LOWER BOUNDS FOR
ESSENTIAL DIMENSIONS IN CHARACTERISTIC 2
VIA ORTHOGONAL REPRESENTATIONS

ANTONIO BABIC AND VLADIMIR CHERNOUSOV

LOWER BOUNDS FOR
ESSENTIAL DIMENSIONS IN CHARACTERISTIC 2
VIA ORTHOGONAL REPRESENTATIONS

ANTONIO BABIC AND VLADIMIR CHERNOUSOV

Dedicated to the memory of Robert Steinberg

We give a lower bound for the essential dimension of a split simple algebraic group of "adjoint" type over a field of characteristic 2. We also compute the essential dimension of orthogonal and special orthogonal groups in characteristic 2.

1. Introduction

Informally speaking, the essential dimension of an algebraic object can be thought of as the minimal number of independent parameters needed to define it. Essential dimension assigns a numerical invariant (a nonnegative integer) to each algebraic object and allows us to compare their relative complexity. Naturally, the fewer parameters needed for definition, the simpler the object is.

The notion of essential dimension first appeared in the work of J. Buhler and Z. Reichstein [1997] in the context of finite groups. Later on, A. Merkurjev generalized this notion to arbitrary functors from the category of fields to the category of sets; see [Berhuy and Favi 2003]. For the definition, properties, and results on essential dimension of algebraic groups and various functors, we refer to the recent surveys [Merkurjev 2013] and [Reichstein 2010].

In the past 15 years this numerical invariant has been extensively studied by many people. To the best of our knowledge, in all publications on this topic the only approach for computing the essential dimension $\mathrm{ed}(G)$ of an algebraic group G consisted of finding its upper and lower bounds. If, by lucky circumstance, both bounds for G are equal then of course their common value is $\mathrm{ed}(G)$. We remark that this strategy has worked in all cases where $\mathrm{ed}(G)$ is known.

The aim of the current paper is two-fold. We recall that a general method for computing lower bounds of the essential dimensions of simple algebraic groups defined over fields of characteristic $\neq 2$ via orthogonal representations was developed in [Chernousov and Serre 2006]. Our first goal is to extend this approach to characteristic 2. In Section 12, we prove the incompressibility of the so-called canonical monomial quadratic forms and this result leads us to Theorem 2.1 below, which says that for any simple split "adjoint group" G defined over a field of characteristic 2 one has $\mathrm{ed}(G) \geq r + 1$ where $r = \mathrm{rank}(G)$. Second, we show that for an adjoint split group G of type B_r one has $\mathrm{ed}(G) = r + 1$. Thus, this result indicates that the lower bound $r + 1$ of the essential dimension in Theorem 2.1 is optimal for groups of adjoint type in the general case and it seems inevitable that any future progress, if possible, will be based on case by case consideration.

2. The main theorems

We now pass to the precise description of the main results of the paper. In what follows, we assume that k is an algebraically closed field of characteristic 2 and all fields and rings under consideration will contain k.

Let G° be a simple algebraic group over k of adjoint type, and let T be a maximal torus of G°. Let $c \in \mathrm{Aut}(G^\circ)$ be such that $c^2 = 1$ and $c(t) = t^{-1}$ for every $t \in T$ (it is known that such an automorphism exists; see, e.g., [SGA 3$_{\mathrm{III}}$ 1970, exposé XXIV, proposition 3.16.2, p. 355]). This automorphism is inner (i.e., belongs to G°) if and only if -1 belongs to the Weyl group of (G, T). When this is the case, we put $G = G^\circ$. If not, we define G to be the subgroup of $\mathrm{Aut}(G^\circ)$ generated by G° and c. We have

- $G = G^\circ$ for types A_1, B_r, C_r, D_r (r even), G_2, F_4, E_7, E_8;

- $(G : G^\circ) = 2$ and $G = \mathrm{Aut}(G^\circ)$ for types A_r ($r \geq 2$), D_r (r odd), E_6.

Let $r = \dim(T)$ be the rank of G.

Theorem 2.1. *If G is as above, we have* $\mathrm{ed}(G) \geq r + 1$.

Our second main theorem deals with orthogonal and special orthogonal groups.

Theorem 2.2. *Let q be a nondegenerate n-dimensional quadratic form over k.*

(a) *If $n = 2r$, then* $\mathrm{ed}(\mathrm{O}(q)) = r + 1$.

(b) *If $n = 2r$ and r is even, then* $\mathrm{ed}(\mathrm{SO}(q)) = r + 1$.

(c) *If $n = 2r$ and r is odd, then* $r \leq \mathrm{ed}(\mathrm{SO}(q)) \leq r + 1$.

(d) *If $n = 2r + 1$, then* $\mathrm{ed}(\mathrm{O}(q)) = \mathrm{ed}(\mathrm{SO}(q)) = r + 1$.

3. Strategy of the proof of main theorems

For groups of type G_2 and F_4 in Theorem 2.1 there is an easy reduction to orthogonal groups (see Section 14 below). For all other adjoint types, orthogonal and special orthogonal groups, we follow the same approach as in [Chernousov and Serre 2006]. Namely:

(a) We construct a G-torsor θ_G over a suitable extension K/k with tr. $\deg_k(K) = r+1$ (see below).

(b) We show that there exists a suitable representation $\rho : G \to O_N$ such that the image of θ_G in $H^1(K, O_N)$ is incompressible; this implies that θ_G itself is incompressible, and Theorems 2.1 and 2.2 follow.

For the readers' convenience, we recall that a class $[\theta] \in H^1(K, G)$ is called *incompressible* if it doesn't descend to a subfield $F \subset K$ of smaller transcendence degree.

Let us start with part (a) for an adjoint group G. Let R be the root system of G with respect to T, and let R_{sh} be the (sub-) root system formed by the short roots of R. Let $\Delta = \{\alpha_1, \dots, \alpha_r\}$ be a basis of R_{sh}. The root lattices of R and R_{sh} are the same; hence Δ is a basis of the character group $X(T)$. This allows us to identify T with $\mathrm{G}_m \times \cdots \times \mathrm{G}_m$ using the basis Δ.

Call A_0 the kernel of "multiplication by 2" on T. Let

$$A = A_0 \times \{1, c\}$$

be the subgroup of G generated by A_0 and by the element c defined above. The group A is isomorphic to $\mu_2 \times \cdots \times \mu_2 \times \mathbb{Z}/2$.

Take $K = k(t_1, \dots, t_r, x)$ where $t_1, \dots, t_r$ and x are independent indeterminates. We have

$$H^1(K, A) = H^1(K, \mu_2) \times \dots \times H^1(K, \mu_2) \times H^1(K, \mathbb{Z}/2).$$

We make the identifications

$$H^1(K, \mu_2) \simeq K^\times / (K^\times)^2 \quad \text{and} \quad H^1(K, \mathbb{Z}/2) \simeq K/\wp(K)$$

as usual. Here $\wp : K \to K$ is the Artin–Schreier map given by $\wp(a) = a^2 + a$. Then x and the t_i define elements (x) and (t_i) of $H^1(K, \mathbb{Z}/2)$ and $H^1(K, \mu_2)$, respectively. Let θ_A be the element of $H^1(K, A)$ with components $((t_1), \dots, (t_r), (x))$. Let θ_G be the image of θ_A in $H^1(K, G)$. We will prove in Section 14:

Theorem 3.1. (K, θ_G) *is incompressible.*

Note that Theorem 3.1 implies Theorem 2.1 since tr. $\deg K = r+1$. Its proof relies on studying properties of the so-called monomial quadratic forms (see Section 10 below) which are also crucial for the proof of Theorem 2.2.

4. Review: quadratic spaces in characteristic 2

The purpose of this section is to review some properties of quadratic forms in characteristic 2 needed for construction of a representation of our group G with the required property explained above. To this end we will introduce the notion of a "normalization" (or "smoothing") of a quadratic form which may not be standard.

Let K be an arbitrary field of characteristic 2. Recall that a quadratic space over K is a pair (V, q) where V is a vector space over K and q is a quadratic form on V. As usual, for any $a, b \in K$ we will denote by $[a, b]$ a 2-dimensional quadratic form given by $[a, b] = ax^2 + xy + by^2$. The form $[0, 0]$ is called the hyperbolic plane and is denoted by $\mathbb{H}$. Similarly, for $a \in K$ we denote by $\langle a \rangle$ the quadratic form ax^2.

There is a special class of quadratic forms called n-fold Pfister forms; see [Elman et al. 2008]. Recall that, by definition, a quadratic form $[1, a]$ where $a \in K$ is called a 1-fold Pfister form and denoted $\langle\langle a]]$. A quadratic form isometric to

$$\langle\langle a_1, \ldots, a_n]] := \langle\langle a_1, \ldots, a_{n-1} \rangle\rangle_b \otimes \langle\langle a_n]]$$

for some $a_1, \ldots, a_n \in K$ is called a quadratic n-fold Pfister form. In this expression, $\langle\langle a_1, \ldots, a_{n-1} \rangle\rangle_b$ is a symmetric bilinear form given by

$$\langle\langle a_1, \ldots, a_{n-1} \rangle\rangle_b = \langle 1, a_1 \rangle_b \otimes \cdots \otimes \langle 1, a_{n-1} \rangle_b.$$

Let K/k be a finitely generated field extension of our base field k and q a quadratic form over K. Then, if there exists another quadratic form g defined over a field L/k satisfying

- $k \subset L \subset K$,
- $\operatorname{tr.deg}_k L < \operatorname{tr.deg}_k K$, and
- $g \otimes_L K \simeq q$,

we say that q is *compressible*. Otherwise, it is *incompressible*.

The bilinear form $b_q : V \times V \to K$ (called the polar form) associated to a quadratic form q is given by

$$b_q(u, v) = q(v + u) - q(u) - q(v).$$

Its *radical* is

$$\operatorname{rad}(b_q) = \{v \in V \mid b_q(v, w) = 0 \text{ for all } w \in V\}$$

and the *quadratic radical* of q is defined as

$$\operatorname{rad}(q) = \{v \in \operatorname{rad}(b_q) \mid q(v) = 0\}.$$

Obviously, both $\operatorname{rad}(b_q)$ and $\operatorname{rad}(q)$ are vector subspaces in V.

One says that q is *regular* if $\mathrm{rad}(q) = 0$ and q is *nondegenerate* if it is regular over any field extension L/K. Note that nondegeneracy is equivalent to the property $\dim(\mathrm{rad}(b_q)) \leq 1$.

It is well-known (see [Elman et al. 2008]) that any nondegenerate quadratic form q of even dimension $n = 2m$ is isometric to $\bigoplus_{i=1}^{m}[a_i, b_i]$ where $a_i, b_i \in K$. In this case the element $c = \sum a_i b_i$ modulo $\wp(K)$ is called the *Arf invariant* of q. If q is nondegenerate and has odd dimension $n = 2m + 1$, then

$$q \simeq \bigoplus_{i=1}^{m} [a_i, b_i] + \langle c \rangle,$$

where $c \in K^{\times}$ is unique up to squares. This element c (modulo $(K^{\times})^2$) is called the *determinant* (or *discriminant*) of q.

