Point Sets up to Rigid Transformations are Determined by the Distribution of their Pairwise Distances

Daniel Chen
Survey of results of M. Boutin and G. Kemper
Outline

• Motivation
• Preliminaries
• Folklore Lemma
• Main Result
• Computation
• Extensions and Open Problems
Motivation

- Shape Distributions of [osada]
- Distribution of different functions on randomly selected points considered.
- Different dissimilarity measures between distributions also considered.
Motivation

• Comparing the distribution of pairwise distances w.r.t $L_1$ norm appears to be a good classifier.

• This paper provides some reasoning on why this might be the case: When the distribution of pairwise distances are identical, then the points in general position are the same up to a rigid transformation.
Preliminaries

- General Position
- Rigid Transformation
- Distribution of Pairwise Distances
- Reconstructibility from Pairwise Distances
General Position

• As defined by Matousek:
  Let a set of $n$ points in $\mathbb{R}^d$ be specified by a vector $t = (t_1, t_2, \ldots, t_m)$ for $m = dn$. Then, a general position condition is a condition that can be expressed as $\bigwedge_i p_i(t) \neq 0$ for a countable number of polynomials $p_i$.

• Set of points not in general position has measure zero.
Rigid Transformation

• Definition:

Let \( p \) be a point in \( \mathbb{R}^m \). Then a rigid transformation is a function \( R : \mathbb{R}^m \to \mathbb{R}^m \) that can be written as \( R(p) = Mp + T \) where \( M \) is an orthogonal \( m \)-by-\( m \) matrix and \( T \) is a column vector in \( \mathbb{R}^m \).
Pairwise Distances

• Distribution:

Given a set of points $P$, let the distribution of pairwise distances $d(P)$ be the multiset $\{||p_i - p_j||\}_{i<j}$.

• Reconstructibility:

We say that $p_1, \ldots, p_n \in \mathbb{R}^m$ is reconstructible from pairwise distances if for every $q_1, \ldots, q_n \in \mathbb{R}^m$ with the same distribution of pairwise distances, there exists a rigid transformation $R$ and a permutation $\pi$ of $\{1, \ldots, n\}$, such that $P(p_i) = q_{\pi(i)}$ for every $i \in 1, \ldots, n$. 
Folklore Lemma

- Tricky to work with rigid transformations directly.
- Compare distance matrices instead.

Folklore Lemma:

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 $i, j$ in $1, \ldots, n$, then there exists a rigid transformation $R$ such that $R(p_i) = q_i$ for all $i$. 
Folklore Lemma

**Proof:**

Let $x_i = p_i - p_n$ and $y_i = q_i - q_n$ for $i = 1, \ldots, n$. We claim that $\langle x_i, x_j \rangle = \langle y_i, y_j \rangle$ for all $i, j$. To see this, we have the following calculation:

\[
\langle x_i, x_j \rangle = \langle p_i - p_n, p_j - p_n \rangle = \frac{\langle p_i - p_n, p_i - p_n \rangle + \langle p_j - p_n, p_j - p_n \rangle - \langle p_i - p_j, p_i - p_j \rangle}{2} = \frac{||p_i - p_n|| + ||p_j - p_n|| - ||p_i - p_j||}{2} = \frac{||q_i - q_n|| + ||q_j - q_n|| - ||q_i - q_j||}{2} = \frac{\langle q_i - q_n, q_i - q_n \rangle + \langle q_j - q_n, q_j - q_n \rangle - \langle q_i - q_j, q_i - q_j \rangle}{2} = \langle q_i - q_n, q_j - q_n \rangle = \langle y_i, y_j \rangle
\]

