ON THE USE OF KLEIN QUADRIC FOR GEOMETRIC INCIDENCE PROBLEMS IN TWO DIMENSIONS

MISHA RUDNEV AND J. M. SELIG

ABSTRACT. We discuss a unified approach to a class of geometric combinatorics incidence problems in two dimensions, of the Erdős distance type. The goal is obtaining the second moment estimate. That is, given a finite point set S in $2D$, and a function f on $S \times S$, find the upper bound for the number of solutions of the equation

$$(1) \qquad f(p,p') = f(q,q') \neq 0, \qquad (p,p',q,q') \in S \times S \times S \times S.$$

E.g., f is the Euclidean distance in the plane, sphere, or a sheet of the two-sheeted hyperboloid.

Our ultimate tool is the Guth-Katz incidence theorem for lines in $\mathbb{RP}^3$, but we focus on how the original problem in $2D$ gets reduced to its application. The corresponding procedure was initiated by Elekes and Sharir, based on symmetry considerations. The point we make here is that symmetry considerations, not be necessarily straightforward and potentially requiring group representation machinery can be bypassed or made implicit. The classical Plücker-Klein formalism for line geometry enables one to directly interpret a solution of (1) as intersection of two lines in $\mathbb{RP}^3$. This, e.g., allows for a very brief argument as to how the Euclidean plane distance argument extends to the spherical and hyperbolic distances.

The space of lines in the projective three-space, the Klein quadric $\mathcal{K}$, is four-dimensional. Thus, we start out with an injective map $\mathfrak{F} : S \times S \to \mathcal{K}$, that is from a pair of points (p,q) to a line l_{pq} and seek a corresponding combinatorial problem in the form (1) in two dimensions, which can be solved by applying the Guth-Katz theorem to the set of lines $\{l_{pq}\}$ in $\mathbb{RP}^3$.

We identify a few arguably new such problems, and hence applications of the Guth-Katz theorem and make generalisations of the existing ones. It is the direct approach in question that is the main purpose of this paper.

1. INTRODUCTION

In 2010 Guth and Katz, [4], settled the long standing Erdős distance conjecture. They proved that a set S of N points in $\mathbb{R}^2$ determines $\Omega\left(\frac{N}{\log N}\right)$ distinct Euclidean distances between pairs of points in S.

Their proof has two key steps. The first one is to reduce the problem about distances in $2D$ to that of line-line incidences in $3D$. In order to do so, Guth and Katz used what since has become known as the "Elekes-Sharir framework", presented in [2], see also the references contained therein. Given two points $p,q \in S$, consider the set of rotations in the plane that map p to q. If $p \neq q$, the centre of such a rotation lies on the bisector to $[pq]$, and the cotangent of the half-angle of rotation ϕ changes linearly as one moves along the bisector from the midpoint of $[pq]$. Hence, in the Euclidean coordinates (x,y,z), where (x,y) are the coordinates of the rotation centre and $z = \cot \phi$, the set of plane rotations that take $p = (p_1, p_2)$ to $q = (q_1, q_2)$ is given by a line with the equation

$$(2) \qquad l_{pq}: \qquad (x,y,z)(t) = \left(\frac{p_1 + q_1}{2}, \frac{p_2 + q_2}{2}, 0\right) + t\left(\frac{q_2 - p_2}{2}, \frac{p_1 - q_1}{2}, 1\right).$$

Besides the translation from p to q (which is irrelevant for the ensuing incidence count at the next step) can be associated with the point at infinity on this line, embedded in the projective space $\mathbb{RP}^3$. It follows that for $p, q, p', q' \in S$,

$$\text{(3)} \qquad \|p - p'\| = \|q - q'\| \qquad \Leftrightarrow \qquad l_{pq} \cap l_{p'q'} \neq \emptyset.$$

The second key step was a new incidence theorem on line-line intersections in $\mathbb{R}^3$.

Theorem 1. *Consider a set of N^2 lines in $\mathbb{R}^3$, such that*
  (i) no more than $O(N)$ lines are concurrent,
  (ii) no more than $O(N)$ lines are co-planar,
  (iii) no more than $O(N)$ lines lie in a regulus.[1]
Then the number of pairs of intersecting lines is $O\left(N^3 \log N\right)$.

Once the conditions of Theorem 1 have been checked to be satisfied, one gets the "second moment" upper estimate $O\left(N^3 \log N\right)$ on the number of pairs of congruent line segments with endpoints in S, cf. (3). The lower bound on the cardinality of the distance set $\Delta(S)$, i.e., number of classes of segments by congruence, follows by the Cauchy-Schwarz inequality:

$$\text{(4)} \qquad |\Delta(S)| \geq \frac{N^4}{O(N^3 \log N)} = \Omega\left(\frac{N}{\log N}\right).$$

As usual, we use the notation $|\cdot|$ for cardinalities of finite sets. Symbols $\ll, \gg$, suppress absolute constants in inequalities, as well as respectively do the symbols O and Ω. Besides, $X = \Theta(Y)$ means that $X = O(Y)$ and $X = \Omega(Y)$. The symbols C and c stand for absolute constants, which may change from line to line.

A reasonable question appears to be what other two-dimensional geometric combinatorics problems can be treated in terms of Theorem 1. Tao in his blog[2] stresses the universality of the Elekes-Sharir framework and describes it in the case when S is the point set on the two-sphere $\mathbb{S}^2$, rather than $\mathbb{R}^2$. In the latter case, he argues that the set of isometries of $\mathbb{S}^2$ mapping a point p to a point q can be represented by a great circle on the three-sphere $\mathbb{S}^3$, which doubly covers the symmetry group $SO(3)$. This can be seen by using quaternions. Furthermore, great circles project through the centre of $\mathbb{S}^3$ as lines in $\mathbb{R}^3$, which can be expected to satisfy the conditions of Theorem 1. More generally, one can use for the same purpose the Clifford algebra representation of $SO(3)$ itself – and we spell this out explicitly in the Appendix for comparison with the direct haiku (meaning that it virtually takes three lines) approach in the main body of the paper. Tao also states that in the case of constant negative curvature, that is the hyperbolic plane $\mathbb{H}^2$ replacing $\mathbb{S}^2$, the situation must be essentially the same, and in particular one can pass from both corresponding isometry groups $SO(3)$ and $SL(2)$, to the Euclidean one $SE(2)$ via the limiting process known as Saletan reduction.

Having felt that there is a certain gap between a blog post and a complete proof, we have decided to furnish one. We do it in essentially three lines, and without the symmetry argument.

We then move on to other combinatorial problems in $\mathbb{R}^2$ which can be shown to be amenable to an application of the Guth-Katz theorem. Roche-Newton and the first author analysed the case

---

[1] We adhere in this note to the standard terminology in line geometry texts, where the term *regulus* is used for a single ruling of a doubly-ruled surface.

[2] See terrytao.wordpress.com/2011/03/05/lines-in-the-euclidean-group-se2/.

of the Minkowski metric in [7] and found out that owing to the fact that the distance form is sign-indefinite, the hypothesis (ii) of Theorem 1 generally gets violated[3]. But every line-line incidence inside a plane where the hypothesis was violated was shown to correspond to a zero Minkowski distance. Those could be discounted, once a combinatorial argument to weed the corresponding line intersections in "rich planes" out had been developed. This added the symmetry group $SE(1,1)$ to the list of applications of the Elekes-Sharir/Guth-Katz approach.

The incidence estimate of Theorem 1 is sharp. Moreover, since the space of lines in $\mathbb{RP}^3$ is four-dimensional, and there are four independent parameters in say (2), the family of lines $\{l_{pq}\}$ arising via the Elekes-Sharir framework can indeed yield an extremal incidence configuration, with the number of lines' pair-wise intersections being $\Theta(N^3 \log N)$. This can happen at least in the two cases that have been work out in detail, $SE(2)$ and $SE(1,1)$. What follows upon the application of the Cauchy-Schwarz inequality, cf. (4), is a different matter, beyond the resolution power of the second moment estimate. E.g., in the case of the Euclidean distance, the omnipresent sharpness example when S is a truncated integer lattice suggests that the ultimate lower bound for the number of distinct distances should be $|\Delta(S)| = \Omega\left(\frac{N}{\sqrt{\log N}}\right)$, a fraction of $\log N$ power better than (4). In the Minkowski distance case the same example yields $\Theta\left(\frac{N}{(\log N)^\delta (\log \log N)^{3/2}}\right)$ distinct distances, with $\delta = 0.086071\ldots$, see [3]. Once again, this is not quite $|\Delta(S)| = \Omega\left(\frac{N}{\log N}\right)$, as proved in [7]. On $\mathbb{S}^2$, there may be no point configurations yielding fewer than $|\Delta(S)| = \Omega(N)$ distances, but we would hesitate to suggest that there are none yielding the logarithmic factor in the second moment estimate. Perhaps, the explicit expressions (16) for the lines $\{l_{pq}\}$ we provide for the spherical case be useful to furnish a construction of a point set on $\mathbb{S}^2$ with the extreme value for the second moment if such an example exists.

Whether or not there are point configurations in the $2D$ hyperbolic model $\mathbb{H}^2$, yielding fewer than $\Omega(N)$ distinct hyperbolic distances, appears to be an interesting question, to which we do not know the answer. But in any case, the second moment approach, i.e., counting congruent geodesic segments with endpoints in S is hardly sharp enough to tackle the endpoint issue as to the true minimum number of distinct distances, for one is at the mercy of the application of the Cauchy-Schwarz inequality, à-la (4).

All the listed applications of Theorem 1 began with the same initial step: symmetry considerations within the Elekes-Sharir framework. In this note we aim to somewhat turn things around and bypass symmetry considerations. We show that one can map directly a point pair $(p, q) \in S \times S$ to a Plücker vector in the Klein quadric $\mathcal{K}$, that is the space of lines in $\mathbb{FP}^3$. Thus our main point is simplification of the procedure, which arguably makes it more flexible. We anticipate this to be even more so if one deals with largely open Erdős type geometric combinatorics problems in three, rather than two dimensions, in which case the $4D$ "phase space", the Klein quadric in $\mathbb{FP}^5$, gets naturally replaced by the Study quadric in $\mathbb{FP}^7$ and more generally by a Grassmann manifold..

