Distinct distances on algebraic curves

Frank de Zeeuw – EPFL

IPAM Workshop I:
Combinatorial geometry problems at the algebraic interface

March 27, 2014
**SSS** - Micha Sharir, Adam Sheffer, and József Solymosi, 
*Distinct distances on two lines*, 

**PZ** - János Pach and Frank de Zeeuw, 
*Distinct distances on algebraic curves in the plane*, 

**VZ** - Claudiu Valculescu and Frank de Zeeuw, 
*Distinct pinned triangle areas on algebraic curves*, 
Background

- **Elekes-Rónyai** (2000): Given two sets of \(n\) points on two lines in \(\mathbb{R}^2\), the number of distinct distances between the sets is superlinear, unless the lines are parallel or orthogonal. 
  (Corollary of a more general theorem about polynomials, improved by Raz-Sharir-Solymosi in 2014.)

- **Elekes** (1999): The number of distances is \(\Omega(n^{5/4})\), unless the two lines are parallel or orthogonal.

- **Conjecture**: \(\Omega(n^{2-\epsilon})\)
Distances between two algebraic curves

**Theorem (Sharir-Sheffer-Solymosi, 2013)**

*Given two n-point sets on two lines in \( \mathbb{R}^2 \), the number of distances between them is \( \Omega(n^{4/3}) \), unless the lines are parallel or orthogonal.*

- \( cn \) distances on parallel lines:
- \( cn \) distances on orthogonal lines:

**Theorem (Pach-De Zeeuw, 2013)**

*Given two n-point sets on two irreducible algebraic curves of degree \( d \) in \( \mathbb{R}^2 \), there are \( \Omega_d(n^{4/3}) \) distances between them, unless the curves are parallel lines, orthogonal lines, or concentric circles.*

- \( cn \) on concentric circles:
Theorem (Charalambides, July 2013)

Given $n$ points on an irreducible algebraic curve of degree $d$ in $\mathbb{R}^2$, there are $\Omega_d(n^{5/4})$ distinct distances, unless it is a line or a circle.

Charalambides used the approach of Elekes’s 1999 paper, with some algebraic geometry, analysis, and rigidity theory.

Theorem (PZ, August 2013)

Given $n$ points on an irreducible algebraic curve of degree $d$ in $\mathbb{R}^2$, there are $\Omega_d(n^{4/3})$ distinct distances, unless it is a line or a circle.

Charalambides proved his bound in any dimension, with the exceptional curves being “algebraic helices” like

$$\gamma(t) = (\cos(\lambda_1 t), \sin(\lambda_1 t), \cos(\lambda_2 t), \sin(\lambda_2 t)), \quad \lambda_i \in \mathbb{Q} \cdot \pi.$$
Motivation

**Theorem (PZ)**

*Given $n$ points on an irreducible algebraic curve of degree $d$ in $\mathbb{R}^2$, there are $\geq c_d n^{4/3}$ distances, unless it is contains a line or circle.*

**Interpolation:** Given any $n$ points in $\mathbb{R}^2$, there is a curve of degree $c \sqrt{n}$ passing through them.

Suppose we lived in a fantasy world where we could prove the above with $c_d = d^{-2/3}$. Then it would follow that a set with $o(n)$ distinct distances would have to have many points on lines or circles. That sounds like a grid...

Back to the real world. In the current proof we have $c_d = d^{-11}$. It seems that the best we could do with this setup is $d^{-4/3}$. 
Main open problems

- Improve the exponent $4/3$.

- Extend to curves in **higher dimensions**.

- Extend to **general polynomials** $F: \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$: For $S \subset C$ we should have
  $$|F(S, S)| = \Omega_{\deg(C), \deg(F)} \left(|S|^{4/3}\right),$$
  unless $C$ is special or $F$ is special.

- Extend to functions with **more variables**, like distinct areas of triangles determined by triples of points on a curve.

- Extend to **“implicit functions”**: e.g., show that if $n$ points on a curve span $\Omega(n^{2-\alpha})$ triple lines, then it must be a cubic curve (done for small $\alpha$ by Elekes-Szabó). Or with unit area triangles.
For \( p, q \in \mathbb{R}^2 \), let \( F(p, q) = y_px_q - x_py_q \). Then \( |F(p, q)|/2 \) is the area of the triangle spanned by \( p, q, \) and the origin.

