A Reduction for the Distinct Distances Problem in $\mathbb{R}^d$

Sam Bardwell–Evans* Adam Sheffer†

June 1, 2017

Abstract

We introduce a reduction from the distinct distances problem in $\mathbb{R}^d$ to an incidence problem with $(d-1)$-flats in $\mathbb{R}^{2d-1}$. Deriving the conjectured bound for this incidence problem (the bound predicted by the polynomial partitioning technique) would lead to a tight bound for the distinct distances problem in $\mathbb{R}^d$. The reduction provides a large amount of information about the $(d-1)$-flats, and a framework for deriving more restrictions that these satisfy.

Our reduction is based on introducing a Lie group that is a double cover of the special Euclidean group. This group can be seen as a variant of the Spin group, and a large part of our analysis involves studying its properties.

1 Introduction

The *Erdős distinct distances problem* is a main problem in Discrete Geometry, which asks for the minimum number of distinct distances spanned by a set of n points in $\mathbb{R}^2$. That is, denoting the distance between two points $p, q \in \mathbb{R}^2$ as $|pq|$, we wish to find $\min_{|\mathcal{P}|=n} |\{|pq| : p, q \in \mathcal{P}\}|$.

In 1946, Erdős [3] observed that a $\sqrt{n} \times \sqrt{n}$ section of the integer lattice $\mathbb{Z}^2$ spans $\Theta(n/\sqrt{\log n})$ distinct distances (this observation is an immediate corollary of a number theoretic result of Landau and Ramanujan). Erdős conjectured that no set of n points in $\mathbb{R}^2$ spans an asymptotically smaller number of distinct distances. Proving that every set of n points in $\mathbb{R}^2$ spans $\Omega(n/\sqrt{\log n})$ distinct distances turned out to be a difficult problem, to have a deep underlying theory, and to have strong connections to several other parts of mathematics.

After over 60 years and many works on the distinct distances problem, Guth and Katz [6] proved that every set of n points in $\mathbb{R}^2$ spans $\Omega(n/\log n)$ distinct distances. Their proof involves studying properties of polynomials, partly by using tools from Algebraic Geometry. This work began a new era of polynomial methods in Discrete Geometry.

Already in his 1946 paper, Erdős observed that a $n^{1/d} \times n^{1/d} \times \cdots \times n^{1/d}$ section of the integer lattice $\mathbb{Z}^d$ spans $\Theta(n^{2/d})$ distinct distances. He then conjectured that this construction is asymptotically best possible, in the sense that every set of n points in $\mathbb{R}^d$ spans $\Omega(n^{2/d})$ distinct distances. When the Guth–Katz paper first appeared, it seemed that similar techniques might solve the distinct distance problem in $\mathbb{R}^d$. However, over six years have passed and no new results were obtained for this problem. Before the new era of polynomial methods, Solymosi and Vu [10] derived a lower bound for the number of distinct distances in $\mathbb{R}^d$. This bound was obtained by an induction on the dimension d. The current best bounds for distinct distances in $\mathbb{R}^d$ are obtained

*California Institute of Technology, Pasadena, CA, USA. Supported by Caltech's Summer Undergraduate Research Fellowships (SURF) program. *sam.bardwell.evans@gmail.com*.

†California Institute of Technology, Pasadena, CA, USA. *adamsh@gmail.com*.

by using this induction, with the planar distinct distances theorem as the induction basis. For example, this implies that every n points in $\mathbb{R}^3$ determine $\Omega^*(n^{3/5})$ distinct distances.[1]

The proof of the planar distinct distances theorem reduces the problem into a point-line incidence problem in $\mathbb{R}^3$ (based on a previous work by Elekes and Sharir [2]), and then solves the incidence problem by using polynomial methods. Specifically, given a finite set of lines $\mathcal{L}$ in $\mathbb{R}^d$ and a positive integer k, we say that a point in $\mathbb{R}^d$ is *k-rich* if it is contained in at least k lines of $\mathcal{L}$. The planar distinct distances theorem was reduced to the following problem.

Theorem 1.1 (Guth and Katz [6]). *Let $\mathcal{L}$ be a set of n lines in $\mathbb{R}^3$ such that no point of $\mathbb{R}^3$ is contained in more than $\sqrt{n}$ lines of $\mathcal{L}$. Moreover, every plane, hyperbolic paraboloid, or single-sheeted hyperboloid contains $O(\sqrt{n})$ lines of $\mathcal{L}$. Then for every $k \geq 2$, the number of k-rich points is $O\left(\frac{n^{3/2}}{k^2} + \frac{n}{k}\right)$.*

It is possible to imitate the reduction of the planar distinct distances problem in higher dimensions. However, already for distinct distances in $\mathbb{R}^3$ this leads to an incidence problem with somewhat involved varieties that are difficult to study. For example, it is not clear how to bound the number of varieties that can be contained in a hyperplane.

The main contribution of this paper is a more involved reduction that leads to a simpler incidence problem. It is significantly easier to establish properties of the varieties in this problem. We refer to k-dimensional planes in $\mathbb{R}^d$ as *k-flats*. Let $\mathbb{S}^d$ be the hypersphere in $\mathbb{R}^{d+1}$ that is centered at the origin and of radius 1.

Theorem 1.2. *The problem of deriving a lower bound on the minimum number of distinct distances spanned by n points in $\mathbb{R}^d$ can be reduced to the following problem:*

> *Let $\mathcal{F}$ be a set of n distinct $(d-1)$-flats in $\mathbb{R}^{2d-1}$, such that every two flats intersect in at most one point, every point of $\mathbb{R}^{2d-1}$ is contained in $O(\sqrt{n})$ flats of $\mathcal{F}$, and every hyperplane in $\mathbb{R}^{2d-1}$ contains $O(\sqrt{n})$ of these flats. Find an upper bound on the number of k-rich points, for every $2 \leq k = O(n^{1/d+\varepsilon})$ (for some $\varepsilon > 0$).*

Deriving the bound $O\left(\frac{n^{(2d-1)/d}}{k^{2+\varepsilon}}\right)$ for the number of k-rich points would yield the conjectured lower bound of $\Omega(n^{2/d})$ distinct distances.

Remarks. (i) Using our methods, we obtained the same reduction for the case where the points are on the hypersphere $\mathbb{S}^d$ rather than in $\mathbb{R}^d$. Since the paper is already rather long and technical, we decided not to include the proof of this case.
(ii) For $\alpha \geq 0$, deriving the bound $O\left(\frac{n^{\alpha+(2d-1)/d}}{k^{2+\varepsilon}}\right)$ for the number of k-rich points would yield a lower bound of $\Omega(n^{2/d-2\alpha})$ distinct distances.
(iii) The ε in the bound $k = O(n^{1/d+\varepsilon})$ comes from an incidence bound of Solymosi and Tao [9]. It is conjectured that this ε can be removed from the bound of [9], and this would immediately remove the ε from the restriction on k.
(iv) Usually a bound on the number of k-rich points also includes an extra term of the form n/k, which dominates the bound when k is large. Since we are only interested in small values of k, this extra term is not relevant in our case.

The current best bounds for incidences with varieties in $\mathbb{R}^d$ are obtained by the *polynomial partitioning* technique (for example, see [4, 9]). We can efficiently apply this technique to incidences with $(d-1)$-flats in $\mathbb{R}^{2d-2}$, but the case of $(d-1)$-flats in $\mathbb{R}^{2d-1}$ seems to be just beyond the

[1] In the $\Omega^*(\cdot)$-notation we ignore polylogarithmic factors.

current capabilities. There is a simple way to estimate the bounds that the polynomial partitioning technique is expected to yield after overcoming the current issues.[2] In the case of $(d-1)$-flats in $\mathbb{R}^{2d-1}$, the expected incidence bound is $m_k = O\left(\frac{n^{(2d-1)/d}}{k^{(3d-2)/d}} + \frac{n}{k}\right)$. Note that this is the incidence bound required in Theorem 1.2 to obtain a tight bound for the distinct distances problem in $\mathbb{R}^d$.

Theorem 1.2 states three restrictions on the set of flats $\mathcal{F}$: the maximum number of flats incident to a common point, the maximum number of flats contained in a common hyperplane, and the size of the intersection of any two flats. Our framework can be used to obtain additional information about the flats of $\mathcal{F}$. In particular, before obtaining the set $\mathcal{F}$ of $(d-1)$-flats in $\mathbb{R}^{2d-1}$, we get a set $\mathcal{L}$ of $\binom{d}{2}$-flats in $\mathbb{R}^{\binom{d+1}{2}}$. To move to the space $\mathbb{R}^{2d-1}$ from the statement of Theorem 1.2, we intersect $\mathcal{L}$ with a generic $(2d-1)$-flat. In Section 6 we describe the exact structure of the flats of $\mathcal{L}$ (that is, the equations that define each flat). This structure can be used to obtain additional properties of the flats of $\mathcal{L}$, and thus of the flats of $\mathcal{F}$. It is currently unclear what additional properties would be needed to solve the resulting incidence problem, but given such properties it seems reasonable that our techniques would lead to the derivation of the corresponding restrictions.

The inspiration for this work came from a blog post of Tao [11]. Tao states that he wrote this post "to record some observations arising from discussions with Jordan Ellenberg, Jozsef Solymosi, and Josh Zahl." The post describes a reduction from the problem of finding a lower bound for the number of distinct distances spanned by points on the sphere $\mathbb{S}^2$ to Theorem 1.1. It also shows how the case of distinct distances in $\mathbb{R}^2$ can be viewed as a scaling limit of the case of distinct distances in $\mathbb{S}^2$. This is an alternative way to reduce the planar distinct distances problem to a point-line incidence problem in $\mathbb{R}^3$. While the original reduction can be seen as based on the Lie group SE(2), the reduction in the blog post is based on the Lie group Spin(3) (a brief introduction to these groups can be found in Section 2). A more direct approach to distinct distances on $\mathbb{S}^2$ was presented by Rudnev and Selig [7].

To derive a reduction from the distinct distances problem in $\mathbb{R}^d$ we introduce a variant of the group Spin(d), which we denote Spun(d). While Spin(d) is a double cover of SO(d), the group Spun(d) is a double cover of SE(d). A large part of our analysis deals with studying properties of Spun(d).

In Section 2 we briefly describe several Lie groups that we rely on. In Section 3 we introduce the group Spun(d) and study its structure. In Section 4 we derive Theorem 1.2 for the special case of distinct distances in $\mathbb{R}^3$. We present this case separately since it is simpler to prove and provides more intuition about what is happening in the proof. In Section 5 we extend the analysis from Section 4 to any dimension. Finally, in Section 6 we derive the defining equations of the flats of $\mathcal{L}$, as stated above.

Acknowledgments. The authors would like to thank William Ballinger and Dmitri Gekhtman for several helpful discussions.

2 Preliminaries: Lie groups

In our analysis we rely on a specific family of Lie groups. In this section we briefly introduce these groups and some of their properties. In Section 3 we will introduce our own Lie group and study it in more detail.

Given a point $p \in \mathbb{R}^d$, we denote by $\|p\|$ the standard Euclidean norm of p. Given two points $p, q \in \mathbb{R}^d$, we denote by $|pq|$ the Euclidean distance between them (that is, $\|p - q\|$).

[2]This is done by bounding the number of incidences in the cells while ignoring the incidences on the partition itself. See for example [8, Chapter 8].

Groups of rigid motions. A *rigid motion* (or *isometry*) of $\mathbb{R}^d$ is a transformation $T : \mathbb{R}^d \to \mathbb{R}^d$ that preserves Euclidean distances. That is, for every $v, u \in \mathbb{R}^d$ we have that $|uv| = |T(u)T(v)|$. It is well known that every rigid motion of $\mathbb{R}^d$ is a combination of translations, rotations, and reflections. A rigid motion is said to be *proper* if it is a combination of translations and rotations. In $\mathbb{R}^2$, a rigid motion is proper if and only if for every three points $a, b, c \in \mathbb{R}^d$, the path $a \to b \to c$ forms a right turn if and only if $T(a) \to T(b) \to T(c)$ forms a right turn (that is, if the rigid motion is *orientation preserving*). A similar definition exists in higher dimensions. The *Special Euclidean group* of $\mathbb{R}^d$, denoted $\mathrm{SE}(d)$, is the group of proper rigid motions of $\mathbb{R}^d$ under the operation of composition.

The *Orthogonal group* $\mathrm{O}(d)$ is the group of rigid motions of $\mathbb{R}^d$ that fix the origin. It consists of the rotations around the origin and the reflections about a hyperplane incident to the origin. Equivalently, we can think of $\mathrm{O}(d)$ as the set of rigid motions that take $\mathbb{S}^{d-1}$ to itself. The *Special Orthogonal group* $\mathrm{SO}(d)$ is the group of *proper* rigid motions of $\mathbb{R}^d$ that fix the origin (equivalently, of proper rigid motions that take $\mathbb{S}^{d-1}$ to itself). It consists of the rotations around the origin. Note that $\mathrm{SO}(d)$ is a subgroup of both $\mathrm{O}(d)$ and $\mathrm{SE}(d)$.

For any unproved claims in the the remainder of this section, see [5, Sections 1.2–1.4].

Clifford algebras. A *Clifford algebra* is defined with respect to a vector space and to a symmetric bilinear form. We only define a special case of this algebra: the Clifford algebra associated with $\mathbb{R}^d$ and the Euclidean norm. This is a real unitary algebra $C\ell_d$ with a linear map $i : \mathbb{R}^d \to C\ell_d$ that satisfies the following two properties. For every $v \in \mathbb{R}^d$, we have $i(v)^2 = -\|v\|^2 \cdot \mathbf{1}$, where $\mathbf{1}$ is the multiplicative identity element of $C\ell_d$. Moreover, if A is a real algebra and $f : \mathbb{R}^d \to A$ is a linear map satisfying $f(v)^2 = -\|v\|^2 \cdot \mathbf{1}$ for all $v \in \mathbb{R}^d$, then there exists an algebra homomorphism $\phi : C\ell_d \to A$ such that $f = \phi \circ i$. It can be shown that the algebra $C\ell_d$ is unique up to an isomorphism.

We now present a more constructive definition of the Clifford algebra $C\ell_d$ (the definition that we will actually rely is in the following paragraph). For a vector space V, we denote by $V^{\otimes k}$ the k-fold tensor product of V with itself. Consider the direct sum $\bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k}$, and let $\mathcal{I}$ be the ideal in this tensor algebra that is generated by all elements of the form $v \otimes v + \|v\|^2 \cdot \mathbf{1}$. Then we can write $C\ell_d$ as the quotient

$$\bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k} / \mathcal{I}.$$

Let $j : \mathbb{R}^n \to \bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k}$ be the natural injection, and let $\pi : \bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k} \to \bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k} / \mathcal{I}$ be the natural quotient map. Then the linear map associated with $C\ell_d$ is the composition $\pi \circ j$.

For our purposes, it would be more intuitive to think of the Clifford algebra $C\ell_d$ as follows. Let $e_1, \ldots, e_d$ denote the image of an element of the standard basis of $\mathbb{R}^n$ under the map i. When dealing with tensor products of elements of $C\ell_d$, we will write xy instead of $x \otimes y$. Note that $C\ell_d$ is a 2^d-dimensional real vector space with basis $\mathbf{1}, e_1, \ldots, e_d, e_1e_2, \ldots, e_1e_d, e_2e_3, \ldots, e_1 \cdots e_d$ (that is, the 2^d subsets of $\{e_1, \ldots, e_d\}$). Recalling the definition of $\mathcal{I}$, we note that the Clifford algebra satisfies $e_j^2 = -\mathbf{1}$ for every $1 \le j \le d$. Moreover, a simple argument shows that $e_je_k = -e_ke_j$ for every $1 \le j, k \le d$ with $j \ne k$. This explains why in the basis of $C\ell_d$ we do not have combinations of elements $e_1, \ldots, e_d$ where some e_k repeats more than once.

Let $\alpha : C\ell_d \to C\ell_d$ be the automorphism satisfying $\alpha(\mathbf{1}) = \mathbf{1}$ and $\alpha(e_j) = -e_j$ for all j. Let $t : C\ell_d \to C\ell_d$ be the anti-automorphism satisfying $t(xy) = t(y)t(x)$, $t(e_j) = e_j$ for all j, and $t(\mathbf{1}) = \mathbf{1}$. For example, we have $\alpha(e_1 + e_1e_2) = -e_1 + e_1e_2$ and $t(e_1 + e_1e_2) = e_1 + e_2e_1 = e_1 - e_1e_2$. It can be shown that the functions α and t are uniquely defined. We define the *conjugate* of $x \in C\ell_d$ as $\overline{x} = \alpha(t(x)) = t(\alpha(x))$. We also define the norm $N(x) = x\overline{x}$. Returning to the above example, we have $\overline{e_1 + e_1e_2} = -e_1 - e_1e_2$ and $N(e_1 + e_1e_2) = 2 \cdot \mathbf{1}$. Note that for every $v \in \mathbb{R}^d$ and $x = i(v)$ we have $\overline{x} = -x$, which in turn implies $N(x) = \|v\|^2$.

We are especially interested in elements $x \in C\ell_d$ that satisfy $\alpha(x)i(v)x^{-1} \in i(\mathbb{R}^d)$ for every $v \in \mathbb{R}^d$. One advantage of working with such elements is that their norm is well behaved.

Lemma 2.1.
(i) Let $x \in C\ell_d$ satisfy $\alpha(x)i(v)x^{-1} \in i(\mathbb{R}^d)$ for every $v \in \mathbb{R}^d$. Then $N(x) = r \cdot \mathbf{1}$ for some $r \in \mathbb{R}$.
(ii) Consider a second element $y \in C\ell_d$ that satisfies $\alpha(y)i(v)y^{-1} \in i(\mathbb{R}^d)$ for every $v \in \mathbb{R}^d$. Then $N(xy) = N(x)N(y)$.
(iii) Let $x = i(u)$ for $u \in \mathbb{R}^d$. Then $\alpha(x)i(v)x^{-1} \in i(\mathbb{R}^d)$ for every $v \in \mathbb{R}^d$.

Proof. (i) See [5, Proposition 1.8].

(ii) By part (i) of the lemma, $N(y) = r \cdot \mathbf{1}$ for some $r \in \mathbb{R}$, so $N(y)$ commutes with everything in $C\ell_d$. This implies

$$N(xy) = xy\overline{xy} = xy\overline{y}\,\overline{x} = xN(y)\overline{x} = x\overline{x}N(y) = N(x)N(y).$$

(iii) See [5, Proposition 1.6]. □

Rather than working with all of $C\ell_d$, we will rely on the subalgebra

$$C\ell_d^0 = \{x \in C\ell_d :\, \alpha(x) = x\}.$$

This is the 2^{d-1}-dimensional subspace of $C\ell_d$ generated by the elements of the basis of $C\ell_d$ that are the product of an even number of distinct e_j's. Similarly, we set $C\ell_d^1 = \{x \in C\ell_d :\, \alpha(x) = -x\}$. This is a 2^{d-1}-dimensional subspace (not a subalgebra), and is generated by the elements of the basis of $C\ell_d$ that are the product of an odd number of distinct e_j's.

Spin groups. Denote the multiplicative groups of $C\ell_d$ and $C\ell_d^0$ as $C\ell_d^\times$ and $C\ell_d^{0\times}$, respectively. We define the Lie groups

$$\begin{aligned} \mathrm{Pin}(d) &= \{x \in C\ell_d^\times \;:\, N(x) = \mathbf{1} \quad \text{and} \quad \alpha(x)i(v)x^{-1} \in i(\mathbb{R}^d) \;\text{ for every } v \in \mathbb{R}^d\}, \\ \mathrm{Spin}(d) &= \{x \in C\ell_d^{0\times} \;:\, N(x) = \mathbf{1} \quad \text{and} \quad xi(v)x^{-1} \in i(\mathbb{R}^d) \;\text{ for every } v \in \mathbb{R}^d\}. \end{aligned} \tag{1}$$

Note that in the definition of $\mathrm{Spin}(d)$ we can replace $xi(v)x^{-1}$ with $\alpha(x)i(v)x^{-1}$, since $x = \alpha(x)$ for every $x \in C\ell_d^{0\times}$.

An equivalent definition for $\mathrm{Pin}(d)$ is the set of elements that can be written as $i(v_1)i(v_2)\cdots i(v_k)$, where $v_1, \ldots, v_k \in \mathbb{S}_{d-1}$ (and k is not fixed). Similarly, an equivalent definition of $\mathrm{Spin}(d)$ is the set of elements that can be written as $i(v_1)i(v_2)\cdots i(v_k)$, where $v_1, \ldots, v_k \in \mathbb{S}_{d-1}$ and k is even.

For $\gamma \in \mathrm{Pin}(d)$ and $v \in \mathbb{R}^d$, we denote the group action of γ on p as p^γ. This group action is $v^\gamma = i^{-1}(\alpha(\gamma)i(v)\gamma^{-1})$. Notice that i is injective when considered as a function from $\mathbb{R}^d$ to $i(\mathbb{R}^d)$. When $v \in \mathbb{R}^d$ we have $\alpha(\gamma)i(v)\gamma^{-1} \in i(\mathbb{R}^d)$, so $v^\gamma = i^{-1}(\gamma i(v)\gamma^{-1})$ is well defined.

By Lemma 2.1, any $\gamma \in \mathrm{Pin}(n)$ satisfies

$$N(\alpha(\gamma)i(v)\gamma^{-1}) = N(\alpha(\gamma))N(i(v))N(\gamma^{-1}) = N(i(v)) = \|v\|^2 \cdot \mathbf{1}.$$

That is, the transformation of $\mathbb{R}^d$ induced by the action of γ preserves the Euclidean norm, and is thus in $\mathrm{O}(d)$. Letting $\rho : \mathrm{Pin}(d) \to \mathrm{O}(d)$ be defined by $\rho(x)(v) = i^{-1}(\alpha(x)i(v)x^{-1})$, we get that ρ is surjective with kernel $\{\mathbf{1}, -\mathbf{1}\}$. That is, $\mathrm{Pin}(d)$ is a double cover of $\mathrm{O}(d)$. In the special case where $\gamma = i(w) \in i(\mathbb{R}^d) \subseteq \mathrm{Pin}(d)$, the action of $\rho(\gamma)$ corresponds to a reflection of $\mathbb{R}^d$ about the hyperplane orthogonal to w and incident to the origin.

