3, 265-304.

[RY00] Reichstein, Zinovy; Youssin, Boris. *Essential dimensions of algebraic groups and a resolution theorem for G -varieties.* With an appendix by János Kollár and Endre Szabó. Canad. J. Math. 52 (2000), no. 5, 1018-1056.

[R10] Reichstein, Zinovy. *Essential Dimension.* Proceedings of the International Congress of Mathematicians, Vol II, 162-188, Hindustan Book Agency, New Delhi, 2010.

[Ru11] Ruozzi, Anthony. *Essential p-dimension of* PGL_n. J. Algebra 328 (2011), 488-494.

[S97] Serre, Jean-Pierre. *Galois cohomology.* Translated from the French by Patrick Ion and revised by the author. Springer-Verlag, Berlin, 1997.

[S98] Saltman, David J. *Lectures on division algebras.* CBMS Regional Conference Series in Mathematics, 94. Published by American Mathematical Society, Providence, RI; on behalf of Conference Board of the Mathematical Sciences, Washington, DC, 1999.

[SV92] Schofield, Aidan; Van den Bergh, Michel. *The index of a Brauer class on a Brauer-Severi variety.* Trans. Amer. Math. Soc. 333 (1992), no. 2, 729-739.

Appendix A Disjoint Central Simple Algebras

Definition A.1. [IK99, Definitsubion 2.5] A collection of central simple algebras $\{A_1, \ldots, A_r\}$ over a field K is called **disjoint** if for all $m_1, \ldots, m_r \in \mathbb{Z}_{\geq 0}$, we have

$$\mathrm{ind}(A_1^{\otimes m_1} \otimes \ldots \otimes A_r^{\otimes m_r}) = \mathrm{ind}(A_1^{\otimes m_1}) \cdot \ldots \cdot \mathrm{ind}(A_r^{\otimes m_r})$$

As a consequence of the latter part of the proof of Theorem 5.1 (in the case $\mu = \{1\}$), we have that there exists K/k and $E_i \in H^1(K, \overline{G}_i)$, $1 \leq i \leq r$, such that the underlying division algebras of the set $\{\delta_K^i(E_i)\}_{i=1,\ldots,r}$ form a disjoint set of division algebras over K, with $\mathrm{ind}(\delta_K^i(E_i)) = p^{a_i}$ and $\exp(\delta_K^i(E_i)) = p^{b_i}$. In the case $\overline{G}_i \in \{\mathrm{PGL}_{n_i}, \mathrm{PGSp}_{2^{a_i}}, \mathrm{PGO}_{2^{a_i}}, \mathrm{PGO}^+_{2^{a_i}}(a_i \geq 2)\}$ we can prove this directly; see Corollary A.6 below. When combined with Remark 1.4 this provides an alternate proof of Theorem 5.1 in these cases.

Theorem A.2. *Let $a_1, \ldots, a_r$ and $b_1, \ldots, b_r$ be positive integers with $b_i \leq a_i$. Then there exists a finitely generated field extension K/k and a disjoint collection $\{Z_1, \ldots, Z_r\}$ of central division algebras over K with $\mathrm{ind}(Z_i) = p^{a_i}$, $\exp(Z_i) = p^{b_i}$, and $\mathrm{ind}(Z_i^{\otimes p^d}) = p^{a_i - d}$ for any $1 \leq d < b_i$.*

We begin with a weaker existence result.

Lemma A.3. *Let $a_1, \ldots, a_r$ be positive integers. Then there exists a finitely generated field extension K/k and a disjoint collection $\{A_1, \ldots, A_r\}$ of central division algebras over K with $\mathrm{ind}(A_i) = \exp(A_i) = p^{a_i}$.*

We require some preliminary results before the proof. We may assume k contains all primitive $p^{d^{\text{th}}}$ roots of unity for all d, and choose a sequence $\{1 = \zeta_1, \zeta_p, \zeta_{p^2}, \ldots\} \subset k$ such that, for all $b \geq 1$, ζ_{p^b} is a primitive $p^{b^{\text{th}}}$ root of unity, and $\zeta_{p^{b+1}}^p = \zeta_{p^b}$. Recall that if $u, w \in K$ and $a \in \mathbb{Z}_{\geq 0}$, then the symbol algebra $(u, w)_{p^a}$ is the (central simple) K-algebra generated by x and y such that $x^{p^a} = u$, $y^{p^a} = w$ and $uw = \zeta_{p^a} wu$.

