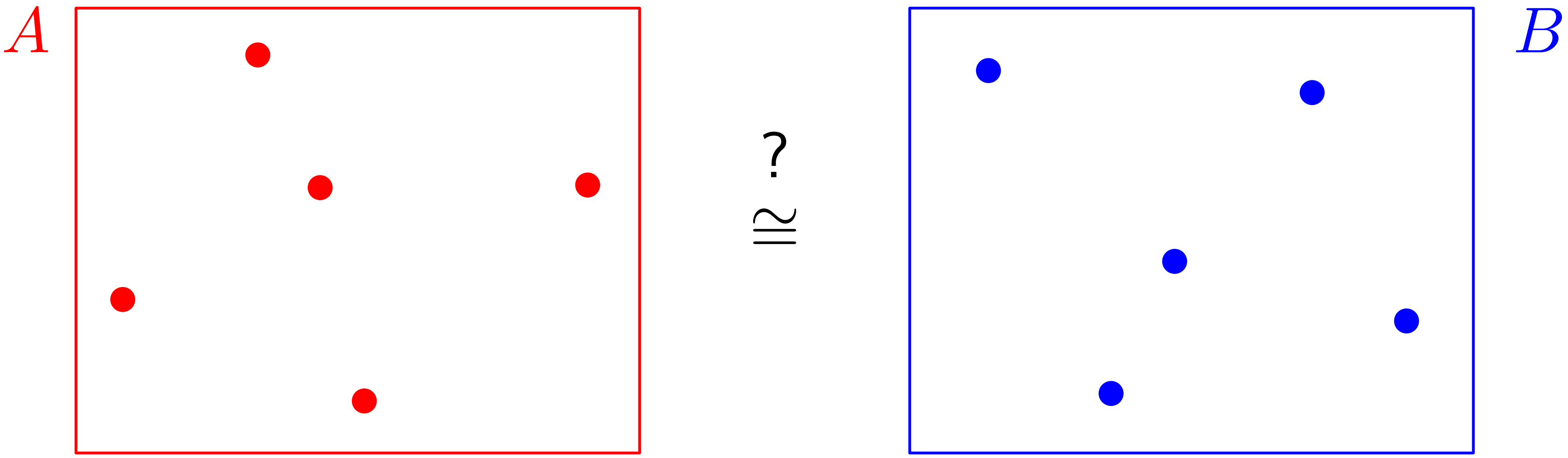
The Computational Geometry of Congruence Testing

Günter Rote

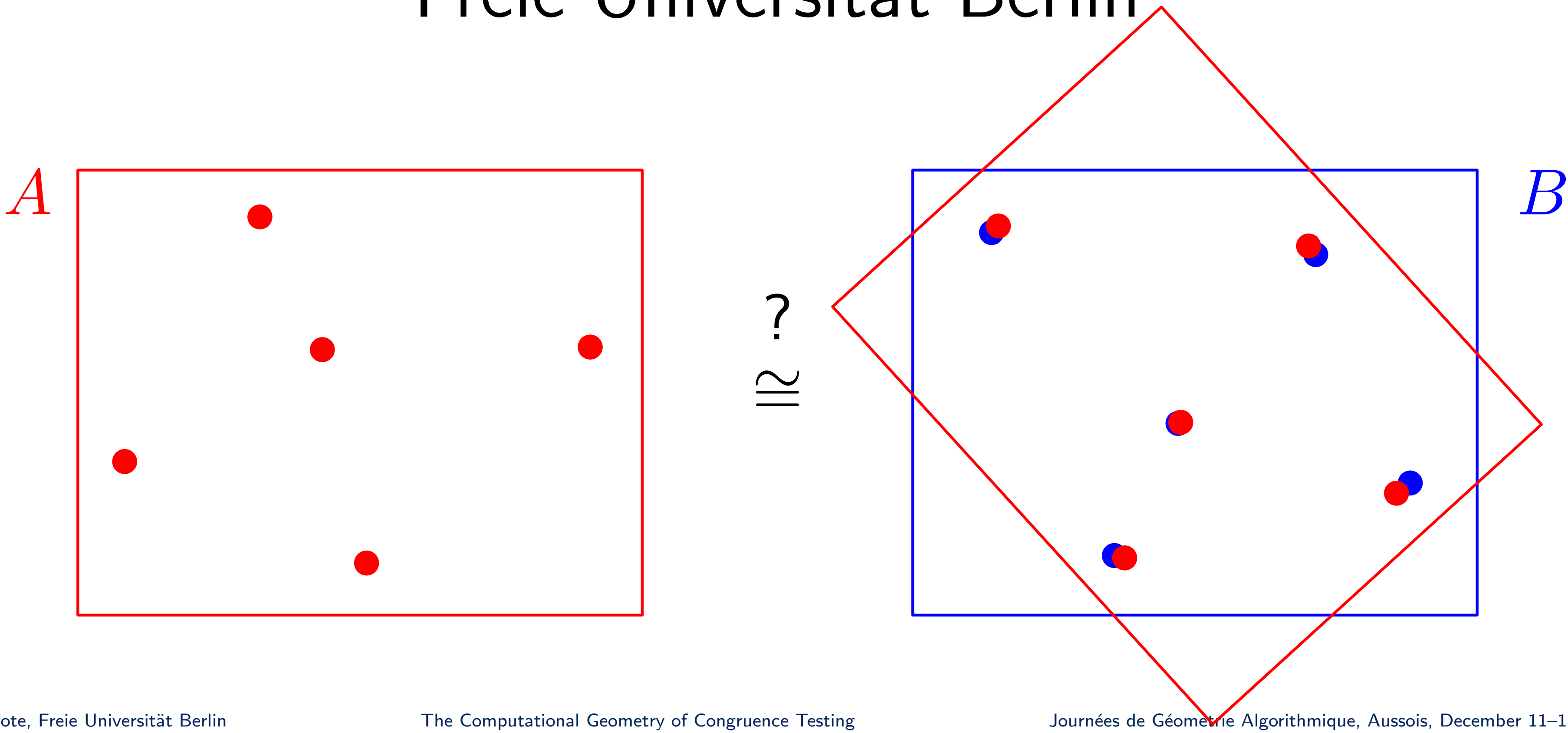
Freie Universität Berlin



The Computational Geometry of Congruence Testing

Günter Rote

Freie Universität Berlin



Overview

- 1 dimension
- 2 dimensions
- 3 dimensions
- 4 dimensions
- d dimensions

Overview

- 1 dimension
- 2 dimensions
- 3 dimensions
- 4 dimensions ← tomorrow (joint work with Heuna Kim)

$\Bigg\}$ $O(n \log n)$ time

- d dimensions $O(n^{\lceil d/3 \rceil} \log n)$ time [Brass and Knauer 2002]

  $O(n^{(1+\lfloor d/2 \rfloor)/2} \log n)$ Monte Carlo [Akutsu 1998/Matoušek]

Overview

- 1 dimension
- 2 dimensions
- 3 dimensions
- 4 dimensions

$\}$ $O(n \log n)$ time

← tomorrow (joint work with Heuna Kim)

- d dimensions $O(n^{\lceil d/3 \rceil} \log n)$ time [Brass and Knauer 2002]

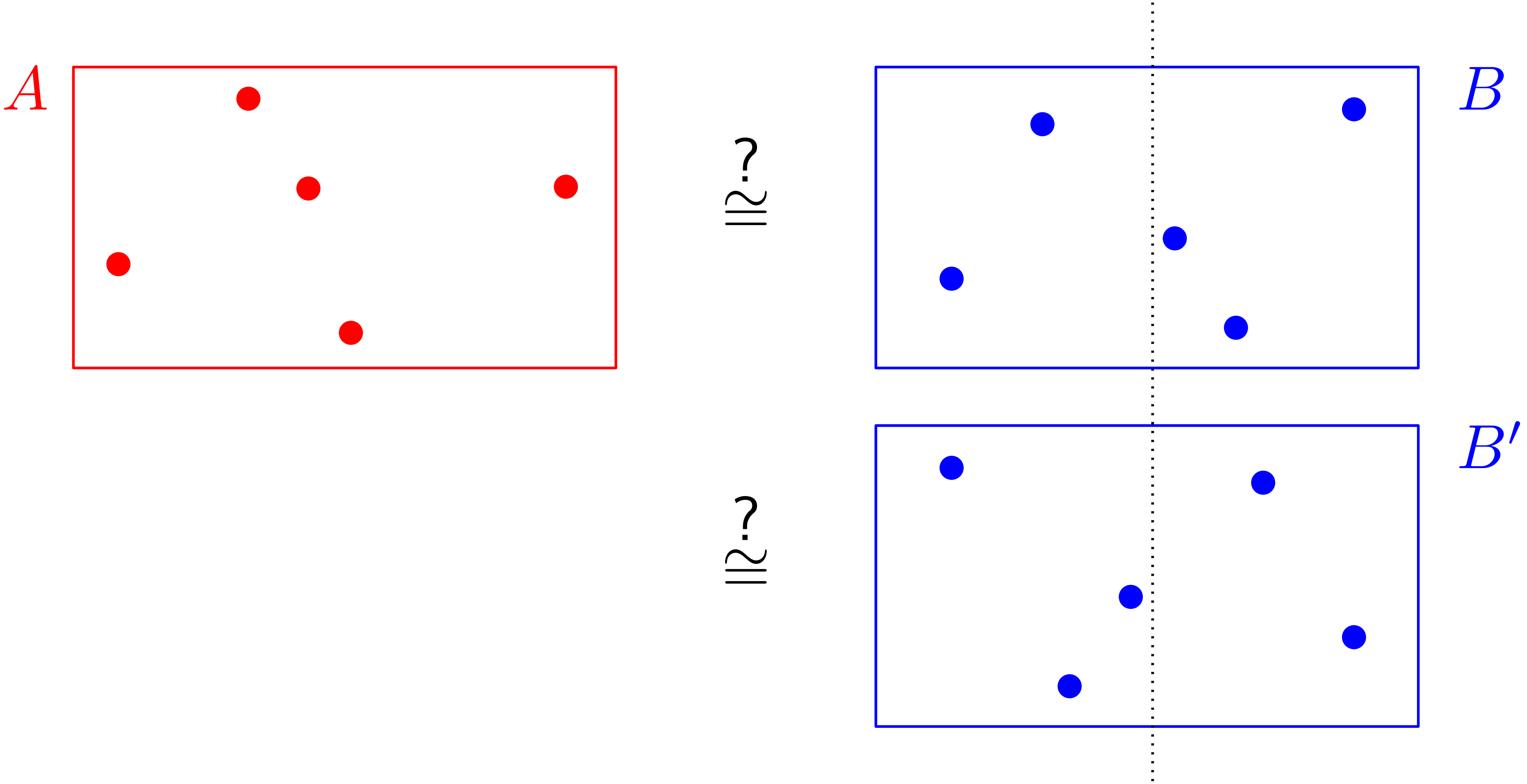
  $O(n^{(1+\lfloor d/2 \rfloor)/2} \log n)$ Monte Carlo [Akutsu 1998/Matoušek]

- Problem statement and variations
- Dimension reduction as in [Alt, Mehlhorn, Wagener, Welzl]
- The birthday paradox [Akutsu]
- Planar graph isomorphism
- Akutsu's canonical form
- Matoušek's closest pairs
- Atkinson's reduction (pruning/condensation)

Rotation or Rotation+Reflection?

