Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Linear Algebra and its Applications 395 (2005) 163–174
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

Siegel transformations for even characteristic

Erich W. Ellers [a,*], Oliver Villa [b]

[a] *Department of Mathematics, University of Toronto, 100 St. George Street, Toronto, Ont., Canada M5S 3G3*
[b] *Department of Mathematics, University College Dublin, Belfield, Dublin 4, Ireland*

Received 27 January 2004; accepted 3 August 2004

Submitted by R.A. Brualdi

Abstract

Let V be a vector space over a field K of even characteristic and $|K| > 3$. Suppose K is perfect and π is an element in the special orthogonal group $SO(V)$ with $\dim B(\pi) = 2d$. Then $\pi = \rho_1 \cdots \rho_{d-1}\kappa$, where ρ_j, $j = 1, \ldots, d-1$, are Siegel transformations and $\kappa \in SO(V)$ with $\dim B(\kappa) = 2$. The length of π with respect to the Siegel transformations is d if π is unipotent or if $\dim B(\pi)/\mathrm{rad}\, B(\pi) \geqslant 4$; otherwise it is $d+1$.

AMS classification: 15A23; 20H20; 51F25; 51N30

Keywords: Factorization; Siegel transformation; Orthogonal group; Quadratic form; Singular vector

1. Introduction

Let G be a group and let S be a set of generators for G. Let π be an element in G, then $\pi = s_1 \cdots s_k$, where all s_j, $j = 1, \ldots, k$, are elements in S. The *length* $\ell(\pi)$ of π with respect to S is the minimal k for which such a factorization exists. For certain groups G and certain generating systems S it is possible to determine $\ell(\pi)$ for each π in G.

* Corresponding author. Tel.: +1 416 978 3462; fax: +1 416 978 4107.
E-mail addresses: ellers@math.toronto.edu (E.W. Ellers), oliver.villa@ucd.ie (O. Villa).

0024-3795/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2004.08.002

Bachmann [1] coined the phrase *length problem* for the program described above. The length problem for the orthogonal groups over fields of characteristic not 2 was solved by Scherk [12]. Further, Dieudonné [3] solved the length problem for several other classical groups. For more references see e.g. Ellers [4,5].

If Q is a nondegenerate singular quadratic form on a vector space V over a field K, then the commutator subgroup $G = \Omega(V)$ of $O(V)$ is generated by the set of Siegel transformations. Assuming that the field K of coefficients has characteristic not 2, Knüppel solved the length problem for $G = \Omega(V)$, where the generating set S is the set of Siegel transformations [10]. In the present paper, we assume that the characteristic of K is even, $|K| > 3$, and K is perfect. Under these conditions we solve the length problem for $\Omega(V)$ with respect to Siegel transformations.

In Section 3, we are laying the groundwork. Here we assume that V is nonsingular and that V contains singular vectors distinct from zero. We see that some of the properties established in [10] for orthogonal groups over fields K of characteristic not 2 are also valid when the characteristic of K is even.

In Section 4, we establish a lower bound for the Siegel length of an isometry. In Section 5, we assume that K is perfect, and we determine the Siegel length of an isometry π, Theorem 5.5. Here our approach differs entirely from that in [10]. Our tools include the factorization of an orthogonal transformation π into a product of two involutions [6,7] and also the factorization of π into a product $\pi = \mu \cdot \nu$, where μ is unipotent and the path of ν is nonsingular [8].

2. Notation

Let V be a vector space of dimension n over a field K where $|K| > 2$, equipped with a *quadratic form* Q (see [2–§16]), defined by $Q(\alpha v) = \alpha^2 Q(v)$ and $Q(v + w) = Q(v) + Q(w) + f(v, w)$ for some bilinear form f, where $\alpha \in K$ and $v, w \in V$. Two vectors $v, w \in V$ are called *perpendicular*, $v \perp w$, if $f(v, w) = 0$. A vector $v \in V$ is called *isotropic* if $f(v, v) = 0$ and *singular* if $Q(v) = 0$. Let W be a subspace of V. Then W is called *totally isotropic* if $f(u, w) = 0$ for all $u, w \in W$ and *totally singular* if $Q(w) = 0$ for all $w \in W$. A totally singular subspace is also totally isotropic, but the converse is not necessarily true. The subspaces $\operatorname{rad} W = W \cap W^{\perp}$ and $SW = \{x \in \operatorname{rad} W \mid Q(x) = 0\}$ are called the *radical* of W and the *singular* of W, respectively. The space W is said to be *nonsingular* if $\operatorname{rad} W = 0$.

The orthogonal group on V, denoted $O(V)$, is the set of isometries, i.e. of all transformations that preserve the value of Q. For $\pi \in O(V)$ we define $B(\pi) := V(\pi - 1)$ and $F(\pi) := \ker(\pi - 1)$. The subspaces $B(\pi)$ and $F(\pi)$ of V are called *path* and *fixed space* of π, respectively.

We shall always assume that V is nonsingular and that there is at least one $v \in V \setminus \{0\}$ such that $Q(v) = 0$.

We shall state a number of facts (see e.g. [13]).

The transformation π is an element in the *special orthogonal group* $SO(V)$ if $\pi \in O(V)$ and $\dim B(\pi)$ is even.

Let $z \in V$ with $Q(z) \neq 0$. Then σ_z denotes the reflection in $z^\perp$, i.e.,

$$\sigma_z : V \to V : x \to x - \frac{f(x,z)}{Q(z)} z.$$

Let $\pi \in O(V)$ and $K \neq F_2$, then $\pi = \sigma_1 \cdots \sigma_k$, where σ_j is a reflection for $j = 1, \ldots, k$, and $k = \dim B(\pi)$ or $k = \dim B(\pi) + 2$.

