Points, lines and polynomial identities

Amir Shpilka
Tel Aviv University
Outline

• **Points and lines**: Sylvester-Gallai theorem and relatives

• **Applications**:
  • Locally correctable codes
  • Algebraic identity testing (aka polynomial identity testing)

• **Higher degree analog**

• **Proof sketch**
Point-line incidences

Main theme: Given a collection of points and lines satisfying certain properties, bound some combinatorial measure (number of incidences, number of lines, number of points,...)

Many results and conjectures: Szemeredi-Trotter, Guth-Katz (Erdös distinct distance problem), Kakeya,...

This talk: Sylvester-Gallai theorem and relatives
Sylvester-Gallai theorem

Conjectured by Sylvester'93 and Erdös'43, proved by Melchior'41 and Gallai'44:

• A finite set of points $P \subseteq \mathbb{R}^2$
• Any line through any two points in $P$ meets a 3$\text{rd}$ point in $P$ (special line)

$\Rightarrow$ Points are colinear ($\dim(\text{affine-span } P) = 1$)
Proof

Let $p$ and $\ell$ be the closest point-line pair (line that passes through at least 3 points)

Important: $P$ finite (otherwise $P=\mathbb{R}^2$), over $\mathbb{R}$

Same proof for $P \subseteq \mathbb{R}^n$
Some important relatives

[**Kelly'86**]: Over $\mathbb{C}$, same condition $\implies \dim(\text{affine-span } P) \leq 2$

[**Edelstein-Kelly'66**]: Colorful version: $P = R \sqcup G \sqcup B$
   Every non-monochromatic line contains all 3 colors
   $\implies \dim(\text{affine-span } P) \leq 3$

[**Barak-Dvir-Wigderson-Yehudayoff'11, Dvir-Saraf-Wigderson'12**]:
Robust version:
   Special lines through every $p \in P$ cover $\delta$-fraction of $P$
   $\implies \dim(\text{affine-span } P) \leq O(1/\delta)$
Algebraic/Dual rephrasing

Finite set of homogeneous linear equations: 
\{L_1(x_1,\ldots,x_n),\ldots,L_m(x_1,\ldots,x_n)\} \subseteq \mathbb{R}[x_1,\ldots,x_n]

Any solution to any two equations also solves a 3rd equation 
\implies \dim(\text{span}\{L_i\}) \leq 2 \ (\text{over } \mathbb{C}: \dim(\text{span}\{L_i\}) \leq 3)

Reduction:
Linear equation L: \langle v, x \rangle = 0 \iff \text{span}\{v\} \text{ in } \mathbb{R}^n
H a hyperplane in general position
point corresponding to L : \text{p}_L = \text{span}\{v\} \cap H
L_3 \in \text{span}(L_1,L_2) \iff \text{p}_1,\text{p}_2,\text{p}_3 \text{ colinear}
Applications

[Dvir-S'05]: SG-type theorem relevant for:
• Locally Correctable Codes (LCCs)
• Polynomial Identity Testing (PIT) of depth-3 circuits

[Beecken-Mittmann-Saxena'13, Gupta'14]:
Higher degree version of SG type theorems relevant for PIT of depth-4 circuits
Error correcting codes

- Many applications in practice (communication, storage) and theory (PCP, crypto,...)
- Typical goals: minimize overhead (i.e. higher rate $|x|/|\text{Enc}(x)|$), decoding from a large fraction of errors (higher $\delta$), efficient decoding
Locally correctable codes

- **Locality**: super efficient local correction. Is it achievable?
- **Assume**: $\text{Enc}$ is a linear map $\text{Enc}(x)_i = L_i(x)$
- If $L_i$ can be recovered from $L_j, L_k$ then they satisfy the SG property
- High probability decoding $\implies$ many colinear triplets
- (robust) SG theorem $\implies$ $\text{Dim} (\text{span} L_i) =$ small $\implies$ Rate is zero

Diagram:
- Message $x$ passed to encoder $\text{Enc}(x)$
- Noisy channel
- $\delta n$ errors
- Decoded using $q=2$ queries with high probability
Polynomial identity testing (PIT)

