ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2018, Vol. 303, pp. 129–139. © Pleiades Publishing, Ltd., 2018.
Published in Russian in Trudy Matematicheskogo Instituta imeni V.A. Steklova, 2018, Vol. 303, pp. 142–154.

Finite Point Configurations in the Plane, Rigidity and Erdős Problems

A. Iosevich[a] and J. Passant[a]

Received June 1, 2018

Abstract—For a finite point set $E \subset \mathbb{R}^d$ and a connected graph G on $k+1$ vertices, we define a G-framework to be a collection of $k+1$ points in E such that the distance between a pair of points is specified if the corresponding vertices of G are connected by an edge. We consider two frameworks the same if the specified edge-distances are the same. We find tight bounds on such distinct-distance drawings for rigid graphs in the plane, deploying the celebrated result of Guth and Katz. We introduce a congruence relation on a wider set of graphs, which behaves nicely in both the real-discrete and continuous settings. We provide a sharp bound on the number of such congruence classes. We then make a conjecture that the tight bound on rigid graphs should apply to all graphs. This appears to be a hard problem even in the case of the nonrigid 2-chain. However, we provide evidence to support the conjecture by demonstrating that if the Erdős pinned-distance conjecture holds in dimension d, then the result for all graphs in dimension d follows.

DOI: 10.1134/S0081543818080114

1. INTRODUCTION

Given a set E in $\mathbb{R}^d$, the distance set of E is

$$\Delta_d(E) = \{|x-y|\colon\ x, y \in E\} \subseteq \mathbb{R}.$$

In [8] Erdős posed the following question: What is the minimal number of distinct distances determined by a finite point set E in $\mathbb{R}^d$? This has been thoroughly studied in the $d=2$ case, with the cascade of improvements to Erdős's original $|E|^{1/2}$ by authors including Moser [12], Chung [5], Chung, Szemerédi and Trotter [6], Székely [17], Solymosi and Tóth [14] and Tardos [18] and, most recently, the solution of the problem due to Guth and Katz [10]. In higher dimensions, a simple variant of Erdős's original argument gives $|E|^{1/d}$ in dimension d. An improvement in three dimensions due to Clarkson, Edelsbrunner, Guibas, Sharir and Welzl [7] proved that one obtains at least $|E|^{1/2}$ distances. The three-dimensional bound was furthered by Aronov, Pach, Sharir and Tardos [1], who also proved a small improvement over the $|E|^{1/d}$ bound in dimension d. This was then improved significantly by Solymosi and Vu [16] (see also [15]), who proved that one obtains at least $|E|^{2/d-2/(d(d+2))}$ distances, a near optimal bound for large dimensions.

The study of distance sets may be viewed as the study of congruence classes of two-point configurations. If we consider a pair of points x, y and another pair x', y', then there exists a rigid motion T such that $Tx = x'$ and $Ty = y'$ if and only if $|x-y| = |x'-y'|$. A similar question can be asked about configurations involving more points. In this paper we will consider $(k+1)$-point configurations. Suppose that $k \le d$ and let $x^1, x^2, \dots, x^{k+1}$ be linearly independent. Also assume that $y^1, y^2, \dots, y^{k+1}$ are linearly independent. Then the question of whether the two collections are congruent, i.e., whether there exists a rigid motion T such that $y^j = Tx^j$, $1 \le j \le k+1$, reduces to checking whether $|x^i - x^j| = |y^i - y^j|$ for all $1 \le i < j \le k+1$.

[a] Department of Mathematics, University of Rochester, Rochester, NY 14627, USA.
E-mail addresses: iosevich@math.rochester.edu (A. Iosevich), jpassant@ur.rochester.edu (J. Passant).

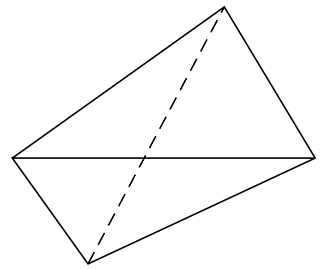

Fig. 1. $d = 2$ and $k = 3$.

In the situation when $k > d$, significant new complications arise. Mainly that without further assumptions on the structure of the distances provided we cannot guarantee that a rigid motion exists. Consider a four-point configuration in the plane determined by side lengths 3, 1, 1 and 1; here we already see multiple issues. There is sufficient flexibility to fix one edge and, by perturbing the nonfixed points by small motions, give infinite realizations of the quadrilateral. There is no hope of having a nice rigid map between such realizations. This particular issue can be solved by specifying enough edges to restrict the flexibility to a finite number of realizations dependent on k and d (the best one can hope for).

As a simple example, consider Fig. 1. The length of the dashed line is determined by the lengths of the five solid lines. The natural dimension of the configuration space, in the sense that will be made precise, is 5; i.e., we need five specified distances between our four points to guarantee we have a rigid motion.

In general, the following heuristic is extremely useful in understanding the situation. Each of the $k+1$ points of our point set has d coordinates. The dimension of the Euclidean motion group in $\mathbb{R}^d$ is equal to d plus the dimension of the orthogonal group. This gives the dimension of the configuration space as

$$d(k+1) - d - \binom{d}{2} = d(k+1) - \binom{d+1}{2} < \binom{k+1}{2}.$$

So we can specify enough of the distances to rigidify our $k+1$ point configuration. This is where we follow the approach of [4, 13]. To do this, we need to introduce minimal infinitesimal rigidity, which allows us to bound the number of realizations and provides the necessary rigid motion. For motivation on minimal infinitesimal rigidity, see [2, 9].