Let σ_u be the reflection in $u^\perp$, where $u \in V$. The *spinorial norm* $\Theta(\sigma_u) = Q(u) \cdot K^{\star 2}$.

If $\pi \in O(V)$, then $\pi = \sigma_1 \cdots \sigma_k$ and $\Theta(\pi) = \Theta(\sigma_1) \cdots \Theta(\sigma_k) \cdot K^{\star 2}$.

Assume $\dim V \geqslant 2$. If V contains singular vectors distinct from zero, then $\Omega(V) = \{\pi \in SO(V) \mid \Theta(\pi) = K^{\star 2}\}$.

If $K = K^2$, then $\Omega(V) = SO(V)$.

3. Siegel transformations

We shall give the definition of a Siegel transformation and also collect a number of properties for Siegel transformations and their products (see [13,8]). In [8], Siegel transformations are called Eichler transformations.

Let $i, w \in V \setminus \{0\}$. If i is singular and $w \in i^\perp$, then

$$\rho_{i,w} : V \to V : x \to x + f(x,w)i - f(x,i)w - Q(w)f(x,i)i$$

is a *Siegel transformation*.

Clearly, $B(\rho_{i,w}) = \langle i, w\rangle$ with $i \in B(\rho_{i,w}) \cap F(\rho_{i,w})$. If w is isotropic, then $B(\rho_{i,w}) \subset F(\rho_{i,w})$. If $w \in \langle i\rangle$, then $\rho_{i,w} = I$; if $w \notin \langle i\rangle$, then $\dim B(\rho_{i,w}) = 2$.

If i is singular, $w, w_1, w_2 \in i^\perp$, and $\pi \in O(V)$, then $\rho_{\alpha i,w} = \rho_{i,\alpha w}$, $\rho_{i,w_1+w_2} = \rho_{i,w_1}\rho_{i,w_2}$, and $\pi^{-1}\rho_{i,w}\pi = \rho_{i\pi,w\pi}$.

The space (V, Q) is spanned by its nonsingular vectors.

If i is singular and $w \in i^\perp$ is nonsingular, then the Siegel transformation $\rho_{i,w}$ is a product of two reflections,

$$\rho_{i,w} = \sigma_{Q(w)i-w}\sigma_w.$$

All Siegel transformations belong to the commutator subgroup $\Omega(V)$ of $O(V)$.

If $\dim V \geqslant 3$, $\operatorname{rad} V = 0$, and if V contains singular vectors, then $\Omega(V)$ is generated by the Siegel transformations of V.

If $\rho_{i,w}$ is a Siegel transformation, then $(\rho_{i,w} - 1)^3 = 0$; if w is isotropic, then $(\rho_{i,w} - 1)^2 = 0$ and therefore $B(\rho_{i,w}) \subset F(\rho_{i,w})$ (see [10]).

Lemma 3.1. *Let π be an isometry of (V, Q). Let $u, v \in V$ and $i = u(\pi - 1)$.*

(1) *Then $Q(i) = -f(i,u)$.*
(2) *If $w = v(\pi - 1)$ and $f(i,w) = 0$, then $f(u,w) = -f(i,v)$.*

Proof.
(1) $Q(i) = Q(u\pi - u) = 2Q(u) - f(u\pi, u) = f(u, u) - f(u\pi, u) = -f(i, u)$;
(2) $f(i, v) = f(i, v\pi - w) = f(i, v\pi) = f(u\pi - u, v\pi)$
$= f(u, v) - f(u, v\pi) = -f(u, w)$. □

Lemma 3.2 (see [10, Lemma 3.14] for char $K \neq 2$). *Let π be an isometry of (V, Q). Let $u, v \in V$ and $i = u(\pi - 1)$, $w = v(\pi - 1)$. Assume $Q(i) = 0 = f(i, w)$ and $f(u, w) = -1$.*

Then $i \neq 0$, the Siegel transformation $\rho_{i,w}$ exists,

$F(\pi\rho_{i,w}) = F(\pi) \oplus Ku \oplus Kv$, and $B(\pi\rho_{i,w}) \subset B(\pi)$; in particular, $\dim B(\pi\rho_{i,w}) = \dim B(\pi) - 2$.

Proof. Clearly, $\rho_{i,w}$ exists and $B(\rho_{i,w}) \subset B(\pi)$. Therefore $F(\rho_{i,w}) = B(\rho_{i,w})^{\perp} \supset B(\pi)^{\perp} = F(\pi)$ and $F(\pi\rho_{i,w}) \supset F(\pi) \cap F(\rho_{i,w}) = F(\pi)$.

Clearly,

$$\begin{aligned}(u)\pi\rho_{i,w} &= (i + u)\rho_{i,w} = i + (u)\rho_{i,w} = i + u + f(u, w)i = u;\\ (v)\pi\rho_{i,w} &= (v)\pi + f((v)\pi, w)i - f((v)\pi, i)w - Q(w)f((v)\pi, i)i\\ &= v + w - f(v, i)w + \big(f(v, w) + f(w, w) - Q(w)f(v, i)\big)i\\ &= v - \big(f(v, w) + Q(w)\big)i = v.\end{aligned}$$

Thus $F(\pi\rho_{i,w}) \supset \langle u, v\rangle$, $\langle u, v\rangle \cap i^{\perp} = \langle u\rangle$, and $i \in B(\pi)$, so $i^{\perp} \supset B(\pi)^{\perp} = F(\pi)$ and $u \notin F(\pi)$ since $f(i, v) = 1$. Thus if $v \in Ku + F(\pi)$, then $v \in i^{\perp}$, a contradiction. □

Lemma 3.3. *Let $W < V$ such that $SW = 0$. If W contains nontrivial singular vectors, then there is a basis of singular vectors for W.*

Proof. Let $z \in W$ with $z \neq 0$ and $Q(z) = 0$. Then $z \notin \operatorname{rad} W$ since $SW = 0$. Clearly, $z^{\perp} \cap W$ is a hyperplane of W. Extend z to a basis T for W by vectors in $W \setminus z^{\perp}$.

