Involutions on a group of Möbius transformations

1 Möbius transformations

For $v, w \in \mathbb{R}^n$, let $v = (v_1, \ldots, v_n)$ with $v_i \in \mathbb{R}, 1 \leq i \leq n$. Let the Euclidean inner-product be denoted by

$$K(v, w) = \sum_{i=1}^{n} v_i w_i.$$ 

Let $\mathbb{R}^n = \mathbb{R}^n \cup \{\infty\}$, and let $B = \{x \in \mathbb{R}^n : \|x\| < 1\}$ be the open unit ball. Let $GM(\mathbb{R}^n)$ denote the group of Möbius transformations of $\mathbb{R}^n$ [1]. Consider the group of Möbius transformations of $\mathbb{R}^n$ that leave the open ball $B$ invariant, namely,

$$GM(B) = \{\phi \in GM(\mathbb{R}^n) : \phi(B) = B\}.$$ 

Let $\text{Cl}(n)$ be the real Clifford algebra generated by $\mathbb{R}^n$ such that

$$vw + uv = -2K(v, w).$$ 

(1) 

Every $\psi \in GM(\mathbb{R}^n)$ may be expressed as a pseudo linear fractional transformation [9]. That is, there is a Vahlen matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\text{Cl}(n)$ satisfying certain restrictions on the entries of $A$ such that $\psi(x) = (ax + b)(cx + d)^{-1}, x \in \mathbb{R}^n$, and $cx + d \neq 0$.

Let $O(n)$ be the real orthogonal group, i.e., the group of invertible linear transformations of $\mathbb{R}^n$ that preserve the inner-product $K$. For any $v \in \mathbb{R}^n$, let $v^\perp = \{x \in \mathbb{R}^n : K(x, v) = 0\}$, span($v$) = $\{\alpha v : \alpha \in \mathbb{R}\}$, and let $\|v\| = K(v, v)^{1/2}$ be the Euclidean norm. Suppose $v$ is a unit vector, i.e., $\|v\| = 1$. Let $f^v \in O(n)$ satisfy $f^v(v) = -v$, and $f^v(x) = x$ whenever $x \in v^\perp$. We set $f^v(\infty) = \infty$. Since $v^2 = -1$ and $xv = -vx$ if $x \in v^\perp$, we obtain $f^v(x) = xvx$ for all $x \in \mathbb{R}^n$. Applying (1), we obtain a well-known identity

$$f^v(x) = x - 2K(x, v)v, x \in \mathbb{R}^n.$$ 

(2) 

Since $v^{-1} = -v$, a Vahlen matrix for $f^v$ is $\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$.

If $a \in B$ and $a \neq 0$, let $a^\dagger = a/\|a\|^2$, and set $r_a = \sqrt{\|a\|^2 - 1}$. Let $S_a = S(a^\dagger, r_a)$ be the sphere centered at $a^\dagger$, and of radius $r_a$. The reflection $\sigma_a$ about the sphere $S_a$ is given by

$$\sigma_a(x) = a^\dagger + r_a^2(x - a^\dagger)^\dagger, x \neq a^\dagger.$$ 

(3) 

Set $\sigma_a(a^\dagger) = \infty$. Note, $ww^\dagger = -1$ if $w \neq 0$. Rewriting, if $x \neq a^\dagger$, we find

$$\sigma_a(x) = (a^\dagger(x - a^\dagger) - (\|a\|^2 - 1))(x - a^\dagger)^{-1}$$

$$= (a^\dagger x + 1)(x - a^\dagger)^{-1}.$$
Then a Vahlen matrix for \( \sigma_a \) is \[
\begin{pmatrix}
a^\dagger & 1 \\
1 & -a^\dagger
\end{pmatrix}.
\]
Let \( T_a = \sigma_a f^{a/\|a\|} \in GM(B) \). If we multiply the Vahlen matrices for \( \sigma_a \) and \( f^{a/\|a\|} \), the product is \( \|a\|^{-1}\begin{pmatrix} 1 & a \\ -a & 1 \end{pmatrix} \).

Then a Vahlen matrix for \( T_a \) is \[
\begin{pmatrix}
1 & a \\
-a & 1
\end{pmatrix}.
\]
Since \( \sigma_a(0) = T_a(0) = a \), we say \( T_a \) is a translation. Since the sphere \( S_a \) is orthogonal to the boundary of open unit ball \( B \), we obtain \( T_a \in GM(B) \) \cite[Theorem 3.4.2]{1} If \( a = 0 \), set \( T_0 = I \). The next lemma is well-known in Möbius geometry.

**Lemma 1** Let \( \psi \in GM(B) \). Then there is a unique pair \((a, \phi) \in B \times O(n)\) such that \( \psi = T_a \phi \).

Fix a unit vector \( v \in \mathbb{R}^n \). Consider the group involution
\[
\sigma : GM(B) \to GM(B)
\]
defined by \( \sigma(\phi) = f^v \phi f^v \), \( \phi \in GM(B) \). If \( \phi \in GM(B) \), let
\[
\phi^* = \sigma(\phi)^{-1}.
\]
If \( a \in B \), \( a \neq 0 \), and \( w \in \mathbb{R}^n \) is a unit vector, we show \( f^w \sigma_a f^w = \sigma_{f^w(a)} \). This follows easily because if we multiply the Vahlen matrices for \( f^w \), \( \sigma_a \), and \( f^w \), we find
\[
\begin{pmatrix}
w & 0 \\
0 & -w
\end{pmatrix}
\begin{pmatrix}
a^\dagger & 1 \\
1 & -a^\dagger
\end{pmatrix}
\begin{pmatrix}
w & 0 \\
0 & -w
\end{pmatrix}
= \|w\|^2
\begin{pmatrix}
\frac{f^w/\|w\|}{1}(a^\dagger) & 1 \\
1 & -\frac{f^w/\|w\|}{1}(a^\dagger)
\end{pmatrix}.
\]
Since \( \phi \in O(n) \) is a product of reflections \( f^w \), we obtain \( \phi \sigma_a \phi^{-1} = \sigma_{f^w(a)} \). A short calculation shows \( \phi f^w \phi^{-1} = f^{\phi(w)} \) for all \( \phi \in O(n) \). Then
\[
\phi T_a \phi^{-1} = (\phi \sigma_a \phi^{-1})(\phi f^{a/\|a\|} \phi^{-1}) = \sigma_{f^w(a)} f^{\phi(a/\|a\|)} = T_{\phi(a)}.
\]

**Lemma 2** Let \( \phi \in O(n) \), \( a \in B \), \( a \neq 0 \), and let \( w \in \mathbb{R}^n \) be a unit vector. Then
1. \( \phi \sigma_a \phi^{-1} = \sigma_{\phi(a)} \),
2. \( \phi f^w \phi^{-1} = f^{\phi(w)} \), and
3. \( \phi T_a \phi^{-1} = T_{\phi(a)} \)

We find the next lemma useful.

**Lemma 3** Let \( a_1, a_2 \in \mathbb{R}^n \) where \( a_1 \neq 0 \). Then \( a_1 a_2 \in \mathbb{R} \) iff \( a_2 \in \text{span}(a_1) \).

**Proof** Let \( a_1 a_2 \in \mathbb{R} \). Since \( a_1^{-1} = -a_1 \|a_1\|^{-2} \), we find
\[
a_1^{-1} + a_2 = a_1^{-1}(1 + a_1 a_2) \in \text{span}(a_1).
\]
Thus, \( a_2 \in \text{span}(a_1) \). The proof of the converse is similar.
Lemma 6

Proof

Since \( a \) obtain

Applying Lemma 3, we find

Corollary 5

diag

is the diagonal matrix

reflections, and

\( A \) is a product of two linearly independent vectors. Then

\[
\begin{pmatrix}
1 & a \\
-a & 1
\end{pmatrix}
\begin{pmatrix}
1 & b \\
-b & 1
\end{pmatrix}
= \begin{pmatrix}
1 - ab & a + b \\
-(a + b) & 1 - ab
\end{pmatrix}
\begin{pmatrix}
1 & -ab \\
-(a + b)(1 - ab)^{-1} & 1
\end{pmatrix}
\]

Suppose \( a \neq 0 \). If \( ab \notin \mathbb{R} \), then \( 1 - ab = -\frac{a}{\|a\|^2}(a + \|a\|^2b) \) is a product of two linearly independent vectors in \( \mathbb{R}^n \). Thus, the Möbius transformation defined by the right most Vahlen matrix in the above equation lies in \( SO(n) \), and is not the identity transformation. Note, \( (a + b)(1 - ab)^{-1} = T_a(b) \).

