Which Point Configurations are Determined by the Distribution of their Pairwise Distances?

Mireille Boutin and Gregor Kemper

January 26, 2004

Abstract

In a previous paper we showed that, for any $n \geq m + 2$, most sets of n points in $\mathbb{R}^m$ are determined (up to rotations, reflections, translations and relabeling of the points) by the distribution of their pairwise distances. But there are some exceptional point configurations which are not reconstructible from the distribution of distances in the above sense. In this paper, we concentrate on the planar case $m = 2$ and present a reconstructibility test with running time $O(n^{11})$. The cases of orientation preserving rigid motions (rotations and translations) and scalings are also discussed.

Introduction

In this paper, we present a quick and easy (but slightly imperfect) solution to the problem of characterizing the shape of sets of n points in Euclidean space, so-called n-point configurations, for any positive integer n. More precisely, an *n-point configuration* is a collection of n points in $\mathbb{R}^m$. Point configurations often arise in biological and medical imagery, as well as in the fields of archaeology, astronomy and cartography, to name just a few. For example, stellar constellations, minutiae of fingerprints, and distinguished points (landmarks) on medical images represent point configurations.

An important problem of computer vision is that of recognizing point configurations. In other words, the problem is to determine whether two point configurations have the same shape, that is to say, whether there exists a rotation and a translation (sometimes a reflection and/or a scaling are allowed as well) which maps the first point configuration onto the second. Let us first concentrate on the case of rigid motions, i.e. rotations, translations and reflections in $\mathbb{R}^m$. Note that any rigid motion can be written as (M, T), where M is an orthogonal m-by-m matrix and T is an m-dimensional (column) vector.

One of the biggest difficulties in trying to identify point configurations up to rigid motions is the absence of labels for the points: one does not know, a priori, which point is going to be mapped to which. If the points were already labeled in correspondence, then, following the so-called Procrustes approach (Gower [10]), one could analytically determine a rigid motion which maps the first string as close as possible (in the L^2 sense, for example) to the second. The statistical analysis of such methods is presented in Goodall [9]. Another way to proceed would be to compare the pairwise (labeled) distances between the points of each point configurations (Blumenthal [3]). Indeed, the following well known fact holds. See, for example, Boutin and Kemper [5] for a simple proof.

Proposition 0.1. *Let $p_1, \ldots, p_n$ and $q_1, \ldots, q_n$ be points in $\mathbb{R}^m$. If $\|p_i - p_j\| = \|q_i - q_j\|$ for every $i, j = 1, \ldots, n$, then there exists a rigid motion (M, T) such that $Mp_i + T = q_i$, for every $i = 1, \ldots, n$.*

A variety of methods have been developed for labeling the points of two n-point configuration in correspondence. See, for example, Hartley and Zisserman [12] for a description of some of these methods. But labeling the points is a complex task which we would much rather do without. Invariant theory suggests a possible approach for recognizing unlabeled points. The idea consists in comparing certain functions of the pairwise distances between the points of the configuration which have the property that they are unchanged by a relabeling of the points. These are often called *graph invariants* and have been computed in the case of

Value	# of Occurrences
1	4
$\sqrt{2}$	2

Table 1: Distribution of distances of a unit square.

$n = 4$ by Aslaksen et al. [1], and $n = 5$ by the second author [7, page 220]. Unfortunately, the case $n = 6$ or larger still stands as a computational challenge. Moreover, the invariants used are polynomial functions of the distances whose number and degrees increase dramatically with n. They are thus very sensitive to round off errors and noise.

In the following, we study an alternative approach based on the use of a very simple object: the distribution of the pairwise distances. The distribution of the pairwise distances of an n-point configuration is an array which lists all the different values of the pairwise distances between the points in increasing order and the number of times each value occurs. For example, the distribution of distances of four points situated at the corners of a unit square is given in Table 1.

Obviously, such a distribution remains unchanged under any rigid motion of the point configuration as well as any relabeling of the points. For $n = 1, 2$ or 3, it is easy to see that the distribution of distances completely characterize the n-point configuration up to a rigid motion. The case $m = 1$ was studied by Piccard (*Piccard* 1939). She claimed that two n-point configurations in $\mathbb{R}$ whose pairwise distances are all distinct are the same up to a rigid motion if and only if their distributions of distances are the same. Unfortunately, this claim was disproved by Bloom who provided a counterexample with $n = 6$ (*Bloom* 1977). For any $n \geq m + 2$, we proved that, *most of the time*, this distribution of the pairwise distances *completely* characterizes the shape of the point configuration (see [5, Theorem 2.6]).

To simplify our discussion, we introduce the concept of reconstructibility from distances.

Definition 0.2. *We say that the n-point configuration represented by $p_1, \ldots, p_n \in \mathbb{R}^m$ is* reconstructible from distances *if, for every $q_1, \ldots, q_n \in \mathbb{R}^m$ having the same distribution of distances, there exists a rigid motion (M, T) and a permutation π of the labels $\{1, \ldots, n\}$ such that $Mp_i + T = q_{\pi(i)}$, for every $i = 1, \ldots, n$.*

In the following, we shall often identify a point configuration and one of its representation $p_1, \ldots, p_n \in \mathbb{R}^m$. This is done for simplicity and we hope it will not create any confusion.

