Sylvester-Gallai Configurations and Algebraic Complexity

Rafael Oliveira
University of Waterloo

Akash Kumar Sengupta
Columbia University

IIT Kanpur
March 2023

Overview

- Introduction
  - Sylvester-Gallai Configurations
  - Previous (and current) Work
- Our Results
  - Radical Sylvester-Gallai Theorem for Cubics
  - Our Tools
  - Complete proof overview
- Conclusion & Open Problems
- Extra: SG generalization for PIT and LCCs
- Proof of Structure Theorem

(Very brief) History

[Sylvester 1893]: given a finite set of points $\mathcal{F} \subset \mathbb{R}^N$ such that:

- any line containing two points of $\mathcal{F}$ must pass through a third.

Must $\mathcal{F}$ be contained in a line?

(Very brief) History

[Sylvester 1893]: given a finite set of points $\mathcal{F} \subset \mathbb{R}^N$ such that:

- any line containing two points of $\mathcal{F}$ must pass through a third.

Must $\mathcal{F}$ be contained in a line?

[Melchior 1940, Gallai 1944]: YES.

(Very brief) History

[Sylvester 1893]: given a finite set of points $\mathcal{F} \subset \mathbb{R}^N$ such that:

- any line containing two points of $\mathcal{F}$ must pass through a third.

Must $\mathcal{F}$ be contained in a line?

[Melchior 1940, Gallai 1944]: YES.

Problem depends on base field.
[Folklore]: over $\mathbb{C}$, torsion points of elliptic curves give 2-dimensional configurations.

[Serre 1966]: given a finite set of points $\mathcal{F} \subset \mathbb{C}^N$ such that:

- any line containing two points of $\mathcal{F}$ must pass through a third.

Must $\mathcal{F}$ be contained in a complex plane?

(Very brief) History

[Sylvester 1893]: given a finite set of points $\mathcal{F} \subset \mathbb{R}^N$ such that:

- any line containing two points of $\mathcal{F}$ must pass through a third.

Must $\mathcal{F}$ be contained in a line?

[Melchior 1940, Gallai 1944]: YES.

Problem depends on base field.
[Folklore]: over $\mathbb{C}$, torsion points of elliptic curves give 2-dimensional configurations.

[Serre 1966]: given a finite set of points $\mathcal{F} \subset \mathbb{C}^N$ such that:

- any line containing two points of $\mathcal{F}$ must pass through a third.

Must $\mathcal{F}$ be contained in a complex plane?

[Hirzebruch 1983] YES, using deep results from AG.

TCS History

Several variations and generalizations.

TCS History

Several variations and generalizations.

- Coloured versions
  - PIT **[Dvir Shpilka 2007]** (conjectured coloured version)

TCS History

Several variations and generalizations.

- Coloured versions
  - PIT **[Dvir Shpilka 2007]** (conjectured coloured version)
- Higher-dimensional analogs:
  - PIT **[Kayal Saraf 2009, Saxena Seshadri 2013]**

TCS History

Several variations and generalizations.

- Coloured versions
  - PIT **[Dvir Shpilka 2007]** (conjectured coloured version)
- Higher-dimensional analogs:
  - PIT **[Kayal Saraf 2009, Saxena Seshadri 2013]**
- Robust analogs:
  - Coding Theory (LCCs) **[BDWY 2011]**
  - Reconstruction (aka tensor decomposition) **[Sinha 2016]**

TCS History

Several variations and generalizations.

- Coloured versions
  - PIT **[Dvir Shpilka 2007]** (conjectured coloured version)
- Higher-dimensional analogs:
  - PIT **[Kayal Saraf 2009, Saxena Seshadri 2013]**
- Robust analogs:
  - Coding Theory (LCCs) **[BDWY 2011]**
  - Reconstruction (aka tensor decomposition) **[Sinha 2016]**
- Higher-degree analogs:
  - PIT **[Gupta 2014]**

TCS History

Several variations and generalizations.

- Coloured versions
  - PIT **[Dvir Shpilka 2007]** (conjectured coloured version)
- Higher-dimensional analogs:
  - PIT **[Kayal Saraf 2009, Saxena Seshadri 2013]**
- Robust analogs:
  - Coding Theory (LCCs) **[BDWY 2011]**
  - Reconstruction (aka tensor decomposition) **[Sinha 2016]**
- Higher-degree analogs:
  - PIT **[Gupta 2014]**

Underlying theme:

Are Sylvester-Gallai type configurations always low-dimensional?

