TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 364, Number 9, September 2012, Pages 5015–5033
S 0002-9947(2012)05639-X
Article electronically published on April 5, 2012

SPACE FORM ISOMETRIES AS COMMUTATORS AND PRODUCTS OF INVOLUTIONS

ARA BASMAJIAN AND BERNARD MASKIT

Abstract. In dimensions 2 and 3 it is well known that given two orientation-preserving hyperbolic isometries that generate a non-elementary group, one can find a triple of involutions so that each isometry can be expressed as a product of two of the three involutions; in this case, we say that the isometries are *linked*.

In this paper, we investigate the extent to which a pair of isometries in higher dimensions can be linked. This question separates naturally into two parts. In the first part, we determine the least number of involutions needed to express an isometry as a product, and give two applications of our results; the second part is devoted to the question of linking.

In general, the commutator (involution) length of a group element is the least number of elements needed to express that element as a product of commutators (involutions), and the commutator (involution) length of the group is the supremum over all commutator (involution) lengths. Let $\mathcal{G}^n$ be the group of orientation-preserving isometries of one of the space forms, the $(n-1)$-sphere, Euclidean n-space, hyperbolic n-space. For $n \geq 3$, we show that the commutator length of $\mathcal{G}^n$ is 1; i.e., every element of $\mathcal{G}^n$ is a commutator. We also show that every element of $\mathcal{G}^n$ can be written as a product of two involutions, not necessarily orientation-preserving; and, depending on the particular space and on the congruence class of $n \mod 4$, the involution length of $\mathcal{G}^n$ is either 2 or 3.

In the second part of the paper, we show that all pairs in SO^4 are linked but that the generic pair in the orientation-preserving isometries of hyperbolic 4-space or in $\mathcal{G}^n$, $n \geq 5$, is not.

1. Introduction

As usual, SO^n denotes the group of orientation-preserving isometries of the $(n-1)$-sphere. We denote the group of orientation-preserving isometries of hyperbolic n-space by $\mathbb{M}^n$, the full group by $\widetilde{\mathbb{M}}^n$, and the group of orientation-preserving isometries of Euclidean n-space by $\mathbb{A}^n$. In general, for any one of these space forms, we denote the group of orientation-preserving isometries by $\mathcal{G}^n$, where, unless specifically stated otherwise, we require $n \geq 3$. The full group is denoted $\widetilde{\mathcal{G}}^n$.

We will at different times need to talk about the geometry of $\mathbb{E}^n$, the n-dimensional Euclidean space whose isometries consist of rotations and translations, and at other times about the geometry of $\mathbb{R}^n$, the real n-dimensional vector space. We will usually think of SO^n as a group of matrices.

Received by the editors January 18, 2011 and, in revised form, May 30, 2011.
2010 *Mathematics Subject Classification.* Primary 51M10; Secondary 30F40.
The first author was supported in part by a PSC-CUNY Grant.

A non-trivial isometry of order 2 is an involution. An involution may either preserve or reverse orientation; where appropriate, we will specify whether or not a given involution preserves orientation. We reserve the symbols α, β and γ for involutions.

An *elementary* group of Möbius transformations is one that contains a finite index subgroup that fixes either one point or a pair of points in $\bar{\mathbb{H}}^n$. We recall the following well-known fact.

Theoerem ([3]). *Let $A, B \in \mathbb{M}^n$, $n = 2, 3$, generate a non-elementary group. Then there exist involutions, α, β and γ, so that $A = \alpha\beta$ and $B = \beta\gamma$, from which it follows that $AB = \alpha\gamma$ and the commutator $[A, B] = (\alpha\gamma\beta)^2$. If $n = 3$, the involutions can be chosen so as to preserve orientation.*

For an algebraic proof the reader is referred to the article by Goldman [2]. The above separates naturally into two parts with the first being whether every isometry can be written as a commutator and/or as a product of two involutions; the second part being whether every pair (A, B) of such isometries is *linked*; that is, whether there are three involutions, α, β, γ, so that $A = \alpha\beta$ and $B = \beta\gamma$.

Let S be a set of generators for the abstract group G. The *length* of an element g in G (with respect to S) is the minimal number of elements of S needed to express g as a product. The supremum of the element lengths is called the length of G (with respect to S). When the generators are involutions (resp. commutators) in G, we call this length the *involution* (resp. *commutator*) *length* of the group, provided of course that G can be generated by involutions (resp. commutators).

Let $A, B \in G$. We say that the pair (A, B) is *linked* in G if there exist involutions α, β and γ in G so that $A = \alpha\beta$ and $B = \beta\gamma$; in this case, we say that β *links* the pair (A, B).

Theorem 1.1. *Assume $n \geq 3$. The involution length of $\mathbb{M}^n$ is,*

$$\begin{cases} 2, & \text{if } n \equiv 0 \mod 4 \text{ or } n \equiv 3 \mod 4. \\ 3, & \text{if } n \equiv 1 \mod 4 \text{ or } n \equiv 2 \mod 4. \end{cases} \tag{1}$$

Furthermore, if $n \equiv 1 \mod 4$ or $n \equiv 2 \mod 4$, then any $A \in \mathbb{M}^n$ is the product of two orientation-reversing involutions.

Similar results, that the involution length is either 2 or 3, depending on congruence mod 4, hold for SO^n, and $\mathbb{A}^n$.

As a consequence we reach two of our goals:

Corollary 1.2. *The commutator length of $\mathcal{G}^n$, $n \geq 3$, is one.*

Corollary 1.3. *For $n \geq 2$, every orientation-preserving element of $\widetilde{\mathbb{M}}^n$ (O^n, $\widetilde{\mathbb{A}}^n$) has involution length 2.*

We remark that, in dimension 2, only hyperbolic elements of $\mathbb{M}^2$ can be written as the composition of two orientation-preserving involutions. Similarly, in dimension 3, the elements of $\mathbb{M}^3$ that can be written as the composition of two orientation-reversing involutions are exactly the elliptic, parabolic, pure hyperbolic, and reverse

hyperbolic (i.e., conjugate to a transformation of the form $z \mapsto -\lambda z$, $\lambda > 1$) transformations.

The fact that every non-elementary pair of elements of $\mathbb{M}^2$ and of $\mathbb{M}^3$ is linked does generalize to certain special cases in hyperbolic dimension 4.

Theorem 1.4. *Every pair of elements of SO^4 is linked.*

This result however does not generalize further.

Theorem 1.5.
(1) *For $n \geq 3$, almost every pair of elements of $\mathbb{A}^n$ is not linked.*
(2) *For $n \geq 4$, almost every pair of elements of $\mathbb{M}^n$ is not linked.*
(3) *For $n \geq 5$, almost every pair of elements of SO^n is not linked.*

We remark that in fact the non-linking above takes place in the full group $\widetilde{\mathcal{G}}^n$ and the almost every language means on a set of full measure in $\mathcal{G}^n \times \mathcal{G}^n$.

The main tool in the proof of these facts is an investigation of common perpendicular subspaces between two planes—that is, subspaces of dimension 2 in $\mathbb{R}^n$. Roughly speaking, two subspaces with non-trivial intersection are perpendicular if they are otherwise orthogonal.

For all $n > 0$, there are natural embeddings of $\mathbb{M}^n$ into $\mathbb{M}^{n+1}$, or SO^n into SO^{n+1}, or $\mathbb{A}^n$ into $\mathbb{A}^{n+1}$; in most cases, there are several such embeddings, but their images are all conjugate.

An element $A \in \mathbb{M}^n$ (SO^n, $\mathbb{A}^n$) is an *extension* if it preserves a co-dimension 1 totally geodesic subspace of $\mathbb{H}^n$ (S^{n-1}, $\mathbb{E}^n$). If A is an extension and A preserves orientation on this subspace, then A is a *strict* extension.

