Available online at www.sciencedirect.com
SCIENCE DIRECT®
Advances in Applied Mathematics 32 (2004) 709–735
ADVANCES IN Applied Mathematics
www.elsevier.com/locate/yaama

On reconstructing n-point configurations from the distribution of distances or areas

Mireille Boutin [a] and Gregor Kemper [b,*]

[a] *Max Planck Institute for Mathematics in the Sciences, Inselstraße 22, 04103 Leipzig, Germany*
[b] *Technische Universität München, Zentrum Mathematik – M11, Boltzmannstraße 3, 85748 Garching, Germany*

Received 23 February 2003; accepted 14 April 2003

Abstract

One way to characterize configurations of points up to congruence is by considering the distribution of all mutual distances between points. This paper deals with the question if point configurations are uniquely determined by this distribution. After giving some counterexamples, we prove that this is the case for the vast majority of configurations.

In the second part of the paper, the distribution of areas of sub-triangles is used for characterizing point configurations. Again it turns out that most configurations are reconstructible from the distribution of areas, though there are counterexamples.

1. Introduction

In this paper, we study a type of shape representation which attempts to combine both the approaches of invariant theory and statistics. We consider the problem of characterizing the *shape* or, more generally, the *geometry* of a configuration of points. More precisely, we are interested in finding a good representation for configurations of points in a vector space modulo the action of a Lie group G. The solution we investigate consists in using distributions of invariants of the action of G.

Our main motivation comes from applications in computer vision. A central problem in image understanding is that of identifying objects from a picture. In that problem, one must take into account that variations in the position of the object or in the parameters of

* Corresponding author.
E-mail addresses: boutin@mis.mpg.de (M. Boutin), kemper@ma.tum.de (G. Kemper).

0196-8858/$ – see front matter
doi:10.1016/S0196-8858(03)00101-5

the camera induce variations in the image which correspond to group transformations that need to be moded out in order to establish the correspondence between two pictures of the same object.

The obvious way to obtain image features which are not affected by the action of the group is to use invariants of the group action. However, in order to be able to positively identify any object, we need to find a set of invariants whose values *completely* characterize the image of the object up to the action of the group. In other words, we need to find a set of invariants such that two images are in the same orbit *if and only if* the values of these invariants evaluated on the two images are the same. Such invariants are called *separating* because they can be used to separate the orbits. In traditional approaches to object recognition (see, for example, [1]), this method is commonly used.

In the following, we address the case of shapes defined by a finite set of points. This is actually an important case for applications. Indeed for many reasons (e.g., the amount of noise or the nature of the data) it is common to represent an object of interest by a finite set of points called *landmarks*. For example, landmarks can be defined by salient features on the boundary of the image of the object. Specifically, one might think of minutiae in fingerprints, corners on edges of archaeological sherds, or stellar constellations. In order to recognize the object, one thus needs to characterize the point configuration given by the landmarks up to the action of the group.

Given a Lie group G acting on a vector space V and two sets of n points $P_1, \ldots, P_n$ and $\overline{P}_1, \ldots, \overline{P}_n \in V$, we want to be able to determine whether there exists $g \in G$ and a permutation $\pi \in S_n$ (since, a priori, we do not know whether the points are labeled in correspondence) such that

$$g(P_i) = \overline{P}_{\pi(i)}, \quad \text{for all } i = 1, \ldots, n.$$

In applications, we are often interested in pictures, so V is usually $\mathbb{R}^2$ or $\mathbb{R}^3$ and the Lie group G is typically a subgroup of the projective group and depends on how the picture of the object was taken. Examples of important groups include $\mathrm{E}(2)$, the group of rigid motions in the plane (rotations, reflections, and translations, sometime also denoted by $\mathrm{AO}(2)$), and $A(2)$, the group of affine transformations in the plane, i.e., all translations and linear maps with determinant ± 1.

In principle, this problem can indeed be solved using invariants. If we assume that the points are distinguishable so we know how to correctly label them, then all we need to do is to find a set of separating invariants of the diagonal action of G on V^n,

$$g \cdot (Q_1, \ldots, Q_n) = \big(g(Q_1), \ldots, g(Q_n)\big) \quad \text{for all } g \in G \text{ and all } Q_1, \ldots, Q_n \in V.$$

For example, if $G = \mathrm{E}(2)$ the group of Euclidean transformations in the plane then two sets of landmarks $P_1, \ldots, P_n$ and $\overline{P}_1, \ldots, \overline{P}_n$ (labeled in correspondence) belong to the same orbit under the action of $\mathrm{E}(2)$ if and only if all their pairwise distances $d(P_i, P_j) = d(\overline{P}_i, \overline{P}_j)$ are the same for all $i, j = 1, \ldots, n$. So the shape of the set of labeled landmarks $P_1, \ldots, P_n$ is completely characterized by the value of the pairwise (labeled) distances between the landmarks.

However, in most applications the point correspondence is unknown so things are more complicated, especially when the number of points n is big. Indeed, labeling the points is a non-trivial task which, although feasible, takes time. (See, for example, [2] for an easy exposition of some existing methods.) And the bigger the number of points, the longer it takes. We would thus prefer to simply skip the labeling step. So, can we, instead, find separating invariants of the action of $\mathrm{E}(2) \times S_n$?

The answer to this question is, of course, yes. For example, in the case $n = 3$, instead of distances one can use the following symmetric functions of the distances:

$$f_1(P_1, P_2, P_3) = d(P_1, P_2) + d(P_1, P_3) + d(P_2, P_3),$$
$$f_2(P_1, P_2, P_3) = d(P_1, P_2)d(P_2, P_3) + d(P_1, P_2)d(P_1, P_3) + d(P_1, P_3)d(P_2, P_3),$$
$$f_3(P_1, P_2, P_3) = d(P_1, P_2)d(P_1, P_3)d(P_2, P_3).$$

These are separating invariants of the action of $\mathrm{E}(2) \times S_3$ on $(\mathbb{R}^2)^3$. Continuing in this way, we can try to find expressions in the distances $d(P_1, P_2)$, $d(P_1, P_3)$, $d(P_1, P_4)$, $d(P_2, P_3)$ $d(P_2, P_4)$, and $d(P_3, P_4)$, which are invariant under the action of S_4 by permuting the P_i, and which form a generating (or at least separating) subset of all such invariants. But notice that the elementary symmetric functions in the distances will not qualify anymore, since these are the invariants under the action of S_6 instead of S_4. Thus this approach requires a fresh computation of invariants for each value of n.

The S_n-invariants needed here are often called *graph invariants*, and have been studied in a graph theoretical context by various authors, e.g., [3–5]. Aslaksen et al. [5] calculated a generating set of graph invariants for $n = 4$, obtaining a minimal set of 9 invariants. But for $n = 5$ the computation of graph invariants is already very hard and stood as a challenge problem for a while (see [3,5]) until the computation was done by the second author (see [6, p. 221]). The minimal generating set for $n = 5$ contains 56 invariants, and storing them takes several MBytes of memory. For $n \geqslant 6$ the computation is presently not feasible. This clearly shows that the approach of using graph invariants is far from practical. Apart from their number and the difficulties of computing them, they cannot be used in practice for questions of robustness, since high degree polynomials vary immensely when small variations in the points $P_1, \ldots, P_n$ are introduced. We thus need to find better invariants than graph invariants; we need invariants that not only separate the orbits of the action of $G \times S_n$ but that are also robust and simple to compute.

We were inspired by looking at what engineers do in practice. In order to identify images of the same object, they often drop the separation requirement and simply look for invariant features of the image of which they compare the distribution. The distribution of the pairwise distances of a set of points is obviously invariant under a relabeling of the point. It is also much more robust than a set of polynomial functions of the pairwise distances. In addition, it is not too complicated to compute and very easy to manipulate.

So we asked ourselves if the distribution of distances of a set of points is actually also a separating invariant and thus completely characterizes point configurations up to rigid motions. In other words, can an n-point configuration be reconstructed uniquely (up to the labeling of the points and up to rigid motions) from the distribution of distances? It turns

out that this is *false* in general, as we demonstrate with counterexamples. But fortunately, counterexamples are rare, in a sense to be explained shortly. This is the contents of our first main result (Theorem 2.6). This result extends to the case where the points come in several colors (see Remark 2.8). Moreover, it is true locally, i.e., the shape of n-point configurations that are close enough can be compared using their distribution of invariants. We also explore methods to verify reconstructibility for particular configurations. Most of the results for the case of distances in the real plane naturally extend to any vector space with a non-degenerate quadratic form over a field of characteristic not equal to 2. We shall thus simply treat this general case in the first part of this paper.

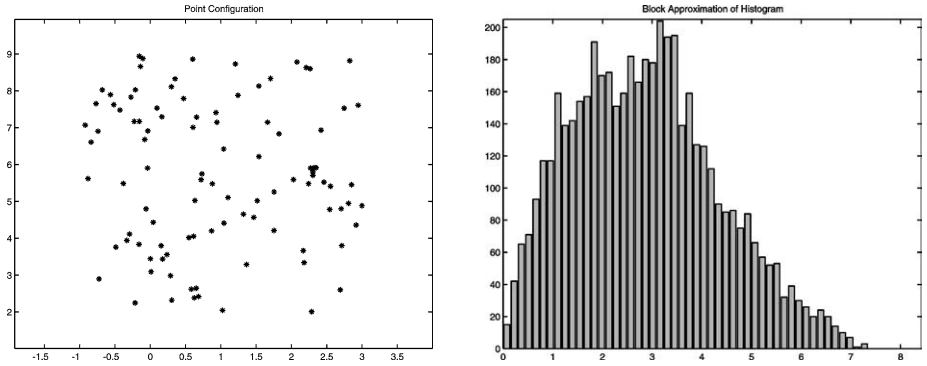
In the second part, we attempt to characterize point configurations up to the action of the equi-affine group $A(2)$ and, again, the symmetric group S_n. This action is relevant in computer vision since, up to a scale factor, it adequately approximates what happens to the camera image of a very distant planar object as it is rotated and translated in three-dimensional space. As above, there are obvious invariants for separating orbits under $A(2)$. These are the areas of triangles spanned by a selection of three of the n points. As before, we attempt to separate S_n-orbits by considering the *distribution* of all these areas. We obtain results which are completely analogous to those in the first section: there are examples of configurations which cannot be reconstructed (up to the action of $A(2) \times S_n$) from the distribution of areas; but a dense open subset of configurations are reconstructible in this sense (see Theorem 3.7). We believe that for most purposes in computer vision, this is a satisfactory result. Again our results generalize to configurations in any dimension and to any ground field.

Let us emphasize here that the use of computer algebra systems played a vital role in the preparation of this paper. In particular, Magma [7] was an indispensable tool. For example, the first example of an n-point configuration which is not reconstructible from distances was the upshot of a prolonged Magma session. The examples in Sections 3.1 and 3.4 were constructed with the help of Magma and Maple [8]. But also the proof of Theorem 2.6 was inspired by sample computations in Magma.

2. Reconstruction from distances

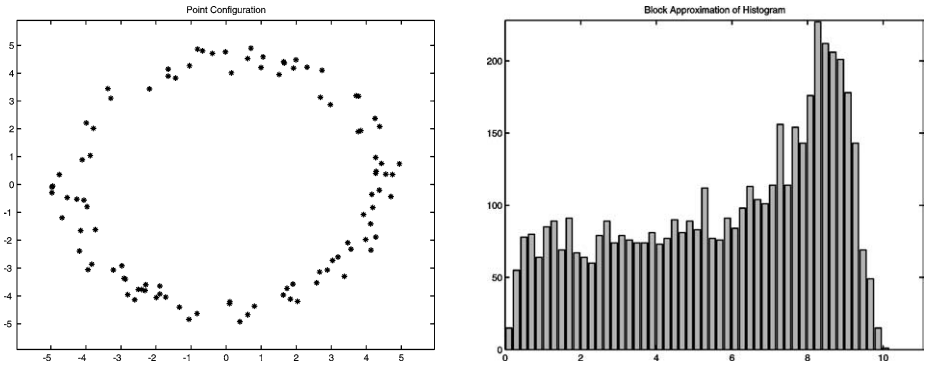
An n-point configuration is a tuple of points $P_1, \ldots, P_n \in \mathbb{R}^m$. To an n-point configuration we associate the squared (Euclidean) distances $d_{i,j}$ between each pair of points P_i and P_j, and then consider the *distribution* of distances, i.e., the relative frequencies of the value of the distances. In other words, the distribution of distances of an n-point configuration tells us how many times each distance occurs relative to the total number of distances. This means that, for n fixed, the distribution of distances is given by the set of the numbers $d_{i,j}$ possibly with multiplicities if some distances occur several times. So considering the distribution of distances of an n-point configuration is equivalent to considering the polynomial

$$F_{P_1,\ldots,P_n}(X) := \prod_{1 \leqslant i < j \leqslant n} (X - d_{i,j}).$$



(a) (b)

Fig. 1. (a) A 100-point configuration, (b) histogram of distances with bin size 0.1470.