We now turn to precise definitions and statements of results. Given a finite set $E \subset \mathbb{R}^d$ of size $> k+1$, we consider $(k+1)$-tuples of vectors in E where the first $d+1$ vectors are affinely independent. We will refer to such $(k+1)$-tuples as nonsingular.

We say that two nonsingular $(k+1)$-tuples $x^1, x^2, \ldots, x^{k+1}$ and $y^1, y^2, \ldots, y^{k+1}$ are congruent if there exists a rotation θ and a translation τ such that

$$y^j = \theta x^j + \tau \qquad \text{for all } j.$$

Let $M_d(k)(\mathbb{R}^d)$ denote the set of the resulting equivalence classes. Let $M_d(k)(E)$ denote the set of resulting equivalence classes where the vectors are restricted to a finite point set E.

Theorem 1.1. *Let E be a finite point set in $\mathbb{R}^2$. Then*

$$|M_2(k)(E)| \gtrsim |E|^k;$$

here and throughout, $\gtrsim$ is used to suppress some constant independent of the controlling parameter.

Moreover, the lower bound is, in general, best possible.

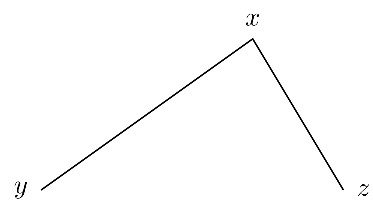

Fig. 2. The hinge.

We could state a higher dimensional version of Theorem 1.1, but it would not be sharp, because our argument relies to a significant extent on the case $k=1$, where the needed bound is only known in two dimensions.

We now deal with point configurations where distances between some pairs of points are specified and others are not. An interesting and deceptively looking example is provided by the hinge (Fig. 2). More precisely, it is reasonable to ask, if E is a finite subset of $\mathbb{R}^2$, whether

$$\bigl|\bigl\{(|x-y|,|x-z|)\colon\ x,y,z\in E\bigr\}\bigr| \gtrapprox |E|^2; \tag{1.1}$$

here and throughout, $X \lessapprox Y$ with a controlling parameter R means that given $\epsilon>0$ there exists $C_\epsilon>0$ such that $X\le C_\epsilon R^\epsilon Y$.

We can gain a nonoptimal bound on the hinge (and, as we will later state, general nonrigid configurations) using pinned-distance bounds. One defines pinned distance in the plane as

$$\Delta_x(E)=\{|x-y|\colon\ y\in E\}$$

for a pin $x\in E$. The best known pinned result for the Erdős distance problem is due to Katz and Tardos [11]. They proved that there exists $x\in E$ such that

$$|\Delta_x(E)| \gtrapprox |E|^{(48-14e)/(55-16e)}. \tag{1.2}$$

It follows that

$$\bigl|\bigl\{(|x-y|,|x-z|)\colon\ x,y,z\in E\bigr\}\bigr| \gtrapprox |E|^{2(48-14e)/(55-16e)}.$$

Taking $E=\mathbb{Z}^2\cap[0,\sqrt{n}\,]^2$ shows that estimate (1.1) would be best possible. While this question looks like a natural variant of the Erdős distance conjecture, it appears to be very difficult. In order to study configurations of this type, we need to build a geometric mechanism for point configurations with distance relations encoded by combinatorial graphs. This is where we now turn our attention. The main theorem resulting from this machinery is Theorem 1.20 below.

1.1. Graph rigidity. To gain sharp bounds on the size of individual congruence classes in the plane, we require more structure on these finite point configurations. To do so, we encode finite point frameworks using combinatorial graphs. We use these graphs to introduce a formal notion of rigidity (minimal infinitesimal rigidity) which allows for an Elekes–Sharir-group-action type argument to be set up.

Let $k\ge 1$ and let K_{k+1} denote the complete graph with vertex set $\{1,\dots,k+1\}$ and edge set ordered lexicographically. Let $G_{k+1,m}$ be a subgraph of K_{k+1} with $k+1$ vertices and m edges inheriting the order.

Definition 1.2. A $(k+1)$-*tuple* $\boldsymbol{x}$ *in* $\mathbb{R}^d$ is a tuple

$$\boldsymbol{x}=(x^1,x^2,\dots,x^{k+1}),\qquad x^j\in\mathbb{R}^d.$$

Definition 1.3. A *framework of* $G_{k+1,m}$ *in* $\mathbb{R}^d$ is a pair $(G_{k+1,m},\boldsymbol{x})$, where $\boldsymbol{x}$ is a $(k+1)$-tuple in $\mathbb{R}^d$.

A convenient way to specify distances is through the distance function which we now define.

Definition 1.4. Given a graph $G_{k+1,m}$, we define the *distance function* $f_{G_{k+1,m}}(\boldsymbol{x})$ on $\boldsymbol{x} = (x^1,\dots,x^{k+1}) \in \mathbb{R}^{d(k+1)}$ by

$$f_{G_{k+1,m}}(\boldsymbol{x}) = \big(|x^i - x^j|\big)_{ij\in G_{k+1,m}}.$$

We also define the *distance-squared function* $F_{G_{k+1,m}}(\boldsymbol{x})$ by

$$F_{G_{k+1,m}}(\boldsymbol{x}) = \big(|x^i - x^j|^2\big)_{ij\in G_{k+1,m}}.$$

Definition 1.5 (graph distances)**.** The value $f_{G_{k+1,m}}(\boldsymbol{x})$ is called the $G_{k+1,m}$*-distance of* $\boldsymbol{x}$. When we restrict our domain to some set $\mathfrak{X} \subseteq \mathbb{R}^{d(k+1)}$, we call $f_{G_{k+1,m}}(\boldsymbol{x})$ a $G_{k+1,m}$*-distance on* $\mathfrak{X}$ and we say that $\boldsymbol{x}$ is a realization of this distance in $\mathfrak{X}$. The set of $G_{k+1,m}$-distances on $\mathfrak{X}$ is $f_{G_{k+1,m}}(\mathfrak{X})$, and we denote it by $\Delta(G_{k+1,m},\mathfrak{X})$.