The field $\mathbb{F}$ for the time being is $\mathbb{R}$, so far as no full extension of Theorem 1 to other fields has been established. Still, we often proceed as long as we can with a general $\mathbb{F}$, since the projective quadric formalism works in a broader context.

2. Main results

We re-state the claim that the main point of this note is not so much the novelty of results, but universality and transparency of the method. Our first theorem is the extension of the Guth-Katz Erdős distance claim to constant curvature metrics in $2D$.

---

[3]In fact, we show below that both hypotheses (i) and (ii) get violated. However, the former hypothesis is violated only at points lying in two planes, which were excluded from the three-space in [7] by the choice of parameterisation.

Theorem 2. *Let S be a set of N points on a $\mathbb{S}^2$ or $\mathbb{H}^2$. Then the number of distinct distances between pairs of points of S is $\Omega\left(\frac{N}{\log N}\right)$.*

Once again, our motive, as to Theorem 2, formulated in the above-mentioned blog by T. Tao is to provide a very short proof, bypassing the symmetry argument.

It turns out that our viewpoint enables one to identify several types of combinatorial problems where, once the problems are over the reals, the Guth-Katz theorem may be used. Our next theorem applies to metric problems and summarises/generalises the Euclidean and Minkowski distance cases as follows.

Theorem 3. *Let $S \subset \mathbb{R}^2$ have N elements and M_1, M_2 be non-degenerate quadratic forms of the same signature. Then the number of solutions of the equation*

$$(5) \qquad M_1(p - p') = M_2(q - q') \neq 0, \qquad (p, p', q, q') \in S \times S \times S \times S$$

is $O(N^3 \log N)$.

The immediate corollary, in the case of $M_1 = M_2 = M$, cf. (4), is the lower bound $\Omega\left(\frac{N}{\log N}\right)$ on the number of values of

$$M(p - p') \equiv (p - p')^T M(p - p'),$$

unless they are all zero. In the future, we identify the notation for a quadratic form with that for its matrix.

The next problem we consider appears to be new.

Theorem 4. *Let $S \subset \mathbb{R}^2$ have N elements. Let (a, c), (β, δ) be two pairs of fixed non-collinear - within each pair – vectors in $\mathbb{R}^2$. Then the number of solutions of the equation*

$$(6) \qquad (p - p')^T ac^T (p - p') = (q - q')^T \beta\delta^T (q - q') \neq 0, \qquad (p, p', q, q') \in S \times S \times S \times S$$

is $O(N^3 \log N)$.

The immediate corollary, in the case $a = \beta$, $c = \delta$ is the lower bound $\Omega\left(\frac{N}{\log N}\right)$ on the number of values of $(p - p')^T ac^T (p - p')$, cf. (4). Or, exclusively, all these values are zero.

Note that as far as Theorem 3 is concerned, if the signature of the quadratic forms involved is $(1, 1)$, each quadratic form M_1, M_2 has two isotropic directions $p : M_i(p) = 0$. Thus, one can trivially have, say half of the points on an isotropic line for M_1 and the other half on an isotropic line for M_2. Had the zero value been not excluded, the number of solutions of the equation (5) would have been $\Omega(N^4)$. The same scenario may occur as to Theorem 4. There, in place of M_1 one has a non-symmetric degenerate matrix ac^T, which has a left isotropic direction – orthogonal to a, and a right one – orthogonal to c. Theorems 3 and 4 respectively imply that in the case $M_1 = M_2$ and $ac^T = \beta\delta^T$, either the corresponding quadratic form has $\Omega\left(\frac{N}{\log N}\right)$ distinct values, evaluated on $p - p'$, or the only value it returns is zero.

The other type of problems we identify is counting quadruples of points of S which determine similar directions. More precisely, let $\lambda \neq 0$. For $p, p', q, q' \in S$, with $p = (p_1, p_2)$, and so on, what is the maximum number of solutions of the equation

$$(7) \qquad \lambda \frac{p_2 - p_2'}{p_1 - p_1'} = \frac{q_2 - q_2'}{q_1 - q_1'} ?$$

The problem of finding the minimum number of distinct directions, determined by a non-collinear set of points in $\mathbb{R}^2$ was solved, up to the best constant, by the early 1980s. See, e.g., [9], which has

a self-explanatory title *2N Noncollinear points determine at least 2N directions* and the references contained therein.

Proving an upper bound on the number of solutions of (7) appears to be more involved, and needs the full power of the Guth-Katz theorem. Note that owing to the possible presence of a single very rich line, supporting, say half of the points, the total number of solutions of (7) can trivially be $\Omega(N^4)$. So, we have to narrow the point sets $S \subset \mathbb{R}^2$ in question down to the case when every line supports $O(\sqrt{N})$ points, and then ask for the number of solutions of (7). The example to bear in mind is again the truncated integer lattice, when the number of solutions of equation (7) with $\lambda = 1$ is $\Omega(N^3 \log N)$.

Theorem 5. *Let $S \subset \mathbb{R}^2$ have N elements with $O(\sqrt{N})$ points on any straight line. Then, for any $\lambda \neq 0$, the number of solutions of the equation (7) is $O(N^3 \log N)$.*

Once again, for $\lambda = 1$, Theorem 1 provides a sharp bound $O(N^3 \log N)$ on the number of solutions of the equation (7). On the other hand, the logarithmic factor disappears if one asks for the total number of distinct directions. The application of the Cauchy-Schwarz inequality, cf (4), is to blame for that.

The scopes of Theorems 3 - 5 somewhat intersect. E.g., if one takes in Theorem 4 $a = \beta = (0,1)$ and $c = \delta = (1,0)$, then one ends up dealing with Minkowski distances. The same concerns Theorem 5 in the special case $S = A \times A$, when in fact a stronger result can be obtained via the Szemerédi-Trotter theorem, [6].

We end this section by stating the following slight generalisation of the Guth-Katz theorem, Theorem 1, which is implicit in [7]. It will be used "as a hammer" after the initial set-up procedure in the Klein quadric, the main focus of this paper, has been completed.

Theorem 1'. *Let L_1, L_2 be two distinct sets of N^2 lines each in $\mathbb{R}^3$, such that*
  (i) at any concurrency point there meet no more than $O(N)$ lines from one of the two sets,
  (ii) no more than $O(N)$ lines from one of the two sets lie in a plane,
  (iii) no more than $O(N)$ lines lie in a regulus.
  Then the number of intersecting pairs of lines $(l_1, l_2) \in L_1 \times L_2$ is $O(N^3 \log N)$.

3. Mapping pairs of points to Klein quadric

In this section we see what happens if one takes a pair of points $(p, q) \in S \times S$ and maps it linearly and injectively to the Klein quadric $\mathcal{K}$, thereby defining a line l_{pq} in $\mathbb{FP}^3$. This can be done in many ways. We seek to identify the maps, where one is able to interpret the intersection of l_{pq} with $l_{p'q'}$ in $\mathbb{FP}^3$ as an instance of the general equation (1). This roughly speaking requires the pairs of variables (p, q), (p', q') corresponding to the lines l_{pq} and $l_{p'q'}$ to separate into pairs (p, p'), (q, q').

3.1. **Background.** We start with a minimum background which casts, in particular, Conditions (i)-(iii) of Theorem 1 in terms of the Klein quadric $\mathcal{K}$. See [8] for more details.

The space of lines in $\mathbb{FP}^3$ is represented as a projective quadric, known as the Klein quadric $\mathcal{K}$ in $\mathbb{FP}^5$, with projective coordinates $(P_{01} : P_{02} : P_{03} : P_{23} : P_{31} : P_{12})$, known as Plücker coordinates. The line through two points $(q_0 : q_1 : q_2 : q_3)$ and $(u_0 : u_1 : u_2 : u_3)$ in $\mathbb{FP}^3$ has Plücker coordinates, defined as follows

$$(8) \qquad\qquad P_{ij} = q_i u_j - q_j u_i.$$

Hence, for a line in $\mathbb{F}^3$, obtained by setting $q_0 = u_0 = 1$, the Plücker coordinates acquire the meaning of a projective pair of three-vectors $(\boldsymbol{\omega} : \boldsymbol{v})$, where $\boldsymbol{\omega}$ is a vector in the direction of the

line and for any point $\boldsymbol{q} = (q_1, q_2, q_3)$ on the line, $\boldsymbol{v} = \boldsymbol{q} \times \boldsymbol{\omega}$ is the line's moment vector, with respect to some fixed origin. We use the boldface notation for three-vectors throughout.

Conversely, one can denote $\boldsymbol{\omega} = (P_{01}, P_{02}, P_{03})$, $\boldsymbol{v} = (P_{23}, P_{31}, P_{12})$, the Plücker coordinates then become $(\boldsymbol{\omega} : \boldsymbol{v})$, and treat $\boldsymbol{\omega}$ and $\boldsymbol{v}$ as vectors in $\mathbb{F}^3$, bearing in mind that, in fact, as a pair they are projective quantities. The lines in the plane at infinity in $\mathbb{FP}^3$ are represented by Plücker vectors $(\boldsymbol{0} : \boldsymbol{v})$. The equation of the Klein quadric $\mathcal{K}$ in $\mathbb{FP}^5$ is

$$(9) \qquad\qquad P_{01}P_{23} + P_{02}P_{31} + P_{03}P_{12} = 0, \quad \text{i.e.} \quad \boldsymbol{\omega} \cdot \boldsymbol{v} = 0.$$

Equivalently, equation (9) arises after writing out, with the notations (8), the condition

$$\det \begin{pmatrix} q_0 & u_0 & q_0 & u_0 \\ q_1 & u_1 & q_1 & u_1 \\ q_2 & u_2 & q_2 & u_2 \\ q_3 & u_3 & q_3 & u_3 \end{pmatrix} = 0.$$

Two lines l, l' in $\mathbb{FP}^3$, represented by points $L, L' \in \mathcal{K}$, with Plücker coordinates

$$L = (P_{01} : P_{02} : P_{03} : P_{23} : P_{31} : P_{12}), \qquad L' = (P'_{01} : P'_{02} : P'_{03} : P'_{23} : P'_{31} : P'_{12})$$

meet in $\mathbb{FP}^3$ if and only if

$$(10) \qquad\qquad P_{01}P'_{23} + P_{02}P'_{31} + P_{03}P'_{12} + P'_{01}P_{23} + P'_{02}P_{31} + P'_{03}P_{12} = 0.$$

The left-hand side in the elation (10) above is known as the reciprocal product, and can be re-stated as $L^T \mathcal{Q} L' = 0$, where

$$\mathcal{Q} = \begin{pmatrix} 0 & I_3 \\ I_3 & 0 \end{pmatrix},$$

where I_3 is the 3×3 identity matrix. To avoid confusion we use the lowercase notation for lines l in $\mathbb{FP}^3$; they are represented by points $L \in \mathcal{K}$, the uppercase notation.