Robust Sylvester-Gallai

Definition (Robust linear Sylvester Gallai)

$\mathcal{F} := \{v_1, \ldots, v_m\} \subset \mathbb{C}^N$ is a δ-linear-SG configuration if for all $i \in [m]$, there are $\delta(m-1)$ indices j such that:

$$\text{there is } k \neq i, j \text{ such that } v_k \in \mathrm{span}_{\mathbb{C}} \{v_i, v_j\}.$$

Robust Sylvester-Gallai

Definition (Robust linear Sylvester Gallai)

$\mathcal{F} := \{v_1, \ldots, v_m\} \subset \mathbb{C}^N$ is a δ-linear-SG configuration if for all $i \in [m]$, there are $\delta(m-1)$ indices j such that:

$$\text{there is } k \neq i, j \text{ such that } v_k \in \mathrm{span}_{\mathbb{C}} \{v_i, v_j\}.$$

Theorem (robust linear SG theorem – **[BDWY 2011]**)

If $\mathcal{F}$ is δ-linear-SG configuration, then $\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1/\delta^2)$.

Robust Sylvester-Gallai

Definition (Robust linear Sylvester Gallai)

$\mathcal{F} := \{v_1, \ldots, v_m\} \subset \mathbb{C}^N$ is a δ-linear-SG configuration if for all $i \in [m]$, there are $\delta(m-1)$ indices j such that:

$$\text{there is } k \neq i, j \text{ such that } v_k \in \text{span}_{\mathbb{C}}\{v_i, v_j\}.$$

Theorem (robust linear SG theorem – **[BDWY 2011]**)

If $\mathcal{F}$ is δ-linear-SG configuration, then $\dim \text{span}_{\mathbb{C}}\{\mathcal{F}\} = O(1/\delta^2)$.

- Improved to $O(1/\delta)$ by **[Dvir Saraf Wigderson 2014]**.

Why Should I Care?

- Mathematicians & complexity theorists:

  It's a structural study of cancellations/relations (syzygies).

Why Should I Care?

- Mathematicians & complexity theorists:

  It's a structural study of cancellations/relations (syzygies).

Cancellations in SG configurations make them quite complex!

Mayr-Meyer

[Mayr Meyer 1982]: "cancellations in algebraic geometry are EXPSPACE hard"
[Brownawell 1987, Kollar 1988]: "radical cancellations" are in PSPACE.

Where are the cancellations?

- $\mathcal{F} = \{v_1, \ldots, v_m\} \subset \mathbb{R}^2$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that v_i, v_j, v_k colinear.

Where are the cancellations?

- $\mathcal{F} = \{v_1, \ldots, v_m\} \subset \mathbb{R}^2$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that v_i, v_j, v_k colinear.

- Duality: $\mathcal{F} = \{\ell_1, \ldots, \ell_m\} \subset \mathbb{R}[x, y]_1$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that $\ell_k \in (\ell_i, \ell_j)$.

Where are the cancellations?

- $\mathcal{F} = \{v_1, \dots, v_m\} \subset \mathbb{R}^2$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that v_i, v_j, v_k colinear.

- Duality: $\mathcal{F} = \{\ell_1, \dots, \ell_m\} \subset \mathbb{R}[x, y]_1$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that $\ell_k \in (\ell_i, \ell_j)$.

  1. $\ell_k \in (\ell_i, \ell_j) \Leftrightarrow \exists \alpha_i, \alpha_j, \alpha_k \in \mathbb{R}$ such that

$$\alpha_i \ell_i + \alpha_j \ell_j + \alpha_k \ell_k = 0$$

Where are the cancellations?

- $\mathcal{F} = \{v_1, \dots, v_m\} \subset \mathbb{R}^2$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that v_i, v_j, v_k colinear.

- Duality: $\mathcal{F} = \{\ell_1, \dots, \ell_m\} \subset \mathbb{R}[x, y]_1$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that $\ell_k \in (\ell_i, \ell_j)$.