Model: algebraic circuits (computations using +,×)
Challenge: Given algebraic circuit C decide C(x)=0?
Efficient Randomized algorithm [Schwartz'80, Zippel'79, DeMillo-Lipton’78]
Goal: A proof. I.e., a deterministic algorithm
Motivation:
• Primality testing [Agrawal-Kayal-Saxena'02]
• Parallel algorithms for finding perfect matching [Karp-Upfal-Wigderson'85, Mulmuley-Vazirani-Vazirani'87]
• Efficient deterministic algorithms implies lower bounds [Kabanets-Impagliazzo'03]
Identity testing of depth-3 algebraic circuits

Example: Let $\omega^d=1$ is the following true:

$$
\prod_{i=1 \ldots d}(3\omega^5X+(2\omega^5-5\omega^i)Y-6\omega^iZ) + \\
\prod_{i=1 \ldots d}(-2\omega^iX+(3\omega^i+5)Y+(6-5\omega^i)Z) + \\
\prod_{i=1 \ldots d}((2\omega^{2}-3\omega^i)X-(3\omega^i+2\omega^i)Y+5\omega^2Z) =? 0
$$

Solution: Let

$U= 3X+2Y$

$V=5X+6Z$

$W=2X-3Y+5Z$

After simple manipulation:

$$
\prod(U-\omega^iV) + \prod(V-\omega^iW) + \prod(W-\omega^iU) = (U^d-V^d) + (V^d-W^d) + (W^d-U^d) = 0
$$
Identity testing of $\Sigma \prod \Sigma$ circuits

Let $A = \prod a_i$, $B = \prod b_i$, $C = \prod c_i$, $a_i, b_i, c_i \in \mathbb{R}[x_1, \ldots, x_n]$ linear forms

Decide whether $A + B + C = 0$

First nontrivial case ($A + B = 0$ verified by unique factorization)

[Dvir-S'05]: If we set $a_i = b_j = 0$ then $\exists k$ such that $c_k = 0$, can use colorful SG

[Kayal-Saraf'09]: If $A + B + \ldots + M = 0$ then (morally) $\dim(\{a_i\}, \{b_i\}, \ldots, \{m_i\}) = m^{O(m)}$

PIT algorithm: Find basis, expand and verify identity in $O(1)$ variables

[Saxena-Seshadhri'11]: BB-PIT for $m$ summands in $n^{O(m)}$ time (any field)

[Gupta-Kamath-Kayal-Saptharishi'13]: PIT for $\Sigma \prod \Sigma$ (unbounded degree) $\implies$ PIT for general circuits
Identity testing of $\sum^{[3]}\prod\prod\prod$ circuits

Let $A=\prod a_i$, $B=\prod b_i$, $C=\prod c_i$, $a_i,b_i,c_i \in \mathbb{R}[x_1,\ldots,x_n]$ degree d polynomials
Decide whether $A+B+C=0$

Theorem [Agrawal-Vinay '08]: PIT for homogeneous depth-4 $\Rightarrow$ PIT for general circuits

Conjecture [Beecken-Mittmann-Saxena '13, Gupta '14]:
If $A+B+C=0$ disjoint then algebraic-rank($\{a_i\},\{b_i\},\{c_i\}$)=O(1)

Intuition: If we set $a_i=b_j=0$ then there is some $k$ such that $c_k=0$.
Need degree d Edelstein-Kelly theorem (colorful degree d SG)

Example: $a=xy+zw$, $b=xy-zw$, $c_1 \cdot c_2 \cdot c_3 \cdot c_4 = (x+z)(x+w)(y+z)(y+w)$
Problem: Product vanishes when $a=b=0$ but not always the same $c_k$
Our results
Higher degree SG type theorems

$A=\{a_i\}$ quadratic polynomials

- For every $a_i,a_j$ there is $a_k$ that vanishes whenever $a_i$ and $a_j$ do
  
  \[ S'19 \Rightarrow \dim(\{a_i\})=O(1) \]

  if $A=\mathbb{R} \cup G \cup B$ ...