If the Plücker coordinates of the two lines are written as $L = (\boldsymbol{\omega} : \boldsymbol{v})$ and $L' = (\boldsymbol{\omega}' : \boldsymbol{v}')$, then the zero reciprocal product condition can be expressed as

$$(11) \qquad\qquad \boldsymbol{\omega} \cdot \boldsymbol{v}' + \boldsymbol{v} \cdot \boldsymbol{\omega}' = 0.$$

Using the latter three equations, it is easy to see, by taking the gradient of (9) that a $\mathbb{FP}^4$ in $\mathbb{FP}^5$ is tangent to $\mathcal{K}$ at some point L if an only if the corresponding dual vector, defining the hyperplane is itself in the Klein quadric in $\mathbb{FP}^{5*}$. Moreover, it follows from (10) that $T_L\mathcal{K} \cap \mathcal{K}$ consists of $L' \in \mathcal{K}$, representing all lines l' in $\mathbb{FP}^3$, incident to the line l. This set of lines is usually called a singular line complex.

The largest dimension of a projective subspace contained in $\mathcal{K}$ is two. Copies of $\mathbb{FP}^2$ contained in $\mathcal{K}$ have important meaning which we describe next. To this end, $\mathcal{K}$ has two (assuming $\text{char}(\mathbb{F}) \neq 2$) "rulings" by planes, which lie entirely in the quadric, with the fibre space of each ruling being $\mathbb{FP}^3$. The other important type of subvarieties in $\mathcal{K}$, relevant to the subject of this note are conics, arising as transverse intersections of $\mathcal{K}$ with two-planes.

The Klein quadric contains a three-dimensional family of projective two-planes, called α-planes. Elements of a single α-plane are lines, concurrent at some point $(q_0 : q_1 : q_2 : q_3) \in \mathbb{FP}^3$. If the concurrency point is $(1 : \boldsymbol{q})$, which is identified with $\boldsymbol{q} \in \mathbb{F}^3$, the α-plane is a graph $\boldsymbol{v} = \boldsymbol{q} \times \boldsymbol{\omega}$. Otherwise, an ideal concurrency point $(0 : \boldsymbol{\omega})$ gets identified with some fixed $\boldsymbol{\omega}$, viewed as a projective vector. The corresponding α-plane is the union of the set of parallel lines in $\mathbb{F}^3$ in the direction of $\boldsymbol{\omega}$, with Plücker coordinates $(\boldsymbol{\omega} : \boldsymbol{v})$, so $\boldsymbol{v} \cdot \boldsymbol{\omega} = 0$, by (9), and the set of lines in the plane at infinity incident to the ideal point $(0 : \boldsymbol{\omega})$. The latter lines have Plücker coordinates $(\boldsymbol{0} : \boldsymbol{v})$, with once again $\boldsymbol{v} \cdot \boldsymbol{\omega} = 0$.

Similarly, the Klein quadric contains another three-dimensional family of two-planes, called β-planes, which represent co-planar lines in $\mathbb{FP}^3$. A "generic" β-plane is a graph $\boldsymbol{\omega} = \boldsymbol{u} \times \boldsymbol{v}$, for some $\boldsymbol{u} \in \mathbb{F}^3$. The case $\boldsymbol{u} = \boldsymbol{0}$ corresponds to the plane at infinity, otherwise the equation of the co-planarity plane in $\mathbb{F}^3$ becomes

$$(12) \qquad\qquad\qquad\qquad \boldsymbol{u} \cdot \boldsymbol{q} = -1.$$

If $\boldsymbol{u}$ gets replaced by a fixed ideal dual point $(0 : \boldsymbol{v})$, the corresponding β-plane comprises lines, coplanar in planes through the origin: $\boldsymbol{v} \cdot \boldsymbol{q} = 0$. The corresponding β-plane in the Klein quadric is formed by the set of lines with Plücker coordinates $(\boldsymbol{\omega} : \boldsymbol{v})$, plus the set of lines through the origin in the co-planarity plane. The latter lines have Plücker coordinates $(\boldsymbol{\omega} : \boldsymbol{0})$. In both cases one requires $\boldsymbol{\omega} \cdot \boldsymbol{v} = 0$.

Two planes of the same ruling of $\mathcal{K}$ always meet at a point, which is the line defined by the two concurrency points in the case of α-planes. A α- and a β-plane typically do not meet; if they do this means that the concurrency point, defining the α-plane lives in the plane π, defining the β-plane. The intersection is then a straight line, a copy of $\mathbb{FP}^1$ in $\mathcal{K}$, representing a *plane pencil of lines* – the lines in π via the concurrency point. These are lines in $\mathbb{FP}^3$, which are co-planar in π and concurrent at the concurrency point. Conversely, each line in $\mathcal{K}$ identifies the pair (α-plane, β-plane), that is the plane pencil of lines uniquely. Moreover points $L, L' \in \mathcal{K}$ can be connected by a straight line in $\mathcal{K}$ if and only if the corresponding lines l, l' in $\mathbb{FP}^3$ meet, cf. (10).

These α- and β-planes represent a specific case when a subspace $\Pi = \mathbb{FP}^2$ of $\mathbb{FP}^5$ is contained in $\mathcal{K}$. A semi-degenerate case is when the two-subspace Π contains a line in $\mathcal{K}$. The non-degenerate situation would be the two-plane intersecting $\mathcal{K}$ along a conic. If the field $\mathbb{F}$ is algebraically closed, then any Π intersects $\mathcal{K}$. Otherwise this is not necessarily the case, take e.g the case when Π is defined by the condition $\boldsymbol{\omega} = \boldsymbol{v}$ for $\mathbb{F} = \mathbb{R}$.

Assume that the equations of the two-plane Π can be written as

$$A\boldsymbol{\omega} + B\boldsymbol{v} = \boldsymbol{0},$$

where A, B are some 3×3 matrices. How can one describe the union in $\mathbb{FP}^3$ of lines represented by $\Pi \cap \mathcal{K}$? For points in $\Pi \cap \mathcal{K}$, which do not represent lines in the plane at infinity in $\mathbb{FP}^3$, we can write $\boldsymbol{v} = \boldsymbol{q} \times \boldsymbol{\omega}$, where $\boldsymbol{q}$ is some point in $\mathbb{F}^3$, on the line with Plücker coordinates $(\boldsymbol{\omega} : \boldsymbol{v})$, and $\boldsymbol{\omega} \neq \boldsymbol{0}$. If Q is the skew-symmetric matrix $ad(\boldsymbol{q})$ (that is the cross product of $\boldsymbol{q}$ with a vector is Q times this vector as a column-vector) we obtain

$$(A - BQ)\boldsymbol{\omega} = \boldsymbol{0} \qquad \Rightarrow \qquad \det(A - BQ) = 0.$$

This a quadratic equation in $\boldsymbol{q}$, since Q is a 3×3 skew-symmetric matrix, so $\det Q = 0$. If the above equation has a linear factor in $\boldsymbol{q}$, defining a plane in $\mathbb{FP}^3$, then $\Pi \cap \mathcal{K}$ contains a line, which represents a pencil of lines in the latter plane in $\mathbb{FP}^3$. If the above quadratic polynomial in $\boldsymbol{q}$ is irreducible, then if the field $\mathbb{F}$ is algebraically closed we always get a quadric surface in $\mathbb{FP}^3$. This is the precisely the non-degenerate intersection case, when $\mathcal{K} \cap \Pi$ is a conic.

In the latte case the two-plane Π in $\mathbb{FP}^5$ can be obtained as the intersection of three four-planes, tangent to $\mathcal{K}$ at some three points L_1, L_2, L_3, corresponding to three mutually skew lines in $\mathbb{FP}^3$. Thus the intersection is a regulus: the set of all lines in $\mathbb{FP}^3$, meeting three given mutually skew lines l_1, l_2, l_3.

3.1.1. *Proof of Theorem 2.* We now move on to proofs of our main results. For motivation, let us first show how the Elekes-Sharir symmetry argument can be bypassed if one deals with the second moment estimate for plane Euclidean distances. Rewrite the equation (3) as

$$p \cdot p' - q \cdot q' - (\|p\|^2 + \|p'\|^2 - \|q\|^2 - \|q'\|^2) = 0.$$

(For two-vectors we do not use the boldface notation.) The latter equation (cf. (2) and (10)) is the condition of the zero reciprocal product of two points L_{pq} and $L_{p'q'}$ in the Klein quadric, with the Plücker coordinates

$$(13) \qquad L_{pq} = \left[\frac{q_2 - p_2}{2} : \frac{p_1 - q_1}{2} : 1 : \frac{p_2 + q_2}{2} : -\frac{p_1 + q_1}{2} : \frac{\|p\|^2 - \|q\|^2}{4} \right],$$

the same with prime indices for $L_{p'q'}$, where $p = (p_1, p_2)$, etc. The above expression just the Plücker coordinate expression for the line, given by equation (2). Indeed, the first three Plücker coordinates are the line's direction vector $\boldsymbol{\omega}$, the remaining three are the cross product of the point $\boldsymbol{q} = \left(\frac{p_1 + q_1}{2}, \frac{p_2 + q_2}{2}, 0 \right)$ on the line with $\boldsymbol{\omega}$.

Hence, estimating the number of solutions of (3) is tantamount to estimating the number of pairwise intersections of the lines $\{l_{pq}\}_{(p,q) \in S \times S}$. The fact that this set of lines satisfies the hypotheses of Theorem 1 is verified in [4]; we will shortly do this as to the lines arising in the context of Theorem 2.

We now prove Theorem 2 in the case when the point set S is supported on the two-sphere $\mathbb{S}^2$ and for the hyperbolic model. Along the lines of Section 3.1 we use boldface notation for three-vectors, except in the notations for the lines l_{pq}.