Proposition A.4. *(see [D83, Chapter 11], or [R88, Proposition 7.1.17]) Let* $c, d \in K$, $a \in Z_{\geq 1}$

i) $(c,d)_{p^a}^{\otimes p}$ *is Brauer equivalent to* $(c,d)_{p^{a-1}}$ *(Here,* $(c,d)_1 = K$ *is split).*

ii) $(c,d)_{p^a}^n$ *is Brauer equivalent to* $(c,d^n)_{p^a}$.

Lemma A.5. *Let* $a_1, \ldots, a_r$ *be non-negative integers,* $u_1, \ldots, u_r, w_1, \ldots, w_r$ *be commuting indeterminates and* $K = k(u_1, \ldots, u_r, w_1, \ldots, w_r)$. *Then the central simple* K*-algebra*

$$A = (u_1, w_1)_{p^{a_1}} \otimes \cdots \otimes (u_r, w_r)_{p^{a_r}}$$

is a division algebra.

Proof. Let $\{x_1, \ldots, x_r, y_1, \ldots, y_r\}$ be the elements in A such that by definition $x_i^{p^{a_i}} = u_i$ and $y_i^{p^{a_i}} = w_i$. Consider the k-algebra R generated by $x_1, \ldots, x_r, y_1, \ldots, y_r$. Each element of R has a unique expression as a finite sum of the form

$$\sum_{0 \leq i_1, \ldots, i_r, j_1, \ldots, j_r} \lambda_{i_1, \ldots, j_r} x_1^{i_1} \ldots x_r^{i_r} y_1^{j_1} \ldots y_r^{j_r}$$

with each $\lambda_{i_1, \ldots, j_r} \in k$.

A standard leading monomial trick shows that R is a domain, and it is easy to see that $Z(R) = k[u_1, \ldots, u_r, w_1, \ldots, w_r]$. Thus A is the central localization of R, and since R is a domain, so is A. □

Proof of Lemma A.3. Take $K = k(u_1, \ldots, u_r, w_1, \ldots, w_r)$ as in the previous lemma. Let $A_i = (u_i, w_i)_{p^{a_i}}$. Since $\deg(A_i) = p^{a_i}$, to see that A_i has exponent (and thus also index) p^{a_i} it suffices to show that $A_i^{p^{a_i - 1}}$ is not split. Using Proposition A.4i) repeatedly, it is equivalent to show that $(u_i, w_i)_p$ is not split, and this follows from Lemma A.5 with $a_i = 1$ and $a_j = 0$ for $j \neq i$.

Let $m_1, \ldots, m_r \in \mathbb{Z}_{\geq 0}$. We wish to show

$$\mathrm{ind}(A_1^{\otimes m_1} \otimes \ldots \otimes A_r^{\otimes m_r}) = \mathrm{ind}(A_1^{\otimes m_1}) \cdot \ldots \cdot \mathrm{ind}(A_r^{\otimes m_r})$$

Observe that replacing each $A_i^{\otimes m_i}$ with a Brauer-equivalent element does not change either side. Thus first, if $A_i^{\otimes m_i}$ is split for any i, then we remove it from both sides. Next, we apply Proposition A.4i) repeatedly. Thus we can remove factors of p from each of the m_i (and consequently reduce the a_i), and so we can assume without loss of generality that $(m_i, p) = 1$ for all i.

By Proposition A.4ii), $A_i^{\otimes m_i} \overset{\mathrm{Br}}{\sim} (u_i, w_i^{m_i})_{p^{a_i}}$. Let $D_i = (u_i, w_i^{m_i})_{p^{a_i}}$. Let K' be the subfield of K given by $k(u_1, \ldots, u_r, w_1^{m_1}, \ldots, w_r^{m_r})$. Then each $D_i^{\otimes m_i}$ is defined over K'. By Lemma A.5, $D_1^{\otimes m_1} \otimes \ldots \otimes D_r^{\otimes m_r}$ is a division algebra over K', and so in particular

$$\mathrm{ind}(D_1^{\otimes m_1} \otimes \ldots \otimes D_r^{\otimes m_r}) = \mathrm{ind}(D_1^{\otimes m_1}) \cdot \ldots \cdot \mathrm{ind}(D_r^{\otimes m_r})$$

over K'. Since $(m_i, p) = 1$ we have that K/K' is an extension of degree prime to p. Since each D_i has index a power of p, by [GS06, Corollary 4.5.11b] we have that the equality still holds after scalar extension to K, which was the desired result. □