The actual reconstruction of a point configuration will *not* be addressed in this paper. However, to put this research in context, we like to make a few remarks. The problem of reconstructing a point configuration from its distribution of distances is encountered in X-ray crystallography (*Patterson* 1935, *Patterson* 1944) and in the mapping of restriction sites of DNA (*Stefik* 1978, *Dix & Kieronska* 1988, *Gwangsoo* 1988). For $m = 1$, it is known as the *turnpike problem* or, in the context of molecular biology, as the *partial digest problem*. An algebraic solution based on polynomial factorization which runs in pseudo-polynomial time was given by Rosenblatt and Seymour (*Rosenblatt & Seymour* 1982). Lemke and Werman showed that, in the case where the distances are integers, this solution runs in polynomial time (*Lamke & Werman* 1988). For the general case $m = 1$, Skiena et al. (*Skiena, Smith & Lemke* 2003) used a backtracking procedure that runs in $O(2^n n \log n)$, while Dakić (*Dakić* 2000) showed that in certain instances the reconstruction problem can be written as $0 - 1$ quadratic program and solved in polynomial time. These instances include the case where the solution to the reconstruction problem is unique. In general, the complexity of an algorithm to generate all the pairwise configurations with a given distribution of distances depends on the number of different solutions.

Theorem 2.6 of Boutin and Kemper [5] actually implies that there exists an open and dense subset $\Omega \subset (\mathbb{R}^m)^n$ of reconstructible point configurations. In Section 1, we concentrate on the planar case $m = 2$ and give an algorithm in $O(n^{11})$ steps to determine whether a point lies in Ω. A generalization to other dimensions m is also mentioned. Section 3 describes how an additional distribution can be used in the planar case in order to compare the orientation of two point configurations. In Section 4, we show that a slightly modified distribution can be used to completely characterize most point configurations up to rigid motions and scalings.

1 Reconstructible configurations

Denote by $\mathcal{P}$ the set of pairs

$$\mathcal{P} = \{\{i,j\} | i \neq j, i,j = 1,\dots,n\}.$$

Consider the group of permutations $S_{\binom{n}{2}}$ of the elements of $\mathcal{P}$. For any $\varphi \in S_{\binom{n}{2}}$ and any $\{i,j\} \in \mathcal{P}$, we denote by $\varphi \cdot \{i,j\}$ the image of $\{i,j\}$ under φ. For two point configurations to have the same distribution of distances means that there exists a permutation $\varphi \in S_{\binom{n}{2}}$ which maps the labeled pairwise distances of the first configuration onto the labeled pairwise distances of the second configuration. More precisely, if $p_1,\dots,p_n \in \mathbb{R}^m$ and $q_1,\dots,q_n \in \mathbb{R}^m$ have the same distribution of distances, let $d_{i,j} = \|p_i - p_j\|^2$ and $d'_{i,j} = \|q_i - q_j\|^2$, for all $\{i,j\} \in \mathcal{P}$. Then there exists $\varphi \in S_{\binom{n}{2}}$ such that

$$d_{\varphi\cdot\{i,j\}} = d'_{\{i,j\}}, \text{ for all } \{i,j\} \in \mathcal{P}.$$

For close enough point configurations, we have proved in [5] that one does not need to keep track of the labeling of the points. The proof is very short and we reproduce it here for completeness.

Proposition 1.1. *For any n-point configuration $p_1,\dots,p_n \in \mathbb{R}^m$, there exists a neighborhood U of $(p_1,\dots,p_n) \in (\mathbb{R}^m)^n$ such that if $(q_1,\dots,q_n) \in U$ is an n-point configuration with the same distribution of distances as that of $(p_1,\dots,p_n)$, then the two point configurations are the same up to a rigid motion and a relabeling of the points.*

Proof. Let us assume the contrary. Then there exists a sequence of n-point configurations $\{q_1^k,\dots,q_n^k\}_{k=1}^\infty$ converging to $p_1,\dots,p_n$, and a sequence of permutations $\{\varphi_k\}_{k=1}^\infty \subset S_{\binom{n}{2}}$ such that none of the $q_1^k,\dots,q_n^k$ can be mapped to $p_1,\dots,p_n$ by a rotation and a translation and a relabeling, but the distances $d_{\{i,j\}} = \|p_i - p_j\|^2$ are mapped to the distances $d^k_{\{i,j\}} = \|q_i^k - q_j^k\|^2$ by φ_k so $d_{\varphi_k\cdot\{i,j\}} = d^k_{\{i,j\}}$ for all $\{i,j\} \in \mathcal{P}$. By taking a subsequence, we may assume that $\varphi_k = \varphi$ is the same for every k since $S_{\binom{n}{2}}$ is a finite group. Taking the limit, we obtain that $d_{\varphi\cdot\{i,j\}} = \lim_{k\to\infty} d^k_{\{i,j\}}$, for $\{i,j\} \in \mathcal{P}$. By continuity of the distance, this implies that $d_{\varphi\cdot\{i,j\}} = d_{\{i,j\}}$, for all $\{i,j\} \in \mathcal{P}$. Therefore, $d_{\{i,j\}} = d^k_{\{i,j\}}$ for every $\{i,j\} \in \mathcal{P}$. By Proposition 0.1, this implies that $q_1^k,\dots,q_n^k$ and $p_1,\dots,p_n$ are the same up to a rigid motion, for every k, which contradicts our hypothesis, and the conclusion follows. $\square$