Theorem (Iosevich-Roche-Newton-Rudnev, 2011)

A set of \( n \) points in \( \mathbb{R}^2 \) determines \( \Omega(n/\log(n)) \) distinct values of \( F \), unless the points lie on a line (through the origin).
Pinned triangle areas on curves

Theorem (Charalambides, 2013)

Given $n$ points on an irreducible algebraic curve of degree $d$ in $\mathbb{R}^2$, there are $\Omega_d(n^{5/4})$ distinct values of $F$, unless the curve is a line, ellipse centred at the origin, or hyperbola centred at the origin.

Theorem (Valculescu-De Zeeuw, 2014)

Given $n$ points on an irreducible algebraic curve of degree $d$ in $\mathbb{R}^2$, there are $\Omega_d(n^{4/3})$ distinct values of $F$, unless the curve is a line, ellipse centred at the origin, or hyperbola centred at the origin.
Proof of SSS

Recall:

**Theorem (Sharir-Sheffer-Solymosi, 2013)**

*Given two lines in $\mathbb{R}^2$ with $n$ points each, the number of distances is $|D| = \Omega(n^{4/3})$, unless the two lines are parallel or orthogonal.*

We have $S_1 \subset l_1$, $S_2 \subset l_2$, $|S_1| = |S_2| = n$.

We count the quadruples

$$Q = \{(p, p', q, q') \in S_1^2 \times S_2^2 : d(p, q) = d(p', q')\}.$$

Then

$$\frac{n^4}{|D|} \leq |Q| \preceq cn^{8/3} \implies |D| = \Omega(n^{4/3}).$$

The lower bound for $|Q|$ is easy with Cauchy-Schwarz; the upper bound is all the work. The main tool is Pach-Sharir.
Proof of SSS

For \( p_i, p_j \in S_1 \) define an algebraic curve in \( \mathbb{R}^4 \) by

\[
\gamma_{ij} = \left\{ (q, q') \in l_2 \times l_2 : d(p_i, q) = d(p_j, q') \right\},
\]

which is actually a hyperbola on a fixed plane. We have \( n^2 \) curves in

\[
\Gamma = \{ \gamma_{ij} : p_i, p_j \in S_1 \}
\]

and \( n^2 \) points in

\[
P = \{ (q_s, q_t) : q_s, q_t \in S_2 \}.
\]

Then

\[
|Q| = I(P, \Gamma) = |\{(p, \gamma) \in P \times \Gamma : p \in \gamma\}|.
\]
Theorem (Pach-Sharir, 1992)

Given $P \subset \mathbb{R}^D$ and $\Gamma$ a set of algebraic curves in $\mathbb{R}^D$ with two degrees of freedom:

- any $\gamma, \gamma' \in \Gamma$ intersect in at most $s$ points of $P$,
- any $p, p' \in P$ belong to at most $s$ curves of $\Gamma$.

Then

$$I(P, \Gamma) = O_s \left( |P|^{2/3} |\Gamma|^{2/3} + |P| + |\Gamma| \right).$$
Proof of SSS

Our $P, \Gamma$ have two degrees of freedom:

• Because the lines are not parallel or orthogonal, the curves are distinct and irreducible, so $|\gamma_{ij} \cap \gamma_{kl}| \leq 4$ by Bézout. (Write out the equation: reducible $\Rightarrow$ parallel, non-distinct $\Rightarrow$ orthogonal)

• Define “dual” curves for $q_s, q_t \in S_2$:

$$\tilde{\gamma}_{st} = \{(p, p') \in l_1 \times l_1 : d(p, q_s) = d(p', q_t)\}.$$  

Then $|\tilde{\gamma}_{st} \cap \tilde{\gamma}_{uv}| \leq 4$ means $(q_s, q_t), (q_u, q_v)$ belong to $\leq 4 \gamma_{ij} \in \Gamma$.

So:

$$I(P, \Gamma) = O \left( (n^2)^{2/3} (n^2)^{2/3} \right) = O \left( n^{8/3} \right).$$

Done.
Recall $F(p, q) = y_p x_q - x_p y_q$.