In section 2, we find all elements of SO^n, $n > 2$, that can be written as the composition of two orientation-preserving involutions and as the composition of two orientation-reversing involutions. We use this information to show that every element is a commutator and to find all elements that are commutators of two involutions. As a byproduct, we determine the involution length of SO^n. Then, in section 3, we apply these results to obtain the corresponding results for $\mathbb{A}^n$. In section 4, we apply the results of the preceding two sections to obtain the corresponding results for $\mathbb{M}^n$. The work in the earlier sections is then put together in section 5 to prove Theorem 1.1. Sections 6-9 address the linking question. Specifically, in section 6 we investigate the notion of planes in higher dimensions having a common perpendicular. In section 7, we relate the property of linking in SO^n with the existence of common perpendiculars, proving Theorem 1.5 for SO^n, $n \geq 5$, and Theorem 1.4. In sections 8 and 9 the property of linking is related to elements of $\mathbb{M}^n$ and $\mathbb{A}^n$, respectively. Finally we put the work in the previous sections together to prove Theorem 1.5 in section 10, finishing with some observations.

We require $n \geq 3$ throughout. Our commutator results do not hold for SO^2, which is abelian, or for $\mathbb{A}^2$, which is not equal to its commutator subgroup. We remark that it is true that every element of $\mathbb{M}^2$ is a commutator, although our methods do not yield this result, which is easily shown using computations in $PSL(2, \mathbb{R})$. We also incidentally remark that there is exactly one element, -1, in $SL(2, \mathbb{R})$ that is not a commutator.

Factoring elements into involutions or commutators has been studied from a mostly algebraic view by, among others, Pasiencier and Wang [4], Ree [6], Thompson [7], and Wonenburger [8]. For work relating discreteness conditions and factoring elements, see Puri [5].

2. Isometries of spheres as commutators and products of involutions

Let $A \in SO^n$; we consider A as acting on $\mathbb{E}^n$. Then, by choosing appropriate orthonormal coordinates for $\mathbb{E}^n$, we can write the matrix for A in the usual normal form. That is, every entry in the matrix is zero, except for m consecutive 2×2 blocks down the main diagonal, followed by $2p$ entries of -1 on the main diagonal, followed by $q = n - 2m - 2p$ entries of $+1$ on the main diagonal. For each of the m 2×2 blocks, there is an invariant plane P_i on which A acts as a rotation; we write the angle of rotation in the plane P_i as θ_i. Since we have separated out the diagonal entries of ± 1, the rotation angle $\theta_i \neq 0, \pi$.

We remark that it is an easy consequence of this normal form that every $A \in SO^n$ has a square root.

Proposition 2.1. *A is an extension if and only if $n > 2m$; that is, A has a real eigenvalue. Further, A is a strict extension if and only if $q > 0$; i.e., $+1$ is an eigenvalue of A.*

Proof. It is immediate from the definition that if A is an extension, then it preserves the line orthogonal to the invariant hyperplane, and hence has a real eigenvalue. Further, since A is orientation-preserving, it preserves direction on this line if and only if it preserves orientation on the hyperplane. Conversely, if A has a real eigenvalue, then, in its action on $\mathbb{E}^n$, it has an invariant line. The orthogonal complement to this line is an invariant hyperplane. A preserves orientation on this line, and hence on its orthogonal complement, if and only if the real eigenvalue is equal to $+1$. □

Proposition 2.2. *If $A \in SO^n$ is not an extension, then n is even.*

Proof. This follows at once from the normal form for an orthogonal matrix. □

Theorem 2.3. *If $A \in SO^n$ is an extension (in particular, when n is odd), then A can be written as both a composition of two orientation-preserving involutions and as a composition of two orientation-reversing involutions.*

Proof. We first define the involutions, α and β on the planes, P_i, $i = 1, \ldots, m$. For each plane P_i, we write $\alpha|P_i(z) = \bar{z}$ and $\beta|P_i(z) = e^{i\theta_i}\bar{z}$.

We now have defined α and β in each of the m 2×2 blocks. We still need to define them on the orthogonal complement.

We know that $p + q > 0$. We first take up the case that $p > 0$. In this case, we first copy all entries of $+1$ in the matrix for A into the corresponding places on the main diagonal for the matrices of α and β. For our first choice of α, we copy the odd numbered entries of -1 on the main diagonal of A into the corresponding places in the matrix for α, while replacing the corresponding even numbered entries by $+1$. We likewise copy the even numbered entries of -1 in the matrix for A into the matrix for β, while replacing the odd numbered entries by $+1$. Depending on the parity of $m+p$, the resulting involutions, α and β, either both preserve or both reverse orientation. We note that the last q entries down the main diagonal will be $+1$ for both α and β. We also observe that α and β are conjugate involutions with $A = \alpha\beta$.

We obtain a different choice of α and β, with reversed orientation by looking at one of the entries of -1 in the matrix for A, and switching the two corresponding

entries for α and β. That is, we obtain new matrices, α and β, with orientation opposite to that obtained above, by multiplying the entries in both α and β in the $(2m+1)$-st position on the main diagonal by -1. In this case, we still have $A = \alpha\beta$, but now these involutions are not conjugate, as they have fixed point sets of different dimensions.

We next take up the case that $p = 0$ and $q > 0$. In this case, we define α and β on the 2×2 blocks exactly as above. For one choice of α and β, we reproduce the entries of $+1$ on the main diagonal of A; for the other choice, we replace the first $+1$ by entries of -1 in both α and β. We note that, in this case, both choices yield conjugate involutions. □

Proposition 2.4. *Let $A = \alpha\beta \in SO^n$. If P_i is an A-invariant subspace of $\mathbb{E}^n$, then $\alpha(P_i) = \beta(P_i) = P_j$ is also an A-invariant subspace.*

Proof. Since $A(P_i) = \alpha\beta(P_i) = P_i$, $\alpha(P_i)$ is kept invariant by $\alpha A\alpha^{-1} = \beta\alpha = A^{-1}$. Similarly with $\beta(P_i)$. □

Theorem 2.5. *Assume $A \in SO^n$ is not an extension.*

1. *$A = \alpha\beta$, where α and β are orientation-preserving if and only if $n \equiv 0 \mod 4$.*
2. *$A = \alpha\beta$, where α and β are orientation-reversing if and only if $n \equiv 2 \mod 4$.*

Proof. Since A is not an extension, $p = q = 0$, and $n = 2m$. For each $i = 1, \ldots, m$, the action of A on the plane P_i is a non-trivial rotation through an angle different from π. We can find involutions, α_i and β_i, acting on P_i, so that $A|P_i = \alpha_i\beta_i$, if and only if α_i and β_i both reverse orientation. Hence we can define the involutions α and β, by $\alpha|P_i = \alpha_i$, $\beta|P_i = \beta_i$, $i = 1, \ldots, m$. Of course, if m is even, then α and β both preserve orientation, while they reverse orientation if m is odd. This completes the proof that we can find the requisite involutions.

If we can write $A = \alpha\beta$, then, for each invariant plane P_i, there is a perhaps different invariant plane, P_j, so that $\alpha(P_i) = \beta(P_i) = P_j$. Since α and β are involutions, we must also have that $\alpha(P_j) = \beta(P_j) = P_i$. If $P_i = P_j$, then $\alpha|P_i$ and $\beta|P_i$ both necessarily reverse orientation. If $P_i \neq P_j$, then α and β both either preserve or reverse orientation on both P_i and P_j. It follows that, of necessity, if m is even, α and β both preserve orientation, while if m is odd, they both reverse orientation. □

Proposition 2.6. *$A \in SO^n$ is a strict extension if and only if there exists $B \in SO^n$, where B is a strict extension and $B^2 = A$.*

Proof. If A is a strict extension, then let A' be the restriction of A to the invariant hyperplane, let B' be an orientation-preserving square root of A', and let B be its strict extension. Then $B^2 = A$. The converse is immediate. □

We remark that if B is an extension, then B^2 is either trivial or a strict extension.