Proof. Let $S \subset \mathbb{S}^2$ be the set of N points. Let $\boldsymbol{p} = (p_1, p_2, p_3)$ be the Euclidean coordinates of $\boldsymbol{p} \in S$. Clearly, the geodesic segment congruency condition (3) the distance now being the restriction of the Euclidean distance on $\mathbb{S}^2$ rewrites as

$$(14) \qquad \boldsymbol{p} \cdot \boldsymbol{p}' = \boldsymbol{q} \cdot \boldsymbol{q}',$$

where $\cdot$ is the dot product in $\mathbb{R}^3$ (the distance between $\boldsymbol{p}$ and $\boldsymbol{p}'$ on the unit sphere being $\arccos(\boldsymbol{p} \cdot \boldsymbol{p}')$.)

The latter can be rewritten as

$$(15) \qquad (\boldsymbol{p} + \boldsymbol{q}) \cdot (\boldsymbol{p}' - \boldsymbol{q}') + (\boldsymbol{p}' + \boldsymbol{q}') \cdot (\boldsymbol{p} - \boldsymbol{q}) = 0.$$

Now, the left-hand side is the reciprocal product of two Plucker vectors L_{pq} and $L_{p'q'}$, where

$$(16) \qquad L_{pq} = (\boldsymbol{p} + \boldsymbol{q} : \boldsymbol{p} - \boldsymbol{q}) = [p_1 + q_1 : p_2 + q_2 : p_3 + q_3 : p_1 - q_1 : p_2 - q_2 : p_3 - q_3],$$

similarly for $L_{p'q'}$. (We do not use the boldface notations for the subscripts in L_{pq}, for the set S is two-dimensional.) Observe that the reciprocal product of L_{pq} with itself equals $\|\boldsymbol{p}\|^2 - \|\boldsymbol{q}\|^2$, which is zero for any $\boldsymbol{p}, \boldsymbol{q} \in S$.

Let us verify that the corresponding set of lines $\{l_{pq}\}_{(p,q) \in S \times S}$ satisfies the hypotheses of Theorem 1. Consider the hypothesis (i). Assuming concurrency at some point in $\mathbb{R}^3$, there is $\boldsymbol{u} = (u_1, u_2, u_3)$, such that

$$(17) \qquad \boldsymbol{u} \times (\boldsymbol{p} + \boldsymbol{q}) = (\boldsymbol{p} - \boldsymbol{q}).$$

Let U be the skew-symmetric matrix $ad(\boldsymbol{u})$, thus, with I for the 3×3 identity matrix, we have

$$(U - I)\boldsymbol{p} = -(U + I)\boldsymbol{q}.$$

Both matrices in brackets is non-degenerate, and therefore for every $\boldsymbol{p}$ we have at most one $\boldsymbol{q}$, satisfying the latter equation. If concurrency occurs at a point at infinity, this fixes $\boldsymbol{p} + \boldsymbol{q}$, hence the same conclusion.

Therefore the hypothesis (i) is satisfied: for every concurrency point $\boldsymbol{u}$, there is at most one line l_{pq} passing through it, for each fixed $\boldsymbol{p}$. The verification of (ii) is exactly the same, for now one repeats the argument as to $(\boldsymbol{p} + \boldsymbol{q}) = \boldsymbol{u} \times (\boldsymbol{p} - \boldsymbol{q})$.

Finally, to verify the hypothesis (iii) we refer the reader to the forthcoming Lemma 3.1, which does it in a fairly general context.

In the case of the hyperbolic plane $\mathbb{H}^2$, by analogue with the above, we take the Hyperboloid model of the hyperbolic metric instead (which is isometric to other models, say $\mathbb{H}^2$ or the Poincaré disk, see e.g. [1].) I.e. let $\mathbb{L} \subset \mathbb{R}^3$ (which in the literature stands, apparently, for "Loid", [1]) have equation

$$x_1^2 + x_2^2 - x_3^2 = -1, \qquad x_3 > 0,$$

and $S \subset \mathbb{L}$. The hyperbolic distance between $\boldsymbol{p}, \boldsymbol{p}' \in \mathbb{L}$ equals $\cosh^{-1}(\boldsymbol{p} \cdot \boldsymbol{p}') = p_3 p_3' - p_1 p_1' - p_2 p_2'$, that is now (and only through the rest of this proof) $\cdot$ stands for the Minkowski dot product. So the geodesic segment congruency condition (3), the distance now being the restriction of the Euclidean distance on $\mathbb{L}$, is given again by (14), (15) only in terms of the Minkowski dot product.

Now, the left-hand side of (15) is the reciprocal product of two Plucker vectors L_{pq} and $L_{p'q'}$, where

$$(18) \qquad L_{pq} = [p_1 + q_1 : p_2 + q_2 : p_3 + q_3 : p_1 - q_1 : p_2 - q_2 : -(p_3 - q_3)],$$

similarly for $L_{p'q'}$. Thus, the only difference so far with the case $S \subset \mathbb{S}^2$ is the sign change of the last component of the Plücker 6-tuple. Observe that the reciprocal product of L_{pq} with itself equals zero for any $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{L}$.

To verify the hypothesis (i) of Theorem 1 one now has the analogue of (17), with the matrix $D = \text{diaq}(1, 1, -1)$ as follows:

$$D\boldsymbol{p} - \boldsymbol{u} \times \boldsymbol{p} = D\boldsymbol{q} + \boldsymbol{u} \times \boldsymbol{q}.$$

The condition $D\boldsymbol{p} - \boldsymbol{u} \times \boldsymbol{p} = 0$, which is necessary for having more than one one line l_{pq} passing through the concurrency point $\boldsymbol{u}$ for each fixed $\boldsymbol{q}$, means that $\boldsymbol{p}$ is such that its reflection w.r.t. the $(x_1 x_2)$-plane is tantamount to vector multiplication by $\boldsymbol{u}$. This is only possible when $u_3 = 0$ and $\boldsymbol{p}$ lie on the light cone $x_1^2 + x_2^2 - x_3^2 = 0$, but not on $\mathbb{L}$. The same conclusion holds for concurrency at infinity, which requires that $\boldsymbol{p} + \boldsymbol{q}$ be fixed. Hence, as long as $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{L}$, the hypothesis (i) of Theorem 1 is satisfied. The same argument applies to the hypothesis (ii). To verify the hypothesis (iii) the reader is referred to the forthcoming Lemma 3.1.

$\square$

3.2. Map $\mathfrak{F}$ and separating variables.

From now on, till the Appendix, we deal with the plane set $S \in \mathbb{F}^2$ (to apply the Guth-Katz theorem one must have $\mathbb{F} = \mathbb{R}$). We now consider linear maps of $(p, q) \in S \times S$ to $\mathcal{K}$ as follows. Let $a, \alpha, b, \beta, c, \gamma, d, \delta \in \mathbb{F}^2$. Let

$$(19) \qquad \begin{aligned} L_1(p, q) &= a \cdot p + \alpha \cdot q, & L_2(p, q) &= b \cdot p + \beta \cdot q, \\ L_3(p, q) &= c \cdot p + \gamma \cdot q, & L_4(p, q) &= d \cdot p + \delta \cdot q. \end{aligned}$$

(We hope that our re-use of the symbols α, β as two-vectors will not cause confusion: in Section 3.1 we defined α- and β-planes in the Klein quadric $\mathcal{K}$.)

Map $(p, q) \to \mathcal{K}$ as follows:

$$(20) \qquad \begin{aligned} \mathfrak{F} : \ (p, q) &\to L_{pq} \\ &= [L_1(p, q) : L_2(p, q) : 1 : L_3(p, q) : L_4(p, q) : -L_1(p, q)L_3(p, q) - L_2(p, q)L_4(p, q)], \end{aligned}$$

where the right-hand side is Plücker coordinates. The linear forms $L_1, \ldots, L_4$ should be linearly independent to ensure injectivity of the assignment. We shall make explicit checks with the particular choices, in the context of Theorems 3-5.

Linear independence of the linear forms $L_1, \ldots, L_4$ alone ensures that Condition (iii) of Theorem 1 is satisfied. What follows is an easy generalisation of Lemma 2.9 in [4].

Lemma 3.1. *If the linear forms $L_1, \ldots, L_4$ are linearly independent, Condition (iii) of Theorem 1 is satisfied for the family of lines $\{l_{pq}\}$ defined by (20). It is also satisfied for the families $\{l_{pq}\}$ defined by (16), (18) in the context of Theorem 2.*

Proof. If the linear forms $L_1, \ldots, L_4$ are linearly independent, the map (20) is injective. Fix p and treat q as a variable in (19). This is also the case with the maps $S \times S \to \mathcal{K}$, defined by (16), (18). For each p, the map from $q \to \mathcal{K}$ has full rank. Hence, its image in $\mathcal{K}$ is the intersection of $\mathcal{K}$ with a projective subspace $\mathbb{FP}^3$ in $\mathbb{FP}^5$, which is called in line geometry literature a linear *congruence*[4].

A regulus, that is a conic, arising as the transverse intersection of $\mathcal{K}$ with a $\mathbb{FP}^2$, will be either contained in the above congruence or intersect it at most two points.

Hence, given a regulus in $\mathbb{FP}^3$, it is either contained in the family of lines $\{l_{pq}\}_{q \in \mathbb{F}^2}$ for a fixed p or has at most two lines with the latter set in common. It follows that the maximum number of lines from the finite collection $\{l_{pq}\}$ that can lie in a regulus is $2N$, and therefore at most $4N$ in a doubly-ruled surface in $\mathbb{FP}^3$. $\square$

Two lines l_{pq} and $l_{p'q'}$ in $\mathbb{FP}^3$ defined by (20) intersect in $\mathbb{FP}^3$ if and only if the zero reciprocal product condition (10) is satisfied. I.e.:

$$(L_1(p,q) - L_1(p',q'), L_2(p,q) - L_2(p',q')) \cdot (L_3(p,q) - L_3(p',q'), L_4(p,q) - L_4(p',q')) = 0.$$

Hence,

$$L_1(p - p', q - q')L_3(p - p', q - q') + L_2(p - p', q - q')L_4(p - p', q - q') = 0.$$

This means, in view of (19), introducing three 2×2 matrices

(21) $$M_1 = ac^T + bd^T, \qquad M_2 = -(\alpha\gamma^T + \beta\delta^T), \qquad M_3 = a\gamma^T + b\delta^T + c\alpha^T + d\beta^T,$$

that

(22) $$(p - p')^T M_1 (p - p') - (q - q')^T M_2 (q - q') + (p - p')^T M_3 (q - q') = 0.$$

Our goal is to be able to separate variables in (22), that is to be able to rewrite it as $f(p, p') = g(q, q')$, for some functions f, g. There are several cases to consider.

