LOWER BOUNDS FOR ESSENTIAL DIMENSIONS IN CHARACTERISTIC 2 VIA ORTHOGONAL REPRESENTATIONS

A. BABIC AND V. CHERNOUSOV

Abstract. 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.
Keywords: Linear algebraic group, essential dimension, torsor, orthogonal representation, Killing form, quadratic form.
MSC 2010 11E04, 11E57, 11E72, secondary 11E81, 14L35, 20G15.

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 non-negative integer) to algebraic objects 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 a 1997 paper by J. Buhler and Z. Reichstein [BuRe] within the context of finite groups. Later on A. Merkurjev extended this notion to arbitrary functors; see [BF]. For the definition, properties and results on essential dimension of algebraic groups and various functors we refer to recent surveys [Me] and [Re].

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.

Date: November 21, 2014.
V. Chernousov was partially supported by the Canada Research Chairs Program and an NSERC research grant.

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 [ChSe]. Our first goal is to extend this approach to characteristic 2 case. 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.

We now pass to the precise description of the main results of the paper.

2. The main Theorems

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. [DG], Exp. XXIV, Prop. 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.

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

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

2.2. **Theorem.** *Let q be a non-degenerate n-dimensional quadratic form over k. We have:*

(a) *if $n = 2r$ then* $\mathrm{ed}(\mathbf{O}(q)) = r+1$*;*

(b) *if $n = 2r$ and r is even then* $\mathrm{ed}(\mathbf{SO}(q)) = r+1$*;*

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

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 [ChSe]. Namely,

a) we construct a G-torsor θ_G over a suitable extension K/k with $\mathrm{tr.deg}_k(K) = r+1$, see below;
b) we show that there exists a suitable representation $\rho : G \to \mathbf{O}_N$ such that the image of θ_G in $H^1(K, \mathbf{O}_N)$ is incompressible; this implies that θ_G itself is incompressible, and Theorems 2.1 and 2.2 follow.

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 $\mathbf{G}_m \times \cdots \times \mathbf{G}_m$ 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

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

Identify $H^1(K, \mu_2)$ with $K^\times/(K^\times)^2$ and $H^1(K, \mathbb{Z}/2)$ with $K/\wp(K)$ 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's 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:

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

Note that Theorem 3.1 implies Theorem 2.1 since $\mathrm{tr.deg.}\, K = r + 1$. 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" 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 [EKM]). 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

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

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

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

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*.

Given a quadratic form q one associates the bilinear form (called the polar form of q) $b_q : V \times V \to K$ given by

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

Its *radical* is

$$\operatorname{rad}(b_q) = \{v \in V \mid b_q(v, w) = 0 \quad \forall\, w \in V\}$$

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 non-degenerate if it is regular over any field extension L/K. Note that non-degeneracy is equivalent to the property $\dim(\mathrm{rad}(b_q)) \leq 1$.

It is well-known (see [EKM]) that any non-degenerate quadratic form q of even dimension $n = 2m$ is isometric to $q \simeq \oplus_{i=1}^{m}[a_i, b_i]$ 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 non-degenerate and has odd dimension $n = 2m + 1$ then $q \simeq \oplus_{i=1}^{m}[a_i, b_i] + \langle\, c\,\rangle$ where $c \in K^\times$ is unique up to squares. This element c (modulo $(K^\times)^2$) is called the *determinant* (= *discriminant*) of q.

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

4.1. **Definition.** *We will say that $\overline{q}$ is the (non-degenerate) normalization of q.*

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

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

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

It easily follows from the definition that its normalization is the following 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 $\overline{q}$ is non-degenerate.

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

$$\mathbf{O}(V, q) = \{x \in \mathrm{GL}(V) \mid q(x(v)) = q(v) \ \forall\ v \in V\}.$$

We define a map

$$\lambda \colon \mathbf{O}(V, q) \longrightarrow \mathbf{O}(\overline{V}, \overline{q}).$$

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

Let us first show that $\overline{x}$ 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 $\overline{x} \in \mathbf{O}(\overline{V}, \overline{q})$. However,

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

Thus we have the following result:

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

$$\lambda \colon \mathbf{O}(V, q) \longrightarrow \mathbf{O}(\overline{V}, \overline{q}).$$

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

Let G be as in Theorem 2.1 and let $\widetilde{G}$ 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 how the "normalized" Killing symmetric bilinear (resp. quadratic) form $\mathcal{K}_b$ (resp. $\mathcal{K}_q$) of the Lie algebra $\mathrm{Lie}(\widetilde{G})$ looks like.

Since our main 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 g.c.d., 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

$$\mathcal{L} = \mathcal{L}_0 \oplus (\coprod_{\alpha \neq 0} \mathcal{L}_\alpha)$$

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 non-trivial 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^+ (resp. Φ^-) positive (resp. negative) roots.

It is known (see [St]) that there exist elements $\{H_{\alpha_i} | \, \alpha_i \in \Delta\}$ in $\mathcal{H}$ and $X_\alpha \in \mathcal{L}_\alpha,\ \alpha \in \Phi$ such that the set

$$\{H_{\alpha_i} | \, \alpha_i \in \Delta \ \} \cup \{X_\alpha | \, \alpha \in \Phi^+\} \cup \{X_{-\alpha} | \, \alpha \in \Phi^+\} \tag{5.0.1}$$

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 $(-,-)$ 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 $\mathcal{L}$.