Theorem 2.7. *$A \in SO^n$, $n > 2$, is the commutator of two orientation-preserving involutions if and only if either A is a strict extension or $n \equiv 0 \mod 4$.*

Proof. First assume that A is a strict extension. Then there is a strict extension $B \in SO^n$, with $B^2 = A$. Write $B = \alpha\beta$, where these are orientation-preserving involutions. Then $A = [\alpha, \beta]$.

Next, assume that $n \equiv 0 \mod 4$, and that A is not a strict extension. Let B be some square root of A. Note that since A is not a strict extension, B is not an extension. By Theorem 2.5, we can write B as the composition of two orientation-preserving involutions, $B = \alpha\beta$. As above, $A = [\alpha, \beta]$.

Conversely, assume that $A = [\alpha, \beta]$, where α and β are orientation-preserving involutions. Then $B = \alpha\beta$ is a square root of A. By Theorem 2.5, either B is an extension or $n \equiv 0 \mod 4$. If B is an extension, then $A = B^2$ is a strict extension. □

Theorem 2.8. *If $A = [\alpha', \beta'] \in SO^n$, where α' and β' are involutions, then there are conjugate involutions α and β, so that $A = [\alpha, \beta]$.*

Proof. We know from the above that either A is a strict extension, or $n \equiv 0 \mod 4$. In either case, we write the matrix for the normal form of A as $m' = (m + p)$ 2×2 boxes down the main diagonal, followed by q entries of $+1$ on the main diagonal; that is, we pair the entries of -1 on the main diagonal and consider each such pair as a 2×2 box. Then A has a square root, B, with the same normal form structure, and the same invariant planes, $P_1, \ldots, P_{m'}$. Let α_i and β_i be conjugate orientation-reversing involutions in O^2, keeping the plane P_i invariant, so that $B|P_i = \alpha_i\beta_i$. For $i = 1, \ldots, m'$, define $\alpha|P_i = \alpha_i$, and $\beta|P_i = \beta_i$. If m' is even, set α and β equal to the identity on the subspace orthogonal to all P_i, $i = 1, \ldots, m'$. If m' is odd, then, since either A is an extension, or $n \equiv 0 \mod 4$, we must have $q > 0$. Pick a line, L, orthogonal to all P_i, $i = 1, \ldots, m'$, set $\alpha|L = \beta|L = -1$, and then set α and β equal to the identity on the orthogonal subspace. We have constructed α and β so that they are conjugate, and so that $\alpha\beta = \alpha'\beta'$. □

Theorem 2.9. *Let $A \in SO^n$, $n > 2$, where A cannot be written in the form $A = \alpha\beta$, where α and β preserve orientation. Then there exist orientation-preserving involutions, α, β and γ, so that $A = \alpha\beta\gamma$.*

Proof. We already know from Theorems 2.3 and 2.5 that this can occur only if A is not an extension and $n \equiv 2 \mod 4$. Further, we know from Proposition 2.1 that, in normal form, the matrix for A has m 2×2 boxes down the main diagonal, and no real eigenvalues. Since $n > 2$, m is odd and ≥ 2. For each $i = 1, \ldots, m$, we write the action of A on the plane P_i as $A|P_i = \alpha_i\beta_i$, where α_i and β_i are orientation-reversing involutions. We now define the involutions α, β and γ as follows:

$$\begin{aligned}
&\alpha|P_1 = \alpha_1, \quad \alpha|P_2 = 1, \quad \alpha|P_i = \alpha_i,\ i = 3, \ldots, m.\\
&\beta|P_1 = 1, \quad \beta|P_2 = \alpha_2, \quad \beta|P_i = \beta_i,\ i = 3, \ldots, m.\\
&\gamma|P_1 = \beta_1, \quad \gamma|P_2 = \beta_2, \quad \gamma|P_i = 1,\ i = 3, \ldots, m.
\end{aligned}$$

□

To summarize:

Theorem 2.10. *Assume $n \geq 3$. The involution length of SO^n is*

$$\begin{cases} 2, & \text{if } n \not\equiv 2 \mod 4.\\ 3, & \text{if } n \equiv 2 \mod 4. \end{cases} \tag{2}$$

Furthermore, when $n \equiv 2 \mod 4$ any $A \in SO^n$ is the product of two orientation reversing involutions.

We will also need the following variation of Theorem 2.9 for the parabolic and hyperbolic cases.

Theorem 2.11. *Let $A \in SO^n$, $n > 2$, where A cannot be written in the form $A = \alpha\beta$, where α and β reverse orientation. Then there exist involutions, α, β and γ, where α and β reverse orientation, and γ is orientation-preserving, so that $A = \alpha\beta\gamma$.*

Proof. The proof is essentially the same as that given above. As above, the normal form for the matrix for A has m 2×2 boxes, and no real eigenvalues; however, now m is even. We write α, β and γ exactly as above, and observe that, in this case, α and β reverse orientation, while γ preserves orientation. □

Theorem 2.12. *Let $A \in SO^n$, $n > 2$. Then A is a commutator.*

Proof. Choose $B \in SO^n$ so that $B^2 = A$. If B can be written as the composition of two involutions, $\alpha, \beta \in SO^n$, then $A = [\alpha, \beta]$. If not, then by Theorem 2.9, there are involutions α, β and γ in SO^n so that $B = \alpha\beta\gamma$. Then $A = (\alpha\beta\gamma)^2 = [\alpha\gamma, \gamma\beta]$. □

3. Euclidean isometries as commutators and products of involutions

In this section, we find all elements of $\mathbb{A}^n$ that can be written as the composition of two orientation-preserving involutions, or of two orientation-reversing involutions, and as above, we both show that every element is a commutator, and, for the cases where an element cannot be written as a product of two involutions, we show that it can be written as a product of three involutions.

In general, we restrict our attention to the case, $n > 2$, since $\mathbb{A}^2$ is not equal to its commutator subgroup. We do note however, that for $n = 2$, every parabolic element can be written as a product of two involutions, that every elliptic element can be written as a product of two orientation-reversing involutions, and that no non-trivial elliptic element, other than an involution, can be written as a product of any number of orientation-preserving involutions; that is, the involution length of $\mathbb{A}^2$ is infinite.

Since a parabolic transformation acting on hyperbolic n-space is conjugate to an isometry of $\mathbb{E}^{n-1}$, in order to avoid confusion, we refer here to Euclidean space as $\mathbb{E}^m$, and its orientation-preserving isometry group as $\mathbb{A}^m$, where $m = n - 1$. It is well known that every isometry of $\mathbb{E}^m$ can be written uniquely in the form $A = TR$, where T is a translation of the form $T(x) = x + x_0$, and $R \in O^m$. The isometry A can also be written, again uniquely, in the form $A = RT'$, where T' is a perhaps different translation. It is well known that every isometry is conjugate to an isometry in *normal form* $A = TR = RT$. It is clear that an isometry is in normal form if and only if $R(x_0) = x_0$, where $T(x) = x + x_0$. For a transformation in normal form, R is called the *rotational part* of A, $(R = \mathcal{R}(A))$, and T is called the *translational part* of A $(T = \mathcal{T}(A))$.

Since our results are all conjugation invariant, we assume from here on without loss of generality that any given transformation is in normal form: $A = RT = TR$, with $T(0) = x_0$ and $R(x_0) = x_0$. Observe that the hyperplane, H^{m-1}, passing through the origin and orthogonal to x_0, is invariant under R; define the *restricted rotational part*, $R_0 \in O^{m-1}$, by $R_0 = R|H^{m-1}$. Note that $R_0 \in SO^m$ if and only if $R \in SO^m$, which in turn occurs if and only if A preserves orientation. We also reserve the symbol x_0 for $T(0)$, and we denote the line $\{tx_0\}$ by L_0.

The transformation A is elliptic if it has a fixed point in $\mathbb{E}^m$; it is parabolic otherwise. It is clear that A in normal form is elliptic if and only if $\mathcal{T}(A) = 1$.

In this and subsequent sections, we will use the term *orthogonal* for its usual meaning concerning vectors and vector subspaces. We will use the term *perpendicular* in its usual sense as concerns Euclidean and/or hyperbolic flats.