Let $t_j \in T \setminus \{z\}$, then $\alpha_j z + t_j$ is singular for some $\alpha_j \in K$, $j = 1, \ldots, n - 1$. Further, $\{z\} \cup \{\alpha_j z + t_j \mid t_j \in T \setminus \{z\}\}$ is a basis of singular vectors for W. □

Lemma 3.4 (see [9, Lemma 3.5] for char $K \neq 2$). *Let $W < V$ be a nonsingular orthogonal subspace of V containing nontrivial singular vectors. Assume* char $K =$ 2, $\dim W > 3$, *and let $H \subset W$ be a hyperplane of W. If $\psi \in O(W, Q)$ and $J\psi = J$ for each singular 1-dimensional subspace J of W which is not contained in H, then $\psi = 1_W$.*

Proof. By Lemma 3.3 the space W has a basis of singular vectors.

First, let $Z < W$ such that $\dim Z = 3$, Z contains nontrivial singular vectors but no 2-dimensional totally singular subspace, $SZ = 0$, and $Z \not\subset H$. Then $\psi|_Z = 1_Z$.

Indeed, by Lemma 3.3 there is a basis $\{a, b, c\}$ of singular vectors for Z. We show that the subspace Z contains at least $|K| + 1$ 1-dimensional singular subspaces. Observe that $\langle b, c\rangle \neq a^\perp \cap Z$, otherwise $\langle a, b\rangle$ would be a 2-dimensional totally singular subspace of Z. Let $\langle d\rangle \subset \langle b, c\rangle$ and, if $Q(d) \neq 0$, let $Q(a + \delta d) = \delta^2 Q(d) + \delta f(a, d) = 0$ for some $\delta \in K$. Here $\delta = 0$ occurs for only one subspace $\langle d\rangle \subset \langle b, c\rangle$ and there are $|K| + 1$ subspaces $\langle d\rangle \subset \langle b, c\rangle$. At most two of the $|K| + 1$ singular subspaces lie in H (indeed, suppose $\langle x\rangle, \langle y\rangle \subset H$ and $\langle x + y\rangle$ are singular; if $\langle x\rangle \neq \langle y\rangle$, then $H \cap Z$ is totally singular and 2-dimensional). Hence we may assume $a, b, c \notin H$. Now $\langle a, b\rangle$, $\langle b, c\rangle$, $\langle c, a\rangle$ are hyperbolic planes whose 1-dimensional singular subspaces are ψ-invariant. Hence $a\psi = \lambda a$, $b\psi = \lambda^{-1} b$, $c\psi = \lambda c$, $a\psi = \lambda^{-1} a$ for some $\lambda \in K^\star$. Clearly $\lambda^2 = 1$, so $\lambda = 1$.

Second, each singular vector $x \in W$ satisfies $x\psi = x$.

Indeed, let $x \in W$, $x \neq 0$, be singular. Select $y \in W \setminus (x^\perp \cup H)$. Then $T := \langle x, y\rangle$ is a hyperbolic plane. Choose some nonsingular $z \in T^\perp \cap W$. Let $Z := \langle x, y, z\rangle$. Then $\operatorname{rad} Z = Kz$ and $SZ = 0$. Thus Z fulfills the requirements of our first statement and the assertion follows. □

The following two lemmas are key tools in Section 5, where we determine the Siegel length of an orthogonal transformation.

Lemma 3.5. *Let π be an isometry of (V, Q) and $Q(i) = 0$, where $i = u\pi - u$ for some $u \in V \setminus F(\pi)$.*

Then there is some $w \in B(\pi)$ such that $f(u, w) = -1$.

If in addition $w \in i^\perp$, in particular if $i \in \operatorname{rad} B(\pi)$, i.e. $i \in SB(\pi)$, then a Siegel transformation $\rho_{i,w}$ exists with

$$B(\rho_{i,w}) \subset B(\pi) \text{ and } \dim B(\pi\rho_{i,w}) = \dim B(\pi) - 2.$$

Proof. Suppose $f(u, w) = 0$ for all $w \in B(\pi)$, then $u \in B(\pi)^\perp = F(\pi)$, contradicting our assumption. Thus $f(u, w) = -1$ for some $w \in B(\pi)$. If $i \in \operatorname{rad} B(\pi)$, then $f(i, w) = 0$, proving the existence of $\rho_{i,w}$. □

Lemma 3.6. *Let (V, Q) be an orthogonal space. Assume* $\operatorname{char} K = 2$, $|K| > 3$. *Let $\pi \in O(V, Q)$ and $Q(i) = 0$, where $i = u\pi - u$ for some $u \in V \setminus F(\pi)$ and $i \notin \operatorname{rad} B(\pi)$. Suppose* $\dim\big(B(\pi)/SB(\pi)\big) \geqslant 3$.