Unfortunately, the size of the neighborhood is unknown and varies with the points $p_1,\dots,p_n$, so this local result is not very practical. We now consider the global case. Observe that some of the permutations in $S_{\binom{n}{2}}$ correspond to a relabeling of the points. More precisely, φ corresponds to a relabeling of the points if there exists a permutation $\pi : \{1,\dots,n\} \hookrightarrow \{1,\dots,n\}$ of the indices such that $\varphi\cdot\{i,j\} = \{\pi(i),\pi(j)\}$, for every $\{i,j\} \in \mathcal{P}$. Relabelings are the *good* permutations: if the permutation mapping the labeled pairwise distances of a point configuration onto the labeled pairwise distances of another configuration is a relabeling, then the two configurations are the same up to a rigid motion. We need to know what distinguishes the good permutations from the bad permutations. The following lemma, which is central to our argument, says that, informally speaking, a permutation is a relabeling if it preserves adjacency.

Lemma 1.2. *Suppose $n \neq 4$. A permutation $\varphi \in S_{\binom{n}{2}}$ is a relabeling if and only if for all pairwise distinct indices $i,j,k \in \{1,\dots,n\}$ we have*

$$\varphi\cdot\{i,j\} \cap \varphi\cdot\{i,k\} \neq \emptyset. \tag{1.1}$$

Proof. For $n \leq 3$, every $\varphi \in S_{\binom{n}{2}}$ is a relabeling, and the condition (1.1) is always satisfied. Thus we may assume $n \geq 5$. It is also clear that every relabeling satisfies (1.1).

Suppose that $\varphi \in S_{\binom{n}{2}}$ is a permutation of $\mathcal{P}$ which satisfies (1.1). Take any $i,j,k,l \in \{1,\dots,n\}$ pairwise distinct and assume, by way of contradiction, that $\varphi\cdot\{i,j\} \cap \varphi\cdot\{i,k\} \cap \varphi\cdot\{i,l\} = \emptyset$. Then the injectivity of φ and the condition (1.1) imply that we can write $\varphi \cdot \{i,j\} = \{a,b\}$, $\varphi \cdot \{i,k\} = \{a,c\}$, and $\varphi \cdot \{i,l\} = \{b,c\}$ with $a,b,c \in \{1,\ldots,n\}$ pairwise distinct. Now choose $m \in \{1,\ldots,n\} \setminus \{i,j,k,l\}$. Then $\varphi \cdot \{i,m\}$ must meet each of the sets $\{a,b\}$, $\{a,c\}$, and $\{b,c\}$. Being itself a set of two elements, $\varphi \cdot \{i,m\}$ must be one of the sets $\{a,b\}$, $\{a,c\}$, or $\{b,c\}$, contradicting the injectivity of φ. Therefore $\varphi \cdot \{i,j\} \cap \varphi \cdot \{i,k\} \cap \varphi \cdot \{i,l\} \neq \emptyset$.

Fix an index $i \in \{1,\ldots,n\}$ and choose $j,k \in \{1,\ldots,n\} \setminus \{i\}$. Then $\varphi \cdot \{i,j\} \cap \varphi \cdot \{i,k\}$ is a set with one element, and by the above this one element must also lie in every $\varphi \cdot \{i,l\}$ with $l \in \{1,\ldots,n\} \setminus \{i\}$. Hence $\bigcap_{l \neq i} \varphi \cdot \{i,l\} \neq \emptyset$. This allows us to define a map σ: $\{1,\ldots,n\} \to \{1,\ldots,n\}$ with

$$\bigcap_{\substack{j=1 \\ j \neq i}}^{n} \varphi \cdot \{i,j\} = \{\sigma(i)\}. \tag{1.2}$$

For $i \in \{1,\ldots,n\}$ define $M_i := \{\{i,j\} \mid j \in \{1,\ldots,n\} \setminus \{i\}\}$. Then (1.2) tells us that $\varphi \cdot M_i \subseteq M_{\sigma(i)}$. Since $|M_i| = |M_{\sigma(i)}|$ and since φ is injective, this implies $\varphi \cdot M_i = M_{\sigma(i)}$. Take $i,i' \in \{1,\ldots,n\}$ with $\sigma(i) = \sigma(i')$. Then $\varphi \cdot M_i = \varphi \cdot M_{i'}$, which implies $M_i = M_{i'}$ and therefore $i = i'$. Thus σ is injective.

Equation (1.2) implies that for $i,j \in \{1,\ldots,n\}$ distinct we can write $\varphi \cdot \{i,j\} = \{\sigma(i), \gamma_i(j)\}$ with γ_i: $\{1,\ldots,n\} \setminus \{i\} \to \{1,\ldots,n\}$. But applying (1.2) with the roles of i and j interchanged yields

$$\{\sigma(j)\} = \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \varphi \cdot \{i,j\} = \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \{\sigma(i), \gamma_i(j)\}.$$

By the injectivity of σ this implies $\sigma(j) = \gamma_i(j)$ for all $i \neq j$. We conclude that $\varphi \cdot \{i,j\} = \{\sigma(i), \sigma(j)\}$ for all $i,j \in \{1,\ldots,n\}$ distinct. But this means that φ is a relabeling, as claimed. □