In what follows, we will denote the fixed point set of the element $A \in \mathbb{A}^m$ by $Fix(A)$. Note that if this is not empty, then it is either a point or a translate of a non-empty vector subspace of $\mathbb{E}^m$. We say that the line L is *perpendicular* to $Fix(A)$ if it meets $Fix(A)$ in exactly one point, and if, in the case that $Fix(A)$ consists of more than one point, L is indeed perpendicular to $Fix(A)$.

It is essentially immediate from the definition that if the line L is perpendicular to $Fix(\alpha)$, where α is an involution, then $\alpha(L) = -L$; i.e., α preserves the line and reverses orientation on it.

Proposition 3.1. *Let $\alpha \neq \beta$ be involutions. Then $A = \alpha\beta$ is elliptic if and only if $Fix(\alpha) \cap Fix(\beta) \neq \emptyset$.*

Proof. If $Fix(\alpha) \cap Fix(\beta) \neq \emptyset$, then $A = \alpha\beta$ has a fixed point, and so is elliptic.

If $Fix(\alpha) \cap Fix(\beta) = \emptyset$, then let L be a shortest line between $Fix(\alpha)$ and $Fix(\beta)$. It is clear that L is perpendicular to both $Fix(\alpha)$ and $Fix(\beta)$, that it is preserved by $A = \alpha\beta$, and that A acts without fixed points on L. In fact, for any $x \in L$, $A^p(x)$ diverges to infinity as p increases. Since A is an isometry, it follows that A cannot have a fixed point, and so is parabolic. □

We now know that an elliptic element $A \in \mathbb{A}^m$ can be written as the composition, $A = \alpha\beta$ if and only if A, α and β all share a fixed point. Hence we can assert that an elliptic element $A \in \mathbb{A}^m$ can be written as $A = \alpha\beta$ if and only if it is conjugate to an element of SO^m that can be so written. We can also assert that every elliptic element of $\mathbb{A}^m$ is a commutator.

We next turn to the parabolic case. Here we say that A is an *extension* if its restricted rotational part R_0 is an extension. A is a *strict* extension if R_0 is a strict extension.

Proposition 3.2. *Let L be an invariant line for the parabolic transformation, $A = RT = TR$. Then L is of the form $x + tx_0$, where $x \in Fix(R)$; in particular, L and L_0 are parallel.*

Proof. Let x be some point on L, and let $A(x) = x + y$. Then $A^{-1}(x) = x - y$. Easy computations show that x is an eigenvector of $R + R^{-1}$ with eigenvalue $+2$, from which it follows that $R(x) = x$; it then follows that $y = x_0$. □

Proposition 3.3. *Let $A = RT = TR \in \mathbb{A}^m$ be parabolic. Then A can be written as $A = \alpha\beta$, where α and β both preserve (resp. reverse) orientation, if and only if the restricted rotational part of A can be written as the composition of two involutions that reverse (resp. preserve) orientation.*

Proof. Write $\mathbb{E}^m = L \oplus V$, where L is a line kept invariant by A, R and T, and where V is the orthogonal complement, so that R_0 acts on V. If we can write $R_0 = \alpha_0\beta_0$, then define α and β by $\alpha|V = \alpha_0$, $\alpha|L = -1$, $\beta|V = \beta_0$ and $\beta|L = -1$.

Conversely, assume that $A = \alpha\beta$. Since A is parabolic, $Fix(\alpha) \cap Fix(\beta) = \emptyset$. Let M be a line perpendicular to both $Fix(\alpha)$ and $Fix(\beta)$, where M meets $Fix(\alpha)$ at a, and meets $Fix(\beta)$ at b. Then $\alpha(M) = \beta(M) = -M$, from which it follows

that $A(M) = M$. It follows from Proposition 3.2 that we can write M in the form $M = b + tx_0$, and that $R(b) = b$.

Let $S(x) = x + b$, and let $A' = SAS^{-1}$. Note that S commutes with both R and T; hence $A' = A = S\alpha S^{-1} S\beta S^{-1}$. Now $S\beta S^{-1} \in O^m$, and $S\beta S^{-1}(x_0) = -x_0$; let β_0 be the restriction of the action of $S\beta S^{-1}$ to the hyperplane orthogonal to the line $S(M) = L_0$. Next observe that $S\alpha S^{-1}(S(M)) = S(M)$. The action of $S\alpha S^{-1}$ is the same on any hyperplane orthogonal to $S(M)$. Hence we can choose α_0 to be the action of $S\alpha S^{-1}$ on the hyperplane passing through the origin. Then $\alpha_0\beta_0$ is equal to the action of R on this same hyperplane.

We note that, since α and β both reverse orientation on M, α and α_0 have opposite orientations, as do β and β_0. □

Theorem 3.4. *Let $A \in \mathbb{A}^m$, $m > 2$, be parabolic.*

1. *$A = \alpha\beta$, where α and β both preserve orientation, if and only if either A is an extension or $m \not\equiv 1 \bmod 4$;*
2. *$A = \alpha\beta$, where α and β both reverse orientation, if and only if either A is an extension or $m \not\equiv 3 \bmod 4$.*

Proof. This follows at once from the above, together with Theorems 2.3 and 2.5. □

Proposition 3.5. *Every parabolic $A \in \mathbb{A}^m$, $m > 2$, has a square root in $\mathbb{A}^n$.*

Proof. It suffices to consider A in normal form. Then both the rotational and translational parts have square roots that keep the line L_0 invariant. Hence these square roots commute, from which the result follows. □

Theorem 3.6. *The parabolic element $A \in \mathbb{A}^m$, $m > 2$, is the commutator of two involutions if and only if either A is a strict extension, or $m \equiv 3 \bmod 4$.*

Proof. As in the elliptic case, choose a square root B of A, where B is a strict extension if A is. If either B is a strict extension, or $n \equiv 3 \bmod 4$, we can write $B = \alpha\beta$, from which it follows that $A = [\alpha, \beta]$.

For the converse, we can assume that A is in normal form. If $A = [\alpha, \beta]$, then $B = \alpha\beta$ is a square root of A. By Theorem 3.4, we have that either B is an extension, in which case, A is a strict extension, or that $m \not\equiv 1 \bmod 4$. The result follows from the fact that B is an extension if m is even. □

Theorem 3.7. *Let $A \in \mathbb{A}^m$, $m > 2$, be parabolic. Then the involution length of A is*

$$\begin{cases} 2, & \text{if } m \not\equiv 1 \bmod 4. \\ 2 \text{ or } 3, & \text{if } m \equiv 1 \bmod 4. \end{cases} \tag{3}$$

Proof. If $m \not\equiv 1 \bmod 4$, then this is immediate from Theorem 3.4.

If $m \equiv 1 \bmod 4$, then either A is an extension, in which case, the involution length of A is 2, or, as seen in Theorem 2.11, we can write $R_0 = \alpha\beta\gamma$, where α and β reverse orientation and γ preserves orientation. The result now follows by combining α and β with orientiation-reversing involutions, each of which act as the identity on the hyperplane orthogonal to the line L_0, and whose product is the translational part of A. □

Theorem 3.8. *Let $A \in \mathbb{A}^m$, $m > 2$, be parabolic. Then A is a commutator.*

Proof. We can assume that A is in normal form. If A is not the commutator of two involutions, then it is not a strict extension and $m \equiv 1 \bmod 4$. Let B be some square root of A; we can assume that B is also in normal form. By Theorem 2.11, we can find three involutions, α', β', and γ', where α' and β' reverse orientation, and γ' preserves orientation, so that $R' = \alpha'\beta'\gamma'$, where R' is the rotational part of B. We decompose $\mathcal{T}(B)$ into a product of orientation-reversing involutions: $\mathcal{T}(B) = \gamma\delta$, where γ and δ have codimension 1 hyperplanes as fixed point sets. Set $\alpha = \alpha'\gamma$, and set $\beta = \beta'\delta$. Then $B = \alpha\beta\gamma'$, where these all preserve orientation. Then $A = (\alpha\beta\gamma')^2 = [\alpha\gamma', \gamma'\beta]$. □

Combining Theorem 3.7 with the corresponding results for elliptic elements, we have:

Theorem 3.9. *Assume $m \geq 3$. The involution length of $\mathbb{A}^n$ is*

$$\begin{cases} 2, \text{ if } m \equiv 0 \bmod 4 \text{ or } m \equiv 3 \bmod 4. \\ 3, \text{ if } m \equiv 1 \bmod 4 \text{ or } m \equiv 2 \bmod 4. \end{cases} \tag{4}$$

4. Hyperbolic isometries as commutators and products of involutions

We now turn to the case that $A \in \mathbb{M}^n$, $n > 2$.