The restricted transformation $\rho : \mathrm{Spin}(d) \to \mathrm{SO}(d)$ is also surjective with kernel $\{\mathbf{1}, -\mathbf{1}\}$. For some intuition, recall that the composition of two reflections about hyperplanes incident to the origin is a rotation centered at the origin. Thus, the tensor product of two elements of $i(\mathbb{R}^d)$ corresponds to a rotation in $\mathrm{Spin}(d)$. Similarly, the composition of rotations around the origin is a rotation around the origin.

A proof of the following lemma can be found in [5, Section 1.4].

Lemma 2.2. *Let $d \le 5$ and let $x \in C\ell_d^0$ satisfy $N(x) = \mathbf{1}$. Then for every $v \in \mathbb{R}^d$ we have $xi(v)x^{-1} \in i(\mathbb{R}^d)$.*

The claim of Lemma 2.2 is false for $d \ge 6$. Combining this lemma with the definition in (1) yields the following result.

Corollary 2.3. *For $d \le 5$, we have*

$$\mathrm{Spin}(d) = \{x \in C\ell_d^{0\times} \ : N(x) = \mathbf{1}\}.$$

We will also rely on the following observation.

Lemma 2.4. *If $u, v \in \mathbb{R}^d$ are orthogonal vectors then $i(u)i(v) = -i(v)i(u)$.*

Proof. We set $u' = u/\|u\|$ and $v' = v/\|v\|$, so that $u', v' \in \mathbb{S}^{d-1}$. Since u and v are orthogonal, so are u' and v'. Thus, there exists $\gamma \in \mathrm{Spin}(d)$ that corresponds to a rotation taking e_1 to u' and e_2 to v'. Since $e_1e_2 = -e_2e_1$, we have

$$\gamma e_1 \gamma^{-1} \gamma e_2 \gamma^{-1} = -\gamma e_2 \gamma^{-1} \gamma e_1 \gamma^{-1} \quad \text{which implies} \quad i(u')i(v') = -i(v')i(u').$$

The assertion of the lemma is obtained by multiplying both sides by $\|u\| \cdot \|v\|$.

The above argument holds for $d \ge 3$. When $d = 2$, there might not exist $\gamma \in \mathrm{Spin}(d)$ that takes e_1 to u' and e_2 to v'. In that case we can consider instead $\gamma \in \mathrm{Spin}(d)$ that takes e_1 to v' and e_2 to u' $\square$

3 The group $\mathrm{Spun}(d)$

In this section we introduce the group $\mathrm{Spun}(d)$. We first construct a variant X_d of the Clifford algebra $C\ell_d$. Consider the direct sum $\bigoplus_{k \in \mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k}$, and let $\mathcal{I}$ be the ideal in this tensor algebra that is generated by

$$\{e_j \otimes e_k + e_k \otimes e_j : \ 1 \le 1 \le j, k \le d+1\} \bigcup \{e_{d+2} \otimes e_{d+2}\} \\ \bigcup \{e_j \otimes e_j + \mathbf{1}, e_{d+2} \otimes e_j - e_j \otimes e_{d+2} : \ 1 \le 1 \le j \le d+1\}.$$

Then we write X_d as the quotient

$$\bigoplus_{k \in \mathbb{N}} \left(\mathbb{R}^d\right)^{\otimes k} / \mathcal{I}.$$

For brevity we write e_ie_j instead of $e_i \otimes e_j$. Let $i : \mathbb{R}^d \to X_d$ be the linear map that takes the standard basis elements of $\mathbb{R}^d$ to $e_1, \ldots, e_d$, respectively. Let $\alpha : X_d \to X_d$ be the automorphism satisfying $\alpha(\mathbf{1}) = \mathbf{1}$, $\alpha(e_j) = -e_j$ for every $1 \le j \le d+1$, and $\alpha(e_{d+2}) = e_{d+2}$. Let $t : X_d \to X_d$ be the anti-automorphism satisfying $t(xy) = t(y)t(x)$, $t(e_j) = e_j$ for every $1 \le j \le d+2$, and $t(\mathbf{1}) = \mathbf{1}$. For example, when $d = 4$ we have

$$\alpha(e_3e_4 + e_1e_5e_6 + e_2e_6) = e_3e_4 + e_1e_5e_6 - e_2e_6,$$
$$t(e_3e_4 + e_1e_5e_6 + e_2e_6) = -e_3e_4 - e_1e_5e_6 + e_2e_6.$$

For every $x \in X$, we define the *conjugate* of x as $\overline{x} = \alpha(t(x)) = t(\alpha(x))$, and the norm of x as $N(x) = x\overline{x}$. Note that for every $x = i(v) \in i(\mathbb{R}^d)$ we have $\overline{x} = -x$, which in turn implies $N(x) = \|v\|^2 \cdot \mathbf{1}$.

We define the standard basis of X_d to consist of $\mathbf{1}$ and of the tensor products of any number of distinct elements from $\{e_1, \ldots, e_{d+2}\}$. It is not difficult to verify that this set generates X_d and is linearly independent. Let $Z_d^0 \subset X_d^0$ be the subspace generated by $\mathbf{1}$ and by products of an even number of elements from $\{e_1, e_2, \ldots, e_d, e_{d+1}e_{d+2}\}$ (note that $e_{d+1}e_{d+2}$ is a single element).

For $1 \le k \le d+1$, note that the subspace of X_k generated by $\mathbf{1}$ and by products of distinct elements from $\{e_1, \ldots, e_k\}$ is a subalgebra of X_d. This subalgebra is isomorphic to the Clifford algebra $C\ell_k$, and we thus refer to it as $C\ell_k$. With this notation, the above definition of the norm $N(\cdot)$ of X_d generalizes the definition of a norm in $C\ell_k$. Similarly, the subalgebra $C\ell_d^0$ is contained in Z_d^0.

We are now ready to define our variant of $\text{Spin}(d)$.

$$\text{Spun}(d) = \big\{ z \in Z_d^0 :\ N(z) = \mathbf{1} \text{ and for every } v \in \mathbb{R}^d \text{ there exists } w \in \mathbb{R}^d \text{ such that } z\,(e_{d+2}i(v) + e_{d+1})\,\overline{z} = e_{d+2}i(w) + e_{d+1} \big\}. \tag{2}$$

We will prove that $\text{Spun}(d)$ is indeed a group and a double cover of $\text{SE}(d)$. But first we give a brief intuition for the definition in (2). We can think of this definition as extending $\text{Spin}(d)$ with the two extra elements e_{d+1} and e_{d+2}. The addition of e_{d+1} leads us to the group $\text{Spin}(d+1)$, which is a double cover of $\text{SO}(d+1)$. The role of e_{d+2} is to imitate a scaling limit argument as in [11]. We think of e_{d+2} as a small $\varepsilon > 0$, or as the restriction to a small disc on $\mathbb{S}^d$. As ε approaches zero, this disc behaves more like a flat so $\text{Spin}(d+1)$ becomes more similar to $\text{SE}(d)$.

Note that for every $\gamma \in \text{Spin}(d)$ we have that $\gamma e_{d+1} = e_{d+1}\gamma$, and similarly for e_{d+2}.

Theorem 3.1. *The set* $\text{Spun}(d)$ *is a group under the product operation of* X_d*. Moreover, the inverse of every* $x \in \text{Spun}(d)$ *is* $\overline{x}$*.*

Proof. We first show that for every $x, y \in \text{Spun}(d)$ we have $xy \in \text{Spun}(d)$. Indeed, note that

$$N(xy) = xy\overline{y}\,\overline{x} = xN(y)\overline{x} = x\overline{x} = N(x) = \mathbf{1}.$$

Moreover, for every $v \in \mathbb{R}^d$ there exist $u, w \in \mathbb{R}^d$ such that

$$xy\,(e_{d+2}i(v) + e_{d+1})\,\overline{xy} = x(y(e_{d+2}i(v) + e_{d+1})\overline{y})\overline{x} = x(e_{d+2}i(w) + e_{d+1})\overline{x} = e_{d+2}i(u) + e_{d+1}.$$

Since the product operation of X_d is clearly associative and $\mathbf{1}$ is the identity element, it remains to prove that every $x \in \text{Spun}(d)$ has an inverse in $\text{Spun}(d)$. We will prove that $x\overline{x} = \overline{x}x = \mathbf{1}$ and that $\overline{x} \in \text{Spun}(d)$. Fix $x \in \text{Spun}(d)$, and write $x = \gamma_1 + e_{d+1}e_{d+2}\gamma_2$ where $\gamma_1 \in C\ell_{d+1}^0$ and $\gamma_2 \in C\ell_d^1$. Since $x\overline{x} = N(x) = \mathbf{1}$, we have

$$\mathbf{1} = x\overline{x} = (\gamma_1 + e_{d+1}e_{d+2}\gamma_2)(\overline{\gamma_1} + e_{d+1}e_{d+2}\overline{\gamma_2}) = \gamma_1\overline{\gamma_1} + e_{d+2}(\gamma_1 e_{d+1}\overline{\gamma_2} + e_{d+1}\gamma_2\overline{\gamma_1}).$$

By comparing the parts that do not involve e_{d+2} on both sides of the equation, we get $\gamma_1\overline{\gamma_1} = \mathbf{1}$. By comparing the parts that contain e_{d+2}, we get $\gamma_1 e_{d+1}\overline{\gamma_2} = -e_{d+1}\gamma_2\overline{\gamma_1}$.

Since $x \in \mathrm{Spun}(d)$, for every $v \in \mathbb{R}^d$ there exists $w \in \mathbb{R}^d$ such that $x(e_{d+2}i(v) + e_{d+1})\overline{x} = e_{d+2}i(w) + e_{d+1}$. In particular, there exists $w_0 \in \mathbb{R}^d$ such that $xe_{d+1}\overline{x} = x(e_{d+2} \cdot i(0) + e_{d+1})\overline{x} = e_{d+2}i(w_0) + e_{d+1}$. Fixing $v, w \in \mathbb{R}^d$ as defined above and setting $u = w - w_0$ gives

$$e_{d+2}xi(v)\overline{x} = x(e_{d+2}i(v) + e_{d+1})\overline{x} - xe_{d+1}\overline{x} = e_{d+2}i(w) + e_{d+1} - (e_{d+2}i(w_0) + e_{d+1}) = e_{d+2}i(u).$$

We also have

$$e_{d+2}xi(v)\overline{x} = e_{d+2}(\gamma_1 + e_{d+1}e_{d+2}\gamma_2)i(v)(\overline{\gamma_1} + e_{d+1}e_{d+2}\overline{\gamma_2}) = e_{d+2}\gamma_1 i(v)\overline{\gamma_1}.$$

Combining the above gives $\gamma_1 i(v)\overline{\gamma_1} = i(u) \in i(\mathbb{R}^d)$. That is, $\gamma_1 i(v)\overline{\gamma_1} \in i(\mathbb{R}^d)$ for every $v \in \mathbb{R}^d$.

We have

$$\begin{aligned} e_{d+2}i(w_0) + e_{d+1} = xe_{d+1}\overline{x} &= (\gamma_1 + e_{d+1}e_{d+2}\gamma_2)\, e_{d+1}\, (\overline{\gamma_1} + e_{d+1}e_{d+2}\overline{\gamma_2}) \\ &= \gamma_1 e_{d+1}\overline{\gamma_1} + e_{d+2}\left(\gamma_1 e_{d+1}e_{d+1}\overline{\gamma_2} + e_{d+1}\gamma_2 e_{d+1}\overline{\gamma_1}\right). \end{aligned} \tag{3}$$

By again comparing the terms that do not involve e_{d+2} we get $\gamma_1 e_{d+1}\overline{\gamma_1} = e_{d+1}$.

Since $\gamma_1 i(v)\overline{\gamma_1} \in i(\mathbb{R}^d)$ for every $v \in \mathbb{R}^d$ and $\gamma_1 e_{d+1}\overline{\gamma_1} = e_{d+1}$, we get that $\gamma_1 i(v')\overline{\gamma_1} \in i(\mathbb{R}^{d+1})$ for every $v' \in \mathbb{R}^{d+1}$. Combining this with $N(\gamma_1) = \gamma_1\overline{\gamma_1} = \mathbf{1}$ implies that $\gamma_1 \in \mathrm{Spin}(d+1)$. In particular, the inverse of γ_1 is $\overline{\gamma_1}$. Multiplying the above equation $\gamma_1 e_{d+1}\overline{\gamma_1} = e_{d+1}$ by γ_1 from the right leads to $\gamma_1 e_{d+1} = e_{d+1}\gamma_1$. Since γ_1 commutes with e_{d+1} we have $\gamma_1 \in C\ell_d^0$, which in turn implies $\gamma_1 \in \mathrm{Spin}(d)$.

We next wish to show that $\overline{x}x = \mathbf{1}$. Since $x\overline{x} = \mathbf{1}$, it suffices to prove that $x\overline{x} = \overline{x}x$, or equivalently

$$\gamma_1\overline{\gamma_1} + e_{d+2}\left(\gamma_1 e_{d+1}\overline{\gamma_2} + e_{d+1}\gamma_2\overline{\gamma_1}\right) = \overline{\gamma_1}\gamma_1 + e_{d+2}\left(e_{d+1}\overline{\gamma_2}\gamma_1 + \overline{\gamma_1}e_{d+1}\gamma_2\right).$$

Since the inverse of γ_1 is $\overline{\gamma_1}$, we have that $\gamma_1\overline{\gamma_1} = \mathbf{1} = \overline{\gamma_1}\gamma_1$. It remains to prove that

$$\gamma_1 e_{d+1}\overline{\gamma_2} + e_{d+1}\gamma_2\overline{\gamma_1} = e_{d+1}\overline{\gamma_2}\gamma_1 + \overline{\gamma_1}e_{d+1}\gamma_2.$$

Since e_{d+1} commutes with γ_1 and $\overline{\gamma_1}$, this equation becomes $\gamma_1\overline{\gamma_2} + \gamma_2\overline{\gamma_1} = \overline{\gamma_2}\gamma_1 + \overline{\gamma_1}\gamma_2$.

Above we proved that $\gamma_1 e_{d+1}\overline{\gamma_2} = -e_{d+1}\gamma_2\overline{\gamma_1}$. Since e_{d+1} commutes with γ_1 and $\overline{\gamma_1}$, we get $\gamma_1\overline{\gamma_2} = -\gamma_2\overline{\gamma_1}$. Multiplying by $\overline{\gamma_1}$ from the left and by γ_1 from the right gives $\overline{\gamma_2}\gamma_1 = -\overline{\gamma_1}\gamma_2$. Combining these two inequalities leads to the required equation $\gamma_1\overline{\gamma_2} + \gamma_2\overline{\gamma_1} = 0 \cdot \mathbf{1} = \overline{\gamma_2}\gamma_1 + \overline{\gamma_1}\gamma_2$. We conclude that $\overline{x}x = \mathbf{1}$. That is, $x^{-1} = \overline{x}$.

To complete the proof of the lemma we need to show that $\overline{x} \in \mathrm{Spun}(d)$. We already know that $N(\overline{x}) = \overline{x}x = \mathbf{1}$. It remains to prove that for every $v \in \mathbb{R}^d$ there exists $w \in \mathbb{R}^d$ such that $\overline{x}\left(e_{d+2}i(v) + e_{d+1}\right)x = e_{d+2}i(w) + e_{d+1}$.

By considering the coefficients of e_{d+2} in (3), we get

$$i(w_0) = \gamma_1 e_{d+1}e_{d+1}\overline{\gamma_2} + e_{d+1}\gamma_2 e_{d+1}\overline{\gamma_1} = \gamma_2\overline{\gamma_1} - \gamma_1\overline{\gamma_2}.$$

Multiplying by γ_1 from the right and by $\overline{\gamma_1}$ from the left gives $\overline{\gamma_1}i(w_0)\gamma_1 = \overline{\gamma_1}\gamma_2 - \overline{\gamma_2}\gamma_1$. Since $\overline{\gamma_1} \in \mathrm{Spin}(d)$, there exists $w_1 \in \mathbb{R}^d$ such that $\overline{\gamma_1}i(w_0)\gamma_1 = i(w_1)$.

We have that

$$\overline{x}e_{d+1}x = (\overline{\gamma_1} + e_{d+1}e_{d+2}\overline{\gamma_2})\, e_{d+1}\, (\gamma_1 + e_{d+1}e_{d+2}\gamma_2) = e_{d+1} + e_{d+2}\left(\overline{\gamma_2}\gamma_1 - \overline{\gamma_1}\gamma_2\right) = e_{d+1} - e_{d+2}i(w_1).$$

Since $\overline{\gamma_1} \in \mathrm{Spin}(d)$, for every $v \in \mathbb{R}^d$ there exists $u \in \mathbb{R}^d$ such that $\overline{\gamma_1} i(v)\gamma_1 = i(u)$. By combining the above, we get

$$\begin{aligned}\overline{x}\left(e_{d+2}i(v) + e_{d+1}\right)x &= e_{d+2}\overline{x}i(v)x + \overline{x}e_{d+1}x \\ &= e_{d+2}\left(\overline{\gamma_1} + e_{d+1}e_{d+2}\overline{\gamma_2}\right)i(v)\left(\gamma_1 + e_{d+1}e_{d+2}\gamma_2\right) + e_{d+1} - e_{d+2}i(w_1) \\ &= e_{d+2}\left(\overline{\gamma_1}i(v)\gamma_1 - i(w_1)\right) + e_{d+1} = e_{d+2}i(u - w_1) + e_{d+1}.\end{aligned}$$

□

Now that we established the $\mathrm{Spun}(d)$ is a group, we start to study its structure.

Lemma 3.2. *We have* $\mathrm{Spun}(d) = \{\gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right) : \gamma \in \mathrm{Spin}(d),\ v \in \mathbb{R}^d\}$. *Every element of* $\mathrm{Spun}(d)$ *corresponds to a unique pair* $(\gamma, v) \in \mathrm{Spin}(d) \times \mathbb{R}^d$.

Proof. For arbitrary $\gamma \in \mathrm{Spin}(d)$ and $v \in \mathbb{R}^d$, we set $x = \gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right)$. Then

$$\begin{aligned}N(x) = \gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right)\left(\overline{\mathbf{1} + e_{d+1}e_{d+2}i(v)}\right)\overline{\gamma} &= \gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right)\left(\mathbf{1} - e_{d+1}e_{d+2}i(v)\right)\overline{\gamma} \\ &= \gamma(\mathbf{1} - e_{d+1}e_{d+2}i(v) + e_{d+1}e_{d+2}i(v))\overline{\gamma} = \gamma\overline{\gamma} = \mathbf{1}.\end{aligned}$$

Since $\gamma \in \mathrm{Spin}(d)$, there exists $w_1 \in \mathbb{R}^d$ such that $\gamma i(v)\overline{\gamma} = i(w_1)$. For every $u \in \mathbb{R}^d$ there exists $w_2 \in \mathbb{R}^d$ such that $\gamma i(u)\overline{\gamma} = i(w_2)$, so

$$\begin{aligned}&x(e_{d+2}i(u) + e_{d+1})\overline{x} = e_{d+2}(xi(u)\overline{x}) + xe_{d+1}\overline{x} \\ &\quad = e_{d+2}\gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right)i(u)\left(\mathbf{1} - e_{d+1}e_{d+2}i(v)\right)\overline{\gamma} + \gamma\left(e_{d+1} + e_{d+2}i(v)\right)\left(\mathbf{1} - e_{d+1}e_{d+2}i(v)\right)\overline{\gamma} \\ &\quad = e_{d+2}\gamma i(u)\overline{\gamma} + \gamma(e_{d+1} + 2e_{d+2}i(v))\overline{\gamma} = e_{d+2}i(w_2 + 2w_1) + e_{d+1} \in \left(e_{d+2}i(\mathbb{R}^d) + e_{d+1}\right).\end{aligned}$$

We conclude that $\{\gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right) : \gamma \in \mathrm{Spin}(d), v \in \mathbb{R}^d\} \subseteq \mathrm{Spun}(d)$.

For the other direction, consider an element $x \in \mathrm{Spun}(d)$, and recall from the proof of Theorem 3.1 that $x = \gamma_1 + e_{d+1}e_{d+2}\gamma_2$ for some $\gamma_1 \in \mathrm{Spin}(d)$ and $\gamma_2 \in C\ell_d^1$. By definition, there exists $w_0 \in \mathbb{R}^d$ such that $xe_{d+1}\overline{x} = x(e_{d+2}i(0) + e_{d+1}\overline{x} = e_{d+2}i(w_0) + e_{d+1}$. In the proof of Theorem 3.1 it is also shown that $i(w_0) = \gamma_2\overline{\gamma_1} - \gamma_1\overline{\gamma_2}$ and that $\gamma_1\overline{\gamma_2} = -\gamma_2\overline{\gamma_1}$. Together these imply $\gamma_2\overline{\gamma_1} = i(w_0)/2$. Since $\gamma_1 \in \mathrm{Spin}(d)$, it has the inverse $\overline{\gamma_1}$. Thus, there exists $w_1 \in \mathbb{R}^d$ such that

$$\gamma_2 = (\gamma_2\overline{\gamma_1})\gamma_1 = i(w_0)\gamma_1/2 = \gamma_1\overline{\gamma_1}i(w_0)\gamma_1/2 = \gamma_1 i(w_1)/2.$$

We conclude that $x = \gamma_1(\mathbf{1} + e_{d+1}e_{d+2}i(w_1)/2)$ where $\gamma_1 \in \mathrm{Spin}(d)$. That is, $\mathrm{Spun}(d) \subseteq \{\gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(v)\right) : \gamma \in \mathrm{Spin}(d), v \in \mathbb{R}^d\}$.

Note that γ is uniquely determined by x, since it is exactly the part of x that does not involve e_{d+2}. Once γ is fixed, there is a unique $v \in \mathbb{R}^d$ that satisfies $\gamma e_{d+1}e_{d+2}i(v) = e_{d+1}e_{d+2}\gamma_2$. That is, the pair (γ, v) is uniquely determined. □

Recall that every transformation of $\mathrm{SE}(d)$ can be seen as a translation followed by a rotation, which is a pair in $\mathrm{SO}(d) \times \mathbb{R}^d$. Lemma 3.2 states that every element of $\mathrm{Spun}(d)$ corresponds to a unique pair of $\mathrm{Spin}(d) \times \mathbb{R}^d$. Since $\mathrm{Spin}(d)$ is a double cover of $\mathrm{SO}(d)$, we are starting to see why $\mathrm{Spun}(d)$ is a double cover of $\mathrm{SE}(d)$. The following result proves this property, and provides a variant of the homomorphism $\rho : \mathrm{Spin}(d) \to \mathrm{SO}(d)$ defined above.