Remark 1.6. The distance set $\Delta(G_{k+1,m},\mathfrak{X})$ depends on the numbering of the vertices and the order of the edges. Whereas the order of the edges is superficial, inducing only a permutation in the components of the $G_{k+1,m}$-distances, the numbering of the vertices can significantly change the $G_{k+1,m}$-distance set. Consider $\mathfrak{X} = \{\boldsymbol{x}_0\}\times\mathbb{R}^d\times\ldots\times\mathbb{R}^d$ and a graph $G = G'\cup G''\cup\{e\}$ where e is a bridge between G' and G''. Then if we number the vertices of G' followed by those of G'', we essentially capture G''-distances only, whereas if we reverse the numbering order of the vertices of G, we will capture G'-distances only. In the rest of this paper we take $\mathfrak{X} = E^{k+1}$ for some finite $E\subset\mathbb{R}^d$, so that the numbering of the vertices becomes superficial as well. In particular, the size of the $G_{k+1,m}$-distance set is independent of the vertex numbering and edge order.

We consider the following conjecture.

Conjecture 1.7. *Let E be a finite set in the plane of size n and $G_{k+1,m}$ be a connected graph on $k+1$ vertices having m edges. Then,* $|\Delta(G_{k+1,m},E^{k+1})| \gtrapprox n^k$.

Theorem 1.8. *Conjecture* 1.7 *is sharp.*

Our main results here concern the size of the set $\Delta(G_{k+1,m},E^{k+1})$. An important role is played by properties of the graph $G_{k+1,m}$. In particular, it is essential whether the graph is rigid or not.

The key heuristic notion of this paper is that a graph $G_{k+1,m}$ is *rigid in* $\mathbb{R}^d$ if once the m quantities t_{ij} in

$$|x^i - x^j| = t_{ij}, \qquad ij\in G_{k+1,m},$$

are specified, the other distances $|x^i - x^j|$ for $ij\notin G_{k+1,m}$ can only take finitely many values as the frameworks $(G_{k+1,m},\boldsymbol{x})$ vary over the set of nondegenerate frameworks (see generic frameworks below for a formal definition of this nondegeneracy).

For technical reasons, we use a more precise and flexible notion of rigidity described below. A simple example that illustrates the technical obstacles one must contend with is the following. Consider a quadrilateral in the plane with side-lengths 1, 1, 1 and 3. This configuration is perfectly rigid in the heuristic sense, but it is not *minimally infinitesimally rigid*, as the reader will see, roughly because the rigidity in this case is not stable under small perturbations.

We now turn to precise definition.

Definition 1.9. An *infinitesimal motion* $\boldsymbol{u} = (u^1,\dots,u^{k+1})$ *in* $\mathbb{R}^d$ *of* $G_{k+1,m}$ *at* $\boldsymbol{x}$ is a $(k+1)$-tuple $\boldsymbol{u}$ of vectors $u^j\in\mathbb{R}^d$ such that

$$DF_{G_{k+1,m}}(\boldsymbol{x})\cdot\boldsymbol{u} = 0.$$

The set of infinitesimal motions in $\mathbb{R}^d$ of $G_{k+1,m}$ at $\boldsymbol{x}$ is the kernel of $DF_{G_{k+1,m}}(\boldsymbol{x})$. Let us denote by $\mathcal{V}(G_{k+1,m},\boldsymbol{x})$ the set of infinitesimal motions in $\mathbb{R}^d$ of $G_{k+1,m}$ at $\boldsymbol{x}$. Let $\mathcal{D}(\boldsymbol{x})$ be the set of infinitesimal motions in $\mathbb{R}^d$ of K_{k+1} at $\boldsymbol{x}$.

Remark 1.10. It is evident that $\mathcal{D}(\boldsymbol{x}) \subseteq \mathcal{V}(G_{k+1,m}, \boldsymbol{x})$, because the system of equations $DF_{G_{k+1,m}}(\boldsymbol{x}) \cdot \boldsymbol{u} = 0$ is included in $DF_{K_{k+1}}(\boldsymbol{x}) \cdot \boldsymbol{u} = 0$.

Definition 1.11. A framework $(G_{k+1,m}, \boldsymbol{x})$ is said to be *infinitesimally rigid in* $\mathbb{R}^d$ when $\mathcal{V}(G_{k+1,m}, \boldsymbol{x}) = \mathcal{D}(\boldsymbol{x})$.

It is unnecessarily restrictive to require of a graph that all its frameworks be infinitesimally rigid. We will only require it of a certain family of frameworks which we call generic frameworks. Below we define the set of generic tuples as the complement of the zero set of a certain polynomial. This notion is independent of the graph $G_{k+1,m}$, depending only on the dimension d and the number of vertices $k+1$.

We also define the notion of independence for subsets of the edge set of K_{k+1} and of maximal independence for subsets of the edge set of $G_{k+1,m}$.

Let us use the following notation for our matrices: If a_{ij} is a matrix, $(i,j) \in I \times J$, then for $B \subseteq I$ and $C \subseteq J$ we define $a_{B,C}$ to be the submatrix a_{ij} with $(i,j) \in B \times C$.