Variables will separate if $M_3 = 0$ or otherwise possibly when $M_1 = M_2 = 0$.

The condition $M_3 = 0$ means that

(23) $$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix} \begin{pmatrix} \gamma_1 & \gamma_2 \\ \delta_1 & \delta_2 \\ \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} = 0.$$

Thus, two pairs of four-vectors $(a_1, b_1, c_1, d_1), (a_2, b_2, c_2, d_2)$ and $(\gamma_1, \delta_1, \alpha_1, \beta_1), (\gamma_2, \delta_2, \alpha_2, \beta_2)$ lie in mutually orthogonal two-spaces in $\mathbb{F}^4$.

There are three cases to consider in this context as far as the matrices M_1 and M_2 in (22) are concerned. The first two cases arise in the context of Theorem 3. They are: when both M_1, M_2 are symmetric positive definite (if $\mathbb{F} = \mathbb{R}$ or more generally if -1 is not a square in $\mathbb{F}$), and when they are both symmetric signature $(1, 1)$ (if $\mathbb{F} = \mathbb{R}$ or more generally, -1 is a square in $\mathbb{F}$). The third case arises in the context of Theorem 4: the matrices M_1, M_2 are non-symmetric degenerate.

Finally, if $M_3 \neq 0$, there will be an additional case when $M_1 = M_2 = 0$ and M_3 either diagonal or has zeroes on the main diagonal. This is the subject of Theorem 5.

---

[4]In fact, the intersection is transverse, in which case this is a *linear elliptic congruence*, a two-dimensional family of pair-wise skew lines. This is a well known figure with many interesting properties, for example it can be viewed as a set of reguli on concentric hyperboloids, see e.g., [5] .

3.2.1. *Positive definite metric case.* Take nonzero

$$c = a, \ d = b, \ \gamma = -\alpha, \ \delta = -\beta; \qquad a \neq \lambda b, \ \alpha \neq \lambda \beta, \text{ for } \lambda \in \mathbb{F}. \tag{24}$$

Clearly, (23) is thus satisfied, and we get from (22):

$$M_1 = \begin{pmatrix} a_1^2 + b_1^2 & a_1 a_2 + b_1 b_2 \\ a_1 a_2 + b_1 b_2 & a_2^2 + b_2^2 \end{pmatrix}, \quad M_2 = \begin{pmatrix} \alpha_1^2 + \beta_1^2 & \alpha_1 \alpha_2 + \beta_1 \beta_2 \\ \alpha_1 \alpha_2 + \beta_1 \beta_2 & \alpha_2^2 + \beta_2^2 \end{pmatrix},$$
$$(p - p')^T M_1 (p - p') \ = \ (q - q')^T M_2 (q - q'). \tag{25}$$

The matrices M_1, M_2 are symmetric positive definite and generalise the case of the Euclidean distance considered in [4]. Note that this case differs in a general $\mathbb{F}$ from the next one only if -1 is not a square in $\mathbb{F}$.

3.2.2. *Signature* $(1, 1)$ *metric case.* To generalise the case of the Minkowski distance considered in [7], take nonzero

$$c = a, \ d = -b, \ \gamma = -\alpha, \ \delta = \beta; \qquad a \neq \lambda b, \ \alpha \neq \lambda \beta, \text{ for } \lambda \in \mathbb{F}. \tag{26}$$

Then the variables in (22) separate as follows:

$$M_1 = \begin{pmatrix} a_1^2 - b_1^2 & a_1 a_2 - b_1 b_2 \\ a_1 a_2 - b_1 b_2 & a_2^2 - b_2^2 \end{pmatrix}, \quad M_2 = \begin{pmatrix} \alpha_1^2 - \beta_1^2 & \alpha_1 \alpha_2 - \beta_1 \beta_2 \\ \alpha_1 \alpha_2 - \beta_1 \beta_2 & \alpha_2^2 - \beta_2^2 \end{pmatrix},$$
$$(p - p')^T M_1 (p - p') \ = \ (q - q')^T M_2 (q - q'). \tag{27}$$

The matrices M_1, M_2 are symmetric non-degenerate, with signature $(1, 1)$, thus generalising the Minkowski distance in the case $\mathbb{F} = \mathbb{R}$.

To this end, let us calculate the "light cone" isotropic directions for the matrices M_1, M_2.

Lemma 3.2. $x = (-(a_2 \pm b_2), a_1 \pm b_1)$ *are isotropic vectors for* M_1*, that is* $x^T M_1 x = 0$*. Similarly,* $x = (-(\alpha_2 \pm \beta_2), \alpha_1 \pm \beta_1)$ *are isotropic vectors for* M_2*.*

Proof. The verification is a brute force calculation. $\qquad\square$

3.2.3. *Degenerate case.* Take

$$b = d = \alpha = \gamma = 0, \text{ and nonzero } a \neq \lambda c; \ \beta \neq \lambda \delta, \text{ for } \lambda \in \mathbb{F}. \tag{28}$$

Then the variables in (22) separate as in the last line of (25), (27):

$$M_1 = \begin{pmatrix} a_1 c_1 & a_1 c_2 \\ a_2 c_1 & a_2 c_2 \end{pmatrix}, \qquad M_2 = -\begin{pmatrix} \beta_1 \delta_1 & \beta_1 \delta_2 \\ \beta_2 \delta_1 & \beta_2 \delta_2 \end{pmatrix}. \tag{29}$$

In the formulation of Theorem 4 we've changed $\beta \to -\beta$.

Clearly, $y^T M_1 x = (y \cdot a)(x \cdot c)$, and hence will be zero if and only if either y is orthogonal to a or x is orthogonal to c. This defines the left and right kernels for M_1, and similarly for M_2.

3.2.4. *Directions' case.* Variables in (22) also separate in the special case when $M_1 = M_2 = 0$, and M_3 is diagonal or has zeroes on the main diagonal. We consider the latter situation and set, for some $\lambda \neq 0$,

$$c = d = \alpha = \beta = 0, \ \gamma_1 = \lambda b_1, \ \delta_1 = -\lambda a_1, \ \gamma_2 = b_2, \ \delta_2 = -a_2, \ a_2 b_1 - a_1 b_2 \neq 0. \tag{30}$$

Hence, we have

$$\lambda_1 = a_2 b_1 - a_1 b_2, \qquad \lambda_2 = \lambda \lambda_1,$$

(31)
$$M_3 = \begin{pmatrix} 0 & -\lambda_1 \\ \lambda_2 & 0 \end{pmatrix},$$

$$\lambda \frac{p_2 - p_2'}{p_1 - p_1'} = \frac{q_2 - q_2'}{q_1 - q_1'}.$$

This generalises the problem of counting pairs of points in S, which lie on some line in a given direction, then summing over directions.

4. Proof of Theorems 3-5

We have identified four cases of the injective map $\mathfrak{F} : S \times S \to \mathcal{K}$ to obtain families $\{l_{pq}\}_{(p,q) \in S \times S}$ of lines in $\mathbb{FP}^3$, whose pair-wise intersections are in one-to-one correspondence with the solutions of equations (5) (the first two cases), (6) (the third case), (7) (the fourth case). Also, by Lemma 3.1, the regulus condition (iii) if Theorem 1 is automatically satisfied by these families of lines. That remains is to check Conditions (i) and (ii) of Theorem 1. It turns out that these conditions may fail, but "not too badly", namely that the situation is nonetheless amenable to the slight generalisation of Theorem 1, Theorem 1′.

4.1. **Checking Conditions (i), (ii) of Theorem 1.** In this section we identify the scenarios under which the concurrency/coplanarity conditions of the family of lines $\{l_{pq}\}$ in $\mathbb{FP}^3$ defined by (20) may fail, for all of the four cases above. We also describe their possible failures in terms of the underlying problem in the plane. This having been done, proofs of Theorems 3-5 will be completed in the next section, after the original plane problems have been restricted to ensure that Conditions (i),(ii) of Theorem 1 have been satisfied. In the forthcoming argument we will use the discussion in Section 3.1 about α- and β-planes in $\mathcal{K}$, corresponding to concurrency/coplanarity of lines in $\mathbb{FP}^3$.

4.1.1. *Positive definite metric case.* In this case the Plücker vector L_{pq}, assigned to (p, q) via (20) is

(32) $[a \cdot p + \alpha \cdot q : b \cdot p + \beta \cdot q : 1 : a \cdot p - \alpha \cdot q : b \cdot p - \beta \cdot q : -(a \cdot p)^2 - (b \cdot p)^2 + (\alpha \cdot q)^2 + (\beta \cdot q)^2].$

Note that in the special case (2) of the Euclidean distance, considered in [4], one has equation (13), i.e.

$$L_{pq} = \left[\frac{q_2 - p_2}{2} : \frac{p_1 - q_1}{2} : 1 : \frac{p_2 + q_2}{2} : -\frac{p_1 + q_1}{2} : \frac{p_1^2 + p_2^2 - q_1^2 - q_2^2}{4} \right].$$

Lemma 4.3. *The case satisfies conditions of Theorem 1, given that -1 is not a square in $\mathbb{F}$.*

Proof. Since a is not a multiple of b and α is not a multiple of β, the linear forms $L_1, \ldots, L_4$ thus defined are linearly independent.

Let us check the concurrency condition (i) of Theorem 1.