Proof of Theorem A.2. Using the previous lemma, for some field K/k, there is a disjoint collection $B_1, \ldots, B_r$ of central division K-algebras such that $\mathrm{ind}(B_i) = \exp(B_i) = p^{a_i}$. Let t be maximal, with $1 \leq t \leq r+1$, such that there exists a field L/K with the following properties:

1. $\{B_i \otimes_K L\}_{i=1,\ldots,r}$ is a disjoint collection of central division E-algebras.
2. If $i < t$ then $\exp(B_i \otimes_K L) = p^{b_i}$ and $\mathrm{ind}((B_i \otimes L)^{\otimes p^d}) = p^{a_i - d}$ for any $0 \leq d < b_i$.
3. If $t \leq i \leq r$ then $\mathrm{ind}(B_i \otimes_K L) = \exp(B_i \otimes_K L) = p^{a_i}$.

If $t = r+1$ then we are done, so towards a contradiction suppose $t < r+1$. Let L/K be a field extension satisfying the three properties, and set $A_i = B_i \otimes_K L$ for all i. Let L_t be the function field of the Brauer Severi variety of $A_t^{\otimes p^{b_t}}$. Now consider the r-tuple $(A_1 \otimes_L L_t, \ldots, A_r \otimes_L L_t)$ of central simple algebras over L_t. Using the fact that $\mathrm{ind}((A_j \otimes_L L_t)^{\otimes m}) = \mathrm{ind}(A_j^{\otimes m} \otimes_L L_t)$, the index reduction formula of Schofield and Van Den Bergh [SV92, Theorem 1.3], and the properties above, we get the following formula for any positive integer d:

$$\begin{aligned} \mathrm{ind}\left((A_i \otimes_L L_t)^{\otimes p^d}\right) &= \min_{z \in \mathbb{Z}} \left(\mathrm{ind}(A_i^{\otimes p^d} \otimes_L A_t^{\otimes z p^{b_t}})\right) \\ &= \begin{cases} \mathrm{ind}(A_i^{\otimes p^d}), \text{ if } t \neq i \\ \mathrm{ind}(A_i^{\otimes p^d}) \text{ if } t = i, d < b_t \\ 1, \text{ if } t = i, d \geq b_t \end{cases} \end{aligned}$$

In particular, for $i \neq t$ we have that the exponent and index of $A_i \otimes_L L_t$ are the same as the exponent and index respectively of A_i. For $i = t$, if $d < b_t$ then from $\mathrm{ind}(A_t) = \exp(A_t) = p^{a_t}$, we get:

$$\mathrm{ind}\left((A_t \otimes_L L_t)^{\otimes p^d}\right) = \mathrm{ind}(A_i^{\otimes p^d}) = p^{a_i - d}$$

and we also have $\exp(A_i \otimes_L L_t) = p^{b_t}$. Thus conditions ii) and iii) above are satisfied for the algebras $\{A_1 \otimes_L L_t, \ldots, A_r \otimes_L L_t\}$ with $t+1$ replacing t. Since $A_i \otimes_L L_t = B_i \otimes_K L_t$ for $i \leq i \leq r$, to arrive at a contradiction it suffices to verify condition i) for the algebras $\{A_1 \otimes_L L_t, \ldots, A_r \otimes_L L_t\}$.

We will prove this using our inductive hypothesis that $A_1, \ldots, A_r$ are disjoint, and the index reduction formula used above. Let $m_1, \ldots, m_r \in \mathbb{Z}$. Then

$$
\begin{aligned}
\operatorname{ind}\bigotimes_{i=1}^{r}(A_i \otimes_L L_t)^{\otimes m_i} &= \operatorname{ind}\left(\left(\bigotimes_{i=1}^{r} A_i^{\otimes m_i}\right) \otimes_L L_t\right) \\
&= \min_{z\in\mathbb{Z}} \operatorname{ind}\left(\left(\bigotimes_{i=1}^{r} A_i^{\otimes m_i}\right) \otimes_L A_t^{zp^{b_t}}\right) \\
&= \left(\prod_{\substack{1\le i\le r\\ i\neq t}} \operatorname{ind}(A_i^{\otimes m_i})\right) \cdot \min_{z\in\mathbb{Z}} \operatorname{ind}(A_t^{\otimes m_t} \otimes_L A_t^{zp^{b_t}}) \\
&= \left(\prod_{\substack{1\le i\le r\\ i\neq t}} \operatorname{ind}\left((A_i \otimes_L L_t)^{\otimes m_i}\right)\right) \cdot \operatorname{ind}(A_t^{\otimes m_t} \otimes_L L_t) \\
&= \prod_{1=1}^{r} \operatorname{ind}\left((A_i \otimes_L L_t)^{\otimes m_i}\right)
\end{aligned}
$$