    1. $\ell_k \in (\ell_i, \ell_j) \Leftrightarrow \exists \alpha_i, \alpha_j, \alpha_k \in \mathbb{R}$ such that
    $$\alpha_i \ell_i + \alpha_j \ell_j + \alpha_k \ell_k = 0$$
    2. Are these relations enough to show that $\dim\langle\mathcal{F}\rangle = 1$?

- (Non-linear) Generalization **[Gupta 2014]**:
    - $\mathcal{F} = \{F_1, \dots, F_m\} \subset \mathbb{C}[x_1, \dots, x_N]$ is a SG configuration if for all $i, j \in [m]$, there is $k \neq i, j$ such that
    $$F_k \in \mathrm{rad}(F_i, F_j)$$

Generalization – geometrically

General conjecture

Definition (Radical Sylvester Gallai – [Gupta 2014])

$\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{C}[x_1, \ldots, x_N]$ is a d-radical-SG config. if:

1. F_i irreducible for all $i \in [m]$
2. $\deg(F_i) \leq d$ for all $i \in [m]$ (low degree)
3. $F_i \notin (F_j)$ for $i \neq j$ ("distinct")
4. for all i, j, there is $k \neq i, j$ such that (SG dependency)

$$F_k \in \mathrm{rad}(F_i, F_j)$$

General conjecture

Definition (Radical Sylvester Gallai – **[Gupta 2014]**)

$\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{C}[x_1, \ldots, x_N]$ is a d-radical-SG config. if:

1. F_i irreducible for all $i \in [m]$
2. $\deg(F_i) \leq d$ for all $i \in [m]$ (low degree)
3. $F_i \notin (F_j)$ for $i \neq j$ ("distinct")
4. for all i, j, there is $k \neq i, j$ such that (SG dependency)

$$F_k \in \mathrm{rad}(F_i, F_j)$$

Conjecture (**[Gupta 2014]**)

There is $\lambda : \mathbb{N} \to \mathbb{N}$ *s.t. if* $\mathcal{F}$ *is a* d-radical-SG *configuration, then*

$$\text{tr-deg}(\mathcal{F}) \leq \lambda(d).$$

Informally: must every SG configuration be in "few variables"?

General conjecture

Definition (Radical Sylvester Gallai – [Gupta 2014])

$\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{C}[x_1, \ldots, x_N]$ is a d-radical-SG config. if:

1. F_i irreducible for all $i \in [m]$
2. $\deg(F_i) \leq d$ for all $i \in [m]$ (low degree)
3. $F_i \notin (F_j)$ for $i \neq j$ ("distinct")
4. for all i, j, there is $k \neq i, j$ such that (SG dependency)

$$F_k \in \mathrm{rad}(F_i, F_j)$$

Conjecture

There is $\lambda : \mathbb{N} \to \mathbb{N}$ *s.t. if* $\mathcal{F}$ *is a* d-radical-SG *configuration, then*

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq \lambda(d).$$

Previous (and current) Works

Theorem (Linear SG – **[Hirzebruch 1983]**)

If $\mathcal{F}$ is 1-radical-SG *configuration, then* $\dim \text{span}_{\mathbb{C}} \{\mathcal{F}\} \leq 2$.

Another proof given by **[Dvir Saraf Wigderson 2014]**

Previous (and current) Works

Theorem (Linear SG – [Hirzebruch 1983])

If $\mathcal{F}$ is 1-radical-SG *configuration, then* $\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} \leq 2$.

Another proof given by **[Dvir Saraf Wigderson 2014]**

Theorem (Quadratic radical SG theorem – [Shpilka 2020])

If $\mathcal{F}$ is 2-radical-SG *configuration, then* $\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Previous (and current) Works

Theorem (Linear SG – **[Hirzebruch 1983]**)

If $\mathcal{F}$ *is* 1-radical-SG *configuration, then* $\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} \leq 2$*.*

Another proof given by **[Dvir Saraf Wigderson 2014]**

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ *is* 2-radical-SG *configuration, then* $\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$*.*

Theorem (Cubic radical SG theorem – **[O. Sengupta 2022]**)

If $\mathcal{F}$ *is* 3-radical-SG *configuration, then* $\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$*.*

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ is 2-radical-SG *configuration, then* $\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ *is* 2-radical-SG *configuration, then* $\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Proof outline:

- Structure theorem: how can $F_k \in \mathrm{rad}(F_i, F_j)$?
  1. $F_k \in \mathsf{span}_{\mathbb{C}} \{F_i, F_j\}$

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ *is* 2-radical-SG *configuration, then* $\dim \mathsf{span}_{\mathbb{C}}\{\mathcal{F}\} = O(1)$.