Let $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{\omega} = (a \cdot p + \alpha \cdot q, b \cdot p + \beta \cdot q, 1)$, and

$$\boldsymbol{v} = (a \cdot p - \alpha \cdot q, b \cdot p - \beta \cdot q, -(a \cdot p)^2 - (b \cdot p)^2 + (\alpha \cdot q)^2 + (\beta \cdot q)^2).$$

Suppose, we deal with the case of concurrency at the point $\boldsymbol{u} \in \mathbb{F}^3$, that is $\boldsymbol{v} = \boldsymbol{u} \times \boldsymbol{\omega}$. This means,

$$u_1 = u_3(a \cdot p + \alpha \cdot q) - b \cdot p + \beta \cdot q,$$
$$u_2 = u_3(b \cdot p + \beta \cdot q) + a \cdot p - \alpha \cdot q.$$

The matrices multiplying p and q are, respectively

$$\left(\begin{array}{c} u_3 a^T - b^T \\ u_3 b^T + a^T \end{array} \right), \qquad \left(\begin{array}{c} u_3 \alpha^T + \beta^T \\ u_3 \beta^T - \alpha^T \end{array} \right).$$

These matrices, since a, b, as well as α, β are linearly independent, are non-degenerate, provided that -1 is not a square in $\mathbb{F}$. Hence, given $\boldsymbol{u} \in \mathbb{F}^3$, at most one line l_{pq} for each q may be incident to $\boldsymbol{u}$, that is Condition (i) is satisfied at $\boldsymbol{u}$.

The special case of concurrency at infinity, would fix the values of $a \cdot p + \alpha \cdot q$ and $b \cdot p + \beta \cdot q$. (See the discussion in Section 3.1 concerning α-and β-planes.) The same conclusion then follows by linear independence of of a and b, as well as α and β.

Let us check the coplanarity condition (ii) of Theorem 1. Suppose we are in the generic case of planes with equations $\boldsymbol{u} \cdot \boldsymbol{q} = -1$, when $\boldsymbol{\omega} = \boldsymbol{u} \times \boldsymbol{v}$, for some $\boldsymbol{u} \in \mathbb{F}^3$. (Throughout this section the boldface $\boldsymbol{q}$ denotes a variable in $\mathbb{F}^3$, not to be confused with $q \in S$). This means,

$$(33) \qquad \begin{array}{rcl} u_1(b \cdot p - \beta \cdot q) - u_2(a \cdot p - \alpha \cdot q) & = & 1, \\ u_2 v_3 - u_3(b \cdot p - \beta \cdot q) & = & a \cdot p + \alpha \cdot q, \\ -u_1 v_3 + u_3(a \cdot p - \alpha \cdot q) & = & b \cdot p + \beta \cdot q. \end{array}$$

Suppose, both $u_1, u_2 \neq 0$. Then we basically copy the discussion as to the concurrency case. From the last two equations, and using the first one

$$\begin{array}{rl} u_1(b \cdot p - \beta \cdot q) - u_2(a \cdot p - \alpha \cdot q) & = 1, \\ u_1(a \cdot p + \alpha \cdot q) + u_2(b \cdot p + \beta \cdot q) & = -u_3. \end{array}$$

The matrices multiplying p and q are, respectively

$$\left(\begin{array}{c} u_1 b^T - u_2 a^T \\ u_1 a^T + u_2 b^T \end{array} \right), \qquad \left(\begin{array}{c} -u_1 \beta^T + u_2 \alpha^T \\ u_1 \alpha^T + u_2 \beta^T \end{array} \right),$$

Since pairs of vectors a, b and α, β are linearly independent, the two matrices are non-degenerate, given that -1 is not a square in $\mathbb{F}$. Hence for each q, there is a unique p, satisfying these equations and vice versa.

Besides, if, say $u_2 = 0$, then $u_1 \neq 0$, and the first two equations (33) become

$$u_1(b \cdot p - \beta \cdot q) = 1, \qquad a \cdot p + \alpha \cdot q = -\frac{u_3}{u_1}.$$

Hence in both cases, for each variable q, there is a unique p, satisfying equations (33) and vice versa.

We conclude that whenever $\mathbb{F}$ is such that -1 is not a square, that is whenever it is meaningful to speak of positive definite matrices, Condition (ii) of Theorem 1 is satisfied. To be fair, the above consideration has not yet dealt with the special case of co-planarity in the plane through the origin. (See the discussion in Section 3.1 concerning α-and β-planes.) The latter case fixes the values of $a \cdot p - \alpha \cdot q$ and $b \cdot p - \beta \cdot q$. The same conclusion follows by linear independence of a and b, as well as α and β. $\qquad \square$

4.1.2. *Signature* $(1, 1)$ *metric case.* In this case the Plücker vector L_{pq}, assigned to (p, q) via (20) is

$$(34) \quad [a \cdot p + \alpha \cdot q : b \cdot p + \beta \cdot q : 1 : a \cdot p - \alpha \cdot q : -b \cdot p + \beta \cdot q : -(a \cdot p)^2 + (b \cdot p)^2 + (\alpha \cdot q)^2 - (\beta \cdot q)^2].$$

Lemma 4.4. *Conditions (i), (ii) of Theorem 1 may fail at certain points, as well as in certain planes. However, lines l_{pq} and $l_{p'q'}$ are concurrent at such a point or coplanar in such a plane if and only if*

$$(p - p')^T M_1 (p - p') = (q - q')^T M_2 (q - q') = 0.$$

Proof. Since a is not a multiple of b and α is not a multiple of β, the linear forms $L_1, \ldots, L_4$ are linearly independent. We verify conditions (i), (ii) of Theorem 1 only in the case of "generic" α- and β-planes as described in Section 3.1. The special case of concurrency at infinity or co-planarity in a plane $\boldsymbol{u} \cdot \boldsymbol{q} = 0$ through the origin in $\mathbb{F}^3$ follows as in the previous lemma.

Let $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{\omega} = (a \cdot p + \alpha \cdot q, b \cdot p + \beta \cdot q, 1)$, and

$$\boldsymbol{v} = (a \cdot p - \alpha \cdot q, -b \cdot p + \beta \cdot q, -(a \cdot p)^2 + (b \cdot p)^2 + (\alpha \cdot q)^2 - (\beta \cdot q)^2).$$

Suppose, $\boldsymbol{v} = \boldsymbol{u} \times \boldsymbol{\omega}$. This means,

$$
\begin{aligned}
(35) \qquad u_1 &= u_3(a \cdot p + \alpha \cdot q) + b \cdot p - \beta \cdot q, \\
u_2 &= u_3(b \cdot p + \beta \cdot q) + a \cdot p - \alpha \cdot q.
\end{aligned}
$$

The matrices multiplying p and q are, respectively,

$$\begin{pmatrix} u_3 a^T + b^T \\ u_3 b^T + a^T \end{pmatrix}, \qquad \begin{pmatrix} u_3 \alpha^T - \beta^T \\ u_3 \beta^T - \alpha^T \end{pmatrix}.$$

These matrices are degenerate if and only if $u_3 = \pm 1$. Otherwise, for each q, there is a unique p, satisfying the concurrency equations and vice versa, i.e. unless $u_3 = \pm 1$, Condition (i) of Theorem 1 is satisfied at $\boldsymbol{u}$.

If $u_3 = \pm 1$, the equations (35) become

$$
\begin{aligned}
u_1 &= (b \pm a) \cdot p + (\pm \alpha - \beta) \cdot q, \\
u_2 &= (a \pm b) \cdot p + (\pm \beta - \alpha) \cdot q.
\end{aligned}
$$

Suppose, lines l_{pq} and $l_{p'q'}$ both find themselves concurrent at such a point $(u_1, u_2, \pm 1)$. It follows that

$$(a \pm b) \cdot (p - p') = (\alpha \pm \beta)(q - q') = 0.$$

Thus, by Lemma 3.2 the Minkowski distances between p, p', as well as q, q' are zero. The converse is also true by construction and Lemma 3.2: if the latter equation is satisfied, the lines $l_{pq}, l_{p'q'}$ are concurrent at a point with $u_3 = \pm 1$.

Let us check the coplanarity condition (ii) of Theorem 1. Suppose now, $\boldsymbol{\omega} = \boldsymbol{u} \times \boldsymbol{v}$. This means,

$$
\begin{aligned}
(36) \qquad u_1(-b \cdot p + \beta \cdot q) - u_2(a \cdot p - \alpha \cdot q) &= 1, \\
u_2 v_3 - u_3(-b \cdot p + \beta \cdot q) &= a \cdot p + \alpha \cdot q, \\
-u_1 v_3 + u_3(a \cdot p - \alpha \cdot q) &= b \cdot p + \beta \cdot q.
\end{aligned}
$$

If, say $u_2 = 0$, then $u_1 \neq 0$, and the first two equations (33) become

$$u_1(-b \cdot p + \beta \cdot q) = 1, \qquad a \cdot p + \alpha \cdot q = -\frac{u_3}{u_1}.$$

Since the pairs of vectors a, b and α, β are linearly independent, the coplanarity condition in such a plane $\boldsymbol{u} \cdot \boldsymbol{q} = -1$ is satisfied.

Suppose now, both $u_1, u_2 \neq 0$. Then we basically copy the discussion as to the concurrency case. Eliminating the term with v_3 from the last two equations and using the first one

$$
\begin{aligned}
(37) \qquad -u_1(-b \cdot p + \beta \cdot q) + u_2(a \cdot p - \alpha \cdot q) &= -1, \\
u_1(a \cdot p + \alpha \cdot q) + u_2(b \cdot p + \beta \cdot q) &= -u_3.
\end{aligned}
$$

The matrices multiplying p and q are, respectively,

$$\begin{pmatrix} u_1 b^T + u_2 a^T \\ u_1 a^T + u_2 b^T \end{pmatrix}, \qquad \begin{pmatrix} -u_1 \beta^T - u_2 \alpha^T \\ u_1 \alpha^T + u_2 \beta^T \end{pmatrix}.$$

Hence, the coplanarity condition of Theorem 1 may be violated in the plane $\boldsymbol{u} \cdot \boldsymbol{q} = -1$ if only if $u_1 = \pm u_2$.

If $u_1 = \pm u_2 \neq 0$ equation (37) become

$$
\begin{aligned}
(a \pm b) \cdot p - (\alpha \pm \beta) \cdot q &= \tfrac{1}{u_1}, \\
(a \pm b) \cdot p + (\alpha \pm \beta) \cdot q &= -\tfrac{u_3}{u_1}.
\end{aligned}
$$

Suppose, lines l_{pq} and $l_{p'q'}$ both find themselves in such exceptional plane. It follows that

$$
(a \pm b) \cdot (p - p') = (\alpha \pm \beta)(q - q') = 0.
$$

Thus, by Lemma 3.2 the Minkowski distances between p, p', as well as q, q' are zero. The converse is also true by construction and Lemma 3.2: if the latter equation is satisfied, the lines $l_{pq}, l_{p'q'}$ are coplanar in an exceptional plane as above.