Then there is some nonsingular vector $w \in B(\pi) \cap i^\perp$ and a Siegel transformation $\rho_{i,w}$ exists with $B(\rho_{i,w}) \subset B(\pi)$ and $\dim B(\pi\rho_{i,w}) = \dim B(\pi) - 2$.

Proof. Take the vector u as assumed. Suppose $f(w, u) = 0$ for all nonsingular $w \in B(\pi) \cap i^\perp$. Then $u \in (B(\pi) \cap i^\perp)^\perp = F(\pi) + Ki$ and thus $u = \alpha i + b$, where $b \in F(\pi)$ and $\alpha \neq 0$ since $u \notin F(\pi)$. Therefore $i = u\pi - u = \alpha(i\pi - i)$ and finally $i\pi = (1 + \alpha^{-1})i$ which implies $Ki\pi = Ki$ for all singular vectors $i \in B(\pi) \setminus \operatorname{rad} B(\pi)$. Let $B(\pi) = W \oplus \operatorname{rad} B(\pi)$, where $i \in W$ for some $i \notin \operatorname{rad} B(\pi)$. Then

Lemma 3.4 yields $\pi|_W = 1$, because $\dim W > 3$. Since $\operatorname{rad} B(\pi) \subset F(\pi)$, this implies $B(\pi) \subset F(\pi)$, contradicting $i \notin \operatorname{rad} B(\pi)$. □

Let π and κ be linear transformations. Then $B(\pi) \cap B(\kappa) = \{0\}$ implies $F(\pi\kappa) = F(\pi) \cap F(\kappa)$ and $F(\pi) + F(\kappa) = V$ implies $B(\pi\kappa) = B(\pi) + B(\kappa)$.

Lemma 3.7. *If the isometry π is a product of Siegel transformations, then* $\dim B(\pi)$ *is even.*

Proof. The Theorems 11.41(i) and 11.44 in [13] yield the result. □

Lemma 3.8 (see [10, Lemma 3.11] for char $K \neq 2$). *Let π be a product of Siegel transformations and let ρ be a Siegel transformation.*

If $\dim(B(\pi) \cap B(\rho)) = 1$, *then* $\dim B(\pi) = \dim B(\pi\rho)$.

Proof. Put $\kappa = \pi\rho$. Evidently, $B(\kappa) \subset B(\pi) + B(\rho)$ and $B(\pi) \subset B(\kappa) + B(\rho)$, thus $B(\kappa) + B(\rho) = B(\pi) + B(\rho)$.

The dimension theorem yields

$$\begin{aligned}\dim B(\kappa) - \dim B(\pi) &= \dim(B(\kappa) \cap B(\rho)) - \dim(B(\pi) \cap B(\rho)) \\ &= \dim(B(\kappa) \cap B(\rho)) - 1.\end{aligned}$$

The left-hand side is even and less than two, so it is zero. □

A transformation π in $GL(V)$ is called *unipotent* if $(\pi - 1)^m = 0$ for some $m \in \mathbb{N}$.

Lemma 3.9 (see [10, Lemma 4.1] for char $K \neq 2$). *Let $\rho = \rho_{i,w}$ be a Siegel transformation. (This implies that i is singular.) If $\pi \in O(V)$ such that $B(\rho) \subset B(\pi)$ and $i \in F(\pi)$, then*

$$(\pi\rho - 1)^j = (\pi - 1)^{j-1}(\pi\rho - 1) \quad \textit{for all } j \in \mathbb{N}.$$

Further, if π is unipotent, then $\pi\rho$ is unipotent.

The proof in [10] is still valid if char $K = 2$.

Lemma 3.10 (see [11, p. 198, Theorem]). *Let $\pi \in O(V)$ and $\pi^2 \neq 1$. Then there are involutions π_1 and π_2 in $O(V)$ such that $\pi = \pi_1\pi_2$ and $B(\pi) = B(\pi_1) + B(\pi_2)$.*

Proof. The existence of π_1 and π_2 was shown in [7]. It remains to be seen that the mappings π_1 and π_2 that were given in [7], satisfy $B(\pi_1), B(\pi_2) \subset B(\pi)$.

Let V be an n-dimensional vector space ($n \geqslant 1$) over a field K. Assume V is π-cyclic for some $\pi \in O(V)$ and u is a generator of V. Then $\{u, u\pi, \ldots, u\pi^{n-1}\}$ is a basis for V.

We define orthogonal mappings π_1 and π_2 by

$$u\pi^j\pi_1 = u\pi^{n-j} \quad \text{and} \quad u\pi^j\pi_2 = u\pi^{n+1-j} \quad \text{for } j = 0, \ldots, n-1.$$

Clearly,

$$B(\pi_1) = \langle u(\pi^{n-j} - \pi^j);\ j = 0, \ldots, m-1 \rangle \quad \text{if } n = 2m \text{ and}$$
$$B(\pi_1) = \langle u(\pi^{n-j} - \pi^j);\ j = 0, \ldots, m \rangle \quad \text{if } n = 2m+1,$$
$$B(\pi_2) = \langle u(\pi^{n+1-j} - \pi^j);\ j = 0, \ldots, m \rangle.$$

Let $k = n$ or $n+1$. Then

$$\begin{aligned} u(\pi^{k-j} - \pi^j) &= u\pi^j(\pi^{k-2j} - 1) \\ &= u\pi^j(\pi^{k-2j-1} + \cdots + \pi + 1)(\pi - 1) \in B(\pi). \end{aligned}$$

Thus $B(\pi_1), B(\pi_2) \subset B(\pi)$. Since $B(\pi) = B(\pi_1\pi_2) \subset B(\pi_1) + B(\pi_2)$, we get $B(\pi) = B(\pi_1) + B(\pi_2)$. □

Lemma 3.11. *Let* $\pi \in O(V)$, $\operatorname{char} K = 2$, *and* $\operatorname{rad} B(\pi) = 0$. *If* $\pi = \pi_1\pi_2$ *with* $B(\pi) = B(\pi_1) + B(\pi_2)$, *where* π_j *are involutions in* $O(V)$, *then* $B(\pi_1) \cap B(\pi_2) = 0$.

