CAYLEY PARAMETRIZATION AND THE ROTATION GROUP
OVER A NON-ARCHIMEDEAN PYTHAGOREAN FIELD

M. G. MAHMOUDI

Abstract. Using Cayley transform, we show how to construct rotation matrices infinitely near the identity matrix over a non-archimedean pythagorean field. As an application, an alternative way to construct non-central proper normal subgroups of the rotation group over such fields is provided.

Mathematics Subject Classification: 11E57, 12D15, 20G15, 65F35.

Keywords: Cayley parametrization; Frobenius norm; orthogonal group; rotation group; pythagorean field; non-archimedean field.

1. Introduction

The Cayley transform provides an important parametrization of the rotation group of the euclidean space. This map which was introduced by Arthur Cayley in 1846, associates a rotation matrix to every skew symmetric matrix of eigenvalues different from $-1$. The Cayley parameterization was used by J. Dieudonné in [3] §15, §16 to construct normal subgroups of the rotation group of a vector space $V$ of dimension $n = 3$ equipped with an anisotropic quadratic form over the field of $p$-adic numbers or the field of formal Laurent series in one variable over the field of real numbers for arbitrary $n \geq 3$. Later, using the properties of Elliptic spaces, E. Artin in [1, Ch. V, §25] constructed non-central subgroups of the rotation group $SO(V)$ of a vector space $V$ of dimension $n \geq 3$ equipped with an anisotropic quadratic $q$ form over a field $F$ with a non-archimedean ordering.

We simplify the Artin construction using the Cayley parametrization. The main new observations that make this simplification possible are the following:

(1) Assume that $n$ is odd or $n$ is even and $\det q$ is trivial. If $F$ is not formally real pythagorean then the rotation group $SO(V)$ is never projectively simple (see [5,1] and [5,2]). This enables us to concentrate on the case where the base field $F$ is pythagorean, hence the Frobenius norm is at disposal and one may consider it instead of the maximum norm as used in [1, Ch. V, §3].

(2) If $F$ is a formally real pythagorean field with a non-archimedean ordering then one can find a rotation matrix $A \in M_n(F)$ such that the Frobenius norm of $A - I \neq 0$ is infinitely small (see [5,3]).

Finally, as another application, we complement a result due to L. Bröcker [2], which implies that the orthogonal groups $SO(V)$ are all projectively simple for the case where the Witt index $\nu$ of $q$ is zero, $n \geq 3$ and $n \neq 4$ precisely in the case where $F$ is pythagorean formally real field, admits only of archimedean ordering and $q$ is similar to $x_1^2 + x_2^2 + \cdots + x_n^2$. This addresses the following passage by J. Dieudonné in [3] p. 39: "... la simplicité du groupe des rotations (pour $\nu = 0$, $n > 2$ et $n \neq 4$) sur le corps des nombres réels $\mathbb{R}$, apparaît comme un phénomène très particulier, dû à la structure très spéciale du corps $\mathbb{R}$ parmi les corps commutatifs. Il y aurait lieu de rechercher s’il existe d’autres corps qui partagent avec lui cette propriété.".
2. Notation and Terminology

Throughout this paper, $F$ denotes a field of characteristic different from two. Let $(V, b)$ be bilinear space of dimension $n$ over a field $F$ and let $q : V \to F$ be its associated nondegenerate quadratic form given by $q(x) = b(x, x)$. The determinant of $b$ is the determinant of a Gram matrix of $b$ modulo $F^\times 2$ and is denoted by $\det b$ or $\det q$. One says that $b$ or $q$ represents a scalar $\lambda \in F$ if there exists a nonzero vector $v \in V$ such that $b(v, v) = \lambda$. A vector $u \in V$ is called anisotropic (resp. isotropic) if $q(u) \neq 0$ (resp. $q(u) = 0$). A quadratic form $q$ is said to be anisotropic if all nonzero vectors in $V$ are anisotropic, otherwise $q$ is called isotropic. The Witt index $\nu$ of $(V, b)$ is defined as the maximal dimension of a totally isotropic subspace of $V$. As the characteristic of $F$ is different from two, there exists an orthogonal basis $\{e_1, \cdots, e_n\}$ of $(V, b)$. It is known that for $n \geq 3$ the group $\text{SO}(V)$ is a non-abelian group and its center is either $\{\pm \text{id}\}$ or $\{\text{id}\}$ depending on the parity of $n$ (see [4] p. 51).

