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

Sam Bardwell–Evans* Adam Sheffer†

October 31, 2018

**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.

**Keywords.** Distinct distances, Combinatorial Geometry, Incidences, Lie groups, Spin group.

## 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 [4] 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 [7] 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 [14]

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

†Department of Mathematics, Baruch College, City University of New York, NY, USA. *adamsh@gmail.com*. Supported by NSF grant DMS-1710305. Corresponding author. 55 Lexington Ave, New York, NY 10010, room 6-291.

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 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 [3]), 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 [7])**.** *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 $\varepsilon$ in the bound $k = O(n^{1/d+\varepsilon})$ comes from an incidence bound of Solymosi and Tao [13]. It is conjectured that this $\varepsilon$ can be removed from the bound of [13], and this would immediately remove the $\varepsilon$ 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 incidence problem stated in Theorem 1.2 is false without including additional restrictions. That is, one can obtain point-flat constructions in $\mathbb{R}^{2d-1}$ that have too many incidences. Using our

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

framework, one can overcome this issue by deriving many additional restrictions for the incidence problem. We do not mention such restrictions in Theorem 1.2, since it is not clear what are the natural restrictions for deriving the incidence bounds. Instead, in Section 7 we demonstrate how our framework can be used to derive additional restrictions, considering specifically the case of distinct distances in $\mathbb{R}^3$.

The problem of distinct distances in $\mathbb{R}^3$ leads to an incidence problem with 2-flats in $\mathbb{R}^5$. In Section 7, we bound the number of such 2-flats that can be contained in a constant-degree variety in $\mathbb{R}^5$. We also bound the number of 2-flats that can have a one-dimensional intersection with a constant-degree two-dimensional variety in $\mathbb{R}^5$. Some of these results are conditional on having a good distinct distances bound for points on constant-degree surfaces in $\mathbb{R}^3$. Thus, to obtain the conjectured distinct distances bound in $\mathbb{R}^3$, it is possible that one would first need to derive a distinct distances bound for the special case of points on a surface in $\mathbb{R}^3$. Currently, such bounds are known for planes, spheres, and two-sheeted hyperboloids (for example, see [15]). However, we are far from having this bound for arbitrary constant-degree surfaces in $\mathbb{R}^3$. For more details, see Sharir and Solomon [11].

The current best bounds for incidences with varieties in $\mathbb{R}^d$ are obtained by the *polynomial partitioning* technique (for example, see [5, 13]). 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 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 [15]. 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 [10].

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

[2] This is done by bounding the number of incidences in the cells while ignoring the incidences on the partition itself. See for example [12, Chapter 8].

$\mathrm{Spun}(d)$.

In Section 2 we briefly describe several Lie groups that we rely on. In Section 3 we introduce the group $\mathrm{Spun}(d)$ 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.** We would like to thank Joshua Zahl for many discussions that eventually led to Section 7. We wish to thank William Ballinger and Dmitri Gekhtman for several helpful discussions. We would also like to thank the anonymous referees for helping to improve a previous draft of this work.

## 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, $\|p - q\|$).

**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 [6, 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 $\alpha$ 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 [6, 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 [6, 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 $\gamma$ on $p$ as $p^\gamma$. 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 $\gamma$ 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 $\rho$ 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 [6, Section 1.4].

**Lemma 2.2.** *Let $d \leq 5$ 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 $d \geq 6$. Combining this lemma with the definition in (1) yields the following result.

**Corollary 2.3.** *For $d \leq 5$, 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 $d \geq 3$. 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 $u'$ □

## 3 The group Spun($d$)

In this section we introduce the group Spun($d$). We first construct a variant $X_d$ of the Clifford algebra $C\ell_d$. Consider the direct sum $\bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^{d+2}\right)^{\otimes k}$, and let $\mathcal{I}$ be the ideal in this tensor algebra that is generated by

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

Then we write $X_d$ as the quotient

$$\bigoplus_{k\in\mathbb{N}} \left(\mathbb{R}^{d+2}\right)^{\otimes k} / \mathcal{I}.$$

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 $1 \leq j \leq d+1$, 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 $1 \leq j \leq d+2$, 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 $1 \leq k \leq d+1$, 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 Spin($d$).

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

We will prove that Spun($d$) is indeed a group and a double cover of SE($d$). But first we give a brief intuition for the definition in (2). We can think of this definition as extending 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 Spin($d+1$), which is a double cover of SO($d+1$). The role of $e_{d+2}$ is to imitate a scaling limit argument as in [15]. We think of $e_{d+2}$ as a small $\varepsilon > 0$, or as the restriction to a small disc on $\mathbb{S}^d$. As $\varepsilon$ approaches zero, this disc behaves more like a flat so Spin($d+1$) becomes more similar to SE($d$).

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

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

*Proof.* We first show that for every $x, y \in \mathrm{Spun}(d)$ we have $xy \in \mathrm{Spun}(d)$. 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 $x \in \mathrm{Spun}(d)$ has an inverse in $\mathrm{Spun}(d)$. We will prove that $x\overline{x} = \overline{x}x = \mathbf{1}$ and that $\overline{x} \in \mathrm{Spun}(d)$. Fix $x \in \mathrm{Spun}(d)$, and write $x = \gamma_1 + e_{d+1}e_{d+2}\gamma_2$ where $\gamma_1 \in C\ell^0_{d+1}$ and $\gamma_2 \in C\ell^1_d$. 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

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

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 $\gamma_1$ is $\overline{\gamma_1}$. Multiplying the above equation $\gamma_1 e_{d+1}\overline{\gamma_1} = e_{d+1}$ by $\gamma_1$ from the right leads to $\gamma_1 e_{d+1} = e_{d+1}\gamma_1$. Since $\gamma_1$ commutes with $e_{d+1}$ we have $\gamma_1 \in C\ell^0_d$, 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

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

Since the inverse of $\gamma_1$ 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 $\gamma_1$ 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 $\gamma_1$ 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 $\gamma_1$ 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 $\gamma_1$ 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

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

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

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

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

Note that $\gamma$ is uniquely determined by $x$, since it is exactly the part of $x$ that does not involve $e_{d+2}$. Once $\gamma$ 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 $(\gamma, v)$ 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 $x \in \mathrm{Spun}(d)$ can be written as $\gamma_x\,(\mathbf{1} + e_{d+1}e_{d+2}i(v_x))$ where $\gamma_x \in \mathrm{Spin}(d)$ 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

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

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

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

Note that $p_x$ and $\Gamma_x$ 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 $\gamma \in \mathrm{Spin}(d)$, by setting $i(u) = \frac{1}{2}\,(\overline{\gamma}p\gamma - i(a)) \in i(\mathbb{R}^d)$ we get

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

Combining this with (4) and with Lemma 3.2 implies that for every $p \in i(\mathbb{R}^d)$ and $\gamma \in \mathrm{Spin}(d)$ there exists $x \in \mathrm{Spun}(d)$ such that $p = p_x$ and $\gamma = \gamma_x$. Every transformation $M \in \mathrm{SE}(d)$ can be written as $(M(a))^+ \circ R \circ (-a)^+$ for some transformation $R \in \mathrm{SO}(d)$. Indeed, note that for any $R \in \mathrm{SO}(d)$ 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 $\rho$ is surjective.