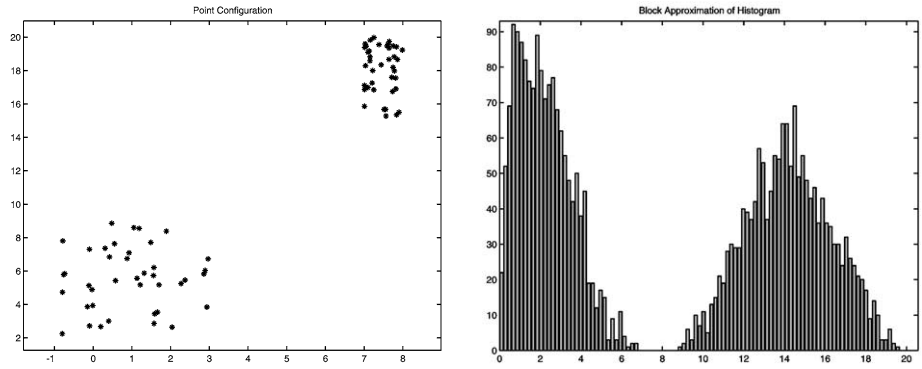
(a) (b)

Fig. 2. (a) A 100-point configuration, (b) histogram of distances with bin size 0.1993.

In order to better visualize the information contained in a distribution of distances, one can plot a histogram of the distances, i.e., one can group the data into bins of a fixed size and count how many distances lie in each bin. Figures 1–3 show examples of n-point configurations in the plane together with a histogram of their distances.

Clearly the distribution of distances is *invariant* under permutations of the points and under the (simultaneous) action of the Euclidean group. The question is whether an n-point configuration can be reconstructed from its distribution of distances.

Definition 2.1. An n-point configuration $P_1, \ldots, P_n \in \mathbb{R}^m$ is called *reconstructible from distances* if the following holds. If $Q_1, \ldots, Q_n$ is another n-point configuration with $F_{P_1,\ldots,P_n}(X) = F_{Q_1,\ldots,Q_n}(X)$, then there exists a permutation $\pi \in S_n$ and a Euclidean transformation $g \in \mathrm{E}_m(\mathbb{R})$ such that $g(P_{\pi(i)}) = Q_i$ holds for all i.



(a) (b)

Fig. 3. (a) An 80-point configuration, (b) histogram of distances with bin size 0.1947.

The notion of reconstructibility from distances generalizes naturally to any vector space V with a non-degenerate quadratic form $\langle \cdot\,, \cdot \rangle$ over a field of characteristic not equal to 2. In this context, one simply uses $\langle P_i - P_j, P_i - P_j \rangle$ as the "distance" between P_i and P_j, for any $P_i, P_j \in V$ and replaces the Euclidean group by $\mathrm{AO}(V) = \mathrm{O}(V) \ltimes V$ where $\mathrm{O}(V) \subseteq \mathrm{GL}(V)$ is the orthogonal group given by the form $\langle \cdot\,, \cdot \rangle$.

2.1. Non-reconstructible configurations

It is clear that in two-dimensional Euclidean space all triangles are reconstructible from distances, and the same is true for all 2-point configurations. So the quest for examples of non-reconstructible n-point configurations becomes interesting for $n \geqslant 4$. Figure 4 shows such an example. We have put the (non-squared) distances along the lines connecting pairs of points. Note that the upper point in the first configuration is moved diagonally downward to obtain the second configuration, while the other three points remain inert.

Further examples can be constructed by adding an arbitrary number of additional points on the dotted line and at the same position in both configurations (such as the slightly thicker dot in each picture). Thus, we get examples of non-reconstructible n-point

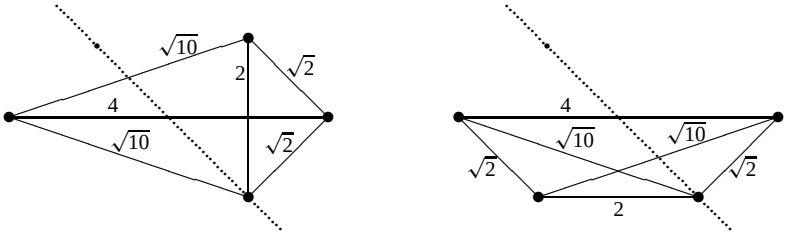


Fig. 4. Two 4-point configurations with the same distribution of distances.

configurations for any $n \geqslant 4$. By embedding these into a space of higher dimension, we also get examples in any dimension $m \geqslant 2$. The fact that we can add points at arbitrary positions on the dotted line shows that the symmetry of the configuration is not responsible for the fact that it is not reconstructible.

2.2. Relation-preserving permutations

Let K be a field of characteristic not equal to 2 ($K = \mathbb{C}$ and $K = \mathbb{R}$ will be the most important examples). Let V be an m-dimensional vector space over K with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. With a suitable choice of a basis, this form is given by $\langle (x_1, \ldots, x_m), (y_1, \ldots, y_m) \rangle = \sum_{k=1}^{m} a_k x_k y_k$ with $a_k \in K \setminus \{0\}$. If $v_1, \ldots, v_n$ are vectors in V, then the Gram matrix $(\langle v_i, v_j \rangle)_{i,j=1,\ldots,n}$ has rank at most m, hence the $(m+1) \times (m+1)$-minors are zero. By the following well-known proposition, this gives all relations between the scalar products of n vectors. Part (b) gives the relations between the distances between n points. In fact, Proposition 2.2(a) is the "second fundamental theorem" of invariant theory of orthogonal groups.

Proposition 2.2. *Let $x_{i,k}$ be indeterminates over K $(i = 1, \ldots, n, k = 1, \ldots, m)$.*

(a) *Let $s_{i,j}$ be further indeterminates $(1 \leqslant i \leqslant j \leqslant n)$. Then the kernel of the map*

$$K[s_{1,1}, \ldots, s_{n,n}] \to K[x_{1,1}, \ldots, x_{n,m}], \quad s_{i,j} \mapsto \sum_{k=1}^{m} a_k x_{i,k} x_{j,k}$$

is generated (as an ideal) by the $(m+1) \times (m+1)$-minors of the matrix $(s_{i,j})_{i,j=1,\ldots,n}$, where we set $s_{i,j} := s_{j,i}$ for $i > j$.

(b) *Let $D_{i,j}$ be indeterminates $(1 \leqslant i < j \leqslant n)$. Then the kernel of the map*

$$K[D_{1,2}, \ldots, D_{n-1,n}] \to K[x_{1,1}, \ldots, x_{n,m}], \quad D_{i,j} \mapsto \sum_{k=1}^{m} a_k (x_{i,k} - x_{j,k})^2$$

is generated (as an ideal) by the $(m+1) \times (m+1)$-minors of the matrix

$$\mathcal{D} = (D_{i,j} - D_{i,n} - D_{j,n})_{i,j=1,\ldots,n-1}, \tag{2.1}$$

where we set $D_{i,i} := 0$ and $D_{i,j} := D_{j,i}$ for $i > j$.

Proof. For part (a), see [9] or [10, Theorem 5.7] (the latter reference takes care of the positive characteristic case). Part (b) follows from (a) since for points $P_1, \ldots, P_n \in V$ we have

$$\langle P_i - P_n, P_j - P_n\rangle = \frac{1}{2}\big(\langle P_i - P_n, P_i - P_n\rangle + \langle P_j - P_n, P_j - P_n\rangle - \langle P_i - P_j, P_i - P_j\rangle\big). \qquad \square \tag{2.2}$$

We will now study monomials occurring in elements of the ideal given by Proposition 2.2(b). From now on it is useful to use sets $\{i, j\}$ as indices of the d's rather than pairs i, j.

Lemma 2.3. *Let K be a field of characteristic not equal to 2 and let $D_{\{i,j\}}$ be indeterminates $(i, j = 1, \ldots, n,\ i \neq j)$. For an integer r with $1 \leqslant r \leqslant n-1$ consider the ideal I generated by all $(r \times r)$-minors of the matrix $\mathcal{D} := (D_{\{i,j\}} - D_{\{i,n\}} - D_{\{j,n\}})_{i,j=1,\ldots,n-1}$, where we set $D_{\{i,i\}} := 0$. Let $t = \prod_{\nu=1}^{r} D_{\{i_\nu, j_\nu\}}$ be a monomial of degree r. Then the following are equivalent*:

(a) *The monomial t occurs in a polynomial from I.*
(b) *Every index from $\{1, \ldots, n\}$ occurs at most twice among the i_ν and j_ν. More formally, for every $k \in \{1, \ldots, n\}$ we have $|\{\nu \mid i_\nu = k\}| + |\{\nu \mid j_\nu = k\}| \leqslant 2$.*

Proof. It follows from Proposition 2.2(b) that the ideal I is stable under the natural action by the symmetric group S_n. Thus, t occurs in a polynomial from I if and only if all images of t occur.

First, assume that there exists a $k \in \{1, \ldots, n\}$ which occurs more than twice among the i_ν and j_ν. By the previous remark we may assume $k = 1$. If t occurs in a polynomial of I it must also occur in an $(r \times r)$-minor of $\mathcal{D}$ (since $\deg(t) = r$). But in order to obtain t as a monomial in an $(r \times r)$-minor, one has to choose the first row or the first column of $\mathcal{D}$ at least twice, since entries involving the index 1 only occur in the first row and column. But that is impossible. This proves that (a) implies (b).

Now assume that (b) is satisfied. Consider the graph $\mathcal{G}$ with vertices indexed $1, \ldots, r$, where the number of edges between vertex ν and μ is $|\{i_\nu, j_\nu\} \cap \{i_\mu, j_\mu\}|$, i.e., the number of indices shared by the νth and μth indeterminate in t. By the hypothesis (b) every vertex is connected to at most two others, hence every connected component of $\mathcal{G}$ is a line (including the case of an unconnected vertex) or a loop (including the case of a loop of two vertices corresponding to indeterminates $D_{\{i_\nu, j_\nu\}}$ and $D_{\{i_\mu, j_\mu\}}$ which are equal). By renumbering, we may assume that the first connected component is given by the first m vertices. By the remark at the beginning of the proof, we may further assume that the first m indeterminates in t are $D_{\{1,2\}}, D_{\{2,3\}}, \ldots, D_{\{m,m+1\}}$ (forming a line in $\mathcal{G}$) or $D_{\{1,2\}}, D_{\{2,3\}}, \ldots, D_{\{m-1,m\}}, D_{\{1,m\}}$ (a loop). Since $m \leqslant r \leqslant n-1$, it can only happen in the first case that the index n is involved in these indeterminates. Thus, if n is involved, then $m = n-1$ and $t = \prod_{\nu=1}^{n-1} D_{\{\nu,\nu+1\}}$. It is easily seen that in this case t occurs in $\det(\mathcal{D})$ with coefficient $2 \cdot (-1)^{n-1}$. Having settled this case, we may assume that $m < n-1$. We proceed by induction on the number of connected components of $\mathcal{G}$.