Proof outline:

- Structure theorem: how can $F_k \in \mathrm{rad}(F_i, F_j)$?
  1. $F_k \in \mathsf{span}_{\mathbb{C}}\{F_i, F_j\}$
  2. $\ell^2 \in \mathsf{span}_{\mathbb{C}}\{F_i, F_j\}$

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ is 2-radical-SG *configuration, then* $\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Proof outline:

- Structure theorem: how can $F_k \in \mathrm{rad}(F_i, F_j)$?
  1. $F_k \in \mathsf{span}_{\mathbb{C}} \{F_i, F_j\}$
  2. $\ell^2 \in \mathsf{span}_{\mathbb{C}} \{F_i, F_j\}$
  3. $F_i, F_j, F_k \in (x, y)$ for some linear x, y

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ *is* 2-radical-SG *configuration, then* $\dim \text{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Proof outline:

- Structure theorem: how can $F_k \in \text{rad}(F_i, F_j)$?
  1. $F_k \in \text{span}_{\mathbb{C}} \{F_i, F_j\}$
  2. $\ell^2 \in \text{span}_{\mathbb{C}} \{F_i, F_j\}$
  3. $F_i, F_j, F_k \in (x, y)$ for some linear x, y
- Main idea: "linearize" the configuration

  quadratics not robust linear configuration $\Rightarrow$ must look alike.

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ is 2-radical-SG configuration, then $\dim \text{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Proof outline:

- Structure theorem: how can $F_k \in \text{rad}(F_i, F_j)$?
  1. $F_k \in \text{span}_{\mathbb{C}} \{F_i, F_j\}$
  2. $\ell^2 \in \text{span}_{\mathbb{C}} \{F_i, F_j\}$
  3. $F_i, F_j, F_k \in (x, y)$ for some linear x, y
- Main idea: "linearize" the configuration

  quadratics not robust linear configuration $\Rightarrow$ must look alike.

Upshot: non-linear SG dependencies involve special linear forms.

Quadratic Case (1-page Amir)

Theorem (Quadratic radical SG theorem – **[Shpilka 2020]**)

If $\mathcal{F}$ is 2-radical-SG *configuration, then* $\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1)$.

Proof outline:

- Structure theorem: how can $F_k \in \mathrm{rad}(F_i, F_j)$?
  1. $F_k \in \mathsf{span}_{\mathbb{C}} \{F_i, F_j\}$
  2. $\ell^2 \in \mathsf{span}_{\mathbb{C}} \{F_i, F_j\}$
  3. $F_i, F_j, F_k \in (x, y)$ for some linear x, y
- Main idea: "linearize" the configuration

  quadratics not robust linear configuration $\Rightarrow$ must look alike.
- Extract linear Sylvester-Gallai configuration from remaining linear forms (combinatorially involved)

Some Notation

- Graded rings: $R = \bigoplus_{d \geq 0} R_d$ such that

$$R_i R_j \subset R_{i+j}$$

  $R_d :=$ set of elements of degree d.

Some Notation

- Graded rings: $R = \bigoplus_{d \geq 0} R_d$ such that

$$R_i R_j \subset R_{i+j}$$

  $R_d :=$ set of elements of degree d.
- Polynomial ring graded by degree

Some Notation

- Graded rings: $R = \bigoplus_{d \geq 0} R_d$ such that

$$R_i R_j \subset R_{i+j}$$

  $R_d :=$ set of elements of degree d.
- Polynomial ring graded by degree
- Given graded vector space $V = V_1 + \cdots + V_d$ can construct graded algebra $\mathbb{C}[V]$

How can we induct?

Approach to induct generalizes **[Shpilka 2020]** in several ways.

How can we induct?

Approach to induct generalizes **[Shpilka 2020]** in several ways.

- Observation: if there is vector space $V = V_1 + V_2$ such that $\mathcal{F} \subset \mathbb{C}[V]$, then

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq (\dim V)^3.$$

Enough to construct small algebra $\mathbb{C}[V]$ with $\dim V = O(1)$.

How can we induct?

Approach to induct generalizes **[Shpilka 2020]** in several ways.