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

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

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 $\rho$ is a group homomorphism. Note that the action

of $\gamma_{xy}$ is first performing the action of $\gamma_y$ and then the action of $\gamma_x$. 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 $\rho$. Let $I$ be identity element of $\mathrm{SE}(d)$ and let $x \in \mathrm{Spun}(d)$ 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 $\Gamma_x$ 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 $\rho$ 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

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

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

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

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. □

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

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

**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

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

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 $2 \leq k = O(n^{1/3+\varepsilon})$ (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 $\rho$ 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

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

That is, $N(x) = \mathbf{1}$ if and only if $x \in \mathcal{C} \cap G$. Combining this with (2) implies that 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 $\gamma_1 \in$ 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

$$\begin{aligned}x\left(e_5i(v) + e_4\right)\overline{x} &= \left(\gamma_1 + e_4e_5\gamma_2\right)\left(e_5i(v) + e_4\right)\left(\overline{\gamma_1} + e_4e_5\overline{\gamma_2}\right) \\ &= \gamma_1e_5i(v)\overline{\gamma_1} + (\gamma_1 + e_4e_5\gamma_2)e_4(\overline{\gamma_1} + e_4e_5\overline{\gamma_2}) \\ &= e_5\gamma_1i(v)\overline{\gamma_1} + \gamma_1e_4\overline{\gamma_1} + \gamma_1e_4e_4e_5\overline{\gamma_2} + e_4e_5\gamma_2e_4\overline{\gamma_1} \\ &= e_5\left(\gamma_1i(v)\overline{\gamma_1} + \gamma_2\overline{\gamma_1} - \gamma_1\overline{\gamma_2}\right) + e_4.\end{aligned}$$

By the above, $\gamma_1i(v)\overline{\gamma_1} + \gamma_2\overline{\gamma_1} - \gamma_1\overline{\gamma_2} \in i(\mathbb{R}^3)$. From the definition in (2), we conclude that $x \in$ Spun(3). That is, $\mathcal{C} \cap G \subseteq$ Spun(3), which in turn implies $S \cap G =$ Spun(3). □

The proof of Lemma 4.3 also implies that 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.

[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.

We define $\pi : \mathbb{R}^8 \setminus H_0 \to \mathbb{R}^7$ as $\pi(x) = \pi_8(\lambda_x x)$. That is, $\pi$ 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 $\pi_8$ 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

$$\begin{aligned} T_{ap} &= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right) T_{00} \left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right) \\ &= \left(\left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right) F_{00} \left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right)\right) \bigcap \left(\left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right) \mathcal{C} \left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right)\right) \\ &= F_{ap} \cap \mathcal{C}. \end{aligned}$$

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 $\pi$ 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 $(x_2, \ldots, x_8) \in \mathbb{R}^7$, let $x = (1, x_2, \ldots, x_8)$. Then there exists $r \in \mathbb{R}$ such that $y = rx$ is the unique point on $\mathcal{C}_+$ that satisfies $\pi(y) = (x_2, \ldots, x_8)$. That is, the restriction of $\pi$ to $\mathcal{C}_+$ is a bijection between $\mathcal{C}_+$ and $\mathbb{R}^7$. Moreover, $\pi$ 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 $\pi_7$ to $G_7$ is injective. Since $\pi_7$ 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 $\pi_7$ to $G_7$ and the restriction of $\pi$ 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 $\left(\mathbf{1} + \frac{1}{2}e_4e_5i(v)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5i(v)\right) =$

**1**. Combining this with the definition of $F_{ap}$ gives

$$\begin{aligned} F_{ap} \cap F_{bq} &= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5i(p)\right)(F_{ap} \cap F_{bq})\left(\mathbf{1} + \frac{1}{2}e_4e_5i(a)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right) \\ &= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\left(C\ell_3^0 \cap F_{(b-a)(q-p)}\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right). \end{aligned}$$

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

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

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 $\overline{\gamma}\overline{i(q-p)}i(q-p)\gamma = \|q-p\|^2\overline{\gamma}\gamma$ is equal to the coefficient of $\mathbf{1}$ in $\gamma i(b-a)\overline{i(b-a)}\overline{\gamma} = \|b-a\|^2\gamma\overline{\gamma}$. 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

$$\beta_{ap} = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\beta\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right) = \beta + \frac{1}{2}e_4e_5(i(p)\beta - \beta i(a)) \in T_{ap}.$$

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 $\beta_{ap}$ takes $b$ to $q$. Indeed, recalling that $\beta$ takes $b-a$ to $q-p$ gives

$$\begin{aligned} \beta_{ap}(e_5i(b)+e_4)\overline{\beta_{ap}} &= \left(\beta + \frac{1}{2}e_4e_5(i(p)\beta - \beta i(a))\right)(e_5i(b)+e_4)\left(\overline{\beta} + \frac{1}{2}e_4e_5(i(a)\overline{\beta} - \overline{\beta}i(p))\right) \\ &= \beta(e_5i(b)+e_4)\overline{\beta} + \frac{1}{2}e_5\left(\beta e_4e_4(i(a)\overline{\beta} - \overline{\beta}i(p)) + e_4(i(p)\beta - \beta i(a))e_4\overline{\beta}\right) \\ &= \beta(e_5i(b))\overline{\beta} + e_4 + \frac{1}{2}e_5\left(-(\beta i(a)\overline{\beta} - i(p)) + (i(p) - \beta i(a)\overline{\beta})\right) \\ &= e_5(\beta i(b-a)\overline{\beta}) + e_4 + e_5i(p) = e_5i(q-p) + e_4 + e_5i(p) = e_5i(q) + e_4. \end{aligned}$$

□

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*

$$F_{ap} \cap F_{bq} = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\beta \cdot C\ell_2^0 \cdot \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right),$$

*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 $\alpha$ and $\beta$ are valid. Let

$$N_{ap} = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\beta \cdot C\ell_2^0 \cdot \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right).$$

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

$$\begin{aligned}
\alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right) &= \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a-b+b)\right) = \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a-b)\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5i(b)\right) \\
&= \left(\alpha - \frac{1}{2}e_4e_5\alpha i(a-b)\alpha^{-1}\alpha\right)\left(\mathbf{1} - \frac{1}{2}e_4e_5i(b)\right) \\
&= \left(\mathbf{1} + \|b-a\|\frac{1}{2}e_4e_5e_3\right)\alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(b)\right). \qquad (12)
\end{aligned}$$

Similarly,

$$\begin{aligned}
\left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\beta &= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p-q+q)\right)\beta = \left(\mathbf{1} + \frac{1}{2}e_4e_5i(q)\right)\left(\mathbf{1} + \frac{1}{2}e_4e_5i(p-q)\right)\beta \\
&= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(q)\right)\beta\left(\mathbf{1} + \frac{1}{2}e_4e_5\beta^{-1}i(p-q)\beta\right) \\
&= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(q)\right)\beta\left(\mathbf{1} - \|q-p\|\frac{1}{2}e_4e_5e_3\right). \qquad (13)
\end{aligned}$$

Combining (12) and (13) gives

$$\begin{aligned}
N_{ap} &= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(p)\right)\beta \cdot C\ell_2^0 \cdot \alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(a)\right) \\
&= \left(\mathbf{1} + \frac{1}{2}e_4e_5i(q)\right)\beta\left(\mathbf{1} - \|q-p\|\frac{1}{2}e_4e_5e_3\right) \cdot C\ell_2^0 \cdot \left(\mathbf{1} + \|b-a\|\frac{1}{2}e_4e_5e_3\right)\alpha\left(\mathbf{1} - \frac{1}{2}e_4e_5i(b)\right).
\end{aligned}$$

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 $F_{ap} \cap F_{bq} \subseteq N_{ap}$. □

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 $\eta$ 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 $\eta'$ as a linear extension of the restricted $\eta$ 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

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

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 $\dim(\langle F_{ap}, F_{bq}\rangle \cap H_0) = 4 + 4 - 2 - 1 = 5$ (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. □

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. □

**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, $L_{apbq} = \eta\left(\langle F_{ap}, F_{bq}\rangle \setminus H_0\right) = \mathbb{R}^6$. □

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). □

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 [13] 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 [12, 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 $\varepsilon'$ to be sufficiently small with respect to $\varepsilon$, 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 $\mathrm{Spun}(d)$ 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 $\mathrm{Spun}(d)$ as in Lemma 4.3. This leads us to study $\mathrm{Spun}(d)$ in a more indirect way.

Recall that $\mathrm{Spun}(d)$ 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 $\mathrm{Spun}(d)$ 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 $\gamma \in \mathrm{Spin}(d)$. Then $\gamma x \gamma^{-1}$ also consists entirely of $m$-terms.*

*Proof.* Let $z \in C\ell_d^0$ and $\gamma \in \mathrm{Spin}(d)$. 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 $\gamma^{-1}$ 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 $\gamma$ 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 $\ell$-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 $\ell$-terms for any $\ell > m$.