Proposition 4.1. *Let $\alpha, \beta \in \mathbb{M}^n$ be involutions, with fixed point sets $Fix(\alpha)$ and $Fix(\beta)$, respectively, and let $A = \alpha\beta$. A is elliptic if and only if $Fix(\alpha) \cap Fix(\beta) \neq \emptyset$; A is parabolic if and only if $Fix(\alpha) \cap Fix(\beta) = \emptyset$ and the (hyperbolic) distance $\rho(Fix(\alpha), Fix(\beta)) = 0$; A is hyperbolic if and only if $\rho(Fix(\alpha), Fix(\beta)) > 0$.*

Proof. It is obvious that A is elliptic, with fixed points at $Fix(\alpha) \cap Fix(\beta)$, if these two sets intersect. If the distance between these sets is zero, but they do not intersect in hyperbolic space, then they do intersect on the sphere at infinity. In the upper half-space model, normalize so that this point is the point at infinity. Then $Fix(\alpha)$ and $Fix(\beta)$ are disjoint Euclidean flats, and α and β both act as isometries on $\mathbb{E}^{n-1}$, from which it follows that $A = \alpha\beta$ is parabolic as an element of $\mathbb{M}^n$.

If the distance beteen these two sets is positive, then there is a unique line L orthogonal to both of them. It is immediate that both α and β preserve L, and that their composition acts without fixed points on it. Hence, in this case, A is hyperbolic. □

It follows from the above that an elliptic element $A \in \mathbb{M}^n$ can be written as a composition $A = \alpha\beta$ if and only if, after appropriate conjugation, we can write $A = \alpha\beta$ in SO^n.

Similarly, a parabolic element $A \in \mathbb{M}^n$ can be written as $A = \alpha\beta$ if and only if, after appropriate conjugation, we can write $A = \alpha\beta$ in $\mathbb{A}^{n-1} = \mathbb{A}^m$.

If $A \in \mathbb{M}^n$ is hyperbolic and $A = \alpha\beta$, then L_A, the axis of A, which is the unique hyperbolic A-invariant line, is the common orthogonal to $Fix(\alpha)$ and $Fix(\beta)$.

Since A preserves direction on L_A, we can write the action on the tangent space, at a point on L_A, as the direct sum of a stretch in the direction of L_A and a

rotation $R_A \in SO^{n-1}$. In analogy with the parabolic case, we call the rotation R_A the *restricted rotational part* of A.

Proposition 4.2. *The hyperbolic element $A \in \mathbb{M}^n$ can be written as $A = \alpha\beta$ if and only if its restricted rotational part R_A can be written in the form $R_A = \alpha'\beta'$, where α' and β' both preserve (resp. reverse) orientation if and only if α and β both reverse (resp. preserve) orientation.*

Proof. If we can write $A = \alpha\beta$, then L_A is orthogonal to both $Fix(\alpha)$ and $Fix(\beta)$; hence α and β both preserve L_A while reversing its direction. Then, in their action on the tangent space, they both preserve the orthogonal complement to L_A, call it C_A. We set $\alpha' = \alpha|C_A$ and $\beta' = \beta|C_A$.

If we can write $R_A = \alpha'\beta'$, then we extend α' (resp. β') to α (resp. β) by the obvious action of reversing L_A, at the point where it meets $Fix(\alpha)$ (resp. $Fix(\beta)$). □

As in the preceding cases, an element $A \in \mathbb{M}^n$ is an extension if R_A has a real eigenvalue; it is a strict extension if this eigenvalue is equal to $+1$.

Using essentially the same argument as in the parabolic case, we easily show the following.

Theorem 4.3. *Let $A \in \mathbb{M}^n$ be hyperbolic.*

1. *$A = \alpha\beta$, where α and β both preserve orientation if and only if either A is an extension or $n \equiv 3 \bmod 4$.*
2. *$A = \alpha\beta$, where α and β both reverse orientation if and only if either A is an extension or $n \equiv 1 \bmod 4$.*

Theorem 4.4. *Let $A \in \mathbb{M}^n$ be hyperbolic. If $A = [\alpha, \beta]$, where α and β preserve orientation, then $A = [\alpha', \beta']$, where α' and β' preserve orientation and are conjugate.*

Theorem 4.5. *Let $A \in \mathbb{M}^n$, $n \geq 2$, be hyperbolic. Then the involution length of A is*

$$\begin{cases} 2, \text{ if } n \not\equiv 1 \bmod 4. \\ 2 \text{ or } 3, \text{ if } n \equiv 1 \bmod 4. \end{cases} \tag{5}$$

Theorem 4.6. *If $A \in \mathbb{M}^n$, $n > 2$, is hyperbolic, then A is a commutator.*

Proof. The proof is essentially the same as that given for Theorem 3.8. □

5. All together: The proof of Theorem 1.1

In order to prove Theorem 1.1, it suffices to gather the requisite information from the preceding sections. The information concerning elliptic transformations can be found in Theorems 2.3, 2.5, and 2.10. The requisite information concerning parabolic transformations can be found in Theorem 3.4 (note that here, if n is odd, then m is even, so every parabolic transformation is a strict extension). The hyperbolic case is covered in Theorem 4.3. We gather this information in the form of a single table. The first row of this table, for example, shows that for $n \equiv 0 \bmod 4$, every elliptic element can be written as the product of two orientation-preserving involutions, and that there are elliptic elements in this dimension that cannot be written as the product of two orientation-reversing involutions.

TABLE 1. Product of two involutions ($n \geq 2$)

Dimension	*Type*	*Orientation +*	*Orientation −*
	Elliptic	Yes	No
$n \equiv 0 \mod 4$	Parabolic	Yes	No
	Hyperbolic	Yes	Yes
	Elliptic	Yes	Yes
$n \equiv 1 \mod 4$	Parabolic	Yes	Yes
	Hyperbolic	No	Yes
	Elliptic	No	Yes
$n \equiv 2 \mod 4$	Parabolic	No	Yes
	Hyperbolic	Yes	Yes
	Elliptic	Yes	Yes
$n \equiv 3 \mod 4$	Parabolic	Yes	Yes
	Hyperbolic	Yes	No

6. Perpendicular subspaces

Let $P \neq Q$ be non-trivial vector subspaces of finite dimensional Euclidean space $\mathbb{E}^n$, $n \geq 3$. P and Q are *perpendicular* if there is an orthonormal basis $e_1, \ldots, e_n$ for $\mathbb{E}^n$, and there are two proper subsets, a and b of this basis, with the following properties.

(1) a is an orthonormal basis for P and b is an orthonormal basis for Q;
(2) a and b each contain at least two elements;
(3) $a \cap b$ has fewer elements than either a or b.

In the case that $a \cap b$ is empty, then P and Q are *orthogonal* subspaces.

One easily shows the following.

Theorem 6.1. *Let $P \neq Q$ be subspaces of $\mathbb{E}^n$ of dimension at least 2. The following are equivalent.*

(1) *P and Q are perpendicular.*
(2) *Let p_P denote the orthogonal projection onto P; then $p_P(Q) = P \cap Q$.*
(3) *Let p_Q denote the orthogonal projection onto Q; then $p_Q(P) = P \cap Q$.*
(4) *$P \cap (P \cap Q)^\perp$ is orthogonal to $Q \cap (P \cap Q)^\perp$.*
(5) *$P + Q$ has the orthogonal decomposition*

$$P + Q = (P \cap Q) \oplus (P \cap (P \cap Q)^\perp) \oplus (Q \cap (P \cap Q)^\perp).$$

It follows almost at once from the definition that if P and Q are perpendicular subspaces of co-dimension at least 2, then $P^\perp$ and $Q^\perp$ are also perpendicular.