- Observation: if there is vector space $V = V_1 + V_2$ such that $\mathcal{F} \subset \mathbb{C}[V]$, then

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq (\dim V)^3.$$

  Enough to construct small algebra $\mathbb{C}[V]$ with $\dim V = O(1)$.
- How to reduce degree? (from $3 \to 2$) Let $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$.
  - it may not be true that $\mathcal{F}_1 \cup \mathcal{F}_2$ is a 2-radical-SG configuration

How can we induct?

Approach to induct generalizes **[Shpilka 2020]** in several ways.

- Observation: if there is vector space $V = V_1 + V_2$ such that $\mathcal{F} \subset \mathbb{C}[V]$, then

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq (\dim V)^3.$$

  Enough to construct small algebra $\mathbb{C}[V]$ with $\dim V = O(1)$.
- How to reduce degree? (from $3 \to 2$) Let $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$.
  - it may not be true that $\mathcal{F}_1 \cup \mathcal{F}_2$ is a 2-radical-SG configuration
  - if could prove
    1. there is small $V = V_1 + V_2$ s.t. $\mathcal{F}_3 \subset \mathbb{C}[V]$
    2. we could solve 2-radical-SG over the algebra $\mathbb{C}[V]$

    then done!

How can we induct?

Approach to induct generalizes **[Shpilka 2020]** in several ways.

- Observation: if there is vector space $V = V_1 + V_2$ such that $\mathcal{F} \subset \mathbb{C}[V]$, then

  $$\dim \text{span}_{\mathbb{C}} \{\mathcal{F}\} \leq (\dim V)^3.$$

  Enough to construct small algebra $\mathbb{C}[V]$ with $\dim V = O(1)$.
- How to reduce degree? (from $3 \to 2$) Let $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$.
  - it may not be true that $\mathcal{F}_1 \cup \mathcal{F}_2$ is a 2-radical-SG configuration
  - if could prove
    1. there is small $V = V_1 + V_2$ s.t. $\mathcal{F}_3 \subset \mathbb{C}[V]$
    2. we could solve 2-radical-SG over the algebra $\mathbb{C}[V]$

    then done!
- Can we do both? YES!

Need a lot of new tools!

Inductive radical SG problem

Original radical SG configuration:

Definition (Radical Sylvester Gallai)

$\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{C}[x_1, \ldots, x_N]$ is a d-radical-SG config. if:

1. F_i irreducible for all $i \in [m]$
2. $\deg(F_i) \leq d$ for all $i \in [m]$ (low degree)
3. $F_i \notin (F_j)$ for $i \neq j$ ("distinct")
4. for all i, j, there is $k \neq i, j$ such that (SG dependency)

$$F_k \in \mathrm{rad}(F_i, F_j) \Leftrightarrow |\mathcal{F} \cap \mathrm{rad}(F_i, F_j)| \geq 3$$

Inductive radical SG problem

Inductive radical SG configuration:

Definition (Radical Sylvester Gallai over algebra)

Let $V = V_1 + \cdots + V_d$. $\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{C}[x_1, \ldots, x_N]$ is a (d, V)-radical-SG configuration if:

1. F_i irreducible for all $i \in [m]$
2. $\deg(F_i) \leq d$ for all $i \in [m]$ (low degree)
3. $F_i \notin (F_j)$ for $i \neq j$ ("distinct")

Inductive radical SG problem

Inductive radical SG configuration:

Definition (Radical Sylvester Gallai over algebra)

Let $V = V_1 + \cdots + V_d$. $\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{C}[x_1, \ldots, x_N]$ is a (d, V)-radical-SG configuration if:

1. F_i irreducible for all $i \in [m]$
2. $\deg(F_i) \leq d$ for all $i \in [m]$ (low degree)
3. $F_i \notin (F_j)$ for $i \neq j$ ("distinct")
4. for all i, j (SG dependency over algebra)

$$|\mathcal{F} \cap \mathrm{rad}(F_i, F_j)| \geq 3 \quad \text{or} \quad \mathrm{rad}(F_i, F_j) \cap \mathbb{C}[V] \not\subset (F_i) \cup (F_j)$$

Upshot: can have pairs i, j with no dependence in $\mathcal{F}$, but it has to have dependence in algebra $\mathbb{C}[V]$.