Note that many people addressed computation of Killing forms (see, for example, [GN], [Ma] [Sel], [SpSt]), 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

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

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

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

for all i and 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 $\langle \, X_\alpha, X_{-\alpha} \, \rangle$, $\alpha \in \Phi^+$.

Another fact which we need is due to Steinberg and Springer [SpSt]: for any long root $\alpha \in \Phi$ one has

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

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

$$\mathcal{K}_b(X_\alpha, X_{-\alpha}) = \frac{1}{2} \mathrm{Tr}(\mathrm{ad}(H_\alpha) \circ \mathrm{ad}(H_\alpha)). \tag{5.0.3}$$

Lastly, we need one more result from [Ma]:

$$\mathcal{K}_b(H_{\alpha_i}, H_{\alpha_j}) = 2\check{h}(\check{\alpha}_i, \check{\alpha}_j)\ , \tag{5.0.4}$$

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, formula (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 equation (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 non adjacent roots, then

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

Indeed this is equivalent to saying that $(\alpha_i, \alpha_j) = 0$ which is true for non adjacent 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 to $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, 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 as follows:

$$\mathcal{K}_q \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \langle c \rangle \oplus \bigoplus_{|\Phi^+|} [0,0], \text{ if n is odd; } c \in \{0,1\}$$

and

$$\mathcal{K}_q \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \bigoplus_{|\Phi^+|} [0,0], \text{ if n is even}$$

5.2. **Remark.** In the above formula c can be 0 and 1. Its value depends on the parity of m where $n = 2m + 1$.

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

5.3. **Type B_n.**

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

and

$$\mathcal{K}_q \simeq \bigoplus_{i=1}^{(n-1)/2} [0,0] \oplus \bigoplus_{|\Phi^+_{long}|} [0,0] \oplus m\langle 0 \rangle, \text{ if n is odd,}$$

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

5.4. **Type C_n.**

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

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

5.5. **Type D_n.**

$$\mathcal{K}_q \simeq \bigoplus_{i=1}^{(n-1)/2}[0,0] \oplus \langle 0\rangle \oplus \bigoplus_{|\Phi^+|}[0,0], \text{ if n is odd;}$$

and

$$\mathcal{K}_q \simeq \bigoplus_{i=1}^{(n-2)/2}[0,0] \oplus \langle c_1\rangle \oplus \langle c_2\rangle \oplus \bigoplus_{|\Phi^+|}[0,0], \text{ if n is even; } c_1, c_2 \in \{0,1\}.$$

where one of c_1 or c_2 equals 0.

5.6. **Type E_6.**

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

5.7. **Type E_7.**

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

5.8. **Type E_8.**

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

5.9. **Type F_4.**

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

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

5.10. **Type G_2.**

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

6. An orthogonal representation

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

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

with the following property:

($*$) *q is non-degenerate and the nonzero weights of T on V are the short roots and they have multiplicity* 1.

Proof. Types A_n, D_n, E_6, E_7, E_8. Let $W = \mathrm{Lie}(\widetilde{G})$. The adjoint representation $\widetilde{G} \to \mathbf{O}(W, \mathcal{K}_q)$ factors through $\widetilde{G} \to G^\circ$. So it induces the representation $\mu : G^\circ \to \mathbf{O}(W, \mathcal{K}_q)$. Let ρ be the composition of μ and the map $\lambda : \mathbf{O}(W, \mathcal{K}_q) \to \mathbf{O}(\overline{W}, \overline{\mathcal{K}_q})$ given in Lemma 4.2. Denote $V = \overline{W}$. The 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 $\mathbf{SO}_{2r+1}$ of dimension $2r+1$.

Type C_r. The formula for $\mathcal{K}_q$ presented in 5.4 shows that the adjoint representation doesn't work. So instead of the adjoint representation of $G = \mathbf{PSp}_{2r}$ we consider its representation on the exterior square.

More precisely, let V_1 be the standard representation of $\widetilde{G} = \mathbf{Sp}_{2r}$ 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 exists 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 a natural action of G on V_2. This action preserves ω and thus we have a natural representation $G \to \mathbf{O}(V_2, \omega)$. 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

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

Note that dividing all coefficients of q_2 by 2 and passing to $\mathbb{Z} \to \mathbb{Z}/2$ 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 $\mathbf{Sp}_{2r}$ 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 $v_1 - v_2, v_2 - v_3, \ldots, v_{r-1} - v_r, v_{ij}, u_{ij}, w_{ij}$. In this basis of V the restriction q of q_2 to V is of the form

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

Dividing all coefficients of q by 4 and taking 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 [Ar1] 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 over K. If f is a non-degenerate quadratic form over $K((\pi))$, we will denote its image in the Witt group $W_q(K((\pi)))$ by f_W.

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

$$[\alpha, \beta\rho^2\pi^{-k}]_W + [\beta, \alpha\rho^2\pi^{-k}]_W = 0 \text{ if } k \text{ is even} \tag{7.1.1a}$$

$$[\alpha\pi^{-1}, \beta\rho^2\pi^{-k+1}]_W + [\beta\pi^{-1}, \alpha\rho^2\pi^{-k+1}]_W = 0 \text{ if } k \text{ is even} \tag{7.1.1b}$$

$$[\alpha, \beta\rho^2\pi^{-k}]_W + [\beta\pi^{-1}, \alpha\rho^2\pi^{-k+1}]_W = 0 \text{ if } k \text{ is odd} \tag{7.1.1c}$$

$$[\alpha, \alpha\rho^2\pi^{-2k}]_W + [\alpha, \rho\pi^{-k}]_W = 0 \tag{7.1.2a}$$

$$[\alpha\pi^{-1}, \alpha\rho^2\pi^{-2k+1}]_W + [\alpha\pi^{-1}, \rho\pi^{-k+1}]_W = 0 \tag{7.1.2b}$$

Here k runs through the non-negative integers and α, β and ρ run through K.