Definition 1.12. We say that $\boldsymbol{x} \in \mathbb{R}^{d(k+1)}$ is a *regular tuple of* $F_{G_{k+1,m}}$ if $\operatorname{rank} DF_{G_{k+1,m}}$ attains its global maximum at $\boldsymbol{x}$. A framework $(G_{k+1,m}, \boldsymbol{x})$ is a *regular framework* if $\boldsymbol{x}$ is a regular tuple of $F_{G_{k+1,m}}$.

Definition 1.13. A subset H of the edge set of K_{k+1} is called *independent in* $\mathbb{R}^d$ *with respect to* $\boldsymbol{x}_0 \in \mathbb{R}^{d(k+1)}$ if the row vectors of $DF_{K_{k+1}}(\boldsymbol{x}_0)$ corresponding to H are linearly independent. We call H *independent in* $\mathbb{R}^d$ if there exists some $\boldsymbol{x}_0$ so that H is independent with respect to $\boldsymbol{x}_0$, and $\boldsymbol{x}_0$ is said to be a *witness to the independence of* H. We also call H a *maximally independent* (*in* $\mathbb{R}^d$) *subset of edges of* $G_{k+1,m}$ when it is independent and it is not contained in a larger independent edge set of $G_{k+1,m}$.

Definition 1.14. For any nonempty independent (in $\mathbb{R}^d$) set H of edges of K_{k+1}, we define the polynomial $P_H(\boldsymbol{x})$ to be the sum of squares of $|H| \times |H|$ minors of the submatrix of rows of $DF_{K_{k+1}}$ corresponding to edges of H. Thus,

$$P_H(\boldsymbol{x}) = \sum_{\substack{A \subset \{1,\dots,d(k+1)\} \\ |A| = |H|}} \left|\det(DF_{K_{k+1}}(\boldsymbol{x})_{H,A})\right|^2.$$

Let X_H denote the zero set of P_H.

We define the set of *generic tuples of* $\mathbb{R}^d$ to be the complement of the zero set X of the polynomial $P(\boldsymbol{x})$ defined by

$$P(\boldsymbol{x}) = \prod_{H \text{ independent}} P_H(\boldsymbol{x}).$$

We call X the set of *critical tuples of* $\mathbb{R}^d$.

Remark 1.15. We have $X = \bigcup_H X_H$, where the union is taken over all the edge sets H which are independent, and the generic tuples are then equal to $\mathbb{R}^{d(k+1)} \setminus X$. Moreover, if a set H of edges is independent, then by Definition 1.14 it is generically independent, i.e., independent with respect to any generic $\boldsymbol{x}$. In fact, the set of generic tuples is precisely the set of tuples that simultaneously witness the independence of every independent edge set.

Remark 1.16. The polynomial $P(\boldsymbol{x})$ is nontrivial, because every P_H is nontrivial, since there is at least one witness $\boldsymbol{x}_H$ for the independence of H, which means that $P_H(\boldsymbol{x}_H) \neq 0$. Thus X is a proper algebraic variety of dimension

$$\dim X \leq d(k+1) - 1. \tag{1.3}$$

Remark 1.17. It is immediate from the definitions that generic tuples are regular tuples. The other implication does not hold in general.

Definition 1.18. A framework $(G_{k+1,m}, \boldsymbol{x})$ is called *generic in* $\mathbb{R}^d$ if $\boldsymbol{x}$ is a generic tuple in $\mathbb{R}^d$, and it is called *critical in* $\mathbb{R}^d$ if $\boldsymbol{x}$ is a critical tuple in $\mathbb{R}^d$.

Using the definitions above, we can define minimally infinitesimally rigid graphs; this is the formal notion of rigidity we will exploit to gain sharp results.

Definition 1.19. A graph $G_{k+1,m}$ is called *infinitesimally rigid in* $\mathbb{R}^d$ if all its generic frameworks are infinitesimally rigid. It is called *minimally infinitesimally rigid in* $\mathbb{R}^d$ if it is infinitesimally rigid and no proper subgraph (on the same vertex set) is infinitesimally rigid.

Using the notion of minimal infinitesimal rigidity, we can gain sharp results for many graphs.

Theorem 1.20. *Let $G_{k+1,m}$ be a minimally infinitesimally rigid connected graph on $k+1$ vertices having m edges and E be a point set in $\mathbb{R}^2$ of size n. Then,*

$$|\Delta(G_{k+1,m}, E^{k+1})| \gtrapprox n^k.$$

This result is proved very quickly using two very helpful results from [4]. The first of these gives a bound on the number of distinct geometric forms of configurations obtained by specifying distances dependent on only k and d. For example, triangles with edges specified can have four different geometric forms where we can only use reflections to map one type to another. The bound on these allows us to focus on the richest of such cases.

The second key result of minimal infinitesimal rigidity in [4] is the fact that two configurations (with the same geometric form) have a rigid motion that takes one to another. This allows us to reduce the above to the result of Guth and Katz.

1.2. Erdős's pinned-distance conjecture.

Our final result allows us to drop the condition that our graph $G_{k+1,m}$ needs to be rigid. We do this by evoking Erdős's pinned-distance conjecture. As stated earlier, the current best known result is (1.2) due to Katz and Tardos [11]. The established conjecture is the following.

Conjecture 1.21. *For a finite point set E in $\mathbb{R}^d$ there is a point y in E such that $|\Delta_y(E)| \approx |E|^{2/d}$.*

It is clear, by considering the integer lattice, that the above conjecture is the best one can hope for. With our current technology we are far from this sharp result; however, we will demonstrate that the general graph distances result is a closely linked, though weaker, result.