Proof. Clearly, $B(\pi_1) \cap B(\pi_2) \subset F(\pi_1) \cap F(\pi_2) \subset F(\pi_1\pi_2) = F(\pi)$ and $B(\pi_1) \cap B(\pi_2) \subset B(\pi)$. Thus $B(\pi_1) \cap B(\pi_2) = 0$. □

4. Factorization

We are going to establish a lower bound for the Siegel length of any isometry in $SO(V)$.

Definition 4.1. Let $\pi \in SO(V)$. Suppose there are Siegel transformations $\rho_i \in SO(V)$ such that $\pi = \rho_1 \cdots \rho_m$. Then the minimal m is the *length of* $\boldsymbol{\pi}$ and we write $m = \ell(\pi)$.

Proposition 4.2. *Let* $\pi \in SO(V)$. *If* $\pi = \rho_1 \cdots \rho_k$, *where each* ρ_j *is a Siegel transformation*, *and* $\dim B(\pi) = 2k$, *then* $B(\pi)$ *contains nontrivial singular vectors*. *Furthermore*, $\dim(B(\pi)/\operatorname{rad} B(\pi)) \geqslant 4$ *or* π *is unipotent*.

Proof. Let $\pi \in SO(V)$. Assume $\pi = \rho_1 \cdots \rho_k$, where all ρ_j are Siegel transformations and $\dim B(\pi) = 2k$.

Put $\overline{B(\pi)} = B(\pi)/SB(\pi) = \{b + SB(\pi) \mid b \in B(\pi)\}$.

Put $\overline{b} = b + SB(\pi)$. Clearly, $\overline{B(\pi)}$ is an orthogonal vector space with $Q(\overline{b}) = Q(b)$ for all $b \in B(\pi)$. Now

$$\begin{aligned}
\operatorname{rad} \overline{B(\pi)} &= \{\overline{c} \in \overline{B(\pi)} \mid f(\overline{c}, \overline{B(\pi)}) = 0\} \\
&= \{\overline{c} \in \overline{B(\pi)} \mid f(c, B(\pi)) = 0\} \\
&= \{\overline{c} \in \overline{B(\pi)} \mid c \in B(\pi) \cap B(\pi)^{\perp}\} \\
&= \{\overline{c} \in \overline{B(\pi)} \mid c \in \operatorname{rad} B(\pi)\} \\
&= \{\overline{c} \in \overline{B(\pi)} \mid \overline{c} \in (\operatorname{rad} B(\pi))/SB(\pi)\} \\
&= \overline{\operatorname{rad} B(\pi)}.
\end{aligned}$$

Thus $\overline{B(\pi)}/\operatorname{rad} \overline{B(\pi)} \cong \overline{B(\pi)}/\overline{\operatorname{rad} B(\pi)} \cong B(\pi)/\operatorname{rad} B(\pi)$ and $S\overline{B(\pi)} = \overline{SB(\pi)} = 0$.

The isometries π and ρ_j leave $B(\pi)$, $\operatorname{rad} B(\pi)$, and $SB(\pi)$ invariant.

Define $(b + SB(\pi))\overline{\pi} = b\pi + SB(\pi)$ and $(b + SB(\pi))\overline{\rho_j} = b\rho_j + SB(\pi)$. Then $\overline{\pi}$ and $\overline{\rho}_j$ are orthogonal transformations on $\overline{B(\pi)}$.

Also, $B(\overline{\rho}_j) \cap \operatorname{rad} \overline{B(\pi)} = B(\overline{\rho}_j) \cap \overline{SB(\pi)} = 0$ by [4–Lemma 3].

Further, $\overline{\rho}_j$ is an involution and thus $B(\overline{\rho}_j)$ is totally isotropic.

If $\dim B(\overline{\rho}_j) = 2$ for some j, then $\dim \overline{B(\pi)}/\operatorname{rad} \overline{B(\pi)} \geqslant 4$.

Now assume $\overline{\rho}_j$ is simple for all j, i.e., $\dim B(\overline{\rho}_j) = 1$.

Then $\overline{\rho}_j$ is a reflection by [4–Lemma 5]. So $B(\overline{\rho}_j)$ is not singular.

Therefore $B(\rho_j)$ contains a nonsingular vector. By Lemma 3.5, there is some $w \in B(\rho_j)$ such that $\rho_j = \rho_{i,w}$, where $Q(w) \neq 0$; and $\rho_{i,w} = \sigma_{Q(w)i-w}\sigma_w$ is a product of two reflections. Clearly, $B(\rho_{i,w}) = B(\sigma_{Q(w)i-w}) \oplus B(\sigma_w)$. So both reflections leave $B(\pi)$, $\operatorname{rad} B(\pi)$, and $SB(\pi)$ invariant. If $\dim B(\overline{\rho}_{i,w}) = 1$, then $B(\overline{\sigma}_{Q(w)i-w}) = B(\overline{\sigma}_w)$ and therefore $\overline{\sigma}_{Q(w)i-w} = \overline{\sigma}_w$ and so $\overline{\rho}_{i,w} = 1$.