$\square$

4.1.3. *Degenerate case.* In this case the Plücker vector, assigned to (p, q) via (20) is

(38) $$ L_{pq} = [a \cdot p : \beta \cdot q : 1 : c \cdot p : \delta \cdot q : -(a \cdot p)(c \cdot p) - (\beta \cdot q)(\delta \cdot q)]. $$

Lemma 4.5. *This case satisfies conditions (i), (ii) of Theorem 1, but for some special points and planes. However, the lines l_{pq} and $l_{p'q'}$ are concurrent at such a point and co-planar in such a plane if and only if $p - p'$ is in a kernel[5] of M_1 and $q - q'$ is in a kernel of M_2.*

Proof. Since a is not a multiple of c and β is not a multiple of δ, the linear forms $L_1, \ldots, L_4$ are linearly independent.

Let us check the concurrency condition (i).

Let $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{\omega} = (a \cdot p, \beta \cdot q, 1)$, and

$$
\boldsymbol{v} = (c \cdot p, \delta \cdot q, -(a \cdot p)(c \cdot p) - (\beta \cdot q)(\delta \cdot q)).
$$

Suppose, we are dealing with the generic concurrency case, that is $\boldsymbol{v} = \boldsymbol{u} \times \boldsymbol{\omega}$. This means,

$$
\begin{aligned}
u_2 - u_3 \beta \cdot q &= c \cdot p, \\
u_3 a \cdot p - u_1 &= \delta \cdot q.
\end{aligned}
$$

There is a unique solution p for every q, and vice versa, except when $u_3 = 0$. In the latter case, given (u_1, u_2), for every (p, q) such that $c \cdot p = u_2$, $\delta \cdot q = -u_1$, the lines l_{pq} can be concurrent at $(u_1, u_2, 0)$. If l_{pq} and $l_{p'q'}$ are concurrent at such point, then $c \cdot (p - p') = \delta \cdot (q - q') = 0$, that is the vector $p - p'$ is in the right kernel of M_1 and $q - q'$ is in the right kernel of M_2. In the case of concurrency at infinity, we fix the values of $a \cdot p$ and $\beta \cdot q$ and therefore come to the same conclusion, only $p - p'$ is now in the left kernel of M_1 and $q - q'$ in the left kernel of M_2.

Let us check the coplanarity condition (ii). Dealing with the special case of planes $\boldsymbol{u} \cdot \boldsymbol{q} = 0$ through the origin in $\mathbb{F}^3$, we fix the values of $c \cdot p$ and $\delta \cdot q$. Two lines l_{pq} and $l_{p'q'}$ are coplanar in such a plane if and only if $c \cdot (p - p') = \delta \cdot (q - q') = 0$, that is $p - p'$ is in the right kernel of M_1 and $q - q'$ is in the right kernel of M_2.

In the generic case of planes $\boldsymbol{u} \cdot \boldsymbol{q} = -1$, suppose $\boldsymbol{\omega} = \boldsymbol{u} \times \boldsymbol{v}$. This means

$$
\begin{aligned}
u_2 v_3 - u_3 \delta \cdot q &= a \cdot p, \\
u_3 c \cdot p - u_1 v_3 &= \beta \cdot q, \\
u_1 \delta \cdot q - u_2 c \cdot p &= 1.
\end{aligned}
$$

Suppose $u_1 = 0$, $u_2 \neq 0$. The equations become $c \cdot p = -\tfrac{1}{u_2}$, $\beta \cdot q = -\tfrac{u_3}{u_2}$, which means Condition (ii) may fail in the plane with the equation $u_2 x_2 + u_3 x_3 = -1$, $u_2 \neq 0$, and every line l_{pq}, such that $c \cdot p = -\tfrac{1}{u_2}$, $\beta \cdot q = -\tfrac{u_3}{u_2}$ lies in this plane.

If l_{pq} and $l_{p'q'}$ are coplanar in such plane, then $c \cdot (p - p') = \beta \cdot (q - q') = 0$, that is $p - p'$ is in the right kernel of M_1 and $q - q'$ is in the left kernel of M_2.

---

[5] We say *a* kernel, since it may be the left or right one. Which one – can bee seen within the proof.

Similarly, we may have exceptional planes with $u_1 \neq 0$, $u_2 = 0$, in which case lines l_{pq} and $l_{p'q'}$ are coplanar in such plane, if and only if $a \cdot (p - p') = \delta \cdot (q - q') = 0$, that is $p - p'$ is in the left kernel of M_1 and $q - q'$ is in the right kernel of M_2.

If both $u_1, u_2 \neq 0$ we get

$$u_1 a \cdot p + u_2 \beta \cdot q + u_1 u_3 \delta \cdot q - u_2 u_3 c \cdot p = 0,$$
$$u_1 \delta \cdot q - u_2 c \cdot p = 1.$$

The matrices, multiplying p and q are, respectively

$$\begin{pmatrix} u_1 a^T - u_2 u_3 c^T \\ -u_2 c^T \end{pmatrix}, \qquad \begin{pmatrix} u_2 \beta^T + u_1 u_3 \delta^T \\ u_1 \delta^T \end{pmatrix},$$

and are both non-singular, which means, the coplanarity condition of Theorem 1 is satisfied. $\qquad \square$

4.1.4. *Directions case.* In this final case we deal with Plücker vectors as follows:

$$(39) \qquad L_{pq} = [a \cdot p : b \cdot p : 1 : \lambda b_1 q_1 + b_2 q_2 : -\lambda a_1 q_1 - a_2 q_2 : (p_1 q_2 - \lambda p_2 q_1)(a_2 b_1 - a_1 b_2)].$$

Lemma 4.6. *The concurrency condition (i) of Theorem 1 is satisfied. The co-planarity condition (ii) is satisfied if and only if the point set S has $O(\sqrt{N})$ points on any straight line.*

Proof. Since a is not a multiple of b and λ, $a_2 b_1 - a_1 b_2 \neq 0$, the linear forms $L_1, \ldots, L_4$ are linearly independent. Moreover, the concurrency condition at infinity fixes the values of $a \cdot p$ and $b \cdot p$ and is therefore satisfied.

Let us check the concurrency condition (i) at a point in $\boldsymbol{u} \in \mathbb{F}^3$.

Let $\boldsymbol{u} = (u_1, u_2, u_3)$, $\boldsymbol{\omega} = (a \cdot p, b \cdot p, 1)$, and

$$\boldsymbol{v} = (\lambda b_1 q_1 + b_2 q_2, -\lambda a_1 q_1 - a_2 q_2, (p_1 q_2 - \lambda p_2 q_1)(a_2 b_1 - a_1 b_2)).$$

Suppose, $\boldsymbol{v} = \boldsymbol{u} \times \boldsymbol{\omega}$. This means,

$$u_2 - u_3 b \cdot p = \lambda b_1 q_1 + b_2 q_2,$$
$$u_3 a \cdot p - u_1 = -\lambda a_1 q_1 - a_2 q_2.$$

The matrix multiplying q is non-degenerate. Thus Condition (i) of Theorem 1 is satisfied: given $\boldsymbol{u}$ and p there is a unique q satisfying these equations.

Let us check the coplanarity condition (ii). Dealing with planes $\boldsymbol{u} \cdot \boldsymbol{q} = 0$ through the origin in $\mathbb{F}^3$ means fixing the values $\lambda b_1 q_1 + b_2 q_2$ and $-\lambda a_1 q_1 - a_2 q_2$, that is fixes q. Thus Condition (ii) is satisfied in these planes.

Suppose $\boldsymbol{\omega} = \boldsymbol{u} \times \boldsymbol{v}$. This means

$$u_2 v_3 + u_3(\lambda a_1 q_1 + a_2 q_2) = a \cdot p,$$
$$u_3(\lambda b_1 q_1 + b_2 q_2) - u_1 v_3 = b \cdot p,$$
$$-u_1(\lambda a_1 q_1 + a_2 q_2) - u_2(\lambda b_1 q_1 + b_2 q_2) = 1.$$

Suppose $u_1 = 0$, $u_2 \neq 0$. The equations become $\lambda b_1 q_1 + b_2 q_2 = -\frac{1}{u_2}$, $b \cdot p = -\frac{u_3}{u_2}$, which means Condition (ii) fails in the plane with the equation $u_2 x_2 + u_3 x_3 = -1$, $u_2 \neq 0$, and every line l_{pq}, such that $b \cdot p = -\frac{u_3}{u_2}$, $\lambda b_1 q_1 + b_2 q_2 = -\frac{1}{u_2}$ lies in this plane. The number of such lines l_{pq} will be $O(N)$ if the point set S has $O(\sqrt{N})$ points on each line in the corresponding two families of parallel lines.

Similarly, one deals with the case $u_1 = 0$, $u_2 \neq 0$.

If both $u_1, u_2 \neq 0$ we get

$$u_1 u_3(\lambda a_1 q_1 + a_2 q_2) - u_1 a \cdot p + u_2 u_3(\lambda b_1 q_1 + b_2 q_2) - u_2 b \cdot p = 0,$$
$$-u_1(\lambda a_1 q_1 + a_2 q_2) - u_2(\lambda b_1 q_1 + b_2 q_2) = 1.$$

If $u_3 = 0$, Condition (ii) fails and any line l_{pq}, such that $(u_1 a + u_2 b) \cdot p = 0$ as well as $q_1 \lambda (u_1 a_1 + u_2 b_1) + q_2 (u_1 a_2 + u_2 b_2) = -1$. Hence we conclude that Condition (ii) will be satisfied if and only if the point set S has $O(\sqrt{N})$ points on *any* straight line.

We finally note that if none of the u_1, u_2, u_3 is zero, Condition (ii) is satisfied, for then both p and q in the latter set of two equations are multiplied by non-degenerate matrices. □

4.2. **Conclusion of proofs of Theorems 3-5.** Theorem 3 in the positive definite case and Theorem 5 follow immediately by Theorem 1, since the families of lines $\{l_{pq}\}$ in $\mathbb{R}^3$, defined via the map (20) as (32) and (39) satisfy all its conditions, by Lemmas 3.1, 4.3, and 4.6.