**Theorem (VZ, 2014)**

*If $S$ is contained in an irreducible algebraic curve $C$ of degree $d$ in $\mathbb{R}^2$, then $|F(S, S)| = \Omega_d(|S|^{4/3})$, unless $C$ is a line, ellipse centred at the origin, or hyperbola centred at the origin.*

**Preparation:** We first prepare $S$ so that it contains at most one point on any line through the origin. This is possible by removing at most $d - 1$ points of $S$ per line, leaving $\geq |S|/d$ points. This does not affect the bound. The reason is that now, for distinct $p_i, p_k$,

$$F(p_i, q) = 0, \quad F(p_k, q) = 0$$

are independent linear equations.
Proof of VZ

We surprise everyone by bounding the quadruples

$$Q = \{(p, p', q, q') \in S^4 : F(p, q) = F(p', q')\}$$

by

$$\frac{n^4}{|F(S, S)|} \leq |Q| = I(P, \Gamma) \leq cn^{8/3} \Rightarrow |F(S, S)| = \Omega(n^{4/3});$$

for the upper bound on $|Q|$ we will define points $P$ and curves $\Gamma$, and show that they have two degrees of freedom.
Proof of VZ

For \( p_i, p_j \in S \) define an algebraic curve in \( \mathbb{R}^4 \):

\[
C_{ij} = \{(q, q') \in C \times C : F(p_i, q) = F(p_j, q')\}.
\]

We have \( n^2 \) curves in \( \Gamma = \{\gamma_{ij} : p_i, p_j \in S\} \) and \( n^2 \) points in \( P = \{(q_s, q_t) : q_s, q_t \in S\} \). Define “dual” curves

\[
\tilde{C}_{st} = \{(p, p') \in C \times C : F(p, q_s) = F(p', q_t)\}.
\]

Finally, define “bad sets”

\[
\Gamma_0 = \{C_{ij} \in \Gamma : \exists C_{kl} \text{ such that } |C_{ij} \cap C_{kl}| = \infty\},
\]

\[
P_0 = \{(q_s, q_t) \in P : \exists \tilde{C}_{uv} \text{ such that } |\tilde{C}_{st} \cap \tilde{C}_{uv}| = \infty\},
\]

and \( \Gamma_1 = \Gamma \setminus \Gamma_0, P_1 = P \setminus P_0 \).
Proof of VZ

Lemma

If \( C_{ij}, C_{kl} \in \Gamma_1 \), then \( |C_{ij} \cap C_{kl}| = O_d(1) \).

Any two points in \( P_1 \) belong to \( O_d(1) \) curves in \( \Gamma \).

Proof.

We want to bound the number of real solutions \((q, q')\) of

\[
 f(q) = 0, \quad f(q') = 0, \quad F(p_i, q) = F(p_j, q'), \quad F(p_k, q) = F(p_l, q'),
\]

where \( f \) is the polynomial defining \( C \). Pick your method:

- Oleinik-Petrovski-Milnor-Thom;
- Move to \( \mathbb{C} \) and use complex Bézout;
- Last two equations define a plane, apply real planar Bézout there.

Do the same for the dual curves.

So \( P_1, \Gamma_1 \) have two degrees of freedom and \( I(P_1, \Gamma_1) = O_d(n^{8/3}) \).
Proof of VZ

Now the bad sets $\Gamma_0, P_0$.
For linear $T : \mathbb{R}^2 \to \mathbb{R}^2$, set $G_T = \{(q, q') \in C \times C : T(q) = q'\}$.

Lemma

For any $C_{ij}, C_{kl} \in \Gamma$ we have $C_{ij} \cap C_{kl} = G_T$ for some linear $T$.
If $|G_T| = |C_{ij} \cap C_{kl}| = \infty$, then $T$ is an automorphism of $C$.

Proof.

If $(q, q') \in C_{ij} \cap C_{kl}$ then since $F(p_i, q) = y_{p_i}x_q - x_{p_i}y_q$ we have

$$M_{ik}q = M_{jl}q' \text{ with } M_{ik} = \begin{pmatrix} y_{p_i} & -x_{p_i} \\ y_{p_k} & -x_{p_k} \end{pmatrix}, \quad M_{jl} = \begin{pmatrix} y_{p_j} & -x_{p_j} \\ y_{p_l} & -x_{p_l} \end{pmatrix}.$$  

The matrices are invertible thanks to the preparation of $S$. So $q' = M_{jl}^{-1}M_{ik}q =: T(q)$. Also vice versa.