This implies $\overline{\pi} = 1$. Consequently, $b\pi + SB(\pi) = b + SB(\pi)$ for all $b \in B(\pi)$. Equivalently, $b\pi - b \in SB(\pi)$ for all $b \in B(\pi)$.

Therefore, $B(\pi)^{\pi-1} \subset SB(\pi)$ and $B(\pi)^{(\pi-1)(\pi-1)} = 0$, i.e., $V^{(\pi-1)^3} = 0$, so π is unipotent. □

5. Length theorems

From now on we shall assume that $\operatorname{char} K = 2$, $|K| > 3$, and K is perfect (hence $K^2 = K$). We shall determine the Siegel length of any isometry π in $SO(V)$.

Let $\{a, b\} \subset V$ be an independent set such that $a \in b^{\perp}$ and $Q(b) \neq 0$. Then $Q(a + \beta b) = Q(a) + \beta^2 Q(b) = 0$ for some suitable element $\beta \in K$.

If W is an at least 2-dimensional totally isotropic subspace of V, then $Q(w) = 0$ for some $w \in W \setminus \{0\}$. For any isometry π in $SO(V)$, the dimension of $\operatorname{rad} B(\pi)$ is even. So, if the singular of $B(\pi)$ is zero, then $\operatorname{rad} B(\pi) = 0$.

Proposition 5.1. *Let $\pi \in SO(V)$ with $\dim B(\pi) = 2k \geqslant 4$.*

Then there are $k-1$ Siegel transformations ρ_r and $\kappa \in SO(V)$ with $\dim B(\kappa) = 2$ such that $\pi = \rho_1 \cdots \rho_{k-1}\kappa$.

Proof. If $\dim \operatorname{rad} B(\pi) \geqslant 2$, then there is a singular vector in $\operatorname{rad} B(\pi)$. By Lemma 3.5 there is a Siegel transformation ρ such that $\dim B(\pi\rho) = \dim B(\pi) - 2$.

If $\dim(B(\pi)/\operatorname{rad} B(\pi)) \geqslant 3$, then there is a singular vector in $B(\pi) \setminus \operatorname{rad} B(\pi)$. Now we can apply Lemma 3.6.

Induction yields the result. □

Assume $\pi \in O(V)$ is unipotent and $\pi \neq 1$, i.e., $(\pi - 1)^m = 0$ and $(\pi - 1)^{m-1} \neq 0$ for some $m > 1$. Then

$$\{0\} \neq V(\pi - 1)^{m-1} \subset F(\pi) \cap B(\pi) = \operatorname{rad} B(\pi).$$

Lemma 5.2. *Let $\pi \in SO(V)$ with $\dim B(\pi) = 2k$.*

If π is unipotent, then π is a product of k Siegel transformations ρ_r:

$$\pi = \rho_1 \cdots \rho_k.$$

Proof. Clearly, $B(\pi) = B \oplus \operatorname{rad} B(\pi)$, where B is nonsingular. If $\pi \neq 1$, then $\dim \operatorname{rad} B(\pi)$ is even and not zero. Therefore there is a singular vector in $\operatorname{rad} B(\pi)$. By Lemma 3.5 there is a Siegel transformation ρ such that $\dim B(\pi\rho) = \dim B(\pi) - 2$. Clearly $\dim F(\pi\rho) = \dim F(\pi) + 2 > 1$. Also, $\pi\rho$ is unipotent by Lemma 3.9. Now we can use induction. □

Lemma 5.3. *Suppose $\dim V \geqslant 4$. Let $\pi \in SO(V)$ with $\dim B(\pi) = 2$.*

If $\operatorname{rad} B(\pi) = B(\pi)$, then π is a Siegel transformation.

If $\operatorname{rad} B(\pi) = 0$, then π is not a Siegel transformation, but π is a product of two Siegel transformations.

Proof. The first assertion is a consequence of Lemma 3.5.

If $\operatorname{rad} B(\pi) = 0$, then π is obviously not a Siegel transformation.

Clearly there is some $w \in B(\pi)$ with $Q(w) \neq 0$. Put $\sigma = \sigma_w$. Then $\dim B(\pi\sigma) = 1$ [4–p. 106] and $B(\pi) = B(\pi\sigma) + B(\sigma)$. If $B(\sigma) \subset B(\pi\sigma)^\perp$, then $B(\sigma)^\perp \supset B(\pi\sigma)$, but $B(\sigma)^\perp \cap B(\pi) = B(\sigma)$, thus $B(\pi\sigma) = B(\sigma)$ which is not possible. So $B(\sigma) \not\subset B(\pi\sigma)^\perp$.

Since $\dim V \geqslant 4$, there is some $t \in w^\perp \setminus B(\pi\sigma)^\perp$ such that $Q(t) = 0$. Then $\dim\langle t, w\rangle = 2$. Since $B(\pi\sigma)^\perp$ is a hyperplane, there is some $\alpha \in K^\star$ such that

$Q(w)\alpha t - w \in B(\pi\sigma)^\perp$. Put $\alpha t = i$ and $\sigma_{Q(w)i-w} = \tau$. Then $B(\pi\sigma\tau) = B(\pi\sigma) + B(\tau)$ which is totally isotropic and $\dim B(\pi\sigma\tau) = 2$. Clearly, $\sigma\tau = \rho_{iw}$ and $\pi\sigma\tau = \rho$ are Siegel transformations. Thus $\pi = \rho\rho_{iw}$. □

An immediate consequence of Proposition 5.1 and Lemma 5.3 is that the Siegel length $\ell(\pi) \leqslant \frac{1}{2}\dim B(\pi) + 1$ for all transformations π in $SO(V)$.