As for Theorem 3 in the signature $(1, 1)$ case, as well as Theorem 4 we act as follows. One can choose two subsets S_1 and S_2 of S, with, say at least $\frac{N}{16}$ elements each, such that for any $(p, p') \in S_1 \times S_2$, neither $(p - p')^T M_1 (p - p')$, nor $(p - p')^T M_2 (p - p')$ equals zero. Define two families of lines

$$L_j = \{l_{pq}\}_{p,q \in S_j}, \qquad j = 1, 2.$$

Apply Theorem 1′, whose conditions are satisfied by Lemmas 4.4, 4.5, respectively as to the Minkowski/degenerate cases. It follows that the equation

$$(p - p')^T M_1 (p - p') = (q - q')^T M_2 (q - q'), \qquad (p, q) \in S_1 \times S_1, \ (p', q') \in S_2 \times S_2$$

has $O(N^3 \log N)$ solutions. Note that the values of the matrix products involved, by the assumptions on S_1, S_2 are nonzero.

One can make $O(1)$ choices of the pair of positive proportion subsets (S_1^i, S_2^i) of S, with $i = 1, \ldots, K = O(1)$, such that whenever

$$(p - p')^T M_1 (p - p') = (q - q')^T M_2 (q - q') \neq 0, \qquad (p, q) \in S \times S, \ (p', q') \in S \times S,$$

then for some $i = 1, \ldots, K$,

$$(p - p')^T M_1 (p - p') = (q - q')^T M_2 (q - q'), \qquad (p, q) \in S_1^i \times S_1^i, \ (p', q') \in S_2^i \times S_2^i.$$

But for the pair of sets S_1^i, S_2^i Theorem 1′ applies as above, and $K = O(1)$. This completes the proof of Theorems 3, 4. □

APPENDIX. DERIVATION OF (16) VIA ELEKES-SHARIR FRAMEWORK

Here we show that in the case $S \subset \mathbb{S}^2$, the line l_{pq}, that is the point in the Klein quadric, arising from the condition (16), is indeed the set of $SO(3)$ symmetries taking $\boldsymbol{p}$ to $\boldsymbol{q}$. We use the Clifford algebra representation of $SO(3)$, whose manifold is $\mathbb{FP}^3$.

Traditionally rotations about a point in three dimensions were represented by unit quaternions. Clifford algebras generalise quaternions. See [8] for their applications in kinematics. The appropriate Clifford algebra to use here is $Cl(3, 0)$. The algebra has 3 generators e_1, e_2 and e_3. These generators anti-commute: $e_i e_j = -e_j e_i$ if $i \neq j$ and they all square to 1.

In this algebra points $\boldsymbol{p} = (p_1, p_2, p_3)$ on the two-sphere can be represented by grade 1 elements of the form

$$(40) \qquad p = p_1 e_1 + p_2 e_2 + p_3 e_3.$$

(We do not use boldface notation for Clifford algebra elements.) The Clifford conjugate of such an element is given by $p^- = -p$, so that

$$pp^- = -(p_1^2 + p_2^2 + p_3^2),$$

and for points on the two-sphere this will be constant.

The spin group in this Clifford algebra lies in the even sub-algebra. A general element of $Spin(3)$ is given as

$$\tilde{g} = s_0 + s_1 e_2 e_3 + s_2 e_1 e_3 + s_3 e_1 e_2, \tag{41}$$

subject to the relation

$$\tilde{g}\tilde{g}^- = s_0^2 + s_1^2 + s_2^2 + s_3^2 = 1,$$

where the Clifford conjugate on a grade 2 element is given by $(e_i e_j)^- = -e_i e_j$, $i \neq j$. The quaternion algebra arises by replacing $e_2 e_3 \to i$, $e_1 e_3 \to j$, $e_1 e_2 \to k$. The group manifold of $Spin(3)$ is thus the three-sphere $\mathbb{S}^3$. The action of this group on points $\boldsymbol{p} \in \mathbb{S}^2$ is given by conjugation of the corresponding grade 1 element p in the Clifford algebra, as follows:

$$g \circ p = \tilde{g} p \tilde{g}^-.$$

It is easy to see that this action preserves the square of the distance pp^- of the point from the origin.

The group $Spin(3)$ double covers the rotation group $SO(3)$, for $\tilde{g}$ and $-\tilde{g}$ give the same rotation about the origin. To avoid this, we can take the parameters $s_0, ..., s_3$ in (41) as homogeneous coordinates in a 3-dimensional projective space $\mathbb{FP}^3$, rather than on $\mathbb{S}^3$. This establishes a one-to-one correspondence between elements of $SO(3)$ and points in $\mathbb{FP}^3$. Notation-wise, to make a difference between $SO(3)$ and its double cover $Spin(3)$, an element of the group $SO(3)$ will be written in the following as

$$g = s_0 + s_1 e_2 e_3 + s_2 e_3 e_1 + s_3 e_1 e_2,$$

that is the tilde will be dropped, meaning that the parameters $(s_0 : s_1 : s_2 : s_3)$ are now homogeneous coordinates. So $gg^- \in \mathbb{F} \setminus 0$. The action of the group on $\mathbb{S}^2$ must also be changed slightly. Rather than (40) points on $\mathbb{S}^2$ will be represented by a quadric in homogeneous coordinates. Consider elements of $\mathbb{FP}^3$ given by $(p_0 : p_1 : p_2 : p_3)$. Now represent these points in the Clifford algebra as

$$p = p_0 + p_1 e_1 + p_2 e_2 + p_3 e_3.$$

So

$$pp^- = p_0^2 - p_1^2 - p_2^2 - p_3^2,$$

and hence p_0 has the meaning of the radius of a sphere, centred at the origin, given that the corresponding elements p in the Clifford algebra satisfy $pp^- = 0$. If $g \in SO(3)$ then the action of g on the sphere can still be written as

$$g \circ p = gpg^-.$$

Now, consider the set of elements of $SO(3)$ which transform a point $\boldsymbol{p} = (p_1, p_2, p_3)$ to a point $\boldsymbol{q} = (q_1, q_2, q_3)$ on the two-sphere. The Clifford algebra representations p, q will satisfy the latter Clifford algebra equation, i.e.,

$$gpg^- = q \qquad \Rightarrow \qquad gp - qg = 0.$$

This gives four linear equations in the quantities $(s_0 : s_1 : s_2 : s_3)$ by equating the coefficients of the basis elements e_1, e_2, e_3 and $e_1 e_2 e_3$. However, only two of the equations are independent and hence we have a line of solutions. That is the set of $SO(3)$-elements transforming $\boldsymbol{p}$ to $\boldsymbol{q}$ on $\mathbb{S}^2$ is a line in $\mathbb{FP}^3$.

This line can be parameterised in several ways. E.g., any rotation that moves $\boldsymbol{p}$ to a non-antipodal $\boldsymbol{q}$ can be decomposed as a rotation about $\boldsymbol{p}$ followed by a rotation by the angle π about the line in the plane of $\boldsymbol{p}$ and $\boldsymbol{q}$ which bisects the two vectors. In the Clifford algebra this can be written as,

$$g = [(p_1 + q_1)e_2 e_3 + (p_2 + q_2)e_3 e_1 + (p_3 + q_3)e_1 e_2][c + s(p_1 e_2 e_3 + p_2 e_1 e_3 + p_3 e_1 e_2)], \tag{42}$$

where c and s can be thought of as homogeneous parameters or the first column of a $SO(2)$ matrix, that is $c = \cos \theta/2$ and $s = \sin \theta/2$, θ being the angle of rotation about $\boldsymbol{p}$.

Passing from equation (42) to Plücker coordinates is a short calculation by formula (8), where the two points on the line one uses for passing to Plücker coordinates via (8) can be taken, for instance, as $(c, s) = (1, 0)$ and $(0, 1)$. The result is precisely (16), where the common factor,

$$(p_1^2 + p_2^2 + p_3^2) + (p_1 q_1 + p_2 q_2 + p_3 q_3) = (q_1^2 + q_2^2 + q_3^2) + (p_1 q_1 + p_2 q_2 + p_3 q_3)$$

has been cancelled from homogeneous Plücker coordinates. We leave the special case of antipodal $\boldsymbol{p}$ and $\boldsymbol{q}$ to the reader.

References

[1] J.W. Cannon, W.J. Floyd, R. Kenyon and W.R. Parry. *Hyperbolic Geometry.* In *Flavors of Geometry,* MSRI Publications, Volume **31**, 1997, 59–115.

[2] G. Elekes, M. Sharir. *Incidences in three dimensions and distinct distances in the plane.* Proceedings 26th ACM Symposium on Computational Geometry (2010), 413–422.

[3] K. Ford. *The distribution of integers with a divisor in a given interval.* Annals of Math., **168** (2008), 367–433.

[4] L. Guth, N. H. Katz. *On the Erdős distinct distance problem in the plane.* Ann. of Math. (2) **181** (2015), no. 1, 155–190.

[5] H. Pottmann and J. Wallner. *Computational line geometry.* Paperback edition. Mathematics and Visualization. Springer-Verlag, Berlin, 2010. 563 pp.

[6] O. Roche-Newton. *A Short proof of a near-optimal cardinality estimate for the product of a sum set.* 31st International Symposium on Computational Geometry, 74–80, LIPIcs. Leibniz Int. Proc. Inform., 34, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2015.

[7] O. Roche-Newton and M. Rudnev. *On the Minkowski distances and products of sum sets.* Israel J. Math. **209**(2015), no. 2, 507–526.

[8] J.M. Selig. *Geometric Fundamentals of Robotics.* Monographs in Computer Science. Springer, 2007, 416 pp.

[9] P. Ungar. *2N Noncollinear points determine at least 2N directions.* J. Combin. Th. A **33**, no 3 (1982), 343–347.

Misha Rudnev, Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom
E-mail address: `m.rudnev@bristol.ac.uk`

J. M. Selig, Faculty of Business, London South Bank University, 103 Borough Road, London SE1 0AA, United Kingdom
E-mail address: `seligjm@lsbu.ac.uk`