Theorem 3.3. *For every d there exists a surjective group homomorphism* $\rho : \mathrm{Spun}(d) \to \mathrm{SE}(d)$ *with* $\ker(\rho) = \{-1, 1\}$. *That is,* $\mathrm{Spun}(d)$ *is a double cover of* $\mathrm{SE}(d)$.

Proof. Let $a \in \mathbb{R}^d$ be a fixed point. By Lemma 3.2, any element $x \in \text{Spun}(d)$ can be written as $\gamma_x (\mathbf{1} + e_{d+1}e_{d+2}i(v_x))$ where $\gamma_x \in \text{Spin}(d)$ and $v_x \in \mathbb{R}^d$ are uniquely determined. We set $p_x = \gamma_x i(a + 2v_x)\overline{\gamma_x}$ and note that $p_x \in i(\mathbb{R}^d)$. We have

$$\gamma_x + \frac{1}{2}e_{d+1}e_{d+2}\left(p_x\gamma_x - \gamma_x i(a)\right) = \gamma_x + \frac{1}{2}e_{d+1}e_{d+2} \cdot 2\gamma_x i(v_x) = \gamma_x(\mathbf{1} + e_{d+1}e_{d+2}i(v_x)) = x. \quad (4)$$

Thus, for any $x \in \text{Spun}(d)$ there exist unique $p_x \in i(\mathbb{R}^d)$ and $\gamma_x \in \text{Spin}(d)$ such that $x = \gamma_x + \frac{1}{2}e_{d+1}e_{d+2}\left(p_x\gamma_x - \gamma_x i(a)\right)$. We now rely on this observation to define the map $\rho : \text{Spun}(d) \to \text{SE}(d)$. For any $v \in \mathbb{R}^d$, denote the translation of $\mathbb{R}^d$ by v as $v^+ \in \text{SE}(d)$. Similarly, for any $p \in i(\mathbb{R}^d)$, we set $p^+ = (i^{-1}(p))^+ \in \text{SE}(d)$. As stated in Section 2, there is a unique $\Gamma_x \in \text{SO}(d)$ that corresponds to γ_x. We set

$$\rho(x) = p_x^+ \circ \Gamma_x \circ (-a)^+.$$

Note that p_x and Γ_x are uniquely determined by x. Recalling that a is fixed, we conclude that the map $\rho(\cdot)$ is well-defined.

For every $p \in i(\mathbb{R}^d)$ and $\gamma \in \text{Spin}(d)$, by setting $i(u) = \frac{1}{2}\left(\overline{\gamma}p\gamma - i(a)\right) \in i(\mathbb{R}^d)$ we get

$$\gamma\left(\mathbf{1} + e_{d+1}e_{d+2}i(u)\right) = \gamma + \frac{1}{2}e_{d+1}e_{d+2}\left(p\gamma - \gamma i(a)\right).$$

Combining this with (4) and with Lemma 3.2 implies that for every $p \in i(\mathbb{R}^d)$ and $\gamma \in \text{Spin}(d)$ there exists $x \in \text{Spun}(d)$ such that $p = p_x$ and $\gamma = \gamma_x$. Every transformation $M \in \text{SE}(d)$ can be written as $(M(a))^+ \circ R \circ (-a)^+$ for some transformation $R \in \text{SO}(d)$. Indeed, note that for any $R \in \text{SO}(d)$ the map $(M(a))^+ \circ R \circ (-a)^+$ takes a to $M(a)$, so we just need to choose the R that rotates the space properly around a. We conclude that ρ is surjective.

For $x, y \in \text{Spun}(d)$, we now consider how the product $xy \in \text{Spun}(d)$ behaves. Since $\overline{\gamma_y} \in \text{Spin}(d)$, there exists $v_z \in \mathbb{R}^d$ such that $i(v_z) = \overline{\gamma_y}i(v_x)\gamma_y$. Then

$$\begin{aligned}
xy &= \gamma_x\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_x)\right)\gamma_y\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_y)\right) \\
&= \gamma_x\left(\gamma_y + e_{d+1}e_{d+2}i(v_x)\gamma_y\right)\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_y)\right) \\
&= \gamma_x\gamma_y\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_z)\right)\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_y)\right) = \gamma_x\gamma_y\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_z + v_y)\right).
\end{aligned}$$

This implies that $\gamma_{xy} = \gamma_x\gamma_y$ and that $v_{xy} = v_z + v_y$. This in turn implies that $p_{xy} = \gamma_{xy}i(a + 2v_z + 2v_y)\overline{\gamma_{xy}}$. We are now ready to verify that ρ is a group homomorphism. Note that the action of γ_{xy} is first performing the action of γ_y and then the action of γ_x. That is, $\Gamma_{xy} = \Gamma_x \circ \Gamma_y$. For the same reason we have

$$\begin{aligned}
\rho(x)\rho(y) &= p_x^+ \circ \Gamma_x \circ (-a)^+ \circ p_y^+ \circ \Gamma_y \circ (-a)^+ = p_x^+ \circ \Gamma_x \circ (p_y - i(a))^+ \circ \Gamma_y \circ (-a)^+ \\
&= p_x^+ \circ (\gamma_x(p_y - i(a))\overline{\gamma_x})^+ \circ \Gamma_x \circ \Gamma_y \circ (-a)^+ \\
&= (p_x + \gamma_x(p_y - i(a))\overline{\gamma_x})^+ \circ \Gamma_{xy} \circ (-a)^+ \\
&= \left(\gamma_x\left(i(a + 2v_x) + \gamma_y i(a + 2v_y)\overline{\gamma(y)} - i(a)\right)\overline{\gamma_x}\right)^+ \circ \Gamma_{xy} \circ (-a)^+ \\
&= (\gamma_x\gamma_y(2\overline{\gamma_y}i(v_x)\gamma_y + i(a + 2v_y))\overline{\gamma_x\gamma_y})^+ \circ \Gamma_{xy} \circ (-a)^+ \\
&= (\gamma_{xy}i(a + 2v_{xy})\overline{\gamma_{xy}})^+ \circ \Gamma_{xy} \circ (-a)^+ = p_{xy}^+ \circ \Gamma_{xy} \circ (-a)^+ = \rho(xy).
\end{aligned}$$

It remains to find the kernel of the homomorphism ρ. Let I be identity element of $\text{SE}(d)$ and let $x \in \text{Spun}(d)$ satisfy $\rho(x) = p_x^+ \circ \Gamma_x \circ (-a)^+ = I$. That is, $p_x^+ \circ \Gamma_x = a^+$. The composition of a rotation and a translation cannot be a translation, so Γ_x is the identity of $\mathrm{SO}(d)$ and $p_x = i(a)$. This implies that $\gamma_x \in \{-\mathbf{1}, \mathbf{1}\} \subset \mathrm{Spin}(d)$. Combining the above with (4) gives

$$\ker(\rho) = \rho^{-1}(I) = \left\{ -\mathbf{1} + \frac{1}{2} e_{d+1} e_{d+2} \left(-i(a) + i(a) \right), \mathbf{1} + \frac{1}{2} e_{d+1} e_{d+2} \left(i(a) - i(a) \right) \right\} = \{-\mathbf{1}, \mathbf{1}\}.$$

□

Let $\tau : \{e_{d+2} i(v) + e_{d+1} : v \in \mathbb{R}^n\} \to \mathbb{R}^n$ be the map defined by $\tau(e_{d+2} i(v) + e_{d+1}) = v$. The following lemma studies the behaviour of the homomorphism ρ from Theorem 3.3.

Lemma 3.4. *For every $w \in \mathbb{R}^d$ and $x \in \mathrm{Spun}(d)$,*

$$\rho(x)(w) = \tau(x(e_{d+2} i(w) + e_{d+1})\overline{x}).$$

Proof. By Lemma 3.2, every $x \in \mathrm{Spun}(d)$ can be written as $\gamma_x \left(\mathbf{1} + e_{d+1} e_{d+2} i(v_x) \right)$ for some $\gamma_x \in \mathrm{Spin}(d)$ and $v_x \in \mathbb{R}^d$. Recalling that $p_x = \gamma_x i(a + 2v_x)\overline{\gamma_x}$, we have

$$\begin{aligned} x(e_{d+2} i(w) + e_{d+1})\overline{x} &= \gamma_x \left(\mathbf{1} + e_{d+1} e_{d+2} i(v_x) \right) \left(e_{d+2} i(w) + e_{d+1} \right) \left(\mathbf{1} - e_{d+1} e_{d+2} i(v_x) \right) \overline{\gamma_x} \\ &= \gamma_x e_{d+2} i(w) \overline{\gamma_x} + \gamma_x \left(\mathbf{1} + e_{d+1} e_{d+2} i(v_x) \right) e_{d+1} \left(\mathbf{1} - e_{d+1} e_{d+2} i(v_x) \right) \overline{\gamma_x} \\ &= e_{d+2} \gamma_x i(w) \overline{\gamma_x} + \gamma_x \left(e_{d+1} + e_{d+1} e_{d+2} i(v_x) e_{d+1} - e_{d+1} e_{d+1} e_{d+2} i(v_x) \right) \overline{\gamma_x} \\ &= e_{d+2} \gamma_x (i(w) + 2i(v_x)) \overline{\gamma_x} + \gamma_x e_{d+1} \overline{\gamma_x} \\ &= e_{d+2} \big(p_x + \gamma_x (i(w) - i(a)) \overline{\gamma_x} \big) + e_{d+1}. \end{aligned}$$

That is, the operation of $\tau(x(e_{d+2} i(w) + e_{d+1})\overline{x})$ can be seen as first translating w by $-a$, then performing the rotation of $\gamma_x \in \mathrm{Spin}(d)$, and finally translating by p_x. This is exactly the operation $\rho(x) = p_x^+ \circ \Gamma_x \circ (-a)^+$. □

For $w \in \mathbb{R}^d$ and $x \in \mathrm{Spun}(d)$, we write $w^x = \rho(x)(w) = \tau(x(e_{d+2} i(w) + e_{d+1})\overline{x})$.

3.1 The sets T_{ap}

Given points $a, p \in \mathbb{R}^d$, we define

$$T_{ap} = \left\{ x \in \mathrm{Spun}(d) : \ a^x = p \right\}. \tag{5}$$

That is, T_{ap} is the set of elements of $\mathrm{Spun}(d)$ that correspond to a proper rigid motion of $\mathbb{R}^d$ that takes a to p. In this section we study the structure of T_{ap}. We begin by presenting a relatively simple description of this set.

Lemma 3.5. *For any $a, p \in \mathbb{R}^d$, we have*

$$T_{ap} = \left\{ \gamma + \frac{1}{2} e_{d+1} e_{d+2} \left(i(p)\gamma - \gamma i(a) \right) : \gamma \in \mathrm{Spin}(d) \right\}.$$

Proof. Let $x \in \left\{ \gamma + \frac{1}{2} e_{d+1} e_{d+2} \left(i(p)\gamma - \gamma i(a) \right) : \gamma \in \mathrm{Spin}(d) \right\}$. That is, there exists $\gamma_x \in \mathrm{Spin}(d)$ such that $x = \gamma_x + \frac{1}{2} e_{d+1} e_{d+2} \left(i(p)\gamma_x - \gamma_x i(a) \right)$. We get that

$$\begin{aligned} N(x) = x\overline{x} &= \left(\gamma_x + \frac{1}{2} e_{d+1} e_{d+2} \left(i(p)\gamma_x - \gamma_x i(a) \right) \right) \left(\overline{\gamma_x} + \frac{1}{2} e_{d+1} e_{d+2} \left(i(a)\overline{\gamma_x} - \overline{\gamma_x} i(p) \right) \right) \\ &= \gamma_x \overline{\gamma_x} + \frac{1}{2} e_{d+1} e_{d+2} \left(\gamma_x i(a) \overline{\gamma_x} - i(p) + i(p) - \gamma_x i(a) \overline{\gamma_x} \right) = \mathbf{1}. \end{aligned}$$

For every $u \in \mathbb{R}^d$ we have

$$\begin{aligned}
&x(e_{d+2}i(u) + e_{d+1})\overline{x} \\
&\quad = \left(\gamma_x + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)\gamma_x - \gamma_x i(a)\right)\right)\left(e_{d+2}i(u) + e_{d+1}\right)\left(\overline{\gamma_x} + \frac{1}{2}e_{d+1}e_{d+2}\left(i(a)\overline{\gamma_x} - \overline{\gamma_x}i(p)\right)\right) \\
&\quad = \gamma_x(e_{d+2}i(u) + e_{d+1})\overline{\gamma_x} + \frac{1}{2}e_{d+2}\big(e_{d+1}\left(i(p)\gamma_x - \gamma_x i(a)\right)e_{d+1}\overline{\gamma_x} + \gamma_x e_{d+1}e_{d+1}\left(i(a)\overline{\gamma_x} - \overline{\gamma_x}i(p)\right)\big) \\
&\quad = e_{d+2}\gamma_x i(v)\overline{\gamma_x} + e_{d+1} + \frac{1}{2}e_{d+2}\big(\left(i(p) - \gamma_x i(a)\overline{\gamma_x}\right) - \left(\gamma_x i(a)\overline{\gamma_x} - i(p)\right)\big) \\
&\quad = e_{d+2}\left(\gamma_x i(v-a)\overline{\gamma_x} + i(p)\right) + e_{d+1} \in \left(e_{d+2}i(\mathbb{R}^d) + e_{d+1}\right). \qquad (6)
\end{aligned}$$

By combining the above, we get that $x \in \mathrm{Spun}(d)$. From (6) we obtain

$$x(e_{d+2}i(a) + e_{d+1})\overline{x} = e_{d+2}\left(\gamma_x i(a-a)\overline{\gamma_x} + i(p)\right) + e_{d+1} = e_{d+2}i(p) + e_{d+1}.$$

Since the action of x takes a to p, we have that $x \in T_{ap}$. This in turn implies

$$\left\{\gamma + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)\gamma - \gamma i(a)\right) : \gamma \in \mathrm{Spin}(d)\right\} \subseteq T_{ap}.$$

For the other direction, consider $y \in T_{ap} \subset \mathrm{Spun}(d)$. By Lemma 3.2, there exist $\gamma_y \in \mathrm{Spin}(d)$ and $v_y \in \mathbb{R}^d$ such that $y = \gamma_y\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_y)\right)$. We also know that

$$\begin{aligned}
e_{d+2}i(p) + e_{d+1} &= y(e_{d+2}i(a) + e_{d+1})\overline{y} \\
&= \gamma_y\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_y)\right)\left(e_{d+2}i(a) + e_{d+1}\right)\left(\mathbf{1} - e_{d+1}e_{d+2}i(v_y)\right)\overline{\gamma_y} \\
&= \gamma_y\left(e_{d+2}i(a) + e_{d+1} + e_{d+1}e_{d+2}i(v_y)e_{d+1} - e_{d+1}e_{d+1}e_{d+2}i(v_y)\right)\overline{\gamma_y} \\
&= e_{d+2}\gamma_y\left(i(a) + 2i(v_y)\right)\overline{\gamma_y} + e_{d+1}.
\end{aligned}$$

The above calculation implies that $i(p) = \gamma_y\left(i(a) + 2i(v_y)\right)\overline{\gamma_y}$. After rearranging we get $i(v_y) = (\overline{\gamma_y}i(p)\gamma_y - i(a))/2$. We thus have

$$\begin{aligned}
y = \gamma_y\left(\mathbf{1} + e_{d+1}e_{d+2}i(v_y)\right) &= \gamma_y\left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}(\overline{\gamma_y}i(p)\gamma_y - i(a))\right) \\
&= \gamma_y + \frac{1}{2}e_{d+1}e_{d+2}(i(p)\gamma_y - \gamma_y i(a)).
\end{aligned}$$

We conclude that $T_{ap} \subseteq \left\{\gamma + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)\gamma - \gamma i(a)\right) : \gamma \in \mathrm{Spin}(d)\right\}$, which in turn implies that the two sets are identical. $\square$

The following lemma provides a more geometric representation of the sets T_{ap}: the intersection of $\mathrm{Spun}(d)$ with the linear subspace. Let

$$F_{ap} = \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)C\ell_d^0\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right). \qquad (7)$$

Lemma 3.6. *For $a, p \in \mathbb{R}^d$, we have $T_{ap} = F_{ap} \cap \mathrm{Spun}(d)$.*

Proof. Let $x \in F_{ap} \cap \mathrm{Spun}(d)$. Since $x \in F_{ap}$, there exists $\delta \in C\ell_d^0$ such that

$$x = \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)\delta\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) = \delta + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)\delta - \delta i(a)\right). \qquad (8)$$

As in the proof of Theorem 3.3, since $x \in \mathrm{Spun}(d)$ there exist $\gamma_x \in \mathrm{Spin}(d)$ and $p_x \in i(\mathbb{R}^d)$ such that $x = \gamma_x + \frac{1}{2}e_{d+1}e_{d+2}\left(p_x\gamma_x - \gamma_x i(a)\right)$. Combining this with (8) implies that $\gamma_x = \delta$ and $p_x = i(p)$. By Lemma 3.5 we get that $x \in T_{ap}$. We conclude that $F_{ap} \cap \mathrm{Spun}(d) \subseteq T_{ap}$.

For the other direction, consider $x \in T_{ap}$. By Lemma 3.5, there exists $\gamma \in \mathrm{Spin}(d)$ such that

$$x = \gamma + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)\gamma - \gamma i(a)\right) = \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)\gamma\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) \in F_{ap}.$$

That is $T_{ap} \subseteq F_{ap}$. By definition, we have that $T_{ap} \subset \mathrm{Spun}(d)$. This implies $T_{ap} \subseteq \mathrm{Spun}(d) \cap F_{ap}$ and completes the proof of the lemma. □

4 Distinct distances in $\mathbb{R}^3$

In this section we prove Theorem 1.2 for the case of $\mathbb{R}^3$. The proof is based on the Spun(3) group that was defined in Section 3. We note that $C\ell_3^0$ is isomorphic to $\mathbb{R}^4$ as a vector space. Specifically, we consider the basis $\mathbf{1}, e_1e_2, e_1e_3, e_2e_3$ of $C\ell_3^0$ and write

$$x = x_1 \cdot \mathbf{1} + x_2e_1e_2 + x_3e_1e_3 + x_4e_2e_3.$$

Lemma 4.1. *For every $x \in C\ell_3^0$ we have $N(x) = \sum_{j=1}^4 x_j^2 \cdot \mathbf{1}$.*

Proof. Using the above notation

$$\overline{x} = \alpha(t(x_1 \cdot \mathbf{1} + x_2e_1e_2 + x_3e_1e_3 + x_4e_2e_3)) = x_1 \cdot \mathbf{1} - x_2e_1e_2 - x_3e_1e_3 - x_4e_2e_3.$$

This immediately implies $N(x) = x\overline{x} = x_1^2 + x_2^2 + x_3^2 + x_4^2$. □

By combining Corollary 2.3 and Lemma 4.1, we get that

$$\mathrm{Spin}(3) = \left\{ (x_1, x_2, x_3, x_4) \in C\ell_3^0 : \sum_{j=1}^4 x_j^2 = 1 \right\}. \tag{9}$$

We are now ready to derive our reduction for distinct distances in $\mathbb{R}^3$.

Theorem 4.2. *The problem of deriving a lower bound on the minimum number of distinct distances spanned by n points in $\mathbb{R}^3$ can be reduced to the following problem:*

> *Let $\mathcal{F}$ be a set of n distinct 2-flats in $\mathbb{R}^5$, such that every two flats intersect in at most one point, every point of $\mathbb{R}^5$ is contained in $O(\sqrt{n})$ flats of $\mathcal{F}$, and every hyperplane in $\mathbb{R}^5$ contains $O(\sqrt{n})$ of these flats. Find an upper bound on the number of k-rich points, for every $2 \le k = O(n^{1/3+\varepsilon})$ (for some $\varepsilon > 0$).*

Deriving the bound $O\left(\frac{n^{5/3}}{k^{2+\varepsilon}}\right)$ for the number of k-rich points would yield the conjectured lower bound of $\Omega(n^{2/3})$ distinct distances.

Proof. Let $\mathcal{P}$ be a set of n points in $\mathbb{R}^3$. Let D denote the number of distinct distances that are spanned by $\mathcal{P}$, and denote these distances as $\delta_1, \ldots, \delta_D$. Recalling that $|uv|$ is the distance between the points u and v, we set

$$Q = \left\{(a, b, p, q) \in \mathcal{P}^4 : |ab| = |pq| > 0\right\}.$$

The quadruples of Q are ordered, so (a,b,p,q) and (b,a,p,q) are considered as two distinct elements of Q. The proof is based on double counting $|Q|$.

For every $j \in \{1,\ldots,D\}$, let $E_j = \{(a,b) \in \mathcal{P}^2 : |ab| = \delta_j\}$. Since every ordered pair of distinct points $(a,b) \in \mathcal{P}^2$ appears in exactly one set E_j, we have that $\sum_{j=1}^{D} |E_j| = n^2 - n > n^2/2$. The Cauchy-Schwarz inequality implies

$$|Q| = \sum_{j=1}^{D} |E_j|^2 \geq \frac{1}{D}\left(\sum_{j=1}^{D} |E_j|\right)^2 > \frac{n^4}{4D}. \tag{10}$$

For $a,b,p,q \in \mathbb{R}^3$ with $a \neq b$, we have $|ab| = |pq|$ if and only if there exists a proper rigid motion in SE(3) that takes both a to p and b to q. Thus, for every $(a,p) \in \mathcal{P}^2$ we set

$$R_{ap} = \{\gamma \in \mathrm{SE}(3) :\ a^\gamma = p\}.$$

To derive an upper bound for $|Q|$ it suffices to bound the number of quadruples $(a,b,p,q) \in \mathcal{P}^4$ that satisfy $a \neq b$ and $R_{ap} \cap R_{bq} \neq \emptyset$. Since we wish to work in Spun(3) rather than in SE(3), we recall the following definition from (5).

$$T_{ap} = \{x \in \mathrm{Spun}(3) :\ a^x = p\} = \rho^{-1}(R_{ap}).$$

Recall from Theorem 3.3 that the homomorphism ρ is surjective with kernel $\{\mathbf{1}, -\mathbf{1}\}$. That is, for every point of $R_{ap} \cap R_{bq}$ there are two corresponding points in $T_{ap} \cap T_{bq}$. It thus suffices to bound the number of quadruples $(a,b,p,q) \in \mathcal{P}^4$ that satisfy $a \neq b$ and $T_{ap} \cap T_{bq} \neq \emptyset$.