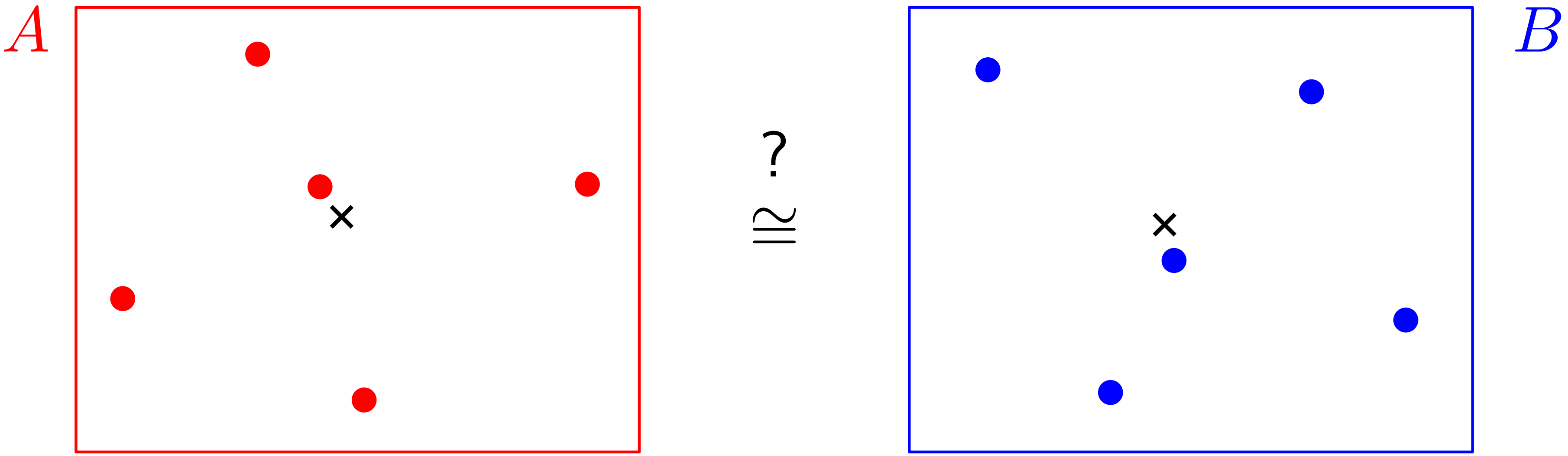
We only need to consider *proper* congruence (orientation-preserving congruence, of determinant $+1$).

If mirror-congruence is also desired, repeat the test twice, for B and its mirror image B'.



Congruence = Rotation + Translation

Translation is easy to determine:
The centroid of A must coincide with the centroid of B.

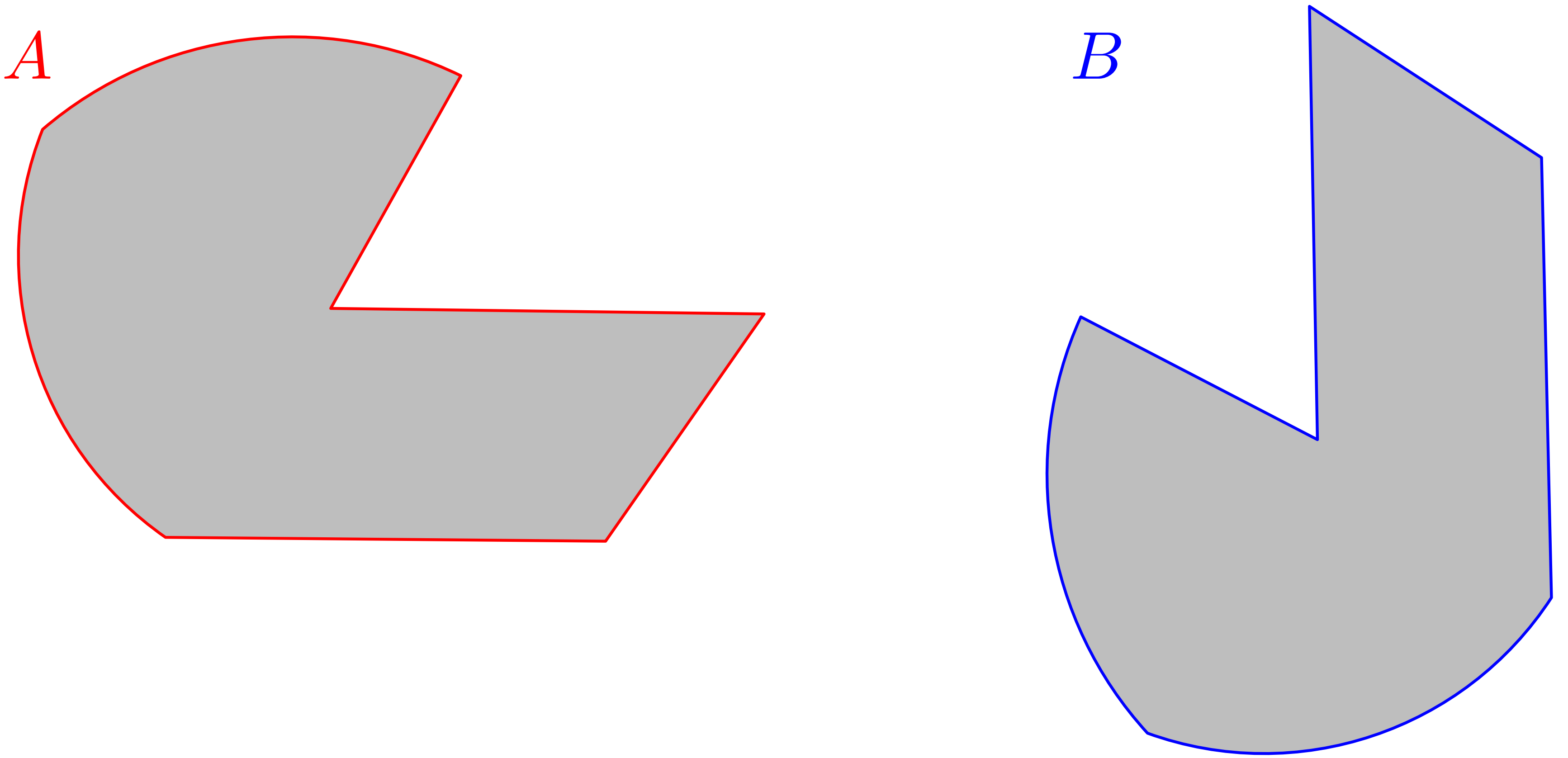


$\rightarrow$ from now on: All point sets are centered at the origin 0:

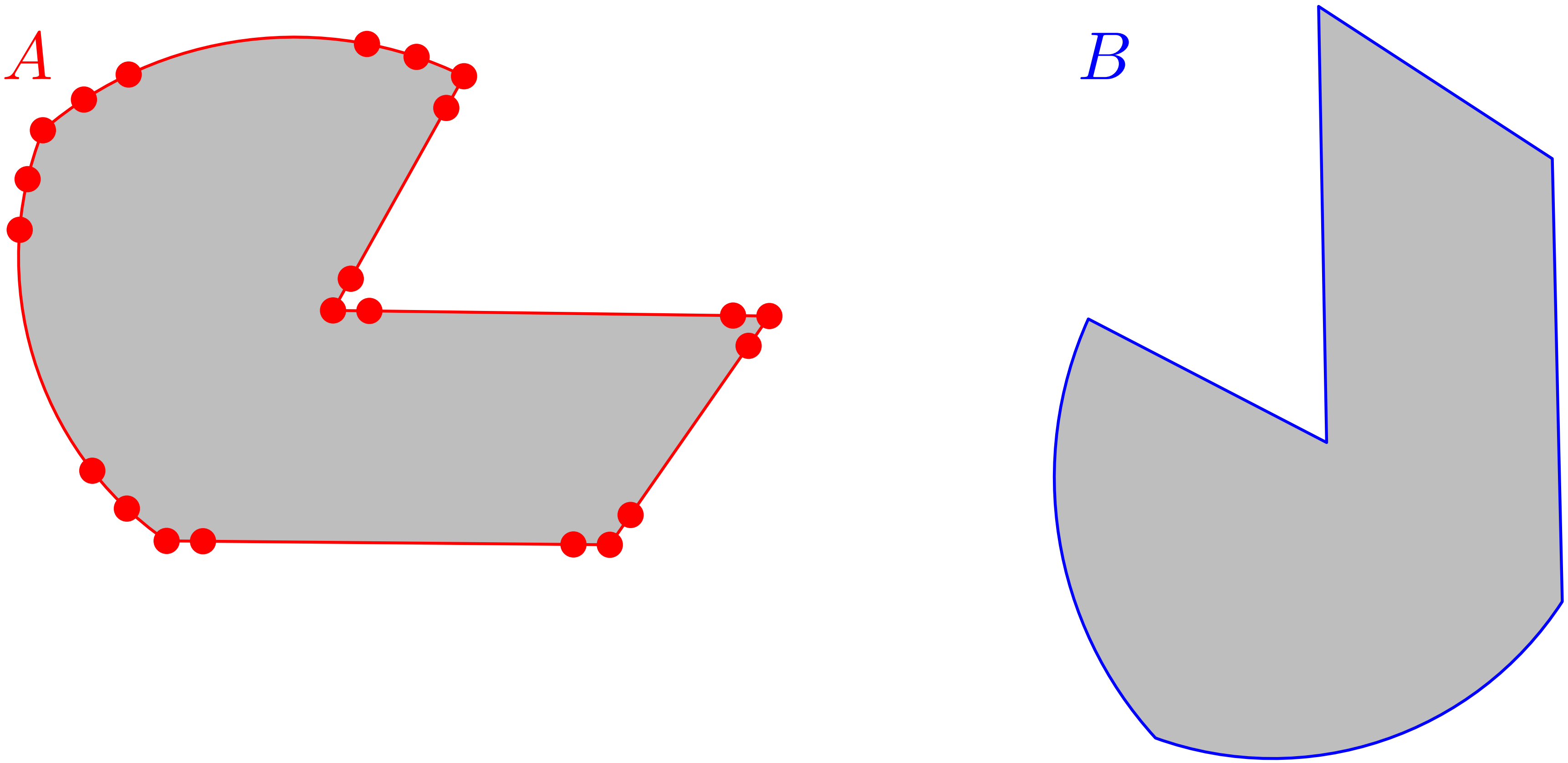
$$\sum_{a\in A} a = \sum_{b\in B} b = 0$$

We need to find a rotation around the origin (orthogonal matrix T with determinant $+1$) which maps A to B: $TA = B$