  \[ \Rightarrow \dim(\{a_i\})=O(1) \]

- For every $a_i,a_j$ whenever $a_i$ and $a_j$ vanish then so does $\prod_{k \neq i,j} a_k$
  
  \[ Peleg-S'20 \Rightarrow \dim(\{a_i\})=O(1) \]

- $A=\prod a_i$, $B=\prod b_i$, $C=\prod c_i$, quadratic polynomials

  \[ Peleg-S'21 \] If $A+B+C=0$ disjoint (wlog) then $\dim(\{a_i\},\{b_i\},\{c_i\})=O(1)$
  
  (via colorful version of $Peleg-S'20$)

Answers $[Beecken-Mittmann-Saxena'13, Gupta'14]$ for degree $d=2$
Proof ingredients
Main tool I: Algebraic Structure Theorem

Theorem [S'19, Peleg-S'20]: \( Q_1, Q_2, \{P_i\} \) quadratics s.t. \( Q_1(v) = Q_2(v) = 0 \implies \prod P_i(v) = 0 \)

Then one of the following cases must hold:

1. Some \( P_i \) is in the linear span of \( Q_1, Q_2 \)
2. \( \exists \) linear functions \( \ell_1, \ell_2 \) s.t. \( \ell_1 \ell_2 \in \text{span}\{Q_1, Q_2\} \)
3. \( \exists \) linear functions \( \ell_1, \ell_2 \) s.t. \( Q_1 = Q_2 = 0 \mod \ell_1, \ell_2 \)

Examples:

2. \( Q_2 = Q_1 + \ell \ell', P_1 = (Q_1 + \ell \ell_1) P_2 = (Q_1 + \ell' \ell_2) \)
3. \( Q_1 = xa+yb, Q_2=xc+yd, P_1 = (ad-bc), P_2 = x, P_3 = y \)

Proof idea: Analyzing how the resultant of \( Q_1, Q_2 \) factorizes
Different cases roughly correspond to different degrees of factors
Main tool II: Robust version of E-K theorem

Recall [Edelstein-Kelly'66]: Colorful version: $P = R \cup G \cup B$
Every non-monochromatic line contains all 3 colors
$\implies \dim(\text{affine-span } P) \leq 3$

Robust-EK-Thm [S'19]: $P = R \cup G \cup B$ s.t. every point in one set spans with a $\delta$-fraction of points in the other two sets a point in the third set
$\implies \dim(\text{affine-span } P) = O(1/\delta^3)$

Remark: probably not tight
(rough) Proof outline of [S'19, Peleg-S'20, Peleg-S'21]

Use the algebraic structure theorem to argue that either

- Coefficient vectors of quadratic polynomials satisfy the robust-SG/EK theorem (and we are done), or
- Each quadratic is a function of a few linear functions
  - Then show that these linear functions satisfy the conditions of the robust-SG/EK theorem themselves

**Intuition**: If (vector of coefficients of) a polynomial Q is on many special lines, then Q has a very restricted structure

**Actual proofs**: A lot of case analysis
Follow up and related work

SG:
• [de Oliveira-Sengupta'22]: SG for cubic polynomials (for every two cubics there exists a third...) by extension of structure theorem to cubics
• [Peleg-S'22, Garg-de Oliveira-Sengupta'22]: Robust Quadratic-SG theorem (for every $Q_i$, for $\delta$-fraction of $Q_j$, there exists a $Q_k$...)

PIT:
• [Limaye-Srinivasan-Tavenas'21]: $n^{\epsilon}$ PIT for bounded depth circuits
• [Dutta-Dwivedi-Saxena'21]: Quasi-polynomial time BB PIT for $\Sigma^{[O(1)]} \Pi \Sigma \Pi^{[\log(n)^{O(1)}]}$ using a different techniques
Conclusion

Saw applications of problems in discrete geometry in
• Locally correctable codes
• Verifying algebraic identities

Saw generalization to algebra-geometric questions that are also relevant for identity testing

Many open questions – higher degrees, more sets,...

Thank You!