Let $q : V \to K$ be a quadratic form. We denote $\overline{V} := V/\mathrm{rad}(q)$ and let $\pi : V \to \overline{V}$ be the canonical map. It is straightforward to check that the mapping $\bar{q} : \overline{V} \to K$ given by $\bar{q}(\bar{v}) = q(v)$ is well defined. Thus, a quadratic space (V, q) gives rise to a quadratic space $(\overline{V}, \bar{q})$. We will see in the example below that $\bar{q}$ is nondegenerate, but first we state the following definition.

Definition 4.1. We will say that $\bar{q}$ is the (nondegenerate) *normalization* of q.

Example. Let q be a quadratic form over k. Since k is algebraically closed, it is isometric to a quadratic form

$$\langle 0 \rangle \oplus \cdots \oplus \langle 0 \rangle \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H} \quad \text{or} \quad \langle 0 \rangle \oplus \cdots \oplus \langle 0 \rangle \oplus \langle 1 \rangle \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}.$$

It easily follows from the definition that its normalization is the quadratic form

$$\mathbb{H} \oplus \cdots \oplus \mathbb{H} \quad \text{or} \quad \langle 1 \rangle \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}.$$

In particular, $\bar{q}$ is nondegenerate.

Lastly, we want to relate the orthogonal group of a quadratic form q to that of its normalization. Recall that given a quadratic space (V, q) the *orthogonal group* of (V, q) is

$$\mathrm{O}(V, q) = \{x \in \mathrm{GL}(V) \mid q(x(v)) = q(v) \text{ for all } v \in V\}.$$

We define a map

$$\lambda : \mathrm{O}(V, q) \longrightarrow \mathrm{O}(\overline{V}, \bar{q}).$$

by $x \mapsto \bar{x}$, where $\bar{x}(\bar{v}) = \overline{x(v)}$ for all $\bar{v} \in \overline{V}$.

Let us first show that $\bar{x}$ is well defined, i.e., $x(\mathrm{rad}(q)) \subset \mathrm{rad}(q)$ or, equivalently, $x(v) \in \mathrm{rad}(b_q)$ for $v \in \mathrm{rad}(q)$ (because x preserves length of vectors). Let $w_0 \in V$.

Since x is invertible, we have $x(w) = w_0$ for some $w \in V$. Then

$$
\begin{aligned}
b_q(x(v), w_0) &= q(x(v) + w_0) + q(x(v)) + q(w_0) \\
&= q(x(v) + x(w)) + q(x(v)) + q(x(w)) \\
&= q(x(v + w)) + q(x(v)) + q(x(w)) \\
&= q(v + w) + q(v) + q(w) = b_q(v, w) = 0,
\end{aligned}
$$

because $v \in \mathrm{rad}(q) \subset \mathrm{rad}(b_q)$. Thus, $x(v) \in \mathrm{rad}(q)$, as required.

It remains to see that $\bar{x} \in \mathrm{O}(\overline{V}, \bar{q})$. Indeed,

$$
\bar{q}(\bar{x}(\bar{v})) = \bar{q}(\overline{x(v)}) = q(x(v)) = q(v) = \bar{q}(\bar{v}).
$$

Thus, we have the following result:

Lemma 4.2. *The canonical map $V \to \overline{V}$ induces a natural morphism*

$$
\lambda : \mathrm{O}(V, q) \longrightarrow \mathrm{O}(\overline{V}, \bar{q}).
$$

5. Killing forms of simple Lie algebras over $\mathbb{Z}$

Let G be as in Theorem 2.1 and let $\tilde{G}$ be a universal simply connected covering of its connected component G°. To construct the required orthogonal representation ρ of G (see part (b) of our strategy described in Section 3) we need to know what the "normalized" Killing symmetric bilinear form $\mathcal{K}_b$ (and quadratic form $\mathcal{K}_q$) of the Lie algebra $\mathrm{Lie}(\tilde{G})$ look like.

Since our base field has characteristic 2, we begin by computing $\mathcal{K}_q$ in a Chevalley basis of the Lie algebra $\mathcal{L}$ of a split simple simply connected algebraic group defined over $\mathbb{Z}$. We then pass to k by first normalizing $\mathcal{K}_b$, i.e., by dividing all its coefficients by their gcd, and then applying the base change $\mathbb{Z} \to \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} \hookrightarrow k$.

Recall that a Chevalley basis is a canonical basis of $\mathcal{L}$ which arises from a decomposition of

$$
\mathcal{L} = \mathcal{L}_0 \oplus \bigoplus_{\alpha \neq 0} \mathcal{L}_\alpha
$$

into a direct sum of the weight subspaces $\mathcal{L}_\alpha$ with respect to a split maximal toral subalgebra $\mathcal{H} = \mathcal{L}_0 \subset \mathcal{L}$. Note that the set of all nontrivial weights in the above decomposition forms a simple root system and that for every root α we have $\dim(\mathcal{L}_\alpha) = 1$.

In what follows Φ will denote the set of all roots of $\mathcal{L}$ with respect to $\mathcal{H}$, $\Delta \subset \Phi$ its basis, and Φ^+ and Φ^- its positive and negative roots, respectively. It is known (see [Steinberg 1968]) that there exist elements $\{H_{\alpha_i} \mid \alpha_i \in \Delta\}$ in $\mathcal{H}$ and $X_\alpha \in \mathcal{L}_\alpha$, $\alpha \in \Phi$, such that the set

(5.0.1) $\{H_{\alpha_i} \mid \alpha_i \in \Delta\} \cup \{X_\alpha \mid \alpha \in \Phi^+\} \cup \{X_{-\alpha} \mid \alpha \in \Phi^+\}$

forms a basis for $\mathcal{L}$, known as a *Chevalley basis*, and these generators are subject to the following relations:

- $[H_{\alpha_i}, H_{\alpha_j}] = 0$;

- $[H_{\alpha_i}, X_\alpha] = \langle \alpha, \alpha_i \rangle X_\alpha$;

- $H_\alpha := [X_\alpha, X_{-\alpha}] = \sum_{\alpha_i \in \Delta} n_i H_{\alpha_i}$, where $n_i \in \mathbb{Z}$;

- $[X_\alpha, X_\beta] = \begin{cases} 0 & \text{if } \alpha + \beta \notin \Phi, \\ \pm(p+1)X_{\alpha+\beta} & \text{otherwise,} \end{cases}$

where p is the greatest positive integer such that $\alpha - p\beta \in \Phi$. Here, for two roots $\alpha, \beta \in \Phi$, the scalar $\langle \alpha, \beta \rangle$ is given by

$$\langle \alpha, \beta \rangle = \frac{2(\alpha, \beta)}{(\beta, \beta)},$$

where $(\cdot, \cdot)$ denotes the standard inner product on the root lattice. It is in this Chevalley basis (5.0.1) that we will compute the Killing form $\mathcal{K}_q$ of $\mathcal{L}$.

Many people have addressed the computation of Killing forms (see, for example, [Gross and Nebe 2004; Malagon 2009; Seligman 1957; Springer and Steinberg 1970]), but we could not find in the literature explicit formulas valid in characteristic 2. Below we produce such formulas for the normalized Killing forms for each type with the use of the following known facts.

Recall that for any $X, Y \in \mathcal{L}$ one has

$$\mathcal{K}_b(X, Y) = \text{Tr}(\text{ad}(X) \circ \text{ad}(Y)) \quad \text{and} \quad \mathcal{K}_q(X) = \mathcal{K}_b(X, X)$$

where $\text{ad} : \mathcal{L} \to \text{End}(\mathcal{L})$ is the adjoint representation of $\mathcal{L}$. It is straightforward to check that

$$\mathcal{K}_b(H_{\alpha_i}, X_\alpha) = 0 \quad \text{and} \quad \mathcal{K}_b(X_\alpha, X_\beta) = 0$$

for all i and for all roots $\alpha, \beta \in \Phi$ such that $\alpha + \beta \neq 0$; in particular, $\mathcal{K}_q(X_\alpha) = \mathcal{K}_b(X_\alpha, X_\alpha) = 0$. Thus, as a vector space $\mathcal{L}$ is decomposed into an orthogonal sum of its subspaces $\mathcal{H}$ and $\langle X_\alpha, X_{-\alpha} \rangle$, for $\alpha \in \Phi^+$.

It is shown in [Springer and Steinberg 1970] that, for any long root $\alpha \in \Phi$,

$$(5.0.2) \qquad \mathcal{K}_b(H_\alpha, H_\alpha) = \text{Tr}(\text{ad}(H_\alpha) \circ \text{ad}(H_\alpha)) = 4\check{h},$$

where $\check{h}$ is the dual Coxeter number of the given Lie algebra. Also, for any root $\alpha \in \Phi$, we have

$$(5.0.3) \qquad \mathcal{K}_b(X_\alpha, X_{-\alpha}) = \tfrac{1}{2} \text{Tr}(\text{ad}(H_\alpha) \circ \text{ad}(H_\alpha)).$$

Lastly, we need one more result from [Malagon 2009]:

$$(5.0.4) \qquad \mathcal{K}_b(H_{\alpha_i}, H_{\alpha_j}) = 2\check{h}(\check{\alpha}_i, \check{\alpha}_j), \quad \text{where } \check{\alpha}_i = \frac{2\alpha_i}{(\alpha_i, \alpha_i)}$$

and $(\check\alpha, \check\beta)$ is the Weyl-invariant inner product such that $(\check\alpha, \check\alpha) = 2$ for a long root α. Note that the above formula requires $(\check\alpha, \check\alpha) = 2$ for a long root α, so that for groups of type C_n and G_2 we will have to multiply the standard inner product by an appropriate scalar to match this condition.

Combining the above mentioned results, we see that for computation of $\mathcal{K}_b$ we need to know only how $\mathcal{K}_b$ looks on the Cartan subalgebra $\mathcal{H}$. Indeed, (5.0.3) allows us to compute the restriction of $\mathcal{K}_b$ to each 2-dimensional subspace $\langle X_\alpha, X_{-\alpha}\rangle$. Furthermore, for each long root α we know by (5.0.2) that

$$\mathcal{K}_b(H_\alpha, H_\alpha) = 4\check{h}.$$

Similarly, by using (5.0.4) and the fact that the Killing form is W-invariant, where W is the corresponding Weyl group, we see that $\mathcal{K}_b(H_\beta, H_\beta)$ is a constant value for all short roots β, but this value will depend on the type of Φ. Finally, we remark that if $\alpha_i, \alpha_j \in \Delta \subset \Phi$ are nonadjacent roots, then

$$\mathcal{K}_b(H_{\alpha_i}, H_{\alpha_j}) = \mathrm{Tr}\big(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_j})\big) = 0.$$

Indeed, this is equivalent to saying that $(\alpha_i, \alpha_j) = 0$, which is true for nonadjacent roots.