Geometric Shapes



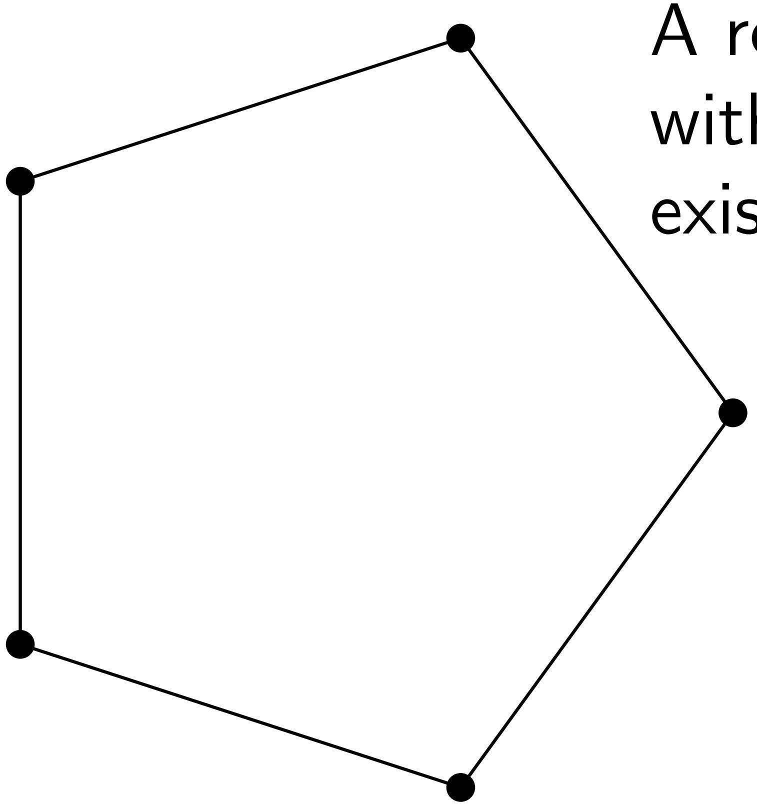
Geometric Shapes



Geometric shapes
can be represented by “marked” (colored) point sets.

Exact Arithmetic

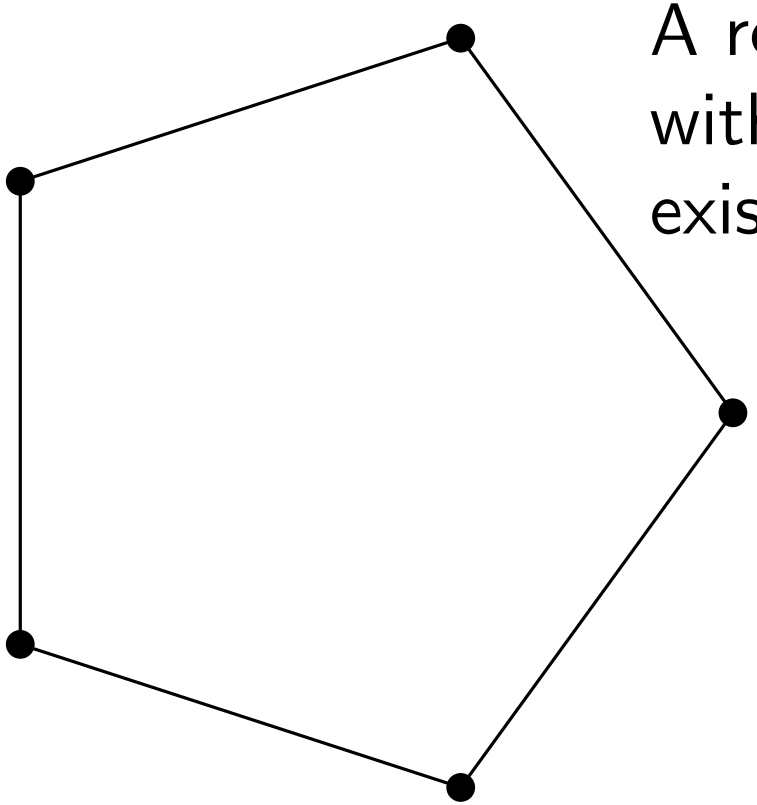
The proper setting for this (mathematical) problem requires real numbers as inputs and exact arithmetic.
$\rightarrow$ the *Real RAM* model (RAM $=$ random access machine):
One elementary operation with real numbers ($+$, $\div$, $\sqrt{}$, $\sin$) is counted as one step.



A regular 5-gon, 7-gon, 8-gon, . . . with rational coordinates does not exist in any dimension.

Exact Arithmetic

The proper setting for this (mathematical) problem requires real numbers as inputs and exact arithmetic.
→ the *Real RAM* model (RAM = random access machine):
One elementary operation with real numbers ($+$, $\div$, $\sqrt{}$, $\sin$) is counted as one step.



A regular 5-gon, 7-gon, 8-gon, ... with rational coordinates does not exist in any dimension.

[Arvind, Rattan 2016]:
Rational coordinates with L bits:

$$2^{O(d \log d)} \cdot \mathrm{poly}(nL) \text{ time}$$

(fixed-parameter tractable, FPT)
Previously: $2^{O(d^4)} \cdot \mathrm{poly}(nL)$
[Evdokimov, Ponomarenko 1997]

Applications

Congruence testing is the basic problem for many pattern matching tasks

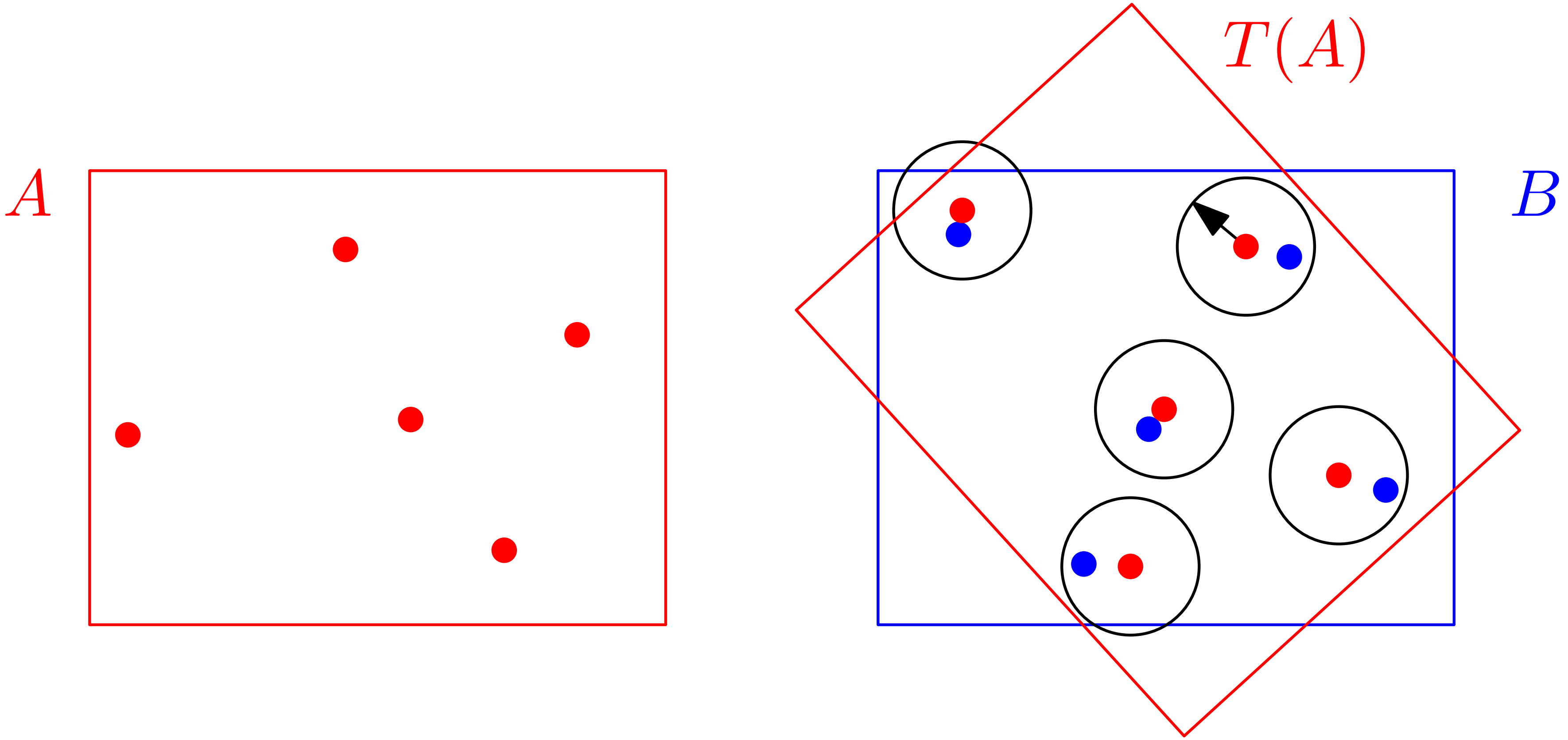
- computer vision
- star matching
- brain matching
- ...

The proper setting for this applied problem requires tolerances, partial matchings, and other extensions.

Approximate matching

Given two sets A and B in the plane and an error tolerance ε, find a bijection $f\colon A \to B$ and a congruence T such that

$$\|T(a) - f(a)\| \le \varepsilon, \text{ for every } a \in A.$$



$O(n^8)$ time in the plane [Alt, Mehlhorn, Wagener, Welzl 1988]

Arbitrary Dimension

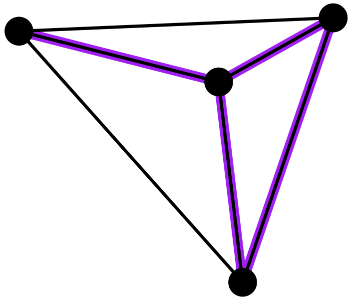
$A, B \subset \mathbb{R}^d$, $|A| = |B| = n$.

We consider the problem for fixed dimension d.

When d is unrestricted, the problem is equivalent to graph isomorphism:

$G = (V, E)$, $V = \{1, 2, \ldots, n\}$

$$\mapsto A = \underbrace{\{e_1, \ldots, e_n\}}_{\text{regular simplex}} \cup \{ \tfrac{e_i + e_j}{2} \mid ij \in E \} \subset \mathbb{R}^n$$



$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

MAIN CONJECTURE:
Congruence can be tested in $O(n \log n)$ time for every fixed dimension d.

Current best bound: $O(n^{\lceil d/3 \rceil} \log n)$ time

Arbitrary Dimension

$A, B \subset \mathbb{R}^d$, $|A| = |B| = n$.

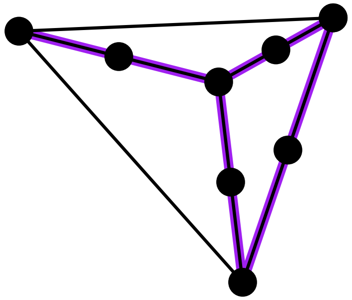
We consider the problem for fixed dimension d.