as required. □

Corollary A.6. *Let p be prime, with integers $a_1, \ldots, a_r$ and groups $G_1, \ldots, G_r$ as in the Introduction. Suppose $\overline{G}_i \in \{\mathrm{PGL}_{n_i},\ \mathrm{PGSp}_{2^{a_i}},\ \mathrm{PGO}_{2^{a_i}},\ \mathrm{PGO}^{+}_{2^{a_i}}\ (a_i \geq 2)\}$. Then there exists K/k and $E_i \in H^1(K, \overline{G}_i)$ such that the underlying division algebras of the set $\{\delta^i_K(E_i)\}_{i=1,\ldots,r}$ form a disjoint set of division algebras over K, with $\operatorname{ind}(\delta^i_K(E_i)) = p^{a_i}$ and $\exp(\delta^i_K(E_i)) = p^{b_i}$.*

Proof. From [KMRT98, Section 29], the image of $H^1(K, \overline{G}_i)$ in $\mathrm{Br}(K)$ under the boundary map is given by the following (modulo Brauer equivalence):

$$
\delta^i_K(H^1(K, \mathrm{PGL}_{n_i})) = \left\{ \text{ divisional algebras over } K \text{ of index dividing } n_i \right\}
$$

$$\delta_K^i(H^1(K,\mathrm{PGSp}_{2^{a_i}})) = \left\{ \begin{array}{l} \text{divisional algebras over } K \text{ of index dividing} \\ 2^{a_i} \text{ and exponent dividing } 2 \end{array} \right\}$$

$$\delta_K^i(H^1(K,\mathrm{PGO}_{2^{a_i}})) = \left\{ \begin{array}{l} \text{divisional algebras over } K \text{ of index dividing} \\ 2^{a_i} \text{ and exponent dividing } 2 \end{array} \right\}$$

$$\delta_K^i(H^1(K,\mathrm{PGO}^+_{2^{a_i}})) = \left\{ \begin{array}{l} \text{divisional algebras } A \text{ over } K \text{ of index dividing} \\ 2^{a_i}, \text{ exponent dividing 2, and for which there} \\ \text{exists an involution } \sigma \text{ on } A \text{ with trivial} \\ \text{discriminant} \end{array} \right\}$$

Note that $\delta_K^i(H^1(K,\mathrm{PGO}^+_{2^{a_i}}))$ contains the class of any division algebra over K of index dividing 2^{a_i} and exponent dividing 2 which can be properly decomposed as the product of division algebras of exponent dividing 2. The result is now an easy application of Theorem A.2. $\square$

Appendix B Quotient Stacks

In this section we will further discuss the proof of Theorem 2.7, beginning with the lower bound. Recall that we have an exact sequence $1 \to D \to H \to H/D \to 1$ with D central and diagonalizable, and such that the image of the coboundary map $d_K : H^1(K, H/D) \to H^2(K, D)$ consists of only p-primary elements for any K/k. We need to show that there exists K/k and $E \in H^1(K, H/D)$ with $\operatorname{cdim}_K([E/H]; p) = \max_{A,L}(\operatorname{cdim}_L([A/H]; p))$ (over all L/k and $A \in H^1(K, H/D)$) such that

$$\operatorname{ed}_k(H; p) \geq \operatorname{cdim}_K([E/H]; p) + \operatorname{ed}_k(D; p) - \dim(\overline{H}).$$

This result follows from [M13, Theorem 5.11], but the result was only stated in the case $D = \mu_p^t$ for some t. We will prove the result instead (Corollary B.4) using [M13, Theorem 5.11] and [KM08, Theorem 4.4 & Remark 4.5].