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

(1) $W_q(K((\pi)))_0$ 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.

(2) 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.

(3) 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 $\beta \otimes \alpha$.

By the above theorem one has

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

so that we have two natural projections

$$\partial_1 : W_q(K((\pi)))_0 \to W_q(K) \text{ and } \partial_2 : W_q(K((\pi))) \to W_q(K)$$

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 the zero term of the Witt group of Arason's filtration and the first residue don't depend on presentation $L = K((\pi)))$. In other words, they don't depend on a choice of a coefficient field $\widetilde{K} \subset L$ (for the notion of coefficient fields we refer to Section 9 below) nor of a choice of a uniformizer of L and that the second residue is defined up to similarity only. We leave the details of the verification to the reader.

8. Presentation of quadratic forms inside 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 non-degenerate quadratic form f defined over $K((\pi))$, we may decompose its image f_W in the Witt group as

$$f_W = f'_{m,W} + f'_{m-1,W} + ... + f'_{0,W} \tag{8.0.1}$$

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 decomposition is not unique. The following lemma allows us to choose the homogeneous components of f_W in a canonical way.

8.1. **Lemma.** *Let $\{\alpha_i\}_{i=1}^N$ be a basis for K as a K^2-vector space and let f be a non-degenerate quadratic form over $K((\pi))$. Then f_W admits a decomposition $f_W = f_{m,W} + f_{m-1,W} + ... + f_{0,W}$ such that it satisfies the following:*

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 $u_i, v_j \in K$;

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 $[\ ,\ ]_W$ and the fact $[uv^2, w] = [u, v^2w]$ for all $u, v, w \in K((\pi))$ we get that $f'_{2s,W}$ can be written in the form

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

where $u_i, v_j, u'_i, v'_j \in K$ and $w_{ij} = u_iv_j$, $w'_{ij} = u'_iv'_j$. 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 shows 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 provides us with the uniqueness of the above decomposition.

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

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

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

are 2 different decompositions of f_W. We first claim that $n = m$. Suppose not. Then without loss of generality we may assume $m > n$. 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 $g_{n,W} + g_{n-1,W} + \dots + g_{0,W}$ equals 0 whereas the other decomposition has image the class of $f_{m,W}$. We consider separately the cases m is even and odd.

m is even: write

$$f_{m,W} \overset{8.1}{=} \sum_{i<j} [\alpha_i, u_j^2 \alpha_j s^{-m}]_W + \sum_{i<j} [\alpha_i s^{-1}, v_j^2 \alpha_j s^{-m+1}]_W$$

and let

$$\phi\colon W_q(K((s)))_m/W_q(K((s)))_{m-1} \overset{7.2}{\simeq} K \wedge_{K^2} K \oplus K \wedge_{K^2} K$$

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 $K \wedge_{K^2} K$,

$$\phi(f_{m,W}) = 0 \Leftrightarrow u_j^2 = v_j^2 = 0 \ \ \forall\, j.$$

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

m is odd: let

$$f_{m,W} \overset{8.1}{=} \sum_{i,j=1}^{N} [\alpha_i, u_j^2 \alpha_j s^{-m}]_W$$

and

$$\phi\colon W_q(K((s)))_n/W_q(K((s)))_{n-1} \overset{7.2}{\simeq} K \otimes_{K^2} K \, .$$

Then we have

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

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

$$\phi(f_{m,W}) = 0 \Leftrightarrow u_j^2 = 0 \ \forall\, j,$$

a contradiction.

Thus $m = n$. If m is even, from $\phi(f_{m,W}) = \phi(g_{m,W})$ we conclude 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 $u_j^2 = u_j'^2$ and $v_j^2 = v_j'^2$, hence $f_{m,W} = g_{m,W}$. Similarly we can see that $f_{m,W} = g_{m,W}$ if m is odd. Then from the equality

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

it follows that

$$f_{0,W} + \dots + f_{m-1,W} = f'_{0,W} + \dots + f'_{m-1,W}\,.$$

By induction, the proof is completed. □

9. Differential bases, 2-bases, 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.

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

(1) *B is a separating transcendence basis for K over k;*
(2) *B is a 2-basis for K over k:*
(3) *B is a differential basis for K/k.*

Proof. See [Ei, 16.14]. □

Assume now that K is equipped with a discrete valuation trivial on k. We denote its valuation ring by R and residue field by $\overline{K}$. Since our valuation is trivial on k residue field $\overline{K}$ contains a copy of k. Let π be a uniformizer. Choose $a_1, \dots, a_n \in R$ such that their images $\overline{a}_1, \dots, \overline{a}_n$ under the canonical map $R \to \overline{K}$ form a differential basis for $\overline{K}/k$. Note that, by Theorem 9.1, we have $\operatorname{tr.deg}_k(\overline{K}) = n$, hence $\operatorname{tr.deg}_k(K) = n + 1$. Then we claim that

$$B = \{a_1, \dots, a_n, \pi\} \tag{9.1.1}$$

is a differential basis for K/k. Indeed, it is straightforward to check that all monomials $a_1^{\epsilon_1} \dots a_n^{\epsilon_n} \pi^{\epsilon_{n+1}}$ with $\epsilon_1, \dots, \epsilon_{n+1} = 0, 1$ are linearly independent over $kK^2 = K^2$. This implies that B is a 2-basis for K over k. Hence the claim follows from Theorem 9.1.