When d is unrestricted, the problem is equivalent to graph isomorphism:

$G = (V, E)$, $V = \{1, 2, \dots, n\}$

$$\mapsto A = \underbrace{\{e_1, \dots, e_n\}}_{\text{regular simplex}} \cup \{ \tfrac{e_i + e_j}{2} \mid ij \in E \} \subset \mathbb{R}^n$$

$$e_i = (0, \dots, 0, 1, 0, \dots, 0)$$



MAIN CONJECTURE:
Congruence can be tested in $O(n \log n)$ time for every fixed dimension d.

Current best bound: $O(n^{\lceil d/3 \rceil} \log n)$ time

One dimension

Trivial.
(after shifting the centroid to the origin and getting rid of reflection):

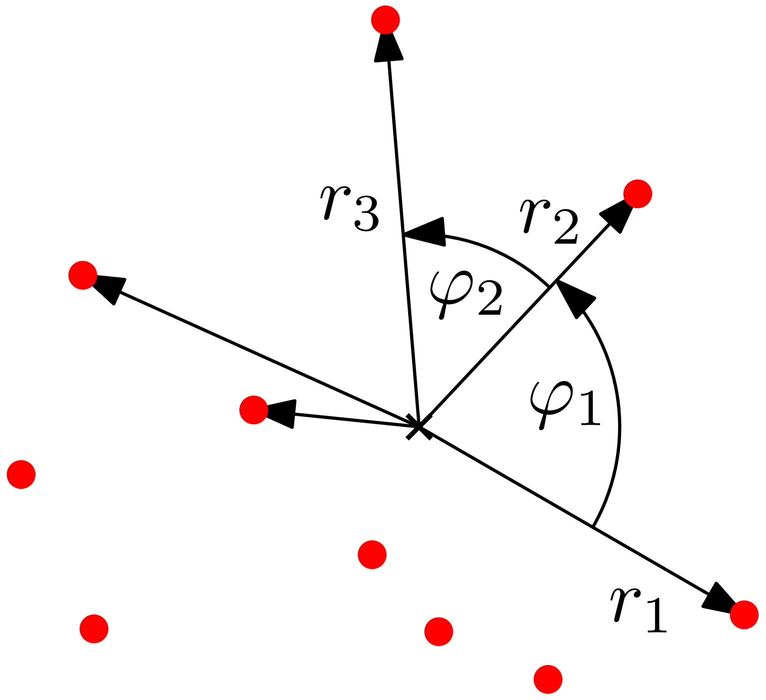
Test if $A = B$. $O(n \log n)$ time.

Two dimensions

Can be done by string matching. [Manacher 1976]

Sort points around the origin.

Encode alternating sequence of distances r_i and angles φ_i.



$$(r_1, \varphi_1; r_2, \varphi_2; \ldots; r_n, \varphi_n)$$

Check whether the corresponding sequence of B is a cyclic shift.

$\rightarrow O(n \log n) + O(n)$ time.

Two dimensions

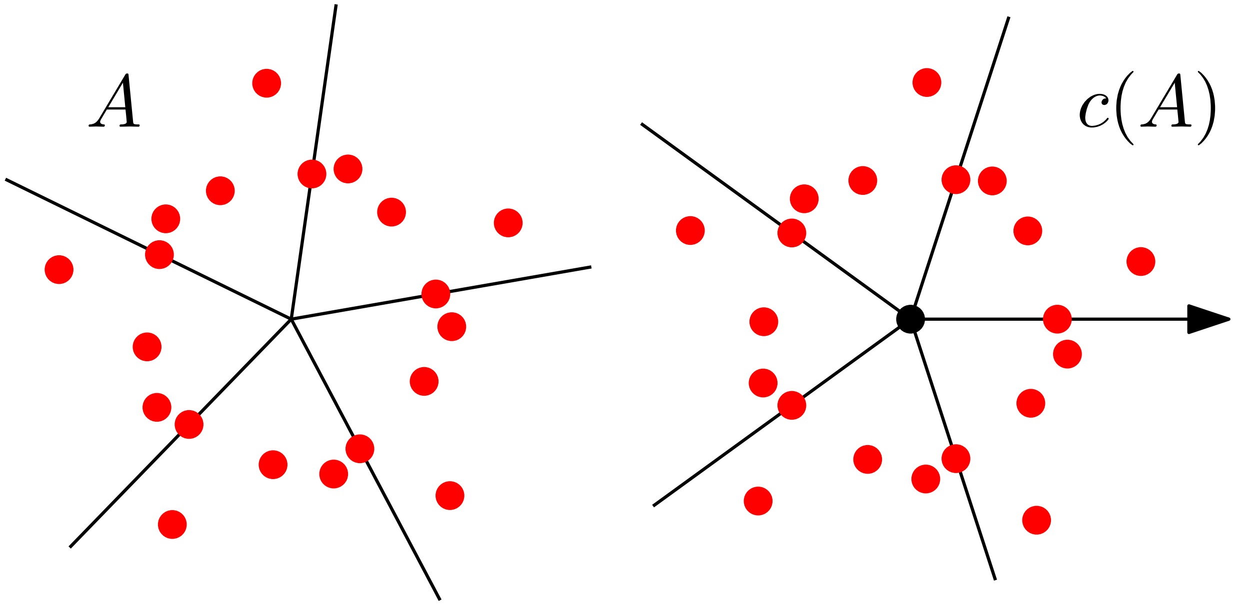
Can be done by string matching. [Manacher 1976]

Sort points around the origin.

Encode alternating sequence of distances r_i and angles φ_i.

Even more can be done:

CANONICAL DIRECTIONS



The *canonical set* $c(A)$: [Akutsu 1992]

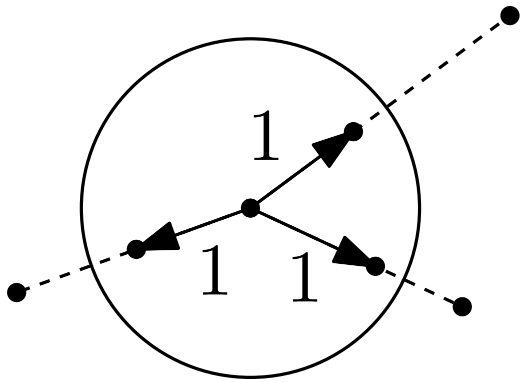
$$A \cong B \iff c(A) = c(B)$$

$\rightarrow$ searching in a database

Three dimensions

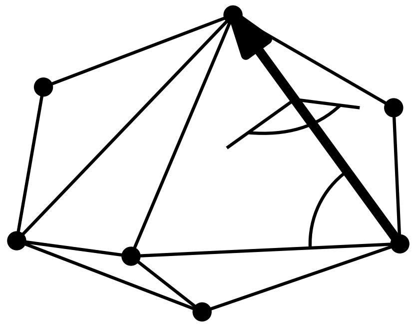
[Sugihara 1984; Alt, Mehlhorn, Wagener, Welzl 1988]

Project points to the unit sphere,
and keep distances as *labels*.



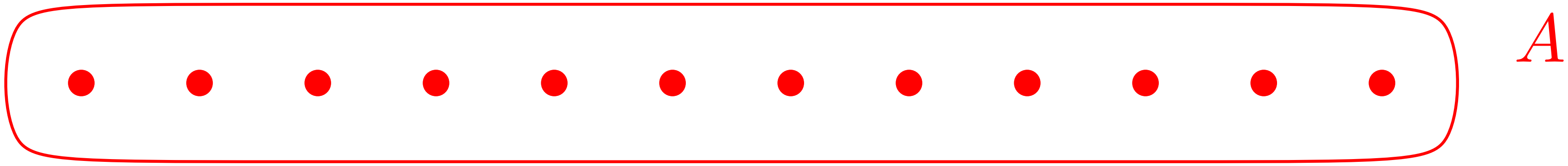
Compute the convex hulls $P(A)$ and $P(B)$, in $O(n \log n)$ time.

Check isomorphism between the corresponding LABELED planar graphs.
Vertex labels: from the radial projection
Edge labels: dihedral angles and face angles.

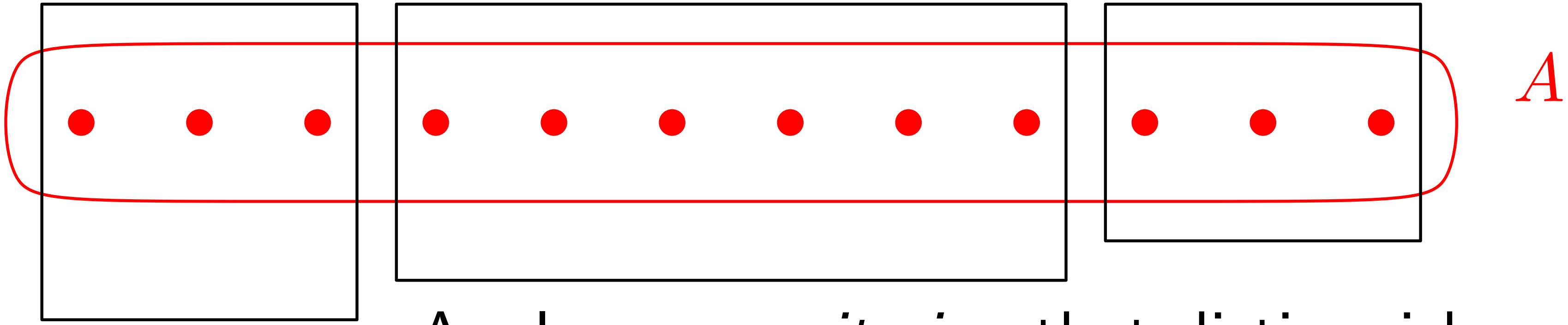


In $O(n)$ time, [Hopcroft and Wong 1974]
or in $O(n \log n)$ time. [Hopcroft and Tarjan 1973]