Now, let $X = [x_1, \ldots, x_n]$ and $Y = [y_1, \ldots, y_n]$. We have shown above that $X^T X = Y^T Y$. Now, $X^T X$ is symmetric and positive semidefinite, and hence can be written as $Q\Lambda Q^T$ for an orthogonal $Q$ and a non-negative diagonal matrix $\Lambda$. Since $\Lambda$ is non-negative, we can write $X^T X = Y^T Y = Q\Lambda^{1/2}Q^T$. Therefore, using the singular value decomposition, we can write $X$ as $U_X \Lambda^{1/2}Q^T$ and $Y$ as $U_Y \Lambda^{1/2}Q^T$ for orthogonal $U_X$ and $U_Y$. Then, we can write $Y = MX$ for orthogonal $M = U_Y U_X^T$. Moreover, it is easy to verify that $Mx_i = y_i$ for $i = 1, \ldots, n$. To finish the proof, we note that $M(p_i - p_n) = q_i - q_n$ or $q_i = Mp_i + q_n - Mp_n$ so there is a rigid transformation from $p_i$ to $q_i$ with the orthogonal matrix $M$ and translation vector $q_n - Mp_n$. 
Digression: Counterexample

• 1D Counterexample:

\[ P = \{0, 1, 4, 10, 12, 17\} \quad Q = \{0, 1, 8, 11, 13, 17\} \]

It can be verified that the distribution of distances is the multiset:

\[ d(P) = d(Q) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17\} \]

• 2D Counterexample:
Main Idea

• With Folklore Lemma in mind, show that if two point sets have the same distribution of pairwise distances, they have the same distance matrices up to a relabeling of the points.
Some Notation

• Convention:

Let $P = \{p_1, \ldots, p_n\}$ be a labeled set of $n$ points. Then we let $d_P : \mathcal{P} \to \mathbb{R}$ be defined as $d_P(\{i, j\}) = ||p_i - p_j||^2$.

• Corollary:

If $n$-point configurations $P$ and $Q$ have the same distribution of distances, then there exists a permutation $\phi$ of $\mathcal{P}$ such that $d_P(\phi(\{i, j\})) = d_Q(\{i, j\})$ for all $\{i, j\} \in \mathcal{P}$. 
A Weaker Result

Let $P$ be a configuration of $n$ points. Then, there exists neighborhoods of $p_i$ such that if $Q$ if a configuration of $n$ points with $q_i$ in the neighborhood of $p_i$ and having the same distribution of distances as $P$, then $P$ and $Q$ are the same up to a rigid transformation and a relabeling of the points.

- **Proof:**

Suppose for the purpose of contradiction that there exists a sequence of configurations $\{Q_k\}_{k=1}^{\infty}$ converging to $P$ such that none of $Q_k$ can be mapped to $P$ via rigid transformation and relabeling, but there exists a sequence of permutations $\{\phi_k\}_{k=1}^{\infty}$ such that $d_P(\phi_k(\{i, j\})) = d_{Q_k}(\{i, j\})$. Since there are finitely many permutations $\phi_k$, we can pick $\phi_1$, for instance, and let $\{R_l\}_{l=1}^{\infty}$ be the subsequence of $\{Q_k\}_{k=1}^{\infty}$ where $\phi_k = \phi_1$. Then, taking the limit $|\to\infty$, we have $d_P(\phi_1(\{i, j\})) = \lim_{l \to \infty} d_{R_l}(\{i, j\})$. Since $\{R_l\}_{l=1}^{\infty}$ converges to $P$, we then have $d_P(\phi_1(\{i, j\})) = d_P(\{i, j\})$. But then, we have $d_P(\{i, j\}) = d_{Q_k}(\{i, j\})$ and by the Folklore Lemma, there is a rigid transformation from $P$ to $Q_k$, so we have a contradiction.
Relabelings

A permutation $\phi$ of $\mathcal{P}$ is a relabeling if there exists a permutation $\pi$ of $\{1, \ldots, n\}$ such that $\phi(\{i, j\}) = \{\pi(i), \pi(j)\}$.

- **Corollary:**

  If there exists a relabeling $\phi$ of $\mathcal{P}$ such that $d_P(\phi(\{i, j\})) = d_Q(\{i, j\})$, then there is a permutation $\pi$ of $\{1, \ldots, n\}$ such that $p_{\pi(1)}, \ldots, p_{\pi(n)}$ has the same distance matrix as $q_1, \ldots, q_n$, and therefore, by the Folklore Lemma, there is a rigid transformation from $p_{\pi(1)}, \ldots, p_{\pi(n)}$ to $q_1, \ldots, q_n$.