In order to determine which transformations π can be expressed as a product of $\frac{1}{2}\dim B(\pi)$ Siegel transformations we need more detailed information. The result is stated in Theorem 5.5.

Theorem 5.4. *Let* $\pi \in SO(V)$. *If* $\dim B(\pi) \geqslant 4$ *and* $\operatorname{rad} B(\pi) = 0$, *then* $\ell(\pi) = \frac{1}{2}\dim B(\pi)$.

Proof. The Lemmas 3.10 and 3.11 yield $\pi = \pi_1\pi_2$, where $B(\pi) = B(\pi_1) \oplus B(\pi_2)$ and $\pi_1^2 = \pi_2^2 = 1$. If $\dim B(\pi_1)$ is even, then $\pi_1, \pi_2 \in SO(V)$. Since both π_1 and π_2 are unipotent, we have $\pi = \rho_1 \cdots \rho_k$, where $k = \frac{1}{2}\dim B(\pi)$.

Now we deal with the case where $\dim B(\pi_j)$ is odd for $j = 1, 2$. By [8–8.2.21], there is some nonsingular $v \in B(\pi_1)$, $v \neq 0$. Clearly, $\dim B(\pi_1\sigma_v) = \dim B(\pi_1) - 1$ is even and $\pi_1\sigma_v = \sigma_v\pi_1$ is an involution in $SO(V)$. If $B(\pi_2) \subset v^\perp$ for some nonsingular $v \in B(\pi_1)$, then $\pi_2\sigma_v = \sigma_v\pi_2$ is also an involution in $SO(V)$ and $\dim B(\pi_2\sigma_v) = \dim B(\pi_2) + 1$. Thus $\pi = \rho_1 \cdots \rho_k$, where $k = \frac{1}{2}\dim B(\pi)$.

If there is a nonsingular vector $w \in B(\pi_2) \cap v^\perp$, then $\sigma_w\pi_2 = \pi_2\sigma_w$ and $\dim B(\pi_2\sigma_w) = \dim B(\pi_2) - 1$. Also, $\sigma_v\sigma_w = \sigma_w\sigma_v$ is a Siegel transformation since $B(\sigma_v\sigma_w) = Kv + Kw \subset F(\sigma_v\sigma_w)$. Consequently, $\pi = (\pi_1\sigma_v)(\sigma_v\sigma_w)(\sigma_w\pi_2)$ is a product of three involutions and we get again $\ell(\pi) = \frac{1}{2}\dim B(\pi)$.

Now we assume that $v^\perp \cap B(\pi_2)$ is totally singular for all nonsingular $v \in B(\pi_1)$. Then $\dim(v^\perp \cap B(\pi_2)) = \dim B(\pi_2) - 1$ and $v^\perp \cap B(\pi_2)$ is the singular of $B(\pi_2)$. Also, we assume that $w^\perp \cap B(\pi_1)$ is totally singular for all nonsingular $w \in B(\pi_2)$. Then $\dim(w^\perp \cap B(\pi_1)) = \dim B(\pi_1) - 1$ and $w^\perp \cap B(\pi_1)$ is the singular of $B(\pi_1)$. Since $v^\perp \cap B(\pi_2) = SB(\pi_2) \subset B(\pi_2)$ for all nonsingular $v \in B(\pi_1)$, we get

$$(SB(\pi_2))^\perp = Kv + F(\pi_2) \supset F(\pi_2) \supset B(\pi_2).$$

There is a basis $\{v_1, \ldots, v_k\}$ for $B(\pi_1)$ consisting of nonsingular vectors v_j in $B(\pi_1)$. Therefore, $Kv_j + F(\pi_2) = Kv + F(\pi_2)$. This implies $B(\pi_1) = \langle v_1, \ldots, v_k\rangle \subset Kv + F(\pi_2) = (SB(\pi_2))^\perp$.

Thus $(SB(\pi_2))^\perp \supset B(\pi_1) \oplus B(\pi_2)$ and $SB(\pi_2) \subset F(\pi_1) \cap F(\pi_2)$.

Similarly, $SB(\pi_1) \subset F(\pi_1) \cap F(\pi_2)$, so

$$SB(\pi_1) \oplus SB(\pi_2) \subset F(\pi_1) \cap F(\pi_2) \subset F(\pi).$$

Clearly, $SB(\pi_1) \oplus SB(\pi_2) \subset B(\pi_1) \oplus B(\pi_2) = B(\pi)$.

Therefore, $SB(\pi_1) \oplus SB(\pi_2) \subset B(\pi) \cap F(\pi) = \operatorname{rad} B(\pi)$.

Thus $\dim \operatorname{rad} B(\pi) \geqslant \dim B(\pi) - 2 \geqslant 2$, contradicting our assumption. □

Theorem 5.5. *Let $\pi \in SO(V)$. If π is unipotent or if* $\dim B(\pi)/\operatorname{rad} B(\pi) \geqslant 4$, *then* $\ell(\pi) = \frac{1}{2}\dim B(\pi)$. *Otherwise* $\ell(\pi) = \frac{1}{2}\dim B(\pi) + 1$.

Proof. By Proposition 5.1 and Lemma 5.3 we know that $\ell(\pi) \leqslant \frac{1}{2}\dim B(\pi) + 1$.