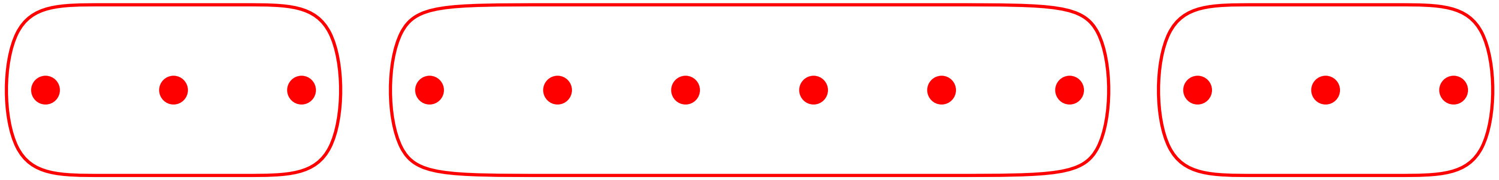
Pruning/Condensing



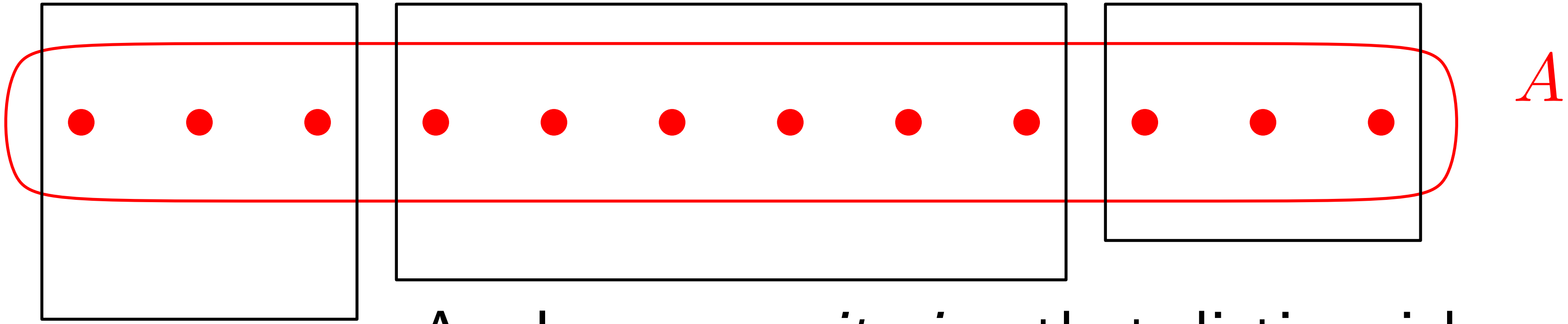
Pruning/Condensing



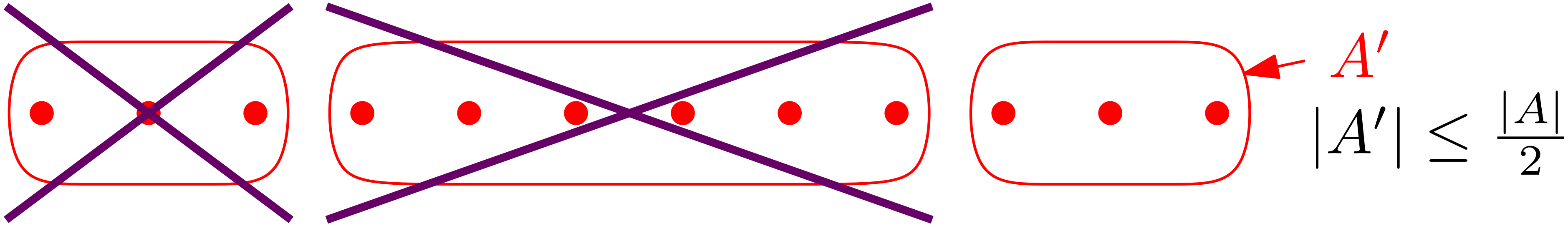
Apply some *criterion* that distinguishes points
(distance from the center,
number of closest neighbors, . . .)



Pruning/Condensing



Apply some *criterion* that distinguishes points (distance from the center, number of closest neighbors, . . .)

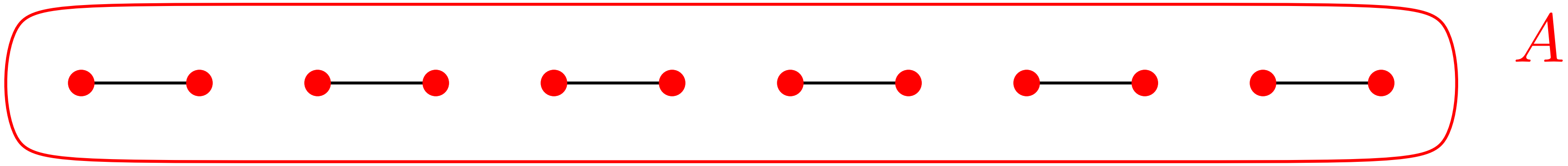


Throw away all but the smallest resulting class, and repeat.

Simultaneously apply this procedure to B.

A' and B' may have *more* congruences!

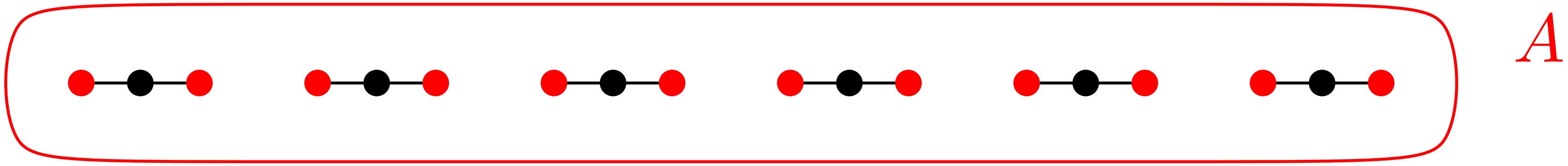
Pruning/Condensing



Make some *construction*
(midpoints of closest-pair edges, . . .)

Simultaneously apply this procedure to B.
A' and B' may have *more* congruences!

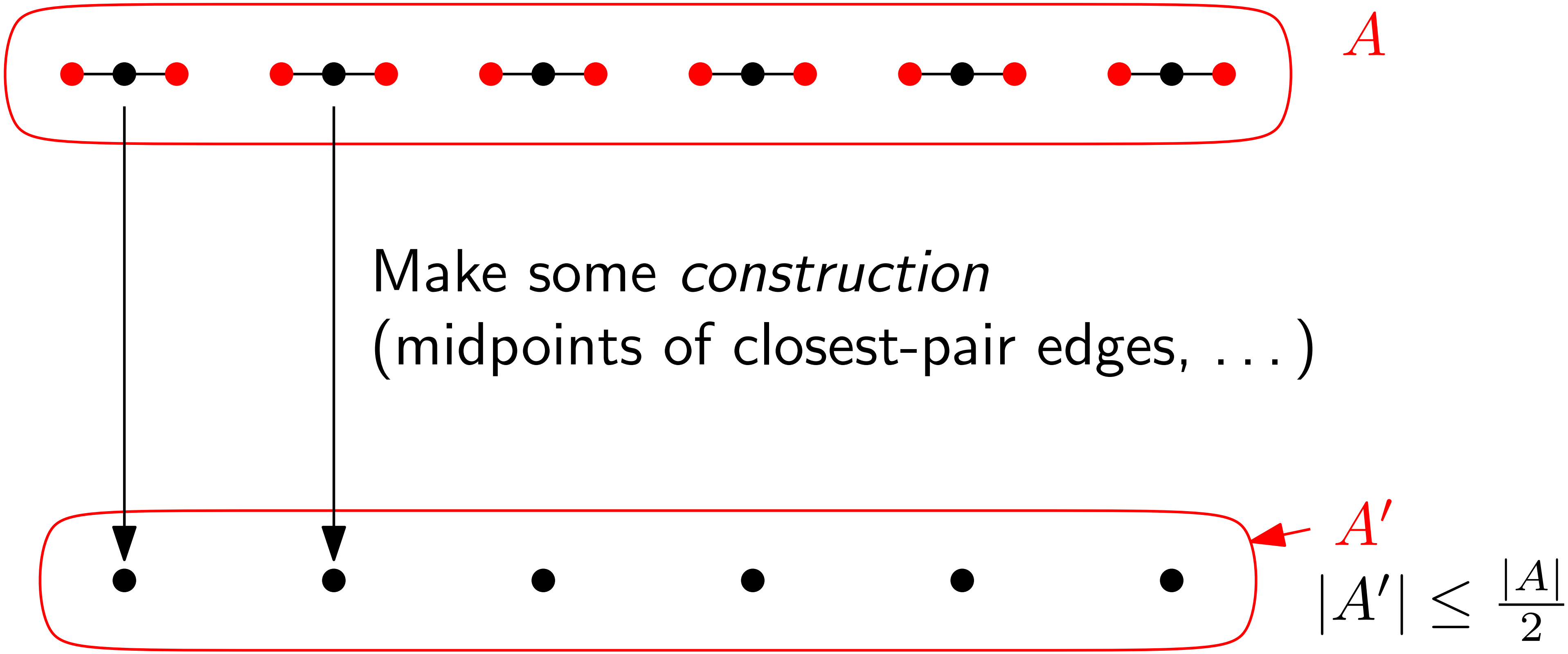
Pruning/Condensing



Make some *construction*
(midpoints of closest-pair edges, . . .)

Simultaneously apply this procedure to B.
A' and B' may have *more* congruences!

Pruning/Condensing



Make some *construction*
(midpoints of closest-pair edges, . . .)

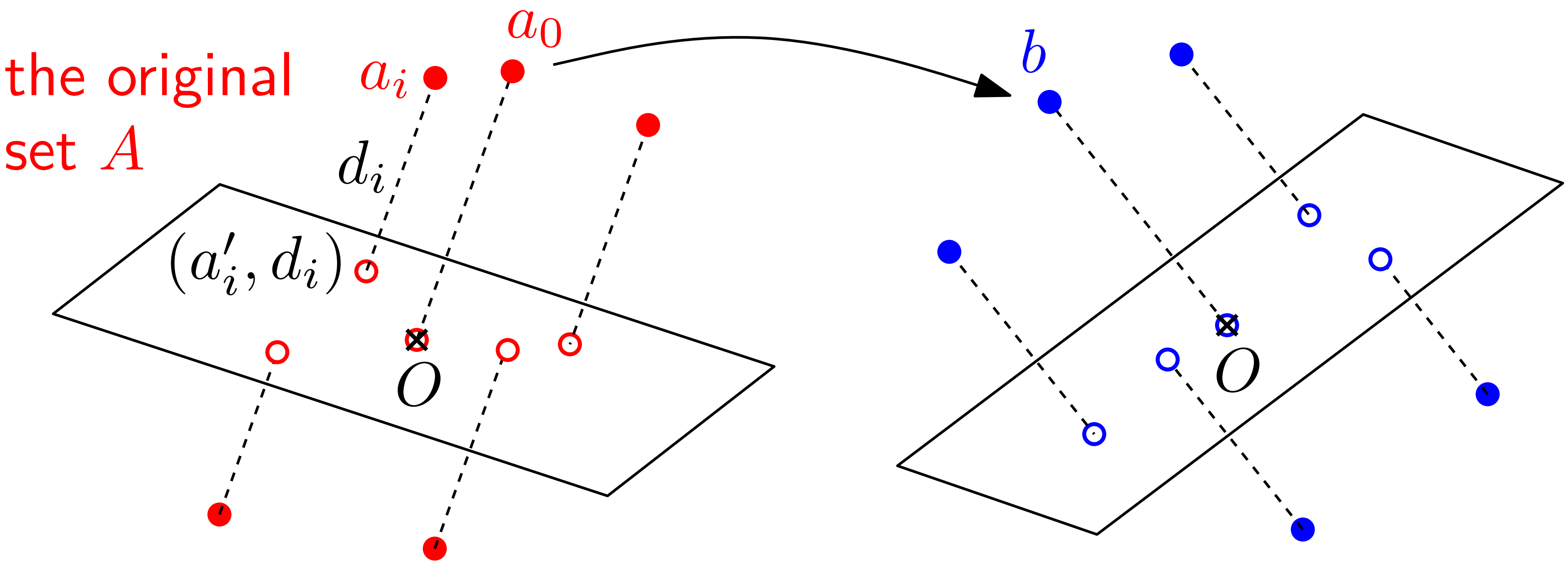
$|A'| \le \frac{|A|}{2}$

Simultaneously apply this procedure to B.
A' and B' may have *more* congruences!