We write $\gamma x \gamma^{-1} = \delta + \delta'$, where $\delta$ consists entirely of $m$-terms and $\delta'$ 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 $\ell$-vector terms with $\ell < m$, the first coordinate of (16) is zero. Since conjugation by $\gamma$ 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 $\delta$ and $\delta'$ 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 $x \in C\ell^0_{d-1}$ 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 $z \in Z^0_d \setminus \{0 \cdot \mathbf{1}\}$ 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 $z = z_1 + z_2 e_{d+1}e_{d+2}$ where $z_1 \in C\ell^0_d$ and $z_2 \in C\ell^1_d$. We then have

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

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 $\eta$ 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 $\pi_1$). 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 $\eta_3$ is indeed the map $\eta$ from Section 4.

We first claim that the restriction of $\pi_1$ 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 $\lambda_x$ 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 $x \in \mathrm{Spun}(d)_+$ such that $\pi_1(x) = y$.

Set

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

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 $\eta_d$ and about the structure of $\mathrm{Spun}(d)$.

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 $g/r \in \mathrm{Spin}(d)$. 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 $g/r \in \mathrm{Spin}(d)$ on $v$, it is a rotation of $\mathrm{SO}(d)$. 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 $x = e_d\left(e_d + i(u)\right)/s \in \mathrm{Spin}(d)$. 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

$$xi(u)x^{-1} = \frac{e_d\left(e_d + i(u)\right) i(u) \left(e_d + i(u)\right) e_d}{s^2} = \frac{e_d\left(i(u) + e_d\right)\left(\frac{i(u)+e_d}{2} + \frac{i(u)-e_d}{2}\right)\left(e_d + i(u)\right) e_d}{s^2}$$

$$= \frac{e_d\left(i(u) + e_d\right)^2 \left(\left(i(u) + e_d\right) - \left(i(u) - e_d\right)\right) e_d}{2s^2} = \frac{-e_d \cdot 2e_d \cdot e_d}{2} = e_d.$$

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

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

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 $z/r \in \mathrm{Spun}(d)$. By Lemma 3.2, there exist $\gamma \in \mathrm{Spin}(d)$ and $u \in \mathbb{R}^d$ such that $z/r = \gamma\left(\mathbf{1} + e_{d+2}e_{d+1}i(u)\right)$. 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 $\eta_d$ to $\mathrm{Spun}(d)_+$ 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 $g = h\left(e_di(u) - \mathbf{1}\right)$ and $g' = h'\left(e_di(u') - \mathbf{1}\right)$.

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

$$g = h\left(e_di(u) - \mathbf{1}\right) = he_di(u) - r \cdot \mathbf{1} - h_2 - h_+.$$

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

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

A symmetric argument gives

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

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 $he_di(u_*)$ and $h'e_di((u')_*)$ 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,

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

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

$$re_di(u_*) + \sum_{1\leq j<k\leq d-1} \lambda_{j,k}e_je_k(u_je_de_j + u_ke_de_k) \\ = \ell r_x e_di((u')_*) + \ell \sum_{1\leq j<k\leq d-1} \lambda_{j,k}e_je_k(u'_je_de_j + u'_ke_de_k).$$

Simplifying, we have

$$re_di(u_*) + \sum_{1\leq j<k\leq d-1} \lambda_{j,k}(-u_je_ke_d + u_ke_je_d) \\ = \ell re_di((u')_*) + \ell \sum_{1\leq j<k\leq d-1} \lambda_{j,k}(-u'_je_ke_d + u'_ke_je_d).$$

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 $1 \leq j \leq d-1$.

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

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

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 $g = g'$. □

**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 $g_2 = \sum_{1\le j<k\le d} \lambda_{j,k}e_je_k$, 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 $e_je_{d+1}e_{d+2}$ with $1 \le j \le d$. Since $x$ and $y$ have the same 2-terms, we have

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

Simplifying, we have

$$\begin{aligned} r_xe_{d+1}e_{d+2}i(u_x) + \sum_{1\le j<k\le d} \lambda_{j,k}(-u_{x,j}e_ke_{d+1}e_{d+2} + u_{x,k}e_je_{d+1}e_{d+2}) \\ = r_xe_{d+1}e_{d+2}i(u_y) + \sum_{1\le j<k\le d} \lambda_{j,k}(-u_{y,j}e_ke_{d+1}e_{d+2} + u_{y,k}e_je_{d+1}e_{d+2}). \end{aligned}$$

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 $x = y$. □

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

*Proof.* Consider two elements $x, y \in \mathrm{Spun}(d)_+$ 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 $\mathrm{Spun}(d)_+$, there is a unique $r \in \mathbb{R}$ such that $r \cdot x' \in \mathrm{Spun}(d)_+$. We thus conclude that $x = y$. □

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

**Lemma 5.8.** *Consider $r \in \mathbb{R}$ and elements $\lambda_{j,k} \in \mathbb{R}$ for every $1 \leq j < k \leq d$, 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 $1 \leq j < k \leq d-1$. 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 $1 \leq j < k \leq d-1$. We now consider the terms of the form $e_j e_d$ in $g$, and observe that these are all in $-h e_d i(u)$. Let $u_j$ denote the $j$'th coordinate of $u$. Since for every $1 \leq j \leq d-1$ 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 $u_1, \ldots, u_{d-1}$ 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 $1 \leq j < k \leq d+1$, 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 $1 \leq j < k \leq d$. We set $g = h - h e_{d+1} e_{d+2} i(u) \in J_d$, 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 $1 \leq j < k \leq d$. 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 $-h e_{d+1} e_{d+2} i(u)$. Let $u_j$ denote the $j$'th coordinate of $u$. Since for every $1 \leq j \leq d$ 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 $u_1, \ldots, u_d$ 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 $\eta_d$ 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 $\eta_d$ to $\mathrm{Spun}(d)_+$ is surjective on $\mathbb{R}^{\binom{d+1}{2}}$. □

Now that we established that the restriction of $\eta_d$ to $\mathrm{Spun}(d)_+$ is a bijection, we move to study the image of $T_{ap} \cap \mathrm{Spun}(d)_+$ under $\eta_d$. 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

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

Since $C\ell_d^0$ is contained in $Z_d^0$, we can also think of $G_d$ as contained in $Z_d^0$. 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 $\eta_d$ 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 $Z_d^0$ that are 2-terms. We can think of $\eta_d'$ as a linear extension of the restricted $\eta_d$ 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 $\eta_d$ 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 $C\ell_d^0$ 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 $\dim F_{ap} = \dim(C\ell_d^0) = 2^{d-1}$ 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 $\tau_{ap} : Z_d^0 \to Z_d^0$ 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

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

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 $\tau_{ap}$ 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 $\beta \in \mathrm{Spin}(d)$ 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 $\gamma$ is the product of two elements from $i(\mathbb{S}^{d-1})$, we have that $\gamma \in \mathrm{Spin}(d)$, which in turn implies that $\alpha \in \mathrm{Spin}(d)$. We get that

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

We can thus use these $\alpha$ and $\beta$ 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 $\beta \in \mathrm{Spin}(d)$ 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 $\gamma = \frac{1}{\|e_d + B\|} e_d (e_d + B)$ and $\alpha = \gamma\beta^{-1}$. Since $\gamma$ is the product of two elements from $i(\mathbb{S}^{d-1})$, we have that $\gamma \in \mathrm{Spin}(d)$, which in turn implies that $\alpha \in \mathrm{Spin}(d)$. 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 $\alpha$ and $\beta$ in (18).

Let

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

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 $\mathrm{Spun}(d)$, we have that $x \in \mathrm{Spun}(d)$. Lemma 3.6 implies $T_{ap} \cap T_{bq} = F_{ap} \cap F_{bq} \cap \mathrm{Spun}(d)$, so $x \in T_{ap} \cap T_{bq}$. We conclude that $T_{ap} \cap T_{bq} \not\subseteq H_0$, which completes the proof. □

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

*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 $\dim ((L_{ap} - v) \cap (L_{bq} - v)) = \binom{d-1}{2}$. By Lemma 5.13,

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

By the extension of Lemma 4.5 to $\mathbb{R}^d$, we have that $\dim (F_{ap} \cap F_{bq}) = \dim(C\ell_{d-1}) = 2^{d-2}$. 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 $\dim(F_{ap} \cap F_{bq} \cap H_0) = 2^{d-2} - 1$. It remains to show that $\dim(F_{ap} \cap F_{bq} \cap H_0 \cap \ker(\eta'_d)) = 2^{d-2} - \binom{d-1}{2} - 1$.