First, assume that the first component is a loop. We wish to build an $(r \times r)$-submatrix of $\mathcal{D}$ whose determinant contains t as a monomial. To this end, we start by choosing the first m rows and the first m columns from $\mathcal{D}$. Temporarily setting all $D_{\{i,n\}} := 0$, we obtain a matrix $\mathcal{D}'$ with

$$\mathcal{D}'|_{D_{\{i,n\}}=0} = \begin{pmatrix} 0 & D_{\{1,2\}} & \cdots & D_{\{1,m-1\}} & D_{\{1,m\}} \\ D_{\{1,2\}} & 0 & \cdots & D_{\{2,m-1\}} & D_{\{2,m\}} \\ \vdots & & \ddots & & \vdots \\ D_{\{1,m-1\}} & D_{\{2,m-1\}} & \cdots & 0 & D_{\{m-1,m\}} \\ D_{\{1,m\}} & D_{\{2,m\}} & \cdots & D_{\{m-1,m\}} & 0 \end{pmatrix}.$$

Clearly, the product $t' := D_{\{1,2\}}D_{\{2,3\}}\cdots D_{\{m-1,m\}}D_{\{1,m\}}$ occurs with coefficient $2(-1)^{m-1}$ (or -1 if $m=2$) in $\det(\mathcal{D}')$. Since the first m indeterminates in t form a connected component in $\mathcal{G}$, the indeterminates in $t'' := t/t'$ involve none of the indices $1,\ldots,m$. Thus, by induction we can choose $r-m$ rows, all below the mth row, and $r-m$ columns, all right of the mth column, such that t'' occurs as a monomial of the determinant of the corresponding submatrix $\mathcal{D}''$. Finally, in order to get all of $t = t'\cdot t''$ as a monomial in a minor, choose the rows and columns as in $\mathcal{D}''$ together with the first m rows and columns. This yields a submatrix of $\mathcal{D}$ of block structure

$$\begin{pmatrix} \mathcal{D}' & * \\ * & \mathcal{D}'' \end{pmatrix},$$

where indeterminates $D_{\{i,j\}}$ with both indices $\leqslant m$ only occur in $\mathcal{D}'$. Now clearly t occurs with non-zero coefficient in the determinant of this matrix.

Let us treat the second case, so assume that the first component of $\mathcal{G}$ is a line $D_{\{1,2\}}, D_{\{2,3\}}, \ldots, D_{\{m,m+1\}}$. Taking rows $1,\ldots,m$ and columns $2,\ldots,m+1$ yields a matrix $\mathcal{D}'$ with

$$\mathcal{D}'|_{D_{\{i,n\}}=0} = \begin{pmatrix} D_{\{1,2\}} & D_{\{1,3\}} & \cdots & D_{\{1,m\}} & D_{\{1,m+1\}} \\ 0 & D_{\{2,3\}} & \cdots & D_{\{2,m\}} & D_{\{2,m+1\}} \\ D_{\{2,3\}} & 0 & \cdots & D_{\{3,m\}} & D_{\{3,m+1\}} \\ \vdots & & \ddots & & \vdots \\ D_{\{2,m\}} & D_{\{3,m\}} & \cdots & 0 & D_{\{m,m+1\}} \end{pmatrix}.$$

The product $t' := D_{\{1,2\}}D_{\{2,3\}}\cdots D_{\{m,m+1\}}$ occurs with coefficient 1 in $\det(\mathcal{D}')$. As above, the monomials in the remaining part $t'' := t/t'$ of t only involve indices strictly bigger than $m+1$. Thus, we may choose $r-m$ rows and columns which are all below and right of the $(m+1)$st, respectively, to form a submatrix $\mathcal{D}''$ which has t'' in its determinant. Again, putting together the rows and columns that we chose yields a submatrix with block structure as above. We see that also in this case t occurs as a monomial in an $(r\times r)$-minor of $\mathcal{D}$. □

If two n-point configurations have the same distribution of distances, this means that the distances of both configurations coincide up to some permutation. But the permuted distances must again satisfy the relations given by the ideal from Proposition 2.2. Therefore, it is crucial to determine how this ideal behaves under permutations of

the $D_{\{i,j\}}$. We show that all permutations which preserve this ideal are in fact induced from permutations of the n points. This provides the core of our argument.

Lemma 2.4. *Let K be a field of characteristic not equal to 2 and let $D_{\{i,j\}}$ be indeterminates $(i, j = 1, \ldots, n,\ i \neq j)$. For an integer r with $3 \leqslant r \leqslant n-1$ consider the ideal I generated by all $(r \times r)$-minors of the matrix $\mathcal{D} := (D_{\{i,j\}} - D_{\{i,n\}} - D_{\{j,n\}})_{i,j=1,\ldots,n-1}$, where we set $D_{\{i,i\}} := 0$. Let ϕ be a permutation of the $D_{\{i,j\}}$ which maps I to itself. Then there exists a permutation $\pi \in S_n$ such that*

$$\phi\big(D_{\{i,j\}}\big) = D_{\{\pi(i),\pi(j)\}} \quad \text{for all } i, j.$$

Proof. We write $\phi(D_{\{1,2\}}) = D_{\{i,j\}}$ and $\phi(D_{\{1,3\}}) = D_{\{k,l\}}$. Assume that $\{i, j\} \cap \{k, l\} = \emptyset$. Then by Lemma 2.3 a monomial t of degree r occurs in an element of I such that t is divisible by $D_{\{i,j\}}^2 D_{\{k,l\}}$. By the hypothesis, $\phi^{-1}(t)$ also occurs in an element of I. But $\phi^{-1}(t)$ is divisible by $D_{\{1,2\}}^2 D_{\{1,3\}}$, contradicting Lemma 2.3. This argument shows that if the index sets of two $D_{\{\nu,\mu\}}$'s intersect, then the same is true for their images under ϕ. This will be used several times during the proof. Here, after possibly reordering the index sets (recall that we do not assume $i < j$ or $k < l$) we obtain $i = l$. Thus, $\phi(D_{\{1,3\}}) = D_{\{i,k\}}$. Now we write $\phi(D_{\{1,4\}}) = D_{\{m,p\}}$ and conclude, as above, that $\{m, p\} \cap \{i, j\} \neq \emptyset$ and $\{m, p\} \cap \{i, k\} \neq \emptyset$. Assume, by way of contradiction, that $i \notin \{m, p\}$. Then $\{m, p\} = \{j, k\}$, so $\phi(D_{\{1,4\}}) = D_{\{j,k\}}$. By Lemma 2.3 a monomial t of degree r occurs in an element of I such that t is divisible by $D_{\{i,j\}} D_{\{i,k\}} D_{\{j,k\}}$. Then $\phi^{-1}(t)$ also occurs in a polynomial from I, but $\phi^{-1}(t)$ is divisible by $D_{\{1,2\}} D_{\{1,3\}} D_{\{1,4\}}$. This contradicts Lemma 2.3. Hence, our assumption was false and we conclude that $i \in \{m, p\}$, so with suitable renumbering $\phi(D_{\{1,4\}}) = D_{\{i,m\}}$.

Replacing 4 by any other index between 4 and n, we conclude that $\phi(D_{\{1,\mu\}}) = D_{\{i,\pi(\mu)\}}$ with π a permutation from S_n (where we may assign $\pi(1) = i$). Now take $\nu, \mu \in \{2, \ldots, n\}$ with $\nu \neq \mu$. Writing $\phi(D_{\{\nu,\mu\}}) = D_{\{x,y\}}$, we conclude that $\{x, y\} \cap \{i, \pi(\mu)\} \neq \emptyset$ and $\{x, y\} \cap \{i, \pi(\nu)\} \neq \emptyset$. But assuming $i \in \{x, y\}$ (after renumbering $i = x$, say) leads to the contradiction $\phi(D_{\{\nu,\mu\}}) = D_{\{i,y\}} = \phi(D_{\{1,\pi^{-1}(y)\}})$. Hence, $\{x, y\} = \{\pi(\nu), \pi(\mu)\}$ and therefore $\phi(D_{\{\nu,\mu\}}) = D_{\{\pi(\nu),\pi(\mu)\}}$, which concludes the proof. □

2.3. Most n-point configurations are reconstructible from distances

In this section K is a field of characteristic not equal to 2 (e.g., $K = \mathbb{R}$ or $K = \mathbb{C}$) and V is an m-dimensional vector space over K equipped with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. Let $G = \mathrm{O}(V) \subseteq \mathrm{GL}(V)$ be the orthogonal group given by this form. The following proposition is folklore.

Proposition 2.5. *Let $v_1, \ldots, v_n, w_1, \ldots, w_n \in V$ be vectors with*

$$\langle v_i, v_j \rangle = \langle w_i, w_j \rangle \quad \text{for all } i, j \in \{1, \ldots, n\}.$$

Set $r := \min\{n, m\}$. If some $(r \times r)$-minor of the Gram matrix $(\langle v_i, v_j \rangle)_{i,j=1,\ldots,n} \in K^{n \times n}$ is non-zero, then there exists a $g \in G$ such that $w_i = g(v_i)$ for all i.

Proof. After renumbering we may assume that $A := (\langle v_i, v_j\rangle)_{i,j=1,\dots,r}$ is invertible. In particular, $v_1, \dots, v_r$ are linearly independent. By the hypothesis, the same holds for $w_1, \dots, w_r$, and $v_i \mapsto w_i$ gives an isomorphism between $\bigoplus_{i=1}^r K v_i$ and $\bigoplus_{i=1}^r K w_i$ which respects the form. By Witt's extension theorem there exists a $g \in G$ with $g(v_i) = w_i$ for $i \leqslant r$. This concludes the proof for $n \leqslant m$. Now assume $n > m$ and take an index $i > m$. There exist $\alpha_1, \dots, \alpha_m \in K$ such that $v_i = \sum_{j=1}^m \alpha_j v_j$. So for $1 \leqslant k \leqslant m$ we have $\langle v_k, v_i\rangle = \sum_{j=1}^m \langle v_k, v_j\rangle \cdot \alpha_j$. It follows that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = A^{-1} \begin{pmatrix} \langle v_1, v_i\rangle \\ \vdots \\ \langle v_m, v_i\rangle \end{pmatrix}.$$

By the hypothesis, it follows that w_i can be expressed as a linear combination of $w_1, \dots, w_m$ *with the same coefficients*. Therefore,

$$w_i = \sum_{j=1}^m \alpha_j w_j = \sum_{j=1}^m \alpha_j g(v_j) = g(v_i). \qquad \square$$

We come to the main theorem of this section. We assume that K, V, and m are as above. We write V^n for the direct sum of n copies of V, so an n-point configuration is an element from V^n. $K[V^n]$ is the ring of polynomials on V^n.

Theorem 2.6. *Let n be a positive integer with $n \leqslant 3$ or $n \geqslant m+2$. Then there exists a non-zero polynomial $f \in K[V^n]$ such that every n-point configuration $(P_1, \dots, P_n)$ with $f(P_1, \dots, P_n) \neq 0$ is reconstructible from distances.*

Proof. The cases $n = 1$ or $m = 0$ are trivial. The case $m = 1$ will be proved in Section 3 (see Theorem 3.7). Therefore, we may assume that $2 \leqslant n \leqslant 3$ or $2 \leqslant m \leqslant n-2$.

Take indeterminates $D_{\{i,j\}}$ indexed by sets $\{i, j\} \subset \{1, \dots, n\}$ with $i \neq j$ and form the matrix

$$\mathcal{D} := \left(D_{\{i,j\}} - D_{\{i,n\}} - D_{\{j,n\}}\right)_{i,j=1,\dots,n-1}, \tag{2.3}$$

where we set $D_{\{i,i\}} := 0$ as usual. If $2 \leqslant m \leqslant n-2$, let I be the ideal of $(m+1) \times (m+1)$-minors of $\mathcal{D}$. Each permutation $\pi \in S_n$ induces a permutation ϕ_π of the $D_{\{i,j\}}$ by $\phi_\pi(D_{\{i,j\}}) = D_{\{\pi(i),\pi(j)\}}$. Let $H \leqslant S_{\binom{n}{2}}$ be the subgroup containing all the ϕ_π, and let $\mathcal{T}$ be a set of left coset representatives of H, so we have a disjoint union

$$S_{\binom{n}{2}} = \dot{\bigcup_{\psi \in \mathcal{T}}} \psi H.$$

We may assume that $\mathrm{id} \in \mathcal{T}$. Lemma 2.4 says that for every $\psi \in \mathcal{T} \setminus \{\mathrm{id}\}$ there exists an $F_\psi \in I$ such that $\psi(F_\psi) \notin I$. Set $F_1 := \prod_{\psi \in \mathcal{T} \setminus \{\mathrm{id}\}} \psi(F_\psi)$. If, on the other hand, $2 \leqslant n \leqslant 3$,

set $F_1 := 1$. In either case, set $r := \min\{n-1, m\}$ and let F_2 be a non-zero $(r \times r)$-minor of $\mathcal{D}$ (e.g., choose the first r rows and columns). Now set $F := F_1 F_2$.