Below we skip straightforward computations of $\mathcal{K}_b(H_{\alpha_i}, H_{\alpha_i})$ and $\mathcal{K}_b(H_{\alpha_i}, H_{\alpha_{i+1}})$ for each type and present the final result only.

5.1. Type A_n. We have:

$$\mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_i})) = 4\check{h} \quad \text{and} \quad \mathrm{Tr}(\mathrm{ad}(H_{\alpha_i}) \circ \mathrm{ad}(H_{\alpha_{i+1}})) = -2\check{h}.$$

Thus, the Killing quadratic form $\mathcal{K}_q$ restricted to the Cartan subalgebra $\mathcal{H}$ of the Lie algebra $\mathcal{L}$ of type A_n is of the form

$$\mathcal{K}_q|_{\mathcal{H}} = 4\check{h}\left(\sum_{i=1}^{n} x_i^2\right) - 4\check{h}\left(\sum_{i=1}^{n-1} x_i x_{i+1}\right).$$

and the Killing form on all of $\mathcal{L}$ is

$$\mathcal{K}_q = \mathcal{K}_q|_{\mathcal{H}} + 4\check{h}\left(\sum_{|\Phi^+|} y_i y_{i+1}\right).$$

To pass to the main field k we first modify (normalize) $\mathcal{K}_q$ by dividing all coefficients of $\mathcal{K}_q$ by $4\check{h}$. After doing so, our modified Killing form (still denoted by $\mathcal{K}_q$) becomes

$$\mathcal{K}_q = \sum_{i=1}^{n} x_i^2 - \sum_{i=1}^{n-1} x_i x_{i+1} + \sum_{|\Phi^+|} y_i y_{i+1}.$$

Passing from $\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$, which is a field of characteristic 2, we finally would like to "diagonalize" our form. Simple computations show that a diagonalization of $\mathcal{K}_q$ looks like

$$\mathcal{K}_q \simeq \begin{cases} \displaystyle\bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \langle 1 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], & \text{if } n \equiv 1 \pmod 4; \\[2em] \displaystyle\bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \langle 0 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], & \text{if } n \equiv 3 \pmod 4; \\[2em] \displaystyle\bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0], & \text{if } n \text{ is even.} \end{cases}$$

Similar arguments work for each type. Below we present the final result only.

5.2. Type B_n.

$$\mathcal{K}_q \simeq \begin{cases} \displaystyle\bigoplus_{i=1}^{(n-2)/2} [0,0] \oplus \bigoplus_{|\Phi^+_{\text{long}}|} [0,0] \oplus \langle c \rangle \oplus m\langle 0 \rangle, & \text{if } n \text{ is even, with } c \in \{0,1\} \\[2em] \displaystyle\bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \bigoplus_{|\Phi^+_{\text{long}}|} [0,0] \oplus m\langle 0 \rangle, & \text{if } n \text{ is odd,} \end{cases}$$

where $m = 2|\Phi^+_{\text{short}}| + 1$.

5.3. Type C_n.

$$\mathcal{K}_q \simeq \langle 1 \rangle \oplus \bigoplus_{|\Phi^+_{\text{long}}|} [0,0] \oplus m\langle 0 \rangle$$

where $m = (n-1) + 2|\Phi^+_{\text{short}}|$.

5.4. Type D_n.

$$\mathcal{K}_q \simeq \begin{cases} \displaystyle\bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \langle 0 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], & \text{if } n \text{ is odd,} \\[2em] \displaystyle\bigoplus_{i=1}^{(n-2)/2} [0,0] \oplus \langle c_1 \rangle \oplus \langle c_2 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], & \text{if } n \text{ is even, with } c_1, c_2 \in \{0,1\}, \end{cases}$$

where one of c_1 or c_2 equals 0.

5.5. Type E_6.

$$\mathcal{K}_q \simeq [0,0] \oplus [0,0] \oplus [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0].$$

5.6. Type E_7.

$$\mathcal{K}_q \simeq [0,0] \oplus [0,0] \oplus [0,0] \oplus \langle 1 \rangle \oplus \bigoplus_{|\Phi^+|} [0,0].$$

5.7. Type E_8.

$$\mathcal{K}_q \simeq [0,0] \oplus [0,0] \oplus [0,0] \oplus [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0].$$

5.8. Type F_4.

$$\mathcal{K}_q \simeq [0,0] \oplus \bigoplus_{|\Phi^+_{\text{long}}|} [0,0] \oplus m\langle 0 \rangle,$$

where $m = 2 + |\Phi^+_{\text{short}}|$.

5.9. Type G_2.

$$\mathcal{K}_q \simeq [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0].$$

6. An orthogonal representation

Proposition 6.1. *Let G° be a split simple adjoint algebraic group over k of one of the following types*: A_r, B_r, C_r, D_r, E_6, E_7, E_8. *Then, there exists a quadratic space (V, q) over k, and an orthogonal linear representation*

$$\rho : G^\circ \longrightarrow O(V, q)$$

with the following property:

$$(*) \qquad \begin{cases} q \text{ is nondegenerate}; \\ \text{the nonzero weights of } T \text{ on } V \text{ are the short roots}; \\ \text{each nonzero weight occurs with multiplicity } 1. \end{cases}$$

Proof. We treat each root system individually.

Types A_n, D_n, E_6, E_7, E_8. Let $W = \text{Lie}(\tilde{G})$. Then, the adjoint representation $\tilde{G} \to O(W, \mathcal{K}_q)$ factors through $\tilde{G} \to G^\circ$, so it induces the representation $\mu : G^\circ \to O(W, \mathcal{K}_q)$. Let ρ be the composition of μ and the map $\lambda : O(W, \mathcal{K}_q) \to O(\overline{W}, \overline{\mathcal{K}_q})$ constructed in Lemma 4.2, and let $V = \overline{W}$. Inspection of the normalized Killing form $\mathcal{K}_q$ presented in Section 5 shows that ρ has the required property.

Type B_r. We take V to be the standard representation of SO_{2r+1} of dimension $2r+1$.

Type C_r. The formula for $\mathcal{K}_q$ presented in Section 5.3 shows that the adjoint representation doesn't work. So, instead of the adjoint representation of $G = \text{PSp}_{2r}$, we consider its representation on the exterior square.

More precisely, let V_1 be the standard representation of $\tilde{G} = \text{Sp}_{2r}$ over $\mathbb{Z}$ equipped with a standard skew-symmetric bilinear form ω. Choose a standard basis $\{e_1, \ldots, e_r, e_{-r}, \ldots, e_{-1}\}$ of V_1. There is a natural embedding $\bigwedge^2(V_1) \to V_1 \otimes V_1$ given by $v \wedge w \to v \otimes w - w \otimes v$. We extend ω to a symmetric bilinear form on $V_1 \otimes V_1$ by

$$\omega(v_1 \otimes v_2, w_1 \otimes w_2) = \omega(v_1, w_1)\omega(v_2, w_2)$$

and take its restriction (still denoted by ω) to $V_2 = \bigwedge^2(V_1)$.

Consider the natural action of G on V_2. This action preserves ω, and thus we have a natural representation $G \to \mathrm{O}(V_2, \omega)$. Let $q_2(x) = \omega(x, x)$ be the quadratic form on V_2 corresponding to ω. Denote $v_i = e_i \wedge e_{-i}$. Also if $i < j$ let $v_{ij} = e_i \wedge e_j$, $w_{ij} = e_{-i} \wedge e_{-j}$ and $u_{ij} = e_i \wedge e_{-j}$ for all $i \neq j$. It is straightforward to check that the subspaces $\langle v_i \rangle$, $\langle v_{ij}, w_{ij} \rangle$, $\langle u_{ij}, u_{ji} \rangle$ of V_2 are orthogonal to each other and that q_2 written in the bases $v_i, v_{ij}, u_{ij}, w_{ij}$ of V_2 is of the form

$$q_2 = 2\left(\sum x_i^2\right) \oplus 4\left(\sum y_{ij} z_{ij}\right).$$

Note that by dividing all coefficients of q_2 by 2 and passing from $\mathbb{Z}$ to $\mathbb{Z}/2$ we don't achieve our goal since the resulting quadratic form is "highly degenerate". So instead of considering the representation of G on V_2 we do the following. One can easily check that any (hyperplane) reflection $\tau : V_1 \to V_1$ acts trivially on a 1-dimensional subspace of V_2 spanned by $v = v_1 + \cdots + v_r$. It follows that Sp_{2r} acts trivially on $\langle v \rangle$ and hence so does G. This implies that G acts on the orthogonal complement $V = \langle v \rangle^{\perp}$ (with respect to ω). This subspace is spanned by linearly independent vectors $v_1 - v_2, v_2 - v_3, \ldots, v_{r-1} - v_r, v_{ij}, u_{ij}, w_{ij}$. In this basis of V, the restriction q of q_2 to V is of the form

$$q = 4\left(\sum x_i^2 - \sum x_i x_{i+1}\right) \oplus 4\left(\sum y_{ij} z_{ij}\right).$$

By dividing all coefficients of q by 4 and applying the base change $\mathbb{Z} \to \mathbb{Z}/2 \subset k$, we obtain an orthogonal representation of G over k with the required property. $\square$

7. The Witt group in characteristic 2

In this section we summarize Arason's results [2006b; 2006a] on the structure of the Witt group of quadratic forms over complete fields of characteristic 2 used in our present work.

Let K be a field of characteristic 2, π an indeterminate over K, and let $K((\pi))$ be the field of formal Laurent series with coefficients in K. If f is a nondegenerate quadratic form over $K((\pi))$ of even dimension, we will denote its image in the Witt group $W_q(K((\pi)))$ by f_W.

Theorem 7.1. *The Witt group $W_q(K((\pi)))$ is the additive group generated by the elements $[\alpha, \beta \pi^{-m}]_W$ and $[\alpha \pi^{-1}, \beta \pi^{-m+1}]_W$, where $m \in \mathbb{Z}$, $m \geq 0$, and $\alpha, \beta \in K$, with the condition that $[\alpha, \beta \pi^{-m}]_W$ and $[\alpha \pi^{-1}, \beta \pi^{-m+1}]_W$ are biadditive as functions of α, β and satisfy the following sets of relations:*

(7.1.1a) $\qquad\qquad [\alpha, \beta \rho^2 \pi^{-m}]_W + [\beta, \alpha \rho^2 \pi^{-m}]_W = 0 \qquad$ *if m is even,*

(7.1.1b) $\qquad [\alpha \pi^{-1}, \beta \rho^2 \pi^{-m+1}]_W + [\beta \pi^{-1}, \alpha \rho^2 \pi^{-m+1}]_W = 0 \qquad$ *if m is even,*

(7.1.1c) $\qquad\quad [\alpha, \beta \rho^2 \pi^{-m}]_W + [\beta \pi^{-1}, \alpha \rho^2 \pi^{-m+1}]_W = 0 \qquad$ *if m is odd,*

and

(7.1.2a) $$[\alpha, \alpha\rho^2\pi^{-2m}]_W + [\alpha, \rho\pi^{-m}]_W = 0,$$

(7.1.2b) $$[\alpha\pi^{-1}, \alpha\rho^2\pi^{-2m+1}]_W + [\alpha\pi^{-1}, \rho\pi^{-m+1}]_W = 0.$$

Here m runs through the nonnegative integers and α, β, and ρ run through K.