Before getting to the more technical details of the proof, we provide a brief sketch of the rest of the proof. We will show that Spun(3) can be embedded in $\mathbb{R}^8$ as a well-behaved six-dimensional variety (see Lemma 4.3). Under this embedding, each set T_{ap} is a three-dimensional variety that corresponds to an intersection of the Spun(3) variety with a four-dimensional linear subspace. We project the Spun(3) variety in $\mathbb{R}^8$ from the origin onto the hyperplane defined by $x_1 = 1$, and then perform a standard projection by removing the coordinates x_1 and x_8.

Combining the above projections gives a map that is a bijection between most of the Spun(3) variety and $\mathbb{R}^6$. This map takes each set T_{ap} to a 3-flat in $\mathbb{R}^6$, and every two such 3-flats are either disjoint or intersect in a line. Since the map is a bijection only after removing a small part of Spun(3), we get that a quadruple (a,p,b,q) is in Q if and only if the two corresponding 3-flats in $\mathbb{R}^6$ are contained in a common hyperplane. By performing a generic projective transformation and then intersecting the 3-flats with a hyperplane, we obtain an incidence problem between points and 2-flats in $\mathbb{R}^5$.

From Spun(3) **to** $\mathbb{R}^6$**.** Recall that Spun(3) is contained in the eight-dimensional subspace $Z_3^0 \subset X_3$ generated by $\mathbf{1}, e_1e_2, e_1e_3, e_2e_3, e_1e_4e_5, e_2e_4e_5, e_3e_4e_5, e_1e_2e_3e_4e_5$. We consider Z_3^0 as $\mathbb{R}^8$ by mapping these basis elements to the standard basis vectors of $\mathbb{R}^8$. That is, we write $x = x_1 \cdot \mathbf{1} + x_2e_1e_2 + x_3e_1e_3 + x_4e_2e_3 + x_5e_1e_4e_5 + x_6e_2e_4e_5 + x_7e_3e_4e_5 + x_8e_1e_2e_3e_4e_5$ as the point $(x_1, x_2, \ldots, x_8) \in \mathbb{R}^8$. With this notation, we study the behavior of Spun(3) as a set in $\mathbb{R}^8$. Set

$$G = \left\{x \in \mathbb{R}^8 :\ x_1x_8 - x_2x_7 + x_3x_6 - x_4x_5 = 0\right\} \quad \text{and} \quad \mathcal{C} = \left\{x \in \mathbb{R}^8 :\ x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\right\}.$$

Lemma 4.3. Spun(3) $= G \cap \mathcal{C}$.

Proof. For every $x \in Z_3^0$ we have

$$\begin{aligned}\overline{x} &= \alpha(t(x_1 \cdot \mathbf{1} + x_2e_1e_2 + x_3e_1e_3 + x_4e_2e_3 + x_5e_1e_4e_5 + x_6e_2e_4e_5 + x_7e_3e_4e_5 + x_8e_1e_2e_3e_4e_5)) \\ &= x_1 \cdot \mathbf{1} - x_2e_1e_2 - x_3e_1e_3 - x_4e_2e_3 - x_5e_1e_4e_5 - x_6e_2e_4e_5 - x_7e_3e_4e_5 + x_8e_1e_2e_3e_4e_5,\end{aligned}$$

and thus

$$N(x) = x\overline{x} = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right) \mathbf{1} + 2\left(x_1x_8 - x_2x_7 + x_3x_6 - x_4x_5\right) e_1e_2e_3e_4e_5. \qquad (11)$$

That is, $N(x) = \mathbf{1}$ if and only if $x \in \mathcal{C} \cap G$. Combining this with (2) implies that $\mathrm{Spun}(3) \subseteq \mathcal{C} \cap G$.

For the other direction, consider $x \in \mathcal{C} \cap G$. By (11) we have that $N(x) = \mathbf{1}$. Note that we can write $x = \gamma_1 + e_4e_5\gamma_2$ from some $\gamma_1 \in C\ell_3^0$ and $\gamma_2 \in C\ell_3^1$. We then get

$$\mathbf{1} = N(x) = (\gamma_1 + e_4e_5\gamma_2)(\overline{\gamma_1} + e_4e_5\overline{\gamma_2}) = \gamma_1\overline{\gamma_1} + e_4e_5(\gamma_1\overline{\gamma_2} + \gamma_2\overline{\gamma_1}).$$

This implies that $N(\gamma_1) = \gamma_1\overline{\gamma_1} = \mathbf{1}$ and $\gamma_1\overline{\gamma_2} = -\gamma_2\overline{\gamma_1}$. From (9) we get that $\gamma_1 \in \mathrm{Spin}(3)$.

Since $\gamma_2\overline{\gamma_1} \in C\ell_3^1$, there exist $u \in \mathbb{R}^3$ and $\lambda \in \mathbb{R}$ such that $\gamma_2\overline{\gamma_1} = i(u) + \lambda e_1e_2e_3$. Since $\overline{e_1e_2e_3} = e_1e_2e_3$, we have $\overline{\gamma_2\overline{\gamma_1}} = -i(u) + \lambda e_1e_2e_3$. On the other hand, we have

$$\overline{\gamma_2\overline{\gamma_1}} = \gamma_1\overline{\gamma_2} = -\gamma_2\overline{\gamma_1} = -i(u) - \lambda e_1e_2e_3.$$

Thus, it must be that $\lambda = 0$. This in turn implies that $\gamma_2\overline{\gamma_1} \in i(\mathbb{R}^3)$ and $\gamma_1\overline{\gamma_2} = -\gamma_2\overline{\gamma_1} \in i(\mathbb{R}^3)$.

For every $v \in \mathbb{R}^3$, we have

$$\begin{aligned}
x\left(e_5 i(v) + e_4\right)\overline{x} &= \left(\gamma_1 + e_4e_5\gamma_2\right)\left(e_5 i(v) + e_4\right)\left(\overline{\gamma_1} + e_4e_5\overline{\gamma_2}\right)\\
&= \gamma_1 e_5 i(v)\overline{\gamma_1} + (\gamma_1 + e_4e_5\gamma_2)e_4(\overline{\gamma_1} + e_4e_5\overline{\gamma_2})\\
&= e_5\gamma_1 i(v)\overline{\gamma_1} + \gamma_1e_4\overline{\gamma_1} + \gamma_1e_4e_4e_5\overline{\gamma_2} + e_4e_5\gamma_2e_4\overline{\gamma_1}\\
&= e_5\left(\gamma_1 i(v)\overline{\gamma_1} + \gamma_2\overline{\gamma_1} - \gamma_1\overline{\gamma_2}\right) + e_4.
\end{aligned}$$

By the above, $\gamma_1 i(v)\overline{\gamma_1} + \gamma_2\overline{\gamma_1} - \gamma_1\overline{\gamma_2} \in i(\mathbb{R}^3)$. From the definition in (2), we conclude that $x \in \mathrm{Spun}(3)$. That is, $\mathcal{C} \cap G \subseteq \mathrm{Spun}(3)$, which in turn implies $S \cap G = \mathrm{Spun}(3)$. $\square$

The proof of Lemma 4.3 also implies that $\mathrm{Spun}(3) = \left\{x \in Z_3^0 :\ N(x) = \mathbf{1}\right\}$. We will not rely on this observation.

We now perform a *gnomonic projection*[3], although with the cylindrical hypersurface $\mathcal{C}$ rather than a sphere. Let $\pi_8 : \mathbb{R}^8 \to \mathbb{R}^7$ be the projection defined by $\pi_8(x_1, x_2, ..., x_8) = (x_2, ..., x_8)$. Let H_0 denote the hyperplane in $\mathbb{R}^8$ defined by $x_1 = 0$ and let H_1 denote the hyperplane defined by $x_1 = 1$. For each $x \in \mathbb{R}^8 \setminus H_0$ there exists a unique $\lambda_x \in \mathbb{R}$ such that the x_1-coordinate of $\lambda_x x$ is 1. We define $\pi : \mathbb{R}^8 \setminus H_0 \to \mathbb{R}^7$ as $\pi(x) = \pi_8(\lambda_x x)$. That is, π projects x from the origin onto H_1 and then removes the first coordinate of the resulting point.

For points $a, p \in \mathcal{P}$, let F_{ap} be defined as in (7). Note that $F_{ap} \subset Z_3^0$ is a four-dimensional subspace of $\mathbb{R}^8$. Since F_{ap} is ruled by lines incident to the origin, we have that $\pi(F_{ap} \setminus H_0) = \pi_8(F_{ap} \cap H_1)$ and $F_{ap} \not\subseteq H_1$. In the definition (7), by taking an element of $C\ell_3^0$ with a constant term $1 \cdot \mathbf{1}$ we get that $F_{ap} \cap H_1 \neq \emptyset$. Since F_{ap} is a 4-flat and H_1 is a hyperplane that intersects F_{ap} without containing it, the intersection $F_{ap} \cap H_1$ is a 3-flat. Since the restriction of π_8 to H_1 is linear and injective, we get that $\pi(F_{ap} \setminus H_0)$ is a 3-flat in $\mathbb{R}^7$.

Note that $\mathcal{C}$ is a cylindrical hypersurface, and let $\mathcal{C}_+$ be set of points of $\mathcal{C}$ with a positive x_1-coordinate. By Lemmas 3.6 and 4.3 we have $T_{ap} = F_{ap} \cap \mathcal{C} \cap G$, which implies $\pi(T_{ap} \cap \mathcal{C}_+) \subseteq \pi(F_{ap} \setminus H_0)$. By (9) we have that $T_{00} = \mathrm{Spin}(3) = F_{00} \cap \mathcal{C}$. This implies

$$\begin{aligned}
T_{ap} &= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right) T_{00} \left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right)\\
&= \left(\left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right) F_{00} \left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right)\right) \bigcap \left(\left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right) \mathcal{C} \left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right)\right)\\
&= F_{ap} \cap \mathcal{C}.
\end{aligned}$$

[3] Recall that in a gnomonic projection we project the sphere $\mathbb{S}^2$ onto a tangent plane, by shooting rays from the center of $\mathbb{S}^2$ onto the plane.

Thus, for every $v \in H_1 \cap F_{ap}$ there exists $r \in \mathbb{R}$ such that $rv \in \mathcal{C}_+$. That is, $\pi(F_{ap} \setminus H_0) \subseteq \pi(T_{ap} \cap \mathcal{C}_+)$, which in turn implies $\pi(T_{ap} \cap \mathcal{C}_+) = \pi(F_{ap} \setminus H_0)$. We conclude that π maps each set $T_{ap} \cap \mathcal{C}_+$ onto a 3-flat in $\mathbb{R}^7$.

Let $g : \mathbb{R}^8 \to \mathbb{R}$ be the map defined by $g(x_1, ..., x_8) = x_1x_8 - x_2x_7 + x_3x_6 - x_4x_5$. Note that $G = g^{-1}(0)$. For every $v \in G$ and $r \in \mathbb{R}$ we have $g(rv) = r^2 g(v)$, so $rv \in G$. That is, G is ruled by lines incident to the origin, which implies that $\pi(G \setminus H_0) = \pi_8(G \cap H_1)$. Let $g_7 : \mathbb{R}^7 \to \mathbb{R}$ be the map defined by $g_7(x_2, ..., x_8) = x_8 - x_2x_7 + x_3x_6 - x_4x_5$ and note that $\pi(G \setminus H_0) = g_7^{-1}(0)$. We set $G_7 = g_7^{-1}(0) \subset \mathbb{R}^7$. Since each $T_{ap} \cap \mathcal{C}_+ \subset \mathrm{Spun}(3) \subset G$, every 3-flat of the form $\pi(T_{ap} \cap \mathcal{C}_+)$ is contained in G_7. Given $(x_2, \dots, x_8) \in \mathbb{R}^7$, let $x = (1, x_2, \dots, x_8)$. Then there exists $r \in \mathbb{R}$ such that $y = rx$ is the unique point on $\mathcal{C}_+$ that satisfies $\pi(y) = (x_2, \dots, x_8)$. That is, the restriction of π to $\mathcal{C}_+$ is a bijection between $\mathcal{C}_+$ and $\mathbb{R}^7$. Moreover, π maps G to G_7 (it is not injective in this domain) and maps each $T_{ap} \cap \mathcal{C}_+$ to a 3-flat contained in G_7.

Let $\pi_7 : \mathbb{R}^7 \to \mathbb{R}^6$ be the projection that is defined by $\pi_7(x_2, ..., x_7, x_8) = (x_2, ..., x_7)$. Since $g_7(x_2, ..., x_7, x_8) = g_7(x_2, ..., x_7, x_8')$ implies $x_8 = x_8'$, the restriction of π_7 to G_7 is injective. Since π_7 is linear and every 3-flat of the form $\pi(T_{ap} \cap \mathcal{C}_+)$ is contained in G_7, we get that $\pi_7(\pi(T_{ap} \cap \mathcal{C}_+))$ is a 3-flat in $\mathbb{R}^6$. Furthermore, since both the restriction of π_7 to G_7 and the restriction of π to $\mathcal{C}_+$ are bijections, the restriction of $\pi_7 \circ \pi$ to $\mathcal{C}_+ \cap G$ is injective. For every $v \in G \setminus H_0$ there exists $r \in \mathbb{R}$ such that $rv \in \mathcal{C}_+ \cap G$. That is, $\eta = \pi_7 \circ \pi$ is a bijection from $G \cap \mathcal{C}_+$ to $\mathbb{R}^6$.

Studying intersections of 3-flats. Recall from Lemma 3.6 that $T_{ap} = F_{ap} \cap \mathrm{Spun}(3)$. To study intersections of the 3-flats in $\mathbb{R}^6$, we first study the intersections $F_{ap} \cap F_{bq}$.

Lemma 4.4. *We have that $T_{ap} \cap T_{bq} = \emptyset$ if and only if $F_{ap} \cap F_{bq} = \{0\}$.*

Proof. By Lemma 3.6, $T_{ap} = F_{ap} \cap \mathrm{Spun}(3)$ and $T_{bq} = F_{bq} \cap \mathrm{Spun}(3)$. Thus, $F_{ap} \cap F_{bq} = \{0\}$ immediately implies $T_{ap} \cap T_{bq} = \emptyset$.

Next, we assume that $F_{ap} \cap F_{bq} \neq \{0\}$. For any $v \in \mathbb{R}^3$ we have $\left(\mathbf{1} + \frac{1}{2}e_4e_5 i(v)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(v)\right) = \mathbf{1}$. Combining this with the definition of F_{ap} gives

$$\begin{aligned} F_{ap} \cap F_{bq} &= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(p)\right)(F_{ap} \cap F_{bq})\left(\mathbf{1} + \frac{1}{2}e_4e_5 i(a)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right) \\ &= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\left(C\ell_3^0 \cap F_{(b-a)(q-p)}\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right). \end{aligned}$$

Since $F_{ap} \cap F_{bq} \neq \{0\}$, we have that $C\ell_3^0 \cap F_{(b-a)(q-p)} \neq \{0\}$. That is, there exist $\gamma, \delta \in C\ell_3^0$ such that

$$\gamma = \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(q-p)\right)\delta\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(b-a)\right).$$

By comparing the terms that do not depend on e_5, we get $\gamma = \delta$. By then comparing the coefficient of e_5 on each side, we get $i(q-p)\gamma = \gamma i(b-a)$.

Note that for any $x \in C\ell_3^0$, the coefficient of $\mathbf{1}$ in $x\overline{x}$ is equal to the coefficient of $\mathbf{1}$ in $\overline{x}x$ (this coefficient equals $\|x\|^2$ when thinking of x as a point in $\mathbb{R}^4$, as in the beginning of this section). Recall that for any $s \in \mathbb{R}^3$ we have $i(s)\overline{i(s)} = \overline{i(s)}i(s) = \|s\|^2 \cdot \mathbf{1}$. By taking $x = i(q-p)\gamma = \gamma i(b-a)$, we get that the coefficient of $\mathbf{1}$ in $\overline{\gamma i(q-p)}i(q-p)\gamma = \|q-p\|^2\overline{\gamma}\gamma$ is equal to the coefficient of $\mathbf{1}$ in $\gamma i(b-a)\overline{i(b-a)\gamma} = \|b-a\|^2\gamma\overline{\gamma}$. Since the coefficients of $\mathbf{1}$ in $\overline{\gamma}\gamma$ and $\gamma\overline{\gamma}$ are equal, it follows that $\|b-a\| = \|q-p\|$. Since the vectors $b-a, q-p \in \mathbb{R}^3$ have the same length, there exists a rotation $\beta \in \mathrm{Spin}(3)$ such that $\beta i(b-a)\beta^{-1} = i(q-p)$. By Lemma 3.5, we have

$$\beta_{ap} = \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\beta\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right) = \beta + \frac{1}{2}e_4e_5(i(p)\beta - \beta i(a)) \in T_{ap}.$$

To prove that $T_{ap} \cap T_{bq} \neq \emptyset$, we show that $\beta_{ap} \in T_{bq}$. Since $\beta_{ap} \in T_{ap}$, we have that $\beta_{ap} \in \mathrm{Spun}(3)$. It remains to prove that β_{ap} takes b to q. Indeed, recalling that β takes $b-a$ to $q-p$ gives

$$\begin{aligned}
\beta_{ap}(e_5 i(b) + e_4)\overline{\beta_{ap}} &= \left(\beta + \frac{1}{2}e_4e_5(i(p)\beta - \beta i(a))\right)(e_5 i(b) + e_4)\left(\overline{\beta} + \frac{1}{2}e_4e_5(i(a)\overline{\beta} - \overline{\beta} i(p))\right) \\
&= \beta(e_5 i(b) + e_4)\overline{\beta} + \frac{1}{2}e_5\left(\beta e_4 e_4(i(a)\overline{\beta} - \overline{\beta} i(p)) + e_4(i(p)\beta - \beta i(a))e_4\overline{\beta}\right) \\
&= \beta(e_5 i(b))\overline{\beta} + e_4 + \frac{1}{2}e_5\left(-(\beta i(a)\overline{\beta} - i(p)) + (i(p) - \beta i(a)\overline{\beta})\right) \\
&= e_5(\beta i(b-a)\overline{\beta}) + e_4 + e_5 i(p) = e_5 i(q-p) + e_4 + e_5 i(p) = e_5 i(q) + e_4.
\end{aligned}$$

□

We next study the case where $F_{ap} \cap F_{bq} \neq \{0\}$.

Lemma 4.5. *If $F_{ap} \neq F_{bq}$ and $F_{ap} \cap F_{bq} \neq \{0\}$, then*

$$F_{ap} \cap F_{bq} = \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\beta \cdot C\ell_2^0 \cdot \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right),$$

for any $\alpha, \beta \in \mathrm{Spin}(3)$ that satisfy $\alpha\frac{i(b-a)}{\|b-a\|}\alpha^{-1} = e_3$ and $\beta e_3 \beta^{-1} = \frac{i(q-p)}{\|q-p\|}$.

Proof. By the assumptions and Lemma 4.4, we have that $a \neq b$ and $p \neq q$, so $\|b-a\|$ and $\|q-p\|$ are nonzero. Thus, the definitions of α and β are valid. Let

$$N_{ap} = \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\beta \cdot C\ell_2^0 \cdot \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right).$$

Since $\alpha, \beta \in C\ell_3^0$, we have $\beta \cdot C\ell_2^0 \cdot \alpha \subset C\ell_3^0$ so $N_{ap} \subseteq F_{ap}$. We note that

$$\begin{aligned}
\alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right) &= \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a-b+b)\right) = \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a-b)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(b)\right) \\
&= \left(\alpha - \frac{1}{2}e_4e_5 \alpha i(a-b)\alpha^{-1}\alpha\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(b)\right) \\
&= \left(\mathbf{1} + \|b-a\|\frac{1}{2}e_4e_5e_3\right)\alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(b)\right). \qquad (12)
\end{aligned}$$

Similarly,

$$\begin{aligned}
\left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\beta &= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p-q+q)\right)\beta = \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(q)\right)\left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p-q)\right)\beta \\
&= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(q)\right)\beta\left(\mathbf{1} + \frac{1}{2}e_4e_5 \beta^{-1} i(p-q)\beta\right) \\
&= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(q)\right)\beta\left(\mathbf{1} - \|q-p\|\frac{1}{2}e_4e_5e_3\right). \qquad (13)
\end{aligned}$$

Combining (12) and (13) gives

$$\begin{aligned}
N_{ap} &= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(p)\right)\beta \cdot C\ell_2^0 \cdot \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(a)\right) \\
&= \left(\mathbf{1} + \frac{1}{2}e_4e_5 i(q)\right)\beta\left(\mathbf{1} - \|q-p\|\frac{1}{2}e_4e_5e_3\right) \cdot C\ell_2^0 \cdot \left(\mathbf{1} + \|b-a\|\frac{1}{2}e_4e_5e_3\right)\alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5 i(b)\right).
\end{aligned}$$

By Lemma 4.4, the assumption $F_{ap} \cap F_{bq} \neq \{0\}$ implies $T_{ap} \cap T_{bq} \neq \emptyset$. That is, there exists a rigid motion of SE(3) that takes both a to p and b to q, which in turn implies that $\|b-a\| = \|q-p\|$. Thus, for any $\gamma \in C\ell_2^0$ we have $\left(\mathbf{1} - \|q-p\|\frac{1}{2}e_4e_5e_3\right)\gamma\left(\mathbf{1} + \|b-a\|\frac{1}{2}e_4e_5e_3\right) = \gamma$. Combining this with the calculation above yields

$$N_{ap} = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(q)\right)\beta \cdot C\ell_2^0 \cdot \alpha \left(\mathbf{1} - \frac{1}{2}e_4e_5i(b)\right) \subseteq F_{bq}.$$

We conclude that $N_{ap} \subseteq F_{ap} \cap F_{bq}$. To prove the other direction, consider $x \in F_{ap} \cap F_{bq}$. By definition, there exist $\gamma, \gamma' \in C\ell_3^0$ such that

$$x = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\gamma\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right) = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(q)\right)\gamma'\left(\mathbf{1} - \frac{1}{2}e_4e_5i(b)\right). \qquad (14)$$

The part of x that does not involve e_5 needs to be identical in both definitions, so $\gamma = \gamma'$. The part of x that does involve e_5 also needs to be identical in both definitions, so $i(p)\gamma - \gamma i(a) = i(q)\gamma - \gamma i(b)$, or equivalently $\gamma i(b-a) = i(q-p)\gamma$. This implies that

$$\beta^{-1}\gamma\alpha^{-1}\alpha i(b-a)\alpha^{-1} = \beta^{-1}i(q-p)\beta\beta^{-1}\gamma\alpha^{-1},$$

which in turn implies $\beta^{-1}\gamma\alpha^{-1}e_3 = e_3\beta^{-1}\gamma\alpha^{-1}$. Since e_3 commutes with $\beta^{-1}\gamma\alpha^{-1}$, we get that $\beta^{-1}\gamma\alpha^{-1} \in C\ell_2^0$. That is, $\gamma \in \beta \cdot C\ell_2^0 \cdot \alpha$. By combining this with the first equality of (14), we conclude that $x \in N_{ap}$ and thus that $F_{ap} \cap F_{bq} \subseteq N_{ap}$. $\square$

Let $L_{ap} = \eta(T_{ap} \setminus H_0)$ be the 3-flat in $\mathbb{R}^6$ that corresponds to T_{ap}. Given points $a, p, b, q \in \mathbb{R}^3$, we now study the intersection $L_{ap} \cap L_{bq}$. Let $L_{apbq} = \eta\left(\langle F_{ap}, F_{bq}\rangle \setminus H_0\right)$. By comparing the definitions of F_{ap} and L_{ap}, we note that $L_{ap} \cup L_{bq} \subset L_{apbq}$.