Here we will be primarily concerned with subspaces of dimension 2, which we call planes.

In what follows, we will say that W is a *common perpendicular* between P and Q to mean that W non-trivially meets both P and Q, and is perpendicular to each of them.

We remark that if P and Q are distinct planes having non-trivial intersection, then there is a unique plane in the 3-space spanned by P and Q perpendicular to both of them. This is essentially equivalent to the statement that if P and Q

are distinct complete geodesics on the 2-sphere, then they have a unique common perpendicular geodesic. In higher dimensions, it is clear that the plane spanned by $P \cap Q$ and any vector orthogonal to both P and Q is a common perpendicular.

In the case that P and Q are orthogonal planes, then one easily sees that for every $p \in P$ and for every $q \in Q$, the plane spanned by p and q is a common perpendicular.

From here on in this section, we assume that P and Q are planes that are not orthogonal and have trivial intersection. We will use the following notation throughout. If p is a unit vector in the plane P, then $\tilde{p}$ is an orthogonal unit vector in the plane P. Similarly, if q is a unit vector in the plane Q, then $\tilde{q} \in Q$ is an orthogonal unit vector.

Proposition 6.2. *The plane W spanned by p and q is a common perpendicular of P and Q if and only if $p \cdot \tilde{q} = \tilde{p} \cdot q = 0$.*

Proof. Let $w_P \in W$ be a unit vector orthogonal to p. Then w_P and $\tilde{p}$, each of which is orthogonal to p, are themselves orthogonal if and only if W is perpendicular to P. Writing w_P as a linear combination of p and q, we see that $w_P \cdot \tilde{p} = 0$ if and only if $\tilde{p} \cdot q = 0$. We similarly see that $\tilde{q} \cdot p = 0$ if and only if W is perpendicular to Q. □

Interchanging the roles of p and $\tilde{p}$, and interchanging the roles of q and $\tilde{q}$ in the above, we obtain the following.

Proposition 6.3. *The plane W spanned by p and q is a common perpendicular of P and Q if and only if the plane $\widetilde{W}$, spanned by $\tilde{p}$ and $\tilde{q}$, which is orthogonal to W, is also a common perpendicular.*

We note incidentally that if W is a common perpendicular of P and Q, then W and $\widetilde{W}$ are orthogonal.

Proposition 6.4. *For every unit vector $p \in P$, there is at most one common perpendicular between P and Q passing through p.*

Proof. Suppose we had two common perpendiculars, one spanned by p and $q \in Q$, and the other spanned by p and $q' \in Q$. We write $\tilde{q}'$ as a linear combination of q and $\tilde{q}$. Since $p \cdot \tilde{q}' = p \cdot \tilde{q} = 0$, we obtain that $p \cdot q = 0$. Similarly, since $\tilde{p} \cdot q = \tilde{p} \cdot q' = 0$, we obtain that $\tilde{p} \cdot \tilde{q} = \tilde{p} \cdot q = 0$, contradicting our basic assumption that P and Q are not orthogonal. □

Proposition 6.5. *P and Q have at least one common perpendicular plane.*

Proof. Let μ be the maximum of $p' \cdot q'$, where $p' \in P$ and $q' \in Q$ are unit vectors. Since P and Q intersect trivially and are not orthogonal, $0 < \mu < 1$. Let $p \in P$ and $q \in Q$ be unit vectors with $p \cdot q = \mu$. As above, let $\tilde{p} \in P$ be a unit vector orthogonal to p, and let $\tilde{q} \in Q$ be a unit vector orthogonal to q.

Let $q' \in Q$ be any unit vector. We can write $q' = \cos\theta q + \sin\theta \tilde{q}$. Then $p \cdot q' = \cos\theta p \cdot q + \sin\theta p \cdot \tilde{q}$. Differentiating with respect to θ, since $p' \cdot q'$ is maximal at $\theta = 0$, we obtain that $p \cdot \tilde{q} = 0$. Similarly, one obtains that $\tilde{p} \cdot q = 0$. □

We now know that P and Q have at least two distinct common perpendiculars; we next ask the question whether there might be others.

Proposition 6.6. *Suppose W is spanned by $p \in P$ and $q \in Q$ is a common perpendicular. Then P and Q have more than two common perpendiculars if and only if $p \cdot q = \pm\tilde{p} \cdot \tilde{q}$. Further, if P and Q have more than two common perpendiculars, then there is a unique common perpendicular passing through every unit vector in P, and there is a unique common perpendicular passing through every unit vector in Q.*

Proof. Assume that A, spanned by the unit vectors p and q is a common perpendicular, and assume that the plane B spanned by the unit vectors $p' = \cos\theta p + \sin\theta\tilde{p}$ and $q' = \cos\phi q + \sin\phi\tilde{q}$ is also a common perpendicular. Choose $\tilde{p}' = -\sin\theta p + \cos\theta\tilde{p}$, and choose $\tilde{q}' = -\sin\phi q + \cos\phi\tilde{q}$. Since we must have $p' \cdot \tilde{q}' = \tilde{p}' \cdot q' = 0$, we obtain

$$\cos\theta \sin\phi p \cdot q = \sin\theta \cos\phi \tilde{p} \cdot \tilde{q} \tag{6}$$

and

$$\cos\theta \sin\phi \tilde{p} \cdot \tilde{q} = \sin\theta \cos\phi p \cdot q. \tag{7}$$

Since we are assuming that p' and q' span a common perpendicular in addition to the common perpendiculars spanned by p and q and by $\tilde{p}$ and $\tilde{q}$, we can assume that none of $\sin\theta$, $\cos\theta$, $\sin\phi$ or $\cos\phi$ are equal to 0. The above equations can then be simultaneously solved only if $p \cdot q = \tilde{p} \cdot \tilde{q} = 0$ or, equivalently, if $\tan^2\theta = \tan^2\phi$.

We cannot have $p \cdot q = \tilde{p} \cdot \tilde{q} = 0$, for if we did, then we would have that p and $\tilde{p}$ are both orthogonal to both q and $\tilde{q}$, which cannot be, as P and Q are not orthogonal.

We conclude that $\tan\theta = \pm\tan\phi$, from which it follows that $p \cdot q = \pm\tilde{p} \cdot \tilde{q}$. We also observe that for every θ, we can set $\phi = \theta$, and so satisfy the above equations. □

We next exhibit two examples: one of two planes with exactly two common perpendiculars, and a second example of two planes with a circle of common perpendiculars. For both examples, it suffices to assume that $n = 4$. Also, for both examples, we take $p = (1, 0, 0, 0)$ and $\tilde{p} = (0, 1, 0, 0)$.

Example 1. $q = \frac{1}{\sqrt{3}}(1, 0, 1, -1)$ and $\tilde{q} = \frac{1}{\sqrt{6}}(0, 2, 1, 1)$.

Example 2. $q = \frac{1}{\sqrt{3}}(1, 0, 1, -1)$ and $\tilde{q} = \frac{1}{\sqrt{3}}(0, 1, 1, 1)$.

We conclude this section with the observation that we have proven the following.

Theorem 6.7. *Let P be a plane in $\mathbb{E}^n$, $n \geq 4$. For almost all planes $Q \subset \mathbb{E}^n$, we have that P and Q intersect trivially, are non-orthogonal, and have exactly two common perpendiculars.*

7. Linking, common perpendiculars, and the proof of Theorem 1.4

We remind the reader that a common perpendicular between subspaces P and Q must non-trivially meet P and Q as well as be perpendicular to each of them.