Theorem 7.2. *Let $m \geq 0$ and let $W_q(K((\pi)))_m$ be the subgroup of $W_q(K((\pi)))$ generated by $[\alpha, \beta\pi^{-i}]_W$ and $[\alpha\pi^{-1}, \beta\pi^{-i+1}]_W$, where $i \in \mathbb{Z}, 0 \leq i \leq m$ and $\alpha, \beta \in K$. Then:*

 (a) *$W_q(K((\pi)))_0$ is isomorphic to $W_q(K) \oplus W_q(K)$. A generator $[\alpha, \beta]_W$ of $W_q(K((\pi)))_0$ is sent to $[\alpha, \beta]_W$ in the first summand $W_q(K)$, but a generator $[\alpha\pi^{-1}, \beta s]_W$ corresponds to $[\alpha, \beta]_W$ in the second summand.*

 (b) *If $n > 0$, then $W_q(K((\pi)))_{2n}/W_q(K((\pi)))_{2n-1}$ is isomorphic to $K \wedge_{K^2} K \oplus K \wedge_{K^2} K$. The class of a generator $[\alpha, \beta\pi^{-2n}]_W$ corresponds to $\alpha \wedge \beta$ in the first summand, but the class of a generator $[\alpha\pi^{-1}, \beta\pi^{-2n+1}]_W$ corresponds to $\alpha \wedge \beta$ in the second summand.*

 (c) *If $n \geq 0$, then $W_q(K((\pi)))_{2n+1}/W_q(K((\pi)))_{2n}$ is isomorphic to $K \otimes_{K^2} K$. The class of a generator $[\alpha, \beta\pi^{-2n+1}]_W$ corresponds to $\alpha \otimes \beta$, but the class of a generator $[\alpha\pi^{-1}, \beta\pi^{-2n}]_W$ corresponds to $\beta \otimes \alpha$.*

The filtration

$$W_q(K((\pi)))_0 \subset W_q(K((\pi)))_1 \subset W_q(K((\pi)))_2 \subset \cdots$$

of the group $W_q(K((\pi)))$ will be called Arason's filtration. Note that by the above theorem,

$$W_q(K((\pi)))_0 \simeq W_q(K) \oplus W_q(K),$$

so that we have two natural projections:

$$\partial_1 : W_q(K((\pi)))_0 \rightarrow W_q(K) \quad \text{and} \quad \partial_2 : W_q(K((\pi)))_0 \rightarrow W_q(K),$$

which we will call the *first and second residues* (of the zero term of Arason's filtration).

Using the fact that $[f, g] \simeq \mathbb{H}$ for all $f, g \in K((\pi))$ such that $fg \in \pi K[\![\pi]\!]$, it is straightforward to show that the zero term of the Witt group of Arason's filtration and the first residue don't depend on the presentation $L = K((\pi))$. In other words, they don't depend on a choice of a coefficient field $\tilde{K} \subset L$ (for the notion of coefficient fields we refer to Section 9 below) nor of a choice of a uniformizer of L, and the second residue is defined up to similarity only. We leave the details of the verification to the reader.

8. Presentation of quadratic forms in the Witt group

In this section we will work with the Witt group of quadratic forms over a field of Laurent series $K((\pi))$, where the coefficient field K is of characteristic 2 and is finitely generated over k. By Theorems 7.1 and 7.2, given a nondegenerate quadratic form f defined over $K((\pi))$, we may decompose its image f_W in the Witt group as

$$(8.0.1) \qquad f_W = f'_{m,W} + f'_{m-1,W} + \cdots + f'_{0,W}$$

where $f'_{i,W} \in W_q(K((\pi)))_i$ is homogeneous of degree i, i.e., a sum of elements of the form $[\alpha, \beta\pi^{-i}]$ and $[\alpha\pi^{-1}, \beta\pi^{-i+1}]$ with $\alpha, \beta \in K$. Such a decomposition is not unique. The following lemma allows us to choose the homogeneous components of f_W in a canonical way.

Lemma 8.1. *Let $\{\alpha_i\}_{i=1}^N$ be a basis for K as a K^2-vector space and let f be a nondegenerate quadratic form over $K((\pi))$. Then, f_W admits a decomposition $f_W = f_{m,W} + f_{m-1,W} + \cdots + f_{0,W}$ satisfying these conditions:*

- *If n is even, then*

$$f_{n,W} = \sum_{i<j}[\alpha_i, u_j^2\alpha_j\pi^{-n}]_W + \sum_{i<j}[\alpha_i\pi^{-1}, v_j^2\alpha_j\pi^{-n+1}]_W,$$

  where $u_j, v_j \in K$.

- *If n is odd, then*

$$f_{n,W} = \sum_{i,j=1}^N[\alpha_i, u_j^2\alpha_j\pi^{-n}]_W,$$

  where $u_j \in K$.

Proof. Take decomposition (8.0.1). Suppose first that $n = 2s$ is even. Write $f'_{2s,W}$ in the form

$$f'_{2s,W} = \sum[p_i, q_i\pi^{-2s}]_W + \sum[p'_i\pi^{-1}, q'_i\pi^{-2s+1}]_W,$$

where $p_i, q_i, p'_i, q'_i \in K$. Since $\{\alpha_i\}_{i=1}^N$ is a basis for K/K^2, one has

$$p_i = \sum_{i,j=1}^N e_{ij}^2\alpha_j,$$

where $e_{i,j} \in K$ and similarly for the q_i, p'_i, q'_i. Replacing the p_i, q_i, p'_i, q'_i with

these expressions and using the biadditivity of $[\,\cdot\,,\,\cdot\,]_W$ and the fact that $[uv^2, w] = [u, v^2 w]$ for all $u, v, w \in K((\pi))$, we can write $f'_{2s,W}$ in the form

$$f'_{2s,W} = \sum_{i,j=1}^{N} [u_i^2 \alpha_i, v_j^2 \alpha_j \pi^{-2s}]_W + \sum_{i,j=1}^{N} [u_i'^2 \alpha_i \pi^{-1}, v_j'^2 \alpha_j \pi^{-2s+1}]_W$$

$$= \sum_{i,j=1}^{N} [\alpha_i, w_{ij}^2 \alpha_j \pi^{-2s}]_W + \sum_{i,j=1}^{N} [\alpha_i \pi^{-1}, w_{ij}'^2 \alpha_j \pi^{-2s+1}]_W,$$

where $u_i, v_j, u_i', v_j' \in K$ and $w_{ij} = u_i v_j$, $w_{ij}' = u_i' v_j'$. If $i = j$, we have

$$[\alpha_i, w_{ii}^2 \alpha_i \pi^{-2s}]_W \overset{(7.1.2a)}{=} [\alpha_i, w_{ii} \pi^{-s}]_W$$

and

$$[\alpha_i \pi^{-1}, w_{ii}'^2 \alpha_i \pi^{-2s+1}]_W \overset{(7.1.2b)}{=} [\alpha_i \pi^{-1}, w_{ii}' \pi^{-s+1}]_W.$$

If $i > j$ we get

$$[\alpha_i, w_{ij}^2 \alpha_j \pi^{-2s}]_W \overset{(7.1.1a)}{=} [\alpha_j, w_{ij}^2 \alpha_i \pi^{-2s}]_W$$

and

$$[\alpha_i \pi^{-1}, w_{ij}'^2 \alpha_j \pi^{-2s+1}]_W \overset{(7.1.1b)}{=} [\alpha_j \pi^{-1}, w_{ij}'^2 \alpha_i \pi^{-2s+1}]_W.$$

If $n = 2s - 1$ is odd, similar arguments show that $f'_{2s-1,W}$ can be written as a sum of symbols of the form $[\alpha_i, u^2 \alpha_j \pi^{-2s+1}]_W$ where $u \in K$. Collecting all summands in the above decompositions of all $f'_{2s,W}$ and $f'_{2s-1,W}$ of the same degree together, we obtain the required decomposition of f_W. □

The following proposition shows the decomposition above is unique.

Proposition 8.2. *Given a quadratic form f, its image in the Witt group can be decomposed uniquely as $f_W = f_{m,W} + f_{m-1,W} + \cdots + f_{0,W}$, where $f_{m,W}, \ldots, f_{0,W}$ are as in Lemma 8.1.*

Proof. We already know that a decomposition exists, so we only need to prove uniqueness. Suppose

$$f_W = f_{m,W} + f_{m-1,W} + \cdots + f_{0,W} = g_{n,W} + g_{n-1,W} + \cdots + g_{0,W}$$

are two different decompositions of f_W. We first claim that $n = m$. Suppose not, say $m > n$. Let us compare the images of these decompositions in the quotient group $W_q(K((s)))_m / W_q(K((s)))_{m-1}$. Since $n < m$, the image of $g_{n,W} + g_{n-1,W} + \cdots + g_{0,W}$ equals 0 whereas the other decomposition has image the class of $f_{m,W}$. We consider separately the cases when m is even and odd.

When m is even: By Lemma 8.1, write

$$f_{m,W} = \sum_{i<j} [\alpha_i, u_j^2 \alpha_j s^{-m}]_W + \sum_{i<j} [\alpha_i s^{-1}, v_j^2 \alpha_j s^{-m+1}]_W,$$

and by Theorem 7.2,

$$\phi : W_q(K((s)))_m / W_q(K((s)))_{m-1} \simeq K \wedge_{K^2} K \oplus K \wedge_{K^2} K$$

be the canonical isomorphism. Then,

$$\phi(f_{m,W}) = \left(\sum_{i<j} u_j^2 (\alpha_i \wedge \alpha_j), \sum_{i<j} v_j^2 (\alpha_i \wedge \alpha_j) \right).$$

Since $\{\alpha_i \wedge \alpha_j\}_{i<j}$ is a basis for $K \wedge_{K^2} K$,

$$\phi(f_{m,W}) = 0 \iff u_j^2 = v_j^2 = 0 \quad \text{for all } j.$$

This would imply that $f_{m,W} = 0$, a contradiction.