Note that the map $\eta(x)$ is well-defined for every point $x \in \mathbb{R}^8 \setminus H_0$. Additionally, when we restrict the domain of η to H_1 it becomes a linear map. Let $\eta' : \mathbb{R}^8 \to \mathbb{R}^6$ be the standard linear projection satisfying $\eta'(x_1, x_2, ..., x_8) = (x_2, ..., x_7)$. We think of η' as a linear extension of the restricted η to $\mathbb{R}^8$. Denote by $\langle F_{ap}, F_{bq}\rangle$ the linear subspace that is spanned by F_{ap} and F_{bq}.

Lemma 4.6. *If $T_{ap} \cap T_{bq} \not\subseteq H_0$ and $T_{ap} \neq T_{bq}$, then $L_{ap} \cap L_{bq}$ is a line.*

Proof. From $T_{ap} \cap T_{bq} \not\subseteq H_0$ we have that $L_{ap} \cap L_{bq} \neq \emptyset$. Since L_{ap} and L_{bq} are distinct 3-flats in $\mathbb{R}^6$, their intersection is a flat of dimension between zero and two. If $\dim(L_{ap} \cap L_{bq}) = 2$ then $\dim(F_{ap} \cap F_{bq} \cap H_1) = 2$, which in turn implies $\dim(F_{ap} \cap F_{bq}) = 3$. This contradicts Lemma 4.5 which states that $\dim(F_{ap} \cap F_{bq}) = 2$. Thus, it remains to prove that $L_{ap} \cap L_{bq}$ is not a single point.

For any $v \in \langle F_{ap}, F_{bq}\rangle \cap H_1$, we have

$$L_{apbq} = \eta(\langle F_{ap}, F_{bq}\rangle \setminus H_0) = \eta'(\langle F_{ap}, F_{bq}\rangle \cap H_1) = \eta'(\langle F_{ap}, F_{bq}\rangle \cap H_0) + \eta'(v).$$

This implies that

$$\dim L_{apbq} = \dim\left(\langle F_{ap}, F_{bq}\rangle \cap H_0\right) - \dim\left(\langle F_{ap}, F_{bq}\rangle \cap H_0 \cap \ker(\eta')\right). \qquad (15)$$

By Lemma 4.5, $\dim(F_{ap} \cap F_{bq}) = \dim C\ell_2^0 = 2$. Since $\dim F_{ap} = \dim F_{bq} = \dim C\ell_3^0 = 4$, we have $\dim\left(\langle F_{ap}, F_{bq}\rangle \cap H_0\right) = 4 + 4 - 2 - 1 = 5$ (by definition both F_{ap} and F_{bq} intersect H_0 but are not contained in it). Combining this with (15) leads to $\dim L_{apbq} \leq 5$. This completes the proof, since the intersection of two 3-flats in a 5-dimensional space cannot be a single point. $\square$

Next, we study what happens to L_{ap} and L_{bq} when $T_{ap} \cap T_{bq} = \emptyset$.

Lemma 4.7. *For any $a, p, b, q \in \mathbb{R}^3$, any flat in $\mathbb{R}^6$ that contains L_{ap} and L_{bq} also contains L_{apbq}.*

Proof. Let W be a flat that contains L_{ap} and L_{bq}. Then there exists a linear subspace $V \subseteq \mathbb{R}^6$ such that for any $w \in W$ we have $W = w + V$. Recall that $F_{ap} \cap H_1 \neq \emptyset$. For any $x \in \langle F_{ap}, F_{bq} \rangle \cap H_1$,

$$L_{apbq} = \eta\left(\langle F_{ap}, F_{bq}\rangle \setminus H_0\right) = \eta\left(\langle F_{ap}, F_{bq}\rangle \cap H_1\right) = \eta'\left(\langle F_{ap}, F_{bq}\rangle \cap H_1\right) = \eta'\left(\langle F_{ap}, F_{bq}\rangle \cap H_0\right) + \eta(x).$$

For $x \in F_{ap} \cap H_1$ we have that $W = \eta(x) + V$ and $L_{ap} = \eta'(x + F_{ap} \cap H_0) = \eta(x) + \eta'(F_{ap} \cap H_0)$. Combining this with $L_{ap} \subseteq W$ gives $\eta'(F_{ap} \cap H_0) \subseteq V$. Similarly, by taking $y \in F_{bq} \cap H_1$ we get $W = \eta(y) + V$, which in turn implies $\eta'(F_{bq} \cap H_0) \subseteq V$. Combining the above yields $\eta'\left(\langle F_{ap}, F_{bq}\rangle \cap H_0\right) \subseteq V$. We conclude that $L_{apbq} \subseteq W$, as desired. $\square$

Corollary 4.8. *If $T_{ap} \cap T_{bq} = \emptyset$ then no hyperplane contains both L_{ap} and L_{bq}.*

Proof. Lemma 4.7 implies that L_{apbq} is the smallest flat that contains $L_{ap} \cup L_{bq}$. By Lemma 4.4, the assumption $T_{ap} \cap T_{bq} = \emptyset$ implies that $F_{ap} \cap F_{bq} = \{0\}$. Since F_{ap} and F_{bq} are 4-flats in $Z_3^0 \cong \mathbb{R}^8$ that intersect in a single point, we have $\langle F_{ap}, F_{bq}\rangle = Z_3^0$. That is, $L_{apbq} = \eta\left(\langle F_{ap}, F_{bq}\rangle \setminus H_0\right) = \mathbb{R}^6$. $\square$

We are now ready to state the connection between the distinct distances problem and the flats L_{ap}. Let Q' be the set of quadruples $(a, p, b, q) \in \mathcal{P}^4$ such that $T_{ap} \cap T_{bq} \not\subseteq H_0$. The following corollary is a special case of Corollary 5.16 that we will prove in Section 5.

Corollary 4.9. *We have that $Q' \subset Q$ and $|Q'| \geq |Q|/2$.*

Flats in $\mathbb{R}^6$ and in $\mathbb{R}^5$. We set

$$\mathcal{L} = \{L_{ap} : \ a, p \in \mathcal{P} \text{ and } a \neq p\}.$$

Note that $\mathcal{L}$ is a set of $\Theta(n^2)$ flats of dimension three in $\mathbb{R}^6$. By Corollary 4.9, to get an asymptotic upper bound for the number of quadruples in Q it suffices to derive an upper bound for the number of quadruples $(a, p, b, q) \in \mathcal{P}^4$ such that $T_{ap} \cap T_{bq} \not\subseteq \emptyset$. By Lemma 4.6, for every such quadruple we have that $L_{ap} \cap L_{bq}$ is a line. On the other hand, when $T_{ap} \cap T_{bq} \subseteq H_0$ we have that $L_{ap} \cap L_{bq} = \emptyset$. Thus, it remains to derive an upper bound on the number of pairs of flats of $\mathcal{L}$ that intersect (in a line).

Lemma 4.10. *(a) Every point of $\mathbb{R}^6$ is contained in at most n flats of $\mathcal{L}$.*
(b) Every hyperplane in $\mathbb{R}^6$ contains at most n flats of $\mathcal{L}$.

Proof. Consider three distinct points $a, p, q \in \mathcal{P}$ and note that $T_{ap} \cap T_{aq} = \emptyset$, since a rigid motion cannot simultaneously take a into two distinct points. This immediately implies part (a) of the lemma. By Corollary 4.8, L_{ap} and L_{aq} cannot be in the same hyperplane, which implies part (b). $\square$

Let H_g be a generic hyperplane in $\mathbb{R}^6$, in the sense that every 3-flat of $\mathcal{L}$ intersects H_g in a 2-flat, and every line of the form $L_{ap} \cap L_{bq}$ (with $a, b, p, q \in \mathcal{P}$) intersects H_g at a single point. Let $\mathcal{F} = \{L_{ap} \cap H_g : L_{ap} \in \mathcal{L}\}$ and consider H_g as $\mathbb{R}^5$. Note that $\mathcal{F}$ is a set of $\Theta(n^2)$ distinct 2-flats. Every two 2-flats of $\mathcal{F}$ are either disjoint or intersect in a single point. By Lemma 4.10, every point of $\mathbb{R}^5$ is incident to at most n of the 2-flats of $\mathcal{F}$ and every hyperplane in $\mathbb{R}^5$ contains at most n of the 2-flats of $\mathcal{F}$.

For every integer $k \geq 2$, let m_k denote the number of points of $\mathbb{R}^5$ that are contained in exactly k of the 2-flats of $\mathcal{F}$. Similarly, let $m_{\geq k}$ denote the number of points of $\mathbb{R}^5$ that are contained in *at least* k of the 2-flats of $\mathcal{F}$. Then $|Q|$ is the number of pairs of intersecting flats of $\mathcal{F}$, and

$$|Q| = \sum_{k=2}^{n} m_k \cdot 2\binom{k}{2} < \sum_{k=2}^{n} k^2 m_k = O\left(\sum_{k=1}^{\log n} 2^{2k} m_{\geq 2^k}\right).$$

If we had the bound $m_{\geq k} = O\left(\frac{n^{10/3}}{k^{2+\varepsilon}}\right)$ for some $\varepsilon > 0$, then the above would imply $|Q| = O(n^{10/3})$. Combining this with (10) would imply that the points of $\mathcal{P}$ span $\Omega\left(n^{2/3}\right)$ distinct distances.

An incidence result of Solymosi and Tao [9] implies that the number of incidences between m points and n 2-flats in $\mathbb{R}^5$, with every two 2-flats intersecting in at most one point, is $O(m^{2/3+\varepsilon'} n^{2/3} + m+n)$ (for any $\varepsilon' > 0$). Every incidence bound of this form has a dual formulation involving k-rich points (for example, see [8, Chapter 1]). In this case, the dual bound is: Given n^2 2-flats in $\mathbb{R}^5$ such that every two intersect in at most one point, for every $k \geq 2$ the number of k-rich points is $O\left(\frac{n^{4/(1-\varepsilon')}}{k^{3/(1-\varepsilon')}} + \frac{n^2}{k}\right)$. By taking ε' to be sufficiently small with respect to ε, we obtain the bound $m_{\geq k} = O\left(\frac{n^{4+\varepsilon}}{k^3} + \frac{n^2}{k}\right)$. This bound is stronger than the required bound when $k = \Omega(n^{2/3+\varepsilon})$. That is, it remains to consider the case where $k = O(n^{2/3+\varepsilon})$. This completes the proof of Theorem 4.2. □

5 Distinct distances in $\mathbb{R}^d$

In this section we prove Theorem 1.2 in every dimension. While the general outline of the proof remains the same as in the proof of Theorem 4.2, several steps become significantly more involved. As before, we embed Spun(d) in a real space and then perform several projections to lower dimensional spaces. Since Corollary 2.3 does not hold for $d \geq 6$, we do not have a simple description of Spun(d) as in Lemma 4.3. This leads us to study Spun(d) in a more indirect way.

Recall that Spun(d) is contained in the subspace $Z_d^0 \subset X_d$ generated by $\mathbf{1}$ and by products of an even number of elements from $\{e_1, e_2, \ldots, e_d, e_{d+1}e_{d+2}\}$. Note that Z_d^0 has a basis of size 2^d. We consider Z_d^0 as $\mathbb{R}^{2^d}$ by mapping the above basis elements to the standard basis vectors of $\mathbb{R}^{2^d}$. With this notation, we study the behavior of Spun(d) as a set in $\mathbb{R}^{2^d}$.

5.1 Studying m-terms

For an even integer $m > 0$, an *m-term* of $C\ell_d^0$ is a product of m distinct elements from $\{e_1, e_2, \ldots, e_d\}$ (together with a real coefficient). Similarly, an m-term of Z_d^0 is a product of m distinct elements from $\{e_1, e_2, \ldots, e_d, e_{d+1}e_{d+2}\}$ (together with a real coefficient). In both cases a 0-term is $\mathbf{1}$ multiplied some real number. In this section we study several basic properties of m-terms. Since these are just straightforward calculations, the reader might prefer to skip this section and refer to it when necessary.

Lemma 5.1. *For a fixed even m, let $x \in C\ell_d^0 \backslash \{0 \cdot \mathbf{1}\}$ consist entirely of m-terms and let $\gamma \in$ Spin(d). Then $\gamma x \gamma^{-1}$ also consists entirely of m-terms.*

Proof. Let $z \in C\ell_d^0$ and $\gamma \in$ Spin(d). We think of $C\ell_d^0$ as $\mathbb{R}^{2^d}$ and write $\|z\|$ for the Euclidean norm of z in $\mathbb{R}^{2^d}$. Note that the first coordinate of $z\overline{z}$ is $\|z\|$ and so is the first coordinate of

$\overline{z}z$ (since $\|z\| = \|\overline{z}\|$). Since $z\gamma^{-1}\overline{z\gamma^{-1}} = z\gamma^{-1}\gamma\overline{z} = z\overline{z}$, by considering the first coordinate of these expressions we get that $\|z\| = \|z\gamma^{-1}\|$. That is, multiplication by γ^{-1} from the right is an orthogonal transformation (with respect to the Euclidean norm). Similarly, $\overline{\gamma z}\gamma z = \overline{z}z$ implies that multiplication by γ from the left is also an orthogonal transformation. We conclude that the conjugation $z \to \gamma z\gamma^{-1}$ is orthogonal with respect to the Euclidean norm. Combining this with $\gamma\mathbf{1}\gamma^{-1} = \mathbf{1}$ implies that z and $\gamma z\gamma^{-1}$ have the same first coordinate.

For $u_1, \ldots, u_m \in \mathbb{R}^d$, the product $i(u_1)\cdots i(u_m)$ cannot contain ℓ-terms for any $\ell > m$. Moreover, for any m-term $e_{k_1}e_{k_2}\cdots e_{k_m}$ we have that $\gamma e_{k_1}e_{k_2}\cdots e_{k_m}\gamma^{-1} = \gamma e_{k_1}\gamma^{-1}\gamma e_{k_2}\gamma^{-1}\ldots\gamma e_{k_m}\gamma^{-1}$. This implies that $\gamma x\gamma^{-1}$ cannot contain ℓ-terms for any $\ell > m$.

We write $\gamma x\gamma^{-1} = \delta + \delta'$, where δ consists entirely of m-terms and δ' consists entirely of smaller terms. We have

$$\begin{aligned} N(x - \gamma^{-1}\delta'\gamma) - N(x) - N(\gamma^{-1}\delta'\gamma) &= (x - \gamma^{-1}\delta'\gamma)\overline{(x - \gamma^{-1}\delta'\gamma)} - x\overline{x} - \gamma^{-1}\delta'\overline{\delta'}\gamma \\ &= -\left(x\overline{\gamma^{-1}\delta'\gamma} + \gamma^{-1}\delta'\gamma\overline{x}\right). \end{aligned} \tag{16}$$

For any $y, z \in C\ell_d^0$, the first coordinate of $y\overline{z}$ is the dot product of y and z as vectors in $\mathbb{R}^{2^d}$. Since $\gamma^{-1}\delta'\gamma$ consists entirely of ℓ-vector terms with $\ell < m$, the first coordinate of (16) is zero. Since conjugation by γ preserves the first coordinate, we have that the first coordinate of $(x - \gamma^{-1}\delta'\gamma)\overline{(x - \gamma^{-1}\delta'\gamma)} - x\overline{x} - \gamma^{-1}\delta'\overline{\delta'}\gamma$ is the same as the first coordinate of

$$\begin{aligned} &\gamma\left((x - \gamma^{-1}\delta'\gamma)\overline{(x - \gamma^{-1}\delta'\gamma)} - x\overline{x} - \gamma^{-1}\delta'\overline{\delta'}\gamma\right)\gamma^{-1} \\ &\quad = \gamma(x - \gamma^{-1}\delta'\gamma)\gamma^{-1}\gamma\overline{(x - \gamma^{-1}\delta'\gamma)}\gamma^{-1} - \gamma x\gamma^{-1}\gamma\overline{x}\gamma^{-1} - \delta'\overline{\delta'} \\ &\quad = \delta\overline{\delta} - \left(\delta\overline{\delta} + \delta'\overline{\delta'} + \delta\overline{\delta'} + \delta'\overline{\delta}\right) - \delta'\overline{\delta'} = -\left(\delta\overline{\delta'} + \delta'\overline{\delta} + 2\delta'\overline{\delta'}\right). \end{aligned}$$

Since δ and δ' do not have terms of the same size, the first coordinates of $\delta\overline{\delta'}$ and $\delta'\overline{\delta}$ are both zero. This implies that first coordinate of $\delta'\overline{\delta'}$ is zero. Since this first coordinate equals $\|\delta'\|$, we get that $\delta' = 0$ and complete the proof. ∎

Lemma 5.2. *For a fixed even m, let $x \in C\ell_{d-1}^0$ consist entirely of m-terms. Then for every $a \in \mathbb{R}^d$ the expression $xe_d(i(a) + e_d)$ consists entirely of m-terms and $(m+2)$-terms. It the d'th coordinate of a is not -1, then $xe_d(i(a) + e_d)$ contains at least one m-term.*

Proof. Let a_d be the d'th coordinate of a and let $a' = a - (0, \ldots, 0, a_d)$. We have that

$$xe_d(i(a) + e_d) = x\left((-1 - a_d)\mathbf{1} + e_d i(a')\right) = -(1 + a_d)x - xi(a')e_d.$$

Since $xi(a') \in C\ell_{d-1}$ consists entirely of $(m-1)$-terms and $(m+1)$-terms, we have that $xi(a')e_d$ consists entirely of m-terms and $(m+2)$-terms, as desired. Since no term of x contains e_d and every term of $xi(a')e_d$ contains e_d, if $a_d \neq -1$ then the m-terms from $-(1 + a_d)x$ are nonzero and do not get canceled by other terms. ∎

Lemma 5.3. *For a fixed even m, let $z \in Z_d^0 \setminus \{0 \cdot \mathbf{1}\}$ contain only m-terms and let $a, p \in \mathbb{R}^d$. Then $(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p))z(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a))$ contains only m-terms and $(m+2)$-terms. This expression contains at least one nonzero m-term.*

Proof. We write $z = z_1 + z_2e_{d+1}e_{d+2}$ where $z_1 \in C\ell_d^0$ and $z_2 \in C\ell_d^1$. We then have

$$\left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)z\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) = z + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)z_1 - z_1i(a)\right).$$

We observe that both $i(p)z_1$ and $z_1 i(a)$ contain only $(m+1)$-terms and $(m-1)$-terms, and do not contain $e_{d+1}e_{d+2}$. This implies that $\frac{1}{2}e_{d+1}e_{d+2}\left(i(p)z_1 - z_1 i(a)\right)$ contains only $(m+2)$-terms and m-terms. Additionally, the part of $z + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)z_1 - z_1 i(a)\right)$ that does not involve $e_{d+1}e_{d+2}$ is exactly z_1. Thus, if $z_1 \neq 0 \cdot \mathbf{1}$ then we have at least one m-term. If $z_1 = 0 \cdot \mathbf{1}$ then $z + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)z_1 - z_1 i(a)\right) = z$, and we again have an m-term. □

5.2 Proof of Theorem 1.2.

Let $\mathcal{P}$ be a set of n points in $\mathbb{R}^d$. Let D denote the number of distinct distances that are spanned by $\mathcal{P}$ and denote these distances as $\delta_1, \ldots, \delta_D$. We set

$$Q = \left\{(a,b,p,q) \in \mathcal{P}^4 : |ab| = |pq| > 0\right\}.$$

The quadruples of Q are ordered, so (a,b,p,q) and (b,a,p,q) are considered as two distinct elements of Q. Our proof is based on double counting $|Q|$.

For every $j \in \{1,\ldots,D\}$, let $E_j = \{(a,b) \in \mathcal{P}^2 : |ab| = \delta_j\}$. Since every ordered pair of distinct points $(a,b) \in \mathcal{P}^2$ appears in exactly one set E_j, we have that $\sum_{j=1}^{D}|E_j| = n^2 - n > n^2/2$. The Cauchy-Schwarz inequality implies

$$|Q| = \sum_{j=1}^{D}|E_j|^2 \geq \frac{1}{D}\left(\sum_{j=1}^{D}|E_j|\right)^2 > \frac{n^4}{4D}. \tag{17}$$

For $a,b,p,q \in \mathbb{R}^d$ with $a \neq b$, we have $|ab| = |pq|$ if and only if there exists a proper rigid motion in $\mathrm{SE}(d)$ that takes both a to p and b to q. Thus, for every $(a,p) \in \mathcal{P}^2$ we set

$$R_{ap} = \{\gamma \in \mathrm{SE}(d) :\ a^\gamma = p\}.$$

To derive an upper bound for $|Q|$ it suffices to bound the number of quadruples $(a,b,p,q) \in \mathcal{P}^4$ that satisfy $a \neq b$ and $R_{ap} \cap R_{bq} \neq \emptyset$. Since it would be simpler to work in $\mathrm{Spun}(d)$ rather than in $\mathrm{SE}(d)$, we recall the following definition from (5).

$$T_{ap} = \{x \in \mathrm{Spun}(d) :\ a^x = p\} = \rho_d^{-1}(R_{ap}).$$

From $\mathrm{Spun}(d)$ **to** $\mathbb{R}^{\binom{d+1}{2}}$**.** In Section 4 we studied the bijection η from the set of points of $\mathrm{Spun}(3)$ that have a positive x_1-coordinate to $\mathbb{R}^6$. We now generalize this bijection to the case of $\mathrm{Spun}(d)$. Let $\mathrm{Spun}(d)_+$ be the set of points of $\mathrm{Spun}(d)$ that have a positive first coordinate (the coordinate that corresponds to the coefficient of $\mathbf{1}$).