Lemma 4 Let \( a, b \in B \) and let \( c = T_a(b) \).

1. If \( ab \in \mathbb{R} \), then \( T_aT_b = T_c \)
2. If \( ab \notin \mathbb{R} \), then \( T_aT_b = T_c\phi \) for some \( \phi \in SO(n) \), \( \phi \neq I \).
3. \( (T_a)^{-1} = T_a \)

The next result follows from Corollary 2 and Lemma 4.

Corollary 5 Let \( a \in B \), and \( \phi \in O(n) \). Then we have

1. \( \sigma(T_a) = T_{f^v(a)} \) and \( (T_a)^* = T_{-f^v(a)} \)
2. \( \sigma(T_a) = T_a \) if and only if \( a \in v^\perp \).
3. \( (T_a)^* = T_a \) if and only if \( a \in \text{span}(v) \).

The next lemma is an unexpected result.

Lemma 6 Let \( a_1, a_2 \in B \) satisfy \( a_1 \in \text{span}(v) \), \( a_2 \in v^\perp \), \( a_1 \neq 0 \), and \( a_2 \neq 0 \). If \( a = a_1 + a_2 \), then \( T_aT_a^* \neq (T_b)^2 \) for any \( b \in B \).

Proof Since \( f^v(a) = -a_1 + a_2 \) and \( K(a_1, a_2) = 0 \), we find

\[
a f^v(a) = (a_1 + a_2)(-a_1 + a_2)
= \|a_1\|^2 - \|a_2\|^2 + 2a_1a_2
\]

Applying Lemma 3, we find \( a_1a_2 \notin \mathbb{R} \) and \( 1 + af^v(a) \notin \mathbb{R} \). Applying Lemma 4, we obtain \( T_aT_a^* = T_cA \) where \( c = T_a(-f^v(a)), A \in SO(n) \), and a Vahlen matrix for \( A \) is the diagonal matrix \( \text{diag}(1 + af^v(a), 1 + af^v(a)) \). However,

\[
1 + af^v(a) = a(-a\|a\|^{-2} + f^v(a))
\]

is a product of two linearly independent vectors. Then \( A \) is a product of two reflections, and \( A \neq I \). On the contrary, suppose \( T_aT_a^* = (T_b)^2 \) for some \( b \in B \).
Then $(T_b)^2 = T_d$ where $d = T_b(b)$. Applying Lemma 1, by uniqueness we find $c = d$ and $A = I$. However, this is a contradiction.

The following is another identity.

**Lemma 7** Let $a \in B$, $a \neq 0$, and let $w \in \mathbb{R}^n$ be a unit vector. Then 

$$\sigma_a f^w \sigma_a = \begin{cases} f^w & \text{if } w \in a^\perp \\ \sigma_b & \text{if } w \notin a^\perp \end{cases}, \quad b = \sigma_a f^w(a).$$

**Proof** A Möbius transformation maps each sphere and hyperplane onto either a sphere or hyperplane. Then $\sigma_a(w^\perp)$ is either a sphere or a hyperplane. The reflection $\tilde{\sigma}$ about $\sigma_a(w^\perp)$ fixes the points of $\sigma_a(w^\perp)$. Then $\tilde{\sigma} = \sigma_a f^w \sigma_a$.

Suppose $w \in a^\perp$. Recall, $a^\perp = a/\|a\|^2$ is the center of the sphere $S_a$. Notice, $\tilde{\sigma}(\infty) = \sigma_a f^w \sigma_a(\infty) = \sigma_a f^w(a^\perp) = \sigma_a(a^\perp) = \infty$. Then $\sigma_a(w^\perp)$ is a hyperplane. Notice, $\tilde{\sigma}(0) = \sigma_a f^w \sigma_a(0) = \sigma_a f^w(a) = \sigma_a(a) = 0$. Then $\sigma_a(w^\perp)$ is a hyperplane passing through the origin. If $x \in w^\perp$, then $K(\sigma_a(x), w) = K(a^\perp + r_a^2(x-a^\perp)^\perp, w) = 0$. Thus, $\sigma_a(w^\perp) \subset w^\perp$. Consequently, $f^w \sigma_a(x) = \sigma_a(x)$. Then $\tilde{\sigma}(x) = x$ for all $x \in w^\perp$. Since $\tilde{\sigma}$ is not the identity mapping, $\tilde{\sigma} = f^w$.

Suppose $w \notin a^\perp$. Notice, $\tilde{\sigma}(\infty) = \sigma_a f^w \sigma_a(\infty) = \sigma_a f^w(a^\perp) \neq \sigma_a(a^\perp) = \infty$ or $\tilde{\sigma}(\infty) \neq \infty$. Then $\sigma_a(w^\perp)$ is a sphere that is centered at $\tilde{\sigma}(\infty) = \sigma_a f^w(a^\perp)$. Now, let $\sigma_0(x) = x^\perp$ denote the inversion about the unit sphere $S^1 = S(0,1)$ centered at the origin with radius 1. The product of the Vahlen matrices for $\sigma_o, \sigma_a$, and $f^w$ satisfies

$$\begin{pmatrix} 0 & (-1)^{n}e \\ e & 0 \end{pmatrix} \begin{pmatrix} a^\perp & 1 \\ 1 & -a^\perp \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix} = \begin{pmatrix} (-1)^n e v & (-1)^n e a^\perp v \\ e a^\perp v & -e v \end{pmatrix}.$$  

Recall, $e x = (-1)^{n+1} x e$ for all $x \in \mathbb{R}^n$. Then the Vahlen matrix in the above right side is the same as the Vahlen matrix in the left side below

$$\begin{pmatrix} -ve & (-1)^{n}a^\perp ve \\ a^\perp ve & (-1)^n ve \end{pmatrix} = \begin{pmatrix} a^\perp & 1 \\ 1 & -a^\perp \end{pmatrix} \begin{pmatrix} w & 0 \\ 0 & -w \end{pmatrix} \begin{pmatrix} 0 & (-1)^n e \end{pmatrix}.$$  

Thus, $\sigma_0 \sigma_a f^w = \sigma_a f^w \sigma_0$. If we evaluate at $a$, we find $\sigma_a f^w(a^\perp) = (\sigma_a f^w(a))^\perp$. Let $b = \sigma_a f^w(a) \in B$. Then $\tilde{\sigma}(\infty) = b^\perp$ and $\sigma_a(w^\perp)$ is a sphere centered at $b^\perp$. Notice,

$$\tilde{\sigma}(b) = \sigma_a f^w \sigma_a(\sigma_a f^w(a)) = \sigma_a(a) = 0.$$  

Applying Theorem 3.4.2 in [1], the sphere $\sigma_a(w^\perp)$ is orthogonal to the unit sphere $S^1$. Hence, $\tilde{\sigma} = \sigma_b$.

**Definition 1** Consider the following fixed points in $GM(B)$.

1. $GM(B)^o = \{ \psi \in GM(B) : \sigma(\psi) = \psi \}$
2. $GM(B)^s = \{ \psi \in GM(B) : \psi^s = \psi \}$
Let \( \phi \in O(n) \) and suppose \( f^v \phi f^v = \phi \). Then \(-f^v \phi(v) = \phi(v)\), and consequently \( \phi(v) \in \text{span}(v) \). Since \( \phi \in O(n) \), we find \( \phi(v) = v \) or \( \phi(v) = -v \). Conversely, if \( \phi(v) = v \) or \( \phi(v) = -v \), then \( f^v \phi f^v(v) = -f^v \phi(v) = \phi(v) \). If \( x \in v^\perp \) and since \( \phi(v) = v \) or \( \phi(v) = -v \), we find \( 0 = K(x, v) = K(\phi(x), \phi(v)) \). Then \( \phi(x) \in v^\perp \) and \( f^v \phi f^v(x) = f^v \phi(x) = \phi(x) \). Thus, \( f^v \phi = \phi f^v \) iff \( f^v \phi f^v = \phi \) iff \( \phi(v) = v \) or \( \phi(v) = -v \). Note,

\[
\phi \phi^* = (f^v \phi f^v)^{-1} f^v = f^\phi(v) f^v.
\]

On the other hand, \( \phi^* = \phi \) iff \( f^v \phi^{-1} f^v = \phi \) iff \( (\phi f^v)^{-1} = \phi f^v \).