Remark. For $n = 4$, Lemma 1.2 becomes false. An example is given by $\varphi \in S_{\binom{4}{2}}$ defined as

$$\begin{aligned} &\varphi \cdot \{1,2\} = \{1,2\}, \quad \varphi \cdot \{1,3\} = \{1,3\}, \quad \varphi \cdot \{1,4\} = \{2,3\}, \\ &\varphi \cdot \{2,3\} = \{1,4\}, \quad \varphi \cdot \{2,4\} = \{2,4\}, \quad \varphi \cdot \{3,4\} = \{3,4\}. \end{aligned}$$

This permutation satisfies (1.1), but it is not a relabeling. Lemma 1.2 becomes true for $n = 4$ if we add the additional condition

$$\varphi \cdot \{1,2\} \cap \varphi \cdot \{1,3\} \cap \varphi \cdot \{1,4\} \neq \emptyset. \tag{1.3}$$

◁

Do non-reconstructible point configurations exist? The answer is yes. Some examples can be found in Boutin and Kemper [5]. Fortunately, non-reconstructible configurations are rare. The key to this fact is contained in the functional relationships between the pairwise distances of a point configuration. These relationships are well-known from classical invariant theory. For example, a planar configuration of four points p_i, p_j, p_k, and p_l satisfies

$$\det \begin{pmatrix} -2d_{\{i,l\}} & d_{\{i,j\}} - d_{\{i,l\}} - d_{\{j,l\}} & d_{\{i,k\}} - d_{\{i,l\}} - d_{\{k,l\}} \\ d_{\{i,j\}} - d_{\{i,j\}} - d_{\{j,l\}} & -2d_{\{j,l\}} & d_{\{j,k\}} - d_{\{j,l\}} - d_{\{k,l\}} \\ d_{\{i,k\}} - d_{\{i,l\}} - d_{\{k,l\}} & d_{\{j,k\}} - d_{\{j,l\}} - d_{\{k,l\}} & -2d_{\{k,l\}} \end{pmatrix} = 0.$$

We can also express this relationship as follows. Define the polynomial

$$\begin{aligned} g(U,V,W,X,Y,Z) := {} & 2U^2Z + 2UVX - 2UVY - 2UVZ - 2UXW - 2UXZ + 2UYW - \\ & 2UYZ - 2UWZ + 2UZ^2 + 2V^2Y - 2VXY - 2VXW + 2VY^2 - 2VYW - \\ & 2VYZ + 2VWZ + 2X^2W - 2XYW + 2XYZ + 2XW^2 - 2XWZ. \end{aligned}$$

Then

$$g\left(d_{\{i,j\}}, d_{\{i,k\}}, d_{\{i,l\}}, d_{\{j,k\}}, d_{\{j,l\}}, d_{\{k,l\}}\right) = 0. \tag{1.4}$$

For simplicity, we continue to concentrate on the planar case $m = 2$ although other dimensions can be treated similarly. Recall that $\mathcal{P}$ denotes the set of pairs $\mathcal{P} = \{\{i,j\} | i \neq j, i,j = 1,\dots,n\}$. The following theorem gives a practical test for reconstructibility of planar point configurations.

Theorem 1.3. *Let $n \geq 5$, let $p_1,\dots,p_n \in \mathbb{R}^2$ and let $d_{\{i,j\}} = \|p_i - p_j\|^2$ be the square of the Euclidean distance between p_i and p_j, for every $\{i,j\} \in \mathcal{P}$. Suppose that for each choice of indices $i_0, i_1, i_2, j_1, j_2, k_1, k_2, l_1, l_2, m_1, m_2 \in \{1,\dots,n\}$ such that the pairs $\{i_0,i_1\}$, $\{i_0,i_2\}$, $\{j_1,j_2\}$, $\{k_1,k_2\}$, $\{l_1,l_2\}$, $\{m_1,m_2\} \in \mathcal{P}$ are distinct, we have*

$$g\left(d_{\{i_0,i_1\}}, d_{\{j_1,j_2\}}, d_{\{k_1,k_2\}}, d_{\{l_1,l_2\}}, d_{\{m_1,m_2\}}, d_{\{i_0,i_2\}}\right) \neq 0. \tag{1.5}$$

Then $p_1,\dots,p_n$ is reconstructible from distances.

Proof. Let $q_1,\dots,q_n \in \mathbb{R}^2$ be a point configuration with the same distribution of distances as $p_1,\dots,p_n$. Write $d'_{\{i,j\}} = \|q_i - q_j\|^2$. Then there exists a permutation $\varphi \in S_{\binom{n}{2}}$ of the set $\mathcal{P}$ such that

$$d'_{\{i,j\}} = d_{\varphi\cdot\{i,j\}}.$$

We wish to use Lemma 1.2 for showing that φ^{-1} is a relabeling, which will imply that φ is also a relabeling. Take any pairwise distinct indices $i,j,k,l \in \{1,\dots,n\}$. Then the above equation and (1.4) imply

$$g\left(d_{\varphi\cdot\{i,j\}}, d_{\varphi\cdot\{i,k\}}, d_{\varphi\cdot\{i,l\}}, d_{\varphi\cdot\{j,k\}}, d_{\varphi\cdot\{j,l\}}, d_{\varphi\cdot\{k,l\}}\right) = \\ g\left(d'_{\{i,j\}}, d'_{\{i,k\}}, d'_{\{i,l\}}, d'_{\{j,k\}}, d'_{\{j,l\}}, d'_{\{k,l\}}\right) = 0.$$