Remark B.1. For any K/k and $E \in H^1(K, H/D)$, by [KM08, Theorem 2.1 & Remark 2.9] we can write

$$\operatorname{cdim}([E/H]; p) = \min_{\chi_1,\dots,\chi_t} \sum_{i=1}^{t} \operatorname{ind}(\chi_{i*} \circ d_K(E))$$

where the minimum is taken over all generating sets of $X(D)$. By Theorem 5.2, $\operatorname{cdim}_K([E/H]; p)$ can be maximized by choosing K and E such that for any $\chi \in X(D)$ we have

$$\operatorname{ind}(\chi_* \circ d_L(A)) = \gcd\left\{\dim(V) \mid V \in \operatorname{Rep}^{(\chi)}(H)\right\}.$$

Let D_p be the p-torsion subgroup of D, so that we have an exact sequence $1 \to D_p \to H \to H/D_p$, and let $d'_L : H^1(L, H/D_p) \to H^2(L, D_p)$ be the coboundary map for any L/k.

For $\chi \in X(D)$ and $\chi' \in X(D_p)$, let $\operatorname{Rep}_D^{(\chi)}(H)$ denote the category of all finite dimensional representations ρ of H such that $\rho(z)$ is multiplication

by $\chi(z)$ for all $z \in D$, and let $\mathrm{Rep}_{D_p}^{(\chi')}(H)$ denote the category of all finite dimensional representations ρ' of H such that $\rho'(z)$ is multiplication by $\chi'(z)$ for all $z \in D_p$.

Choose K/k, K'/k, $E \in H^1(K, H/D)$ and $E' \in H^1(K, H/D_p)$ so that for all $\chi \in X(D), \chi' \in X(D_p)$:

$$\mathrm{ind}(\chi_* \circ d_K(E)) = \gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_D^{(\chi)}(H)\right\}$$

$$\mathrm{ind}(\chi'_* \circ d'_{K'}(E')) = \gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_{D_p}^{(\chi')}(H)\right\}$$

Lemma B.2. *Let $\chi' \in X(D_p)$ and let χ_i $(i \in I)$ be the preimages of χ' under the natural map $X(D) \to X(D_p)$. In other words, $(\chi_i)|_{D_p} = \chi'$ $\forall i$. Then*

$$\mathrm{ind}(\chi'_* \circ d'_{K'}(E)) = \min_{i \in I}\left(\mathrm{ind}(\chi_{i*} \circ d_K(E))\right)$$

Proof. By our choice of E and E', it is equivalent to show

$$\gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_{D_p}^{(\chi')}(H)\right\} = \min_{i \in I}\left(\gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_D^{(\chi_i)}(H)\right\}\right)$$

Since $\mathrm{Rep}_{D_p}^{(\chi')}(H) = \bigcup_{i \in I} \mathrm{Rep}_D^{(\chi_i)}(H)$, using general properties of gcd we have

$$\gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_{D_p}^{(\chi')}(H)\right\} = \gcd_{i \in I}\left(\gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_D^{(\chi_i)}(H)\right\}\right)$$

Since $\gcd\left\{\dim(V) \mid V \in \mathrm{Rep}_D^{(\chi_i)}(H)\right\}$ is a power of p for all i by assumption, we can replace $\gcd_{i \in I}$ by $\min_{i \in I}$ and the result follows.

□

Theorem B.3. *Let K/k, K'/k, $E \in H^1(K, H/D)$ and $E' \in H^1(K', H/D_p)$ be as chosen above. Then* $\mathrm{cdim}_K(E/H) = \mathrm{cdim}_{K'}(E'/H) = \mathrm{cdim}_K(E/H; p) = \mathrm{cdim}_{K'}(E'/H; p)$.

Proof. Define

$$T_{E,K} = \langle \chi_* \circ d_K(E)) \rangle_{\chi \in X(D)}$$

and

$$T_{E',K'} = \langle \chi'_* \circ d'_K(E') \rangle_{\chi' \in X(D_p)}.$$

Then, by assumption, both $T_{E,K}$ and $T_{E',K'}$ are (finite) p-groups. As in Section 5, let $b_1, \ldots, b_l$ be a generating set of $T_{E,K}$ with $\sum_{i=1}^{l} \mathrm{ind}(b_i)$ minimal, and define

$$\mathrm{ind}(E,K) = \sum_{i=1}^{l} (\mathrm{ind}(b_i) - 1)$$

Similarly, let $b'_1, \ldots, b'_t$ be a generating set of $T_{E',K'}$ with $\sum_{i=1}^{t} \mathrm{ind}(b_i)$ minimal, and define

$$\mathrm{ind}(E',K') = \sum_{i=1}^{l} (\mathrm{ind}(b'_i) - 1)$$

By applying [KM08, Theorem 2.1 & Remark 2.9] it is equivalent to show $\mathrm{ind}(E,K) = \mathrm{ind}(E',K')$.