Let $\pi_1 : \mathbb{R}^{2^d} \to \mathbb{R}^{2^d-1}$ be the projection defined by $\pi_1(x_1, x_2, ..., x_{2^d}) = (x_2, ..., x_{2^d})$. Let H_0 denote the hyperplane in $\mathbb{R}^{2^d}$ defined by $x_1 = 0$ and let H_1 denote the hyperplane defined by $x_1 = 1$. For each $x \in \mathbb{R}^{2^d} \setminus H_0$ there exists a unique $\lambda_x \in \mathbb{R}$ such that the x_1-coordinate of $\lambda_x x$ is 1. We define $\pi : \mathbb{R}^{2^d} \setminus H_0 \to \mathbb{R}^{2^d-1}$ as $\pi(x) = \pi_1(\lambda_x x)$. We think of elements of $\mathbb{R}^{2^d-1}$ as corresponding to elements of Z_d^0, except for the coefficient of $\mathbf{1}$ (which was removed by π_1). Let $\pi' : \mathbb{R}^{2^d-1} \to \mathbb{R}^{\binom{d+1}{2}}$ be the projection that keeps only the $\binom{d+1}{2}$ coordinates corresponding to 2-terms of Z_d^0. We will see that we do not lose information of elements of $\mathrm{Spun}(d)_+$ by keeping only these coordinates. Finally, let $\eta_d = \pi' \circ \pi_1$. Note that η_3 is indeed the map η from Section 4.

We first claim that the restriction of π_1 to $\mathrm{Spun}(d)_+$ is injective. Indeed, assume that $\pi_1(x) = y$ for $x \in \mathrm{Spun}(d)_+$ and write $y = (y_2, ..., y_{2^d}) \in \mathbb{R}^{2^d-1}$. This implies that $\lambda_x x = (1, y_2, ..., y_{2^d})$. Since $x \in \mathrm{Spun}(d)_+$, we have that $N(x) = x\overline{x} = \mathbf{1}$ and thus $N(\lambda_x x) = \lambda_x^2 \cdot \mathbf{1}$. That is, the value of λ_x

is determined up to a sign by $N(\lambda_x x)$. This sign has to be positive, since the first coordinate of x must be positive. We conclude that for every $y \in \mathbb{R}^{2^d-1}$ there exists at most one $x \in \text{Spun}(d)_+$ such that $\pi_1(x) = y$.

Set

$$G_d = \{r \cdot \gamma \in C\ell_d^0 : \ r \in \mathbb{R} \setminus \{0\} \text{ and } \gamma \in \text{Spin}(d)\},$$
$$J_d = \{r \cdot x \in Z_d^0 : \ r \in \mathbb{R} \setminus \{0\} \text{ and } x \in \text{Spun}(d)\}.$$

Note that G_d is a group under the product operation of $C\ell_d^0$. Similarly, J_d is a group under the product operation of Z_d^0. By studying these groups, we will obtain information about η_d and about the structure of $\text{Spun}(d)$.

The following lemma provides a consistent form for writing elements of G_d. Below we will rely on this lemma to prove various claims by induction on d.

Lemma 5.4. *(a) For every element $g \in G_d$ there exists $h \in G_{d-1}$ that satisfies the following. Either $g = he_{d-1}e_d$ or there exists $u \in \mathbb{S}^{d-1} \setminus \{i^{-1}(-e_d)\}$ such that $g = h\,(e_d i(u) - \mathbf{1})$.*
(b) For every $z \in J_d$ there exist $v \in \mathbb{R}^d$ and $g \in G_d$ such that $z = g\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(v)\right)$.

Proof. (a) By definition, for every $g \in G_d$ there exists $r \in \mathbb{R} \setminus \{0\}$ such that $g/r \in \text{Spin}(d)$. This implies that $(g/r)^{-1} = \overline{g/r}$, so $(g/r)\overline{(g/r)} = 1$. That is, $g^{-1} = \overline{g}/r^2$. We define the group action of g on $v \in \mathbb{R}^d$ to be

$$i^{-1}(gi(v)g^{-1}) = i^{-1}\left(\frac{g}{r} i(v) \overline{\left(\frac{g}{r}\right)}\right) = i^{-1}\left(\frac{g}{r} i(v) \left(\frac{g}{r}\right)^{-1}\right).$$

Since this is the action of $g/r \in \text{Spin}(d)$ on v, it is a rotation of $\text{SO}(d)$. Thus, the action of g maps some point $u \in \mathbb{S}^{d-1}$ to $i^{-1}(e_d)$.

We first assume that $u \neq i^{-1}(-e_d)$. We write $s = \|u + (0,\ldots,0,1)\|$ and note that $s \neq 0$. Since $i^{-1}(e_d), \frac{u+i^{-1}(e_d)}{s} \in \mathbb{S}^{d-1}$, we get that $x = e_d\,(e_d + i(u))\,/s \in \text{Spin}(d)$. Since $u \in \mathbb{S}^{d-1}$, we note that the vectors $u + i^{-1}(e_d), u - i^{-1}(e_d) \in \mathbb{R}^d$ are orthogonal. By Lemma 2.4 we have

$$\begin{aligned} xi(u)x^{-1} &= \frac{e_d\,(e_d + i(u))\,i(u)\,(e_d + i(u))\,e_d}{s^2} = \frac{e_d\,(i(u) + e_d)\left(\frac{i(u)+e_d}{2} + \frac{i(u)-e_d}{2}\right)(e_d + i(u))\,e_d}{s^2} \\ &= \frac{e_d\,(i(u) + e_d)^2\,((i(u) + e_d) - (i(u) - e_d))\,e_d}{2s^2} = \frac{-e_d \cdot 2e_d \cdot e_d}{2} = e_d. \end{aligned}$$

The above implies that gx^{-1} is in the stabilizer of $i^{-1}(e_d)$. We observe that the stabilizer of $i^{-1}(e_d)$ is G_{d-1}. Setting $h = (g \cdot x^{-1}/s) \in G_{d-1}$, we get that

$$g = gx^{-1}x = he_d\,(e_d + i(u)) = h(e_d i(u) - \mathbf{1}).$$

The above completes the proof of the case where $u \neq i^{-1}(-e_d)$. We now assume that $u = i^{-1}(-e_d)$. That is, that $ge_dg^{-1} = -e_d$. Let $h = -ge_{d-1}e_d$ and note that $h^{-1} = -e_de_{d-1}g^{-1}$. This implies that $he_dh^{-1} = e_d$. As before, since h is in the stabilizer of e_d we have $h \in G_{d-1}$. We get that $g = -ge_{d-1}e_de_{d-1}e_d = he_{d-1}e_d$, as asserted.

(b) Since $z \in J_d$, there exists $r \in \mathbb{R}$ such that $z/r \in \text{Spun}(d)$. By Lemma 3.2, there exist $\gamma \in \text{Spin}(d)$ and $u \in \mathbb{R}^d$ such that $z/r = \gamma\,(\mathbf{1} + e_{d+2}e_{d+1}i(u))$. The assertion of the lemma is obtained by setting $g = r\gamma$ and $v = -2u$. □

The following two lemmas will help us to show that the restriction of η_d to $\text{Spun}(d)_+$ is injective.

Lemma 5.5. *If $g, g' \in G_d$ have the same nonzero first coordinate and the same 2-terms, then $g = g'$.*

Proof. We prove the lemma by induction on d. For the induction basis, note that the claim is trivial when $d \leq 3$. We now assume that the claim holds for G_{d-1} and prove it for G_d.

Consider $g, g' \in G_d$ that satisfy the assumption of the lemma. As in the proof of Lemma 5.4(a), if $g(-e_d)g^{-1} = i^{-1}(e_d)$ then there exists $h \in G_{d-1}$ such that $g = he_de_{d-1}$. This contradicts g having a nonzero first coordinate, so we must have $g(-e_d)g^{-1} \neq i^{-1}(e_d)$. A symmetric argument implies that $g'(-e_d)(g')^{-1} \neq i^{-1}(e_d)$. By Lemma 5.4(a), there exist $h, h' \in G_{d-1}$ and $u, u' \in S^{d-1} \setminus \{-e_d\}$ such that $g = h\,(e_d i(u) - \mathbf{1})$ and $g' = h'\,(e_d i(u') - \mathbf{1})$.

We write $h = r \cdot \mathbf{1} + h_2 + h_+$ such that $r \in \mathbb{R}$, every term of h_2 is a 2-term, and h_+ contains no 0-term and 2-terms. That is, we have

$$g = h\,(e_d i(u) - \mathbf{1}) = he_d i(u) - r \cdot \mathbf{1} - h_2 - h_+.$$

Let u_j be the j'th coordinate of u, and set $u_* = u - (0, \dots, 0, u_d)$. Then

$$g = he_d i(u_*) - r(1 + u_d) \cdot \mathbf{1} - h_2(1 + u_d) - h_+(1 + u_d).$$

A symmetric argument gives

$$g' = h' e_d i((u')_*) - r'(1 + u'_d) \cdot \mathbf{1} - h'_2(1 + u'_d) - h'_+(1 + u'_d).$$

By the assumption on u and u', we have that $u_d \neq -1$ and $u'_d \neq -1$. Since g and g' have nonzero first coordinates, we have that $r \neq 0$ and $r' \neq 0$. Since these first coordinates are identical, $r(1 + u_d) = r'(1 + u'_d)$. By the assumption on the 2-terms of g and g', we have that $(1 + u_d)h_2 = (1 + u'_d)h'_2$ (the expressions $he_d i(u_*)$ and $h' e_d i((u')_*)$ may also contain 2-terms, but these all involve e_d and thus do not affect the terms of $h_2, h'_2 \in C\ell^0_{d-1}$).

By setting $\ell = (1 + u_d)/(1 + u'_d)$ we get that $r' = \ell r \neq 0$ and $h'_2 = \ell h_2$. We may thus apply the induction hypothesis on $h, \ell h' \in G_{d-1}$, to obtain that $h' = \ell h$. That is,

$$g = he_d i(u_*) - h(1 + u_d) \quad \text{ and } \quad g' = \ell he_d i((u')_*) - \ell h(1 + u'_d).$$

We write $h_2 = \sum_{1 \leq j < k \leq d-1} \lambda_{j,k} e_j e_k$, where the coefficients $\lambda_{j,k}$ are in $\mathbb{R}$. Consider the terms of the form $e_j e_d$ for some $1 \leq j \leq d-1$. By the assumption about 2-terms in g and g', we have

$$\begin{aligned} re_d i(u_*) + \sum_{1 \leq j < k \leq d-1} &\lambda_{j,k} e_j e_k (u_j e_d e_j + u_k e_d e_k) \\ &= \ell r_x e_d i((u')_*) + \ell \sum_{1 \leq j < k \leq d-1} \lambda_{j,k} e_j e_k (u'_j e_d e_j + u'_k e_d e_k). \end{aligned}$$

Simplifying, we have

$$\begin{aligned} re_d i(u_*) + \sum_{1 \leq j < k \leq d-1} &\lambda_{j,k} (-u_j e_k e_d + u_k e_j e_d) \\ &= \ell re_d i((u')_*) + \ell \sum_{1 \leq j < k \leq d-1} \lambda_{j,k} (-u'_j e_k e_d + u'_k e_j e_d). \end{aligned}$$

This leads to the following system of linear equations.

$$\begin{pmatrix} r & \lambda_{1,2} & \lambda_{1,3} & \cdots & \lambda_{1,d-1} \\ -\lambda_{1,2} & r & \lambda_{2,3} & \cdots & \lambda_{2,d-1} \\ -\lambda_{1,3} & -\lambda_{2,3} & r & \cdots & \lambda_{3,d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\lambda_{1,d-1} & -\lambda_{2,d-1} & -\lambda_{3,d-1} & \cdots & r \end{pmatrix} \begin{pmatrix} u_1 - \ell u'_1 \\ u_2 - \ell u'_2 \\ u_3 - \ell u'_3 \\ \vdots \\ u_{d-1} - \ell u'_{d-1} \end{pmatrix} = 0.$$

After placing zeros in every cell of the main diagonal, the above matrix becomes skew-symmetric. Recall that the eigenvalues of a skew-symmetric matrix are pure imaginary, and that adding a constant c to every element of the main diagonal adds c to every eigenvalue. Since r is a nonzero real number, we get that the above matrix has no zero eigenvalues, and is thus invertible. This implies that the only solution to the above system is $u_j = \ell u'_j$ for every $1 \le j \le d-1$.

By recalling that $\ell = (1+u_d)/(1+u'_d)$ we get

$$u_d^2 = (\ell(1+u'_d) - 1)^2 = \ell^2(1 + 2u'_d + (u'_d)^2) - 2\ell(1+u'_d) + 1.$$

Combining the above with $u, u' \in \mathbb{S}^{d-1}$ leads to

$$\begin{aligned} 1 = \|u\|^2 = \sum_{j=1}^{d} u_j^2 = \sum_{j=1}^{d-1} \ell^2 (u'_j)^2 + \ell^2(1 + 2u'_d + (u'_d)^2) - 2\ell(1+u'_d) + 1 \\ = 2\ell^2 + 2\ell^2 u'_d - 2\ell - 2\ell u'_d + 1. \end{aligned}$$

Tidying up the above gives $\ell + \ell u'_d = 1 + u'_d$, so $\ell = 1$. We thus get that $h = h'$ and $u = u'$, and conclude that $g = g'$. $\square$

Lemma 5.6. *If $x, y \in J_d$ have the same nonzero first coordinate and the same 2-terms, then $x = y$.*

Proof. By Lemma 5.4(b), there exist $g, h \in G_d$ and $u_x, u_y \in \mathbb{R}^d$ such that $x = g\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(u_x)\right)$ and $y = h\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(u_y)\right)$. We write $g = r_x \cdot \mathbf{1} + g_2 + g'$ where $r_x \in \mathbb{R}$, every term of g_2 is a 2-term, and g' contains no 0-term and no 2-terms. We symmetrically write $h = r_y \cdot \mathbf{1} + h_2 + h'$. That is, we have

$$\begin{aligned} x = g\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(u_x)\right) &= (r_x + g_2 + g')\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(u_x)\right) \\ &= r_x \cdot \mathbf{1} + g_2 + g' - \frac{1}{2}ge_{d+1}e_{d+2}i(u_x), \\ y = h\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(u_y)\right) &= (r_y + h_2 + h')\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(u_y)\right) \\ &= r_y \cdot \mathbf{1} + h_2 + h' - \frac{1}{2}he_{d+1}e_{d+2}i(u_y). \end{aligned}$$

Since x and y have the same first coordinate, we have that $r_x = r_y$. Since $\eta_d(x) = \eta_d(y)$, we have $g_2 = h_2$. By lemma 5.5, we get that $g = h$. We thus have

$$x = g - \frac{1}{2}ge_{d+1}e_{d+2}i(u_x), \quad \text{and} \quad y = g - \frac{1}{2}ge_{d+1}e_{d+2}i(u_y).$$

We write $g_2 = \sum_{1 \le j < k \le d} \lambda_{j,k} e_j e_k$, where the coefficients $\lambda_{j,k}$ are in $\mathbb{R}$. Also, let $u_{x,j}$ denote the j'th coordinate of u_x. We now consider the terms of the form $e_j e_{d+1} e_{d+2}$ with $1 \le j \le d$. Since x

and y have the same 2-terms, we have

$$r_x e_{d+1} e_{d+2} i(u_x) + \sum_{1 \le j < k \le d} \lambda_{j,k} e_j e_k (u_{x,j} e_{d+1} e_{d+2} e_j + u_{x,k} e_{d+1} e_{d+2} e_k)$$
$$= r_x e_{d+1} e_{d+2} i(u_y) + \sum_{1 \le j < k \le d} \lambda_{j,k} e_j e_k (u_{y,j} e_{d+1} e_{d+2} e_j + u_{y,k} e_{d+1} e_{d+2} e_k).$$

Simplifying, we have

$$r_x e_{d+1} e_{d+2} i(u_x) + \sum_{1 \le j < k \le d} \lambda_{j,k} (-u_{x,j} e_k e_{d+1} e_{d+2} + u_{x,k} e_j e_{d+1} e_{d+2})$$
$$= r_x e_{d+1} e_{d+2} i(u_y) + \sum_{1 \le j < k \le d} \lambda_{j,k} (-u_{y,j} e_k e_{d+1} e_{d+2} + u_{y,k} e_j e_{d+1} e_{d+2}).$$

This leads to the following system of linear equations.

$$\begin{pmatrix} r_x & \lambda_{1,2} & \lambda_{1,3} & \cdots & \lambda_{1,d} \\ -\lambda_{1,2} & r_x & \lambda_{2,3} & \cdots & \lambda_{2,d} \\ -\lambda_{1,3} & -\lambda_{2,3} & r_x & \cdots & \lambda_{3,d} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\lambda_{1,d} & -\lambda_{2,d} & -\lambda_{3,d} & \cdots & r_x \end{pmatrix} \begin{pmatrix} u_{x,1} - u_{y,1} \\ u_{x,2} - u_{y,2} \\ u_{x,3} - u_{y,3} \\ \vdots \\ u_{x,d} - u_{y,d} \end{pmatrix} = 0.$$

By repeating the eigenvalues argument from the proof of Lemma 5.5, we get that the only solution to this system is $u_{x,j} = u_{y,j}$ for every $1 \le j \le d$. Since $u_x = u_y$, we conclude that $x = y$. $\square$

Corollary 5.7. *The restriction of η_d to $\text{Spun}(d)_+$ is injective.*

Proof. Consider two elements $x, y \in \text{Spun}(d)_+$ such that $\eta_d(x) = \eta_d(y)$. Let x_1 be the first coordinate of x and let y_1 be the first coordinate of y. We set $x' = x/x_1$ and $y' = y/y'$, and note that $x', y' \in H_1$. Moreover, we have that $\eta_d(x) = \eta_d(x') = \pi' \circ \pi_1(x')$ and $\eta_d(y) = \eta_d(y') = \pi' \circ \pi_1(y')$. This also implies that $\eta_d(x') = \eta_d(y')$, which in turn implies that x' and y' have the same 2-terms. Since x' and y' also have the same first coordinate, Lemma 5.6 states that $x' = y'$. By the definition of $\text{Spun}(d)_+$, there is a unique $r \in \mathbb{R}$ such that $r \cdot x' \in \text{Spun}(d)_+$. We thus conclude that $x = y$. $\square$

We next show that the restriction of η_d to $\text{Spun}(d)_+$ is surjective in a similar manner.

Lemma 5.8. *Consider $r \in \mathbb{R}$ and elements $\lambda_{j,k} \in \mathbb{R}$ for every $1 \le j < k \le d$, such that $r \neq 0$. Then there exists $g \in G_d$ such that the first coordinate of g is r and the coefficient of the term $e_j e_k$ in g is $\lambda_{j,k}$.*

Proof. We prove the lemma by induction on d. For the induction basis, note that the claim is trivial when $d = 1$. For the induction step, we assume that the claim holds for G_{d-1} and consider the case of G_d.

By the induction hypothesis, there exists $h \in G_{d-1}$ with first coordinate r and the term $\lambda_{j,k} e_j e_k$ for every $1 \le j < k \le d-1$. We set $g = h - h e_d i(u) \in G_d$, for some $u \in \mathbb{R}^{d-1}$ that will be determined below. Note that the first coordinate of g is r and the coefficient of the term $e_j e_k$ in g is $\lambda_{j,k}$, for $1 \le j < k \le d-1$. We now consider the terms of the form $e_j e_d$ in g, and observe that these are all in $-he_d i(u)$. Let u_j denote the j'th coordinate of u. Since for every $1 \le j \le d-1$ we would like g to contain the term $\lambda_{j,d} e_j e_d$, we get the following system of linear equations.

$$\begin{pmatrix} r & -\lambda_{1,2} & -\lambda_{1,3} & \cdots & -\lambda_{1,d-1} \\ \lambda_{1,2} & r & -\lambda_{2,3} & \cdots & -\lambda_{2,d-1} \\ \lambda_{1,3} & \lambda_{2,3} & r & \cdots & -\lambda_{3,d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{1,d-1} & \lambda_{2,d-1} & \lambda_{3,d-1} & \cdots & r \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_{d-1} \end{pmatrix} = \begin{pmatrix} \lambda_{1,d} \\ \lambda_{2,d} \\ \lambda_{3,d} \\ \vdots \\ \lambda_{d-1,d} \end{pmatrix}.$$

By repeating the eigenvalues argument from the proof of Lemma 5.5, we get that the above matrix is invertible. Thus, there exists a choice of $u_1, \dots, u_{d-1}$ such that the above system holds. That is, there exists $u \in \mathbb{R}^{d-1}$ such that g satisfies the assertion of the lemma. □

Lemma 5.9. *Consider $r \in \mathbb{R}$ and elements $\lambda_{j,k} \in \mathbb{R}$ for every $1 \le j < k \le d+1$, such that $r \neq 0$. Then there exists $g \in J_d$ such that the first coordinate of g is r and the coefficient of the term $e_j e_k$ in g is $\lambda_{j,k}$ (when $k = d+1$ we consider the term $e_j e_{d+1} e_{d+2}$ instead).*

Proof. By lemma 5.8, there exists $h \in G_d$ such that the first coordinate of h is r and the coefficient of the term $e_j e_k$ is $\lambda_{j,k}$, for every $1 \le j < k \le d$. We set $g = h - he_{d+1}e_{d+2}i(u) \in J_d$, for a vector $u \in \mathbb{R}^d$ that will be determined below. Note that the first coordinate of g is r and the coefficient of the term $e_j e_k$ in g is $\lambda_{j,k}$, for $1 \le j < k \le d$. We now consider the terms of the form $e_j e_{d+1} e_{d+2}$ in g, and observe that these are all in $-he_{d+1}e_{d+2}i(u)$. Let u_j denote the j'th coordinate of u. Since for every $1 \le j \le d$ we would like g to contain the term $\lambda_{j,d+1} e_j e_{d+1} e_{d+2}$, we get the following system of linear equations.

$$\begin{pmatrix} r & -\lambda_{1,2} & -\lambda_{1,3} & \cdots & -\lambda_{1,d} \\ \lambda_{1,2} & r & -\lambda_{2,3} & \cdots & -\lambda_{2,d} \\ \lambda_{1,3} & \lambda_{2,3} & r & \cdots & -\lambda_{3,d} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{1,d} & \lambda_{2,d} & \lambda_{3,d} & \cdots & r \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_d \end{pmatrix} = \begin{pmatrix} \lambda_{1,d+1} \\ \lambda_{2,d+1} \\ \lambda_{3,d+1} \\ \vdots \\ \lambda_{d,d+1} \end{pmatrix}.$$

By repeating the eigenvalues argument from the proof of Lemma 5.5, we get that the above matrix is invertible. Thus, there exists a choice of $u_1, \dots, u_d$ such that the above system holds. That is, there exists $u \in \mathbb{R}^d$ such that g satisfies the assertion of the lemma. □

Theorem 5.10. *The map $\eta_d : \mathrm{Spun}(d)_+ \to \mathbb{R}^{\binom{d+1}{2}}$ is a bijection.*

Proof. By Corollary 5.7 the restriction of η_d to $\mathrm{Spun}(d)_+$ is injective. It remains to show that this restriction is surjective on $\mathbb{R}^{\binom{d+1}{2}}$. Consider $v \in \mathbb{R}^{\binom{d+1}{2}}$. By Lemma 5.9, there exists $g \in J_d$ such that $\eta_d(g) = v$ and the first coordinate of g is 1. By the definition of J_d, there exists $r \in \mathbb{R} \setminus \{0\}$ such that $rg \in \mathrm{Spun}(d)$. We have that $\eta_d(rg) = \eta_d(g) = v$. Thus, the restriction of η_d to $\mathrm{Spun}(d)_+$ is surjective on $\mathbb{R}^{\binom{d+1}{2}}$. □

Now that we established that the restriction of η_d to $\mathrm{Spun}(d)_+$ is a bijection, we move to study the image of $T_{ap} \cap \mathrm{Spun}(d)_+$ under η_d. In particular, we will show that this image is a $\binom{d}{2}$-flat. Similarly to $\mathrm{Spun}(d)_+$, let $\mathrm{Spin}(d)_+$ be the set of elements of $\mathrm{Spin}(d)$ where the term $\mathbf{1}$ has a positive coefficient. We also recall the definition of F_{ap} from (7).