For an arbitrary $\beta \in \mathrm{Spin}(d)$ 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 $\gamma = \frac{1}{\|e_n + B\|} e_n (e_n + B)$ and let $\alpha = \gamma \beta^{-1}$. Since $\gamma$ is the product of two elements from $i(\mathbb{S}^{d-1})$, we have that $\gamma \in \mathrm{Spin}(d)$, which in turn implies that $\alpha \in \mathrm{Spin}(d)$. 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

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

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

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

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

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 $f \in Z^0_d$ 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 $\tau^{-1}_{ap}(g)$ 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 [13] 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 [12, 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 $\varepsilon'$ to be sufficiently small with respect to $\varepsilon$, 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 $\eta_d(T_{ap} \cap \mathrm{Spun}(d)_+)$ 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, $\tau_{ap}$ 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]

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

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

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

□

[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 $\mathbb{R}^{2^d}$.

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 $v_1y_1 + \ldots + v_{2^d}y_{2^d} = 0$. Let $S_{ap}$ be the system of $2^{d-1}$ homogeneous linear equations 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 $\tau_{ap}^{-1}$ 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, $\gamma$ 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 $((\tau_{ap}^{-1})^t \circ (e_j e_{d+1}e_{d+2})^*)^*$ 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 $(\tau_{ap}^{-1})^t \circ ((e_j e_{d+1}e_{d+2})^*)$ for $1 \leq j \leq d$. It follows that the equations of $S'_{00}$ are obtained

[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.

from those defining $S'_{ap}$ by applying $\tau^t_{ap}$ to the coefficient vectors. By the second paragraph of this proof, for every $v \in F'_{ap}$ we have that $\tau^{-1}_{ap}(v) \in F'_{00}$.

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 $e_j e_{d+1} e_{d+2}$ (where $1 \leq j \leq d$). For $v \in F'_{ap} \setminus H_0$, we obtain that $\tau^{-1}_{ap}(v)$ contains no terms of the form $e_j e_{d+1} e_{d+2}$. By Lemmas 5.6 and 5.9, there is a unique $x \in J_d$ with the property that $x - \tau^{-1}_{ap}(v)$ contains no 0-term and no 2-terms. Note that $x$ also contains no terms of the form $e_j e_{d+1} e_{d+2}$, so Lemma 5.8 implies that $x \in G_d$. Since $x \in C\ell^0_d$, we have that $\tau_{ap}(x) \in \tau_{ap}\left(C\ell^0_d\right)$. By Lemma 5.3, the expression $\tau_{ap}\left(x - \tau^{-1}_{ap}(v)\right)$ also contains no 0-term and no 2-terms, so $\eta_d(\tau(x)) = \eta_d(v)$. That is, there exists $\tau_{ap}(x) \in \tau_{ap}\left(C\ell^0_d\right)$ such that $\eta_d(\tau_{ap}(x)) = \eta_d(v)$. Since $v \notin H_0$, we have that $\tau^{-1}_{ap}(v) \notin H_0$, which in turn implies that $x \notin H_0$ and that $\tau(x) \notin H_0$. This implies that $\eta_d(F'_{ap} \setminus H_0) \subseteq \eta_d(\tau_{ap}(C\ell^0_d) \setminus H_0)$ and completes the proof. □

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 $(\tau^{-1}_{ap})^t \circ (e_j e_{d+1} e_{d+2})^*$ for $1 \leq j \leq d$. If $e_j e_{d+1} e_{d+2}$ is the $k$'th element in our ordering of the basis of $Z^0_d$, then $(\tau^{-1}_{ap})^t \circ (e_j e_{d+1} e_{d+2})^*$ 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 $\tau^{-1}_{ap}$. To get this row, we apply $\tau^{-1}_{ap}$ to the basis vectors of $Z^0_d$ and then keep the coefficient of $e_j e_{d+1} e_{d+2}$ (recall that $\tau^{-1}_{ap}$ is defined in (24)). The only basis vectors of $Z^0_d$ for which this coefficient is nonzero are $\mathbf{1}$ and 2-terms involving $e_j$. Repeating this process for every $1 \leq j \leq d$ 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 $\pi'$, we get that $\eta_d(F'_{ap})$ is the solution set of (26). □

# 7 Properties of the 2-flats in $\mathbb{R}^5$

In this section we study the 2-flats in $\mathbb{R}^5$ that are obtained from our reduction of the three-dimensional distinct distances problem. In particular, we show how one can bound the number of

2-flats contained in constant-degree three- and four-dimensional varieties. We also show how one can bound the number of 2-flats that have a one-dimensional intersection with a constant-degree two-dimensional variety. Deriving these results requires several definitions and tools from Algebraic Geometry, and these are described in Section 7.1.

## 7.1 Algebraic Geometry preliminaries

In the following, $\mathbb{F}$ could be taken to be either $\mathbb{C}$ or $\mathbb{R}$. The *variety* defined by the polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_d]$ is

$$\mathbf{V}(f_1, \ldots, f_k) = \left\{(a_1, \ldots, a_d) \in \mathbb{F}^d : f_j(a_1, \ldots, a_d) = 0 \text{ for all } 1 \leq j \leq k\right\}.$$

There are several non-equivalent definitions for the degree of a variety in $\mathbb{R}^d$. For our purposes, we define the degree of a variety $U \subset \mathbb{R}^d$ as

$$\min_{\substack{f_1,\ldots,f_k \in \mathbb{R}[x_1,\ldots,x_d] \\ \mathbf{V}(f_1,\ldots,f_k)=U}} \max_{1 \leq i \leq k} \deg f_i.$$

That is, the degree of $U$ is the minimum integer $D$ such that $U$ can be defined with a finite set of polynomials of degree at most $D$.

A variety $U \subseteq \mathbb{F}^d$ is *reducible* if there exist two proper subvarieties $U', U'' \subset U$ such that $U = U' \bigcup U''$. Otherwise, $U$ is *irreducible*. An *irreducible component* of $U$ is an irreducible variety that is contained in $U$, and not contained in any other irreducible subvariety of $U$.

**Lemma 7.1.** *Let $U \subset \mathbb{R}^d$ be a variety of degree $k$. Then the number of irreducible components of $U$ is $O_{d,k}(1)$.*

Intuitively, we say that a variety $U \subset \mathbb{R}^d$ has dimension $k$ if there exists a subset of $U$ that is homeomorphic to the open $k$-dimensional cube, but no subset of $U$ is homeomorphic to an open cube of a larger dimension. For more information about varieties in $\mathbb{R}^d$ and a more precise definition of dimension, see for example [2].

**Singular points, regular points, and tangent flats.** The *ideal* of a variety $U \subseteq \mathbb{R}^d$, denoted $\mathbf{I}(U)$, is the set of polynomials in $\mathbb{R}[x_1, \ldots, x_d]$ that vanish on every point of $U$. We say that a set of polynomials $f_1, \ldots, f_\ell \in \mathbb{R}[x_1, \ldots, x_d]$ *generate* $\mathbf{I}(U)$ if every element of $\mathbf{I}(U)$ can be written as $\sum_{j=1}^{\ell} f_j g_j$ for some $g_1, \ldots, g_\ell \in \mathbb{R}[x_1, \ldots, x_d]$. We also write $\langle f_1, \ldots, f_\ell \rangle = \mathbf{I}(U)$ to state that $f_1, \ldots, f_\ell$ generate $\mathbf{I}(U)$.

The *Jacobian matrix* of a set of polynomials $f_1, \ldots, f_k \in \mathbb{R}[x_1, \ldots, x_d]$ is

$$\mathbf{J}_{f_1,\ldots,f_k} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \ldots & \frac{\partial f_1}{\partial x_d} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \ldots & \frac{\partial f_2}{\partial x_d} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{\partial f_k}{\partial x_1} & \frac{\partial f_k}{\partial x_2} & \ldots & \frac{\partial f_k}{\partial x_d} \end{pmatrix}$$

Consider a variety $U \subset \mathbb{R}^d$ of dimension $k$, and let $f_1, \ldots, f_\ell \in \mathbb{R}[x_1, \ldots, x_d]$ satisfy $\langle f_1, \ldots, f_\ell \rangle = \mathbf{I}(U)$. We say that $p \in U$ is a *singular* point of $U$ if $\operatorname{rank} \mathbf{J}(p) < d - k$. A point of $U$ that is not singular is said to be a *regular* point of $U$. We denote the set of singular points of $U$ as $U_{\text{sing}}$, and the set of regular points of $U$ as $U_{\text{reg}}$. A $k$-dimensional variety has a unique well-defined tangent $k$-flat at every regular point. We denote the tangent $k$-flat at $p \in U$ as $T_p U$, and think of it as a linear subspace (that is, as incident to the origin). At singular points of a real variety, a unique well-defined tangent flat may or may not exist.