Let \( a \in B \), and \( \xi \in O(n) \). Then \( T_a \xi \in GM(B)_\sigma \) iff \( (T_a \xi)^* = T_a \xi \) iff \( \xi^* T_{-f^v(a)} = T_a \xi \). Thus, \( T_a \xi \in GM(B)_{\sigma^*} \) iff \( \xi^* f^v(a) = -a \) and \( \xi = \xi^* \). However, \( \xi^* f^v(a) = -a \) if and only if \( \xi f^v(a) = -a \).

**Lemma 8** Let \( \phi \in O(n) \), and let \( a \in B \). Then

1. \( \sigma(\phi) = \phi \) iff \( \phi(v) \in \{v, -v\} \) iff \( \phi \phi^* = I \) iff \( f^v \phi = \phi f^v \).
2. \( \sigma(T_a \phi) = T_a \phi \) iff \( a \in v^\perp \) and \( \phi \phi^* = I \).
3. \( \phi^* = \phi \) iff \( (\phi f^v)^2 = I \).
4. \( (T_b \xi)^* = T_b \xi \) iff \( \xi f^v(b) = -b \) and \( \xi = \xi^* \).

**Corollary 9** The following sets of fixed points satisfy

1. \( GM(B)^v = \{T_a \phi : a \in v^\perp, \phi \in O(n), \text{ and } \phi \phi^* = I\} \)
2. \( GM(B)_{\sigma^*} = \{T_b \xi : \xi f^v(b) = -b, \xi \in O(n), \text{ and } \xi^* = \xi\} \)

The next result follows easily from Corollary 5 and Corollary 9.

**Corollary 10** Let \( a \in B \cap \text{span}(v) \). Then \( T_a \in GM(B)_{\sigma^*} \) and \( T_a T_a^* = T_a^2 \).

**Lemma 11** Let \( \phi \in O(n) \). Then \( \phi \phi^* = \xi^2 \) for some \( \xi \in O(n) \cap GM(B)_{\sigma^*} \). We may choose \( \xi \) as follows.

1. If \( \phi \phi^* = I \), let \( \xi = -f^v \).
2. If \( \phi \phi^* \neq I \), let \( \xi = f^w f^v \) where \( w \) is a unit vector that bisects the smaller angle between \( v \) and \( \phi(v) \).

**Proof** Recall, \( \phi \phi^* = f^\phi(v) f^v \) from (6). If \( \phi \phi^* = I \), then a square root of \( I \) is \(-f^v \in GM(B)_{\sigma^*} \). Suppose \( \phi \phi^* \neq I \). Then \( \phi(v) \neq \pm v \). Notice, \( f^\phi(v) f^v \) is a rotation in the two-dimensional subspace spanned by \( v \) and \( \phi(v) \). Then there exists a unique unit vector \( w \) satisfying

1. \( (f^w f^v)^2 = f^\phi(v) f^v \)
2. \( K(v, \phi(v)) = \cos(2\beta), 0 < 2\beta < \pi \)
3. \( K(v, w) = K(\phi(v), w) = \cos(\beta) \).

We say \( w \) bisects the smaller positive angle between the linearly independent vectors \( v \) and \( \phi(v) \). Let \( \xi = f^w f^v \). Clearly, \( \phi\phi^* = \xi^2 \), \( (\xi f^v)^2 = I \), and \( \xi \in GM(B)_\sigma \) by Lemma 8.

Next, we note \( T_a(-f^v) \in GM(B)_\sigma \) because of Lemma 8. Let \( T_a\phi(T_a\phi)^* = (T_a\xi)^2 \) where \( \xi \) is from Lemma 11. Then

\[
T_a\phi\phi^* T_{-f^v(a)} = T_a\xi T_a \xi^{-1} \xi^2 \\
\phi\phi^* T_{-f^v(a)} = T_{\xi(a)} \xi^2 \\
\phi\phi^* T_{-f^v(a)} = \xi^2 T_{\xi^{-1}(a)}.
\]

If \( \phi\phi^* = I \), then choose \( \xi = -f^v \) by Lemma 11. Now, let \( \sqrt{I} \in O(n) \) be a square root of \( I \). Then \( (\sqrt{I} f^v)(\sqrt{I} f^v)^* = I \) iff \( (\sqrt{I} f^v)^2 = I \) iff \( \sqrt{I} f^v = f^v \sqrt{I} \).

**Corollary 12** Let \( a \in B \), \( \phi \in O(n) \), and let \( \sqrt{I} \in O(n) \) be a square root of \( I \). Then

1. \( \phi\phi^* = I \) iff \( T_a\phi(T_a\phi)^* = T_a T_a^* \)
2. \( T_a T_a^* = (T_a(-f^v))^2 \) and \( T_a(-f^v) \in GM(B)_\sigma \)
3. If \( \sqrt{I} f^v = f^v \sqrt{I} \), then \( (T_a\sqrt{I} f^v)(T_a\sqrt{I} f^v)^* = (T_a(-f^v))^2 \).

Given a Vahlen matrix \( A \), let \( F_A \in GM(\mathbb{R}^n) \) denote the corresponding linear fractional transformation defined on \( \mathbb{R}^n \). The next lemma follows from Lemma 4.

**Lemma 13** Let \( a, b \in B \), \( \phi, \xi \in O(n) \), \( c = T_a(-\phi\phi^* f^v(a)) \), and let \( d = T_b(\xi(b)) \). Consider the Vahlen matrices

\[
a) \ A = \begin{pmatrix} 1 + a\phi\phi^* f^v(a) & 0 \\ 0 & 1 + a\phi\phi^* f^v(a) \end{pmatrix} \\
b) \ B = \begin{pmatrix} 1 - b\xi(b) & 0 \\ 0 & 1 - b\xi(b) \end{pmatrix}.
\]

Then each of \( F_A, F_B \in SO(n) \) is a product of two reflections, and satisfying

1. \( (T_a\phi)(T_a\phi)^* = T_c F_A \phi \phi^* \)
2. \( (T_b\xi)^2 = T_d F_B \xi^2 \).

Next, let \( a \in B \), \( a \neq 0 \), and let \( \phi \in O(n) \). Suppose \( f^{\alpha/\|a\|}(v) = -\phi(v) \) and \( \phi\phi^* \neq I \). Let \( w \) be the unit vector in Lemma 11 satisfying \( \xi = f^w f^v \in SO(n) \cap GM(B)_\sigma \), \( \xi^2 = f^{\phi(v)} f^v \), \( K(v, \phi(v)) = \cos(2\beta) \), \( 0 < 2\beta < \pi \), and \( K(v, w) = K(\phi(v), w) = \cos(\beta) \). Note, \( f^{\alpha}(v) \) belongs to span of \( v \) and \( \phi(v) \). Since \( f^{\alpha}(v) = v - 2K(v, w)w \), we find \( K(f^{\alpha}(v), \phi(v)) = -1 \). Then \( f^{\alpha}(v) = -\phi(v) \). Since \( f^{\alpha/\|a\|}(v) = -\phi(v) \),
we obtain \( f^w(v) = f^a/\|a\|(v) \). Then \( a \in \text{span}(w) \) and \( \xi f^v(a) = -a \). Thus, \( T_a \xi \in \text{GM}(B)_\sigma \). Applying Lemma 13, we find \( (T_a \phi)(T_a \phi)^* = (T_a \xi)^2 \).

On the other hand, suppose \( a \in \phi(v)^\perp \). Since \( \phi \phi^* f^v(a) = f^{\phi(v)}(a) = a \), then the Vahlen matrix \( A \) in Lemma 13 is a scalar matrix. Thus, \( F_A = I \). Also, \( T_a (\phi \phi^* f^v(a)) = T_a (a) = 0 \). Applying Lemma 13, we find \( (T_a \phi)(T_a \phi)^* = \phi \phi^* \).

**Theorem 14** Let \( a \in B, a \neq 0 \), and let \( \phi \in O(n) \). Let \( \xi \in \text{SO}(n) \cap \text{GM}(B)_\sigma \) be chosen as in Lemma 11.

1. If \( f^a/\|a\|(v) = -\phi(v) \) and \( \phi \phi^* \neq I \), then \( T_a \phi(T_a \phi)^* = (T_a \xi)^2 \) and \( T_a \xi \in \text{GM}(B)_\sigma \).