Lemma 5.11. *For $a, p \in \mathbb{R}^d$, we have $\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+) = \eta_d(F_{ap} \setminus H_0)$.*

Proof. By Lemma 3.6 we have $T_{ap} \cap \mathrm{Spun}(d)_+ \subseteq F_{ap} \setminus H_0$, which implies that $\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+) \subseteq \eta_d(F_{ap} \setminus H_0)$. For the other direction, we consider $z \in F_{ap} \setminus H_0$. To complete the proof, we will show that there exists $x \in T_{ap} \cap \mathrm{Spun}(d)_+$ such that $\eta_d(z) = \eta_d(x)$.

We recall that $\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)\left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) = \mathbf{1}$. Since $z \in F_{ap}$, we have

$$\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) z \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) \in C\ell^0_d.$$

Since $C\ell^0_d$ is contained in Z^0_d, we can also think of G_d as contained in Z^0_d. Then, by Lemma 5.8 there exists $\gamma \in \mathrm{Spin}(d)_+$ such that

$$\eta_d(\gamma) = \eta_d\left(\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) z \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(a)\right)\right).$$

Thus, there exists $\lambda \in \mathbb{R}\setminus\{0\}$ such that $\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) z \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) - \lambda\gamma$ contains no 0-term and no 2-terms. By Lemma 5.3, multiplying from the left by $\left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)$ and from the right by $\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right)$ cannot create any 0-terms and 2-terms. That is, setting $y = \lambda\left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)\gamma\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right)$, the expression $z - y$ contains no 0-terms and 2-terms. Equivalently, z and y have the same the same 0-terms and 2-terms. Note that y has a nonzero first coordinate, so $\eta_d(y) = \eta_d(z)$.

Set $x = y/\lambda$. By Lemma 3.5, we have

$$x = \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)\gamma\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) = \gamma + \frac{1}{2}e_{d+1}e_{d+2}\left(i(p)\gamma - \gamma i(a)\right) \in T_{ap}.$$

Since $\gamma \in \mathrm{Spin}(d)_+$, we get that $x \in \mathrm{Spun}(d)_+$. Finally, $\eta_d(x) = \eta_d(y) = \eta_d(z)$, as required. □

Note that the map $\eta_d(x)$ is well-defined for every point $x \in \mathbb{R}^{2^d} \setminus H_0$. Additionally, when we restrict the domain of η_d to H_1 it is a linear map. Let $\eta'_d : \mathbb{R}^{2^d} \to \mathbb{R}^{\binom{d+1}{2}}$ be the standard projection that keeps only the coordinates corresponding to basis elements of Z^0_d that are 2-terms. We can think of η'_d as a linear extension of the restricted η_d to $\mathbb{R}^{2^d}$.

Lemma 5.12. *The projection $\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+)$ is a $\binom{d}{2}$-flat.*

Proof. Since F_{ap} is ruled by lines that are incident to the origin, we get that $\eta_d(F_{ap} \setminus H_0) = \eta_d(F_{ap} \cap H_1)$. Since $F_{ap} \cap H_1$ is a flat and the restriction of η_d to H_1 is a linear map, Lemma 5.11 implies that $\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+)$ is a flat in $\mathbb{R}^{\binom{d+1}{2}}$. It remains to establish the dimension of this flat.

From the definition of F_{ap} in (7) we notice that $F_{ap} \cap H_1 \neq \emptyset$ (for example, by taking the element $\mathbf{1}$ from $C\ell^0_d$ in this definition). We also note that every $v \in F_{ap} \cap H_1$ satisfies $F_{ap} \cap H_1 = v + (F_{ap} \cap H_0)$. For such a v we have

$$\eta_d(F_{ap} \setminus H_0) = \eta_d(F_{ap} \cap H_1) = \eta'_d(v + F_{ap} \cap H_0) = \eta_d(v) + \eta'_d(F_{ap} \cap H_0).$$

Combining the above with Lemma 5.11 implies that

$$\dim(\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+)) = \dim(\eta'_d(F_{ap} \cap H_0)) = \dim(F_{ap} \cap H_0) - \dim\left(\ker \eta'_d \cap F_{ap} \cap H_0\right).$$

Since $\dim F_{ap} = \dim(C\ell^0_d) = 2^{d-1}$ and F_{ap} properly intersects the hyperplane H_0, we get that $\dim(F_{ap} \cap H_0) = 2^{d-1} - 1$. Note that the elements of $\ker \eta'_d \cap F_{ap} \cap H_0$ do not have 2-terms and 0-terms. Let $\tau_{ap} : Z^0_d \to Z^0_d$ be the map defined by $\tau_{ap}(x) = (\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p))x(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a))$. By Lemma 5.3, we have that $\ker \eta'_d \cap F_{ap} \cap H_0$ is the subspace generated by

$$\left\{\tau_{ap}(x) : \ x \text{ is an element of the standard basis of } C\ell^0_d \text{ that is an } m\text{-term for some } m \geq 4\right\}.$$

Since $\tau_{ap}^{-1}(x) = \left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) x \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(a)\right)$, we note that τ_{ap} is a linear bijection. This implies that the above generating set is linearly independent, so $\dim\left(\ker \eta_d' \cap F_{ap} \cap H_0\right) = 2^{d-1} - \binom{d}{2} - 1$. We conclude that

$$\dim(\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+)) = 2^{d-1} - 1 - \left(2^{d-1} - \binom{d}{2} - 1\right) = \binom{d}{2}.$$

□

Studying the flats in $\mathbb{R}^{\binom{d+1}{2}}$. Let $L_{ap} = \eta_d(T_{ap} \setminus H_0)$ be the $\binom{d}{2}$-flat in $\mathbb{R}^{\binom{d+1}{2}}$ that corresponds to T_{ap}. Given points $a, p, b, q \in \mathbb{R}^d$, we now study what happens to L_{ap} and L_{bq} when $T_{ap} \cap T_{bq} \neq \emptyset$. This part is mostly identical to the case of $\mathbb{R}^3$ that was presented in Section 4. In particular, the proofs of Lemma 4.4, Lemma 4.5, Lemma 4.7, and Corollary 4.8 easily extend to $\mathbb{R}^d$ (by changing e_4e_5 to $e_{d+1}e_{d+2}$ and other such straightforward revisions).

The proof of Lemma 4.6 does not immediately extend to $\mathbb{R}^d$. Instead of that lemma, we rely on the three following ones. Let T_{ap+} be the set of points of T_{ap} that have a positive first coordinate.

Lemma 5.13. *If $T_{ap} \cap T_{bq} \not\subseteq H_0$ then $L_{ap} \cap L_{bq} = \eta_d\left(F_{ap} \cap F_{bq} \cap H_1\right)$.*

Proof. By Lemma 3.6 we have $T_{ap+} \cap T_{bq+} \subseteq (F_{ap} \cap F_{bq}) \setminus H_0$. This implies that

$$\eta_d(T_{ap+} \cap T_{bq+}) \subseteq \eta_d\left((F_{ap} \cap F_{bq}) \setminus H_0\right) = \eta_d\left(F_{ap} \cap F_{bq} \cap H_1\right).$$

By Lemma 5.11 we have that $\eta_d(T_{ap+}) = \eta_d(F_{ap} \setminus H_0) = \eta_d(F_{ap} \cap H_1)$, and symmetrically $\eta_d(T_{bq+}) = \eta_d(F_{bq} \cap H_1)$. Combining this with Theorem 5.10 implies that

$$\eta_d(T_{ap+} \cap T_{bq+}) = \eta_d(T_{ap+}) \cap \eta_d(T_{bq+}) = \eta_d(F_{ap} \cap H_1) \cap \eta_d(F_{bq} \cap H_1) \supseteq \eta_d\left(F_{ap} \cap F_{bq} \cap H_1\right).$$

Combining the above, we conclude that

$$\eta_d\left(F_{ap} \cap F_{bq} \cap H_1\right) = \eta_d(T_{ap+} \cap T_{bq+}) = L_{ap} \cap L_{bq},$$

as asserted. □

In Lemma 5.15 below, we will study $L_{ap} \cap L_{bq}$ when $T_{ap} \cap T_{bq} \not\subseteq H_0$. Handling the case where $T_{ap} \cap T_{bq} \neq \emptyset$ and $T_{ap} \cap T_{bq} \subseteq H_0$ is more difficult. The following lemma shows that this problematic case cannot happen too often.

Lemma 5.14. *Assume that $T_{ap} \cap T_{bq} \neq \emptyset$. Then $T_{ap} \cap T_{bq} \subseteq H_0$ if and only if $a - b = q - p$.*

Proof. By the (straightforward) extension of Lemma 4.5 to $\mathrm{Spun}(d)$, we have

$$F_{ap} \cap F_{bq} = \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) \beta C\ell^0_{d-1}\alpha \left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right), \tag{18}$$

for any $\alpha, \beta \in \mathrm{Spin}(d)$ that satisfy $\alpha\frac{i(b-a)}{\|b-a\|}\alpha^{-1} = e_d$ and $\beta e_d \beta^{-1} = \frac{i(q-p)}{\|q-p\|}$. Combining this with Lemma 5.3 implies that

$$\left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) \beta C\ell^0_{d-1}\alpha \left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) \subseteq H_0 \tag{19}$$

if and only if $\beta C\ell^0_{d-1}\alpha \subseteq H_0$. By lemma 5.1 we have that $x \in H_0$ if and only if $\beta^{-1}x\beta \in H_0$, so $\beta C\ell^0_{d-1}\alpha \subseteq H_0$ if and only if $C\ell^0_{d-1}\alpha\beta \subseteq H_0$.

Assume that $a-b=q-p$. For an arbitrary $\beta \in \operatorname{Spin}(d)$ such that $\beta e_d \beta^{-1} = \frac{i(q-p)}{\|q-p\|}$, set $\gamma = e_{d-1}e_d$ and $\alpha = \gamma\beta^{-1}$. Since γ is the product of two elements from $i(\mathbb{S}^{d-1})$, we have that $\gamma \in \operatorname{Spin}(d)$, which in turn implies that $\alpha \in \operatorname{Spin}(d)$. We get that

$$\alpha \left(\frac{i(b-a)}{\|b-a\|} \right) \alpha^{-1} = \gamma\beta^{-1} \left(\frac{i(b-a)}{\|b-a\|} \right) \beta\gamma^{-1} = -\gamma\beta^{-1} \left(\frac{i(q-p)}{\|q-p\|} \right) \beta\gamma^{-1} = -\gamma e_d \gamma^{-1} = e_d. \quad (20)$$

We can thus use these α and β in (19). This implies that $C\ell^0_{d-1}\alpha\beta = C\ell^0_{d-1}e_{d-1}e_d \subseteq H_0$, which in turn implies that (19) is false. Combining this with (18) and with Lemma 3.6 implies $T_{ap} \cap T_{bq} \subseteq H_0$.

Next, assume that $a-b \neq q-p$. For an arbitrary $\beta \in \operatorname{Spin}(d)$ such that $\beta e_d \beta^{-1} = \frac{i(q-p)}{\|q-p\|}$, set $B = \beta^{-1}\frac{i(b-a)}{\|b-a\|}\beta$. We have that $-e_d \neq B$, so we may set $\gamma = \frac{1}{\|e_d+B\|} e_d \left(e_d + B\right)$ and $\alpha = \gamma\beta^{-1}$. Since γ is the product of two elements from $i(\mathbb{S}^{d-1})$, we have that $\gamma \in \operatorname{Spin}(d)$, which in turn implies that $\alpha \in \operatorname{Spin}(d)$. Performing a calculation similar to the one in the proof of lemma 5.4, we have that $\alpha \left(\frac{i(b-a)}{\|b-a\|} \right) \alpha^{-1} = e_d$. We can thus use these α and β in (18).

Let

$$x = \left(\mathbf{1} + \frac{1}{2} e_{d+1}e_{d+2}i(p) \right) \beta \mathbf{1} \gamma \beta^{-1} \left(\mathbf{1} - \frac{1}{2} e_{d+1}e_{d+2}i(a) \right). \quad (21)$$

Note that $x \in F_{ap} \cap F_{bq}$. By Lemmas 5.1, 5.2, and 5.3 we have that $x \notin H_0$. Since x is a product of elements of $\operatorname{Spun}(d)$, we have that $x \in \operatorname{Spun}(d)$. Lemma 3.6 implies $T_{ap} \cap T_{bq} = F_{ap} \cap F_{bq} \cap \operatorname{Spun}(d)$, so $x \in T_{ap} \cap T_{bq}$. We conclude that $T_{ap} \cap T_{bq} \not\subseteq H_0$, which completes the proof. $\square$

Lemma 5.15. *If $T_{ap} \neq T_{bq}$ and $T_{ap} \cap T_{bq} \not\subseteq H_0$, then* $\dim\left(L_{ap} \cap L_{bq}\right) = \binom{d-1}{2}$.

Proof. By the assumption $L_{ap} \cap L_{bq} \neq \emptyset$. Let $v \in L_{ap} \cap L_{bq}$, and note that it suffices to prove that $\dim\left((L_{ap} - v) \cap (L_{bq} - v)\right) = \binom{d-1}{2}$. By Lemma 5.13,

$$(L_{ap} - v) \cap (L_{bq} - v) + v = L_{ap} \cap L_{bq} = \eta_d \left(F_{ap} \cap F_{bq} \cap H_1\right) = \eta'_d \left(F_{ap} \cap F_{bq} \cap H_0\right) + v.$$

By the extension of Lemma 4.5 to $\mathbb{R}^d$, we have that $\dim\left(F_{ap} \cap F_{bq}\right) = \dim(C\ell_{d-1}) = 2^{d-2}$. The assumption $T_{ap} \cap T_{bq} \not\subseteq H_0$ implies that $F_{ap} \cap F_{bq}$ properly intersects H_0. This in turn implies $\dim\left(F_{ap} \cap F_{bq} \cap H_0\right) = 2^{d-2} - 1$. It remains to show that $\dim\left(F_{ap} \cap F_{bq} \cap H_0 \cap \ker\left(\eta'_d\right)\right) = 2^{d-2} - \binom{d-1}{2} - 1$.

For an arbitrary $\beta \in \operatorname{Spin}(d)$ that satisfies $\beta e_d \beta^{-1} = \frac{i(q-p)}{\|q-p\|}$, set $B = \beta^{-1}\frac{i(b-a)}{\|b-a\|}\beta$. By Lemma 5.14, the assumption $T_{ap} \cap T_{bq} \not\subseteq H_0$ implies $a-b \neq q-p$, which in turn implies that $B \neq -e_d$. Let $\gamma = \frac{1}{\|e_n+B\|} e_n \left(e_n + B\right)$ and let $\alpha = \gamma\beta^{-1}$. Since γ is the product of two elements from $i(\mathbb{S}^{d-1})$, we have that $\gamma \in \operatorname{Spin}(d)$, which in turn implies that $\alpha \in \operatorname{Spin}(d)$. By repeating the argument in (20), we get that $\alpha\frac{b-a}{\|b-a\|}\alpha^{-1} = e_d$. By the extension of Lemma 4.5 to $\mathbb{R}^d$, we have

$$F_{ap} \cap F_{bq} = \left(\mathbf{1} + \frac{1}{2} e_{d+1}e_{d+2}i(p) \right) \beta C\ell^0_{d-1} \gamma \beta^{-1} \left(\mathbf{1} - \frac{1}{2} e_{d+1}e_{d+2}i(a) \right). \quad (22)$$

Consider the map $\tau_{ap} : Z^0_d \to Z^0_d$ defined by

$$\tau_{ap}(x) = \left(\mathbf{1} + \frac{1}{2} e_{d+1}e_{d+2}i(p) \right) \beta x \alpha \left(\mathbf{1} - \frac{1}{2} e_{d+1}e_{d+2}i(a) \right).$$

Since $\tau_{ap}^{-1}(x) = \beta^{-1}\left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(p)\right) x \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(a)\right)\alpha^{-1}$, we note that τ_{ap} is a linear bijection.

We claim that $F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta_d')$ is generated by

$$\left\{\tau(f) : \ f \text{ is an element of the standard basis of } C\ell_{d-1}^0 \text{ and an } m\text{-term for some } m \geq 4\right\}. \quad (23)$$

Indeed, for any such m-term f, Lemmas 5.1, 5.2, and 5.3 imply that

$$\tau(f) = \left(\mathbf{1} + \frac{1}{2}e_{d+1}e_{d+2}i(p)\right)\beta f \alpha \left(\mathbf{1} - \frac{1}{2}e_{d+1}e_{d+2}i(a)\right) \in H_0 \cap \ker(\eta_d').$$

By (22), this expression is also in $F_{ap} \cap F_{bq}$.

If $f \in Z_d^0$ contains a 0-term or a 2-term, then Lemmas 5.1, 5.2, and 5.3 imply that $\tau_{ap}(f) \notin F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta_d')$. That is, if $g \in F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta_d')$ then $\tau_{ap}^{-1}(g)$ contains no 0-term or 2-terms. We conclude that (23) generates $F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta_d')$. Since $\tau(f)$ is a bijection, the set (23) is a linearly independent subset of $F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta_d')$. This implies that $\dim(F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta_d')) = 2^{d-2} - \binom{d-1}{2} - 1$, which completes the proof. □

We are now ready to state the connection between the distinct distances problem and the flats L_{ap}. Let Q' be the set of quadruples $(a,p,b,q) \in \mathcal{P}^4$ such that $T_{ap} \cap T_{bq} \not\subseteq H_0$. In particular, note that $(a,p,b,q) \in Q'$ implies that $T_{ap} \cap T_{bq} \neq \emptyset$.

Corollary 5.16. *We have that $Q' \subset Q$ and $|Q'| \geq |Q|/2$.*

Proof. Recall that a quadruple $(a,p,b,q) \in \mathcal{P}^4$ is in Q if and only if $T_{ap} \cap T_{bq} \neq \emptyset$. Since $T_{ap} \cap T_{bq} \not\subseteq H_0$ implies $T_{ap} \cap T_{bq} \neq \emptyset$, we have that $Q' \subseteq Q$. It remains to show that at least half of the quadruples of Q are also in Q'. Consider $T_{ap} \neq T_{bq}$ such that $T_{ap} \cap T_{bq} \subseteq H_0$. By Lemma 5.14 we have that $a - b = q - p$. This implies that $b - a \neq p - q$, so $T_{bp} \cap T_{aq} \not\subseteq H_0$ (since $|ab| = |pq|$, we get that $T_{bp} \cap T_{aq} \neq \emptyset$). That is, for every quadruple $(a,p,b,q) \in Q$ not in Q' there exists a distinct quadruple (b,p,a,q) that is in Q'. □

Flats in $\mathbb{R}^{\binom{d+1}{2}}$ and in $\mathbb{R}^{2d-1}$. We set

$$\mathcal{L} = \{L_{ap} : \ a,p \in \mathcal{P} \text{ and } a \neq p\}.$$

Note that $\mathcal{L}$ is a set of $\Theta(n^2)$ flats of dimension $\binom{d}{2}$ in $\mathbb{R}^{\binom{d+1}{2}}$. By Corollary 5.16, to get an asymptotic upper bound for the number of quadruples in Q it suffices to derive an upper bound for the number of quadruples $(a,p,b,q) \in \mathcal{P}^4$ such that $T_{ap} \cap T_{bq} \not\subseteq H_0$. By Lemma 5.15 every such quadruple satisfies $\dim L_{ap} \cap L_{bq} = \binom{d-1}{2}$. On the other hand, when $T_{ap} \cap T_{bq} \subseteq H_0$ we have that $L_{ap} \cap L_{bq} = \emptyset$. Thus, it remains to derive an upper bound on the number of pairs of flats of $\mathcal{L}$ that intersect (in a $\binom{d-1}{2}$-flat).

The proof of the following lemma is identical to the proof of Lemma 4.10.

Lemma 5.17. *(a) Every point of $\mathbb{R}^{\binom{d+1}{2}}$ is contained in at most n flats of $\mathcal{L}$.*
(b) Every hyperplane in $\mathbb{R}^{\binom{d+1}{2}}$ contains at most n flats of $\mathcal{L}$.