It follows from the hypothesis (1.5) that $\varphi\cdot\{i,j\}$ and $\varphi\cdot\{k,l\}$ are disjoint (otherwise they would have an index i_0 in common). So for disjoint sets $\{i,j\}$ and $\{k,l\}$ we have that $\varphi\cdot\{i,j\}$ and $\varphi\cdot\{k,l\}$ are also disjoint. This is equivalent to saying that if $\varphi\cdot\{i,j\}$ and $\varphi\cdot\{k,l\}$ have non-empty intersection, then the same is true for $\{i,j\}$ and $\{k,l\}$. Take $a,b,c \in \{1,\dots,n\}$ pairwise distinct and set $\{i,j\} := \varphi^{-1}\cdot\{a,b\}$ and $\{j,k\} := \varphi^{-1}\cdot\{a,c\}$. Then $\varphi\cdot\{i,j\} \cap \varphi\cdot\{k,l\} = \{a,b\} \cap \{a,c\} = \{a\}$, hence, as seen above, $\{i,j\}$ and $\{k,l\}$ have non-empty intersection. Thus the condition (1.1) of Lemma 1.2 is satisfied for φ^{-1}. It follows that φ^{-1}, and hence also φ, is a relabeling: $\varphi\cdot\{i,j\} = \{\pi(i),\pi(j)\}$ with $\pi \in S_n$. Now it follows from Proposition 0.1 that there exists a rigid motion (M,T) such that

$$q_{\pi(i)} = Mp_i + T$$

for all $i \in \{1,\dots,n\}$. This completes the proof. □

Remark. Take indices $i_0, i_1, i_2, j_1, j_2, k_1, k_2, l_1, l_2, m_1, m_2 \in \{1,\dots,n\}$ as in the hypothesis of Theorem 1.3. Explicit computation shows that

$$g\left(d_{\{i_0,i_1\}}, d_{\{j_1,j_2\}}, d_{\{k_1,k_2\}}, d_{\{l_1,l_2\}}, d_{\{m_1,m_2\}}, d_{\{i_0,i_2\}}\right),$$

viewed as a polynomial in variables $d_{\{i,j\}}$, contains the term $2d^2_{\{i_0,i_1\}}d_{\{i_0,i_2\}}$. Notice that the index i_0 occurs three times in this term (when writing it out as a product rather than squaring the first variable). It follows from Boutin and Kemper [5, Proposition 2.2(b) and Lemma 2.3] that this term does not occur in any relationship of degree 3 between the $d_{\{i,j\}}$. In particular, $g\left(d_{\{i_0,i_1\}}, d_{\{j_1,j_2\}}, d_{\{k_1,k_2\}}, d_{\{l_1,l_2\}}, d_{\{m_1,m_2\}}, d_{\{i_0,i_2\}}\right)$ is not a relationship between the $d_{\{i,j\}}$. It follows that there exists a dense, open subset $\Omega \subseteq \left(\mathbb{R}^2\right)^n$ such that for all point configurations $(p_1,\dots,p_n) \in \Omega$ the hypotheses of Theorem 1.3 are met. This provides a new proof for the fact that "most" point configurations are reconstructible from distances, which appeared in greater generality in [5, Theorem 2.6]. ◁

n	# combinations	CPU time in seconds
5	100,800	72
6	2,059,200	1,170
7	19,535,040	9,920
8	120,556,800	58,375

Table 2: Time required to check for the reconstructibility of an n-point configuration.

How many tests do we have to conduct for checking that the conditions in (1.5) are satisfied? There are n choices for i_0, the index that is repeated. For each choice of i_0, there are $(n-1)(n-2)$ choices for i_1 and i_2 (since these three indices must be distinct). Having chosen i_0, i_1, and i_3, there are $\binom{n}{2}-2$ choices for the set $\{j_1, j_2\}$, $\binom{n}{2}-4$ choices for the set $\{k_1, k_2\}$ and so on. Altogether, we obtain

$$n(n-1)(n-2)\left(\binom{n}{2}-2\right)\left(\binom{n}{2}-3\right)\left(\binom{n}{2}-4\right)\left(\binom{n}{2}-5\right) =$$
$$\frac{1}{16}\left(n^{11}-7n^{10}-8n^9+138n^8-83n^7-983n^6+1074n^5+2996n^4-3672n^3-3296n^2+3840n\right)$$

choices.

Corollary 1.4. *There exists an open and dense set $\Omega \subset (\mathbb{R}^2)^n$ of reconstructible n-point configurations and an algorithm in $O(n^{11})$ steps to determine whether any $(p_1, \ldots, p_n) \in (\mathbb{R}^2)^n$ lies in Ω.*

Remark 1.5. The algorithm given by Theorem 1.3 can be generalized to $\mathbb{R}^m$ if $n \geq m+2$. For each choice of $m+2$ indices $i_0, \ldots, i_{m+1}$ we have the relationship

$$\det\left(d_{\{i_\nu, i_\mu\}} - d_{\{i_\nu, i_0\}} - d_{\{i_\mu, i_0\}}\right)_{\nu,\mu=1,\ldots,m+1} = 0,$$

which can be expressed as $g_m\left(d_{\{i_0,i_1\}}, \ldots, d_{\{i_m,i_{m+1}\}}\right) = 0$ with g_m an appropriate polynomial in $k := \binom{m+2}{2}$ variables. Now we obtain a generalization of Theorem 1.3 which says that if for all pairwise distinct choices $S_1, \ldots, S_k \in \mathcal{P}$ with $S_1 \cap S_k \neq \emptyset$ we have

$$g_m\left(d_{S_1}, \ldots, d_{S_k}\right) \neq 0, \tag{1.6}$$

then the configuration $p_1, \ldots, p_n$ is reconstructible from distances. We see that there are

$$n(n-1)(n-2)\prod_{j=2}^{k-1}\left(\binom{n}{2}-j\right) = O\left(n^{m^2+3m+1}\right)$$

steps for checking the reconstructibility of $p_1, \ldots, p_n$. It also follows from Boutin and Kemper [5, Proposition 2.2(b) and Lemma 2.3] that there exists a dense open subset $\Omega \subseteq (\mathbb{R}^m)^n$ where the inequalities (1.6) are all satisfied.