Dimension Reduction

As soon as $|A'| = |B'| = k$ is small:
Choose a point $a_0 \in A'$ and try all k possibilities of mapping it to a point $b \in B'$.

$\boxed{\text{Fixing } a_0 \mapsto b \text{ reduces the dimension by one.}}$



Project perpendicular to Oa_0 and label projected points a_i' with the signed projection distance d_i as (a_i', d_i).

→ 2-dimensional congruence for LABELLED point sets

Dimension Reduction

As soon as $|A'| = |B'| = k$ is small:
Choose a point $a_0 \in A'$ and try all k possibilities of mapping it to a point $b \in B'$.

$$\boxed{\text{Fixing } a_0 \mapsto b \text{ reduces the dimension by one.}}$$

One problem in d dimensions is reduced to k problems in $d-1$ dimensions.

Three Dimensions [Akutsu 1995]

PRUNE by distance from the origin. If the points lie in a plane or on a line → DIMENSION REDUCTION.

Compute the convex hull.
If there are vertices of different degrees → PRUNE

The number n of vertices is reduced to $\leq n/2$. RESTART.

All n vertices have now degree 3, 4, or 5.
There are $f = \frac{n}{2} + 2$ or $f = n + 2$ or $f = \frac{3n}{2} + 2$ faces.

If the face degrees are not all equal
→ switch to the centroids of the faces and PRUNE them.

n is reduced to $\leq \frac{3n}{4} + 1$. RESTART.

Now $P(A)$ must have the graph of a Platonic solid. $\rightarrow n \leq 20$.
→ DIMENSION REDUCTION.

Three Dimensions [Akutsu 1995]

PRUNE by distance from the origin. If the points lie in a plane or on a line → DIMENSION REDUCTION.

Compute the convex hull. ← $\boxed{O(|A| \log |A|) \text{ time}}$

If there are vertices of different degrees → PRUNE

The number n of vertices is reduced to $\leq n/2$. RESTART.

All n vertices have now degree 3, 4, or 5.

There are $f = \frac{n}{2} + 2$ or $f = n + 2$ or $f = \frac{3n}{2} + 2$ faces.

If the face degrees are not all equal

→ switch to the centroids of the faces and PRUNE them.

n is reduced to $\leq \frac{3n}{4} + 1$. RESTART.

graph-theoretic pruning

$$\boxed{\begin{aligned}&\text{TIME} =\\ &O(n \log n) + O(\tfrac{3}{4}n \log \tfrac{3}{4}n) + O((\tfrac{3}{4})^2 n \log((\tfrac{3}{4})^2 n)) + \ldots\\ &= O(n \log n)\end{aligned}}$$

Three Dimensions [Akutsu 1995]

The doubly-regular planar graphs:
n vertices of degree d_V, f faces of degree d_F, m edges.

$$nd_V = 2m = fd_F$$

$$n + f = m + 2$$ (Euler's formula)

$$\frac{2}{d_V} + \frac{2}{d_F} = 1 + \frac{2}{m}$$

d_V	d_F	m		
3	3	6	tetrahedron	$(n = 4)$
3	4	12	cube	$(n = 8)$
4	3	12	octahedron	$(n = 6)$
3	5	30	dodecahedron	$(n = 20)$
5	3	30	icosahedron	$(n = 12)$

Three Dimensions [Akutsu 1995]

PRUNE by distance from the origin. If the points lie in a plane or on a line → DIMENSION REDUCTION.

Compute the convex hull.
If there are vertices of different degrees → PRUNE

The number n of vertices is reduced to $\leq n/2$. RESTART.

All n vertices have now degree 3, 4, or 5.
There are $f = \frac{n}{2} + 2$ or $f = n + 2$ or $f = \frac{3n}{2} + 2$ faces.

If the face degrees are not all equal
→ switch to the centroids of the faces and PRUNE them.

n is reduced to $\leq \frac{3n}{4} + 1$. RESTART.

Now $P(A)$ must have the graph of a Platonic solid. $\rightarrow n \leq 20$.
→ DIMENSION REDUCTION.

Three Dimensions [Akutsu 1995]

PRUNE by distance from the origin. If the points lie in a plane or on a line → DIMENSION REDUCTION.

Canonical point sets in 3d:

We get ≤ 20 two-dimensional projected point sets.
For each such set:
  Rotate the plane to the x-y-plane.
  Compute the canonical 2-d point set.
$\rightarrow \leq 20$ candidates for canonical 3d point sets:
Choose the lex-smallest one.

Now $P(A)$ must have the graph of a Platonic solid. $\rightarrow n \leq 20$.
→ DIMENSION REDUCTION.

PRUNING/CONDENSING in general

Function $f(A) = A'$, $A' \not\subseteq \{0\}$, equivariant under rotations R:

$$f(RA) = RA'$$

A' has *all symmetries* of A (and maybe more).

Primary goal: $|A'| \le |A| \cdot c$, $c < 1$.

If there is a chance, PRUNE and start from scratch with A' instead of A.

Ultimate goal: $|A| \le$ const

Condensing on the 2-Sphere

Continue Atkonson's algorithm with more geometric pruning (instead of just graph-theoretic pruning)

Equivariant condensation on the 2-sphere:

Input: $A \subseteq \mathbb{S}^2$.
Output: $A' \subseteq \mathbb{S}^2$, $|A'| \le \min\{|A|, 12\}$, $A' = f(A)$ equivariant.

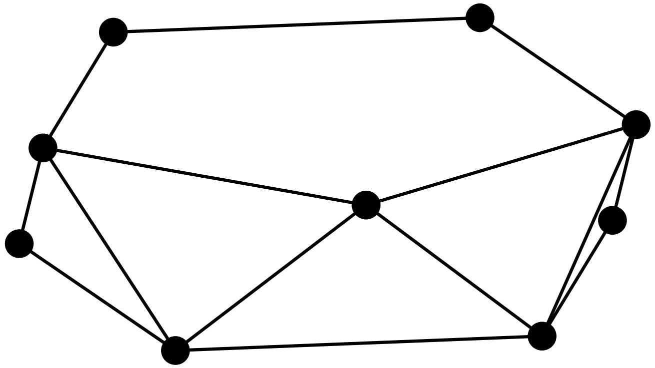
- $A' =$ vertices of a regular icosahedron
- $A' =$ vertices of a regular octahedron
- $A' =$ vertices of a regular tetrahedron
- $A' =$ two antipodal points, or
- $A' =$ a single point.

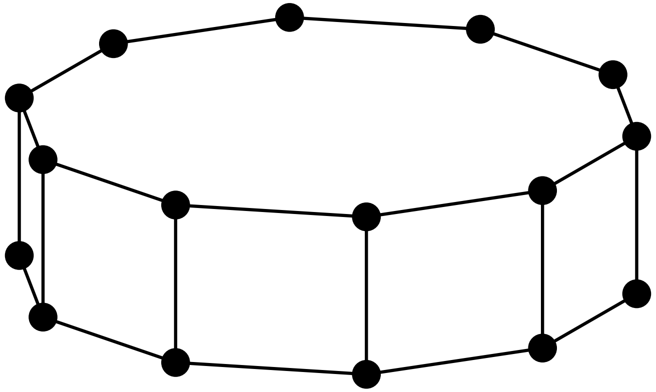
(will be needed later)

Symmetry groups

COROLLARY. The symmetry group of a finite full-dimensional point set in 3-space ($= $ a discrete subgroup of $O(3)$) is

- the symmetry group of a Platonic solid,
- the symmetry group of a regular prism,
- or a subgroup of such a group.





The *point groups* (discrete subgroups of $O(3)$) are classified (Hessel's Theorem).

[F. Hessel 1830, M. L. Frankenheim 1826]

Dimension d

Dimension reduction without pruning:

Pick $a_0 \in A$. Try $a_0 \mapsto b$ for all $b \in B$ (n possibilities).

$\rightarrow O(n^{d-2} \log n)$ time [Alt, Mehlhorn, Wagener, Welzl 1988]

Dimension d

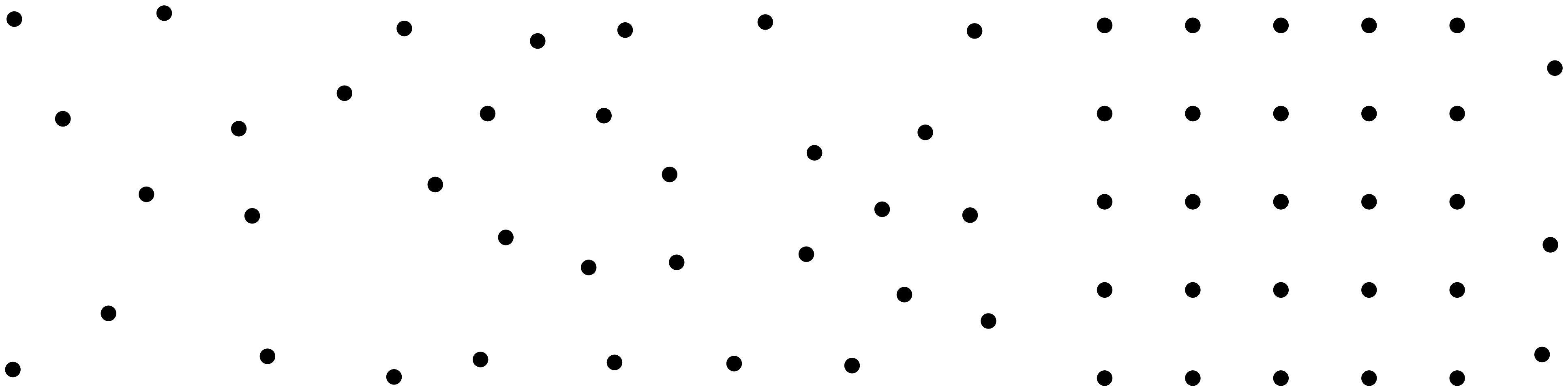
Dimension reduction without pruning:

Pick $a_0 \in A$. Try $a_0 \mapsto b$ for all $b \in B$ (n possibilities).