We will need the following remark for what follows. Suppose the transformation A can be written as the product of two involutions, $A = \alpha\beta$. Let X be an A-invariant set. Then $\alpha(X)$ is invariant under $\alpha A\alpha = \alpha\alpha\beta\alpha = A^{-1}$. Similarly, $\beta A\beta(X) = A^{-1}(X)$. Hence $\beta(X) = \alpha(X)$ is also A-invariant.

An element $A \in O^n$ is called *general* if the following hold:

G1. If n is even, then A has $m = n/2$ orthogonal invariant planes, $P_1, \ldots, P_m$; if n is odd, then A has $m = (n-1)/2$ orthogonal invariant planes. For each such invariant plane P_j, A acts as a non-trivial rotation of order at least 3 of the form $z \mapsto \exp(i\theta_j)z$, where, for every i and every j, $\theta_i \not\equiv \pm\theta_j \mod 2\pi$.

Note that these conditions assure us that if $A = \alpha\beta$, then, for every i, $\alpha(P_i) = \beta(P_i) = P_i$.

Theorem 7.1. *Let A and B be distinct general elements of SO^n. A and B are linked if and only if there is a proper subspace $W \subset \mathbb{E}^n$, where W non-trivially meets and is perpendicular to every invariant plane of A and to every invariant plane of B.*

Proof. Write the invariant planes of A as $P_1, \ldots, P_m$, and write the invariant planes of B as $Q_1, \ldots, Q_m$.

We first assume that A and B are linked, so that $A = \alpha\beta$ and $B = \beta\gamma$. It follows from the above that α and β each preserve each of the planes P_i, and that β and γ each preserve each of the planes Q_j. It follows from **G1** that, for each P_i, α and β both act as reflections, in different lines. Similarly, for each Q_i, β and γ each act as reflections in different lines. Since $\beta|P_i$ is a reflection, the fixed point set W of β intersects P_i in a line, and, since $\beta(P_i) = P_i$, W is perpendicular to P_i. Similarly, W is perpendicular to each Q_j.

Conversely, suppose there is a proper subspace W that meets and is perpendicular to each P_i and to each Q_j. Define β to be the involution with fixed point set W. For $i = 1, \ldots, m$, define $\alpha|P_i$ to be the reflection $A\beta|P_i$. If n is odd, there is a line L, orthogonal to every P_i. Define $\alpha|L = \beta|L$, so that $\alpha\beta|L = 1$. Since A is orientation-preserving, $A|L = 1$. We now have that $A = \alpha\beta$. Similarly, for each Q_j, set $\gamma|Q_j = \beta B|Q_j$, and, if n is odd, set $\gamma|L = \beta|L$; then $B = \beta\gamma$. □

Theorem 1.4. *Every pair of elements of SO^4 is linked.*

Proof. We first take up the case that A and B are general elements of SO^4. In particular, A has an invariant plane P, and B has an invariant plane $Q \neq P$. Let W be a common perpendicular plane between P and Q. Then there is a unit vector $\hat{p} \in W$, orthogonal to P, from which it follows, since $W \neq P^\perp$, that W is also perpendicular to $P^\perp$. Similarly, W is perpendicular to $Q^\perp$. It then follows from Theorem 7.1 that A and B are linked.

The above proof needs only minor modifications for the case that either A or B acts trivially, or as an involution, on or both invariant planes. The only case remaining is that A and B both have the same pair of invariant planes, in which case we can choose W as an arbitrary common perpendicular between the two invariant planes, which are orthogonal. □

Corollary 7.2. *Let $A \neq B$ be non-trivial elements of SO^3. Then A and B are linked.*

Proof. Since A and B are non-trivial, they each have at least one invariant plane on which they act non-trivially. Let P (resp. Q) be such invariant planes for A (resp. B). If $P \neq Q$, then let W be their unique common perpendicular. It is now easy to define β as reflection in W. Then, as above, one can appropriately define α and β. If $P = Q$, choose W to be any plane meeting and perpendicular to P and proceed as above. □

Theorem 7.3. *Let $\mathcal{S}$ denote the set of pairs of elements, $(A, B) \in SO^n \times SO^n$, $n \geq 5$, where A and B are linked general elements of SO^n. Then $\mathcal{S}$ has measure zero.*

Proof. We fix a general element $A \in SO^n$, and consider the set of $B \in SO^n$ so that $(A, B) \in \mathcal{S}$. Let $P_1, \dots, P_m$ be the invariant planes of A, and let $Q_1, \dots, Q_m$ be the invariant planes of B. Note that $m \geq 2$. We note that the set of B for which there is some Q_i either equal to or orthogonal to some P_j, has measure zero. Hence we can assume that no Q_i is either equal to or orthogonal to any P_j. We next note that, by Proposition 6.6, the planes P_j and Q_i have a circle of common perpendiculars if and only if a linear equality is satisfied. Hence we can assume that for each P_i, and for each Q_j, there are exactly two common perpendicular planes.

Let W_1 be a common perpendicular plane between P_1 and Q_1, and let W_2 be a common perpendicular plane between P_1 and Q_2. Let p_1 be a unit vector in $P_1 \cap W_1$, and let p_2 be a unit vector in $P_1 \cap W_2$. If we had $p_2 \neq \pm p_1$ and $p_2 \neq \pm \tilde{p}_1$, then the space spanned by W_1 and W_2 would include all of P_1, so A and B could not be linked. We have shown that $\mathcal{S}$ is contained in the union of the solution sets of the equations: $p_2 = \pm p_1$ and $p_2 = \pm \tilde{p}_1$. Since these are equalities, it suffices to construct an example of four planes, P_1, P_2, Q_1, and Q_2, where P_1 and P_2 are orthogonal, Q_1 and Q_2 are orthogonal, and the common perpendicular plane between P_1 and Q_2 meets P_1 in a line that is distinct from the intersection of P_1 with any common perpendicular plane between P_1 and Q_1.

We construct our example in dimension 5; this example can obviously be embedded in any higher dimensional space.

Let P_1 be spanned by $p_1 = (1, 0, 0, 0, 0)$ and $\tilde{p}_1 = (0, 1, 0, 0, 0)$. Let P_2 be spanned by $p_2 = (0, 0, 1, 0, 0)$ and $\tilde{p}_2 = (0, 0, 0, 1, 0)$.

Let Q_1 be spanned by $q_1 = \frac{1}{\sqrt{3}}(1, 0, 1, -1, 1)$ and $\tilde{q}_1 = \frac{1}{\sqrt{6}}(0, 2, 0, 1, 1)$. Let Q_2 be spanned by $q_2 = \frac{1}{2}(1, 1, -1, 0, 1)$ and $\tilde{q}_2 = \frac{1}{\sqrt{6}}(0, 1, 0, 2, -1)$.

We see at once that there is a common perpendicular plane between P_1 and Q_1 passing through p_1 and q_1, and there is another common perpendicular plane passing through $\tilde{p}_1$ and $\tilde{q}_1$. Since $p_1 \cdot q_1 \neq \pm \tilde{p}_1 \cdot \tilde{q}_1$, there are no others.

It follows from Proposition 6.2 that there is a common perpendicular between P_2 and Q_1 passing through q_1 if and only if, for some θ, we have $\tilde{q}_1 \cdot (0, 0, \cos\theta, \sin\theta, 0) = 0$, and $q_1 \cdot (0, 0, -\sin\theta, \cos\theta, 0) = 0$.

Solving the first equation, we obtain that $\cos\theta = 0$, while the second equation yields $\sin\theta + \cos\theta = 0$, which is impossible. □

8. Linking pairs in hyperbolic spaces

It is well known that, except for the case of two elements that share a fixed point on the sphere at infinity, every pair of elements of $\mathbb{M}^2$, and of $\mathbb{M}^3$, is linked.

For higher dimensions, we will need the following observation.