2 Numerical Experiments

A simple Matlab code (available upon request) was used to check for the reconstructibility of some n-point configurations. We were able to show that some n-point configurations were reconstructible, with $n = 5, 6, 7$ and even 8 in a reasonable time. Corresponding CPU times and number of combinations to be checked are given in Table 2. The computations were done using Matlab version 6.1 on a Sun (4×ultraSPARC-II, 480 MHZ).

An important point to observe is that if a point configuration fails to satisfy one of the conditions in (1.5), it does not mean that it is not reconstructible. For example, it is not hard to show that every square is reconstructible (see Boutin and Kemper [5, Example 2.12]). But, as one can check, squares satisfy neither (1.5) nor (1.3). This is due to the fact that squares have repeated distances. Indeed, any planar n-point configuration with repeated distances will fail the reconstructibility test. (See Boutin and Kemper [5] for a proof of this fact and ideas on how to modify the algorithm to take care of point configurations with repeated distances.) Also, the point configuration given by

$$p_1 = (0,0), p_2 = (7,0), p_3 = (5,-1), p_4 = (3,-3), p_5 = (11,2)$$

does not satisfy (1.5), even though its pairwise distances are all distinct. However, one can show that it is actually reconstructible. (It suffices to show that the permutations of the distances which make g equal to zero all violate one of the relationships that exist between the pairwise distances of five points. We checked this numerically.) Our test is thus not perfect.

Observe that, when using points with small integer coordinates, the polynomial g can be evaluated exactly on a computer. We can thus determine precisely whether such a point configuration satisfies the conditions of (1.5). An interesting question is: given a planar n-point configuration with integer coordinates and lying inside the box $[0,N] \times [0,N]$, what are the chances that it will fail the reconstructibility test? Numerical experiments showed that it is quite likely, even when configurations with repeated distances are excluded. For $N = 3$, we found that about 61% of configurations of four points whose distances are not repeated fail the test. (More precisely, we generated all possible $p_1 = (x_1, y_1)$, $p_2 = (x_2, y_2)$, $p_3 = (x_3, y_3)$, $p_4 = (x_4, y_4)$ with coordinates in $\{0,1,2,3\}$ and such that either $x_i < x_{i+1}$ or $x_i = x_{i+1}$ and $y_i < y_{i+1}$, for all $i = 1,2,3,4$. Of those 1820 four-point configurations, we found that 1636 had repeated distances while a total of 1748 failed the test.) For $N = 4$, this percentage went down to about 30%, which is still quite high.

It would be interesting to determine whether such high rates of failure are also observed when the coordinates of the points are not necessarily integers. But, in general, floating-point arithmetic prevents us for determining whether a polynomial function is exactly zero. We must thus replace the $g = 0$ in conditions 1 and 2 by $|g| \leq \epsilon$, for some ϵ determined by the machine precision and possible noise in the measurements. However, numerical tests have shown that if the coordinates of four points are chosen randomly in $(0,1)$ (using the Matlab *rand* function), then the polynomial g in (1.5) rarely takes very small values. For example, after generating 5000 different random four-point configurations, we found that only 22 of those generated a g with a value less than 10^{-7}. In another set of 5000 four-point configurations, we found only 6 which generated a g with a value less than 10^{-8}. In a final set of 10,000 four-point configurations, we found none which generated a g with a value less than 10^{-9}. As these values are well above the maximal error expected with such data when evaluating g using Matlab, this implies that none of the 20,000 random four-point configurations we generated could possibly fail the test.

3 The Case of Orientation Preserving Rigid Motions in the Plane

In the previous two sections, we considered the case where the shape of an n-point configurations is defined by $p_1, \ldots, p_n \in \mathbb{R}^m$ up to rigid motions. Recall that the group of rigid motions in $\mathbb{R}^m$, sometimes called the Euclidean group and denoted by $E(m)$, is generated by rotations, translations and reflections in $\mathbb{R}^m$. However, in certain circumstances, it may be desirable to be able to determine whether two point configurations are equivalent up to strictly orientation preserving rigid motions. The group of orientation preserving rigid motions, sometimes called the *special Euclidean group* and denoted by $SE(m)$, is the one that is generated by rotations and translations in $\mathbb{R}^m$.