Conversely, if (9.1.1) is a differential basis for $\Omega_{K/k}$ such that all a_i are units in R then $da_1, \dots, da_n$ viewed as elements of $\Omega_{R/k}$ are linearly independent over R. Then from the conormal sequence

$$(\pi)/(\pi)^2 \longrightarrow \overline{K} \otimes_R \Omega_{R/k} \longrightarrow \Omega_{\overline{K}/k} \longrightarrow 0,$$

(see [Ei, page 387]) we conclude that their images $d\,\overline{a}_1, \dots, d\,\overline{a}_n$ are linearly independent over $\overline{K}$. By dimension count $\{\overline{a}_1, \dots, \overline{a}_n\}$ is a differential basis for $\overline{K}/k$.

We will say that a *differential basis* $\{a_1, a_2, \dots, a_{n+1}\}$ *for* K/k *comes from* $\overline{K}$ if a_i is a uniformizer in K and $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n+1}$ are units in R for some index i.

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 [Ei, 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.

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

Proof. See [Ei, Theorem 7.8]. □

10. Monomial quadratic forms

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

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

where $\mu = (\mu_1, ..., \mu_n) \in \mathbb{F}_2^n$, $t^\mu = t_1^{\mu_1} t_2^{\mu_2} \dots t_n^{\mu_n}$ are monomials in $t_1, \dots, t_n$ and $m_f(\mu)$ 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 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 $\mu_1, \mu_2, ...\mu_s$. Then define $u_i = t^{\mu_i}$ for $i = 1, ..., s$. It is easy to see that $u_1, \dots, u_s$ 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 1 so that $t^\mu = u_1^{\alpha_1} ... u_s^{\alpha_s}$.

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

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

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.

10.1. **Proposition.** *Let f be 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 [ChSe, Proposition 5] and we leave the details to the reader. □

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

10.2. **Theorem.** *Let f be a canonical monomial form over K. Then f is incompressible.*

11. Incompressibility of 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 valuation on K associated to t_1. It is characterized by:

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

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 $a_{i_1}, \ldots, a_{i_l} \in K$.

11.1. **Proposition.** *Let $F \subset K$ be a subfield containing k such that* $\operatorname{tr.deg}_k(F) < n+1$. *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 $l \leq$* $\operatorname{tr.deg_k(F)} < \mathrm{n}+1$.

Proof. Choose any 2-basis $\{b_1, \ldots, b_s\}$ for F/k. Since $s = \operatorname{tr.deg}_k(F)$ we get $s < n+1$. Let $L = K^2(b_1, \ldots, b_s)$. Clearly, L contains F and for any $\alpha_1, \ldots, \alpha_s \in K$ one has

$$L = K^2(b_1, \ldots, b_s) = K^2(\alpha_1^2 b_1, \ldots, \alpha_s^2 b_s).$$

The restriction $w = v|_F$ is either nontrivial or trivial.

Case 1*: w is nontrivial and the ramification index* $e(v/w)$ *is even.* Multiplying b_i by an appropriate scalar α_i^2 we may assume that $c_1 = \alpha_1^2 b_1, \dots, c_s = \alpha_s^2 b_s$ are units in R and $F \subset L = K^2(c_1, \dots, c_s)$. Without loss of generality we may also assume that $\{c_1, \dots, c_l\}$ where $l \leq s$ is a minimal set of generators of L over K^2 so that $L = K^2(c_1, \dots, c_l)$. The set of all monomials $c_1^{\epsilon_1} \cdots c_l^{\epsilon_l}$ with $\epsilon_i = 0, 1$ is linearly independent over K^2. Put $a_1 = c_1, \dots, a_l = c_l$ and choose units $a_{l+1}, \dots, a_n$ in R such that $B = \{a_1, \dots, a_n, a_{n+1}\}$ where $a_{n+1} = t_1$ is a 2-basis for K over k. By Theorem 9.1, B is a differential basis for K over k coming from $\overline{K}$ and by construction it has the required property.

Case 2*: w is trivial.* Take $\alpha_i = 1$ and $c_i = b_i$ for all i and apply the same argument as above .

Case 3*: w is nontrivial and the ramification index* $e(v/w)$ *is odd.* Without loss of generality we may assume that $b_1, \dots, b_{s-1}$ are units and b_s is a uniformizer for w. Choose scalars $\alpha_1, \dots, \alpha_s \in K$ such that $c_1 = \alpha_1^2 b_1, \dots, c_{s-1} = \alpha_{s-1}^2 b_{s-1}$ are units in R, $c_s = \alpha_s^2 b_s$ is a uniformizer for v and $F \subset L = K^2(c_1, \dots, c_s)$. Then the same argument as above completes the proof. □

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

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

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

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

11.2. **Lemma.** $(f_{\widehat{K}})_W$ *lives in* $W_q(\widehat{K})_0$. *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. □

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

Proof. Assume the contrary. Let B and g be the corresponding differential basis and quadratic form. The differential basis B gives rise to the coefficient field $E \subset \widehat{K}$ containing all units from B and presentation $\widehat{K} \simeq E((t_1))$.