Theorem 1.22. *Conjecture* 1.7 *holds for any $G_{k+1,m}$ if the pinned-distance conjecture is assumed.*

2. PROOF OF THEOREM 1.1

We begin by deriving the properties of $M_d(k)(\mathbb{R}^d)$ that we will need in the proof.

2.1. Congruence classes of $(k+1)$-tuples.

In this subsection we build a congruence relation—using the action of the orthogonal group—to provide a more general class of configurations where we can gain sharp results on distance tuples.

A $(k+1)$-point configuration in $\mathbb{R}^d$ is given by an arbitrary choice of a point in $\mathbb{R}^{d(k+1)}$. We label this configuration as $(v_0, \dots, v_k)$ with $v_j \in \mathbb{R}^d$ initially.

Recall, $k \geq d$ is assumed and we say that the configuration above is nonsingular if its first $d+1$ vectors $\{v_0, \dots, v_d\}$ are affinely independent.

We denote the space of these nonsingular $(k+1)$-point configurations in $\mathbb{R}^d$ by $N_d(k)$.

Step 1: *Passage to origin-pinned configurations.* Given a nonsingular configuration $(v_0,\dots,v_k)$, we define the associated origin-pinned configuration as $(u_1,\dots,u_k)$ where $u_j=v_j-v_0$ for all $1\le j\le k$. The first d resulting vectors of this process form an invertible matrix whose columns are $u_1,\dots,u_d$, as these vectors were required to be linearly independent and hence are a basis of $\mathbb{R}^d$. Thus we will write the associated origin-pinned configuration as $(\mathbb{A},u_{d+1},\dots,u_k)$.

The space for nonsingular origin-pinned configurations is hence identified as

$$\mathrm{GL}_d(\mathbb{R})\times\mathbb{R}^{d(k-d)}.$$

So, we have a map

$$\pi\colon\ N_d(k)\to\mathrm{GL}_d(\mathbb{R})\times\mathbb{R}^{d(k-d)}$$

given by

$$\pi(v_0,\dots,v_k)=(\mathbb{A},v_{d+1}-v_0,\dots,v_k-v_0).$$

This map is equivalent to passage to translation classes of nonsingular configurations of $k+1$ points in $\mathbb{R}^d$.

Step 2: *Analysis of the* $\mathrm{O}(d)$ *action on pinned configurations and "moving frames."* Congruence classes of such pinned configurations are given by $\mathrm{O}(d)$-orbits of the following action: $B\in\mathrm{O}(d)$ acts on $(\mathbb{A},u_{d+1},\dots,u_k)$ by sending it to $(B\mathbb{A},Bu_{d+1},\dots,Bu_k)$.

This action is complicated by the fact that $\mathrm{O}(d)$ acts on both the matrix $\mathbb{A}$ and the remaining vectors. To simplify future formulas, we fix this by using a method of "moving frames."

All this means is that as the columns of $\mathbb{A}$ are a basis of $\mathbb{R}^d$, we may expand each u_j when $j>d$ as a linear combination of $u_1,\dots,u_d$. If $u_j=\sum_{k=1}^d c_{jk}u_k$, we will define $c_j=(c_{j1},\dots,c_{jd})^{\mathrm{T}}$. Equivalently, $\mathbb{A}c_j=u_j$; note that as $\mathbb{A}$ depends on the first d vectors, this is a variable change of basis, i.e., a "moving frame."

Notice now that when $B\in\mathrm{O}(d)$ acts, $Bu_j=\sum_{k=1}^d c_{jk}Bu_k$, or equivalently $B\mathbb{A}c_j=Bu_j$, and so the c_j vectors themselves are unchanged by the $\mathrm{O}(d)$ action.

In other words, if we reencode pinned configurations as $(u_1,\dots,u_d,c_{d+1},\dots,c_k)$, then the $\mathrm{O}(d)$ action only acts on the first d coordinates and leaves the remaining coordinates unchanged. Thus the action becomes

$$B\cdot(\mathbb{A},c_{d+1},\dots,c_k)=(B\mathbb{A},c_{d+1},\dots,c_k),$$

so now $\mathrm{O}(d)$ will only act on the matrix slot in this coordinate system.

To summarize, we will now use this "moving frame" coordinate system, and thus an origin-pinned configuration is given by $(\mathbb{A},c_{d+1},\dots,c_k)\in\mathrm{GL}_d(\mathbb{R})\times\mathbb{R}^{d(k-d)}$ where $\mathbb{A}c_j=u_j$ relates the original vectors to these new c-vectors.

Step 3: *Quotienting the* $\mathrm{O}(d)$ *action.* Using the moving frame coordinate system, nonsingular origin-pinned configurations of $k+1$ points in $\mathbb{R}^d$ form the space $\mathrm{GL}_d(\mathbb{R})\times\mathbb{R}^{d(k-d)}$. The action of $\mathrm{O}(d)$ is given by $B\cdot(\mathbb{A},c_{d+1},\dots,c_k)=(B\mathbb{A},c_{d+1},\dots,c_k)$, so the final space for nonsingular congruence classes of configurations of $k+1$ points in $\mathbb{R}^d$, which we will call $M_d(k)(\mathbb{R}^d)$, is given by

$$M_d(k)(\mathbb{R}^d)=(\mathrm{O}(d)\backslash\mathrm{GL}_d(\mathbb{R}))\times\mathbb{R}^{d(k-d)},$$

where this is the quotient of the left action of $\mathrm{O}(d)$. To make this more explicit, we recall the LU- or UL-decomposition of nonsingular matrices that comes from the Gram–Schmidt process. Any $\mathbb{A}\in\mathrm{GL}_d(\mathbb{R})$ can be written as $\mathbb{A}=B\mathbb{C}$ for unique $B\in\mathrm{O}(d)$ and $\mathbb{C}\in L$, where L is the Lie group of upper triangular matrices with positive real entries on the diagonal.