<u>When m is odd</u>: By Lemma 8.1, write

$$f_{m,W} = \sum_{i,j=1}^{N} [\alpha_i, u_j^2 \alpha_j s^{-m}]_W$$

and by Theorem 7.2,

$$\phi : W_q(K((s)))_n / W_q(K((s)))_{n-1} \simeq K \otimes_{K^2} K.$$

Then,

$$\phi(f_{m,W}) = \sum_{i,j=1}^{N} u_j^2 (\alpha_i \otimes \alpha_j).$$

Since $\{\alpha_i \otimes \alpha_j\}_{i,j=1}^{N}$ is a basis for $K \otimes_{K^2} K$,

$$\phi(f_{m,W}) = 0 \iff u_j^2 = 0 \quad \text{for all } j,$$

a contradiction.

Thus $m = n$. If m is even, we conclude from $\phi(f_{m,W}) = \phi(g_{m,W})$ that

$$\sum u_j^2 (\alpha_i \wedge \alpha_j) = \sum u_j'^2 (\alpha_i \wedge \alpha_j),$$

where $u_j'^2$ are the corresponding coefficients of $g_{m,W}$, and similarly,

$$\sum v_j^2 (\alpha_i \wedge \alpha_j) = \sum v_j'^2 (\alpha_i \wedge \alpha_j).$$

This implies that $u_j^2 = u_j'^2$ and $v_j^2 = v_j'^2$, hence $f_{m,W} = g_{m,W}$. Similarly, we can easily see that $f_{m,W} = g_{m,W}$ if m is odd. Then, from the equality

$$(f_{0,W} + \cdots + f_{m-1,W}) + f_{m,W} = (g_{0,W} + \cdots + g_{m-1,W}) + g_{m,W},$$

it follows that

$$f_{0,W} + \cdots + f_{m-1,W} = f_{0,W}' + \cdots + f_{m-1,W}'.$$

By induction, the proof is completed. □

The same arguments as in the proofs of Lemma 8.1 and Proposition 8.2 lead us to the following result needed later to establish incompressibility of the so-called canonical monomial quadratic forms.

Corollary 8.3. *Let f_W be as in (8.0.1), and assume that $f_W \in W_q(K((\pi)))_0$. Then,*
$$f'_{m,W} + f'_{m-1,W} + \cdots + f'_{1,W} = 0.$$

9. Differential bases, 2-bases, the Cohen structure theorem, and coefficient fields

Let K/k be a finitely generated field extension. Recall that $\Omega_{K/k}$ denotes the K-vector space of Kähler differentials. A differential basis for K/k is a set of elements $\{\alpha_i\}_{i \in I}$ of K such that $\{d\alpha_i\} \subset \Omega_{K/k}$ is a vector space basis. Recall also that a set of elements $\{x_\lambda\}_{\lambda \in \Lambda}$ of K is a 2-basis for K over k if the set W of monomials in the x_λ having degree < 2 in each x_λ separately forms a vector space basis for K over its subfield $k \cdot K^2 = K^2 \subset K$. The following facts are well known.

Theorem 9.1. *Let $B = \{x_1, \ldots, x_n\} \subset K$ be a subset. The following are equivalent*:

  (a) *B is a separating transcendence basis for K over k.*

  (b) *B is a 2-basis for K over k.*

  (c) *B is a differential basis for K/k.*

Proof. See [Eisenbud 1995, Theorem 16.14]. □

Assume now that K is equipped with a discrete valuation, trivial on k. We denote its valuation ring by R and the residue field by $\overline{K}$. Since our valuation is trivial on k the residue field $\overline{K}$ contains a copy of k. Throughout we assume that v is geometric of rank 1 (for the definition of geometric valuations, see [Merkurjev 2008]), i.e., $\mathrm{tr.\,deg}_k K = \mathrm{tr.\,deg}_k \overline{K} + 1$.

Let π be a uniformizer and $I = (\pi) \subset R$ be the corresponding maximal ideal in R. Choose $a_1, \ldots, a_n \in R$ such that their images $\bar{a}_1, \ldots, \bar{a}_n$ under the canonical map $R \to \overline{K}$ form a differential basis for $\overline{K}/k$. Note that, by Theorem 9.1, we have $\mathrm{tr.\,deg}_k(\overline{K}) = n$, hence $\mathrm{tr.\,deg}_k(K) = n + 1$. We now claim that

(9.1.1) $B = \{a_1, \ldots, a_n, \pi\}$

is a differential basis for K/k.

Indeed, it suffices to see that $da_1, \ldots, da_n, d\pi$ is a system of generators of $\Omega_{K/k}$ (because the K-vector space $\Omega_{K/k}$ has dimension $n+1$). For that in turn, it suffices to show that this is a system of generators for $\Omega_{R/k}$, for formation of differentials commutes with localization. But this easily follows from the conormal sequence

$$I/I^2 \xrightarrow{\ d\ } \overline{K} \otimes_R \Omega_{R/k} \xrightarrow{\ D\phi\ } \Omega_{\overline{K}/k} \longrightarrow 0$$

(see [Eisenbud 1995, p. 389]) and Nakayama's lemma. Thus, B is a differential basis for K/k.

We will say that a differential basis $\{a_1, a_2, \ldots, a_{n+1}\}$ for K/k *comes from* $\overline{K}$ if there exists a subscript $i \in \{1, 2, \ldots, n+1\}$ such that a_i is a uniformizer in K, $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n+1}$ are units in R, and the images of these elements in $\overline{K}$ form a differential basis for $\overline{K}/k$.

Now, let R be a complete discrete valuation ring containing a field k. Denote its quotient field by L and residue field by $\overline{L}$. We will assume throughout that the field extension $\overline{L}/k$ is finitely generated. It follows from the Cohen structure theorem [Eisenbud 1995, Theorem 7.7] that $R \simeq \overline{L}[\![\pi]\!]$ and $L \simeq \overline{L}((\pi))$, where π is a uniformizer. Such decompositions are not unique. They depend on a choice of π and a choice of a coefficient field in L, i.e., a subfield of L contained in R that maps isomorphically onto $\overline{L}$ under the canonical map $R \to \overline{L}$. Such coefficient fields do exist because the field extension $\overline{L}/k$ is separable. The following theorem describe all coefficient fields.

Theorem 9.2. *Let R be as above. If B is a differential basis for $\overline{L}/k$ then there is one-to-one correspondence between coefficient fields $\tilde{E} \subset R$ containing k and the set $\tilde{B} \subset R$ of representatives for B obtained by associating to each $\tilde{E}$ the set $\tilde{B}$ of representatives for B that it contains.*

Proof. See [Eisenbud 1995, Theorem 7.8]. □

10. Monomial quadratic forms

Let $K = k(t_1, t_2, \ldots, t_n, x)$ be a pure transcendental extension of k of transcendence degree $n+1$. We say that a nondegenerate quadratic form f over K is *monomial* if it is of the form

$$f = \bigoplus_{\mu \in \mathbb{F}_2^n} m_f(\mu) t^\mu [1, x] \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H},$$

where $\mu = (\mu_1, \ldots, \mu_n) \in \mathbb{F}_2^n$, the $t^\mu = t_1^{\mu_1} t_2^{\mu_2} \cdots t_n^{\mu_n}$ are monomials in $t_1, \ldots, t_n$, and $m_f(\mu)$ is the number of times a given summand appears. Note that the multiplicity $m_f(\mu)$ may be 0. Since

$$t^\mu [1, x] \oplus t^\mu [1, x] \simeq \mathbb{H} \oplus \mathbb{H},$$

we may assume without loss of generality that $m_f(\mu) = 0$ or $m_f(\mu) = 1$.

Let V be the vector subspace of $\mathbb{F}_2^n$ generated by all μ such that $m_f(\mu) = 1$. Choose a basis of V, say $\mu_1, \mu_2, \ldots, \mu_s$. Then, define $u_i = t^{\mu_i}$ for $i = 1, \ldots, s$. It is easy to see that $u_1, \ldots, u_s$ are algebraically independent over k. Furthermore, any $\mu \in V$ can be written as $\mu = \sum_{i=1}^s \alpha_i u_i$, where $\alpha_i = 0$ or $\alpha_i = 1$, so that $t^\mu = u_1^{\alpha_1} \cdots u_s^{\alpha_s}$.

Thus, f has descent to the subfield $K' = k(u_1, \ldots, u_s, x) \subset K$, and viewed over K', it is of the form

$$f = u_1[1, x] \oplus u_2[1, x] \oplus \cdots \oplus u_s[1, x] \oplus \left(\bigoplus_{\mu \in V} m_f(\mu) u^\mu [1, x] \right) \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}$$

where u^μ are monomials in $u_1, \ldots, u_s$ of length at least 2. When a monomial quadratic form f is written in such a way and is viewed over K', we say that it is a *canonical monomial form*. We also say that f has *rank* s.

For later use we need the following easy observation.

Proposition 10.1. *If f is a canonical monomial form without summands isometric to the hyperbolic plane $\mathbb{H}$, then f is anisotropic.*

Proof. The argument is similar to that in [Chernousov and Serre 2006, Proposition 5], and we leave the details to the reader. □

Our main result related to canonical monomial quadratic forms is the following.

Theorem 10.2. *If f is a canonical monomial form over K, then f is incompressible.*

The proof of this theorem will be given in Section 12.

11. Incompressibility of canonical monomial forms in "codimension 2"

In this section we establish an auxiliary result, Theorem 11.3 below, needed later on to prove Theorem 10.2. Let $K = k(x, t_1, \ldots, t_n)$ be a pure transcendental extension of k of degree $n + 1$ and v the discrete valuation on K associated to t_1. It is characterized by:

$$v(t_1) = 1 \quad \text{and} \quad v(h) = 0 \text{ for all } h \in k(x, t_2, \ldots, t_n)^\times.$$

Let $R \subset K$ be the corresponding valuation ring. Note that $K^2 \subset K$ is a finite field extension of degree 2^{n+1}. As usual, $K^2(a_{i_1}, \ldots, a_{i_l}) \subset K$ denotes the subfield generated by K^2 and elements $a_{i_1}, \ldots, a_{i_l} \in K$.

Proposition 11.1. *Let $F \subset K$ be a subfield containing k such that $\mathrm{tr.}\deg_k(F) < n + 1$. Then there exists a differential basis $\{a_1, \ldots, a_{n+1}\}$ for K/k coming from $\overline{K}$ such that $F \subset K^2(a_1, \ldots, a_l)$ with $l \leq \mathrm{tr.}\deg_k(F) < n + 1$.*

Proof. Choose any 2-basis $\{b_1, \ldots, b_s\}$ for F/k. By hypothesis, $s = \mathrm{tr.}\deg_k(F) < n+1$. Let $L = K^2(b_1, \ldots, b_s)$. Clearly, L contains F (because $F = F^2(b_1, \ldots, b_s)$). Without loss of generality, we may assume that $L = K^2(b_1, \ldots, b_l)$ where $l \leq s$ and the set of all monomials $b_1^{\epsilon_1} \cdots b_l^{\epsilon_l}$ with $\epsilon_i = 0$ or $\epsilon_i = 1$ is linearly independent over K^2.