**Theorem 7.2.** *Let $U \subset \mathbb{R}^d$ be a variety of degree $k$ and dimension $d'$. Then $U_{sing}$ is a variety of dimension smaller than $d'$ and of degree $O_{k,d}(1)$.*

References for the above claims and additional information can be found, for example, in [2].

**Complexification.** Given a variety $U \subset \mathbb{R}^d$, the *complexification* $U^* \subset \mathbb{C}^d$ of $U$ is the smallest complex variety that contains $U$, in the sense that any other complex variety that contains $U$ also contains $U^*$ (for example, see [9, 16]). As shown in [16, Lemma 6], such a complexification always exists, and $U$ is precisely the set of real points of $U^*$.

As shown in [16, Section 10], there is a bijection between the irreducible components of $U$ and the irreducible components of $U^*$, such that each real component is the real part of its corresponding complex component. In particular, the complexification of an irreducible variety is irreducible. The real dimension of a real irreducible component in $\mathbb{R}^d$ is equal to the complex dimension of the corresponding complex component in $\mathbb{C}^d$.

**Constructible sets, semi-algebraic sets, and projections.** As before, $\mathbb{F}$ could be taken to be either $\mathbb{C}$ or $\mathbb{R}$. If $U \subset \mathbb{F}^d$ is a set, the *Zariski closure* $\overline{U}$ is the smallest variety in $\mathbb{F}^d$ that contains $U$. A set $X \subset \mathbb{F}^d$ is *constructible* if there exist non-empty varieties $X_1, \ldots, X_\ell \subset \mathbb{F}^d$ such that $\dim X_{j+1} < \dim X_j$ for every $1 \leq j < \ell$ and

$$X = \Big( ((X_1 \backslash X_2) \cup X_3) \backslash X_4 \ldots \Big). \tag{27}$$

We define $\dim(X) = \dim(\overline{X}) = \dim(X_1)$. We define the *complexity* of $X$ to be $\min(\deg(X_1) + \deg(X_2) + \ldots + \deg(X_\ell))$, where the minimum is taken over all representations of $X$ of the form (27). This definition is not standard. However, since we are interested only in constructible sets of bounded complexity, any reasonable definition of complexity would work equally well. For further details, see for example [8, Chapter 3].

A *semi-algebraic set* in $\mathbb{R}^d$ is the set of points in $\mathbb{R}^d$ that satisfy a given finite Boolean combination of polynomial equations and inequalities in $d$ coordinates. Every constructible set in $\mathbb{R}^d$ is semi-algebraic. On the other hand, a semicircle in $\mathbb{R}^2$ is semi-algebraic but not constructible.

Let $S \subset \mathbb{R}^d$ be a semi-algebraic set defined by a Boolean combination of equations and inequalities involving the polynomials $f_1, \ldots, f_k \in \mathbb{R}[x_1, \ldots, x_d]$ (that is, the $j$'th equation or inequality has zero on one side and $f_j$ on the other). The dimension of $S$ is the dimension of the real variety $\overline{S}$. The complexity of $S$ is $\min\{\deg f_1 + \cdots + \deg f_k\}$, where the minimum is taken over all Boolean combinations that define $S$. Note that the degree of the variety $\overline{S}$ is at most the complexity of $S$.

One can also include the quantifiers $\forall$ and $\exists$ in the definition of a semi-algebraic set, each quantifying an additional variable that is not a coordinate of the points in the set. For every definition of a semi-algebraic set using quantifiers, there exists a definition that does not use quantifiers. For example, the formula $\forall t : (t > 0) \vee (x + y > t)$ defines an open half-plane in $\mathbb{R}^2$, which can easily be defined without the $\forall$ quantifier. In the above definition of the complexity, one may only use definitions of $S$ that do not include such quantifiers. For the following, see for example [1, Section 11.3].

**Lemma 7.3.** *Let $S \subset \mathbb{R}^d$ be a semi-algebraic set using $k$ quantified variables, and $s$ polynomials of degree at most $D$. Then $S$ is of complexity $O_{k,s,D,d}(1)$.*

Both in $\mathbb{R}^d$ and in $\mathbb{C}^d$, the projection of a variety is not necessarily a variety. In $\mathbb{R}^d$, the projection of a constructible set is not necessarily constructible. The following result states properties that are satisfied by every projection. For part (a), see for example [8, Theorem 3.16] (this reference only says that the projection of a constructible set is constructible. However, the proof is constructive

and thus gives us a bound on the complexity of the projection.) Part (b) is implied by Lemma 7.3, noting that the projection of a semi-algebraic set can be obtained by adding $\exists$ quantifiers to its definition.

**Theorem 7.4.**
*(a) Let $X \subset \mathbb{C}^d$ be a constructible set of dimension $d'$ and complexity $k$. Let $\pi : \mathbb{R}^d \to \mathbb{R}^e$ be a projection on $e$ out of the $d$ coordinates of $\mathbb{R}^d$. Then $\pi(X)$ is a constructible set of dimension at most $d'$ and of degree $O_{k,d}(1)$.*
*(b) Let $U \subset \mathbb{R}^d$ be a semi-algebraic set of dimension $d'$ and complexity $k$. Let $\pi : \mathbb{R}^d \to \mathbb{R}^e$ be a projection on $e$ out of the $d$ coordinates of $\mathbb{R}^d$. Then $\overline{\pi(U)}$ is a variety of dimension at most $d'$ and of degree $O_{k,d}(1)$.*

For $d > d'$, let $X \subset \mathbb{C}^d$ be a constructible set and let $Y \subset \mathbb{C}^{d'}$ be an irreducible variety. Let $\pi \colon \mathbb{C}^d \to \mathbb{C}^{d'}$ be a projection onto $d'$ coordinates. We say that $\pi \colon X \to Y$ is *dominant* if $\overline{\pi(X)} = Y$. The following is a corollary of Chevalley's upper semi-continuity theorem (for example, see [8, Corollary 11.13] and the paragraph following it; for the claim that the set is constructible, see also [8, Theorem 3.16]).

**Theorem 7.5.** *Let $X \subset \mathbb{C}^d$ and $Y \subset \mathbb{C}^{d'}$ be irreducible varieties of degrees at most $k$, and suppose $\pi : X \to Y$ is dominant. Then exists a variety $Y' \subset \mathbb{C}^d$ of degree $O_k(1)$ such that $\dim Y' < \dim Y$ and for every $y \in Y \setminus Y'$ we have that $\pi^{-1}(y)$ is a constructible set of dimension $\dim X - \dim Y$ and degree $O_{k,d}(1)$.*

We require a real variant of Theorem 7.5.

**Corollary 7.6.** *Let $U$ be a variety of dimension $d$ in $\mathbb{R}^6$, let $\pi : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the first three coordinates, and let $U_3 = \overline{\pi(U)}$ be of dimension $d_3$. Then there exists a variety $W \subset \mathbb{R}^3$ of degree $O_k(1)$ such that $\dim W < d_3$ and for every $u \in U_3 \setminus W$ we have that $\pi^{-1}(u)$ is a constructible set of dimension at most $d - d_3$ and degree $O_k(1)$.*

*Proof.* Consider the complexification $U^*$ of $U$ and the complexification $U_3^*$ of $U_3$. Note that $U^*$ is of dimension $d$ and that $U_3^*$ is of dimension $d_3$. We extend the projection $\pi : \mathbb{R}^6 \to \mathbb{R}^3$ to $\pi : \mathbb{C}^6 \to \mathbb{C}^3$. As before, this is the projection on the first three coordinates.