We will first show $\mathrm{ind}(E,K) \leq \mathrm{ind}(E',K')$. Choose a generating set $\chi'_1, \ldots, \chi'_m \in X(D_p)$ such that $\chi'_{i*} \circ d'_{K'}(E') = b'_i$ for $i \leq t$ and $\chi'_{i*} \circ d'_{K'}(E') = 0$ for $i > t$. Using Lemma B.2, choose $\chi_1, \ldots, \chi_m \in X(D)$ such that $\chi_i|_{D_p} = \chi'_i$ and $\mathrm{ind}(\chi'_{i*} \circ d'_{K'}(E')) = \mathrm{ind}(\chi_{i*} \circ d_K(E))$. Then $\chi_1, \ldots, \chi_m$ generate $X(D)/pX(D)$, since $pX(D) = \ker(X(D) \to X(D_p))$. Thus $\chi_{1*} \circ d_K(E), \ldots, \chi_{m*} \circ d_K(E)$ generate $T_{E,K}/pT_{E,K}$ which by Lemma 4.1 means they generate $T_{E,K}$. Hence $\mathrm{ind}(E,K) \leq \mathrm{ind}(E',K')$.

To see the reverse direction, choose a generating set (not necessarily of minimal size) $\chi_1, \ldots, \chi_n \in X(D)$ such that $\chi_{i*} \circ d_k(E) = b_i$ for $i \leq l$ and $\chi_{i*} \circ d_k(E) = 0$ for $i > l$. Let $\chi'_i = \chi_i|_{D_p}$. Observe that if we replace χ_i by τ for any $\tau \in X(D)$ with $\tau|_{D_p} = \chi_i|_{D_p}$ then the resulting set $\{\chi_1, \ldots, \chi_n\}$ will still generate $X(D)/pX(D)$ and hence $\{\chi_{1*} \circ d_K(E), \ldots, \chi_{n*} \circ d_K(E)\}$ will

still generate $T_{E,K}$. Thus by Lemma B.2 and the minimality of $\sum b_i$, we have $\mathrm{ind}(\chi_{i*} \circ d_K(E)) = \mathrm{ind}(\chi'_{i*} \circ d'_{K'}(E'))$ for all i. Since the restriction map from $X(D)$ to $X(D_p)$ is surjective, we have that $\{\chi'_{1*} \circ d'_{K'}(E'), \ldots, \chi'_{n*} \circ d'_{K'}(E')\}$ generates $T_{E',K'}$, and the result follows. □

Let K/k and $E \in H^1(K, H/D)$ be as chosen above. In particular, $\mathrm{cdim}_K([E/H]; p) = \max_{A,L}(\mathrm{cdim}_L([A/H]; p))$ over all L/k, $A \in H^1(L, \overline{H})$.

Corollary B.4. *We have*

$$\mathrm{ed}_k(H; p) \geq \mathrm{cdim}_K([E/H]; p) + \mathrm{ed}_k(D; p) - \dim(H/D).$$

Proof. Let K'/k and $E' \in H^1(K', H/D_p)$ also be as chosen above. From [BRV11, Corollary 3.3] (see also [M13, Corollary 5.7]) and [M13, Theorem 5.11], we have:

$$\begin{aligned} \mathrm{ed}_K(H; p) &\geq \mathrm{ed}_{K'}([E'/H]; p) - \dim(H/D_p) \\ &= \mathrm{cdim}_{K'}([E'/H]; p) + \mathrm{ed}_k(D_p; p) - \dim(H) \end{aligned}$$

Since $\mathrm{ed}_k(D_p; p) = \mathrm{ed}_k(D; p) + \dim(D)$ (D is diagonalizable), the result follows from the previous theorem. □

We finish this section with a proof of the upper bound from Theorem 2.7.

Proof of Theorem 2.7.2. Suppose we are given a finitely generated field extension K of k, and $E \in H^1(K, H)$. It suffices to show that

$$\mathrm{ed}_k(E) \leq \mathrm{ed}_k(\overline{H}) + \max_{A,L}(\mathrm{cdim}_L([A/H])) + \mathrm{ed}_k(D)$$