We choose a basis of $V \cong K^m$ such that $\langle \cdot, \cdot \rangle$ takes diagonal form, so $\langle (\xi_1, \ldots, \xi_m), (\eta_1, \ldots, \eta_m) \rangle = \sum_{k=1}^m a_k \xi_k \eta_k$ with $a_k \in K \setminus \{0\}$. Let $x_{i,j}$ be further indeterminates $(i = 1, \ldots, n,\ j = 1, \ldots, m)$, so $K[V^n]$ can be identified with $K[x_{1,1}, \ldots, x_{n,m}]$. Let $\Phi : K[D_{\{1,2\}}, \ldots, D_{\{n-1,n\}}] \to K[x_{1,1}, \ldots, x_{n,m}]$ be the homomorphism of algebras given by $D_{\{i,j\}} \mapsto \sum_{k=1}^m a_k (x_{i,k} - x_{j,k})^2$ (see Proposition 2.2(b)). Recall that I is the kernel of Φ. Since $\psi(F_\psi) \notin I$ for all $\phi \in \mathcal{T} \setminus \{\mathrm{id}\}$ and $F_2 \notin I$ (since each non-zero homogeneous element in I has degree $> m$), we obtain that $f := \Phi(F) \neq 0$.

Let $P_1, \ldots, P_n \in V$ such that $f(P_1, \ldots, P_n) \neq 0$, and let $d_{\{i,j\}} = \langle P_i - P_j, P_i - P_j \rangle$ be the distances. We have

$$F\big(d_{\{1,2\}}, \ldots, d_{\{n-1,n\}}\big) = f(P_1, \ldots, P_n) \neq 0. \tag{2.4}$$

We wish to show that $P_1, \ldots, P_n$ form a reconstructible n-point configuration. Let $Q_1, \ldots, Q_n \in V$ be points with distances $d'_{\{1,2\}}, \ldots, d'_{\{n-1,n\}}$ such that the distribution of distances coincides with that of the P_i. Then there exists a permutation ϕ of the set $\mathcal{J} := \{\{i, j\} \subseteq \{1, \ldots, n\} \mid i \neq j\}$ (the index set of the D's) such that $d'_{\{i,j\}} = d_{\phi(\{i,j\})}$. There exists a permutation $\pi \in S_n$ such that $\phi = \psi \circ \phi_\pi$ with $\psi \in \mathcal{T}$. Thus,

$$d_{\psi(\{i,j\})} = d'_{\{\pi^{-1}(i), \pi^{-1}(j)\}}$$

for all $\{i, j\} \in \mathcal{J}$. Assume, by way of contradiction, that $\psi \neq \mathrm{id}$. Then $n \geqslant m + 2$, since for $n \leqslant 3$ all permutations of $\mathcal{J}$ are induced from permutations from S_n. Clearly, $\phi_{\pi^{-1}}$ preserves the ideal I, hence $F_\psi \in I$, implies $\phi_{\pi^{-1}}(F_\psi) \in I$. Therefore,

$$F_\psi\big(d'_{\{\pi^{-1}(1), \pi^{-1}(2)\}}, \ldots, d'_{\{\pi^{-1}(n-1), \pi^{-1}(n)\}}\big) = \big(\phi_{\pi^{-1}}(F_\psi)\big)\big(d'_{\{1,2\}}, \ldots, d'_{\{n-1,n\}}\big) = 0,$$

and hence

$$\big(\psi(F_\psi)\big)\big(d_{\{1,2\}}, \ldots, d_{\{n-1,n\}}\big) = F_\psi\big(d_{\psi(\{1,2\})}, \ldots, d_{\psi(\{n-1,n\})}\big) = 0,$$

contradicting (2.4). It follows that $\psi = \mathrm{id}$, so $d'_{\{i,j\}} = d_{\{\pi(i), \pi(j)\}}$ for all i, j. We have to show that there exists $g \in \mathrm{AO}(V)$ with $Q_i = g(P_{\pi(i)})$. For this purpose we may assume that π is the identity. By applying a shift with a vector from V we may further assume $P_n = Q_n = 0$. It follows from Eq. (2.2) that the Gram matrices $(\langle P_i, P_j \rangle)_{i,j=1,\ldots,n-1}$ and $(\langle Q_i, Q_j \rangle)_{i,j=1,\ldots,n-1}$ coincide. Moreover, (2.4) implies that an $(r \times r)$-minor of the Gram matrices is non-zero. Now Proposition 2.5 yields the desired result. □

Remark 2.7. For $4 \leqslant n \leqslant m + 1$ (the range not covered by Theorem 2.6), no relations exist between the distances $d_{\{i,j\}}$ of an n-point configuration. If K is algebraically closed, it follows from the surjectiveness of the categorical quotient (see [11, Theorem 3.5(ii)] or [6, Lemma 2.3.2]) that for any given values for the $d_{\{i,j\}}$ there exists an n-point configuration which has these distances. Therefore, in this case no n-point configuration is reconstructible from distances, with the possible exception of configurations where many of the distances are the same. It is not entirely clear whether the same holds for K not

algebraically closed (e.g., $K = \mathbb{R}$), since in this case the categorical quotient is no longer surjective. As an example, for $K = \mathbb{R}$ the distances must satisfy triangle inequalities. Nevertheless, we expect that also for $K = \mathbb{R}$ and $4 \leqslant n \leqslant m + 1$, all n-point configurations lying in some dense open subset are not reconstructible from distances.

Remark 2.8. Theorem 2.6 deals with the situation where all n points are indistinguishable. However, in applications it often happens that the points come in several "colors" (e.g., different sorts of atoms in quantum molecular dynamics). Then the natural permutation group is a direct product $S_{n_1} \times \cdots \times S_{n_r}$ of symmetric groups, where each S_{n_i} permutes the points of color i. Our result extends to this situation as well. For example, if there are red and blue points, one has to take three "partial" distributions: the distribution of distances between all red points, the distribution of distances between all blue points, and the distribution of distances between red and blue points. Together, these partial distributions will separate orbits of $S_{n_{\text{red}}} \times S_{n_{\text{blue}}} \times \mathrm{E}_m$ on a dense open subset. The analogous construction works for an arbitrary number of colors.

The argument why this works is roughly as follows: If the partial distributions coincide for two point configurations, then in particular the total distributions coincide. Hence, Theorem 2.6 applies and tells us that (with the exception of a "thin" closed set) the configurations are linked by a permutation from S_n. Now one uses the hypothesis that the partial distributions coincide (and assumes that the $d_{\{i,j\}}$ are pairwise distinct) to show that this permutation must actually lie in $S_{n_1} \times \cdots \times S_{n_r}$, i.e., every point of color i is again mapped to a point of color i.

2.4. Symmetric n-point configurations

The reconstructibility test provided by Theorem 2.6 fails for a variety of point configurations, including all those with repeated distances.

Lemma 2.9. *Let $P_1, \ldots, P_n \in V$ with $2 \leqslant m \leqslant n - 2$ and consider f, the polynomial function constructed in the proof of Theorem* 2.6. *If the pairwise distances between the P_i's are not all distinct then $f(P_1, \ldots, P_n) = 0$.*

Proof. Denote by $d_{\{i,j\}}$ the distance between P_i and P_j. Assume that there exists i_1, j_1, i_2, j_2 with $\{i_1, j_1\} \neq \{i_2, j_2\}$ such that $d_{\{i_1,j_1\}} = d_{\{i_2,j_2\}}$. Consider the permutation $\varphi \in S_{\binom{n}{2}}$ which permutes $\{i_1, j_1\}$ and $\{i_2, j_2\}$ and leaves all the other pairs $\{i, j\}$ unchanged. Observe that there does not exist $\pi \in S_n$ such that $\varphi\{i, j\} = \{\pi(i), \pi(j)\}$, for all $i, j = 1, \ldots, n$. Therefore, there exists $\psi \in \mathcal{T} \setminus \{\mathrm{id}\}$ and $\varphi_\pi \in H$ induced by a permutation $\pi \in S_n$ such that $\varphi = \psi \circ \varphi_\pi$.

Let F_ψ be any polynomial with $F_\psi \in I$ such that $\psi(F_\psi) \notin I$. We have $d_{\psi\{i,j\}} = d_{\{\pi^{-1}(i),\pi^{-1}(j)\}}$, for all $i, j = 1, \ldots, n$. This means that

$$\begin{aligned} 0 &= F_\psi\left(d_{\{\pi^{-1}(1),\pi^{-1}(2)\}}, \ldots, d_{\{\pi^{-1}(n-1),\pi^{-1}(n)\}}\right) \quad (\text{since } F_\psi \in I) \\ &= F_\psi\left(d_{\psi(\{1,2\})}, \ldots, d_{\psi(\{n-1,n\})}\right) = \psi F_\psi\left(d_{\{1,2\}}, \ldots, d_{\{n-1,n\}}\right). \end{aligned}$$

So one of the factors of $f(P_1, \ldots, P_n)$ is zero and the conclusion follows. □

Corollary 2.10. *If an n-point configuration $P_1, \dots, P_n$ with $2 \leqslant m \leqslant n-2$ has a non-trivial symmetry, i.e., if there exists $g \in \mathrm{AO}(V)$ and $\pi \in S_n \setminus \{\mathrm{id}\}$ such that*

$$(g \cdot P_1, \dots, g \cdot P_n) = \big(P_{\pi(1)}, \dots, P_{\pi(n)}\big),$$

then the polynomial function f constructed in the proof of Theorem 2.6 *is such that $f(P_1, \dots, P_n) = 0$.*

Proof. By the previous lemma, it is sufficient to show that there exists $\{i_1, j_1\} \neq \{i_2, j_2\}$ such that $d_{\{i_1,j_1\}} = d_{\{i_2,j_2\}}$. Since $\pi \neq \mathrm{id}$, there exists i_0 such that $\pi(i_0) \neq i_0$. We have $g \cdot P_i = P_{\pi(i)}$, for all i's, so by invariance of the distance under $\mathrm{AO}(V)$, this means that $d_{\{i_0,j\}} = d_{\{\pi(i_0),\pi(j)\}}$ for all j's. Therefore, $i_1 = i_0$, $i_2 = \pi(i_0)$, $j_2 = \pi(j_1)$, and any $j_1 \neq i_0, \pi(i_0)$ will do the trick. □

This does not mean that no symmetric n-point configuration is reconstructible from distances. Indeed a square is a counterexample for $n = 4$ (see Example 2.12 below). We now give a reconstructibility test which does not exclude all point configurations with repeated distances.

Proposition 2.11. *Let $P_1, \dots, P_n \in V$ be points in an m-dimensional vector space ($2 \leqslant m \leqslant n-2$) over a field K of characteristic not 2 equipped with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. Set $d_{\{i,j\}} := \langle P_i - P_j, P_i - P_j \rangle$, and assume that the matrix $(d_{\{i,j\}} - d_{\{i,n\}} - d_{\{j,n\}})_{i,j=1,\dots,n-1}$ has rank m (the "generic" rank). Let $G \leqslant S_{\binom{n}{2}}$ be the subgroup of all permutations ϕ with $d_{\phi(\{i,j\})} = d_{\{i,j\}}$ for all i, j. (In fact, G may be replaced by any smaller subgroup.) Moreover, let $H \leqslant S_{\binom{n}{2}}$ be the subgroup of all ϕ_π with $\pi \in S_n$, given by $\phi_\pi(\{i, j\}) = \{\pi(i), \pi(j)\}$. Consider a set $\mathcal{T} \subset S_{\binom{n}{2}}$ of double coset representatives with respect to G and H, i.e.,*

$$S_{\binom{n}{2}} = \dot{\bigcup_{\psi \in \mathcal{T}}} G \psi H.$$

Assume that $\mathrm{id} \in \mathcal{T}$*, and for each $\psi \in \mathcal{T} \setminus \{\mathrm{id}\}$ choose $F_\psi \in I \setminus \psi^{-1}(I)$ (where I is the ideal occurring in Lemmas* 2.3 *and* 2.4*), which is possible by Lemma* 2.4*. If*

$$\big(\psi(F_\psi)\big)\big(d_{\{1,2\}}, \dots, d_{\{n-1,m\}}\big) \neq 0$$

for all $\psi \in \mathcal{T} \setminus \{\mathrm{id}\}$, then $(P_1, \dots, P_n)$ is reconstructible from distances.