We argue by induction on n. If $n = 1$ then $L = K^2$. Hence g can be written as a direct sum of 2-dimensional quadratic forms $[u_i, v_i] = [1, w_i^2]$ where $u_i, v_i \in K^2$ and $u_i v_i = w_i^2$. We now pass to $\widehat{K} = E((t_1))$ and view g over $\widehat{K}$. Writing w_i in the form $w_i = t_1^{-s_i}(\sum_{j\geq 0} e_{ij} t_1^j)$ with $e_{ij} \in E$ and using the property $[u(t_1), v(t_1)]_W = 0$ if $v(u(t_1)v(t_1) > 0$ we conclude that $[1, w_i^2]_{\widehat{K},W}$ can be written as a sum of symbols of the form $[1, e_{kj}^2 t_1^{-2k}]_W$ with $e_{kj} \in E$. Thus, $g_{\widehat{K},W}$ can be written as $g_{\widehat{K},W} = g_{n,W} + \cdots + g_{0,W}$ where $g_{i,W}$ is of the form

$$g_{i,W} = \sum_j [1, e_{ij}^2 t_1^{-2i}]_W = [1, (\sum_j e_{ij})^2 t_1^{-2i}]_W$$

with $e_{ij} \in E$. Since $g_{\widehat{K},W} = f_W$, it lives in the zero term of Arason's filtration. Then, by Proposition 8.2, we conclude $g_n = \ldots = g_1 = 0$. Therefore $f_W = g_{\widehat{K},W} = [1, \alpha^2]_W$ for some $\alpha \in E$. But this implies that the second residue of f_W is 0 which contradicts the second assertion in Lemma 11.2.

Now let n be arbitrary and suppose that the statement is true for all canonical monomial forms of rank $< n$. Assume first that $a_1, \ldots, a_{n-1}$ are units in R. Let $g = \oplus_i [u_i, v_i]$ with $u_i, v_i \in L$. Writing

$$u_i = \sum_\epsilon u_\epsilon^2 a_1^{\epsilon_1} \ldots a_{n-1}^{\epsilon_{n-1}}, \quad v_i = \sum_\epsilon v_\epsilon^2 a_1^{\epsilon_1} \ldots a_{n-1}^{\epsilon_{n-1}}$$

where we use multi-index notation $\epsilon = (\epsilon_1, \ldots, \epsilon_{n-1})$ and $u_\epsilon, v_\epsilon \in K$ and arguing as above we conclude that $g_{\widehat{K},W}$ can be written as a sum $g_{\widehat{K},W} = g_{n,W} + \cdots + g_{0,W}$ where the homogeneous component $g_{i,W}$ is of the form

$$g_{i,W} = \sum_{j,\epsilon,\epsilon'} [a_1^{\epsilon_1} \ldots a_{n-1}^{\epsilon_{n-1}}, \alpha_{ij}^2 a_1^{\epsilon'_1} \ldots a_{n-1}^{\epsilon'_{n-1}} t_1^{-i}]_W$$

with $\alpha_{ij} \in E$. Since $g_{\widehat{K},W}$ lives in the zero term of Arason's filtration, application of Proposition 8.2 yields $g_n = \ldots = g_1 = 0$. Then as above we conclude that the second residue of $g_{\widehat{K},W}$ is zero, a contradiction.

Finally, assume that up to numbering a_{n-1} is a uniformizer of v. The same argument as above shows that $g_{\widehat{K},W} = g_{0,W}$ is homogeneous of degree 0 where the component $g_{0,W}$ is a sum of symbols of the form

$$[a_1^{\epsilon_1} \ldots a_{n-2}^{\epsilon_{n-2}} t_1, \alpha_i^2 a_1^{\epsilon'_1} \ldots a_{n-2}^{\epsilon'_{n-2}} t_1^{-1}]_W \quad \text{and} \quad [a_1^{\epsilon_1} \ldots a_{n-2}^{\epsilon_{n-2}}, \beta_i^2 a_1^{\epsilon'_1} \ldots a_{n-2}^{\epsilon'_{n-2}}]_W$$

with $\alpha_i, \beta_i \in E$. Then the first residue of $g_{\widehat{K},W}$ (and hence of f_W) is a sum of symbols

$$[a_1^{\epsilon_1} \ldots a_{n-2}^{\epsilon_{n-2}}, \beta_i^2 a_1^{\epsilon'_1} \ldots a_{n-2}^{\epsilon'_{n-2}}]_W$$

where $\beta_i \in E \simeq \overline{K}$. But $\overline{B} = \{a_1, \ldots, a_{n-2}, a_n, a_{n+1}\}$ is a differential basis for $E \simeq \overline{K}$ over k and the first residue of $f_{\widehat{K},W}$ is a canonical monomial form of rank $n-1$. This contradicts the induction assumption. $\square$

11.4. **Corollary.** *There exists no subfield $k \subset F \subset K$ of transcendence degree $\leq n-1$ and a quadratic form g over F such that $g_K \simeq f$.*

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 keep the above notation. In particular, $K = k(x, t_1, t_2, ..., t_n)$ is a pure transcendental extension of k of transcendence degree $n+1$ equipped with a 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 $\widehat{K} \simeq K_1((\pi))$ 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.