For simplicity, we again restrict ourselves to the planar case $m = 2$. Given a planar point configuration $p_1, \ldots, p_n \in \mathbb{R}^2$, we would like to be able to determine whether any other planar n-point configuration $q_1, \ldots, q_n$ is the same as $p_1, \ldots, p_n$ up to a rotation and a translation? Given any q_i, q_j, q_k in the plane, denote by a_{q_i,q_j,q_k} the signed area of the parallelogram spanned by $q_i - q_j$ and $q_k - q_j$, so

$$a_{q_i,q_j,q_k} = \det(q_i - q_k, q_j - q_k).$$

Since signed areas are unchanged under rotations and translations, the function $I : \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$

defined by

$$I(q_1,q_2,q_3,q_4) = (a^2_{q_1,q_2,q_4} - a^2_{q_1,q_3,q_4})(a^2_{q_1,q_2,q_3} - a^2_{q_1,q_3,q_4})$$
$$(a^2_{q_1,q_2,q_3} - a^2_{q_1,q_2,q_4})(a_{q_1,q_2,q_3} - a_{q_1,q_2,q_4} + 2a_{q_1,q_3,q_4})$$
$$(a_{q_1,q_2,q_3} - 2a_{q_1,q_2,q_4} + a_{q_1,q_3,q_4})(2a_{q_1,q_2,q_3} - a_{q_1,q_2,q_4} + a_{q_1,q_3,q_4}) \quad (3.1)$$

is invariant under the action of $SE(2)$. Moreover, one can check that it is also invariant under a relabeling of the four points q_1, q_2, q_3, q_4. However, it is *not* invariant under rigid motions in general. Indeed, any transformation which is a rigid motion but does *not* preserve the orientation will transform I into $-I$.

Given an n-point configuration $q_1, \dots, q_n$ with $n \geq 4$, we can evaluate I on all possible subsets of four points of $\{q_1, \dots, q_n\}$. We consider the distribution of the value of these I's, i.e. the distribution of the

$$I_{i_1,i_2,i_3,i_4} = I(q_{i_1}, q_{i_2}, q_{i_3}, q_{i_4}), \text{ for all } i_1 < i_2 < i_3 < i_4 \in \{1, \dots, n\}.$$

Proposition 3.1. *Let $n \geq 4$ and let $p_1, \dots, p_n \in \mathbb{R}^2$ be an n-point configuration which is reconstructible from distances. Assume that the distribution of the I's of this point configuration is not a symmetric function (i.e. that the distribution of the I's is not the same as the distribution of the $-I$'s.) Let $q_1, \dots, q_n \in \mathbb{R}^2$ be another n-point configuration. Then both the distribution of the distances and the distribution of the I's of the two point configurations are the same if and only if there exists a rotation and a translation which maps one point configuration onto the other.*

Proof. Observe that, in addition to being invariant under rotations and translations of the points, the distribution of the value of the I's is also independent of the labeling of the points. The same holds for the distribution of pairwise distances. So if two n-point configurations are the same up to a rotation, a translation and a relabeling, then the distribution of the I's and the distribution of the distances are the same for both. Thus the *if* is clear.

Now assume that the distribution of the distances and the distribution of the I's are the same for both point configuration. Since $p_1, \dots, p_n$ is, by hypothesis, reconstructible, this implies that there exists a rigid motion (M, T) and a relabeling $\pi : \{1, \dots, n\} \hookrightarrow \{1, \dots, n\}$ such that $Mp_i + T = q_{\pi(i)}$, for all $i = 1, \dots, n$. If (M, T) is not in $SE(2)$, then it maps each $I(p_{i_1}, p_{i_2}, p_{i_3}, p_{i_4})$ to $-I(p_{i_1}, p_{i_2}, p_{i_3}, p_{i_4}))$. But this is a contradiction, since the distribution of the $I's$ is not symmetric. Thus g is in $SE(2)$. This shows the *only if.* $\square$

Remark 3.2. One can actually show that if $p_1, \dots, p_4$ is equivalent to $q_1, \dots, q_4$ up to a rigid motion, then $p_1, \dots, p_4$ is equivalent to $q_1, \dots, q_4$ up to a rotation and a translation if and only if $I(p_1, \dots, p_4) = I(q_1, \dots, q_4)$. (Indeed, I is one of the two fundamental invariants of the action of $SE(2) \times S_4$ on $\mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2$ which we obtained using the invariant theory package in Magma [4]. By construction, these two invariants thus distinguish the orbits of $SE(2) \times S_3$. The other invariant is actually unchanged under the action of the full Euclidean group $E(2)$ and so I alone distinguishes the orbits of $SE(2)$ within the orbits of $E(2)$.

4 The Case of Rotations, Translations and Scalings

In certain circumstances, it may also be desirable to be able to determine whether two point configurations are the same up to a rigid motion and a scaling. This can be done using a simple variation of the previous approach. Given a distribution of distances $\{d_{\{i,j\}} = ||p_i - p_j||^2\}$, let d_{max} be the largest distance

$$d_{max} = \max\{d_{\{i,j\}} | \{i,j\} \in \mathcal{P}\},$$

which can be assumed to be non-zero since otherwise all points coincide. We can consider the distribution of the rescaled distances $\{\frac{d_{\{i,j\}}}{d_{max}}\}_{\{i,j\} \in \mathcal{P}}$. In addition to being invariant under rigid motions and relabeling, the distribution of the rescaled distances is also invariant under a scaling of the points

$$p_i \mapsto \lambda p_i, \text{ for every } i = 1, \dots, n.$$

for any $\lambda \in \mathbb{R}_{\neq 0}$.