Let us first assume that L contains a uniformizer of v. Modifying the set $b_1, \ldots, b_l$ of generators of L, if necessary, without loss of generality, we may

assume that b_1 is a uniformizer of v. Let $E_0 = K^2 \subset E_1 \subset \cdots \subset E_{n+1} = K$ be a chain of quadratic extensions such that

$$E_1 = K^2(b_1), \; E_2 = K^2(b_1, b_2), \ldots, \; E_l = E_{l-1}(b_l) = K^2(b_1, \ldots, b_l).$$

Passing to the residues we have the chain

$$\overline{K}^2 = \overline{E}_1 \subset \overline{E}_2 \subset \cdots \subset \overline{E}_{n+1} = \overline{K}.$$

Since $[E_i : E_{i-1}] = 2$, we have $[\overline{E}_i : \overline{E}_{i-1}] \leq 2$. On the other hand, since v is a geometric valuation of rank 1 we have $[\overline{K} : \overline{K}^2] = 2^n$. It follows that $[\overline{E}_i : \overline{E}_{i-1}] = 2$ for every $2 \leq i \leq n$.

Now choose elements $\bar{a}_i \in \overline{E}_i \setminus \overline{E}_{i-1}$, $i \geq 2$. They form a 2-basis of $\overline{K}$ over k. Take any lifting a_i of $\bar{a}_i$ in E_i. Then the set $\{a_1, a_2, \ldots, a_{n+1}\}$, where $a_1 = b_1$, is a 2-basis of K over k, and hence a differential basis for K/k coming from $\overline{K}$, and it has the required property.

The case when L doesn't contain a uniformizer of v can be treated similarly. $\square$

Let f be a canonical monomial quadratic form over K given by

$$(11.1.1) \qquad\qquad f = \bigoplus_{\mu \in \mathbb{F}_2^n} m_f(\mu) t^\mu [1, x] \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H},$$

where all multiplicities $m_f(\mu)$ are 1 or 0. Since f is canonical, it contains summands $t_i[1, x]$ for $i = 1, \ldots, n$.

Below we will be considering two Witt groups: $W_q(K)$ and $W_q(\hat{K})$. Here $\hat{K} \simeq k(x, t_2, \ldots, t_n)((t_1))$. There exists a natural map $W_q(K) \to W_q(\hat{K})$, and if there is no risk of confusion we will denote the image of f in both groups by f_W.

Lemma 11.2. *The form $(f_{\hat{K}})_W$ lives in $W_q(\hat{K})_0$. Its first residue is a canonical monomial form of rank $n - 1$, and its second residue up to similarity is a nontrivial monomial form of rank $\leq n - 1$.*

Proof. This follows from the definitions of monomial forms and the first and second residues. $\square$

Theorem 11.3. *There exist no differential basis $B = \{a_1, \ldots, a_{n+1}\}$ for K/k and a nondegenerate quadratic form g defined over $L = K^2(a_1, \ldots, a_{n-1})$ such that $g_{K,W} = f_W$.*

Proof. Assume the contrary. Let B and g be the corresponding differential basis and quadratic form. Arguing as in Proposition 11.1, we may additionally assume that B comes from $\overline{K}$. Then, it gives rise to the coefficient field $E \subset \hat{K}$ containing all units from the set B and a presentation $\hat{K} \simeq E((t_1))$. We argue by induction on n.

<u>Case 1:</u> Let $a_1, \ldots, a_{n-1}$ be units in R. Since $L = K^2(a_1, \ldots, a_{n-1})$, our quadratic form g can be written in $W_q(K)$ as a sum of 2-dimensional quadratic forms of the

shape

$$(11.3.1) \qquad [a_1^{\nu_1} \cdots a_{n-1}^{\nu_{n-1}}, u_\epsilon^2 a_1^{\epsilon_1} \cdots a_{n-1}^{\epsilon_{n-1}}]$$

where $\nu_i, \epsilon_i \in \{0, 1\}$, $u_\epsilon \in K$, and we use multi-index notation $\epsilon = (\epsilon_1, \ldots, \epsilon_{n-1})$. We now pass to $\hat{K} = E((t_1))$ and view g over $\hat{K}$. Writing u_ϵ in the form

$$u_\epsilon = t_1^{-s_i} \sum_{j \geq 0} e_{\epsilon j} t_1^j$$

with $e_{\epsilon j} \in E$ and using the fact that $[\alpha, \beta]_W = 0$ if $\alpha, \beta \in \hat{K}$ with $v(\alpha\beta) > 0$, we conclude that (11.3.1) can be written as a sum of symbols of the form

$$[a_1^{\nu_1} \cdots a_{n-1}^{\nu_{n-1}}, e_{\epsilon j}^2 t_1^{-2j} a_1^{\epsilon_1} \cdots a_{n-1}^{\epsilon_{n-1}}]$$

with $e_{\epsilon j} \in E$.

Thus, $g_{\hat{K}, W}$ can be written as $g_{\hat{K}, W} = g_{n, W} + \cdots + g_{0, W}$ where $g_{j, W}$ are homogeneous of the form

$$g_{j, W} = \sum_{\nu, \epsilon} [a_1^{\nu_1} \cdots a_{n-1}^{\nu_{n-1}}, e_{\epsilon j}^2 t_1^{-2j} a_1^{\epsilon_1} \cdots a_{n-1}^{\epsilon_{n-1}}]_W$$

with $e_{\epsilon j} \in E$. Since $g_{\hat{K}, W} = f_W$, it lives in the zero term of Arason's filtration of $W_q(\hat{K})$, where the filtration is viewed in the presentation $\hat{K} \simeq E((t_1))$. Since $a_1, \ldots, a_{n-1} \in E$, by Corollary 8.3 we conclude that $g_n + \cdots + g_1 = 0$. Therefore,

$$f_W = g_{\hat{K}, W} = g_{0, W} = \sum_{\nu, \epsilon} [a_1^{\nu_1} \cdots a_{n-1}^{\nu_{n-1}}, e_{\epsilon 0}^2 a_1^{\epsilon_1} \cdots a_{n-1}^{\epsilon_{n-1}}]_W.$$

But this implies that the second residue of f_W is 0, which contradicts the second assertion in Lemma 11.2.

Case 2: Assume that $a_1, \ldots, a_{n-2}$ are units in R and a_{n-1} is a uniformizer for v. Our arguments below don't depend on the choice of a uniformizer, so by abusing notation we will assume that $a_{n-1} = t_1$. Arguing as above we find that g_W can be written as a sum of symbols of the form

$$[a_1^{\nu_1} \ldots a_{n-2}^{\nu_{n-2}} t_1^{\nu_{n-1}}, u_\epsilon^2 a_1^{\epsilon_1} \ldots a_{n-2}^{\epsilon_{n-2}} t_1^{\epsilon_{n-1}}],$$

where $\nu_i, \epsilon_i \in \{0, 1\}$ and $u_\epsilon \in K$. Furthermore, by passing to $\hat{K} = E((t_1))$ and taking expansions of u_ϵ, we can write $g_{\hat{K}, W}$ as a sum

$$g_{\hat{K}, W} = g_{n, W} + \cdots + g_{1, W} + g_{0, W},$$

where each homogeneous component $g_{i,W}$ is of the form

$$g_{i,W} = \sum_{j,\nu,\epsilon} [a_1^{\nu_1} \cdots a_{n-2}^{\nu_{n-2}}, \alpha_{\epsilon j}^2 a_1^{\epsilon_1} \cdots a_{n-2}^{\epsilon_{n-2}} t_1^{-i}]_W$$
$$+ \sum_{j,\nu',\epsilon'} ([a_1^{\nu_1'} \cdots a_{n-2}^{\nu_{n-2}'} t_1^{-1}, \beta_{\epsilon' j}^2 a_1^{\epsilon_1'} \cdots a_{n-2}^{\epsilon_{n-2}'} t_1^{-i+1}]_W,$$

with $\alpha_{\epsilon j}, \beta_{\epsilon' j} \in E$.

Since $g_{\hat{K},W}$ lives in the zero term of Arason's filtration, as above, application of Corollary 8.3 yields $g_n + \cdots + g_1 = 0$. Thus, $g_{\hat{K},W} = g_{0,W}$ is homogeneous of degree 0, where the component $g_{0,W}$ is a sum of symbols of the form

$$[a_1^{\nu_1'} \cdots a_{n-2}^{\nu_{n-2}'} t_1, \alpha_{\epsilon' 0}^2 a_1^{\epsilon_1'} \cdots a_{n-2}^{\epsilon_{n-2}'} t_1^{-1}]_W \quad \text{and} \quad [a_1^{\nu_1} \cdots a_{n-2}^{\nu_{n-2}}, \beta_{\epsilon 0}^2 a_1^{\epsilon_1} \cdots a_{n-2}^{\epsilon_{n-2}}]_W,$$

with $\alpha_{\epsilon' 0}, \beta_{\epsilon 0} \in E$. Then, the first residue of $g_{\hat{K},W}$ (and hence of f_W) is a sum of symbols

$$[a_1^{\nu_1} \cdots a_{n-2}^{\nu_{n-2}}, \beta_{\epsilon 0}^2 a_1^{\epsilon_1} \cdots a_{n-2}^{\epsilon_{n-2}'}]_W,$$

where $\beta_{\epsilon 0} \in E \simeq \overline{K}$.

Now recall that by construction, $B = \{a_1, \ldots, a_{n-2}, a_n, a_{n+1}\}$ is a differential basis for $E \simeq \overline{K}$ over k and that the first residue of $f_{\hat{K},W}$ is a canonical monomial form of rank $n - 1$. On the other side, as we have seen above, it comes from the subfield $E^2(a_1, \ldots, a_{n-2}) \subset E$. This contradicts the induction assumption. $\square$

Corollary 11.4. *The quadratic form f does not descend to a subfield $k \subset F \subset K$ of transcendence degree $\leq n - 1$.*

Proof. This follows from Proposition 11.1 and Theorem 11.3. $\square$

12. Incompressibility of canonical monomial quadratic forms

Proof of Theorem 10.2. We continue to keep the above notation. In particular, $K = k(x, t_1, t_2, \ldots, t_n)$ is a pure transcendental extension of k of transcendence degree $n + 1$, equipped with the discrete valuation v associated to t_1 and R the corresponding discrete valuation ring. As a matter of notation we denote $\pi = t_1$ and $K_1 = k(t_2, \ldots, t_n, x)$. Thus, $\hat{K} \simeq K_1((\pi))$ and $\overline{K} \simeq K_1$.