12.1. **Lemma.** *Let $K = k(x)$ and let $f = [1, x] \oplus \mathbb{H} \oplus \cdots \oplus \mathbb{H}$. 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 non-degenerate 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 Witt-equivalence classes 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, and a non-degenerate 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 $W_q(\widehat{K})$ with respect to the presentation $\widehat{K} = K_1((\pi))$. Since b_i, c_i are units, g_W lives in the zero term of Arason's filtration and moreover its second residue is trivial. On the other hand, since $g_{\widehat{K},W} = f_{\widehat{K},W}$ 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. Arguing as in Proposition 11.1 we can choose a differential basis $B = \{a_1, \dots, a_n, \pi\}$ for K/k coming from $\overline{K}$ such that

$$F \subset K^2(a_1, \dots, a_n). \tag{12.1.1}$$

By Theorem 9.2, B gives rise to the coefficient field $E \subset \widehat{K}$ containing $a_1, \dots, a_n$ and presentation $\widehat{K} \simeq E((\pi))$. Clearly, $\{a_1, \dots, a_n\}$ is a 2-basis for E/k. We fix the presentation $\widehat{K} \simeq E((\pi))$ and we will apply Arason's results [Ar1] for this presentation only.

By construction $f_{\widehat{K},W} = g_{\widehat{K},W}$, hence the first residue of $g_{\widehat{K},W}$ is a canonical monomial form of rank $n-1$ and the second residue of $g_{\widehat{K}}$ is nontrivial. We now pass to computing the residues of $g_{\widehat{K}}$ using our presentation $\widehat{K} = E((\pi))$ and inclusion (12.1.1).

Since g is non-degenerate 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, c_i can be written as sums of elements of the form $\alpha^2_{i_1 \dots i_s} a_{i_1} a_{i_2} \cdots a_{i_s}$ with $\alpha_{i_1 \dots i_s} \in K$. Then arguing as in Theorem 11.3 we conclude that the image of $g_{\widehat{K}}$ in $W_q(\widehat{K})$ can be written as a sum of symbols

$$[a_{i_1} a_{i_2} \cdots a_{i_s}, \frac{\alpha^2_{j_1 \dots j_p}}{\pi^{2l}} a_{j_1} a_{j_2} \cdots a_{j_p}]_W$$

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

$$g_W = g_{2n} + g_{2(n-1)} + \dots + g_0$$

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

$$[a_{i_1} a_{i_2} \cdots a_{i_s}, \frac{\alpha^2_{j_1 \dots j_p}}{\pi^{2i}} a_{j_1} a_{j_2} \cdots a_{j_p}]_W$$

with $\alpha_{j_1 \dots j_p} \in E$. Obviously g_0 has trivial second residue (because $a_1, \dots, a_n$ are units). So to get a contradiction it remains to show that $g_{2n} + \cdots + g_2 = 0$ in $W_q(\widehat{K})$.

Let us start from the highest component g_{2n}. Recall that according to Arason's Theorem we have

$$W_q(E((\pi)))_{2n} / W_q(E((\pi)))_{2n-1} \simeq E \wedge_{E^2} E \oplus E \wedge_{E^2} E.$$

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. To simplify writing we introduce multi-indices a_{I_j} where I_j is a set of some indices $i_1, \dots, i_s$ and a_{I_j} is the product of the corresponding a_{i_p}.

Let $a_{I_1}, \dots, a_{I_{2n}}$ be a E^2-basis of E. By construction, g_{2n} is a sum of elements of the form

$$[a_{I_j}, \frac{\alpha_{I_s}^2}{\pi^{2n}} a_{I_s}]_W$$

with $\alpha_{I_s} \in E$. Recall that if $I_j = I_s$ then

$$[a_{I_j}, \frac{\alpha_{I_j}^2}{\pi^{2n}} a_{I_j}]_W = [a_{I_j}, \frac{\alpha_{I_j}}{\pi^n}]_W$$

by (7.1.2a)). It follows that g_{2n} can be written as $g_{2n} = g'_{2n} + g''_n$ where

$$g'_{2n} = \sum_{s<j} [a_{I_j}, a_{I_s} \frac{\alpha_{I_s}^2}{\pi^{2n}}]_W$$

with $\alpha_s \in E$ and g''_n lives in $W_q(E((\pi)))_n$. But g lives in $W_q(E((\pi)))_0$, hence the image of g'_{2n} in $W_q(\widehat{K})_{2n}/W_q(\widehat{K})_{2n-1}$ is trivial and this of course implies $g'_{2n} = 0$, by Theorem 7.2.

Note that arguing in such a way we have eliminated the highest homogeneous component g_{2n} of g living in $W_q(E((\pi)))_{2n}$, but we possibly acquire the component g''_n with $n > 0$ in even or odd degree $W_q(E((\pi)))_n$ (if n is odd).

We can continue to do the same with the next highest homogeneous component of g. If it has even degree the same argument as above reduces it to a smaller component. If it has odd degree $2m+1$ then it can be written in the form

$$\sum_{j,s} [a_{I_j}, \frac{a_{I_s}}{\pi^{2m+1}} \alpha_{I_s}^2]_W$$

with $\alpha_{I_s} \in E$. Then applying Arason's Theorem 7.2, part (3), and arguing similarly we conclude that this component is automatically 0. This completes the proof of the fact that $g_{2n} + \dots + g_2 = 0$ and hence the proof of incompressibility of f_W in the case $e(v/w)$ is even.

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 π for v. So replacing π with $u\pi$ if necessary we may assume without loss of generality that $u = v^2$ for some $v \in R^\times$.