If $\ell(\pi) = \frac{1}{2}\dim B(\pi)$, then either π is unipotent or $\dim B(\pi)/\operatorname{rad} B(\pi) \geqslant 4$ according to Proposition 4.2.

Now we show that a factorization as claimed is possible:

Since $\pi \in SO(V)$, we get $\pi = \mu\nu$, where $\mu, \nu \in O(V)$, $B(\pi) = B(\mu) \oplus B(\nu)$, where μ is unipotent, $\operatorname{rad} B(\nu) = 0$, and $B(\mu) \perp B(\nu)$ (see [8–6.2.2]). Clearly, $\dim B(\nu)$ is even, so $\mu, \nu \in SO(V)$.

If $\dim B(\nu) = 0$, then π is unipotent and our result follows from Lemma 5.2.

If $\dim B(\nu) \geqslant 4$, then Lemma 5.2 and Theorem 5.4 yield the desired result.

Now we deal with the case $\dim B(\nu) = 2$.

Since μ is unipotent and $\mu \neq 1$, the radical $\operatorname{rad} B(\mu) \neq 0$ and therefore $SB(\mu) \neq 0$. So there is some $i \in SB(\mu)$, $i \neq 0$. Let $i = u\mu - u$. Since $\dim(B(\mu)/\operatorname{rad} B(\mu)) \geqslant 2$, there is a basis D of nonsingular vectors for $B(\mu)$. If $f(u, w) = 0$ for all $w \in D$, then $u \in B(\mu)^{\perp} = F(\mu)$, contradicting $i \neq 0$. Thus there is some $w \in D$ such that $f(u, \alpha w) = -1$ for some $\alpha \in K$, $\alpha \neq 0$. After renaming we may assume $f(u, w) = -1$. Then $\rho_{i,w}$ is a Siegel transformation and as in Lemma 3.5 we get $\dim B(\mu\rho_{i,w}) = \dim B(\mu) - 2$. Lemma 3.9 yields that $\mu\rho_{i,w}$ is unipotent. Since $B(\rho_{i,w})$ contains a nonsingular vector, we get $\rho_{i,w} = \sigma_1\sigma_2$, where σ_j are reflections. By [13–Theorem 11.39], $\nu = \sigma_3\sigma_4$, where σ_j are reflections. Clearly, σ_1 and σ_2 commute with σ_3 and σ_4. Also, $B(\sigma_1\sigma_3)$ and $B(\sigma_2\sigma_4)$ are totally isotropic and 2-dimensional. Lemma 5.3 yields that $\sigma_1\sigma_3$ and $\sigma_2\sigma_4$ are Siegel transformations. Now $\mu\rho_{i,w}$ is a product of $\frac{1}{2}\dim B(\mu) - 1$ Siegel transformations. Thus π is a product of $\frac{1}{2}\dim B(\pi)$ Siegel transformations as required. □

Acknowledgments

This research was supported in part by NSERC Canada Grant A7251. The second author was supported by the RTN Network HPRN-CT-2002-00287: Algebraic K-Theory, Linear Algebraic Groups and Related Structures.

References

[1] F. Bachmann, Aufbau der Geometrie aus dem Spiegelungsbegriff, second ed., Grundlehren der mathematischen Wissenschaften, vol. 96, Springer-Verlag, Berlin, Heidelberg, New York, 1973, MR0346643(49#11368).

[2] J. Dieudonné, La Géometrie des Groupes Classiques, Springer-Verlag, Berlin, Göttingen, Heidelberg, 1955, MR0072144(17,236a).

[3] J. Dieudonné, Sur les générateurs des groupes classiques, Summa Bras. Math. 3 (1955) 149–179, MR0080256(18,217c).

[4] E.W. Ellers, Decomposition of orthogonal, symplectic, and unitary isometries into simple isometries, Abh. Math. Sem. Univ. Hamburg 46 (1977) 97–127, MR0467486(57#7343); Zbl 367.50002.
[5] E.W. Ellers, Classical groups, Generators and Relations in Groups and Geometries, NATO ASI Series C, vol. 333, Kluwer Academic Publishers, Dordrecht, Boston, London, 1991, pp. 1–45, MR1206909(94c:51028); Zbl 744.20029.
[6] E.W. Ellers, Bireflectionality of orthogonal and symplectic groups of characteristic 2, Arch. Math. 73 (1999) 414–418, MR1725176(2000j:20082); Zbl 951.20032.
[7] E.W. Ellers, W. Nolte, Bireflectionality of orthogonal and symplectic groups, Arch. Math. 39 (1982) 113–118, MR0675649(84a:51009); Zbl 491.51019.
[8] A.J. Hahn, O.T. O'Meara, The Classical Groups and K-Theory, Grundlehren der mathematischen Wissenschaften, vol. 291, Springer-Verlag, Berlin, Heidelberg, 1989, MR1007302(90i:20002).
[9] F. Knüppel, Products of simple isometries of given conjugacy types, Forum Math. 5 (1993) 441–458, MR1232719(94g:51025).
[10] F. Knüppel, The length problem for Eichler transformations, Forum Math. 10 (1998) 59–74, MR1490138(98j:51023).
[11] K. Nielsen, On bireflectionality and trireflectionality of orthogonal groups, Linear Algebra Appl. 94 (1987) 197–208, MR0902079(88k:15014).
[12] P. Scherk, On the decomposition of orthogonalities into symmetries, Proc. Amer. Math. Soc. 1 (1950) 481–491, MR0036762(12,157c).
[13] D.E. Taylor, The Geometry of the Classical Groups, Heldermann Verlag, Berlin, 1992, MR1189139(94d:20028).