Ket $\overline{E}$ be the image of E under the map $H^1(K, H) \to H^1(K, \overline{H})$. By definition of essential dimension, we can find a k-subfield K_0 of K and $\overline{E_0} \in H^1(K_0, \overline{H})$, with $\mathrm{trdeg}_k(K_0) \leq \mathrm{ed}_k(\overline{H})$, such that $(\overline{E_0})_K = \overline{E}$. Further, if we

view $\overline{E}$ as an H-scheme over K then by Remark 2.6 we have $[\overline{E}/H](K) \neq \emptyset$ since $\overline{E}$ is in the image of $H^1(K,H) \to H^1(K,\overline{H})$. Thus we can find an intermediate field K_1 with $K_0 \subset K_1 \subset K$ such that $[\overline{E_0}/H](K_1) \neq \emptyset$ and $\mathrm{trdeg}_{K_0} K_1 \leq \mathrm{cdim}_{K_0} [\overline{E_0}/H]$. Setting $\overline{E_1} = (\overline{E_0})_{K_1} \in H^1(K_1,\overline{H})$, then again by Remark 2.6 this means that there exists a preimage E_1 of $\overline{E_1}$ under the map $H^1(K_1,H) \to H^1(K_1,\overline{H})$.

We would like to conclude $(E_1)_K = E$, however what we know is:

$$\begin{array}{rcl} H^1(K,H) & \to & H^1(K,\overline{H}) \\ E & \mapsto & \overline{E} \\ (E_1)_K & \mapsto & \overline{E} \end{array}$$

From [S97, I.5.7, Proposition 42], it follows that there exists $a \in H^1(K,D)$ such that, via the action of $H^1(K,D)$ on $H^1(K,H)$, we have $a \cdot (E_1)_K = E$. Again by definition of essential dimension, there exists a field extension K_2/K_1 of transcendence degree at most $\mathrm{ed}_{K_1}(D)$, and $b \in H^1(K_2,D)$ such that $b_K = a$. If we define $E_2 = b \cdot (E_1)_{K_2} \in H^1(K_2,H)$, then we have $(E_2)_K = E$.

Hence,

$$\begin{array}{rcl} \mathrm{ed}(E) \leq \mathrm{trdeg}_k(K_2) & = & \mathrm{trdeg}_k(K_0) + \mathrm{trdeg}_{K_0}(K_1) + \mathrm{trdeg}_{K_1}(K_2) \\ & \leq & \mathrm{ed}_k(\overline{H}) + \mathrm{cdim}_{K_0}[E_0/H] + \mathrm{ed}_{K_1}(D) \\ & \leq & \mathrm{ed}_k(\overline{H}) + \max\limits_{A,L}(\mathrm{cdim}_L([A/H])) + \mathrm{ed}_k(D) \end{array}$$

as required. □

Appendix C Products of Groups with $p \neq 2$

In this section we will consider the case when $p \neq 2$ and

$$G_i \in \{\mathrm{GO}_{n_i}, \mathrm{O}_{n_i}, \mathrm{SO}_{n_i}\}.$$

The key ingredient in these cases is that, since $2 \nmid n_i$, the boundary map $H^1(K, \overline{G}_i) \to H^2(K, Z(G_i))$ is trivial. The results in this section hold under the assumption that each n_i is odd and at least 3 (but not necessarily a prime power). We first study the case where $Z(G)$ is finite.

Theorem C.1. *Let $G_i \in \{\mathrm{O}_{n_i}, \mathrm{SO}_{n_i}\}$ for $1 \leq i \leq r$. Let μ be a central subgroup of G. Then*

$$\mathrm{ed}(G/\mu) = \mathrm{ed}(G/\mu; 2) = \left(\sum_{i=1}^{r} s_i\right) - \mathrm{rank}(\mu)$$

$$\textit{where } s_i = \begin{cases} n_i \textit{ if } G_i = \mathrm{O}_{n_i} \\ n_i - 1 \textit{ if } G_i = \mathrm{SO}_{n_i} \end{cases}$$

Proof. Since n_i is odd, we have $\mathrm{O}_{n_i} \cong \mathrm{SO}_{n_i} \times \mu_2$, and $Z(\mathrm{SO}_{n_i})$ is trivial. Thus if $m = |\{i \mid G_i = \mathrm{O}_{n_i}\}|$, we may write $G \cong \mathrm{SO}_{n_1} \times \cdots \times \mathrm{SO}_{n_r} \times ((\mu_2)^m/\mu)$. Recall that for any algebraic groups H_1 and H_2 we have $\mathrm{ed}_k(H_1 \times H_2) \leq \mathrm{ed}_k H_1 + \mathrm{ed}_k H_2$, and that $\mathrm{ed}_k(\mathrm{SO}_n) = n - 1$ for $n \geq 3$. Since $\mathrm{ed}_k(\mu_2^m/\mu) = \mathrm{rank}(\mu_2^m/\mu) = m - \mathrm{rank}(\mu)$, the upper bound follows.