2. If \( a \in \phi(v)^\perp \), then \( (T_a \phi(T_a \phi)^* = \phi \phi^* = \xi^2 \).

**Lemma 15** Let \( x \in \text{GM}(B) \). If \( xx^* \) has a square root \( \sqrt{xx^*} \in \text{GM}(B)_\sigma \), then \( k = (\sqrt{xx^*})^{-1} x \in \text{GM}(B)_\sigma \). Consequently, \( x = \sqrt{xx^*} k \in \text{GM}(B)_\sigma \cdot \text{GM}(B)_\sigma \).

**Proof** By assumption, \( \sqrt{xx^*} \in \text{GM}(B)_\sigma \). Let \( k = (\sqrt{xx^*})^{-1} x \). Then

\[
k k^* = (\sqrt{xx^*})^{-1} x x^* (\sqrt{xx^*})^{-1} = e
\]

Since \( k = (k^*)^{-1} = \sigma(k^{-1})^{-1} = \sigma(k) \), we find \( k \in \text{GM}(B)_\sigma \).

\( \square \)
2 A matrix group for $GM(B)$

Let $M_n(\mathbb{R})$ denote the set of $n$-by-$n$ real matrices. For $A \in M_n(\mathbb{R})$, let $A^t$ and $\det(A)$ denote the transpose and determinant of matrix $A$, respectively. Let $GL_{n+1}(\mathbb{R})$ be the set of nonsingular matrices in $M_{n+1}(\mathbb{R})$. Let $J = 1 \oplus (-I_n) \in GL_{n+1}(\mathbb{R})$ be a block matrix. We review a model for hyperbolic geometry [1], [8]. If $x = (x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ is a row vector, then

$$x^t J x = x_0^2 - \sum_{i=1}^{n} x_i^2.$$  

Let $Q = \{ x \in \mathbb{R}^{n+1} : x_0 \geq 1, x^t J x = 1 \}$. We know $Q$ is the upper half of a two-sheeted hyperboloid, and we simply say $Q$ is a hyperboloid. For $x \in Q$, let $T_x Q$ be the tangent space to $Q$ at $x$. Notice, if $y \in \mathbb{R}^{n+1}$, then $y \in T_x Q$ if and only if $y^t J x = 0$. For $y, z \in T_x Q$, let $\langle y, z \rangle_x = -y^t J z$. It is known that $\langle \cdot, \cdot \rangle_x$ defines a positive-definite bilinear form on $T_x Q$ [8]. The $n$-dimensional Riemannian manifold $Q$ is the hyperboloid model for hyperbolic geometry.

If $A \in GL_{n+1}(\mathbb{R})$, let $a_{00}$ denote the entry of $A$ that lies in the first row and first column. It is well-known that the group of isometries of $Q$ is the Lie group

$$O^+(1, n) = \{ A \in GL_{n+1}(\mathbb{R}) : a_{00} \geq 1, A^t J A = J \}. \quad (7)$$

In fact, $Ax \in Q$ whenever $x \in Q$ and $A \in O^+(1, n)$. Recall, $B \subset \mathbb{R}^n$ denotes the open unit ball. Let $F_o : Q \to B$ be a bijection from $Q$ onto $B$ such that $F_o(x_0, x_1, \ldots, x_n) = (1+x_0)^{-1}(x_1, \ldots, x_n)$. It is well-known that $F_o A F_o^{-1} \in GM(B)$ whenever $A \in O^+(1, n)$ [1, page 51]. In addition, the mapping

$$F : O^+(1, n) \to GM(B) \quad (8)$$

satisfying $F(A) = F_o A F_o^{-1}$, $A \in O^+(1, n)$, is a group isomorphism from $O^+(1, n)$ onto $GM(B)$. We say $O^+(1, n)$ is a matrix group interpretation for $GM(B)$. The connected component of $O^+(1, n)$ that contains the identity $I_{n+1}$ (see [1], [7]) is the subgroup

$$SO^+(1, n) = \{ A \in O(1, n) : a_{00} > 0, \det(A) = 1 \}.$$  

The Lie algebra of $SO^+(1, n)$ or $O^+(1, n)$ is

$$\mathfrak{s}_0(1, n) = \{ A \in M_{n+1}(\mathbb{R}) : A^T J + J A = 0 \}. \quad \text{(9)}$$

The Lie algebra of the real orthogonal group $O(n)$ is

$$\mathfrak{s}_0(n) = \{ W \in M_n(\mathbb{R}) : W^T = -W \}.$$  

Let $\text{der}(\mathfrak{s}_0(1, n))$ denote the set of derivations of $\mathfrak{s}_0(1, n)$. Let $\text{Int}(\mathfrak{s}_0(1, n))$ be the adjoint group of $\mathfrak{s}_0(1, n)$. The next lemma has some useful facts about $\mathfrak{s}_0(1, n)$.

**Lemma 16** Let $n \geq 2$, and let $A \in M_{n+1}(\mathbb{R})$.  

8
a) $A \in \mathfrak{so}(1,n)$ iff $A = \begin{pmatrix} 0 & w^T \\ w & A_2 \end{pmatrix}$ where $w \in \mathbb{R}^n$ and $A_2 \in \mathfrak{so}(n)$.

b) $\mathfrak{so}(1,n)$ is a real simple Lie algebra.

c) The center of $SO^+(1,n)$ is $\{I_{n+1}\}$.

d) The adjoint representation

$$Ad : SO^+(1,n) \rightarrow Int(\mathfrak{so}(1,n))$$

is an isomorphism, and $ad(\mathfrak{so}(1,n)) = \text{der}(\mathfrak{so}(1,n))$.

e) The exponential mapping $\exp : \mathfrak{so}(1,n) \rightarrow SO^+(1,n)$ is surjective.

f) The Killing form $K$ for $\mathfrak{so}(1,n)$ satisfies

$$K(A,B) = (n-1)\text{Tr}(AB)$$

for all $A, B \in \mathfrak{so}(1,n)$.

**Proof**  Part a) follows from a direct computation. For part b), $\mathfrak{so}(1,n)$ is in the list of simple Lie algebras in [3, page 518, Table V]. Part c) follows from an application of Lemma 1. Since $SO^+(1,n)$ is a connected simple Lie group with trivial center, part d) is a special case of [3, page 129 and 132]. Part e) is proved in [7].

To prove part f), consider the complex orthogonal group $O(n+1, \mathbb{C})$. Let $\mathfrak{o}(n+1)$ be the Lie algebra of $O(n+1, \mathbb{C})$. The Killing form for $\mathfrak{o}(n+1)$ satisfies $K(X,Y) = (n-1)\text{Tr}(XY)$, $X,Y \in \mathfrak{o}(n+1)$ [10, page 390]. It is known that the complexification of $\mathfrak{so}(1,n)$ is $\mathfrak{o}(n+1)$. Then the Killing form for $\mathfrak{so}(1,n)$ is the restriction of the Killing form for $\mathfrak{o}(1+n)$ to $\mathfrak{so}(1,n)$ [3, page 180].

From (4), we recall the involution $\sigma$ of the group $GM(B)$. From the isomorphism $F$ in (8), we determine the corresponding involution of $O^+(1,n)$. If $\phi \in O(n)$, then $1 \oplus \phi \in O^+(1,n)$. We apply the identity $F(1 \oplus \phi) = \phi, \phi \in O(n)$ [1, page 51]. Let

$$L = 1 \oplus f^v \in O^+(1,n).$$

Now, consider the involution

$$\rho : O^+(1,n) \rightarrow O^+(1,n)$$

satisfying $\rho(A) = LAL$ for $A \in O^+(1,n)$. Note, if $n \geq 2$, and $v = e_1$, then $L = \text{diag}(1,-1,I_{n-1})$. Let $\hat{A} = \rho(A)^{-1}$.