Note that $\binom{d+1}{2} - \binom{d-1}{2} = 2d-1$ and that $\binom{d}{2} - \binom{d-1}{2} = d-1$. Let H_g be a generic $(2d-1)$-flat in $\mathbb{R}^{\binom{d+1}{2}}$, in the sense that:

- Every $\binom{d}{2}$-flat of $\mathcal{L}$ intersects H_g in a $(d-1)$-flat.
- Every $\binom{d-1}{2}$-flat of the form $L_{ap} \cap L_{bq}$ (with $a,b,p,q \in \mathcal{P}$) intersects H_g at a single point.

Let $\mathcal{F} = \{L_{ap} \cap H_g : L_{ap} \in \mathcal{L}\}$ and consider H_g as $\mathbb{R}^{2d-1}$. Note that $\mathcal{F}$ is a set of $\Theta(n^2)$ distinct $(d-1)$-flats. Every two $(d-1)$-flats of $\mathcal{F}$ are either disjoint or intersect in a single point. By Lemma 5.17, every point of $\mathbb{R}^{2d-1}$ is incident to at most n of the flats of $\mathcal{F}$ and every hyperplane in $\mathbb{R}^{2d-1}$ contains at most n of the flats of $\mathcal{F}$.

For every integer $k \geq 2$, let m_k denote the number of points of $\mathbb{R}^{2d-1}$ that are contained in exactly k of the $(d-1)$-flats of $\mathcal{F}$. Similarly, let $m_{\geq k}$ denote the number of points of $\mathbb{R}^{2d-1}$ that are contained in *at least* k of the $(d-1)$-flats of $\mathcal{F}$. Then $|Q'|$ is the number of pairs of intersecting $(d-1)$-flats of $\mathcal{F}$, and

$$|Q| \leq 2|Q'| = 2\sum_{k=2}^{n} m_k \cdot 2\binom{k}{2} < 2\sum_{k=2}^{n} k^2 m_k = O\left(\sum_{k=1}^{\log n} 2^{2k} m_{\geq 2^k}\right).$$

If we had the bound $m_{\geq k} = O\left(\frac{n^{(4d-2)/d}}{k^{2+\varepsilon}}\right)$ for some $\varepsilon > 0$, then the above would imply $|Q| = O(n^{(4d-2)/d})$. This would in turn imply that the points of $\mathcal{P}$ span $\Omega\left(n^{2/d}\right)$ distinct distances.

An incidence result of Solymosi and Tao [9] implies that the number of incidences between m points and n flats of dimension $d-1$ in $\mathbb{R}^{2d-1}$, with every two flats intersecting in at most one point, is $O(m^{2/3+\varepsilon'} n^{2/3} + m + n)$ (for any $\varepsilon' > 0$). Every incidence bound of this form has a dual formulation involving k-rich points (for example, see [8, Chapter 1]). In this case, the dual bound is: Given n^2 flats of dimension $d-1$ in $\mathbb{R}^{2d-1}$ such that every two intersect in at most one point, for every $k \geq 2$ the number of k-rich points is $O\left(\frac{n^{4/(1-\varepsilon')}}{k^{3/(1-\varepsilon')}} + \frac{n^2}{k}\right)$. By taking ε' to be sufficiently small with respect to ε, we obtain the bound $m_{\geq k} = O\left(\frac{n^{4+\varepsilon}}{k^3} + \frac{n^2}{k}\right)$ for the number of k-rich points. This bound is stronger than the required bound when $k = \Omega(n^{2/d+\varepsilon})$. That is, it remains to consider the case where $k = O(n^{2/d+\varepsilon})$.

6 The structure of the flats L_{ap}

In this section we study the structure of the $\binom{d}{2}$-flats L_{ap} in $\mathbb{R}^{\binom{d+1}{2}}$. In particular, we derive the equations that define such a flat. This structure is useful for deriving additional properties of the flats, which may be required for solving the incidence problem in Theorem 1.2.

Recall that we think of every coordinate of $\mathbb{R}^{\binom{d+1}{2}}$ as corresponding to a 2-term in the standard basis of Z_d^0. We denote the coordinate corresponding to $e_j e_k$ as $x_{j,k}$, for every $1 \leq j < k \leq d$. Similarly, we denote the coordinate corresponding to $e_j e_{d+1} e_{d+2}$ as $x_{j,d+1}$. For $a \in \mathbb{R}^d$, we denote by a_j the j'th coordinate of a.

Theorem 6.1. *Given $a, p \in \mathbb{R}^d$, the flat $\eta_d(T_{ap} \cap \text{Spun}(d)_+)$ is defined by the following system of d equations in the coordinates of $\mathbb{R}^{\binom{d+1}{2}}$.*

$$\begin{aligned}
a_1 - p_1 =& (a_2 + p_2)x_{1,2} + (a_3 + p_3)x_{1,3} + \cdots + (a_d + p_d)x_{1,d} + 2x_{1,d+1}, \\
a_2 - p_2 =& -(a_1 + p_1)x_{1,2} + (a_3 + p_3)x_{2,3} + \cdots + (a_d + p_d)x_{2,d} + 2x_{2,d+1}, \\
&\vdots \\
a_d - p_d =& -(a_1 + p_1)x_{1,n} - (a_2 + p_2)x_{2,d} - \cdots - (a_{d-1} + p_{d-1})x_{d-1,d} + 2x_{d,d+1}.
\end{aligned}$$

Proof. In the following proof, every reference to orthogonal elements is with respect to the standard inner product $\langle \cdot, \cdot \rangle$ of $\mathbb{R}^{2^d}$. For a vector $v \in \mathbb{R}^{2^d}$, we denote the dual of v as v^*. That is, v^* is the map $v^*(u) = \langle v, u \rangle$. For linear maps $f, g : \mathbb{R}^{2^d} \to \mathbb{R}^{2^d}$, we denote by $f^t(g)(v)$ the transpose $g(f(v))$.

Consider the linear map $\tau_{ap} : Z_d^0 \to Z_d^0$ defined by

$$\tau_{ap}(x) = \left(\mathbf{1} + \frac{1}{2} e_{d+1} e_{d+2} i(p)\right) x \left(\mathbf{1} - \frac{1}{2} e_{d+1} e_{d+2} i(a)\right).$$

We also observe that

$$\tau_{ap}^{-1}(x) = \left(\mathbf{1} - \frac{1}{2} e_{d+1} e_{d+2} i(p)\right) x \left(\mathbf{1} + \frac{1}{2} e_{d+1} e_{d+2} i(a)\right). \tag{24}$$

Thus, τ_{ap} is a linear bijection.

Lemma 6.2. *For $u, w \in Z_d^0$, we have that u is orthogonal to $\tau_{ap}(w)$ if and only if $u = \left((\tau_{ap}^{-1})^t \circ v^*\right)^*$ for some $v \in \mathbb{R}^{2^d}$ orthogonal to w.*

Proof. Let $v \in \mathbb{R}^{2^d}$ be orthogonal to w. We have that[4]

$$\begin{aligned}\langle \left((\tau_{ap}^{-1})^t \circ v^*\right)^*, \tau_{ap}(w)\rangle &= \left(\left((\tau_{ap}^{-1})^t \circ v^*\right)^*\right)^* (\tau_{ap}(w)) = \left((\tau_{ap}^{-1})^t \circ v^*\right)(\tau_{ap}(w)) \\ &= \left(v^* \circ \tau_{ap}^{-1}\right)(\tau_{ap}(w)) = v^*(w) = \langle v, w\rangle = 0.\end{aligned}$$

That is, $\left((\tau_{ap}^{-1})^t \circ v^*\right)^*$ is orthogonal to $\tau_{ap}(w)$, as required.

For the other direction, assume that u is orthogonal to $\tau_{ap}(w)$ and note that

$$u = (u^*)^* = \left((\tau_{ap}^{-1})^t \left(((\tau_{ap}^{-1})^t)^{-1} \circ u^*\right)\right)^*.$$

That is, $u = \left((\tau_{ap}^{-1})^t \circ v^*\right)^*$ for $v = \left(((\tau_{ap}^{-1})^t)^{-1} \circ u^*\right)^*$. We also have that

$$\begin{aligned}\langle v, w\rangle = \left\langle \left(((\tau_{ap}^{-1})^t)^{-1} \circ u^*\right)^*, w \right\rangle &= \left(\left(((\tau_{ap}^{-1})^t)^{-1} \circ u^*\right)^*\right)^* (w) = \left(((\tau_{ap}^{-1})^t)^{-1} \circ u^*\right)(w) \\ &= \left(\tau_{ap}^t(u^*)\right)(w) = u^*\left(\tau_{ap}(w)\right) = \langle u, \tau_{ap}(w)\rangle = 0.\end{aligned}$$

□

Let V_d^0 be the orthogonal complement of $C\ell_d^0$ in Z_d^0. Note that every term of every element of V_d^0 contains $e_{d+1}e_{d+2}$. Lemma 6.2 implies that $\left((\tau_{ap}^{-1})^t \circ \left(V_d^0\right)^*\right)^*$ is the orthogonal complement of $\tau_{ap}\left(C\ell_d^0\right)$. Let $I_{2^{d-1}}$ be the $2^{d-1} \times 2^{d-1}$ identity matrix. We can express $(\tau_{ap}^{-1})^t$ as a $2^d \times 2^d$ matrix of the form[5]

$$\begin{pmatrix} I_{2^{d-1}} & C \\ 0 & I_{2^{d-1}} \end{pmatrix}. \tag{25}$$

Indeed, recall that taking the transpose of a linear transformation corresponds to taking the transpose of the matrix of this transformation. Note that the columns of (25) with index greater than 2^{d-1} form a basis of $(\tau_{ap}^{-1})^t \circ (V_d^0)^*$.

We denote the coordinates of $Z_d^0 \cong \mathbb{R}^{2^d}$ as $y_1, \ldots, y_{2^d}$. Let $(v_1, \ldots, v_{2^d})^* \in \left(Z_d^0\right)^*$ be one of the basis vectors of $(\tau_{ap}^{-1})^t \circ (V_d^0)^*$ that are columns of (25). We associate with this vector the equation $v_1 y_1 + \ldots + v_{2^d} y_{2^d} = 0$. Let S_{ap} be the system of 2^{d-1} homogeneous linear equations

[4]Strictly speaking, $(u^*)^*$ is not equal to u. With a slight abuse of notation, we apply here the natural isomorphism between the space $\left(\mathbb{R}^{2^d *}\right)^*$ and $\mathbb{R}^{2^d}$.

[5]To write this matrix, we must choose a specific ordering of the dual elements of the standard basis of Z_d^0. As long as the elements dual to the basis elements involving $e_{d+1}e_{d+2}$ come after those dual to those that do not, the details of the ordering do not matter.

that are obtained in this way from the column vectors of (25) with index greater than 2^{d-1}. Since $\left((\tau_{ap}^{-1})^t \circ \left(V_d^0\right)^*\right)^*$ is the orthogonal complement of $\tau_{ap}\left(C\ell_d^0\right)$, the set of solutions to S_{ap} is $\tau_{ap}\left(C\ell_d^0\right)$.

We construct a system of homogeneous linear equations S'_{ap} by taking a subset of the equations of S_{ap}, as follows. Let $v_1y_1 + \ldots + v_{2^d}y_{2^d} = 0$ be an equation of S_{ap}. We add this equation to S'_{ap} if for every nonzero coefficient v_j the variable y_j corresponds either to a 0-term or to a 2-term. Let F'_{ap} be the set of solutions to the system S'_{ap}.

Lemma 6.3. $\eta_d(F'_{ap} \setminus H_0) = \eta_d(\tau_{ap}(C\ell_d^0) \setminus H_0)$.

Proof. As stated above, the set of solutions to S_{ap} is $\tau_{ap}(C\ell_d^0)$. Since $S'_{ap} \subset S_{ap}$, we get that $\tau_{ap}(C\ell_d^0) \subset F'_{ap}$. This immediately implies $\eta_d(\tau_{ap}(C\ell_d^0) \setminus H_0) \subseteq \eta_d(F'_{ap} \setminus H_0)$. It remains to prove that $\eta_d(F'_{ap} \setminus H_0) \subseteq \eta_d(\tau_{ap}(C\ell_d^0) \setminus H_0)$.

For a linear equation $w_1y_1+\ldots+w_{2^d}y_{2^d} = 0$, we set $w = (w_1, \ldots, w_{2^d})^*$ and $u = (u_1, \ldots, u_{2^d})^* = \tau_{ap}^t \circ w$. If $z \in Z_d^0$ is a solution to $w_1y_1 + \ldots + w_{2^d}y_{2^d} = 0$ then w^* is orthogonal to z, which in turn implies that $\left(\tau_{ap}^t \circ w\right)^*$ is orthogonal to $\tau_{ap}^{-1}(z)$. That is, $\tau_{ap}^{-1}(z)$ is a solution to $u_1y_1+\ldots+u_{2^d}y_{2^d} = 0$. Conversely, if $z \in Z_d^0$ is a solution to $u_1y_1 + \ldots + u_{2^d}y_{2^d} = 0$ (that is, u^* is orthogonal to z) then $\tau_{ap}(z)$ is orthogonal to $\left((\tau_{ap}^{-1})^t \circ u\right)^* = \left((\tau_{ap}^t)^{-1} \circ u\right)^* = w^*$. We conclude that τ_{ap}^{-1} is a bijection from the solutions to $w_1y_1 + \ldots + w_{2^d}y_{2^d} = 0$ to the solutions to $u_1y_1 + \ldots + u_{2^d}y_{2^d} = 0$.

Recall that every equation of S_{ap} is defined by a dual vector $v \in (\mathbb{R}^d)^*$ of the form $(\tau_{ap}^{-1})^t \circ (\gamma e_{d+1}e_{d+2})^*$, where $\gamma e_{d+1}e_{d+2}$ is a basis vector of V_d^0 (that is, γ is in the standard basis of $C\ell_d^1$). Every non-zero term of such a vector corresponds to a 0-term or a 2-term if and only if $v^* \in \mathbb{R}^d$ is orthogonal to every vector corresponding to an m-term for some $m \geq 4$. Let $w \in \mathbb{R}^d$ be a vector that corresponds to such an m-term. If $\gamma = e_j$ for some $1 \leq j \leq d$, then Lemma 5.3 implies that $\tau_{ap}^{-1}(w)$ is orthogonal to $\gamma e_{d+1}e_{d+2}$. Lemma 6.2 states that $((\tau_{ap}^{-1})^t \circ (e_je_{d+1}e_{d+2})^*)^*$ is orthogonal to $\tau_{ap}((\tau_{ap}^{-1})^t(w)) = w$. That is, when $\gamma = e_j$ the equation defined by v is in S'_{ap}.

Next, assume that $\gamma e_{d+1}e_{d+2}$ is an m-term with $m \geq 4$, and write $u = \gamma e_{d+1}e_{d+2}$. Lemma 5.3 implies that $\tau_{ap}(u)$ contains neither 2-terms nor a 0-term. If $((\tau_{ap}^{-1})^t \circ u^*)^*$ is orthogonal to $\tau_{ap}(u)$ then by (the other direction of) Lemma 6.2 we get that u is orthogonal to u. This contradiction implies that $((\tau_{ap}^{-1})^t \circ u^*)^*$ is not orthogonal to $\tau_{ap}(u)$, so in this case the equation defined by v is not in S'_{ap}.

Combining the two preceding paragraphs implies that the equations of S'_{ap} are determined by the vectors $(\tau_{ap}^{-1})^t \circ ((e_je_{d+1}e_{d+2})^*)$ for $1 \leq j \leq d$. It follows that the equations of S'_{00} are obtained from those defining S'_{ap} by applying τ_{ap}^t to the coefficient vectors. By the second paragraph of this proof, for every $v \in F'_{ap}$ we have that $\tau_{ap}^{-1}(v) \in F'_{00}$.

When $a = p = 0$, we have that (25) is the identity matrix. Thus, each equation of S_{00} consists of a single term. This in turn implies that F'_{00} is the subspace defined by having 0 in every coordinate that corresponds to a 2-term of the form $e_je_{d+1}e_{d+2}$ (where $1 \leq j \leq d$). For $v \in F'_{ap} \setminus H_0$, we obtain that $\tau_{ap}^{-1}(v)$ contains no terms of the form $e_je_{d+1}e_{d+2}$. By Lemmas 5.6 and 5.9, there is a unique $x \in J_d$ with the property that $x - \tau_{ap}^{-1}(v)$ contains no 0-term and no 2-terms. Note that x also contains no terms of the form $e_je_{d+1}e_{d+2}$, so Lemma 5.8 implies that $x \in G_d$. Since $x \in C\ell_d^0$, we have that $\tau_{ap}(x) \in \tau_{ap}\left(C\ell_d^0\right)$. By Lemma 5.3, the expression $\tau_{ap}\left(x - \tau_{ap}^{-1}(v)\right)$ also contains no 0-term and no 2-terms, so $\eta_d(\tau(x)) = \eta_d(v)$. That is, there exists $\tau_{ap}(x) \in \tau_{ap}\left(C\ell_d^0\right)$ such that $\eta_d(\tau_{ap}(x)) = \eta_d(v)$. Since $v \notin H_0$, we have that $\tau_{ap}^{-1}(v) \notin H_0$, which in turn implies that $x \notin H_0$ and that $\tau(x) \notin H_0$. This implies that $\eta_d(F'_{ap} \setminus H_0) \subseteq \eta_d(\tau_{ap}(C\ell_d^0) \setminus H_0)$ and completes the proof. $\square$

By Lemma 6.3, to complete the proof of Theorem 6.1 it suffices to study $\eta_d(F'_{ap} \setminus H_0)$. We move from the coordinate system y_j to the coordinate system $x_{j,k}$, as described before the statement of the theorem. We denote by x_1 the coordinate corresponding to the coefficient of $\mathbf{1}$ (that is, y_1).

We now study the equations of S'_{ap}. As discussed in the proof of Lemma 6.3, these equations correspond to the dual vectors $(\tau_{ap}^{-1})^t \circ (e_j e_{d+1} e_{d+2})^*$ for $1 \le j \le d$. If $e_j e_{d+1} e_{d+2}$ is the k'th element in our ordering of the basis of Z_d^0, then $(\tau_{ap}^{-1})^t \circ (e_j e_{d+1} e_{d+2})^*$ is the k'th column of the matrix (25). Since the transpose of a linear transformation corresponds to the transpose of the matrix of the transformation, the above is also the k'th row of the matrix of τ_{ap}^{-1}. To get this row, we apply τ_{ap}^{-1} to the basis vectors of Z_d^0 and then keep the coefficient of $e_j e_{d+1} e_{d+2}$ (recall that τ_{ap}^{-1} is defined in (24)). The only basis vectors of Z_d^0 for which this coefficient is nonzero are $\mathbf{1}$ and 2-terms involving e_j. Repeating this process for every $1 \le j \le d$ leads to the following system.

$$\begin{aligned}
(a_1 - p_1)x_1 =& (a_2 + p_2)x_{1,2} + (a_3 + p_3)x_{1,3} + \cdots + (a_d + p_d)x_{1,d} + 2x_{1,d+1},\\
(a_2 - p_2)x_1 =& -(a_1 + p_1)x_{1,2} + (a_3 + p_3)x_{2,3} + \cdots + (a_d + p_d)x_{2,d} + 2x_{2,d+1},\\
&\vdots\\
(a_d - p_d)x_1 =& -(a_1 + p_1)x_{1,d} - (a_2 + p_2)x_{2,d} - \cdots - (a_{d-1} + p_{d-1})x_{d-1,d} + 2x_{d,d+1}.
\end{aligned}$$

Recall from the beginning of Section 5 that $\eta_d = \pi' \circ \pi_1$. Since the above is a system of homogeneous linear equations, F'_{ap} is spanned by lines that are incident to the origin. This implies that $\pi(F'_{ap} \setminus H_0) = \pi(F'_{ap} \cap H_1)$. Thus, $\pi(F'_{ap} \setminus H_0)$ is the set of solutions to the system obtained by setting $x_1 = 1$:

$$\begin{aligned}
(a_1 - p_1) =& (a_2 + p_2)x_{1,2} + (a_3 + p_3)x_{1,3} + \cdots + (a_d + p_d)x_{1,d} + 2x_{1,d+1},\\
(a_2 - p_2) =& -(a_1 + p_1)x_{1,2} + (a_3 + p_3)x_{2,3} + \cdots + (a_d + p_d)x_{2,d} + 2x_{2,d+1},\\
&\vdots\\
(a_d - p_d) =& -(a_1 + p_1)x_{1,d} - (a_2 + p_2)x_{2,d} - \cdots - (a_{d-1} + p_{d-1})x_{d-1,d} + 2x_{d,d+1}.
\end{aligned} \tag{26}$$

Since none of the variables $x_{j,k}$ correspond to elements of $\mathbb{R}^{2^d-1}$ that are in the kernel of π', we get that $\eta_d(F'_{ap})$ is the solution set of (26). $\square$

References

[1] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd edition, Springer-Verlag, Heidelberg, 2007.

[2] G. Elekes and M. Sharir, Incidences in three dimensions and distinct distances in the plane, *Combin. Probab. Comput.* **20** (2011), 571–608.

[3] P. Erdős. On sets of distances of n points. *Amer. Math. Monthly* **53** (1946), 248–250.

[4] J. Fox, J. Pach, A. Sheffer, A. Suk, and J. Zahl, A semi-algebraic version of Zarankiewicz's problem, *J. Eur. Math. Soc.*, to appear.

[5] J. Gallier, Clifford Algebras, Clifford Groups, and a Generalization of the Quaternions, arXiv:0805.0311.

[6] L. Guth and N.H. Katz. On the Erdős distinct distances problem in the plane. *Annals Math.* **181** (2015), 155–190.

[7] M. Rudnev and J. M. Selig, On the Use of the Klein Quadric for Geometric Incidence Problems in Two Dimensions, *SIAM J. Discrete Math.* **30** (2016), 934–954.

[8] A. Sheffer, *Incidence Theory with a Focus on the Polynomial Method*, https://adamsheffer.wordpress.com/pdf-files/.

[9] J. Solymosi and T. Tao, An incidence theorem in higher dimensions, *Discrete Comput. Geom.* **48** (2012), 255–280.

[10] J. Solymosi and V. H. Vu, Near optimal bounds for the Erdős distinct distances problem in high dimensions, *Combinatorica* **28** (2008), 113–125.

[11] T. Tao, Lines in the Euclidean group SE(2), blog post, https://terrytao.wordpress.com/2011/03/05/lines-in-the-euclidean-group-se2/