- **We want to show most point sets with the same distribution of distances have a relabeling.**
Key Lemma

Suppose $n \neq 4$. Then a permutation $\phi$ of $P$ is a relabeling if and only if for all pairwise distinct indices $i, j, k$ we have $\phi(\{i, j\}) \cap \phi(\{i, k\}) \neq \emptyset$.

**Proof:**

For every $n \leq 3$, every $\phi$ is a relabeling and $\phi(\{i, j\}) \cap \phi(\{i, k\}) \neq \emptyset$. Therefore, we may assume that $n \geq 5$. The only if part of the statement is clear by the definition of a relabeling, so we will show the if direction.

Suppose we have $\phi$ a permutation of $P$ such that for all pairwise distinct indices $i, j, k$ we have $\phi(\{i, j\}) \cap \phi(\{i, k\}) \neq \emptyset$. We note that since $\phi$ is a permutation, the intersection must then contain only one element. Therefore, we may assume that $n \geq 5$. The only if part of the statement is clear by the definition of a relabeling, so we will show the if direction.

Suppose we have $\phi$ a permutation of $P$ such that for all pairwise distinct indices $i, j, k$ we have $\phi(\{i, j\}) \cap \phi(\{i, k\}) \neq \emptyset$. We note that since $\phi$ is a permutation, the intersection must then contain only one element. Then, we argue that for $i, j, k, l$ pairwise distinct, $\phi(\{i, j\}) \cap \phi(\{i, k\}) \cap \phi(\{i, l\}) \neq \emptyset$.

Suppose otherwise. Then, we can write $\phi(\{i, j\}) = \{a, b\}$, $\phi(\{i, k\}) = \{a, c\}$, and $\phi(\{i, l\}) = \{b, c\}$. Now, since we have more than 4 points, we can choose $m$ distinct from $i, j, k, l$. $\phi(\{i, m\})$ must intersect $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$. Since $\phi(\{i, m\})$ only has two elements, it must be one of the sets $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$, but then that would violate $\phi$ being a permutation. Therefore, $\phi(\{i, j\}) \cap \phi(\{i, k\}) \cap \phi(\{i, l\}) \neq \emptyset$.

Then if we fix an $i$ and choose any distinct $j, k$, $\phi(\{i, j\}) \cap \phi(\{i, k\})$ must contain an distinct element $a$ and the above shows that $a$ belongs to any $\phi(\{i, l\})$ where $l$ is distinct from $i, j, k$. Therefore $\bigcap_{l \neq i} \phi(\{i, l\}) = a$ and we can define the map $\sigma$ from $\{1, \ldots, n\}$ to itself where $\sigma(i) = a$.

To show that $\sigma$ is a permutation, we simply need to show that it is injective. To do this, we let $M_i$ be the set of all pairs with $i$ in them. Then, $\phi(M_i) \subseteq M_{\sigma(i)}$. But $\phi$ is a permutation and $|M_i| = |M_{\sigma(i)}|$ so therefore $\phi(M_i) = M_{\sigma(i)}$. Now consider $i, j$ with $\sigma(i) = \sigma(j)$. Then, $M_{\sigma(i)} = M_{\sigma(j)}$ so $\phi(M_i) = \phi(M_j)$. But $\phi$ is a permutation so $M_i = M_j$ and therefore $i = j$ so $\sigma$ is injective.

Now, consider $\phi(\{i, j\})$. By the above discussion, it contains both $\sigma(i)$ and $\sigma(j)$, so $\phi(\{i, j\})$ must be $\{\sigma(i), \sigma(j)\}$. Since $\sigma$ is a permutation, $\phi$ is therefore a relabeling.
4 Points on a Plane

The proof that most point configurations are reconstructible from pair-wise distances relies on a certain determinant that is zero when four points \( p_i, p_j, p_k, p_l \) lie on a plane:

\[
\det \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} = 0
\]

where
\[
a = -2d_P(\{i, l\}), \quad b = d_P(\{i, j\}) - d_P(\{i, l\}) - d_P(\{j, l\}), \quad c = d_P(\{i, k\}) - d_P(\{i, l\}) - d_P(\{k, l\}),
\]
\[
d = -2d_P(\{j, l\}), \quad e = d_P(\{j, k\}) - d_P(\{j, l\}) - d_P(\{k, l\})
\]
and
\[
f = -2d_P(\{k, l\}).
\]