For every $\sigma \in O(V)$ by the Cartan-Dieudonné theorem, there exists a decomposition $\sigma = \prod_{i=1}^n \tau_{u_i}$, where $m \leq n$ and $\tau_{u_i}$ is a reflection along the anisotropic vectors $u_i \in V$ given by

$$\tau_{u_i}(x) = x - 2\frac{b(x, u_i)}{q(u_i)} u_i.$$ 

It is known that the class of $\theta(\sigma) = \prod_{i=1}^m q(u_i)$ in the quotient group $F^\times / F^\times 2$, which is called the spinor norm of $\sigma$, is independent of the choices and the number of $u_i$'s.

We recall that a field $F$ is said to be formally real (or ordered field) if $-1$ is not a sum of squares in $F$. A field $F$ is called pythagorean if every sum of squares is again a square. An element $c$ of a formally real field $F$ is called totally positive if $c$ is positive with respect to all orderings of $F$.

If $F$ is a pythagorean field then for every matrix $A$ with entries in $F$, the Frobenius norm of $A$, denoted by $\|A\|$, is defined as the absolute value of the square root of the sum of squares of entries of $A$. The Frobenius norm satisfies the inequalities $\|AB\| \leq \|A\|\|B\|$ and $\|A + B\| \leq \|A\| + \|B\|$ when $A$ and $B$ are of appropriate sizes.

For any matrix $A \in M_n(F)$ such that $I + A$ is invertible, the map $A \mapsto (I - A)(I + A)^{-1}$ is called the Cayley map. For any skew-symmetric matrix $A \in M_n(F)$ such that the matrix $I + A$ is invertible, the matrix $Q = C(A)$ satisfies $Q^T Q = I$ and $\det Q = 1$. Conversely for every orthogonal matrix $Q$ such that $I + Q$ is invertible $C(Q)$ is a skew-symmetric matrix, see [3] p. 56.

3. Rotation group over non-archimedean fields

As a first observation we have the following result:

**Proposition 3.1.** Let $(V, b)$ be anisotropic bilinear space of dimension $n \geq 2$ over a field $F$. Then the image of the spinor norm $\theta : \text{SO}(V) \to F^\times / F^\times 2$ is trivial if and only if $F$ is a formally real pythagorean field and $q$ represents only one square class in $F^\times$, in particular $q$ is similar to the quadratic form $x_1^2 + \cdots + x_n^2$.

**Proof.** First assume that the spinor norm map is the trivial map. Let $u \in V$ be an anisotropic vector with $q(u) = d \neq 0$. Then for any anisotropic vector $v \in V$ as $\theta(\tau_{u} \tau_{v})$ is trivial, the scalars $q(u)$ and $q(v)$ are in the same square class in $F^\times$. It follows that $q$ is isomorphic to $dx_1^2 + \cdots + dx_n^2$. Let $\alpha, \beta \in F$, we should prove that there exists $\gamma \in F$ such that $\gamma^2 = \alpha^2 + \beta^2$. As $n \geq 2$, we may consider two orthogonal vectors $u, v \in V$ with $q(u) = q(v) = d \neq 0$. Now consider the vector $w = \alpha u + \beta v \in V$. We have $q(w) = (\alpha^2 + \beta^2)d$. As $q(w)$ and $q(u)$ are in the same square classes, the quantity $\alpha^2 + \beta^2$ is a square in $F$. If $F$ is not formally real,
then $-1$ is a sum of squares in $F$, hence is a square since $F$ is pythagorean. As $q \simeq dx_1^2 + \cdots + dx_n^2$ and $n \geq 2$, the form $q$ would be isotropic, contradiction. The converse follows from the Cartan-Dieudonné theorem and the fact that the current hypotheses imply that the spinor norm of the product of two arbitrary reflections is trivial.

\[ \square \]

**Proposition 3.2.** Let $(V, b)$ be an anisotropic bilinear space of dimension $n \geq 3$ over a field $F$ such that $\text{SO}(V)$ is projectively simple. Then the spinor norm map $\theta: \text{SO}(V) \to F^\times / F^\times 2$ is the trivial map precisely in the following cases (i) $n$ is odd, (ii) $n$ is even and the determinant of $b$ is trivial.