**Definition 2**  Consider the following subsets of $O^+(1,n)$.

1. $O^+(1,n)^\rho = \{\psi \in O^+(1,n) : \rho(\psi) = \psi\}$
2. $O^+(1,n)_{\rho} = \{\psi \in O^+(1,n) : \hat{\psi} = \psi\}$
3. \( P = \{ \psi \hat{\psi} : \psi \in O^+(1, n) \} \)

**Lemma 17** We have the following identities.

1. \( O^+(1, n)_\rho = F^{-1}(GM(B)^\sigma) \)
2. \( O^+(1, n)_\rho = F^{-1}(GM(B)_\sigma) \)
3. \( P = F^{-1}\{ \phi \hat{\phi} : \phi \in GM(B) \} \)

**Proof** Let \( \phi \in GM(B) \). Note, \( \phi \in GM(B) \) if and only if \( f^v \phi f^v = \phi \). Applying \( F^{-1} \), we find \( \phi \in GM(B) \) if and only if \( LF^{-1}(\phi)L = F^{-1}(\phi) \). Thus, \( \phi \in GM(B)^\sigma \) if and only if \( \rho(F^{-1}(\phi)) = F^{-1}(\phi) \). This proves Statement 1. Note, \( \hat{F}^{-1}(\phi) = F^{-1}(\phi^*) \). Then Statements 2 and 3 of the lemma follow.

The differential of \( \rho \) is a Lie algebra involution

\[ d\rho : so(1, n) \to so(1, n) \]

satisfying \( d\rho(A) = LAL, A \in so(1, n) \). Then \( so(1, n) = \mathfrak{K} \oplus \mathfrak{p} \) is a direct sum of eigenspaces

\[ \mathfrak{p} = \{ A \in so(1, n) : d\rho(A) = -A \} \quad (11) \]
\[ \mathfrak{K} = \{ A \in so(1, n) : d\rho(A) = A \} \quad (12) \]

Notice, \( \mathfrak{K} \) is a Lie subalgebra of \( so(1, n) \). Let

\[ K = \{ A \in O^+(1, n) : \rho(A) = A \}. \quad (13) \]

Applying Lemma 8, we find \( A \in K \) if and only if \( A \hat{A} = I \). Let \( X \in so(1, n) \) satisfy \( e^{tX} \in K \) for all \( t \in \mathbb{R} \). Then \( \rho(e^{tX}) = e^{tX} \) for all \( t \in \mathbb{R} \). Equivalently, \( e^{t\rho(X)} = e^{tX} \) for all \( t \in \mathbb{R} \). Since the exponential map is injective in a small neighborhood of 0, \( d\rho(X) = X \). Then the Lie algebra of \( K \) is \( \mathfrak{K} \).

Recall, \( \mathcal{K} \) is the Killing form for \( so(1, n) \). Let

\[ \mathcal{K}_\rho(V, W) = -\mathcal{K}(V, d\rho(W)). \quad (14) \]

for \( V, W \in so(1, n) \).

**Lemma 18** Let \( U, V \in so(1, n) \).

1. If \( A \in \mathfrak{p} \), then \( \mathcal{K}_\rho(\text{ad}(A)U, V) = \mathcal{K}_\rho(U, \text{ad}(A)V) \).
2. If \( A \in \mathcal{K} \), then \( \mathcal{K}_\rho(\text{ad}(A)U, V) = -\mathcal{K}_\rho(U, \text{ad}(A)V) \).
3. If \( X \in O^+(1, n) \), then \( \mathcal{K}_\rho(\text{Ad}(X)U, V) = \mathcal{K}_\rho(U, \text{Ad}(\hat{X})(V)) \).
4. \( \mathcal{K}_\rho(d\rho(U), d\rho(V)) = \mathcal{K}_\rho(U, V) \) and \( \mathcal{K}_\rho(U, V) = \mathcal{K}_\rho(U, V) \)
Proof For any $A \in \mathfrak{so}(1, n)$, we have a well-known identity, $\mathcal{K}([A, V], W) = \mathcal{K}(A, [V, W])$. For any Lie algebra automorphism $s \in Aut(\mathfrak{so}(1, n))$, we recall a well-known identity, $s \circ ad(V) \circ s^{-1} = ad(s(V))$. Then Statements 1 and 2 follow from these two identities. Let $X \in O^+(1, n)$. Applying the identity $\mathcal{K}(s(U), s(V)) = \mathcal{K}(U, V)$, we find

$$\mathcal{K}_\rho(\text{Ad}(X)V, W) = -\mathcal{K}(\text{Ad}(LX^{-1})V, \text{Ad}(L)W)$$

$$= -\mathcal{K}(V, \text{Ad}(LX)W)$$

$$= \mathcal{K}_\rho(V, \text{Ad}(X)(W)).$$

This proves statement 3. Finally, Statement 4 follows easily since $d\rho \in Aut(\mathfrak{so}(1, n))$.

Lemma 19 Let $n \geq 2$, and let $A \in \mathfrak{so}(1, n)$.

1. If $\mathcal{K}_\rho(ad(A)U, V) = \mathcal{K}_\rho(U, ad(A)V)$ for all $U, V \in \mathfrak{so}(1, n)$, then $A \in \mathfrak{p}$.

2. If $\mathcal{K}_\rho(ad(A)U, V) = -\mathcal{K}_\rho(U, ad(A)V)$ for all $U, V \in \mathfrak{so}(1, n)$, then $A \in \mathfrak{r}$.

Proof Suppose $\mathcal{K}_\rho(ad(A)U, V) = \mathcal{K}_\rho(U, ad(A)V)$ for all $U, V \in \mathfrak{so}(1, n)$. Then

$$\mathcal{K}_\rho(e^{ad(A)}U, V) = \mathcal{K}_\rho(U, e^{ad(A)}V).$$

Note, $e^{ad(A)} = Ad(e^A)$. Let $\alpha \in \mathbb{R}$. Applying Lemma 18, we find

$$\mathcal{K}_\rho(U, e^{ad(A)}V) = \mathcal{K}_\rho(U, Ad(e^A)V)$$

$$= \mathcal{K}_\rho(\text{Ad}(e^A)U, V)$$

$$= \mathcal{K}_\rho(e^{-ad(\rho(A))}U, V).$$

Since $\mathcal{K}_\rho$ is a non-degenerate bilinear form, and the exponential mapping is injective on a small neighborhood of $0$, we obtain $ad(A) = -ad(d\rho(A))$. Recall, the center of $\mathfrak{so}(1, n)$ is $\{0\}$ for $n \geq 2$ by Corollary 16. Then $d\rho(A) = -A$ and $A \in \mathfrak{p}$.

Next, suppose $\mathcal{K}_\rho(ad(A)U, V) = -\mathcal{K}_\rho(U, ad(A)V)$ for all $U, V \in \mathfrak{so}(1, n)$. Then $\mathcal{K}_\rho(e^{ad(A)}U, V) = \mathcal{K}_\rho(U, e^{-ad(A)}V)$ for all $\alpha \in \mathbb{R}$. Similarly, we find $A = d\rho(A)$ and $A \in \mathfrak{r}$.

Next, we determine the forms of the matrices in $\mathfrak{p}$ and $\mathfrak{r}$. Let $A = \begin{pmatrix} 0 & w^t \\ w & A_2 \end{pmatrix} \in \mathfrak{so}(1, n)$. Then

1. $LA = (1 \oplus f^v)A = \begin{pmatrix} 0 & w^t \\ f^w & f^v A_2 \end{pmatrix}$

2. $AL = A(1 \oplus f^v) = \begin{pmatrix} 0 & w^t f^v \\ w & A_2 f^v \end{pmatrix}$
Clearly, $d\rho(A) = -A$ if and only if $LA = -AL$ if and only if $f^v w = -w$ and $A_2 f^v = -f^v A_2$. Likewise, $d\rho(A) = A$ if and only if $LA = AL$ if and only if $f^v w = w$ and $A_2 f^v = f^v A_2$.

**Lemma 20** Let $A = \begin{pmatrix} 0 & w^t \\ w & A_2 \end{pmatrix} \in so(1,n)$ where $w \in \mathbb{R}^n$ and $A_2 \in so(n)$.

1. $A \in \mathfrak{p}$ if and only if $A = \begin{pmatrix} 0 & w^t \\ w & A_2 \end{pmatrix}$ where $w \in \text{span}(v)$, $A_2 v \in v^\perp$, and $A_2 (v^\perp) \subset \text{span}(v)$.

2. $A \in \mathfrak{r}$ if and only if $A = \begin{pmatrix} 0 & w^t \\ w & A_2 \end{pmatrix}$ where $w \in v^\perp$, $A_2 v \in \text{span}(v)$, and $A_2 (v^\perp) \subseteq v^\perp$.

**Lemma 21** Let $n \geq 2$, and let $X \in so(1,n)$. If $K_\rho(Ad(e^X) A, B) = K_\rho(A, Ad(e^X) B)$ for all $A, B \in so(1,n)$, then $\rho(e^X) = e^{-X}$.