Consider a canonical monomial quadratic form f over K given by (11.1.1). The proof of incompressibility of f will be carried out by induction on rank n. More precisely, we will prove by induction on n that the image f_W of f in $W_q(K)$ is incompressible. Of course, this would imply incompressibility of f itself. The base of induction $n = 0$ is obvious.

Lemma 12.1. *If $K = k(x)$ and $f = [1, x] \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}$, then f_W is incompressible.*

Proof. Any subfield of K of transcendence degree 0 over k coincides with k. Hence, if f_W were compressible then it would be represented by a nondegenerate quadratic

form defined over k, which is automatically hyperbolic. On the other hand, by Proposition 10.1, f_W is represented by an anisotropic form $[1, x]$, a contradiction.

$\square$

Now let $n > 0$ and suppose that for all canonical monomial quadratic forms of rank $< n$ their classes in the Witt group are incompressible. Suppose that f_W is compressible. Then, there exists a subfield $F \subset K$ containing k (which may be assumed to have transcendence degree n over k by Proposition 11.1 and Theorem 11.3) and a nondegenerate quadratic form g over F such that $(g_K)_W = f_W$.

For the restriction $w = v|_F$ of v to F there are three possibilities.

Case 1: w is trivial. Write g as a direct sum of 2-dimensional forms $[b_i, c_i]$ with $b_i, c_i \in F \subset R$. Consider Arason's filtration of $W_q(\hat{K})$ with respect to the presentation $\hat{K} = K_1((\pi))$. Since b_i, c_i are in R, g_W lives in the zero term of Arason's filtration; moreover, its second residue is trivial. On the other hand, since $g_{\hat{K},W} = f_{\hat{K},W}$ it has nontrivial second residue by Lemma 11.2, a contradiction.

Case 2: w is nontrivial and the ramification index $e(v/w)$ is even. Then, the same arguments as in Theorem 11.3 show that the second residue of g is trivial, which is impossible since $f_{\hat{K},W} = g_{\hat{K},W}$. Indeed, arguing as in Proposition 11.1, we can choose a differential basis $B = \{a_1, \ldots, a_n, \pi\}$ for K/k coming from $\bar{K}$ such that

$$(12.1.1) \qquad\qquad F \subset K^2(a_1, \ldots, a_n).$$

By Theorem 9.2, B gives rise to the coefficient field $E \subset \hat{K}$ containing $a_1, \ldots, a_n$ and presentation $\hat{K} \simeq E((\pi))$. We then fix this presentation and below we consider the corresponding Arason's filtration.

We now pass to computing the residues of $g_{\hat{K}}$ using our presentation $\hat{K} = E((\pi))$ and inclusion (12.1.1). Since g is nondegenerate, it can be written as a direct sum of 2-dimensional forms $[b_i, c_i]$ with $b_i, c_i \in F$. In turn, in view of (12.1.1), b_i and c_i can be written as sums of elements of the form $\alpha_{i_1 \ldots i_s}^2 a_{i_1} a_{i_2} \cdots a_{i_s}$ with $\alpha_{i_1 \ldots i_s} \in K$. Then arguing as in Theorem 11.3 we conclude that the image of $g_{\hat{K}}$ in $W_q(\hat{K})$ can be written as a sum of symbols

$$\left[a_{i_1} a_{i_2} \cdots a_{i_s}, \frac{\alpha_{j_1 \ldots j_p}^2}{\pi^{2l}} a_{j_1} a_{j_2} \cdots a_{j_p} \right]_W,$$

where $\alpha_{j_1 \ldots j_p} \in E$. Thus, we can write $g_{\hat{K},W}$ as the sum

$$g_W = g_{2m} + g_{2(m-1)} + \cdots + g_0,$$

where all homogeneous components g_{2i} have even degree and are sums of symbols

$$\left[a_{i_1} a_{i_2} \cdots a_{i_s}, \frac{\alpha_{j_1 \ldots j_p}^2}{\pi^{2i}} a_{j_1} a_{j_2} \cdots a_{j_p} \right]_W,$$

with $\alpha_{j_1 \ldots j_p} \in E$. By Corollary 8.3 we obtain $g_{2m} + \cdots + g_2 = 0$. Hence, the second residue of g_W is trivial.

Case 3: $e = e(v/w)$ is odd. Let $\pi' \in F$ be a uniformizer for w. Write $\pi' = u\pi^e$ where $u \in R^\times$. Our argument below doesn't depend on a choice of a uniformizer for v. So, after replacing π with $u\pi$ if necessary, we may assume without loss of generality that $u = v^2$ for some $v \in R^\times$.

Note that we may assume additionally that the extension $F \cdot K^2 / K^2$ has degree 2^n, since otherwise we would be in the "codimension" 2 case and so we could apply Theorem 11.3. Then, $[\bar{F} \cdot \bar{K}^2 : \bar{K}^2] = 2^{n-1}$ (because the extension K/K^2 is unramified and $[\bar{K} : \bar{K}^2] = 2^n$). This implies that there exists a differential basis

$$B' = \{a_1, \ldots, a_{n-1}, \pi'\}$$

for F/k coming from residue field $\bar{F}$ and a unit $a_n \in R^\times$ such that $B = B' \cup \{a_n\}$ is a differential basis for K/k coming from $\bar{K}$.

We now pass to the completions $\hat{F} \subset \hat{K}$ with respect to w and v, respectively. The differential bases B' and B for F/k and K/k give rise to the coefficients field E' and E and representations

$$\hat{F} = E'((\pi')) \subset \hat{K} = E((\pi))$$

such that $E' \subset E$. According to Proposition 8.2 our quadratic form g viewed over $\hat{F}$ admits a unique decomposition $g_{\hat{F},W} = g_m + \cdots + g_0$. Taking into account the facts that $E_1 \subset E$, that $\pi' = v^2\pi^e$ with odd e, and that g viewed over $\hat{K}$ lives in the zero term of Arason's filtration of the field $E((\pi))$, one can easily see that the homogeneous components $g_m, \ldots, g_1$ are trivial, so that $g_{\hat{F},W}$ can be written as a sum of symbols

$$[a_1^{v_1} \cdots a_{n-1}^{v_{n-1}}, u_\epsilon^2 a_1^{\epsilon_1} \cdots a_{n-1}^{\epsilon_{n-1}}] \quad \text{and} \quad [a_1^{v_1} \cdots a_{n-1}^{v_{n-1}} \pi', v_\epsilon^2 a_1^{\epsilon_1} \cdots a_{n-1}^{\epsilon_{n-1}} (\pi')^{-1}]$$

where $u_\epsilon, v_\epsilon \in E_1$. It follows that the first residue of $g_{\hat{K},W} = f_{\hat{K},W}$ lives in the subfield E_1 of $\bar{K} = E$ of transcendence degree $n - 1$ over k. On the other side, this residue is a canonical monomial form of rank $n - 1$, which is impossible by the induction assumption. This completes the proof of incompressibility of f. □

13. Orthogonal and special orthogonal groups

Let g be a nondegenerate n-dimensional quadratic form on a vector space V over k, and let F be any extension of k.

Orthogonal groups. It is well known (see [Knus et al. 1998, §29.E]) that if $n = 2r$ is even, then there exists a natural bijection between $H^1(F, O(V, g))$ and the set of isometry classes of n-dimensional nondegenerate quadratic spaces (V', g').

Similarly, if $n = 2r + 1$ is odd, then $H^1(F, \mathrm{O}(V, g))$ is in one-to-one correspondence with the set of isometry classes of $(2r + 1)$-dimensional nondegenerate quadratic spaces (V', q') over F such that $\mathrm{disc}(q') = 1$. Note that any such q' is isometric to a quadratic form of the shape $([a_1, b_1] \oplus \cdots \oplus [a_r, b_r]) \oplus \langle 1 \rangle$. Then, in both cases the incompressibility of canonical monomial quadratic forms provides us with the required lower bound $\mathrm{ed}(\mathrm{O}(V, g)) \geq r + 1$. What is left to finish the proof of Theorem 2.2 for orthogonal groups is to find a "good" upper bound.

Proposition 13.1. *In the above notation*, $\mathrm{ed}(\mathrm{O}(V, g)) \leq r + 1$.

Proof. It suffices to show that any $2r$-dimensional nondegenerate quadratic form depends on at most $2r$ parameters. Let h be such form over F, and write $h = a_1[1, b_1] \oplus \cdots \oplus a_r[1, b_r]$. Each summand $[1, b_i]$ corresponds to a unique element $\xi_i \in H^1(F, \mathbb{Z}/2)$. Let $H = \mathbb{Z}/2 \oplus \cdots \oplus \mathbb{Z}/2$ be the direct sum of r copies of the constant group scheme $\mathbb{Z}/2$ and let $\xi = (\xi_1, \ldots, \xi_r)$. Choose any embedding $H \hookrightarrow \mathrm{G}_{a,k}$, which exists because k is infinite. The exact sequence

$$0 \longrightarrow H \longrightarrow \mathrm{G}_{a,k} \overset{\phi}{\longrightarrow} \mathrm{G}_{a,k} \longrightarrow 0$$

gives rise to

$$F \overset{\phi}{\longrightarrow} F \overset{\psi}{\longrightarrow} H^1(F, H) \longrightarrow 1.$$

Let $a \in F$ be such that $\psi(a) = \xi$. It follows that ξ has descent to the subfield $k(a)$ of F. This amounts to the fact that there exist $b'_1, \ldots, b'_r \in k(a)$ such that the quadratic form $[1, b'_i]$ viewed over F is isometric to $[1, b_i]$. Therefore, h is isometric to the quadratic form $h' = a_1[1, b'_1] \oplus \cdots \oplus a_r[1, b'_r]$ defined over the subfield $k(a, a_1, \ldots, a_r)$ of F of transcendence degree (over k) at most $r + 1$. $\square$

Remark 13.2. If h has trivial Arf invariant then taking a suitable quadratic extension of $k(a, a_1, \ldots, a_r)$ contained in F, if necessary, we may also assume that h' is defined over a subfield of F of transcendence degree $\leq r + 1$ and has trivial Arf invariant.

Special orthogonal groups. We first find upper bounds.

By [Knus et al. 1998, §29.E], if $n = 2r$ is even, then there exists a natural bijection between $H^1(F, \mathrm{SO}(V, g))$ and the set of isometry classes of $(2r)$-dimensional nondegenerate quadratic spaces (V', g') over F such that the Arf invariant of g' is trivial. Therefore, $\mathrm{ed}(\mathrm{SO}(V, g)) \leq r + 1$, by Remark 13.2.

If $n = 2r + 1$ is odd, then there exists a natural bijection between $H^1(F, \mathrm{SO}(V, g))$ and the set of isometry classes of $(2r + 1)$-dimensional nondegenerate quadratic spaces (V', g') over F such that $\mathrm{disc}(g') = 1$. As we mentioned above, any such g' is isometric to a quadratic form of the shape $([a_1, b_1] \oplus \cdots \oplus [a_r, b_r]) \oplus \langle 1 \rangle$ for some $a_i, b_i \in F$. It follows that $\mathrm{ed}(\mathrm{SO}(V, g)) \leq r + 1$, by Proposition 13.1.