Choose a differential basis $B' = \{a_1, \dots, a_{n-1}, \pi'\}$ for F/k coming from residue field $\overline{F}$. Clearly, $F \subset K^2(a_1, \dots, a_{n-1}, \pi')$. We claim that all monomials $a_1^{\epsilon_1} \dots a_{n-1}^{\epsilon_{n-1}}$ with $\epsilon_i = 0, 1$ are linearly independent modulo K^2. Indeed, assume the contrary. Then up to numbering we may assume that $a_1, \dots, a_l$ with $l < n-1$ is a minimal system of generators of $K^2(a_1,\dots,a_{n-1})$ over K^2. Then there exists units $a'_{l+1},\dots,a'_n$ in R such that $\{a_1,\dots,a_l,a'_{l+1},\dots,a'_n,\pi'\}$ is a 2-basis of K over k. Since

$$F\subset K^2(a_1,\dots,a_{n-1},\pi')=K^2(a_1,\dots,a_l,\pi')$$

and $l<n-1$ this contradicts Theorem 11.3.

Now choose $a_n\in R^\times$ such that $B=\{a_1,\dots,a_{n-1},a_n,\pi\}$ is a 2-basis for K over k and hence a differential basis for K/k coming from $\overline{K}$. It follows that two completions $\widehat{F}\subset\widehat{K}$ with respect to w and v respectively admit compatible coefficient fields, i.e. if $E'\subset\widehat{F}$ (resp. $E\subset\widehat{K}$) is a coefficient field corresponding to B' (resp. B) then $E'=E\cap\widehat{F}$ and so we may choose compatible presentations

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

where $E'\subset E$.

The set of all monomials $a_1^{\epsilon_1}\dots a_{n-1}^{\epsilon_{n-1}}$ where $\epsilon_i=0,1$ form a basis of E' over $(E')^2$. Like before, let us number them in any order using multi-indices $a_{I_1},\dots,a_{I_{2^{n-1}}}$. Lemma 8.1 and Proposition 8.2 show that g_W viewed over $\widehat{F}$ can be written uniquely in the form $g_W=g_n+\dots+g_0$ where g_l is of the form:

if l is even then

$$g_{l,W}=\sum_{i<j}[a_{I_i},a_{I_j}\frac{u_j^2}{(\pi')^l}]_W+\sum_{i<j}[a_{I_i}\frac{1}{\pi'},a_{I_j}\frac{v_j^2}{(\pi')^{l-1}}]_W,$$

where $u_i,v_j\in E'$;

if l is odd then

$$g_{l,W}=\sum_{i,j=1}^{2^{n-1}}[a_{I_i},a_{I_j}\frac{u_j^2}{(\pi')^l}]_W$$

where $u_j\in E'$.

We claim that $n=0$. Indeed, if $n\neq 0$ then substituting $\pi'=v^2\pi^e$ in the above expressions for g_i and writing v^{-2n} in the form

$$v^{-2n}=w_0^2+w_1^2\pi^2+w_2^2\pi^4+\cdots$$

where $w_i\in E$, we easily obtain that the highest term in the decomposition of $g_{\widehat{K},W}$ as a sum of its homogeneous components (with respect to presentation $\widehat{K}=E((\pi))$) has degree ne which is impossible because $g_{\widehat{K},W}=f_{\widehat{K},W}$.

Thus $n=0$ and hence g_W is of the form

$$g_W=\sum_{i<j}[a_{I_i},u_j^2a_{I_j}]_W+\sum_{i<j}[a_{I_i}(\pi')^{-1},v_j^2a_{I_j}\pi']_W,$$

where $u_i, v_j \in E'$. It follows that the first residue of g_W(and hence of f_W) lives in a subfield $E' \subset \overline{K} = E$ of transcendence degree $n-1$ over k which contradicts the induction assumption. This completes the proof of incompressibility of f.

13. Orthogonal and special orthogonal groups

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

Orthogonal groups. It is well known (see [KMRT, §29.E]) that if $n = 2r$ is even then there exists a natural bijection between $H^1(F, \mathbf{O}(V, g))$ and the set of isometry classes of n-dimensional non-degenerate quadratic spaces (V', g'). Similarly, if $n = 2r+1$ is odd then $H^1(F, \mathbf{O}(V, g))$ is in one-to-one correspondence with the set of isometry classes of $(2r+1)$-dimensional non-degenerate quadratic spaces (V', q') over F such that $\operatorname{disc}(q') = 1$. 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 $\operatorname{ed}(\mathbf{O}(V, g)) \geq r+1$. What is left to finish the proof of Theorem 2.2 for orthogonal groups is to find a "good" upper bound.

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

Proof. It suffices to show that any $2r$-dimensional non-degenerate quadratic form depends on at most $2r$ parameters. Let h be such form over F. 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 $H \hookrightarrow \mathbf{G}_{a,k}$, which exists because k is infinite. The exact sequence

$$0 \longrightarrow H \longrightarrow \mathbf{G}_{a,k} \xrightarrow{\phi} \mathbf{G}_{a,k} \longrightarrow 0$$

gives rise to

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

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 $r+1$. $\square$

13.2. **Remark.** Note that if h has trivial Arf invariant then taking a suitable quadratic subextension of $k(a, a_1, \dots, a_r)$ in F, if necessary, we may also assume that h' has trivial Arf invariant. Thus, our argument for finding a lower bound of the essential dimension of can be applied to special orthogonal groups as well.