Proof. Since the proof is almost identical to the one of Theorem 2.6, we will be very brief here to avoid repetitions. Let $Q_1, \dots, Q_n \in V$ be points with (squared) distances $d'_{\{i,j\}}$ such that $d'_{\{i,j\}} = d_{\phi(\{i,j\})}$ with $\phi \in S_{\binom{n}{2}}$. Write $\phi = \rho \circ \psi \circ \phi_\pi$ with $\rho \in G$, $\psi \in \mathcal{T}$, and $\pi \in S_n$. Then

$$d_{\psi(\{i,j\})} = d_{(\rho\circ\psi)(\{i,j\})} = d_{(\phi\circ\phi_{\pi^{-1}})(\{i,j\})} = d_{\phi(\{\pi^{-1}(i),\pi^{-1}(j)\})} = d'_{\{\pi^{-1}(i),\pi^{-1}(j)\}},$$

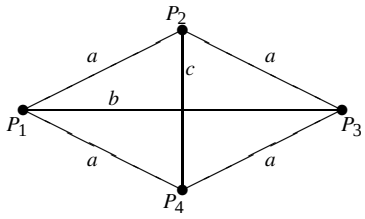


Fig. 5. A rhombus.

where the first equality follows from the definition of G. As in the proof of Theorem 2.6, we conclude from this that $\psi = \mathrm{id}$, so $d'_{\{i,j\}} = d_{(\rho\circ\phi_\pi)(\{i,j\})} = d_{\{\pi(i),\pi(j)\}}$ for all i, j. The rest of the proof proceeds as for Theorem 2.6. □

Example 2.12. In this example we show that all rhombi are reconstructible from distances. Consider a rhombus in K^2 with sides of length a and diagonals of length b and c (see Fig. 5), so

$$d_{\{1,2\}} = d_{\{2,3\}} = d_{\{3,4\}} = d_{\{1,4\}} = a, \qquad d_{\{1,3\}} = b, \quad \text{and} \quad d_{\{2,4\}} = c.$$

We assume that a, b, and c are all non-zero. If we order the 2-sets in $\{1,\dots,4\}$ as $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$, then the "symmetry group" G from Proposition 2.11 is generated by the permutations $(1,3)$ and $(1,3,4,6)$, and G is isomorphic to S_4. The image H of the embedding of S_4 into S_6 is generated by $(2,4)(3,5)$ and $(1,4,6,3)(2,5)$. It turns out that there are two double cosets in this case:

$$S_6 = GH \,\dot\cup\, G\psi H,$$

where ψ can be chosen as $\psi = (1,2)$. Since $m = 2$ and $n = 4$, we have only one generating relation, which is the determinant of the matrix $\mathcal{D}$ defined in (2.3). Choose this determinant as the polynomial F_ψ. Assume that the rhombus is not reconstructible. By Proposition 2.11 this implies $(\psi(F_\psi))(d_{\{1,2\}},\dots,d_{\{3,4\}}) = 0$. We obtain

$$a\big((a-b)^2 + c(c-b-2a)\big) = 0.$$

We have $b + c = 4a$. (This is Pythagoras' theorem, and it also follows from $F_\psi(d_{\{1,2\}},\dots,d_{\{3,4\}}) = bc(b+c-4a)$.) Substituting this into the above relation yields

$$3a(a-b)(c-a) = 0.$$

Since $a \neq 0$, this implies $a = b$ or $a = c$ (here we need to assume that $\mathrm{char}(K) \neq 3$), and by interchanging the roles of b and c we may assume $a = b$. But this means that our rhombus has in fact a bigger symmetry group $\widetilde{G}$ generated by the permutations $(1,2)$ and $(1,2,3,4,6)$. But now we see that $S_6 = \widetilde{G}H$, so there is only the trivial double

coset. It follows from Proposition 2.11 that the rhombus is in fact reconstructible from distances.

The computations for this example were done using the computer algebra system Magma [7].

2.5. Locally reconstructible n-point configurations

In this section, V is an m-dimensional vector space over K equipped with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. We now concentrate on the local characterization of n-point configurations. So we assume that the field K is either $\mathbb{R}$ or $\mathbb{C}$ and consider the problem of reconstructibility on small balls in V^n. Of course, for the concept of ball to make sense, V^n needs to be equipped with a norm. However, in general, the form $\langle \cdot, \cdot \rangle$ is *not* a hermitian dot product and so cannot be used to define the norm. We thus assume that in addition of V being equipped with the form $\langle \cdot, \cdot \rangle$, V^n is equipped with a norm $\| \cdot \|$. This first proposition addresses the problem of local reconstructibility for configurations of points whose mutual distances are all distinct.

Proposition 2.13. *Let $r = \min(n-1, m)$. Suppose that an n-point configuration $P_1, \ldots, P_n \in V$ is such that its distances are all distinct and its Gram matrix (defined as in (2.3)) has rank r. Then there exists a neighborhood N of $(P_1, \ldots, P_n) \in V^n$ such that any two n-point configurations in N are in the same orbit under the action of $\mathrm{AO}(V)$ if and only if their distribution of distances is the same.*

Proof. The distribution of distances is invariant under $\mathrm{AO}(V)$ so one direction of the statement is trivial. To prove the other direction, observe that a minor is a determinant, which is a polynomial function, and therefore continuous. So there exists a neighborhood U of $(P_1, \ldots, P_n) \in V^n$ such that the Gram matrix of any $(Q_1, \ldots, Q_n) \in U$ has a non-zero r-by-r minor.

Let us assume the contrary, so there exist two sequences of n-point configurations $\{Q_1^k, \ldots, Q_n^k\}_{k=1}^\infty$ and $\{R_1^k, \ldots, R_n^k\}_{k=1}^\infty$ in U, both converging to $P_1, \ldots, P_n$, and a sequence of permutations $\{\varphi_k\}_{k=1}^\infty$, such that for every k, $Q_1^k, \ldots, Q_n^k$ and $R_1^k, \ldots, R_n^k$ are not in the same orbit under the action of $\mathrm{AO}(V)$ but the distances $d^{Q^k}_{\{i,j\}} = \langle Q_i^k - Q_j^k, Q_i^k - Q_j^k \rangle$ are mapped to the distances $d^{R^k}_{\{i,j\}} = \langle R_i^k - R_j^k, R_i^k - R_j^k \rangle$ by φ_k so $d^{R^k}_{\{i,j\}} = d^{Q^k}_{\varphi_k\{i,j\}}$ for all distinct $i, j = 1, \ldots, n$. Since $S_{\binom{n}{2}}$ is finite, we may assume that $\varphi_k = \varphi$ is the same for every k. Taking the limit, we have

$$\lim_{k\to\infty} d^{R^k}_{\{i,j\}} = \lim_{k\to\infty} d^{Q^k}_{\varphi\{i,j\}}, \quad \text{for all distinct } i, j = 1, \ldots, n.$$

By continuity of the distance, this implies that for any distinct $i, j = 1, \ldots, n$ the distance $d_{\{i,j\}} = \langle P_i - P_j, P_i - P_j \rangle$ is equal to the distance $d_{\{\bar{i},\bar{j}\}} = \langle P_{\bar{i}} - P_{\bar{j}}, P_{\bar{i}} - P_{\bar{j}} \rangle$ where $\{\bar{i}, \bar{j}\} = \varphi\{i, j\}$. Since all the $d_{\{i,j\}}$ are distinct, then $\varphi = \mathrm{id}$ and thus $d^{R^k}_{\{i,j\}} = d^{Q^k}_{\{i,j\}}$ for every distinct $i, j = 1, \ldots, n$ and every k. By Proposition 2.5, this implies that $Q_1^k, \ldots, Q_n^k$

and $R_1^k, \ldots, R_n^k$ are in the same orbit relative to $\mathrm{AO}(V)$, for every k which contradicts our hypothesis, and the conclusion follows. □

The following proposition addresses the problem of local reconstructibility for n-point configurations in general.

Proposition 2.14. *Let $r = \min(n-1, m)$. Suppose that an n-point configuration $P_1, \ldots, P_n \in V$ is such that its Gram matrix (defined as in (2.3)) has rank r. Then there exists an $\epsilon > 0$ such that if the norm $\|(Q_1, \ldots, Q_n) - (P_1, \ldots, P_n)\| < \epsilon$ for some n-point configuration $Q_1, \ldots, Q_n \in V$ with the same distribution of distances as that of $P_1, \ldots, P_n$, then $Q_1, \ldots, Q_n$ and $P_1, \ldots, P_n$ are in the same orbit relative to $\mathrm{AO}(V)$.*

Proof. Again, by continuity, there exists a neighborhood U of $(P_1, \ldots, P_n) \in V^n$ such that the Gram matrix of any $(Q_1, \ldots, Q_n) \in U$ has a non-zero r-by-r minor. Let us assume the contrary so there exists a sequence of n-point configurations $\{Q_1^k, \ldots, Q_n^k\}_{k=1}^{\infty} \subset U$ converging to $P_1, \ldots, P_n$, and a sequence of permutations $\{\varphi_k\}_{k=1}^{\infty}$, such that none of the $Q_1^k, \ldots, Q_n^k$ are in the same orbit as $P_1, \ldots, P_n$ under the action of $\mathrm{AO}(V)$ but the distances $d_{\{i,j\}} = \langle P_i - P_j, P_i - P_j \rangle$ are mapped to the distances $d_{\{i,j\}}^{Q^k} = \langle Q_i^k - Q_j^k, Q_i^k - Q_j^k \rangle$ by φ_k so $d_{\varphi_k\{i,j\}} = d_{\{i,j\}}^{Q^k}$ for all $i, j = 1, \ldots, n$, $i \neq j$. Again we may assume that $\varphi_k = \varphi$ is the same for every k. Taking the limit, we obtain that $d_{\varphi\{i,j\}} = \lim_{k\to\infty} d_{\{i,j\}}^{Q^k}$, for all distinct $i, j = 1, \ldots, n$. By continuity of the distance, this implies that $d_{\varphi\{i,j\}} = d_{\{i,j\}}$. Therefore, $d_{\{i,j\}} = d_{\{i,j\}}^{Q^k}$ for every k and every distinct $i, j = 1, \ldots, n$. By Proposition 2.5, this implies that $Q_1^k, \ldots, Q_n^k$ and $P_1, \ldots, P_n$ are in the same orbit relative to $\mathrm{AO}(V)$ for every k, which contradicts our hypothesis, and the conclusion follows. □

When $V = \mathbb{R}^m$ (the case that interests us the most for applications), we can actually drop the requirement on the Gram matrix based on the following refinement of Proposition 2.5.

Lemma 2.15. *Let $G = \mathrm{O}(V) \subseteq \mathrm{GL}(V)$ be the orthogonal group given by the form $\langle \cdot, \cdot \rangle$. Let $v_1, \ldots, v_n, w_1, \ldots, w_n \in \mathbb{R}^m$ be vectors with*

$$\langle v_i, v_j \rangle = \langle w_i, w_j \rangle \quad \text{for all } i, j \in \{1, \ldots, n\}.$$

Then there exists a $g \in G$ such that $w_i = g(v_i)$ for all i.

Proof. Observe that since $V = \mathbb{R}$, the rank of the Gram matrix $(\langle v_i, v_j \rangle)_{i,j=1,\ldots,n}$ is equal to the dimension of the vector space spanned by $v_1, \ldots, v_n$. (This is *not* true over the complex field.) So we may assume, after relabeling, that $v_1, \ldots, v_\rho$ with $\rho \geqslant 1$, are linearly independent. By hypothesis, the same is true for $w_1, \ldots, w_\rho$. By Proposition 2.5, there exists $g \in G$ such that $g(v_i) = w_i$, for all $i = 1, \ldots, \rho$.