Set $U' = \overline{\pi(U^*)}$. By Theorem 7.4(a), the variety $U'$ is of degree $O_k(1)$. Since $U_3^*$ is the smallest complex variety containing $U_3$, we have that $U_3^* \subseteq U'$. Consider the cylindrical variety $C = \pi^{-1}(U_3^*) \subset \mathbb{C}^6$, and note that $U$ is contained in the real part of $C$. Since $U^*$ is the smallest variety in $\mathbb{C}^6$ that contains $U$, we have that $U^* \subseteq C$. This in turn implies that $U' \subseteq U_3^*$, so $U' = U_3^*$. In particular, $\dim U' = d_3$.

By Theorem 7.5, there exists a variety $W^* \subset \mathbb{C}^3$ of degree $O_k(1)$ such that $\dim W^* < d_3$ and for every $u \in U' \setminus W^*$ we have that $\pi^{-1}(u)$ is a constructible set of dimension $d - d_3$ and degree $O_k(1)$. We set $W \subset \mathbb{R}^3$ to be the real part of $W^*$, and note that $\dim W < d_3$. Since $(U_3 \setminus W) \subset (U' \setminus W^*)$, for every $u \in U_3 \setminus W$ we have that $\pi^{-1}(u) \subset \mathbb{R}^6$ is a constructible of dimension at most $d - d_3$ and degree $O_k(1)$. □

## 7.2 Flats in $\mathbb{R}^5$.

Theorem 6.1 implies the following for the case of distinct distances in $\mathbb{R}^3$. Given two points $a = (a_1, a_2, a_3)$ and $p = (p_1, p_2, p_3)$ in $\mathbb{R}^3$, the corresponding 3-flat $L_{ap} \subset \mathbb{R}^6$ is defined by

$$\begin{aligned} -(a_1 + p_1)x_2 - (a_2 + p_2)x_3 + 2x_6 &= a_3 - p_3, \\ -(a_1 + p_1)x_1 + (a_3 + p_3)x_3 + 2x_5 &= a_2 - p_2, \\ (a_2 + p_2)x_1 + (a_3 + p_3)x_2 + 2x_4 &= a_1 - p_1. \end{aligned} \tag{28}$$

Note that $\{L_{ap} : a, p \in \mathbb{R}^3\}$ is a six-dimensional family of 3-flats in $\mathbb{R}^6$.

Let $\mathcal{P}$ be a set of $n$ points in $\mathbb{R}^3$, and let $H$ be a hyperplane in $\mathbb{R}^6$, chosen generically with respect to $\mathcal{P}$. For $a, p \in \mathbb{R}^3$ we write $F_{ap} = L_{ap} \cap H$. We consider the sets

$$\mathcal{F} = \{F_{ap} : a, p \in \mathbb{R}^3\} \qquad \text{and} \qquad \mathcal{F}_{\mathcal{P}} = \{F_{ap} : a, p \in \mathcal{P}\}.$$

Since $H$ is chosen generically, $\mathcal{F}_{\mathcal{P}}$ is a set of $n^2$ distinct 2-flats in $H$. We think of $H$ as $\mathbb{R}^5$, so $\mathcal{F}_{\mathcal{P}}$ becomes a set of 2-flats in $\mathbb{R}^5$. As shown in Section 4, every pair of flats in $\mathcal{F}_{\mathcal{P}}$ intersect in at most one point.

**Theorem 7.7.** *Let $U$ be an irreducible three-dimensional variety in $\mathbb{R}^5$ of degree $k$. Then either $U$ contains $O_k\left(n^{2/3}\right)$ flats of $\mathcal{F}_{\mathcal{P}}$ or there exists a curve in $\mathbb{R}^3$ of degree $O_k(1)$ that contains $\Omega_k\left(n^{2/3}\right)$ points of $\mathcal{P}$.*

It is not difficult to show that $n^{2/3}$ points on a constant-degree curve in $\mathbb{R}^3$ span $\Omega\left(n^{2/3}\right)$ distinct distances. This is exactly the conjectured number of distances in $\mathbb{R}^3$, so we may assume that no constant-degree curve in $\mathbb{R}^3$ contains $n^{2/3}$ points of $\mathcal{P}$. Then, Theorem 7.7 implies that every constant-degree three-dimensional variety in $\mathbb{R}^5$ contains $O(n^{2/3})$ flats of $\mathcal{F}_{\mathcal{P}}$.

*Proof of Theorem 7.7.* For any $a, p \in \mathbb{R}^3$, by (28) we have the parametrization

$$L_{ap} = \Big\{(s, t, r, \big(a_1 - p_1 - (a_2+p_2)s - (a_3 + p_3)t\big)/2, \big(a_2 - p_2 + (a_1 + p_1)s - (a_3 + p_3)r\big)/2, \\ \big(a_3 - p_3 + (a_1 + p_1)t + (a_2 + p_2)r\big)/2) \in \mathbb{R}^6 \ : \ s, t, r \in \mathbb{R}\Big\}. \quad (29)$$

To parameterize $L_{ap} \cap H$, we isolate $x_3$ in the linear equation defining $H$ and use this to eliminate the parameter $r$ (since $H$ is generic, its defining equation contains $x_3$). This parametrization of $L_{ap} \cap H$ consists of five linear functions in the two variables $s, t \in \mathbb{R}$, with coefficients that are polynomials of degree at most two in the coordinates of $a$ and $p$.

We identify $H$ with $\mathbb{R}^5$. Equivalently, let $\pi_H : H \to \mathbb{R}^5$ be a the map that takes $H$ to $\mathbb{R}^5$. Since $\pi_H$ can be seen as a translation followed by a rotation and a projection, we can write $\pi_H$ as five linear polynomials in $x_1, \ldots, x_6$. Combining this with the above parametrization, we obtain a parametrization of $F_{ap} = \pi_H(L_{ap} \cap H)$ using five linear functions in the two variables $s, t \in \mathbb{R}$ and coefficients that are polynomials of degree at most two in the coordinates of $a$ and $p$.

Let $f \in \mathbb{R}[x_1, \ldots, x_5]$ be a polynomial of degree $2k$ such that $\mathbf{V}(f) = U$ (if $U$ is defined as $\mathbf{V}(f_1, \ldots, f_m)$ where each $f_j$ is of degree at most $k$, then we take $f = f_1^2 + \cdots + f_m^2$). We think of $f\,|_{\pi_H(L_{ap} \cap H)}$ as a polynomial of degree at most $2k$ in $\mathbb{R}[s, t]$ and coefficients that depend on the coordinates of $a$ and $p$. Note that $F_{ap} \subset U$ if and only if $f|_{\pi_H(L_{ap} \cap H)}$ is identically zero. That is, if and only if the coefficient of every monomial of $f|_{\pi_H(L_{ap} \cap H)}$ is zero. There are $O_k(1)$ such monomials, and the coefficient of each is a polynomial of degree at most $4k$ in the coordinates of $a$ and $p$. This implies that the set

$$\mathcal{F}_U = \big\{(a, p) \in \mathbb{R}^6 : \ F_{ap} \subset U\big\}$$

is a variety of degree $O_k(1)$. We use the notation $\mathcal{F}_U$ to refer both to the above set of points in $\mathbb{R}^6$ and to the set of corresponding 2-flats in $\mathbb{R}^5$.

Let $u$ be a regular point of $U$, and let $F_{ap}, F_{a'p'} \subset U$ be 2-flats of $\mathcal{F}$ incident to $u$. Since any pair of 2-flats of $\mathcal{F}$ intersect in at most one point, we have $F_{ap} \cap F_{a'p'} = \{u\}$, so $T_u F_{ap}$ and $T_u F_{a'p'}$ span a 4-flat in $\mathbb{R}^5$. This is impossible, since both $T_u F_{ap}$ and $T_u F_{a'p'}$ are contained in the 3-flat $T_u U$.

This contradiction implies that every regular point of $U$ is incident to at most one 2-flat of $\mathcal{F}_U$. By Theorem 7.2, the set of singular points $U_{\text{sing}}$ is a two-dimensional variety of degree $O_k(1)$. Thus, the number of 2-flats of $\mathcal{F}$ contained in $U_{\text{sing}}$ is $O_k(1)$, and in particular there are $O_k(1)$ flats of $\mathcal{F}_\mathcal{P}$ in $U_{\text{sing}}$. Every 2-flat of $\mathcal{F}_\mathcal{P}$ that is not contained in $U_{\text{sing}}$ intersects $U_{\text{sing}}$ in a variety of dimension at most one. That is, excluding $O_k(1)$ flats, every flat of $\mathcal{F}_U$ intersects $U_{\text{reg}}$ in a constructible set of dimension two. If $\mathcal{F}_U$ is of dimension at least two then $U$ contains a two-dimensional union of disjoint two-dimensional constructible sets, which in turn implies that $U$ is of dimension at least four. This contradicts the assumption that $U$ is three-dimensional, so $\mathcal{F}_U$ is of dimension at most one.