**Proof.** First suppose that $\theta$ is the trivial map. Let $\{e_1, \ldots, e_n\}$ be an orthogonal basis of $(V, b)$. We have $-\text{id} = \tau_{e_1} \tau_{e_2} \cdots \tau_{e_n}$. It follows that in the case where $n$ is even, $-\text{id} \in \text{SO}(V)$ and $\theta(-\text{id})$ which coincides with the determinant of $b$, is trivial.

Conversely suppose that (i) or (ii) hold. In the case (i) the group $\text{SO}(V)$ has trivial center. Thus the hypotheses actually say that $\text{SO}(V)$ is itself a simple group. It follows that $\ker(\theta)$ is either the trivial group or is the whole $\text{SO}(V)$. The first case is impossible as $\text{SO}(V)$ is non-abelian. The second case implies that $\text{Im}(\theta)$ is trivial.

In the case (ii) the center of $\text{SO}(V)$ is the subgroup $\{\pm \text{id}\}$. As $-\text{id} = \tau_{e_1} \tau_{e_2} \cdots \tau_{e_n}$ and the determinant of $b$ is assumed to be trivial, $\theta(-\text{id})$ is trivial as well. Therefore, the kernel of the spinor norm map $\theta$ is a subgroup of $\text{SO}(V)$ containing $\{\pm \text{id}\}$. As $\text{SO}(V)$ is assumed to be projectively simple, $\ker(\theta)$ is either $\{\pm \text{id}\}$, or $\text{SO}(V)$. If $\ker(\theta) = \{\pm \text{id}\}$, we have $\text{SO}(V)/\{\pm \text{id}\} \simeq \text{Im}(\theta)$. This shows that $\text{SO}(V)/\{\pm \text{id}\}$ is an abelian simple group. It follows that this quotient group is either the trivial group (thus $\text{Im}(\theta)$ is the trivial group) or a group of prime order. The later case is ruled out as a non-abelian group is never projectively cyclic. The former case also implies the triviality of $\text{Im}(\theta)$.

\[ \square \]

**Proposition 3.3.** Let $F$ be a pythagorean field with a non-archimedean ordering $\leq$. Then there exists a matrix $A \in M_n(F)$ with $A \neq \pm I$, $A^TA = I$ and $\det A = 1$ such that $\|I - A\|$ is infinitely small.

**Proof.** Let $\epsilon$ be an infinitely small positive element of $F$ and let $B \in M_n(F)$ be a nonzero skew-symmetric matrix whose entries are rational. Consider the matrix $A = C(\epsilon B)$, where $C$ is the Cayley map. We claim that $\|I - A\|$ is infinitely small. First note that $I + \epsilon B$ is invertible, hence $C(\epsilon B)$ is meaningful and is different from $\pm I$. Let $m$ be an odd positive integer. The relation $I + \epsilon^m B^m = (I + \epsilon B)D$ where $D = (I - \epsilon B + \epsilon^2 B^2 + \cdots + \epsilon^{m-1} B^{m-1})$ implies that $\|(I + \epsilon B)^{-1} - D\| = \epsilon^m \|B^m(I + \epsilon B)^{-1}\|$. By the Cramer rule every entry of $B^m(I + \epsilon B)^{-1}$ is of the form $p(\epsilon)/q(\epsilon)$ where $p(X), q(X) \in \mathbb{Q}[X]$ are of degree at most $n$. It follows that for sufficiently large $m$, the quantity $\|(I + \epsilon B)^{-1} - D\| = \epsilon^m p(\epsilon)/q(\epsilon)$ is infinitely small. Hence

\[
\begin{align*}
\|I - A\| &= \|I - (I - \epsilon B)(I + \epsilon B)^{-1}\| \\
&\leq \|I - (I - \epsilon B)D\| + \|(I - \epsilon B)((I + \epsilon B)^{-1} - D)\| \\
&\leq \|I - (I - \epsilon B)D\| + \|I - \epsilon B||\|(I + \epsilon B)^{-1} - D\|
\end{align*}
\]

Both quantities $\|I - (I - \epsilon B)D\|$ and $\|(I + \epsilon B)^{-1} - D\|$ are infinitely small and the proof is complete.

\[ \square \]

**Proposition 3.4.** Let $F$ be a pythagorean ordered field and let $(V, b)$ be a bilinear space of dimension $n \geq 3$, isometric to $x_1^2 + \cdots + x_n^2$. If $F$ carries a non-archimedean ordering then $\text{SO}(V)$ contains a proper non-central normal subgroup.