For the lower bound we proceed as in [RY00, Theorem 7.8 & Theorem 8.1] (see also [GR09, Theorem 1.2 & Example 9.1]). The subgroup $(A_1, \ldots, A_r, \lambda)$ of G, where each A_i a diagonal matrix in SO_{n_i} with entries ± 1, and $\lambda \in \mu_2^m/\mu$, is a finite 2-subgroup of G of rank

$$\left(\sum_{i=1}^{r}(n_i - 1)\right) + m - \mathrm{rank}(\mu)$$

and this subgroup has a finite centralizer. Thus by [RY00, Theorem 7.8],

$$\mathrm{ed}_K(G;2) \geq \left(\sum_{i=1}^{r}(n_i-1)\right) + m - \mathrm{rank}(\mu) = \left(\sum_{i=1}^{r} s_i\right) - \mathrm{rank}(\mu)$$

as required. □

We now study the case where $Z(G)$ is connected.

Lemma C.2. *Let K/k and $G_i = \mathrm{GO}_{n_i}$ for $1 \leq i \leq r$. Let μ be a central subgroup of G. Then*

$$H^1(K,G) \cong H^1(K,G/\mu)$$

Proof. In this case, $Z(G)$ is a torus. Thus we have an exact sequence

$$1 \to Z(G)/\mu \to G/\mu \to \overline{G} \to 1$$

which yields the following in cohomology:

$$0 \to H^1(K,G/\mu) \xrightarrow{\gamma} H^1(K,\overline{G})$$

Since the boundary map is zero, γ is surjective. By [S97, I.5, Proposition 42], γ is injective. Thus $H^1(K,G/\mu) = H^1(K,\overline{G})$ for any $\mu \leq Z(G)$. In particular, $H^1(K,G) \cong H^1(K,G/\mu)$. □

Lemma C.3. *We have* $\mathrm{ed}_k(\mathrm{GO}_n) \leq n-1$.

Proof. $H^1(K,\mathrm{GO}_n)$ classifies orthogonal involutions on $\mathbb{M}_n(K)$ (see [KMRT98, Section 29]). An orthogonal involution is determined by a non-degenerate symmetric bilinear form on K^n up to scalar multiples, and we can diagonalize the form and multiply by scalars so that it is represented by the diagonal Gram matrix:

$$\begin{bmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_{n-1} & \\ & & & & 1 \end{bmatrix}$$

Thus we conclude $\mathrm{ed}_k(\mathrm{GO}_n) \leq n-1$. □

Theorem C.4. *Let $G_i = \mathrm{GO}_{n_i}$ for $1 \leq i \leq r$. Let μ be a central subgroup of G. Then*

$$\mathrm{ed}(G/\mu) = \mathrm{ed}(G/\mu; 2) = \sum_{i=1}^{r} (n_i - 1).$$

Proof. By Lemma C.2, we may assume μ is the trivial subgroup. The upper bound is now obvious using $\mathrm{ed}_k(H_1 \times H_2) \leq \mathrm{ed}_k(H_1) + \mathrm{ed}_k(H_2)$ and Lemma C.3. Recall also that for any algebraic group H_1 with subgroup H_2 we have $\mathrm{ed}_k(H_1; 2) \geq \mathrm{ed}_k(H_2; 2) - \dim(H_1) + \dim(H_2)$. Now, consider the subgroup $H = \mathrm{O}_{n_1} \times \cdots \times \mathrm{O}_{n_r}$. Then we have

$$\mathrm{ed}_k(G; 2) \geq \mathrm{ed}_k(H; 2) - r$$

By Theorem C.1, $\mathrm{ed}_k(H; 2) = \sum_{i=1}^{r} n_i$, and the result follows. □

Remark C.5. For all groups G/μ studied in this section, $\mathrm{ed}_k(G/\mu; q) = 0$ for primes $q \neq 2$. This is because we have the exact sequence

$$H^1(K, Z(G)/\mu) \to H^1(K, G/\mu) \to H^1(K, \overline{G})$$

and any elements $a \in H^1(K, Z(G)/\mu)$ and $b \in H^1(K, \overline{G})$ can be split by adjoining sufficiently many square roots to K. It follows that any element of $H^1(K, G/\mu)$ can also be split by an extension whose degree is a power of 2.