If $|G_T| = \infty$, then $|T(C) \cap C| = \infty$, so $T(C) = C$. 


Proof of VZ

Lemma

\[ I(P, \Gamma_0) = O_d(n^2), \quad I(P_0, \Gamma) = O_d(n^2). \]

Proof.

By the Automorphism Lemma below, \( C \) has \( \leq 4d \) linear automorphisms, unless it is a special curve. It is not hard to see that each automorphism occurs \( \leq n \) times. So \( |\Gamma_0| \leq 4dn \) and the lemma follows easily.

This finishes the proof:

\[ I(P, \Gamma) \leq I(P_0, \Gamma) + I(P, \Gamma_0) + I(P_1, \Gamma_1) = O_d \left( n^{8/3} \right). \]
Automorphism Lemma

**Lemma**

An irreducible algebraic curve of degree \( d \) has \( \leq 4d \) linear automorphisms, unless it is a line or linearly equivalent to one of:

<table>
<thead>
<tr>
<th>Type</th>
<th>Equation</th>
<th>Matrix</th>
</tr>
</thead>
</table>
| **Ellipses**       | \( x^2 + y^2 = 1 \) | \[
\begin{pmatrix}
\frac{a}{\sqrt{1-a^2}} & -\sqrt{1-a^2} \\
\frac{\sqrt{1-a^2}}{a} & a
\end{pmatrix}
\] |
| **Hyperbolas**     | \( xy = 1 \)       | \[
\begin{pmatrix}
a & 0 \\
0 & a^{-1}
\end{pmatrix}
\] |
| **Parabolas**      | \( x = y^2 \)      | \[
\begin{pmatrix}
a^2 & 0 \\
0 & a
\end{pmatrix}
\] |
| “Pseudohyperbolas” | \( x^p y^q = 1 \)  | \[
\begin{pmatrix}
a^q & 0 \\
0 & a^{-p}
\end{pmatrix}
\] |
| “Pseudocusps”      | \( x^p = y^q \)    | \[
\begin{pmatrix}
a^q & 0 \\
0 & a^p
\end{pmatrix}
\] |

Calculation shows that the last three cannot occur for our \( F \). \( \square \)
About the Automorphism Lemma

Of course, something much stronger has long been known:

**Theorem (Hurwitz, 1893)**

A nonsingular curve of genus $g \geq 2$ has at most $84(g - 1)$ polynomial automorphisms.

But this does not give the detailed information that we need. In particular, it does not apply to singular curves, which is a problem if we want to do interpolation.
About the Automorphism Lemma

Idea of our proof of the Automorphism Lemma:

*Most algebraic curves cannot contain an infinite orbit \( \{ T^{(k)}(p) \} \).*

E.g., let \( C : f(x, y) = \sum a_{ij}x^iy^j \) and \( T = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \lambda, \mu \in \mathbb{R}_{>0}. \)

Then, if \( p = (x_0, y_0) \) and \( T^{(k)}(p) \in C \), we would have

\[
0 = f(\lambda^k x_0, \mu^k y_0) = \sum (a_{ij}x_0^iy_0^j) e^{(\ln(\lambda)i + \ln(\mu)j)k} = \sum b_{ij}e^{c_{ij}k}.
\]

Such a function has only finitely many roots \( k \) (unless...).

We do this for each Jordan form, and we get exactly the exceptions in the lemma.
Proof sketch of PZ

As above but with $F(p, q) = (x_p - x_q)^2 + (y_p - y_q)^2$.
If $(q, q') \in C_{ij} \cap C_{kl}$, then

Suppose $F(p_i, p_k) = F(p_j, p_l)$ (other case is annoying...).
$\Rightarrow \exists$ isometry $T$ so that $T(p_i) = p_k, T(p_j) = p_l \Rightarrow T(q) = q'$ (...)

Then $|C_{ij} \cap C_{kl}| = \infty \Rightarrow |T(C) \cap C| = \infty \Rightarrow T(C) = C$.

**Lemma (Isometry Lemma)**

An irreducible algebraic curve of degree $d$ has at most $4d$ isometries, unless it is a line or a circle.
Main references (in order of appearance)