$\rightarrow O(n^{d-2} \log n)$ time [Alt, Mehlhorn, Wagener, Welzl 1988]

Closest pairs (a, a'): [Matoušek ≈ 1998]

minimum distance $\delta := \|a - a'\|$ among all pairs of vertices



Dimension d

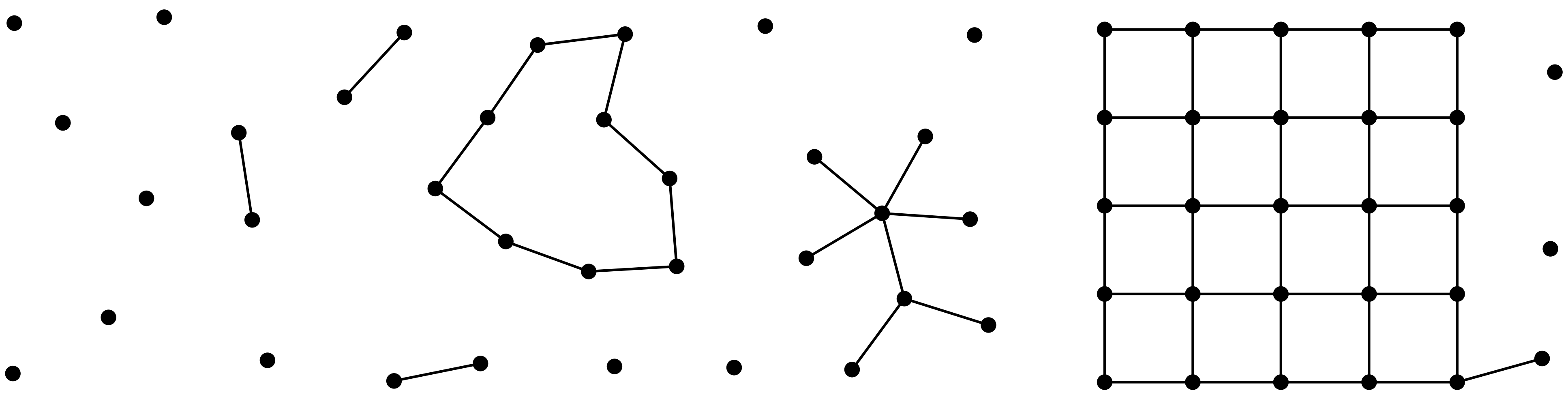
Dimension reduction without pruning:

Pick $a_0 \in A$. Try $a_0 \mapsto b$ for all $b \in B$ (n possibilities).

$\rightarrow O(n^{d-2} \log n)$ time [Alt, Mehlhorn, Wagener, Welzl 1988]

Closest pairs (a, a'): [Matoušek ≈ 1998]

minimum distance $\delta := \|a - a'\|$ among all pairs of vertices



Dimension d

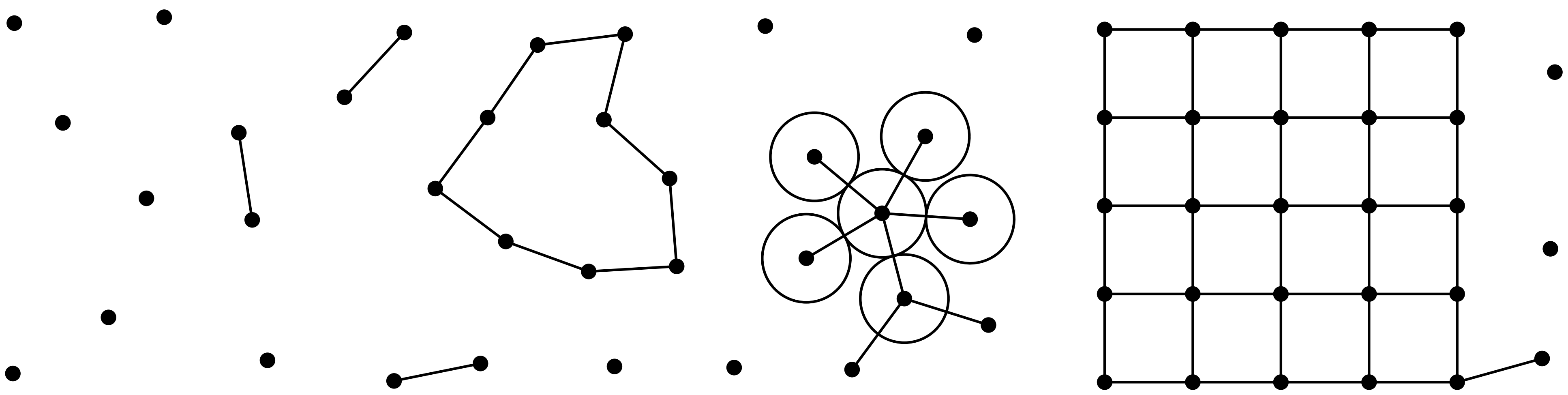
Dimension reduction without pruning:

Pick $a_0 \in A$. Try $a_0 \mapsto b$ for all $b \in B$ (n possibilities).

$\rightarrow O(n^{d-2} \log n)$ time [Alt, Mehlhorn, Wagener, Welzl 1988]

Closest pairs (a, a'): [Matoušek ≈ 1998]

minimum distance $\delta := \|a - a'\|$ among all pairs of vertices



Degree $\leq$ the *kissing number* K_d (by a packing argument).

All closest pairs can be computed in $O(n \log n)$ time (d fixed).

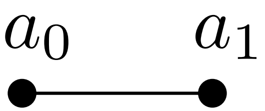
[Bentley and Shamos, STOC 1976]

Dimension d

Dimension reduction without pruning:

Pick $a_0 \in A$. Try $a_0 \mapsto b$ for all $b \in B$ (n possibilities).

$\rightarrow O(n^{d-2} \log n)$ time [Alt, Mehlhorn, Wagener, Welzl 1988]

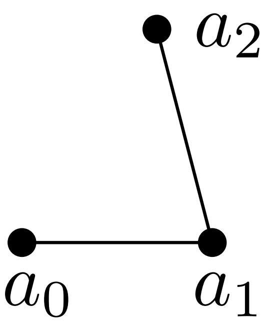


Pick a closest pair a_0a_1 in A. Try $(a_0, a_1) \mapsto (b, b')$ for all closest pairs (b, b') in B.

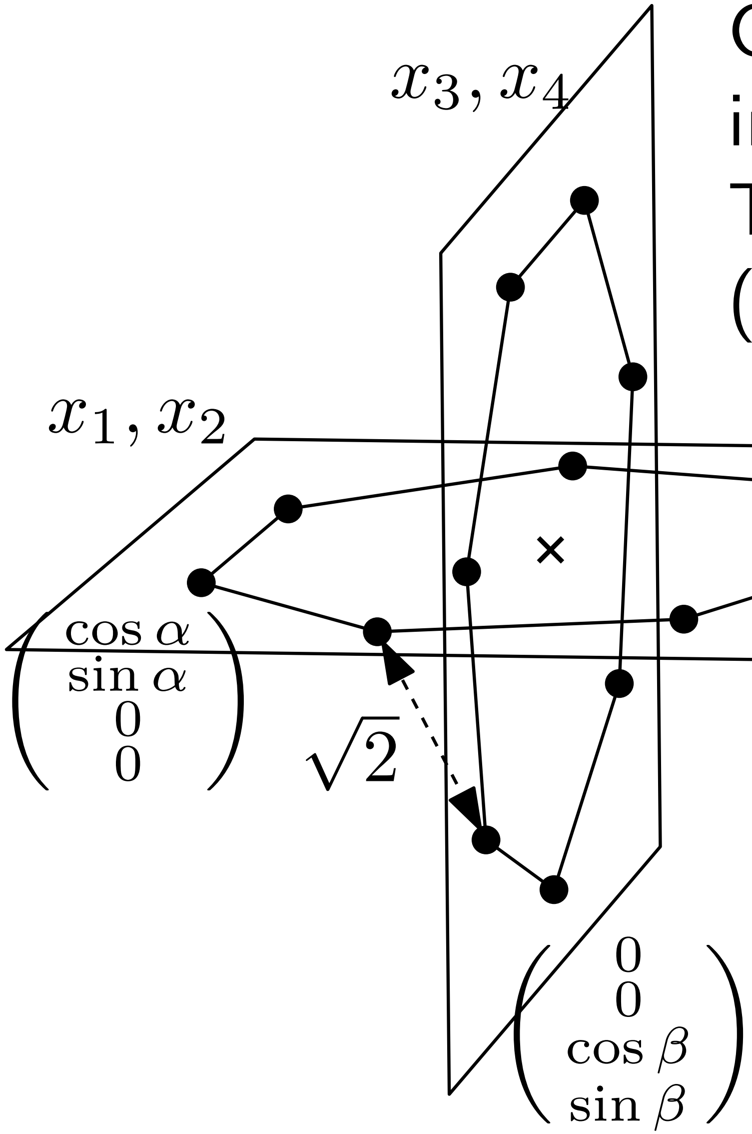
$O(n)$ possibilities, reducing the dimension by two.

$\rightarrow O(n^{\lfloor d/2 \rfloor} \log n)$ time [Matoušek ≈ 1998]

Further improvement: Find a "closest triplet" . . .



Life in Four Dimensions



Consider two regular n-gons
in the x_1x_2-plane and the x_3x_4-plane.
There are $\Theta(n^2)$ "closest triplets".
(Triplets on the same n-gon are not useful.)

The convex hull has
$\Theta(n^2)$ edges and facets.

[Brass and Knauer 2002]
Point sets in orthogonal subspaces
are the only problematic case;
they can be treated specially.

$\to O(n^{\lceil d/3 \rceil} \log n)$ time

The birthday paradox in 4 dimensions

$m :=$ const $\cdot \sqrt{n}$ [Akutsu 1998]

Take a random sample $R \subset A$ of size $|R| = m$

Take a random sample $S \subset B$ of size $|S| = m$

If $TA = B$, then with high prob., $\exists a \in R$, $\exists b \in S$ with $Ta = b$

[$(1 - \frac{m}{n})^m \approx 1 - \frac{m^2}{n}$ small]

$$\left.\begin{array}{l} \rightarrow \text{ labeled 3D sets } A_1, A_2, \ldots, A_m \\ \rightarrow \text{ labeled 3D sets } B_1, B_2, \ldots, B_m \end{array}\right\} A_i \cong B_j$$

$m \times m$ 3D problems $A_i \cong B_j$? (instead of $1 \times n$ 3D problems)

The birthday paradox in 4 dimensions

$m :=$ const $\cdot \sqrt{n}$ [Akutsu 1998]

Take a random sample $R \subset A$ of size $|R| = m$

Take a random sample $S \subset B$ of size $|S| = m$

If $TA = B$, then with high prob., $\exists a \in R$, $\exists b \in S$ with $Ta = b$

[$(1 - \frac{m}{n})^m \approx 1 - \frac{m^2}{n}$ small]

$$\left.\begin{array}{l}\rightarrow \text{ labeled 3D sets } A_1, A_2, \ldots, A_m \\ \rightarrow \text{ labeled 3D sets } B_1, B_2, \ldots, B_m\end{array}\right\} A_i \cong B_j$$

$m \times m$ 3D problems $A_i \cong B_j$? (instead of $1 \times n$ 3D problems)

Compute canonical 3D sets $c(A_1), \ldots, c(A_m); c(B_1), \ldots, c(B_m)$.
Look for duplicates between A and B.

→ Monte Carlo algorithm, $O(n^{3/2} \log n)$ time, $O(n^{3/2})$ space

in d dimensions: $O(n^{(d-2)/2} \log n)$ time, $O(n^{(d-2)/2})$ space

Use Closest Pairs in d Dimensions

$m :=$ const $\cdot \sqrt{n}$. Compute closest-pair graphs $\mathrm{CP}(A)$, $\mathrm{CP}(B)$.