Let $\pi_1 : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the first three coordinates and let $\pi_2 : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the last three coordinates. That is, for points $a, p \in \mathbb{R}^3$ we have $\pi_1(a,p) = a$ and $\pi_2(a,p) = p$. By Theorem 7.4(b), the variety $\gamma_1 = \overline{\pi_1(\mathcal{F}_U)} \subset \mathbb{R}^3$ is of degree $O_k(1)$ and of dimension at most one. We symmetrically define $\gamma_2 = \pi_2(\mathcal{F}_U)$.

Set $\mathcal{P}_1 = \mathcal{P} \cap \gamma_1$ and $\mathcal{P}_2 = \mathcal{P} \cap \gamma_2$. If $|\mathcal{P}_1| = \Omega\left(n^{2/3}\right)$ then we are done, since we found a constant-degree curve in $\mathbb{R}^2$ containing many points of $\mathcal{P}$. We may thus assume that $|\mathcal{P}_1| = O\left(n^{2/3}\right)$, and symmetrically that $|\mathcal{P}_2| = O\left(n^{2/3}\right)$. If $\gamma_1$ is of dimension zero, then by Lemma 7.1 it is a set of $O_k(1)$ points. Since $|\mathcal{P}_2| = O\left(n^{2/3}\right)$, we get that $O_k\left(n^{2/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ are contained in $U$. This completes the proof, so we may assume that $\gamma_1$ is of dimension one.

By Corollary 7.6, excluding $O_k(1)$ exceptional points, for every $a \in \gamma_1$ there are $O_k(1)$ points $w \in \mathcal{F}_U$ such that $\pi_1(w) = a$. Since $|\mathcal{P}_2| = O\left(n^{2/3}\right)$, the exceptional points correspond to $O_k\left(n^{2/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ in $U$. Since $|\mathcal{P}_1| = O\left(n^{2/3}\right)$, the non-exceptional points also correspond to $O_k\left(n^{2/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ in $U$. We conclude that $|\mathcal{P}^2 \cap \mathcal{F}_U| = O_k\left(n^{2/3}\right)$, which completes the proof. □

We now study the number of 2-flats of $\mathcal{F}_\mathcal{P}$ in a four-dimensional constant-degree variety in $\mathbb{R}^5$.

**Theorem 7.8.** *Let $\mathcal{P}$ be a set of $n$ points in $\mathbb{R}^3$ and let $U$ be an irreducible four-dimensional variety in $\mathbb{R}^5$ of degree $k$. Then either $U$ contains $O_k\left(n^{4/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ or there exists a surface in $\mathbb{R}^3$ that contains $\Omega_k\left(n^{2/3}\right)$ points of $\mathcal{P}$.*

*Proof.* The case where $U$ is a hyperplane was already handled in Section 3, so we may assume that $U$ is not a hyperplane. We begin by imitating the proof of Theorem 7.7. As in that proof, we define

$$\mathcal{F}_U = \left\{(a,p) \in \mathbb{R}^6 : \ F_{ap} \subset U\right\},$$

and note that $\mathcal{F}_U$ is a variety of degree $O_k(1)$.

By Theorem 7.2, the set of singular points $U_{\text{sing}}$ is a three-dimensional variety of degree $O_k(1)$. By Lemma 7.1, the set $U_{\text{sing}}$ consists of $O_k(1)$ irreducible components. We apply Theorem 7.7 to each of these components, obtaining that either there exists a one-dimensional variety containing $\Omega\left(n^{2/3}\right)$ points of $\mathcal{P}$, or that the total number of flats from $\mathcal{F}_U$ contained in $U_{\text{sing}}$ is $O\left(n^{2/3}\right)$. We may assume that we are in the latter case, since otherwise we are done.

Let $w$ be a regular point of $U$, and let $\mathcal{F}_w$ be a set of 2-flats of $\mathcal{F}$ that are contained in $U$ and incident to $w$. Note that for every $F_{ap} \in \mathcal{F}_w$ we have $F_{ap} \in U \cap (w + T_w U)$. Since $U$ is not a hyperplane, the intersection $C = U \cap (w + T_w U)$ is a variety of degree at most $k$ and dimension at most three. Since every pair of 2-flats of $\mathcal{F}_w$ intersect in at most one point, every point of $C \setminus \{w\}$ is incident to at most one such flat. It is not difficult to verify that the points in $\mathcal{F}_U$ that correspond to flats of $\mathcal{F}_w$ form a variety. If this variety is of dimension at least two, then $C$ contains a two-dimensional family of 2-flats that intersect only at $w$, so $\dim C = 4$. This contradicts the above claim that $\dim C \leq 3$, so the points of $\mathcal{F}_U$ that correspond to 2-flats in $\mathcal{F}_w$ form a subvariety of $\mathcal{F}_U$ of dimension at most one.

Every 2-flat of $\mathcal{F}_U$ that is not contained in $U_{\text{sing}}$ intersects $U_{\text{reg}}$ in a constructible set of degree $O_k(1)$ and dimension two. Since $U$ is four-dimensional and every point of $U_{\text{reg}}$ is incident to a family of 2-flats of dimension at most one, we conclude that $\mathcal{F}_U$ is of dimension at most three.

Let $\pi_1 : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the first three coordinates and let $\pi_2 : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the last three coordinates. As in the proof of Theorem 7.7, we set $\gamma_1 = \overline{\pi_1(\mathcal{F}_U)}$ and $\gamma_2 = \overline{\pi_2(\mathcal{F}_U)}$. These are two varieties of degree $O_k(1)$ and dimension at most three. We partition the rest of the analysis according to the dimension of $\gamma_1$.

If $\dim \gamma_1 = 0$ then by Lemma 7.1 it consists of $O_k(1)$ points. Each such point can participate in at most $n$ points of $\mathcal{P}^2 \cap \mathcal{F}_\mathcal{P}$, and this sums up to a total of $O_k(n)$ flats of $\mathcal{F}_\mathcal{P}$ in $U$.

If $\dim \gamma_1 = 1$ then we may assume that $\gamma_1$ contains $O\left(n^{2/3}\right)$ points of $\mathcal{P}$, since otherwise we are done. By Corollary 7.6, excluding $O_k(1)$ exceptional points, for every $a \in \gamma_1$ the set of points $w \in \mathcal{F}_U$ satisfying $\pi_1(w) = a$ is contained in a variety of dimension two and of degree $O_k(1)$. Since the set of exceptional points is zero-dimensional, it can be handled as in the case of $\dim \gamma_1 = 0$. Consider a non-exceptional point $a \in \gamma_1$ and set $\gamma_a = \overline{\pi_2(\pi_1^{-1}(a))}$. Note that $\gamma_a \subset \mathbb{R}^3$ is a variety of degree $O_k(1)$ and dimension at most two. If $|\gamma_a \cap \mathcal{P}| = \Omega\left(n^{2/3}\right)$ then we are done. We may thus assume that every non-exceptional point $a \in \gamma_1 \cap \mathcal{P}$ satisfies $|\gamma_a \cap \mathcal{P}| = O\left(n^{2/3}\right)$. This gives a total of $O_k\left(n^{4/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ in $U$.

If $\dim \gamma_1 = 2$ then we may assume that $\gamma_1$ contains $O\left(n^{2/3}\right)$ points of $\mathcal{P}$, since otherwise we are done. By Corollary 7.6, there exists a variety $W \subset \mathbb{R}^3$ of dimension at most one and degree $O_k(1)$ such that for every $a \in \gamma_1 \setminus W$ we have that $\pi^{-1}(a)$ is a constructible set of dimension at most one and degree $O_k(1)$. Since $\dim W \leq 1$, points on $W$ can be handled as in the case of $\dim \gamma_1 = 1$. For a point $a \in \gamma_1 \setminus W$ we set $\gamma_a = \overline{\pi_2(\pi_1^{-1}(a))}$. Note that $\gamma_a \subset \mathbb{R}^3$ is a variety of degree $O_k(1)$ and of dimension at most one. If $|\gamma_a \cap \mathcal{P}| = \Omega\left(n^{2/3}\right)$ then we are done. We may thus assume that every non-exceptional point $a \in \gamma_1 \cap \mathcal{P}$ satisfies $|\gamma_a \cap \mathcal{P}| = O\left(n^{2/3}\right)$. This gives a total of $O_k\left(n^{4/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ in $U$.