This means that as manifolds (but not as groups) $\mathrm{GL}_d(\mathbb{R})$ is diffeomorphic to $\mathrm{O}(d) \times L$, where the left action of $\mathrm{O}(d)$ on $\mathrm{GL}_d(\mathbb{R})$ translates to an action on $\mathrm{O}(d) \times L$, with $\mathrm{O}(d)$ acting only on the left factor by left translation. Thus $\mathrm{O}(d)\backslash\mathrm{GL}_d(\mathbb{R})$ is naturally diffeomorphic to the Lie group L.

Putting this all together, we have

Summary 2.1. Let $(v_0, v_1, \dots, v_k)$ be a $(k+1)$-point configuration in $\mathbb{R}^d$ with $k \geq d$ and the first $d+1$ vectors affinely independent. Then we define $u_j = v_j - v_0$, $1 \leq j \leq k$, and make a matrix $\mathbb{A} \in \mathrm{GL}_d$ with $u_1, \dots, u_d$ as column vectors. The data $(\mathbb{A}, u_{d+1}, \dots, u_k) \in \mathrm{GL}_d \times \mathbb{R}^{d(k-d)}$ encodes the origin-pinned configurations or equivalently the translation classes of nonsingular configurations.

We then change coordinates to a moving frame coordinate system $\mathbb{A}c_j = u_j$ for $d+1 \leq j \leq k$. The data $(\mathbb{A}, c_{d+1}, \dots, c_k)$ also encodes pinned configurations, but now the $\mathrm{O}(d)$ action is only on the $\mathbb{A}$-coordinate.

Finally we mod the $\mathrm{O}(d)$ action to get the space of congruence classes of nonsingular $(k+1)$-point configurations in $\mathbb{R}^d$, which is called $M_d(k)(\mathbb{R}^d)$,

$$M_d(k)(\mathbb{R}^d) = L \times \mathbb{R}^{d(k-d)},$$

where the final data is $(\mathbb{C}, c_{d+1}, \dots, c_k)$ with $\mathbb{A} = B\mathbb{C}$, $B \in \mathrm{O}(d)$, $\mathbb{C} \in L$, the UL-decomposition of $\mathbb{A}$. Here L is the Lie group of upper triangular matrices with positive real entries on the diagonal.

2.2. Proof of Theorem 1.1. To prove Theorem 1.1, we will use the following famous theorem of Guth and Katz that resolved the Erdős distance problem in the plane (see [10]). To do so, we recall that a rigid motion θ acting on a finite point set E is t-rich when $|E \cap \theta E| \geq t$.

Theorem 2.2 (Guth–Katz)**.** *Suppose that E is a finite point set in $\mathbb{R}^2$, and let $\mathcal{R}_t(E)$ be the set of rigid motions that are at least t-rich. Then*

$$|\mathcal{R}_t(E)| \lesssim \frac{|E|^3}{t^2}.$$

Proof of Theorem 1.1. For $\mathcal{S}$ in $M_2(k)(E)$, let $\lambda(\mathcal{S})$ be the orbit of $\mathcal{S}$ under the $\mathrm{O}(2)$ action. Then

$$|E|^{2(k+1)} = \left(\sum_{\mathcal{S} \in M_2(k)(E)} \lambda(\mathcal{S})\right)^2 \leq |M_2(k)(E)| \sum_{\mathcal{S} \in M} \lambda^2(\mathcal{S}).$$

Focusing on the sum, note that two configurations are congruent if and only if there is a $(k+1)$-rich rigid motion taking one to the other. By a simple counting argument each such motion can have at most $\binom{t}{k+1}$ configurations associated to it. Thus, letting $\mathcal{R}_{=t}(E)$ be the set of rigid motions of richness exactly t, we have

$$\begin{aligned} \sum_{\mathcal{S} \in M} \lambda^2(\mathcal{S}) &\leq \sum_{t \geq k+1} \binom{t}{k+1} |\mathcal{R}_{=t}(E)| = \sum_{t > k+1} \binom{t-1}{k} |\mathcal{R}_t(E)| + \text{Error term} \\ &\lesssim \sum_{t > k+1} \binom{t-1}{k} \frac{|E|^3}{t^2} \sim |E|^3 \sum_{k+1 < t \leq |E|} t^{k-2} \sim |E|^{k+2}. \end{aligned}$$

Rearranging gives $|M_2(k)(E)| \gtrsim |E|^k$, as required. □

3. PROOF OF THEOREM 1.20

The proof of Theorem 1.20 follows from the fact that there can only be a constant number, dependent only on the number of points k and the dimension d, of congruences associated to a minimally infinitesimally rigid graph. To prove this result, we will follow the outline of [4].