**Proof** Note, $K_\rho(Ad(e^X) A, B) = K_\rho(A, Ad(e^X) B)$ by (18). Then $K_\rho(A, Ad(e^X) B) = K_\rho(A, Ad(e^X) B)$ for all $A, B \in so(1,n)$ since $K_\rho$ is non-degenerate, $Ad(e^X) = Ad(e^X)$. Recall, the adjoint representation for $SO^+(1,n)$ is injective for $n \geq 2$. Then $e^X = e^X$ or $\rho(e^X) = e^{-X}$.

Let

$$p_0 = \{ A \in so(1,n) : \rho(e^A) = e^{-A} \}.$$ (15)

Clearly, $p \subseteq p_0$.

### 3 The case when $v = e_1$}

The next lemma shows the bilinear form $K_\rho$ is not positive-definite.

**Lemma 22** Let $a \in \mathbb{R}$, $b_1, b_2 \in \mathbb{R}^{n-1}$, and let $C \in so(n-1)$. Let $c_{ij}$ denote the $(i,j)$-entry of $C$, $1 \leq i, j, \leq n - 1$. Let $A \in so(1,n)$ be given by

$$A = \begin{pmatrix} a \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & b_1^T b_2 \\ b_1^T & b_2^T & C \end{pmatrix}.$$ 

Then

$$K_\rho(A, A) = 2(n-1) a^2 b_1 b_2 - b_1^2 b_2^2 + (n-1) \sum c_{ij}^2$$

where the sum is taken over all $1 \leq i, j, \leq n - 1$. 

12
Proof Notice,
\[
d\rho(A) = \begin{pmatrix} -a & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} b_1^T \\ -b_2^T \\ C \end{pmatrix}.
\]

Then
\[
Ad\rho(A) = \begin{pmatrix} -a^2 & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} b_1^T \\ b_2^T \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} b_1^T \\ -b_2^T \end{pmatrix} + C^2
\]

where \(*_1\) and \(*_2\) are other entries. The trace satisfies
\[
Tr(Ad\rho(A)) = -2\left(a^2 - b_1^T b_1 - b_2^T b_2\right) + Tr(C^2)
\]
\[
= -2\left(a^2 - b_1^T b_1 - b_2^T b_2\right) - \sum_{i,j=1}^{n-1} c_{ij}^2.
\]

Applying Lemma 16, part f), we find
\[
K_{\rho}(A,A) = -K_{\rho}(A,d\rho(A)) = -(n-1)Tr(Ad\rho(A)).
\]

Applying Lemma 20 to the case when \(v = e_1\), we find \(p\) consists of real matrices of the form
\[
A = \begin{pmatrix} 0 & a_1 & 0 & \cdots & 0 \\ a_1 & 0 & b_2 & \cdots & b_n \\ 0 & -b_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & -b_n & 0 & \cdots & 0 \end{pmatrix} \in p.
\]

Likewise, if \(v = e_1\), \(K\) consists of real matrices of the form
\[
\begin{pmatrix} 0 & a_2 & \cdots & a_n \\ 0 & 0 & \cdots & 0 \\ a_2 & 0 & c_{11} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & c_{n-1,1} & \cdots & c_{n-1,n-1} \end{pmatrix} \in K
\]

where \((c_{ij}) \in \mathfrak{o}(n-1)\).

Lemma 23 \(p = p_0\ if and only if n = 2\).

Proof From (15), we know \(p \subseteq p_0\). Let \(n = 2\), and let
\[
X = \begin{pmatrix} 0 & x_1 & x_3 \\ x_1 & 0 & x_2 \\ x_3 & -x_2 & 0 \end{pmatrix} \in \mathfrak{o}(1,2).
\]
Then
\[
X^2 = \begin{pmatrix}
  x_1^2 + x_3^2 & -x_2x_3 & x_1x_2 \\
  x_2x_3 & x_1^2 - x_2^2 & x_1x_3 \\
  -x_1x_2 & x_1x_3 & -x_2^2 + x_3^2
\end{pmatrix},
\]

We introduce the following real numbers that depend on \(X\).

1. \(\alpha_X = x_1^2 - x_2^2 + x_3^2\)
2. \(s_X = \sum_{k=0}^{\infty} \frac{(\alpha_X)^k}{(2k+1)!}\)
3. \(c_X = \sum_{k=1}^{\infty} \frac{(\alpha_X)^{k-1}}{(2k)!}\)

For each integer \(k \geq 1\), we find

1. \(X^{2k} = (\alpha_X)^{k-1}X^2\)
2. \(X^{2k+1} = (\alpha_X)^kX\).

Then we find
\[
e^X = I + s_XX + c_XX^2.
\] (17)

If \(\alpha_X = 0\), then identity (17) reduces to \(e^X = I + X + \frac{1}{2}X^2\). Note, because of the eigenvalues of \(d\rho\), we have
\[
d\rho(X) = \begin{pmatrix}
  0 & -x_1 & x_3 \\
  -x_1 & 0 & -x_2 \\
  x_3 & x_2 & 0
\end{pmatrix}.
\]

Suppose \(X \in p_0\). It suffices to show \(x_3 = 0\). For if \(x_3 = 0\), then \(X \in p\) and \(p_0 \subseteq p\).

By definition, \(e^{d\rho(X)} = e^{-X}\). Notice, \(\alpha_X = \alpha_{d\rho(X)} = \alpha_{-X}\), \(s_X \neq 0\), and \(c_X \neq 0\).

Since the (1, 2)-entries of \(e^{d\rho(X)}\) and \(e^{-X}\) are equal, we find
\[
1 - x_1s_X + x_2x_3c_X = 1 - x_1s_X - x_2x_3c_X.
\]

If \(x_3 \neq 0\), then \(x_2 = 0\). Likewise, since the (2, 3)-entries of \(e^{d\rho(X)}\) and \(e^{-X}\) are equal, we find
\[
1 - x_2s_X - x_1x_3c_X = 1 - x_2s_X + x_1x_3c_X.
\]

If \(x_3 \neq 0\), then \(x_1 = 0\). Thus, if \(x_3 \neq 0\), then \(X \in \mathbb{R}\). Then \(e^X = e^{d\rho(X)} = e^{-X}\).

Applying (17), we find
\[
\begin{pmatrix}
  1 + c_Xx_3^2 & 0 & s_Xx_3 \\
  0 & 0 & 0 \\
  s_Xx_3 & 0 & 1 + c_Xx_3^2
\end{pmatrix} = e^X = e^{-X} = \begin{pmatrix}
  1 + c_Xx_3^2 & 0 & -s_Xx_3 \\
  0 & 0 & 0 \\
  -s_Xx_3 & 0 & 1 + c_Xx_3^2
\end{pmatrix}
\]

The above identity implies \(x_3 = 0\) if we assume \(x_3 \neq 0\). A contradiction, thus, \(x_3 = 0\). If \(n = 2\), this proves \(p_0 = p\).
Conversely, let \( n \geq 3 \). Let \( X_\pi = 0 \oplus \left( \begin{array}{cc} 0 & \pi \\ -\pi & 0 \end{array} \right) \) be a block matrix. Then \( X_\pi \in \mathfrak{h}, X_\pi \notin \mathfrak{p} \), and \( e^{X_\pi} = I_{n-1} \oplus (-I_2) \). Consequently, \( X_\pi \in p_0 \). Hence, \( p \neq p_0 \). This completes the proof.

**Corollary 24** Let \( f : \mathfrak{p} \times K \to O^+(1,2) \) be defined by \( f(A,k) = e^{A}k, A \in \mathfrak{p}, k \in K \). Then \( f \) is surjective.

**Proof** Let \( W \in O^+(1,2) \). Then \( \widehat{WW} \in SO^+(1,2) \). Since the exponential mapping for \( SO^+(1,2) \) is surjective by Lemma 16, there exists \( X \in \mathfrak{so}(1,2) \) such that \( \widehat{WW} = e^X \). Then \( \widehat{X} = e^X \). Applying Lemma 23, we find \( X \in p_0 = p \). Since \( p \) is a subspace, \( -X/2 \in p \) and \( e^{-X/2} = e^{-X/2} \).

Let \( W = e^{X/2}Y \) for some \( Y \in O^+(1,n) \). Then

\[
Y \widehat{Y} = e^{-X/2}W \widehat{W}e^{-X/2} = e^{-X/2}e^Xe^{-X/2} = I.
\]

Thus, \( Y \in K \). Hence, \( f \) is surjective.