This determinant can be expanded as a polynomial:

\[
\]

where \( U = d_P(\{i, j\}), V = d_P(\{i, k\}), W = d_P(\{i, l\}), X = d_P(\{j, k\}), Y = d_P(\{j, l\}) \) and \( Z = d_P(\{k, l\}) \).
Let $n \geq 5$ and $P$ be a configuration of $n$ points in $\mathbb{R}^2$. Suppose for choices of indices $a, b, c, d, e, f, g, h, i, j, k$ such that the pairs $U = \{a, b\}, V = \{d, e\}, W = \{f, g\}, X = \{h, i\}, Y = \{j, k\}, Z = \{a, c\}$ are distinct, we have:

\[
g(d_P(U), d_P(V), d_P(W), d_P(X), d_P(Y), d_P(Z)) \neq 0
\]

then $P$ is reconstructible from pairwise distances.

**Proof:** Suppose that $Q$ is an $n$-point configuration in $\mathbb{R}^2$ with the same distribution of distances as $P$. Then, there exists a permutation $\phi$ such that $d_Q(\{i, j\}) = d_P(\phi(\{i, j\}))$ for all $i \neq j$. We then try to show that $\phi^{-1}$ is a relabeling, and thus $\phi$ is also a relabeling.

Now pick any pairwise distinct indices $r, s, t, u$. Now since $q_r, q_s, q_t, q_u$ lie on a plane,

\[
g(d_Q(\{r, s\}), d_Q(\{r, t\}), d_Q(\{r, u\}), d_Q(\{s, t\}), d_Q(\{s, u\}), d_Q(\{t, u\})) = 0
\]

But then, it follows that

\[
g(d_P(\phi(\{r, s\})), d_P(\phi(\{r, t\})), d_P(\phi(\{r, u\})), d_P(\phi(\{s, t\})), d_P(\phi(\{s, u\})), d_P(\phi(\{t, u\}))) = 0
\]

Therefore, it follows that $\phi(\{r, s\})$ and $\phi(\{t, u\})$ are disjoint, otherwise the pairs would satisfy the conditions of the $U, V, W, X, Y, Z$ stated above and

\[
g(d_P(U), d_P(V), d_P(W), d_P(X), d_P(Y), d_P(Z)) \neq 0
\]

so we have show that $\phi$ maps disjoint sets $\{r, s\}$ and $\{t, u\}$ to disjoint sets. We take the contrapositive and note that if $\phi(\{r, s\})$ and $\phi(\{t, u\})$ intersect, then $\{r, s\}$ and $\{t, u\}$ also necessarily intersect. Thus, for all $i, j, k$ we have

\[
\phi^{-1}(\{i, j\}) \cap \phi^{-1}(\{i, k\}) \neq \emptyset
\]

and hence $\phi^{-1}$ is a relabeling. But then there exists a permutation $\pi$ of $\{1, \ldots, n\}$ such that $\phi^{-1}(\{i, j\}) = \{\pi(i), \pi(j)\}$. Then, clearly, $\phi(\{i, j\}) = \{\pi^{-1}(i), \pi^{-1}(j)\}$ and thus $\phi$ is also a relabeling. Thus, by Corollary 4.5, there is a rigid transformation and a relabeling that maps $P$ to $Q$. 

**Main Result**
Generalization

• Can be generalized for points in $\mathbb{R}^m$ for $n$ greater than or equal to $m+2$.

• Similar method.
Computation

- Experiments testing this general position condition are not very fast.

- $O(n^{11})$ time.
More Extensions

- Oriented rigid transformations.
- Scalings.
- Graphs with edge weights using distribution of sub-triangles.
Open Problems

• Complete test for reconstructibility.

• Relate to Gromov-Hausdorff: Point sets are close w.r.t GH distance when their pairwise distance distributions are close under some measure.