For a tuple $\boldsymbol{x}$ in $\mathbb{R}^{d(k+1)}$ it is useful to define the following preimage of $f_{G_{k+1,m}}(\boldsymbol{x})$:

$$N_{\boldsymbol{x}} = \{\boldsymbol{y} \in \mathbb{R}^{d(k+1)}\colon\ f_{G_{k+1,m}}(\boldsymbol{y}) = f_{G_{k+1,m}}(\boldsymbol{x})\}. \tag{3.1}$$

Proposition 3.1 [4, Sect. 3.4]**.** *Suppose $G_{k+1,m}$ is a minimally infinitesimally rigid graph and $\boldsymbol{x}$ is any tuple (not necessarily regular). Let $b_0(N_x/\sim)$ denote the number of connected components of $N_{\boldsymbol{x}}$ under the congruence relation given by the $\mathrm{O}(d)$ action. Then $b_0(N_{\boldsymbol{x}}/\sim) \le C_{k,d}$ for some number $C_{k,d} > 0$ depending only on the dimension d and the number of points k.*

Proposition 3.2 [4, Proposition 4.11]**.** *Suppose $G_{k+1,m}$ is a minimally infinitesimally rigid graph and $\boldsymbol{x}$ is any regular tuple of $G_{k+1,m}$. If $\boldsymbol{y}$ and $\boldsymbol{z}$ are in the same connected component of $N_{\boldsymbol{x}}$, then there is some θ in $\mathrm{ISO}(\mathbb{R}^d)$ such that $\boldsymbol{y} = \theta\boldsymbol{z}$.*

For a more precise version of Proposition 3.1 see [3]; we gain a sharp result without requiring this. We can combine the above two results to give us the theorem.

Let us first define the following set:

$$v(t) = \{\boldsymbol{x} \in E^{k+1}\colon\ f_{G_{k+1,m}}(\boldsymbol{x}) = t\}.$$

Using Proposition 3.1, we can divide $v(t)$ into a finite union of connected components $\widetilde{v}_i$. Thus

$$v(t) = \bigcup_{i=1}^{C_{k,d}} \widetilde{v}_i(t),$$

where some $\widetilde{v}_i(t)$ may be empty. Letting $\widetilde{v}_0(t)$ be the largest of these connected components, we have the following estimate:

$$|E|^{2(k+1)} = \Biggl(\sum_{t\in\Delta(G_{k+1,m},E^{k+1})} v(t)\Biggr)^2 = \Biggl(\sum_{t\in\Delta}\sum_{i=1}^{C_{k,d}} \widetilde{v}_i(t)\Biggr)^2 \le C_{k,d}^2\Biggl(\sum_{t\in\Delta}\widetilde{v}_0(t)\Biggr)^2$$
$$\le C_{k,d}^2|\Delta(G_{k+1,m},E^{k+1})|\sum \widetilde{v}_0^2(t).$$

Thus, to prove the result, it suffices to prove the following bound:

$$\sum_t \widetilde{v}_0^2(t) \lesssim |E|^{k+2}\log|E|.$$

To do this, we need to use Proposition 3.2. Note that

$$\sum_t \widetilde{v}_0^2(t) = \Bigl|\Bigl\{(\boldsymbol{x},\boldsymbol{y})\colon\ f_{G_{k+1,m}}(\boldsymbol{x}) = f_{G_{k+1,m}}(\boldsymbol{y})$$
$$\&\ \boldsymbol{x},\ \boldsymbol{y} \text{ in same maximal connected component of } f^{-1}_{G_{k+1,m}}(\Delta)\Bigr\}\Bigr|.$$

By Proposition 3.2, $\boldsymbol{x}$ and $\boldsymbol{y}$ being in the same connected component of $f^{-1}_{G_{k+1,m}}(\Delta(G_{k+1,m},E^{k+1}))$ means there is a rigid motion θ such that $\boldsymbol{x} = \theta\boldsymbol{y}$. Recalling that these are frameworks, we have $(x^1,\dots,x^{k+1}) = (\theta y^1,\dots,\theta y^{k+1})$. Using that $f_{G_{k+1,m}}(\boldsymbol{x}) = f_{G_{k+1,m}}(\theta\boldsymbol{y})$, we have $x^i - \theta y^i = x^j - \theta y^j = \tau$ if ij an edge in $G_{k+1,m}$, where τ is uniform over the tuple pair $(\boldsymbol{x},\boldsymbol{y})$.

So if we define

$$v_\theta(\tau) = \{(x,y) \in E^2\colon\ x - \theta y = \tau\},$$

we have the following result:

$$\sum_t \widetilde{v}_0^2(t) \le \sum_{\tau\in\mathbb{R}^d}\ \sum_{\theta\in\mathrm{ISO}(\mathbb{R}^d)} v_\theta^{k+1}(\tau).$$

Here we do not necessarily have an equality, as there may be elements counted in the right-hand side that are outside the maximal connected component of $f^{-1}_{G_{k+1,m}}(\Delta(G_{k+1,m},E^{k+1}))$. But certainly all pairs from the maximal connected component are counted.[1] This bound suffices for our purposes and will in fact produce a sharp result. To conclude, we note the following trivial bound:

$$|v_\theta(\tau)| \le |E|,$$

which follows from the fact that the second coordinate is entirely dependent on the choice of the first (once θ and τ are fixed).

Until this stage the calculation works in any dimension d. However, to conclude we are going to apply the Guth–Katz result that leads to the resolution of the Erdős distance problem. This requires that we operate in dimension 2 only. When $d=2$, we have

$$\sum_t \widetilde{v}_0^2(t) \le \sum_{\tau\in\mathbb{R}^2}\sum_{\theta\in\mathrm{ISO}(\mathbb{R}^2)} v_\theta^{k+1}(\tau) \le |E|^{k-1}\sum_{\tau\in\mathbb{R}^2}\sum_{\theta\in\mathrm{ISO}(\mathbb{R}^2)} v_\theta^2(\tau)$$
$$\lesssim |E|^{k-1}|E|^3\log|E| = |E|^{k+2}\log|E|,$$

where the final estimate deploys the Guth–Katz result. This was the bound we required. Thus, for a minimally infinitesimal graph $G_{k+1,m}$, we have

$$|\Delta(G_{k+1,m},E^{k+1})| \gtrapprox |E|^k.$$

4. PROOF OF THEOREM 1.22

Recall we define the pinned-distance set as

$$\Delta_x(E) = \{|x-y|\colon\ y\in E\}$$

for a pin $x\in E$. We call $|\Delta_x(E)|$ the pin-richness of x (in E) and call a set A an r-rich pin set if every point in A has pin-richness at least r.