Take a random sample $R \subset \mathrm{CP}(A)$ of size $|R| = m$

Take a random sample $S \subset \mathrm{CP}(B)$ of size $|S| = m$

$\rightarrow$ labeled sets $A_1, A_2, \ldots, A_m$ in $d - 2$ dimensions

$\rightarrow$ labeled sets $B_1, B_2, \ldots, B_m$ in $d - 2$ dimensions

$\rightarrow$ $O(n^{\lfloor (d-2)/2 \rfloor /2})$ labeled 3D or 2D sets $A'_1, A'_2, \ldots$ of size n

$\rightarrow$ $O(n^{\lfloor (d-2)/2 \rfloor /2})$ labeled 3D or 2D sets $B'_1, B'_2, \ldots$ of size n

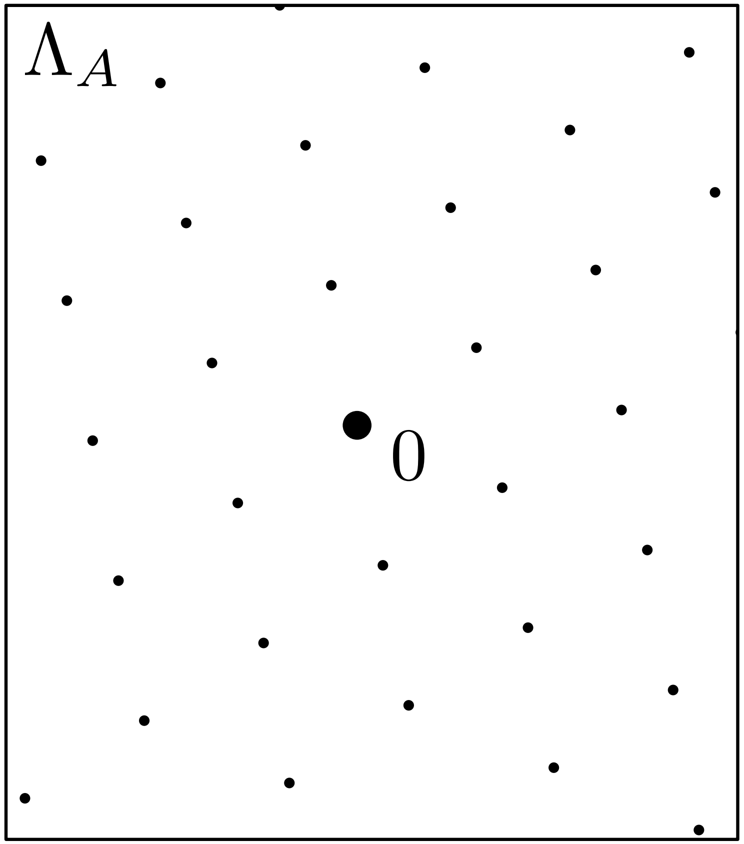
Monte Carlo algorithm,
$O(n^{(\lfloor d/2 \rfloor +1)/2} \log n)$ time, $O(n^{(\lfloor d/2 \rfloor +1)/2})$ space

[Akutsu 1998, improvement due to J. Matoušek, personal communication]

Rational Inputs

Consider the *lattice* spanned by the points $A = \{a_1, \dots, a_n\}$:

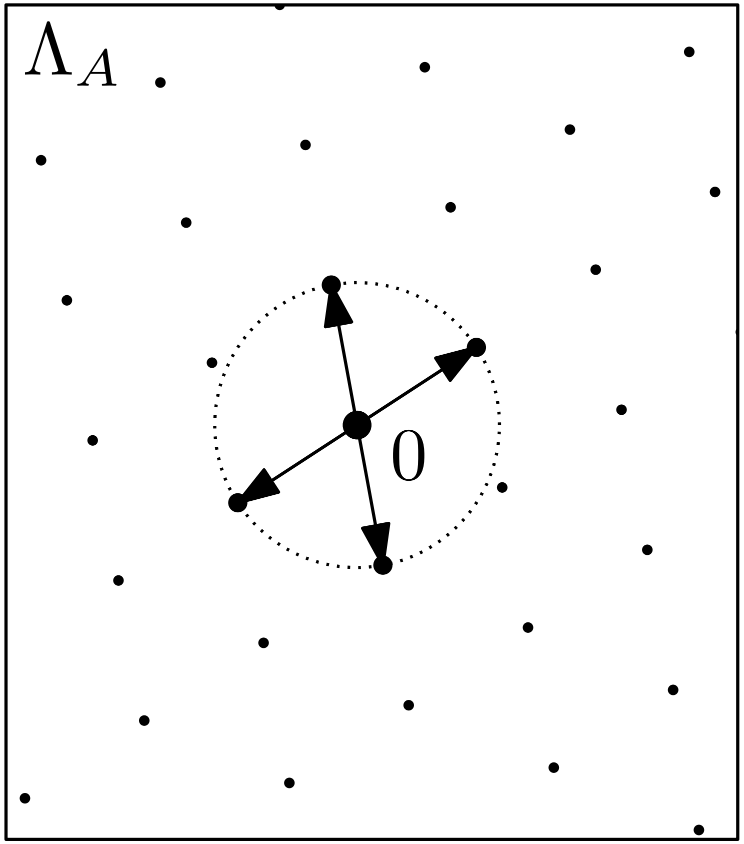
$$\Lambda_A := \{\, z_1 a_1 + \dots + z_n a_n \mid z_i \in \mathbb{Z} \,\}$$



Rational Inputs

Consider the *lattice* spanned by the points $A = \{a_1, \ldots, a_n\}$:

$$\Lambda_A := \{\, z_1 a_1 + \cdots + z_n a_n \mid z_i \in \mathbb{Z} \,\}$$



Shortest vectors in Λ_A must be mapped to shortest vectors in Λ_B.
$\rightarrow$ at most 6 choices.

Integer coordinates with L bits: $O(n \log L + n \log n)$ arithmetic operations

In d dimensions:
– at most $K_d \le 3^d$ shortest vectors
– at most $\binom{3^d}{d}$ choices of a basis

"Geometric graph isomorphism" [Arvind, Rattan 2016]

Related: Unimodular Transformations

$A, B \subset \mathbb{Z}^d$, integer coordinates with L bits

Unimodular transformations:
Integer matrix T (not necessarily orthogonal)
with determinant ± 1, such that $TA = B$

Applications in algebra

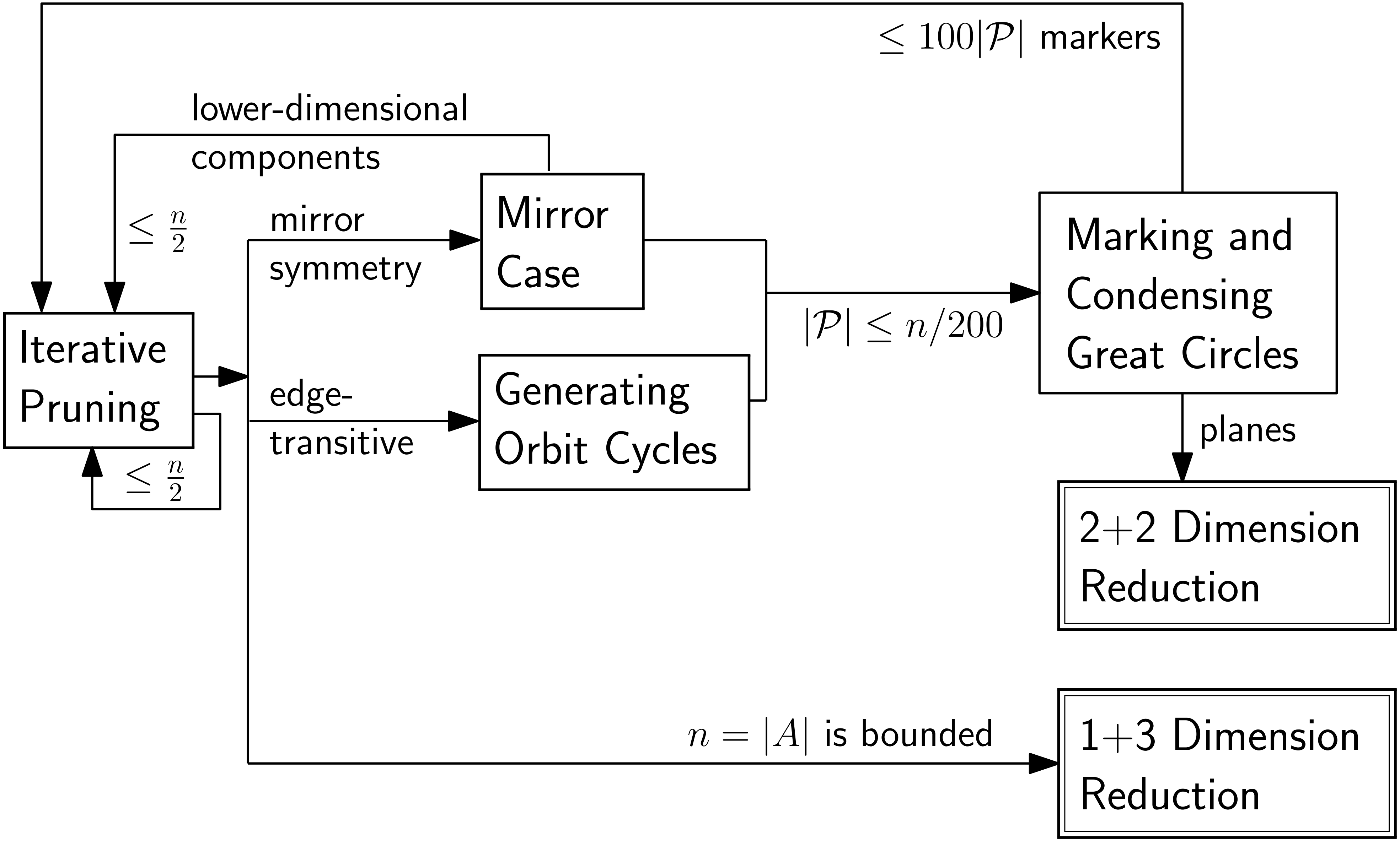
Runtime: $O(F_d \cdot n \log^2 n \cdot L)$ arithmetic operations
[Paolini, DCG 2017]

Fixed-parameter tractable (FPT)

4 Dimensions: Algorithm Overview

Freie Universität Berlin

joint work with Heuna Kim



$\leq 100|\mathcal{P}|$ markers

lower-dimensional components

$\leq \frac{n}{2}$

mirror symmetry

Mirror Case

Marking and Condensing Great Circles

Iterative Pruning

$|\mathcal{P}| \leq n/200$

edge-transitive

Generating Orbit Cycles

planes

$\leq \frac{n}{2}$

2+2 Dimension Reduction

$n = |A|$ is bounded

1+3 Dimension Reduction