For any k such that $n \geqslant k > \rho$, there exists $\alpha_1, \ldots, \alpha_\rho$ such that $v_k = \sum_{j=1}^{\rho} \alpha_j v_j$. So for $1 \leqslant k \leqslant \rho$ we have $\langle v_k, v_i \rangle = \sum_{j=1}^{\rho} \langle v_i, v_j \rangle \cdot \alpha_j$. It follows that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_\rho \end{pmatrix} = \big(\big(\langle v_i, v_j \rangle\big)_{i,j=1,\ldots,\rho}\big)^{-1} \begin{pmatrix} \langle v_1, v_i \rangle \\ \vdots \\ \langle v_\rho, v_i \rangle \end{pmatrix}.$$

By the hypothesis, w_i can be expressed as a linear combination of $w_1, \ldots, w_m$ *with the same coefficients*. Therefore

$$w_i = \sum_{j=1}^{m} \alpha_j w_j = \sum_{j=1}^{m} \alpha_j g(v_j) = g(v_i). \qquad \square$$

Corollary 2.16. *For any n-point configuration $P_1, \ldots, P_n \in \mathbb{R}^m$ whose distances are all distinct, there exists a neighborhood N of $(P_1, \ldots, P_n) \in (\mathbb{R}^m)^n$ such that any two n-point configurations in N are in the same orbit under the action of $\mathrm{AO}(V)$ if and only if their distribution of distances is the same.*

Corollary 2.17. *For any n-point configuration $P_1, \ldots, P_n \in \mathbb{R}^m$ there exists an $\epsilon > 0$ such that if the norm $\|(Q_1, \ldots, Q_n) - (P_1, \ldots, P_n)\| < \epsilon$ for some n-point configuration $Q_1, \ldots, Q_n \in V$ with the same distribution of distances as that of $P_1, \ldots, P_n$, then $Q_1, \ldots, Q_n$ and $P_1, \ldots, P_n$ are in the same orbit relative to $\mathrm{AO}(V)$.*

3. Reconstruction from volumes

Given n points $P_1, \ldots, P_n \in \mathbb{R}^2$ in a plane, we may consider all areas $A_{i,j,k}$ of triangles spanned by three of these points P_i, P_j, and P_k. Clearly, these areas are preserved by the action of all translations and all linear maps with determinant ± 1. As in the preceding section, we can consider the *distribution* of areas, and ask whether an n-point configuration is reconstructible from this distribution up to the above action and permutations of the points. Again we will generalize this to configurations of points P_i lying in K^m, with K a field and m any dimension. Since we are interested in invariants which are preserved by all linear maps with determinant ± 1, it makes sense to consider volumes of m-simplices spanned by $m+1$ points $P_{i_0}, \ldots, P_{i_m}$. These volumes are conveniently expressed by the determinants

$$a_{i_0,\ldots,i_m} := \det\big(P_{i_1} - P_{i_0}, \ldots, P_{i_m} - P_{i_0}\big) \tag{3.1}$$

(where the P_i are takes to be column vectors). The determinants are really the "signed volumes," so we need to consider them up to signs, which is equivalent to taking squares. This discussion leads to the following definition.

Definition 3.1. Let K be a field and $n > m$ positive integers. For an n-point configuration $P_1, \ldots, P_n \in K^m$ form the "volumes" $a_{i_0,\ldots,i_m}$ as in (3.1) and the polynomial

$$V_{P_1,\ldots,P_n}(X) = \prod_{1 \leqslant i_0 < \cdots < i_m \leqslant n} \bigl(X - a^2_{i_0,\ldots,i_m}\bigr).$$

($V_{P_1,\ldots,P_n}(X)$ encodes the distribution of volumes.) An n-point configuration $P_1, \ldots, P_n \in K^m$ is called *reconstructible from volumes* if the following holds: if $Q_1, \ldots, Q_n$ is another n-point configuration with $V_{Q_1,\ldots,Q_n}(X) = V_{P_1,\ldots,P_n}(X)$, then there exist a permutation $\pi \in S_n$, a linear map $\phi \in \mathrm{GL}_m(K)$ with $\det(\phi) = \pm 1$, and a vector $v \in K^m$ such that

$$Q_i = \phi\bigl(P_{\pi(i)} + v\bigr) \quad \text{for all } i = 1, \ldots, n.$$

Remark 3.2.

(a) If we are working in the plane, i.e., $m = 2$, we will of course speak of reconstructibility from *areas* instead of volumes.
(b) For $m = 1$, the above concept of reconstructibility from volumes coincides with reconstructibility from distances introduced in Definition 2.1.

3.1. Non-reconstructible configurations

Again the first issue is to find configurations which are not reconstructible from volumes. Our main interest will be two-dimensional real space. A computation in Magma [7] yields that in $\mathbb{R}^2$ all 4-point configurations are reconstructible from volumes. For $n = 5$ we obtain counterexamples (whose construction also involved Magma computations). One of the simplest of these is given in Fig. 6.

We put the points on a grid of length 1. The two configurations in Fig. 6 lie in different orbits of $S_5 \times \mathrm{AGL}_2(\mathbb{R})$, since in the first configuration all points lie on two parallel lines, which is not the case in the second configuration. But the signed areas $a_{i,j,k}$ are as follows:

	$a_{1,2,3}$	$a_{1,2,4}$	$a_{1,2,5}$	$a_{1,3,4}$	$a_{1,3,5}$	$a_{1,4,5}$	$a_{2,3,4}$	$a_{2,3,5}$	$a_{2,4,5}$	$a_{3,4,5}$
P	1	1	1	−2	−4	−2	−2	−4	−2	0
Q	1	2	2	1	−1	−4	0	−2	−4	−2

So the distributions of areas coincide.

For $n = 6$ we get an even simpler example which is given in Fig. 7.

The configurations in Fig. 7 lie in different orbits of $S_6 \times \mathrm{AGL}_2(\mathbb{R})$ since the first configuration has three connecting vectors between points which are equal and the second one has not. But it is easy to see that the configurations have the same distribution of areas. Moreover, we can add an arbitrary number of points on the upper dotted line in both configurations to obtain pairs of n-point configurations with equal distributions of areas for $n \geqslant 6$.

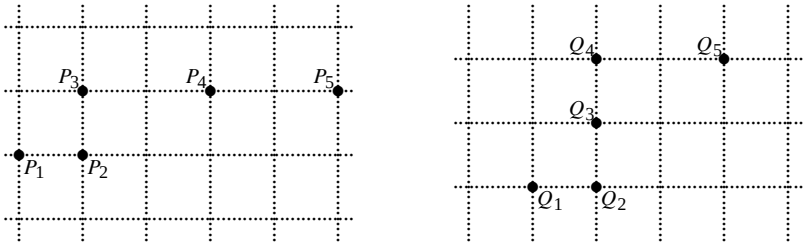


Fig. 6. Two 5-point configurations with the same distribution of areas.

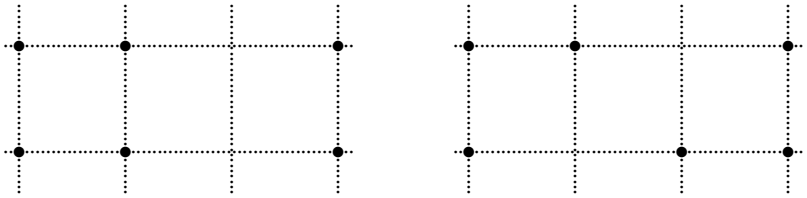


Fig. 7. Two 6-point configurations with the same distribution of areas.

To get examples in dimension $m \geqslant 3$, one can embed the two-dimensional examples given here into m-space and then add the $m-2$ points with coordinates $(0,0,1,0,\ldots,0),\ldots,(0,\ldots,0,1)$.

3.2. Relation-preserving permutations

In this section K is a field, n and m are positive integers with $n > m$, and $x_{i,j}$ are indeterminates ($1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$). For $1 \leqslant i_0 < \cdots < i_m \leqslant n$ we take further indeterminates $A_{i_0,\ldots,i_m}$. Write $K[\underline{A}]$ for the polynomial ring in the $A_{i_0,\ldots,i_m}$ and let $I \subseteq K[\underline{A}]$ be the kernel of the map

$$\Phi : K[\underline{A}] \to K[\underline{x}], \quad A_{i_0,\ldots,i_m} \mapsto \det\bigl(x_{i_j,k} - x_{i_0,k}\bigr)_{j,k=1,\ldots,m}.$$

For $i_0,\ldots,i_m \in \{1,\ldots,n\}$ pairwise distinct, select the permutation π of the set $\{0,\ldots,m\}$ such that $i_{\pi(0)} < i_{\pi(1)} < \cdots < i_{\pi(m)}$ and set

$$A_{i_0,\ldots,i_m} := \operatorname{sgn}(\pi) \cdot A_{i_{\pi(0)},\ldots,i_{\pi(m)}}. \tag{3.2}$$

Lemma 3.3.

(a) *If* $i_0, \ldots, i_{m+1} \in \{1, \ldots, n\}$ *are pairwise distinct, then*

$$\sum_{k=0}^{m+1} (-1)^k A_{i_0,\ldots,i_{k-1},i_{k+1},\ldots,i_{m+1}} \in I.$$

(b) I *is generated by the polynomials* $\sum_{k=0}^{m+1} (-1)^k A_{i_0,\ldots,i_{k-1},i_{k+1},\ldots,i_{m+1}}$ *with* $1 \leqslant i_0 < \cdots < i_{m+1} \leqslant n$ *and by homogeneous polynomial of degree* > 1 *which only involve the* $A_{n,i_1,\ldots,i_m}$ *with* $1 \leqslant i_1 < \cdots < i_m < n$.[1]

(c) *For* $j \in \{1, \ldots, n\}$ *the* $A_{j,i_1,\ldots,i_m}$ *with* $1 \leqslant i_1 < \cdots < i_m \leqslant n$, $i_k \neq j$, *are linearly independent modulo* I.

Proof. It is convenient to write P_i for the (column) vector $(x_{i,1}, \ldots, x_{i,m})^{\mathrm{T}}$, so for $i_0, \ldots, i_m \in \{1, \ldots, n\}$ in increasing order we have

$$\Phi\big(A_{i_0,\ldots,i_m}\big) = \det\big(P_{i_1} - P_{i_0}, \ldots, P_{i_m} - P_{i_0}\big), \tag{3.3}$$

which is equal to $\sum_{k=0}^{m} (-1)^k \det(P_{i_0}, \ldots, P_{i_{k-1}}, P_{i_{k+1}}, \ldots, P_{i_m})$. This shows that (3.3) is also valid if the i_j are not increasing.

(a) By (3.3) we have

$$\begin{aligned}
&\Phi\big(A_{i_0,\ldots,i_m}\big) \\
&\quad = \det\big(\big(P_{i_1} - P_{i_{m+1}}\big) - \big(P_{i_0} - P_{i_{m+1}}\big), \ldots, \big(P_{i_m} - P_{i_{m+1}}\big) - \big(P_{i_0} - P_{i_{m+1}}\big)\big) \\
&\quad = \Phi\big(A_{i_{m+1},i_1,\ldots,i_m}\big) - \Phi\big(A_{i_{m+1},i_0,i_2,\ldots,i_m}\big) + - \cdots + (-1)^m \Phi\big(A_{i_{m+1},i_0,\ldots,i_{m-1}}\big) \\
&\quad = \Phi\big(A_{i_0,\ldots,i_{m-1},i_{m+1}}\big) - + \cdots + (-1)^m \Phi\big(A_{i_1,\ldots,i_m,i_{m+1}}\big).
\end{aligned}$$

This yields (a).

(b) The relations between the $\Phi(A_{n,i_1,\ldots,i_m})$ are known from classical invariant theory (see [9] or [10]) to be the Plücker relations, which are homogeneous and non-linear. Let $J \subseteq K[\underline{A}]$ be the ideal generated by the linear relations given in (b) and the Plücker relations. By (a) we have $J \subseteq I$. Conversely, take $f \in I$. Using the linear relations from (b), we can substitute every $A_{i_0,\ldots,i_m}$ appearing in f by $\sum_{k=0}^{m} (-1)^k A_{n,i_0,\ldots,i_{k-1},i_{k+1},\ldots,i_m}$. In this way we obtain $g \in K[\underline{A}]$ with $f \equiv g \bmod J$, and g only involves indeterminates $A_{i_0,\ldots,i_m}$ with $i_0 = n$. But $f \in I$ implies $g \in I$, so g lies in the ideal generated by the Plücker relations. Thus, $f \in J$.

(c) It follows from (b) that the $\Phi(A_{n,i_1,\ldots,i_m})$ with $1 \leqslant i_1 < \cdots < i_m < n$ are linearly independent. But the same argument can be made with any other index j instead of n. This implies (c). □

[1] The non-linear polynomials are the well-known Plücker relations, which we do not need to present here explicitly.

The next lemma shows that the linear relations given in Lemma 3.3 are the only ones of their kind.