The first part of our proof is to show that if the Erdős pinned-distance conjecture (Conjecture 1.21) holds, then we have many rich pins. We can then use these rich pins as the vertices for our distance graphs, where their richness allows us to construct sufficiently many variations of graph-distance tuples.

Lemma 4.1. *Suppose the Erdős pinned-distance conjecture is satisfied for a point set E. Then there are $\sim|E|$ points x in E such that $|\Delta_x(E)|\approx|E|$.*

Proof. To see this, we use the Erdős pinned-distance conjecture to find a pin x_0 such that $|\Delta_{x_0}(E)|\approx|E|$. We then remove this point from E to gain a modified E_0. We then apply the conjecture to E_0 to gain some x_1 which is a pin of richness $\approx|E|$. We repeat the process $|E|/2$ times gaining a sufficiently rich pin each time. Thus we have $|E|/2$ pins with pin-richness between $|E|$ and $|E|/2$ as claimed. ☐

To finish the proof, we count the number of possible distance drawings using the rich-pin subset of E. Notice that for any graph drawing, once we have determined the position of the vertices, we have no freedom left to select any other edges. Thus we naturally use spanning trees to determine the number of ways we have to draw the graph. It is clear that for a graph on k vertices the number of edges in the spanning tree will be $k-1$. As we have $k\ll|E|$ (in particular, $k\ll|E|/2$), we can choose our edges essentially independently from the set of rich distances.

[1] In fact the right-hand side counts all pairs from each connected component, but not cross pairs. However, we have to reduce to one connected component to pass through the Cauchy–Schwarz step above.

Thus according to Lemma 4.1 the total number of choices for each edge in the spanning tree is $\approx |E|^{2/d}$. As we have $k-1$ such choices and our choices are independent, we have a total number of choices

$$\gtrapprox \left(|E|^{2/d}\right)^{k-1} = |E|^{2(k-1)/d}.$$

We note that this is clearly sharp as the grid in $\mathbb{R}^d$ satisfies the Erdős distance problem criterion, in that each point has $\sim |E|^{2/d}$ unique distances in its pinned-distance set.

ACKNOWLEDGMENTS

This work was partially supported by the NSA grant H98230-15-1-0319.

REFERENCES

1. B. Aronov, J. Pach, M. Sharir, and G. Tardos, "Distinct distances in three and higher dimensions," Comb. Probab. Comput. **13** (3), 283–293 (2004).
2. L. Asimow and B. Roth, "The rigidity of graphs," Trans. Am. Math. Soc. **245**, 279–289 (1978).
3. C. Borcea and I. Streinu, "The number of embeddings of minimally rigid graphs," Discrete Comput. Geom. **31** (2), 287–303 (2004).
4. N. Chatzikonstantinou, A. Iosevich, S. Mkrtchyan, and J. Pakianathan, "Rigidity, graphs and Hausdorff dimension," arXiv: 1708.05919 [math.CA].
5. F. R. K. Chung, "The number of different distances determined by n points in the plane," J. Comb. Theory, Ser. A **36** (3), 342–354 (1984).
6. F. R. K. Chung, E. Szemerédi, and W. T. Trotter, "The number of different distances determined by a set of points in the Euclidean plane," Discrete Comput. Geom. **7** (1), 1–11 (1992).
7. K. L. Clarkson, H. Edelsbrunner, L. J. Guibas, M. Sharir, and E. Welzl, "Combinatorial complexity bounds for arrangements of curves and spheres," Discrete Comput. Geom. **5** (2), 99–160 (1990).
8. P. Erdős, "On sets of distances of n points," Am. Math. Mon. **53**, 248–250 (1946).
9. J. Graver, B. Servatius, and H. Servatius, *Combinatorial Rigidity* (Am. Math. Soc., Providence, RI, 1993), Grad. Stud. Math. **2**.
10. L. Guth and N. H. Katz, "On the Erdős distinct distances problem in the plane," Ann. Math., Ser. 2, **181** (1), 155–190 (2015).
11. N. H. Katz and G. Tardos, "A new entropy inequality for the Erdős distance problem," in *Towards a Theory of Geometric Graphs* (Am. Math. Soc., Providence, RI, 2004), Contemp. Math. **342**, pp. 119–126.
12. L. Moser, "On the different distances determined by n points," Am. Math. Mon. **59** (2), 85–91 (1952).
13. B. Roth, "Rigid and flexible frameworks," Am. Math. Mon. **88** (1), 6–21 (1981).
14. J. Solymosi and Cs. D. Tóth, "Distinct distances in the plane," Discrete Comput. Geom. **25** (4), 629–634 (2001).
15. J. Solymosi and V. Vu, "Distinct distances in high dimensional homogeneous sets," in *Towards a Theory of Geometric Graphs* (Am. Math. Soc., Providence, RI, 2004), Contemp. Math. **342**, pp. 259–268.
16. J. Solymosi and V. H. Vu, "Near optimal bounds for the Erdős distinct distances problem in high dimensions," Combinatorica **28** (1), 113–125 (2008).
17. L. A. Székely, "Crossing numbers and hard Erdős problems in discrete geometry," Comb. Probab. Comput. **6** (3), 353–358 (1997).
18. G. Tardos, "On distinct sums and distinct distances," Adv. Math. **180** (1), 275–289 (2003).