**Theorem 25** Let \( A \in \mathfrak{p} \) be given as in (16). Let \( \alpha = a_1^2 - \sum_{k=2}^{n} b_k^2 \). Then

a) \( e^A = I_{n+1} + A \left( \frac{\sinh(\sqrt{\alpha})}{\sqrt{\alpha}} \right) + A^2 \left( \frac{\cosh(\sqrt{\alpha})-1}{\alpha} \right), \) if \( \alpha \neq 0 \)

b) \( e^A = I_{n+1} + A + \frac{1}{2} A^2, \) if \( \alpha = 0 \).

c) For all \( \alpha \in \mathbb{R} \), the trace satisfies

\[
\text{Tr}(e^A) = (n+1) + 2(\cosh(\sqrt{\alpha}) - 1).
\]

**Proof** We find

\[
A^2 = \begin{pmatrix}
0 & a_1^2 & a_1 b_2 & \cdots & a_1 b_n \\
-\sum_{k=2}^{n} b_k^2 & 0 & a_1 b_2 & \cdots & 0 \\
0 & -b_2^2 & 0 & \cdots & -b_2 b_n \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & -b_2 b_n & \cdots & -b_2^2 & 0
\end{pmatrix}.
\]  

For each integer \( k \geq 1 \), we find

1. \( A^{2k} = \alpha^{k-1} A^2 \)

2. \( A^{2k+1} = \alpha^k A \).

Following the proof Lemma 23, statements a) and b) can be proved similarly. Then statement c) follows from a) and b).

\[\square\]
Corollary 26 The restriction of the exponential mapping to \( p \) is not injective.

Proof In Theorem 25, choose \( A \in p \) such that \( \alpha = -\pi^2 \). Then \( \sinh(\sqrt{\alpha}) = \sinh(i\pi) = 0 \) and \( \cosh(\sqrt{\alpha}) = \cosh(i\pi) = -1 \). By Theorem 25 and identity (18), for any such \( A \), we find \( e^A = I + \frac{2}{\pi^2} A^2 = e^{-A} \). Thus, the lemma is proved. \( \square \)

Let \( M_n(Q) \) denote the set of \( n \)-by-\( n \) matrices with rational entries.

Lemma 27 The restriction of the exponential mapping to \( p \cap M_{1+n}(Q) \) is injective.

Proof For \( i \in \{1, 2\} \), let

\[
A_i = \begin{pmatrix}
0 & a^i_1 & 0 & \cdots & 0 \\
a^i_1 & 0 & b^i_2 & \cdots & b^i_n \\
0 & -b^i_2 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & -b^i_n & 0 & \cdots & 0
\end{pmatrix} \in p \cap M_{1+n}(Q)
\]

and let \( \alpha_i = (a^i_1)^2 - \sum_{k=2}^n (b^i_k)^2 \neq 0 \). Suppose \( e^{A_1} = e^{A_2} \). We divide the proof into cases.

Applying Theorem 25, we have

\[
e^{A_i} = I_{n+1} + A^2_i \left( \frac{\cosh(\sqrt{\alpha_i}) - 1}{\alpha_i} \right) + A_i \left( \frac{\sinh(\sqrt{\alpha_i})}{\sqrt{\alpha_i}} \right)
\]

where \( \alpha_i = (a^i_1)^2 - \sum_{k=2}^n (b^i_k)^2 \neq 0 \).

Case 1: Suppose \( \alpha_1 = 0 \) and \( \alpha_2 = 0 \). Applying Theorem 25 and since \( e^{A_1} = e^{A_2} \), we find \( \frac{1}{2} A^2_1 + A_1 = \frac{1}{2} A^2_2 + A_2 \). Since the location of the zero entries of \( A_i \) and \( A^2_i \) do not coincide, we have \( A_1 = A_2 \).

Case 2: Suppose \( \alpha_1 > 0 \) and \( \alpha_2 = 0 \). Note, \( Tr(e^{A_1}) = Tr(e^{A_2}) \). Applying part c) of Theorem 25, we find \( 1 < \cosh(\sqrt{\alpha_1}) = \cosh(\sqrt{\alpha_2}) = 1 \). A contradiction.

Case 3: Suppose \( \alpha_1 = 0 \) and \( \alpha_2 < 0 \). Applying part c) of Theorem 25, we find

\[1 = \cos \sqrt{-\alpha_2} = \cos \sqrt{-\alpha_2} \leq 1.\]

Then \( \cos \sqrt{-\alpha_2} = 1 \), and consequently, \( \alpha_2 = -4\pi^2 n^2 \) for some integer \( n \). This is a contradiction since \( A_2 \) has only rational entries.

Case 4: Suppose \( \alpha_1, \alpha_2 > 0 \). Applying part c) of Theorem 25, we find \( \cosh(\sqrt{\alpha_1}) = \cosh(\sqrt{\alpha_2}) > 1 \). Since \( \cosh(x) \) is injective on \( (0, \infty) \), we obtain \( \alpha_1 = \alpha_2 \). In identity (18), we notice that the locations of the zero entries of \( A_i \) are the locations of the nonzero entries of \( A^2_i \). Since \( \sinh(\sqrt{\alpha_1}) = \sinh(\sqrt{\alpha_2}) > 0 \) and \( e^{A_1} = e^{A_2} \), we find

\[A_1 \left( \frac{\sinh(\sqrt{\alpha_1})}{\sqrt{\alpha_1}} \right) = A_2 \left( \frac{\sinh(\sqrt{\alpha_2})}{\sqrt{\alpha_2}} \right).\]
Thus, $A_1 = A_2$.

Case 5: Suppose $\alpha_1, \alpha_2 < 0$. Applying part c) of Theorem 25, we find

$$\cos \sqrt{-\alpha_1} = \cosh \sqrt{\alpha_1} = \cosh \sqrt{\alpha_2} = \cos \sqrt{-\alpha_2}.$$ 

Notice, $\sqrt{-\alpha_1} \neq n\pi$ for any integer $n$ since $\alpha_1 \in \mathbb{Q}$ and $\alpha_1 < 0$. Then $\cos \sqrt{-\alpha_1} \neq \pm 1$ and $\sin \sqrt{-\alpha_1} \neq 0$. Similarly, $\sin \sqrt{-\alpha_2} \neq 0$. Recall, the locations of the zero entries of $A_1$ are the locations of the nonzero entries of $A_1^2$. Since $e^{A_1} = e^{A_2}$, and by applying Theorem 25, we obtain

$$A_1 \sin \sqrt{-\alpha_1} = A_2 \sin \sqrt{-\alpha_2}$$

Then $A_1 = A_2$.

Case 6: Suppose $\alpha_1 > 0$ and $\alpha_2 < 0$. Applying part c) of Theorem 25, we find

$$1 < \cosh(\sqrt{-\alpha_1}) = \cos(\sqrt{-\alpha_2}) \leq 1.$$ 

A contradiction. Hence, the proof of the theorem is complete. 

\[ \square \]

**Lemma 28** Let $n \geq 2$. Let $A_1, A_2 \in \mathfrak{p} \cap M_{1+n}(\mathbb{Q})$, and let $k_1, k_2 \in K$. Then $e^{A_1} k_1 = e^{A_2} k_2$ if and only if $A_1 = A_2$ and $k_1 = k_2$.