Lemma 3.4. *Let $l \in K[\underline{A}]$ be a non-zero linear combination of at most $m+2$ of the indeterminates $A_{i_0,\ldots,i_m}$. Assume that all the coefficients in l are 1 or -1, and $l \in I$. Then*

$$l = \sum_{k=0}^{m+1} (-1)^k A_{i_0,\ldots,i_{k-1},i_{k+1},\ldots,i_{m+1}} \tag{3.4}$$

with $i_1, \ldots, i_{m+2} \in \{1, \ldots, n\}$ pairwise distinct.

Proof. Take any $A_{i_0,\ldots,i_m}$ which occurs in l. Define a homomorphism $\phi : K[\underline{A}] \to K[\underline{A}]$ by sending each $A_{j_0,\ldots,j_m}$ with $i_0 \in \{j_0, \ldots, j_m\}$ to itself and by sending each $A_{j_0,\ldots,j_m}$ with $i_0 \notin \{j_0, \ldots, j_m\}$ to $\sum_{k=0}^{m} (-1)^k A_{i_0,j_0,\ldots,j_{k-1},j_{k+1},\ldots,j_m}$. Lemma 3.3(a) implies that $\phi(f) \equiv f \bmod I$ holds for all $f \in K[\underline{A}]$. Thus, $\phi(l) \in I$. But by Lemma 3.3(c) this implies $\phi(l) = 0$. But $A_{i_0,\ldots,i_m}$ occurs as a summand in $\phi(l)$ and must therefore be cancelled out by something. Hence, a summand of the form $\pm A_{j_0,i_1,\ldots,i_m}$ with $j_0 \notin \{i_0, \ldots, i_m\}$ must occur in l. The same argument can be applied to the other indices of $A_{i_0,\ldots,i_m}$, and we find summands $\pm A_{i_0,\ldots,i_{k-1},j_k,i_{k+1},\ldots,i_m}$ with $j_k \notin \{i_0, \ldots, i_m\}$ in l. We have already found $m+2$ summands in l, hence these are all summands.

Now we apply the same argument to $A_{j_0,i_1,\ldots,i_m}$. Doing so we find that for each $k \in \{1, \ldots, m\}$ there must occur an indeterminate in l whose indices include all of $j_0, i_1, \ldots, i_{k-1}, i_{k+1}, \ldots, i_m$. Ruling out all other possibilities, we see that this indeterminate must be $A_{i_0,\ldots,i_{k-1},j_k,i_{k+1},\ldots,i_m}$, so $j_k = j_0$. Setting $i_{m+1} := j_0$, we find that up to the signs the summands of l are as claimed in the lemma.

If K has characteristic 2 then nothing has to be shown about signs and we are done. So assume $\operatorname{char}(K) \neq 2$ and write $l' := \sum_{k=0}^{m+1} (-1)^k A_{i_0,\ldots,i_{k-1},i_{k+1},\ldots,i_{m+1}}$. Assume that l is neither l' nor $-l'$. Since l' lies in I by Lemma 3.3(a), the same is true for $(l+l')/2$. But $(l+l')/2$ is non-zero, has coefficients ± 1, and has fewer than $m+2$ summands. By the above discussion, this is impossible. Hence, we conclude that $l = \pm l'$. Performing a permutation with sign -1 on the indices transforms l' into $-l'$, so the case $l = -l'$ is also dealt with. □

The following proposition is analogous to Lemma 2.4.

Proposition 3.5. *Let $\phi : K[\underline{A}] \to K[\underline{A}]$ be an algebra-automorphism sending each $A_{i_0,\ldots,i_m}$ to $\pm A_{j_0,\ldots,j_m}$ for some $j_0, \ldots, j_m \in \{1, \ldots, n\}$ (where the signs may be chosen independently). If $\phi(I) \subseteq I$, then there exists $\pi \in S_n$ and $\varepsilon \in \{\pm 1\}$ such that for $1 \leqslant i_0 < \cdots < i_m \leqslant n$ we have*

$$\phi\big(A_{i_0,\ldots,i_m}\big) = \varepsilon \cdot A_{\pi(i_0),\ldots,\pi(i_m)}.$$

Proof. If $n = m+1$, there is only one indeterminate $A_{i_0,\ldots,i_m}$, so there is nothing to show. Hence, we may assume that $n \geqslant m+2$. Set $\mathcal{M} := \{S \subset \{1, \ldots, n\} \mid |S| = m+1\}$. We

have a bijection $\psi : \mathcal{M} \to \mathcal{M}$ induced from ϕ by defining $\psi(\{i_0, \ldots, i_m\}) = \{j_0, \ldots, j_m\}$ if $\phi(A_{i_0,\ldots,i_m}) = \pm A_{j_0,\ldots,j_m}$. For $S = \{i_0, \ldots, i_m\} \in \mathcal{M}$ with $i_0 < \cdots < i_m$ we write $A_S := A_{i_0,\ldots,i_m}$, so $\phi(A_S) = \pm A_{\psi(S)}$. The bulk of the proof consists of constructing a permutation $\pi \in S_n$ such that

$$\psi(S) = \pi(S) \tag{3.5}$$

for all $S \in \mathcal{M}$, where the right-hand side means element-wise application of π.

Take a subset $T \subseteq \{1, \ldots, n\}$ with $m+2$ elements and write $T = \{i_0, \ldots, i_{m+1}\}$ with $i_0 < \cdots < i_{m+1}$. By Lemma 3.3(a) the polynomial $l = \sum_{k=0}^{m+1} (-1)^k A_{T\setminus\{i_k\}}$ lies in I, hence also $\phi(l) \in I$. But $\phi(l) = \sum_{k=0}^{m+1} \pm A_{\psi(T\setminus\{i_k\})}$. From Lemma 3.4 we see that $\widetilde{T} := \bigcup_{k=0}^{m+1} \psi(T \setminus \{i_k\})$ must have precisely $m+2$ elements. Since each $\psi(T \setminus \{i_k\})$ has $m+1$ elements, there exists a map $\pi_T : T \to \widetilde{T} \subseteq \{1, \ldots, n\}$ with $\psi(T \setminus \{i_k\}) = \widetilde{T} \setminus \{\pi_T(i_k)\}$. Since ψ is injective this also holds for π_T, so $\pi_T(T) = \widetilde{T}$. Thus, for all $S \in \mathcal{M}$ with $S \subset T$ we have

$$\psi(S) = \pi_T(S) \tag{3.6}$$

(where the right-hand side means element-wise application of π_T).

In the sequel we will make frequent use of the following rule: if two sets $S, S' \in \mathcal{M}$ have m elements in common, then also $\psi(S)$ and $\psi(S')$ share m elements. Indeed, there is a linear polynomial l of the type (3.4) in which both A_S and $A_{S'}$ occur. By Lemma 3.3(a), l lies in I, hence also $\phi(l) \in I$. But $A_{\psi(S)}$ and $A_{\psi(S')}$ occur in $\phi(l)$, hence $|\psi(S) \cap \psi(S')| = m$ by Lemma 3.4.

Now take two subsets $T, T' \subseteq \{1, \ldots, n\}$ with $|T| = |T'| = m+2$ such that $S := T \cap T'$ has $m+1$ elements. We will show that π_T and $\pi_{T'}$ coincide on S. Write

$$T = S \cup \{j\} \quad \text{and} \quad T' = S \cup \{k\}$$

with $j, k \in \{1, \ldots, n\}$. For $l \in S$ set $S_l := T' \setminus \{l\}$, so $S_l \in \mathcal{M}$. Then $|S_l \cap (T \setminus \{l\})| = m$ and $|S_l \cap S| = m$, so $\psi(S_l)$ shares m elements with $\psi(T \setminus \{l\}) = \pi_T(T) \setminus \{\pi_T(l)\}$ and with $\psi(S) = \pi_T(S) = \pi_T(T) \setminus \{\pi_T(j)\}$. But $\psi(S_l)$ cannot be a subset of $\pi_T(T)$ since this would imply

$$\psi(S_l) = \pi_T\big(\pi_T^{-1}\big(\psi(S_l)\big)\big) = \psi\big(\pi_T^{-1}\big(\psi(S_l)\big)\big),$$

contradicting the injectiveness of ψ, since $S_l \not\subseteq T$. It follows that $\psi(S_l) = \pi_T(T \setminus \{j, l\}) \cup \{r_l\}$ with $r_l \in \{1, \ldots, n\} \setminus \pi_T(T)$. We can write this slightly simpler as $\psi(S_l) = \pi_T(S \setminus \{l\}) \cup \{r_l\}$. On the other hand, we have $S_l \subset T'$, so

$$\psi(S_l) = \pi_{T'}(S_l) = \pi_{T'}\big(S \setminus \{l\}\big) \cup \big\{\pi_{T'}(k)\big\}.$$

Intersecting the resulting equality $\pi_T(S \setminus \{l\}) \cup \{r_l\} = \pi_{T'}(S \setminus \{l\}) \cup \{\pi_{T'}(k)\}$ over all $l \in S$ yields $\bigcap_{l\in S}\{r_l\} = \{\pi_{T'}(k)\}$. Thus, $r_l = \pi_{T'}(k)$ independently of l, and $\pi_T(S \setminus \{l\}) = \pi_{T'}(S \setminus \{l\})$ for all $l \in S$. This shows that $\pi_T(l) = \pi_{T'}(l)$ for all $l \in S$, as claimed.

We proceed by taking any two subsets T, $T' \subseteq \{1,\dots,n\}$ with $|T| = |T'| = m+2$. We can move from T to T' by successively exchanging elements. Using the above result, we see that π_T and $\pi_{T'}$ coincide on $T \cap T'$. Thus, we can define $\pi : \{1,\dots,n\} \to \{1,\dots,n\}$ such that for every subset $T \subseteq \{1,\dots,n\}$ with $|T| = m+2$ the restriction $\pi|_T$ coincides with π_T. Now (3.5) follows from (3.6), and it also follows that $\pi \in S_n$.

Take $S \in \mathcal{M}$ and write $S = \{i_0,\dots,i_m\}$ with $i_0 < \cdots < i_m$. The definition of ψ and (3.5) imply that

$$\phi\big(A_{i_0,\dots,i_m}\big) = \varepsilon_S \cdot A_{\pi(i_0),\dots,\pi(i_m)}$$

with $\varepsilon_S \in \{\pm 1\}$. We wish to show that ε_S does not depend on S. To this end, take $T \subseteq \{1,\dots,n\}$ with $|T| = m+2$ and write $T = \{i_0,\dots,i_{m+1}\}$ with $i_0 < \cdots < i_{m+1}$. By Lemma 3.3(a), $l := \sum_{k=0}^{m+1} (-1)^k A_{i_0,\dots,i_{k-1},i_{k+1},\dots,i_{m+1}}$ lies in I, hence $\phi(l) \in I$. But

$$\phi(l) = \sum_{k=0}^{m+1} (-1)^k \varepsilon_{T\setminus\{i_k\}} \cdot A_{\pi(i_0),\dots,\pi(i_{k-1}),\pi(i_{k+1}),\dots,\pi(i_{m+1})}.$$

Lemma 3.4 implies that all $\varepsilon_{T\setminus\{i_k\}}$ coincide. This shows that if two sets S, $S' \in \mathcal{M}$ share m elements, then $\varepsilon_S = \varepsilon_{S'}$. But since we can move from any $S \in \mathcal{M}$ to any other $S' \in \mathcal{M}$ by successively exchanging elements, it follows that indeed all ε_S coincide. This completes the proof. □

3.3. Most n-point configurations are reconstructible from volumes

In this section K is a field and V is an m-dimensional vector space over K. The following proposition is well known.

Proposition 3.6. *Let $v_1,\dots,v_n$, $w_1,\dots,w_n \in V$ be vectors with $n \geqslant m$, such that for all $1 \leqslant i_1 < \cdots < i_m \leqslant n$*

$$d_{i_1,\dots,i_m} := \det\big(v_{i_1} \dots v_{i_m}\big) = \det\big(w_{i_1} \dots w_{i_m}\big).$$

If at least one of the $d_{i_1,\dots,i_m}$ is non-zero, then there exists a $\phi \in \mathrm{SL}(V)$ such that $w_i = \phi(v_i)$ for all i.