Finally, consider the case where $\dim \gamma_1 = 3$. By Corollary 7.6, there exists a variety $W \subset \mathbb{R}^3$ of dimension at most two and degree $O_k(1)$ such that for every $a \in \gamma_1 \setminus W$ we have that $\pi^{-1}(a)$ is a set of $O_k(1)$ points. Since $\dim W \leq 2$, it can be handled as in the cases of $\dim \gamma_1 \leq 2$. For every non-exceptional $a \in \gamma_1$, we have that $\mathcal{F}_U$ contains $O_k(1)$ points of $\{a\} \times \mathcal{P}$. By summing this over every $a \in \mathcal{P} \setminus W$ we get a total of $O_k\left(n^{4/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ in $U$. □

We conclude this section by studying the number of 2-flats of $\mathcal{F}_\mathcal{P}$ that have a one-dimensional intersection with a given two-dimensional variety.

**Theorem 7.9.** *Let $\mathcal{P}$ be a set of $n$ points in $\mathbb{R}^3$ and let $U$ be an irreducible two-dimensional variety in $\mathbb{R}^5$ of degree $k$. Then either $U$ has a one-dimensional intersection with $O_k\left(n^{4/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ or there exists a two dimensional variety of degree $O_k(1)$ in $\mathbb{R}^3$ that contains $\Omega_k\left(n^{2/3}\right)$ points of $\mathcal{P}$.*

*Proof.* Set

$$\mathcal{F}_U = \left\{(a,p) \in \mathbb{R}^6 : \ \dim(F_{ap} \cap U) = 1\right\}.$$

By Lemma 7.1, if a 2-flat in $\mathbb{R}^5$ has a zero-dimensional intersection with $U$, then this intersection consists of $O_k(1)$ points. Denote this maximum number of intersection points as $\alpha_k$. A 2-flat in $\mathbb{R}^5$ intersects $U$ in a variety of dimension at least one if and only if this intersection consists of at least $\alpha_k + 1$ points. That is, $(a,p) \in \mathcal{F}_U$ if and only if $F_{ap} \neq U$ and there exist $\alpha_k + 1$ distinct points of $\mathbb{R}^5$ that are contained in $U \cap F_{ap}$. This is a semi-algebraic condition, so $\mathcal{F}_U$ is semi-algebraic. By Lemma 7.3, the complexity of $\mathcal{F}_U$ is $O_k(1)$.

By Theorem 7.2, the set of singular points $U_{\text{sing}}$ is a one-dimensional variety of degree $O_k(1)$. Thus, for a 2-flat to have a one-dimensional intersection with $U_{\text{sing}}$, the 2-flat must contain a one-dimensional component of $U_{\text{sing}}$. Since any pair of 2-flats of $\mathcal{F}$ intersect in at most one point, the number of 2-flats of $\mathcal{F}$ that have a one-dimensional intersection with $U_{\text{sing}}$ is $O_k(1)$.

Let $w$ be a regular point of $U$, and let $\mathcal{F}_w$ be a set of 2-flats of $\mathcal{F}_U$ such that $w$ is contained in a one-dimensional component of their intersection with $U$. Note that for every $F_{ap} \in \mathcal{F}_w$ we have that $F_{ap} \cap (w + T_w U)$ is a line (or equal to $F_{ap}$). Since every pair of 2-flats of $\mathcal{F}_w$ intersect in at most one point, every point of $(w + T_w U) \setminus \{w\}$ is incident to at most one such line. Thus, $\mathcal{F}_w$ is of dimension at most one. Since $U$ is two-dimensional and every regular point of $U$ is incident to a one-dimensional subset of flats of $\mathcal{F}_U$, we conclude that $\mathcal{F}_U$ is of dimension at most two.

Let $\pi_1 : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the first three coordinates and let $\pi_2 : \mathbb{R}^6 \to \mathbb{R}^3$ be the projection on the last three coordinates. As in the preceding proofs, let $\gamma_1 = \overline{\pi_1(\mathcal{F}_U)}$ and $\gamma_2 = \overline{\pi_2(\mathcal{F}_U)}$. By Theorem 7.4, both $\gamma_1$ and $\gamma_2$ are varieties of degree $O_k(1)$ and dimension at most two. If $|\gamma_1 \cap \mathcal{P}| = \Omega(n^{2/3})$ or $|\gamma_2 \cap \mathcal{P}| = \Omega(n^{2/3})$, then we are done. We may thus assume that $|\gamma_1 \cap \mathcal{P}| = O(n^{2/3})$ and $|\gamma_2 \cap \mathcal{P}| = O(n^{2/3})$. We partition the rest of the analysis according to the dimension of $\gamma_1$.

If $\dim \gamma_1 = 0$ then by Lemma 7.1 it consists of $O_k(1)$ points. Since $|\gamma_2 \cap \mathcal{P}| = O\left(n^{2/3}\right)$, every point of $\gamma_1$ corresponds to $O\left(n^{2/3}\right)$ elements of $\mathcal{F}_U$. By summing this over every point of $\gamma_1$, we get $O\left(n^{2/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ that have a one-dimensional intersection with $U$.

If $\dim \gamma_1 = 1$, then we apply Corollary 7.6 to it. We obtain that, excluding $O_k(1)$ exceptional points, for every $a \in \gamma_1$ we have that $\pi^{-1}(a)$ is contained in a variety of dimension at most one and degree $O_k(1)$. We denote such a variety as $\gamma_a$, and set $\gamma'_a = \overline{\pi_2(\gamma_a)}$. By Theorem 7.4, $\gamma'_a \subset \mathbb{R}^3$ is a variety of dimension at most one and of degree $O_k(1)$. If $|\gamma'_a \cap \mathcal{P}| = \Omega\left(n^{2/3}\right)$ then we are done. It remains to handle the case where for every non-exceptional $a$ we have $|\gamma'_a \cap \mathcal{P}| = O\left(n^{2/3}\right)$. Recalling also that $|\gamma_1 \cap \mathcal{P}| = O\left(n^{2/3}\right)$, we get that $O\left(n^{4/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ have a one-dimensional intersection with $U$.

If $\dim \gamma_1 = 2$, we again apply Corollary 7.6 to it. This implies that there exists a variety $W$ of dimension at most one and degree $O_k(1)$, such that for every $a \in \gamma_1 \setminus W$ we have that $\pi^{-1}(a)$ consits of $O_k(1)$ points. Since $\dim W \leq 1$, it can be handled as the cases of $\dim \gamma_1 \leq 1$. Recalling that $|\gamma_1 \cap \mathcal{P}| = O\left(n^{2/3}\right)$, we conclude that $O\left(n^{2/3}\right)$ flats of $\mathcal{F}_\mathcal{P}$ have a one-dimensional intersection with $U$. □

# References


[1] S. Basu, R. Pollack, and M.-F. Coste–Roy, *Algorithms in real algebraic geometry*, Springer Science & Business Media, 2007.

[2] J. Bochnak, M. Coste, and M. Roy, *Real Algebraic Geometry*, Springer-Verlag, Berlin, 1998.

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

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

[5] J. Fox, J. Pach, A. Sheffer, A. Suk, and J. Zahl, A semi-algebraic version of Zarankiewicz's problem, *J. Eur. Math. Soc.* **19** (2017), 1785–1810.

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

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

[8] J. Harris, *Algebraic geometry: a first course*, Springer, New York, 1992.

[9] M.-F. Roy and N. Vorobjov, The complexification and degree of a semi-algebraic set, *Math. Z.* **239** (2002), 131–142.

[10] 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.

[11] M. Sharir and N. Solomon, Distinct and repeated distances on a surface and incidences between points and spheres, arXiv:1604.01502.

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

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

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

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

[16] H. Whitney, Elementary structure of real algebraic varieties, *Annals Math.* **66** (1957), 545–556.