Special orthogonal groups. By [KMRT, §29.E]), if $n = 2r$ is even then there exists a natural bijection between $H^1(F, \mathbf{SO}(V, g))$ and the set of isometry classes of $(2r)$-dimensional non-degenerate quadratic spaces (V', g') over F such that the Arf invariant of g' is trivial. Taking into consideration Remark 13.2 it follows that the proof of Theorem 2.2 for special orthogonal groups in even dimensional case is similar to that of for orthogonal groups.

Let $n = 2r+1$ be odd. Then there exists a natural bijection between $H^1(F, \mathbf{SO}(V, g))$ and the set of isometry classes of $(2r+1)$-dimensional non-degenerate 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 $\mathrm{ed}(\mathbf{SO}(V, g)) \leq r + 1$.

To find a "good" lower bound we recall that $\mathbf{SO}_{2r+1}(g) = \mathbf{O}_{2r+1}(g)_{red}$, the reduced subscheme of $\mathbf{O}_{2r+1}(g)$. Thus we have a natural closed embedding $\mathbf{SO}_{2r+1}(g) \hookrightarrow \mathbf{O}_{2r+1}(g)$. 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 $\phi_1 : \mathbf{O}_{2r}(h) \hookrightarrow \mathbf{SO}_{2r+1}(g)$ (because $\mathbf{O}_{2r}(h)$ 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

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

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

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

and

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

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

13.3. **Theorem.** *Let g be a non-degenerate quadratic form of dimension $2r + 1$ over k. Then* $\mathrm{ed}\,(\mathbf{SO}_{2r+1})(g) \geq r + 1$.

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 claim 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 $\operatorname{ed}(\mathbf{SO}_{2r+1}(g)) \geq r+1$. □

14. Proof of Theorem 3.1

Types $A_r, B_r, C_r, D_r, E_6, E_7, E_8$. Let $\rho : G^\circ \to \mathbf{O}(V, q)$ be as in Proposition 6.1. As in [ChSe], we can extend it to $\rho_G : G \to \mathbf{O}(V, q)$. Let $\theta_O = \rho_G(\theta_G)$ be the image of θ_G in $H^1(K, \mathbf{O}(V, q))$. Consider the quadratic form q_O on V corresponding to θ_O. If $\dim(q)$ is even then arguing as in [ChSe] 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 non-degenerate quadratic form of even dimension. The twist q_O of q by θ_O is of the form $q_O = \langle 1 \rangle \oplus g$ where g is a canonical monomial form of rank r. Then the proof of Theorem 13.3 shows that q_O is incompressible as well.

Type G_2. Let F be a field of an arbitrary characteristic. By [Se, 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 $\operatorname{ed}(G_2) \leq 3$. Conversely, a generic 3-fold Pfister form is a canonical monomial form of rank 2, hence incompressible. It follows $\operatorname{ed}(G_2) \geq 3$.

Type F_4. Let F be a field of an arbitrary characteristic. It is known that there is a canonical one-two-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 $f_5(J)$ [Pe, 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 $\operatorname{ed}(F_4) \geq 5$.

References

[Ar1] J. Arason, *Generators and relations for $W_q(K((S)))$ in characteristic 2*, Preprint, RH-19-2006 Science Institute University of Iceland Dunhaga 3, IS 107 Reykjavik.

[Ar2] J. Arason, *Generators and relations for $W_q(K)$ in characteristic 2*, Preprint, RH-18-2006 Science Institute University of Iceland Dunhaga 3, IS 107 Reykjavik.

[BF] G. Berhuy, G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Documenta Mathematica **8** (2003), 279-330.

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

[ChSe] V. Chernousov, J.-P. Serre, *Lower bounds for essential dimensions via orthogonal representations*, Journal of Algebra, 305 (2006), no. 2, 1055-1070.

[DG] M. Demazure and A. Grothendieck, *Structure des Schémas en Groupes Réductifs*, SGA 3 III, LN 153, Springer-Verlag, 1970.

[Ei] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer, 1994.

[EKM] R. Elman, N. Karpenko, A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society, 2008.

[GN] B. H. Gross and G. Nebe, *Globally maximal arithmetic groups*, J. Algebra **272** (2004), 625-642.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, American Mathematical Society, USA, 1998.

[Ma] A.L. Malagon, *Killing forms of Lie algebras*, PhD Dissertation at Emory University, 2009.

[Me] A. Merkurjev, *Essential dimension: a survey*, Transformation groups, **18** (2013), no. 2, 415-481.

[Pe] H. P. Petersson, *Structure theorems for Jordan algebras of degree* 3 *over fields of arbitrary characteristic*, Comm. in Algebra **32** (2004), no. 3, 1019-1049.

[Re] Z. Reichstein, *Essential dimension*, Proceedings of the International Congress of Mathematicians, Hyderabad, India, 2010.

[Sel] G. B. Seligman, *Some remarks on classical Lie algebras*, J.Math. Mech. **6** (1957), 549-558.

[Se] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, Séminaire Bourbaki 1993/94, no. 783, Astérisque **227** (1995), 229-257.

[SpSt] T.A. Springer, R. Steinberg, *Conjugacy Classes*, Lecture Notes in Mathematics **131**, 167-266, Springer-Verlag, New York, 1970.

[St] R. Steinberg, *Lectures on Chevalley groups*, Yale University lecture notes, 1967.

Department of Mathematics, University of Alberta, Edmonton, Alberta T6G 2G1, Canada

E-mail address: `ababic@ualberta.ca`

Department of Mathematics, University of Alberta, Edmonton, Alberta T6G 2G1, Canada

E-mail address: `chernous@math.ualberta.ca`