Proof. After renumbering we may assume that $d_{1,2,\dots,m}$ is non-zero. Hence, $v_1,\dots,v_m$ and $w_1,\dots,w_m$ are linearly independent, and there exists a (unique) $\phi \in \mathrm{SL}(V)$ such that $w_i = \phi(v_i)$ for all $i \leqslant m$. Assume $n > m$ and take an index $i > m$. There exist $\alpha_1,\dots,\alpha_m \in K$ such that $v_i = \sum_{j=1}^m \alpha_j v_j$. Indeed, by Cramer's rule we have $\alpha_j = (-1)^{n-j} d_{1,\dots,j-1,j+1,\dots,m,i}/d_{1,\dots,m}$. By the hypothesis, it follows that w_i can be expressed as a linear combination of $w_1,\dots,w_m$ *with the same coefficients*. Therefore,

$$w_i = \sum_{j=1}^m \alpha_j w_j = \sum_{j=1}^m \alpha_j \phi(v_j) = \phi(v_i). \qquad \square$$

We come to the main theorem of this section. We assume that K is a field, V is an m-dimensional vector space over K, and $n > m$ is an integer. We write V^n for the direct sum of n copies of V, so an n-point configuration is an element from V^n. $K[V^n]$ is the ring of polynomials on V^n.

Theorem 3.7. *There exists a non-zero polynomial $f \in K[V^n]$ such that every n-point configuration $(P_1, \ldots, P_n)$ with $f(P_1, \ldots, P_n) \neq 0$ is reconstructible from volumes.*

Proof. Clearly, we may assume $m > 0$. For indices $1 \leqslant i_0 < \cdots < i_m \leqslant n$, let $A_{i_0,\ldots,i_m}$ be an indeterminate, and for $i_0, \ldots, i_m \in \{1, \ldots, n\}$ pairwise distinct define $A_{i_0,\ldots,i_m}$ as in (3.2). Let $I \subseteq K[\underline{A}]$ be the kernel of the map $\Phi : K[\underline{A}] \to K[V^n]$ sending $A_{i_0,\ldots,i_m}$ to the polynomial $\Phi(A_{i_0,\ldots,i_m})$ with $\Phi(A_{i_0,\ldots,i_m})(P_1, \ldots, P_n) = \det(P_{i_1} - P_{i_0}, \ldots, P_{i_m} - P_{i_0})$ for $P_1, \ldots, P_n \in V$. Note that I is precisely the ideal introduced at the beginning of Section 3.2.

Let $G \subseteq \mathrm{Aut}_K(K[\underline{A}])$ be the group of all automorphisms ϕ of $K[\underline{A}]$ sending each $A_{i_0,\ldots,i_m}$ to $\pm A_{j_0,\ldots,j_m}$ with $1 \leqslant j_0 < \cdots < j_m \leqslant n$. For each permutation $\pi \in S_n$ and each $\varepsilon \in \{\pm 1\}$ there is an automorphism $\phi_{\pi,\varepsilon} \in G$ with $\phi_{\pi,\varepsilon}(A_{i_0,\ldots,i_m}) = \varepsilon \cdot A_{\pi(i_0),\ldots,\pi(i_m)}$. Let $H \leqslant G$ be the subgroup of all these $\phi_{\pi,\varepsilon}$, and choose a set $\mathcal{T}$ of left coset representatives of H in G with $\mathrm{id} \in \mathcal{T}$. Proposition 3.5 says that for every $\psi \in \mathcal{T} \setminus \{\mathrm{id}\}$ there exists an $F_\psi \in I$ such that $\psi(F_\psi) \notin I$. Set $F := A_{n,1,2,\ldots,m} \cdot \prod_{\psi \in \mathcal{T} \setminus \{\mathrm{id}\}} \psi(F_\psi)$ and $f := \Phi(F) \in K[V^n]$. $F \notin I$ implies that $f \neq 0$.

Let $P_1, \ldots, P_n \in V$ such that $f(P_1, \ldots, P_n) \neq 0$, and for $1 \leqslant i_0 < \cdots < i_m \leqslant n$ let $a_{i_0,\ldots,i_m} = \det(P_{i_1} - P_{i_0}, \ldots, P_{i_m} - P_{i_0})$ be the "signed volume." We have

$$F(\underline{a}) = f(P_1, \ldots, P_n) \neq 0. \tag{3.7}$$

We wish to show that $P_1, \ldots, P_n$ form a reconstructible n-point configuration. Let $Q_1, \ldots, Q_n \in V$ be points and set $a'_{i_0,\ldots,i_m} := \det(Q_{i_1} - Q_{i_0}, \ldots, Q_{i_m} - Q_{i_0})$. Assume that the distribution of volumes of $Q_1, \ldots, Q_n$ coincides with that of $P_1, \ldots, P_n$, i.e., $V_{Q_1,\ldots,Q_n}(X) = V_{P_1,\ldots,P_n}(X)$. This means that up to signs the $a'_{i_0,\ldots,i_m}$ are a permutation of the $a_{i_0,\ldots,i_m}$, so there exists a $\phi \in G$ such that for all $H \in K[\underline{A}]$ we have

$$\big(\phi(H)\big)(\underline{a}) = H(\underline{a}'). \tag{3.8}$$

There exist $\pi \in S_n$ and $\varepsilon \in \{\pm 1\}$ such that $\phi = \psi \circ \phi_{\pi,\varepsilon}$ with $\psi \in \mathcal{T}$. By way of contradiction, assume that $\psi \neq \mathrm{id}$. Clearly, $\phi_{\pi^{-1},\varepsilon}$ preserves the ideal I, hence $F_\psi \in I$ implies $H := \phi_{\pi^{-1},\varepsilon}(F_\psi) \in I$. Therefore, $H(\underline{a}') = (\Phi(H))(Q_1, \ldots, Q_n) = 0$, so (3.8) yields

$$\big(\psi(F_\psi)\big)(\underline{a}) = \big(\phi(H)\big)(\underline{a}) = H(\underline{a}') = 0,$$

contradicting (3.7). It follows that $\psi = \mathrm{id}$, so $\phi = \phi_{\pi,\varepsilon}$. We have to show that there exist $v \in V$ and $\psi \in \mathrm{GL}(V)$ with $\det(\psi) \in \{\pm 1\}$ such that $Q_i = \psi(P_{\pi(i)} + v)$ for all i. For this purpose we may assume that π is the identity. If $\varepsilon = -1$, we apply an (arbitrary) linear map with determinant -1 to $Q_1, \ldots, Q_n$. This will change all the signs of the $a'_{i_0,\ldots,i_m}$.

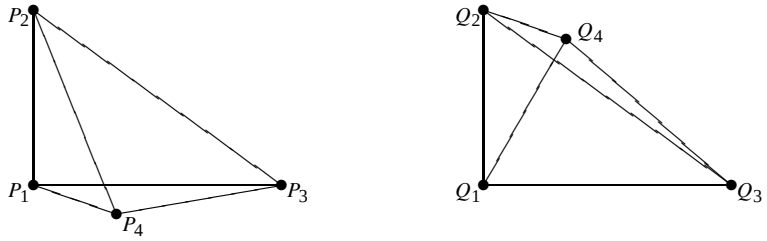


Fig. 8. Two 4-point configurations with the same distribution of distances and the same distribution of areas.

Hence, we may assume that $\varepsilon = 1$, so $\phi = \mathrm{id}$, and (3.8) implies $a'_{i_0,\ldots,i_m} = a_{i_0,\ldots,i_m}$ for all index vectors $i_0, \ldots, i_m$. Since $a_{n,1,2,\ldots,m} \neq 0$ (this was the purpose of introducing $A_{n,1,2,\ldots,m}$ as a factor into F), Proposition 3.6 yields that there exists $\sigma \in \mathrm{SL}(V)$ such that $\sigma(P_i - P_n) = Q_i - Q_n$ for all $i \in \{1, \ldots, n-1\}$. Setting $v := \sigma^{-1}(Q_n) - P_n$ gives the desired result $Q_i = \sigma(P_i + v)$ for $i \in \{1, \ldots, n\}$. □

Remark 3.8. Everything that was said in Section 2.4 about reconstructibility of configurations with symmetries carries over to reconstructibility from volumes. In particular, the analogue of Proposition 2.11 holds. Similarly, the analogues of Propositions 2.13 and 2.14 concerning local reconstructibility are also true.

3.4. Combining distances and volumes

Taking another look at Fig. 4, one notices that although the two configurations have the same distribution of distances, their distributions of areas are different. This brings up the idea to try to distinguish n-point configurations (up to the action of $S_n \times \mathrm{AO}_m(K)$) by considering the distribution of distances *and* the distribution of volumes. Could it be that by combining these data we might be able to separate all orbits? The following example shows that once again this is not the case. We take the following 4-point configurations in $\mathbb{R}^2$ (see Fig. 8):

$$\begin{aligned} P_1 &= (0,0), \quad P_2 = (0,6), \quad P_3 = \bigl(6\sqrt{2}, 0\bigr), \quad P_4 = \bigl(2\sqrt{2}, -1\bigr), \\ Q_1 &= (0,0), \quad Q_2 = (0,6), \quad Q_3 = \bigl(6\sqrt{2}, 0\bigr), \quad Q_4 = \bigl(2\sqrt{2}, 5\bigr). \end{aligned}$$

It is easy to see that the two configurations lie in different orbits of $S_4 \times \mathrm{AO}_2(\mathbb{R})$ (although they lie in the same orbit of $S_4 \times \mathrm{AGL}_2(\mathbb{R})$). We obtain the following distances $\sqrt{d_{i,j}}$ and signed areas $a_{i,j,k}$:

	$\sqrt{d_{1,2}}$	$\sqrt{d_{1,3}}$	$\sqrt{d_{1,4}}$	$\sqrt{d_{2,3}}$	$\sqrt{d_{2,4}}$	$\sqrt{d_{3,4}}$
P	6	$6\sqrt{2}$	3	$6\sqrt{3}$	$\sqrt{57}$	$\sqrt{33}$
Q	6	$6\sqrt{2}$	$\sqrt{33}$	$6\sqrt{3}$	3	$\sqrt{57}$

	$a_{1,2,3}$	$a_{1,2,4}$	$a_{1,3,4}$	$a_{2,3,4}$
P	$-36\sqrt{2}$	$-12\sqrt{2}$	$-6\sqrt{2}$	$-30\sqrt{2}$
Q	$-36\sqrt{2}$	$-12\sqrt{2}$	$30\sqrt{2}$	$6\sqrt{2}$

Acknowledgments

We thank Serkan Hosten and Greg Reid for inviting us to the Symbolic Computational Algebra Conference held in London, Ontario in 2002. This is where we first met and started this project. The idea of using distributions of invariants in order to separate the orbits was inspired by discussions of Mireille Boutin with David Cooper and Senem Velipasalar regarding their work on indexation [12]. This author is grateful to the SHAPE lab of Brown University for providing the environment for these discussions and thus the motivation for this paper.

References

[1] J.L. Mundy, A. Zisserman (Eds.), Geometric Invariance in Computer Vision, Artif. Intell., MIT Press, Cambridge, MA, 1992.
[2] R. Hartley, A. Zisserman, Multiple View Geometry in Computer Vision, Cambridge Univ. Press, Cambridge, 2001.
[3] N.M. Thiéry, Algebraic invariants of graphs: a study based on computer exploration, SIGSAM Bull. 34 (2000) 9–20.
[4] M. Pouzet, Quelques remarques sur les résultats de Tutte concernant le problème de Ulam, Publ. Dép. Math. (Lyon) 14 (1977) 1–8.
[5] H. Aslaksen, S.-P. Chan, T. Gulliksen, Invariants of S_4 and the shape of sets of vectors, Appl. Algebra Engrg. Comm. Comput. 7 (1996) 53–57.
[6] H. Derksen, G. Kemper, Computational Invariant Theory, Encyclopaedia Math. Sci., vol. 130, Springer-Verlag, Berlin, Heidelberg, New York, 2002.
[7] W. Bosma, J.J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997) 235–265.
[8] B. Char, K. Geddes, G. Gonnet, M. Monagan, S. Watt, Maple Reference Manual, Waterloo Maple, Waterloo, Ontario, 1990.
[9] H. Weyl, The Classical Groups, Princeton Univ. Press, Princeton, 1946.
[10] C. de Concini, C. Procesi, A characteristic free approach to invariant theory, Adv. in Math. 21 (1976) 330–354.
[11] P.E. Newstead, Intoduction to Moduli Problems and Orbit Spaces, Springer-Verlag, Berlin, Heidelberg, New York, 1978.
[12] T. Tasdizen, S. Velipasalar, D.B. Cooper, Shape based similarity measure for image retrieval, Technical Report SHAPE-TR-2001-03, SHAPE lab, Brown University, Providence, 2001.