**Proof.** We claim that the group

\[ N = \{\sigma \in \text{SO}(V) : \|x - \sigma(x)\| \text{ is infinitely small if } q(x) = 1\} \]
is a non-trivial normal subgroup of $SO(V)$ (the idea of considering this subgroup was borrowed from [5, p. 150]). To prove this claim we first show that $N$ is a subgroup of $SO(V)$. Consider two elements $\sigma, \tau \in N$. We should prove that $\sigma\tau$ also belongs to $N$. We have $\|x - \sigma\tau(x)\| = \|(x - \tau(x)) + (\tau(x) - \sigma\tau(x))\| \leq \|x - \tau(x)\| + \|\tau(x) - \sigma\tau(x)\| = \|x - \tau(x)\| + \|x - \sigma(x)\|$, which is infinitely small. The fact that $\sigma^{-1} \in N$ when $\sigma \in N$ and the normality of $N$ is straightforward. It remains to show that $N$ is a nontrivial subgroup of $SO(V)$. Consider two orthogonal vectors $u, v \in V$ with $q(u) = q(v) = 1$. Let $\sigma = -\tau_u \in SO(V)$. We have $\|v - \sigma(v)\| = \|v + \tau_u(v)\| = 2\|v\| = 2$. Hence $\sigma \notin N$, thus $N \neq SO(V)$. By (3.3), there exists a rotation matrix $A$ such that $\|I - A\|$ is infinitely small. It follows that for every $x$ with $\|x\| = 1$ we have $\|x - Ax\| \leq \|I - A\|$ is infinitely small. Hence $A \neq \pm I$ is an element of $N$ and $N \neq \{\pm I\}$.

**Corollary 3.5.** (Bröcker) Let $(V, b)$ be a bilinear space of dimension $n \geq 3$ over a field $F$ whose Witt index is zero. Then the rotation group $SO(V)$ is a projectively simple if and only if $F$ is a pythagorean formally real field and $q$ is similar to the quadratic form $x_1^2 + x_2^2 + \cdots + x_n^2$.

**Proof.** In [2], Bröcker proves that if $F$ is a pythagorean formally real field which admits only of archimedean orderings, $n \geq 3$ and $n \neq 4$ and $q$ is anisotropic then the kernel of the spinor norm $\theta : SO(V) \to F^\times/F^\times 2$ coincides with the commutator subgroup $\Omega(V)$ of the orthogonal group $O(V)$ (see [2, (1.7)]) and the group $\Omega(V)$ is projectively simple (see [2, Satz (1.10)]). Of course when $q$ represents only one square class, the whole rotation group $SO(V)$ coincides with the kernel of the spinor norm. Hence the sufficiency of the conditions can be obtained from Bröcker’s theorem. The sufficiency follows from (3.1), (3.2) and (3.4).

**Acknowledgments.** The support from Sharif University of Technology is gratefully acknowledged.

**References**

[1] Artin, E. *Geometric algebra*. Interscience tracts in pure and applied mathematics. No. 3. New York: Interscience Publishers Inc.; London: Interscience Publishers Ltd. (1957).

[2] Bröcker, L. *Zur orthogonalen Geometrie über pythagoreischen Körperrn*. J. Reine Angew. Math. 268/269, 68-77 (1974).

[3] Dieudonné, J. *Sur les groupes classiques*. Publications de l’Institut de Mathématique de l’Université de Strasbourg, VI. Actualités Scientifiques et Industrielles, No. 1040. Hermann, Paris, 1973.

[4] Dieudonné, J. *La géométrie des groupes classiques*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Band 5. Berlin-Heidelberg-New York: Springer-Verlag (1971).

[5] Perrin, D. *Cours d’algèbre*, Paris: Ellipes (1996).

[6] Weyl, H. *The classical groups, their invariants and representations*. Reprint of the second edition (1946) of the 1939 original. Princeton University Press, Princeton, N.J. (1939).

M. G. MAHMOUDI, mmahmoudi@sharif.ir, DEPARTMENT OF MATHEMATICAL SCIENCES, SHARIF UNIVERSITY OF TECHNOLOGY, P. O. BOX 11155-9415, TEHRAN, IRAN.