**Proof** If $e^{A_1} k_1 = e^{A_2} k_2$, then $e^{-A_2} e^{A_1} = k_2 k_1^{-1}$. Recall, $Ad(k)$ is $K_\rho$-orthogonal for all $k \in K$ by (??), and $Ad(e^A)$ is $K_\rho$-symmetric for all $A \in \mathfrak{p}$. For all $v, w \in \sigma(1, n)$, we obtain

$$K_\rho(Ad(e^{-A_2} e^{A_1}) v, w) = K_\rho(Ad(k_2 k_1^{-1}) v, w)$$

$$= K_\rho(v, Ad(k_2 k_1^{-1})^{-1} w)$$

$$= K_\rho(v, Ad(e^{-A_2} e^{A_1})^{-1} w)$$

$$= K_\rho(v, Ad(e^{-A_1}) Ad(e^{A_2}) w)$$

$$= K_\rho(Ad(e^{-A_1}) v, Ad(e^{A_2}) w)$$

$$= K_\rho(Ad(e^{A_2} e^{-A_1}) v, w)$$

Since $K_\rho$ is a non-degenerate bilinear form, $Ad(e^{-A_2} e^{A_1}) = Ad(e^{A_2} e^{-A_1})$. Note, the kernel of the restriction of the adjoint representation $Ad$ to $SO^+(1, n)$ is $\{I\}$, which is the center of $SO^+(1, n)$ for $n \geq 2$. Then $e^{-A_2} e^{A_1} = e^{A_2} e^{-A_1}$ or $e^{2A_2} = e^{2A_1}$. Then $A_1 = A_2$ by Lemma 27. Consequently, $k_1 = k_2$. This proves the necessary direction of the theorem.

\[ \square \]
4 Example: $\mathfrak{o}(1, 3)$

Let $n = 3$. Let $L = \text{diag}(1, -1, 1, 1)$ be a diagonal matrix. If $K_\rho(e^{ad(X)} A, B) = K_\rho(A, e^{ad(X)} B)$ for all $A, B \in \mathfrak{o}(1, 3)$ it does not follow that $X \in \mathfrak{p}$. For instance, if $d_3^2 + d_4^2 - f^2 = -(k\pi)^2$ for any integer $k$, and

$$X = \begin{pmatrix} 0 & 0 & d_3 & d_4 \\ 0 & 0 & 0 & 0 \\ d_3 & 0 & 0 & f \\ d_4 & 0 & -f & 0 \end{pmatrix} \in \mathfrak{r}$$

we find $Tr(e^X A e^{-X} LBL) = Tr(e^X B e^{-X} LAL)$ for all $A, B \in \mathfrak{o}(1, 3)$ by applying Mathematica. Moreover, if $k$ is an even integer, then $e^X = I$. In particular, if

$$X = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \pi \\ 0 & 0 & -\pi & 0 \end{pmatrix} \in \mathfrak{r}$$

then

$$\widetilde{e}^X = e^X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

but

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \widetilde{e}^{X/2} \neq e^{X/2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

5 Polar decomposition

We review the polar decomposition for $O^+(1, n)$. Let $a_0 \geq 1$, $b, c \in \mathbb{R}^n$, and let $A_0 \in M_n(\mathbb{R})$. Let

$$A = \begin{pmatrix} a_0 & b^T \\ c & A_0 \end{pmatrix}. \quad (19)$$

We know $A \in O^+(1, n)$ if and only if $A^T J A = J$. The identity $A^T J A = J$ is equivalent to

$$\begin{pmatrix} a_0^2 - c^T c & a_0 b^T - c^T A_0 \\ a_0 b - A_0^T c & b b^T - A_0^T A_0 \end{pmatrix} = J. \quad (20)$$

From (20), we notice that $c \neq 0$ if and only if $a > 1$. We verify directly that

$$A^{-1} = J A^T J = \begin{pmatrix} a_0 & -c^T \\ -b & A_0^T \end{pmatrix}. \quad (21)$$
Since \( J \in O^+(1, n) \), clearly \( A^T \in O^+(1, n) \). Consider the symmetric matrix

\[
S = \begin{pmatrix} a_0 & c^T \\ c & I_n + \frac{cc^T}{1+a_0} \end{pmatrix}.
\] (21)

If \( c = 0 \), then \( S = I_{n+1} \). If \( c \neq 0 \), we show \( S \) is positive-definite also. Clearly, if \( w \in c^+ \), we find \( Sw = w \). Consider the vectors

1. \( v = \frac{1}{\sqrt{2}} (1, \frac{c}{\sqrt{a_0-1}})^T \in \mathbb{R}^{n+1} \)
2. \( w = \frac{1}{\sqrt{2}} (-1, \frac{c}{\sqrt{a_0-1}})^T \in \mathbb{R}^{n+1} \)

From (20), we find \( v \) and \( w \) are unit vectors. i.e., \( vv^T = 1 = \ww^T \). Moreover,

1. \( Sv = (a_0 + \sqrt{a_0^2 - 1})v \)
2. \( Sw = (a_0 - \sqrt{a_0^2 - 1})w \)

Notice, \( a_0 \pm \sqrt{a_0^2 - 1} > 0 \). This shows \( S \) is a positive-definite symmetric real matrix. From the eigenvalues of \( S \), we find \( \det(S) = 1 \). Moreover, it can be verified that \( S^TJS = J \). Then \( S \in SO^+(1, n) \). Moreover, from (20), we find \( AA^T = S^2 \). Let \( A = SR \) for some \( R \in O^+(1, n) \). Since \( (S^{-1})^T = S^{-1} \). Then

\[
RR^T = S^{-1}AA^T(S^{-1})^T = I_{1,n}.
\]

Then \( R \) is an orthogonal matrix, and we find

\[
R = \begin{pmatrix} 1 & 0 \\ 0 & A_0 - \frac{cb^T}{1+a_0} \end{pmatrix} \in O(1 + n). \] (22)

**Lemma 29** Let \( A, S, R \) be given as in (19), (21), and (22). Then \( A = SR \), \( S \) is a positive-definite symmetric matrix, and \( R \in O(1 + n) \) is an orthogonal matrix.

We recall the group isomorphism in (8). If \( x = (x_0, \ldots, x_n)^T \in Q \), let \( x' = F_0(x) = \frac{1}{1+x_0}(x_1, \ldots, x_n)^T \in B \). For matrix \( A \) in (19), if \( A_0 \in O(n) \), then \( a_0 = 1 \) and \( b = c = 0 \). Consequently,

\[
\begin{align*}
F(A)(x') &= F_0A(x) \\
&= F_0(w)
\end{align*}
\]

where \( w^T = (x_0, (x_1, \ldots, x_n)A_0^T) \). Then \( F(A)(x') = A_0(x') \). Thus, if \( A_0 \in O(n) \) and \( A = 1 \oplus A_0 \in O^+(1, n) \), then

\[
F(1 \oplus A_0) = A_0 \in GM(B).
\] (23)

**Lemma 30** Let \( t \in \mathbb{R}, a = \tanh(t)c_1 \in B \), and let \( r = |\text{csch}(t)| \). Then

\[
T_a = F\left( \begin{pmatrix} \cosh 2t & -\sinh 2t \\ -\sinh 2t & \cosh 2t \end{pmatrix} \oplus I_{n-1} \right).
\]
Finally, applying (23), we find
\[ F \left( \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \oplus I_{n-1} \right) = f^{e_1} \in GM(B). \]

In [1, p. 52-53]], it is shown that
\[ \sigma_a = F \left( \left( \begin{array}{cc} \cosh 2t & \sinh 2t \\ -\sinh 2t & -\cosh 2t \end{array} \right) \oplus I_{n-1} \right). \]

Finally,
\[
T_a = \sigma_a r_a = F \left( \left( \begin{array}{cc} \cosh 2t & \sinh 2t \\ -\sinh 2t & -\cosh 2t \end{array} \right) \oplus I_{n-1} \right) \left( \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \oplus I_{n-1} \right) = F \left( \left( \begin{array}{cc} \cosh 2t & \sinh 2t \\ -\sinh 2t & -\cosh 2t \end{array} \right) \oplus I_{n-1} \right).
\]

Proof Since \( 1 + r_a^2 = |a|^2 \), the sphere \( S(a^1, r_a) \) is orthogonal to \( S^1 \). Let \( \sigma_a \) be the reflection about the sphere \( S(a^1, r_a) \). Recall, \( T_a = \sigma_a f_a/|a| \). Clearly, \( f_a/|a| = f^{e_1} \).

Let \( S \) denote the set of positive-definite symmetric matrices \( R \) in \( O^+(1, n) \)

**Lemma 31** Let \( \phi \in O(n) \), \( a = \tanh(t) \phi(e_1) \in B \), \( a_0 = \cosh(2t) \), and let \( c = -\sinh(2t) \phi(e_1) \). Then

1. \( F \left( \left( \begin{array}{cc} a_0 & c^T \\ c & I_n + \frac{cc^T}{1+a_0} \end{array} \right) \right) = T_a \)

2. \( F \left( \left( \begin{array}{cc} 1+|a|^2 & 2a^T \\ \frac{2a^T}{|a|^2-1} & I_n + \frac{2a^T a}{1-|a|^2} \end{array} \right) \right) = T_a \).

In particular, \( S = \{ T_a : a \in B \} \).
References