To find a "good" lower bound, we recall that $\mathrm{SO}_{2r+1}(g) = \mathrm{O}_{2r+1}(g)_{\mathrm{red}}$, the reduced subscheme of $\mathrm{O}_{2r+1}(g)$. Thus, we have a natural closed embedding $\mathrm{SO}_{2r+1}(g) \hookrightarrow \mathrm{O}_{2r+1}(g)$. Fix a decomposition $g \simeq h \oplus \langle 1 \rangle$ where $h = \mathbb{H} \oplus \cdots \oplus \mathbb{H}$. It induces a natural closed embedding $\phi_1 : \mathrm{O}_{2r}(h) \hookrightarrow \mathrm{SO}_{2r+1}(g)$ (because $\mathrm{O}_{2r}(h)$ is smooth). Furthermore, we can view $\langle 1 \rangle$ as a subform of $[1, 0] \simeq \mathbb{H}$. This allows us to view g as a subform of a $(2r+2)$-dimensional split quadratic form $q = \mathbb{H} \oplus \cdots \oplus \mathbb{H}$ and this induces a natural map

$$\phi_2 : \mathrm{SO}_{2r+1}(g) \hookrightarrow \mathrm{O}_{2r+1}(g) \hookrightarrow \mathrm{O}_{2r+2}(q).$$

The maps ϕ_1 and ϕ_2, in turn, induce the natural maps

$$\psi_1 : H^1(F, \mathrm{O}_{2r}(h)) \to H^1(F, \mathrm{SO}_{2r+1}(g))$$

and

$$\psi_2 : H^1(F, \mathrm{SO}_{2r+1}(g)) \to H^1(F, \mathrm{O}_{2r+2}(q)).$$

It easily follows from the above discussions that ψ_1 is surjective. Also, identifying elements in $H^1(F, \mathrm{O}_{2r}(h))$ and $H^1(F, \mathrm{O}_{2r+2}(q))$ with the isometry classes of the corresponding quadratic spaces, the isometry class of a quadratic form $\bigoplus_{i=1}^{r}[a_i, b_i]$ goes to the isometry class of $\bigoplus_{i=1}^{r}[a_i, b_i] \oplus \mathbb{H}$ under the composition $\psi_2 \circ \psi_1$.

Theorem 13.3. *If g is a nondegenerate quadratic form of dimension $2r + 1$ over k, then* $\mathrm{ed}(\mathrm{SO}_{2r+1}(g)) \geq r + 1$.

Proof. Take a pure transcendental extension $K = k(x, t_1, \ldots, t_r)$ of k of degree $r + 1$ and a canonical monomial form $f = t_1[1, x] \oplus \cdots \oplus t_r[1, x]$ of dimension $2r$. We will show that its image ξ under ψ_1 is incompressible. Indeed, if ξ is compressible, so is $\psi_2(\xi)$. However, $\psi_2(\xi)$ is represented by a canonical monomial form $t_1[1, x] \oplus \cdots \oplus t_r[1, x] \oplus \mathbb{H}$, which is incompressible by Theorem 10.2, a contradiction. Thus, ξ is incompressible itself, implying $\mathrm{ed}(\mathrm{SO}_{2r+1}(g)) \geq r+1$. $\square$

14. Proof of Theorem 3.1

Types A_r, B_r, C_r, D_r, E_6, E_7, E_8. Let $\rho : G^\circ \to \mathrm{O}(V, q)$ be as in Proposition 6.1. As in [Chernousov and Serre 2006], we can extend it to $\rho_G : G \to \mathrm{O}(V, q)$. Let $\theta_O = \rho_G(\theta_G)$ be the image of θ_G in $H^1(K, \mathrm{O}(V, q))$. Consider the quadratic form q_O on V corresponding to θ_O. If $\dim(q)$ is even, then arguing as in [loc. cit.] we conclude that q_O is a canonical monomial form of rank r. By Theorem 10.2, q_O is incompressible and hence so is θ_G.

If $\dim(q)$ is odd, then we can write it as $q = \langle 1 \rangle \oplus q'$, where q' is a nondegenerate quadratic form of even dimension. The twist q_O of q by θ_O is then of the form $q_O = \langle 1 \rangle \oplus g$, where g is a canonical monomial form of rank r. Finally, the proof of Theorem 13.3 shows that q_O is incompressible as well.

Type G_2. Let F be a field of arbitrary characteristic. By [Serre 1995, Théorème 11], there is a canonical one-to-one correspondence between $H^1(F, G_2)$ and the set of isometry classes of 3-fold Pfister forms defined over F, where G_2 denotes a split group of type G_2 over F. Clearly, any 3-fold Pfister form depends on at most 3 parameters implying $\mathrm{ed}(G_2) \leq 3$. Conversely, a generic 3-fold Pfister form is a canonical monomial form of rank 2, hence incompressible. It follows $\mathrm{ed}(G_2) \geq 3$.

Type F_4. Let F be a field of arbitrary characteristic. It is known that there is a canonical one-to-one correspondence between $H^1(F, F_4)$ and the set of isomorphism classes of 27-dimensional exceptional Jordan algebras over F, where F_4 denotes a split group of type F_4 over F. To each such reduced Jordan algebra J one associates a unique (up to isometry) 5-fold Pfister form $f_5(J)$ [Petersson 2004, §4.1]. Moreover, it is known that any 5-fold Pfister form over F corresponds to some Jordan algebra J over F. Since a generic 5-Pfister form is incompressible, we conclude that $\mathrm{ed}(F_4) \geq 5$.

Acknowledgements

References

[Arason 2006a] J. Arason, "Generators and relations for $W_q(K)$ in characteristic 2", preprint RH-18-2006, University of Iceland, Reykjavík, 2006, Available at http://www.raunvis.hi.is/reports/2006/RH-18-2006.pdf.

[Arason 2006b] J. Arason, "Generators and relations for $W_q(K((S)))$ in characteristic 2", preprint RH-19-2006, University of Iceland, Reykjavík, 2006, Available at http://www.raunvis.hi.is/reports/2006/RH-19-2006.pdf.

[Berhuy and Favi 2003] G. Berhuy and G. Favi, "Essential dimension: a functorial point of view (after A. Merkurjev)", *Doc. Math.* **8** (2003), 279–330. MR 2004m:11056 Zbl 1101.14324

[Buhler and Reichstein 1997] J. Buhler and Z. Reichstein, "On the essential dimension of a finite group", *Compositio Math.* **106**:2 (1997), 159–179. MR 98e:12004 Zbl 0905.12003

[Chernousov and Serre 2006] V. Chernousov and J.-P. Serre, "Lower bounds for essential dimensions via orthogonal representations", *J. Algebra* **305**:2 (2006), 1055–1070. MR 2007i:20070 Zbl 1181.20042

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001

[Elman et al. 2008] R. Elman, N. Karpenko, and A. S. Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society Colloquium Publications **56**, American Mathematical Society, Providence, RI, 2008. MR 2009d:11062 Zbl 1165.11042

[Gross and Nebe 2004] B. H. Gross and G. Nebe, "Globally maximal arithmetic groups", *J. Algebra* **272**:2 (2004), 625–642. MR 2005b:20091 Zbl 1113.20040

[Knus et al. 1998] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications **44**, American Mathematical Society, Providence, RI, 1998. MR 2000a:16031 Zbl 0955.16001

[Malagon 2009] A. L. Malagon, *Killing forms of Lie algebras*, thesis, Emory University, Atlanta, GA, 2009, Available at http://search.proquest.com/docview/305091665. MR 2713364

[Merkurjev 2008] A. S. Merkurjev, "Unramified elements in cycle modules", *J. Lond. Math. Soc.* (2) **78**:1 (2008), 51–64. MR 2009i:14008 Zbl 1155.14017

[Merkurjev 2013] A. S. Merkurjev, "Essential dimension: a survey", *Transform. Groups* **18**:2 (2013), 415–481. MR 3055773 Zbl 1278.14066

[Petersson 2004] H. P. Petersson, "Structure theorems for Jordan algebras of degree three over fields of arbitrary characteristic", *Comm. Algebra* **32**:3 (2004), 1019–1049. MR 2005h:17061 Zbl 1088.17014

[Reichstein 2010] Z. Reichstein, "Essential dimension", pp. 162–188 in *Proceedings of the International Congress of Mathematicians, II: Invited lectures* (Hyderabad, 2010), edited by R. Bhatia et al., Hindustan, New Delhi, 2010. MR 2012g:11074 Zbl 1232.14030

[Seligman 1957] G. B. Seligman, "Some remarks on classical Lie algebras", *J. Math. Mech.* **6**:3 (1957), 549–558. MR 19,631e Zbl 0079.04901

[Serre 1995] J.-P. Serre, "Cohomologie Galoisienne: progrès et problèmes", exposé no. 783, 229–257 in *Séminaire Bourbaki,* 1993/94, edited by N. Bourbaki, Astérisque **227**, Société Mathématique de France, Paris, 1995. MR 97d:11063 Zbl 0837.12003

[SGA 3_III 1970] M. Demazure and A. Grothendieck (editors), *Schémas en groupes, Tome III: Structure des schémas en groupes réductifs, Exposés XIX–XXVI* (Séminaire de Géométrie Algébrique du Bois Marie, 1962–1964), Lecture Notes in Mathematics **153**, Springer, Berlin, 1970. MR 43 #223c Zbl 0212.52810

[Springer and Steinberg 1970] T. A. Springer and R. Steinberg, "Conjugacy classes", pp. 167–266 in *Seminar on Algebraic Groups and Related Finite Groups* (Princeton, NJ, 1968/69), Lecture Notes in Mathematics **131**, Springer, Berlin, 1970. MR 42 #3091 Zbl 0249.20024

[Steinberg 1968] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, CT, 1968. MR 57 #6215 Zbl 1196.22001

ANTONIO BABIC
DEPARTMENT OF MATHEMATICAL AND STATISTICAL SCIENCES
UNIVERSITY OF ALBERTA
632 CENTRAL ACADEMIC BUILDING
EDMONTON AB
EDMONTON T6G 2G1
CANADA

ababic@ualberta.ca

VLADIMIR CHERNOUSOV
DEPARTMENT OF MATHEMATICAL AND STATISTICAL SCIENCES
UNIVERSITY OF ALBERTA
632 CENTRAL ACADEMIC BUILDING
EDMONTON AB
EDMONTON AB T6G 2G1
CANADA

chernous@math.ualberta.ca

PACIFIC JOURNAL OF MATHEMATICS

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Robert Finn
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
finn@math.stanford.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

In memoriam: Robert Steinberg