Proposition 4.1. *Let $n \geq m + 2$. There exists an open, dense subset Ω of $(\mathbb{R}^m)^n$ such that if an n-point configuration $p_1, \ldots, p_n$ is such that $(p_1, \ldots, p_n) \in \Omega$, then $p_1, \ldots, p_n$ is uniquely determined, up to rotations, translations, reflections, scalings and relabeling of the points, by the distribution of its rescaled pairwise distances $\{\frac{d_{\{i,j\}}}{d_{max}}\}_{\{i,j\} \in \mathcal{P}}$. Moreover, there is an algorithm in $O(n^{\frac{m^2+3m+12}{2}})$ steps to determine whether $(p_1, \ldots, p_n) \in \Omega$.*

Proof. Let $p_1, \ldots, p_n \in \mathbb{R}^m$ be an n-point configuration which is reconstructible from distances and whose pairwise distances are not all zero. Observe that if $q_1, \ldots, q_n \in \mathbb{R}^2$ is another n-point configuration, then the distributions of the rescaled distances of both point configurations are the same if and only if there exists a rigid motion followed by a scaling which maps one point configuration onto the other. The claim is thus a direct corollary of Theorem 2.6 from Boutin and Kemper [5] and of Remark 1.5. □

Acknowledgments

Mireille Boutin wishes to thank David Cooper and Senem Velipasalar [20] who gave her the initial motivation for this research, Jean-Philippe Tarel for his constructive remarks on this approach and her co-author for being such a joy to work with. Gregor Kemper expresses his gratitude to his hosts at Purdue University, where part of this research took place. Another part of the research was carried out while both authors were visiting the Mathematical Sciences Research Institute in Berkeley. We wish to thank Michael Singer and Bernd Sturmfels for the invitation. We also thank Peter Gritzmann for pointing our attention to the work of Skiena et al. (*Skiena* et al. 2003).

References

[1] Helmer Aslaksen, Shih-Piug Chan, Tor Gulliksen, *Invariants of S_4 and the Shape of Sets of Vectors*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 53–57.

[2] Gary S. Bloom, *A counterexample to a theorem of S. Piccard*, J. Combinatorial Theory Ser. A **22(3)** (1977), 378–379.

[3] Leonard M. Blumenthal, *Theory and applications of distance geometry*, Oxford, at the Clarendon Press, 1953.

[4] Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma Algebra System I: The User Language*, J. Symbolic Comput. **24** (1997), 235–265.

[5] Mireille Boutin, Gregor Kemper, *On reconstructing n-point configurations from the distribution of distances of areas*, Adv. Appl. Math. (to appear).

[6] Tamara Dakić, *On the turnpike problem*, Ph.d. Thesis, School of Computer Science, Simon Fraser University, 2000.

[7] Harm Derksen, Gregor Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, Heidelberg, New York 2002.

[8] T.I. Dix, D.H. Kieronska, *Errors between sites in restriction site mapping*, Comput. Appl. Biol. Sci. **4(1)** (1988), 117–123.

[9] Colin Goodall, *Procrustes methods in the statistical analysis of shape*, J. Roy. Statist. Soc. Ser. B **53(2)** (1991), 285–339.

[10] J.C. Gower, *Generalized procrustes analysis*, Psychometrika **40** (1975), 33–55.

[11] Rhee Gwangsoo, *DNA restriction mapping from random-clone data*, Technical Report **WUCS-88-18**, Department of Computer Science, Washington University St. Louis MO, 1988.

[12] Richard Hartley, Andrew Zisserman, *Multiple View Geometry in Computer Vision*, Cambridge University Press, Cambridge 2001.

[13] P. Lamke, M. Werman, *On the complexity of inverting the autocorrelation function of a finite integer sequence, and the problem of locating n points on a line, given the unlabeled distances between them*, Preprint **453**, IMA, 1988.

[14] A.L. Patterson, *A direct method for the determination of the components of interatomic distances in crystals*, Zeitschr. Krist. **90** (1935), 517–542.

[15] A.L. Patterson, *Ambiguities in the X-ray analysis of crystal structures*, Phys. Review **65** (1944), 195–201.

[16] Sophie Piccard, *Sur les ensembles de distances des ensembles de points d'un espace Euclidien*, Mém. Univ. Neuchâtel, vol. 13, Secrétariat de l'Université, Neuchâtel, 1939.

[17] Joseph Rosenblatt, Paul D. Seymour, *The structure of homometric sets*, SIAM J. Algebraic Discrete Methods **3(3)** (1982), 343–350.

[18] Steven S. Skiena, Warren D. Smith, Paul Lemke, *Reconstructing sets from interpoint distances*, in: *Discrete and computational geometry. The Goodman-Pollack Festschrift*, vol. 25 of *Algorithms and Combinatorics*, pp. 597–632, Springer, Berlin, Berlin 2003.

[19] Mark Stefik, *Inferring DNA structures from segmentation data*, Artificial Intelligence **11** (1978), 85–114.

[20] Tolga Tasdizen, Senem Velipasalar, David B. Cooper, *Shape Based Similarity Measure for Image Retrieval*, Technical Report **SHAPE-TR-2001-03**, SHAPE lab, Brown University, Providence, 2001.

Mireille Boutin
Department of Mathematics
Purdue University
150 N. University St.
West Lafayette, IN
47907, USA
boutin@math.purdue.edu

Gregor Kemper
Technische Universität München
Zentrum Mathematik - M11
Boltzmannstr. 3
85 748 Garching
Germany
kemper@ma.tum.de