Proposition 8.1. *Let A and B be hyperbolic elements of $\mathbb{M}^n$, $n \geq 4$. Let L_A (resp. L_B) be the axis of A (resp. B). Assume L_A and L_B do not meet, even on the sphere at infinity. Let V be the common perpendicular between L_A and L_B. If A and B are linked by β, then V belongs to the fixed point set of β.*

Proof. Assume $A = \alpha\beta$. Then $\beta(L_A)$ is kept invariant by $\beta A \beta = \beta\alpha = A^{-1}$. Since L_A is the unique A-invariant geodesic, $\beta(L_A) = L_A$. One similarly shows that $\beta(L_B) = L_B$. Since β preserves both L_A and L_B, which are assumed to be disjoint, it must pointwise fix their common perpendicular. □

Theorem 8.2. *For $n \geq 4$, the set of linked pairs of elements (A, B) has measure zero in $\mathbb{M}^n \times \mathbb{M}^n$.*

Proof. We need to show that the set of pairs (A, B) that are not linked has full measure. To this end, we can first assume that A and B are both hyperbolic, with non-intersecting axes, and that their rotational parts are general (that is, satisfy **G1** from section 7). Let x and y be the point of intersection of L_A (resp. L_B) with their common perpendicular V. Let R_A be the rotational part of A. We can think of it as an elliptic transformation centered at x; likewise, we can think of R_B, the rotational part of B, as an elliptic transformation centered at y. Let W be the pure hyperbolic transformation, with axis V, mapping y to x, and let $\hat{B} = WBW^{-1}$. Then the rotational part of $\hat{B}$ is $\hat{R}_B = WR_BW^{-1}$, which we regard as an elliptic transformation centered at x.

Lemma 8.3. *If A and B are linked by β, where V is pointwise fixed by β, then A and $\hat{B}$ are linked. Conversely, if A and $\hat{B}$ are linked by $\hat{\beta}$, where V is pointwise fixed by $\hat{\beta}$, then A and B are linked.*

Proof. Assume first that A and B are linked by β. Write $B = \beta\gamma$ and observe that since β pointwise fixes V, β commutes with W. Hence $\hat{B} = WBW^{-1} = W\beta\gamma W^{-1} = \beta(W\gamma W^{-1})$, showing that A and $\hat{B}$ are linked. The proof in the other direction is essentially the same. □

Now suppose that A and B have axes that intersect at the origin (in the ball model), and that they are linked. Then the linking involution β keeps invariant the axes of these two transformations, pointwise fixes their common perpendicular, and it links the rotational part of A with the rotational part of B.

For $n \geq 6$, our result follows immediately from Theorem 7.3.

For $n = 5$, except on a set of measure zero, there are only finitely many possible involutions that link the rotational parts of A and B. Since the axes of A and B are independent of their rotational parts, the involution β that links the rotational parts of A and B will also keep these axes invariant only on a set of measure zero.

For $n = 4$, we need to look more closely at the rotational parts, R_A and R_B. We can assume that these each have an invariant plane, and that the action of R_A on its invariant plane P_A is non-trivial, not an involution and is a rotation through an angle that is distinct from the action of R_B on its invariant plane, P_B. We can assume that P_A and P_B are in general position: they do not intersect and they are not orthogonal. We can also assume that the axes, L_A and L_B of A and B, respectively, are in general position with respect to each other and with respect to the invariant planes; that is, L_A does not lie in P_Q, and is not orthogonal to it, and L_B does not lie in P_A and is not orthogonal to it. We note that β must act as a reflection in both P_A and P_B, and must reverse direction on both L_A and L_B. Let M_A be the line orthogonal to both P_A and L_A, and let M_B be the line orthogonal to both P_B and L_B. As above, we can assume that M_A is not orthogonal to P_B or to L_B, and does not lie in P_B. Likewise, we can assume that M_B does not lie in P_A, and is not orthogonal to either P_A or L_A. We can also assume that neither M_A nor M_B lies in the common perpendicular between P_A and P_B.

Since β reverses orientation on both P_A and L_A, and reverses orientation on both P_B and L_B, and since β must globally either preserve or reverse orientation and must preserve both M_A and M_B, either β acts as the identity on both M_A and

M_B or it acts as -1 on both these lines. If β acts as the identity on both M_A and M_B, then its fixed point set has dimension at least 3. This implies that $L_A = L_B$, for both are orthogonal to the fixed point set of β. If β acts as -1 on both M_A and M_B, then, as above, the eigenspace belonging to the eigenvalue -1 has dimension at least 3, which is also impossible, as the common perpendicular plane between P_A and P_B must belong to the eigenspace for the eigenvalue $+1$. □

9. Linking pairs in Euclidean spaces

Theorem 9.1. *For $n \geq 3$, the set of linked pairs of elements (A, B) has measure zero in $\mathbb{A}^n \times \mathbb{A}^n$.*

Proof. We first remark that for $n \geq 5$, the proof of Theorem 8.2, is easily adapted to the Euclidean case. For odd dimensions, a general element of $\mathbb{A}^n$ has a unique invariant line, so the proof carries over directly. For even dimensions, a generic Euclidean isometry has an invariant plane, foliated by invariant lines. Since, for $n > 4$, two generic planes do not intersect and have a unique common perpendicular, the proof of Theorem 8.2 applies in this case as well.

In dimension 4, A and B each have an invariant plane. Generically, these two invariant planes will have a unique point in common. Each of A and B will have a unique invariant line through this point, and, if they were linked, the linking involution β would have to act as -1 on each of these lines. This is exactly the situation for dimension 4 in Theorem 8.2.

The situation in dimension 3 is somewhat different. The generic element A of $\mathbb{A}^3$ has a unique invariant line L_A. Generically, the invariant lines of A and B will be skew and so have a unique common perpendicular. However, the linking involution β must preserve L_A, while reversing its direction. It must also act as a reflection in the invariant plane orthogonal to L_A, and it must also act as a reflection in the invariant plane orthogonal to L_B. This means that if A and B are linked, then there is a plane, the fixed point set of β, passing through both L_A and L_B. □

10. The proof of Theorem 1.5 and a concluding remark

Theorem 1.5 now follows from Theorems 7.3, 8.2, and 9.1.

The property of being a general element of SO^n is an open, dense condition. It follows that the set of non-linked pairs is a dense open subset of $\mathcal{G}^n \times \mathcal{G}^n$, where $\mathcal{G}^n$ is one of the isometries groups in Theorem 1.5.

References

[1] Alan F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics, 91. Springer-Verlag, New York, 1983. xii+337 pp. MR698777 (85d:22026)

[2] W. M. Goldman, *Trace coordinates on Fricke spaces of some simple hyperbolic surfaces*, Chapter 15, pp. 611–684, Handbook of Teichmüller theory, vol. II (A Papadopoulos, ed.), IRMA Lectures in Mathematics and Physics, volume 13, European Mathematical Society (2008).

[3] B. Maskit, *Kleinian groups*, Springer-Verlag, Berlin, 1988. MR959135 (90a:30132)

[4] S. Pasiencier and H-C. Wang, Commutators in a semi-simple Lie groups, Proceedings of the A.M.S., Vol. 13, No. 6 (Dec., 1962), pp. 907-913. MR0169947 (30:190)

[5] K. M. Puri, Factoring of isometries of hyperbolic 4-space and a discreteness condition, Thesis, Rutgers University 2009.

[6] R. Ree, Commutators in semi-simple algebraic groups, Proceedings of the American Mathematical Society, Vol. 15, No. 3 (Jun., 1964), pp. 457-460. MR0161944 (28:5148)

[7] R. C. Thompson, Commutators in the special and general linear groups, Transactions of the American Mathematical Society, Vol. 101, No. 1 (Oct., 1961), pp. 16-33. MR0130917 (24:A771)
[8] M. J. Wonenburger, Transformations which are products of two involutions, Journal of Mathematics and Mechanics, Vol. 16, no. 4 (1966). MR0206025 (34:5850)

Department of Mathematics, Graduate Center and Hunter College, CUNY, New York, New York 10065
E-mail address: abasmajian@gc.cuny.edu

Department of Mathematics, Stony Brook University, Stony Brook, New York 11794
E-mail address: bernie@math.sunysb.edu