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?
  3. May not be possible in our case:

$$F = x(y_1 z_1 + y_2 z_2 + \cdots + y_n z_n) + uw^2 \in \mathcal{F}_3$$

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?
  3. May not be possible in our case:

$$F = x(y_1 z_1 + y_2 z_2 + \cdots + y_n z_n) + uw^2 \in \mathcal{F}_3$$

- What is next best thing?

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?
  3. May not be possible in our case:

$$F = x(y_1 z_1 + y_2 z_2 + \cdots + y_n z_n) + uw^2 \in \mathcal{F}_3$$

- What is next best thing?
  - Subalgebras that are isomorphic to a polynomial ring AND behave well with $\mathbb{C}[x_1, \ldots, x_N]$

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?
  3. May not be possible in our case:

$$F = x(y_1 z_1 + y_2 z_2 + \cdots + y_n z_n) + uw^2 \in \mathcal{F}_3$$

- What is next best thing?
  - Subalgebras that are isomorphic to a polynomial ring AND behave well with $\mathbb{C}[x_1, \ldots, x_N]$
  - Algebras generated by prime sequences!

    Key properties: Regular Sequence & Intersection flatness

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?
  3. May not be possible in our case:

$$F = x(y_1 z_1 + y_2 z_2 + \cdots + y_n z_n) + uw^2 \in \mathcal{F}_3$$

- What is next best thing?
  - Subalgebras that are isomorphic to a polynomial ring AND behave well with $\mathbb{C}[x_1, \ldots, x_N]$
  - Algebras generated by prime sequences!

    Key properties: Regular Sequence & Intersection flatness

    1. Regular sequence $\Rightarrow$ "free as polynomial ring"

Algebras

- Not all algebras are created equally...
  1. Best algebra: polynomial rings (commutative and free)
  2. Could $\mathcal{F}_3$ be in a small sub-polynomial ring?
  3. May not be possible in our case:

$$F = x(y_1 z_1 + y_2 z_2 + \cdots + y_n z_n) + uw^2 \in \mathcal{F}_3$$

- What is next best thing?
  - Subalgebras that are isomorphic to a polynomial ring AND behave well with $\mathbb{C}[x_1, \ldots, x_N]$
  - Algebras generated by prime sequences!

    Key properties: Regular Sequence & Intersection flatness

    1. Regular sequence $\Rightarrow$ "free as polynomial ring"
    2. Intersection flatness $\Rightarrow$ behaves nicely with $\mathbb{C}[x_1, \ldots, x_N]$

       Primes in the small subalgebra are also primes in $\mathbb{C}[x_1, \ldots, x_N]$

Wide Ananyan-Hochster Algebras

- Suppose I have an algebra $\mathbb{C}[F_1, \ldots, F_k]$ of low degree polynomials which is not nice

Can I convert it into a nice algebra without blowing up the size too much?

Wide Ananyan-Hochster Algebras

- Suppose I have an algebra $\mathbb{C}[F_1, \ldots, F_k]$ of low degree polynomials which is not nice

  Can I convert it into a nice algebra without blowing up the size too much?

- **[Ananyan Hochster 2020]** construct such algebras (and much more!)
  1. Basic idea: if $V = V_1 + V_2$ is such that ANY $Q \in V_2$ has

  $$\text{rank}(Q) \geq \dim V + 3$$

  then $\mathbb{C}[V]$ is a nice algebra (V nice vector space).

Wide Ananyan-Hochster Algebras

- Suppose I have an algebra $\mathbb{C}[F_1, \ldots, F_k]$ of low degree polynomials which is not nice

  Can I convert it into a nice algebra without blowing up the size too much?

- **[Ananyan Hochster 2020]** construct such algebras (and much more!)
  1. Basic idea: if $V = V_1 + V_2$ is such that ANY $Q \in V_2$ has

     $$\text{rank}(Q) \geq \dim V + 3$$

     then $\mathbb{C}[V]$ is a nice algebra (V nice vector space).

- In **[O. Sengupta 2022]** we build upon this to construct wide Ananyan-Hochster algebras
  1. generated by prime sequences (or better)
  2. robust to "small increases"

Our approach

1. Solve $(2, V)$-radical-SG problem

Proposition ([O. Sengupta 2022])

If V is wide AH vector space and $\mathcal{F}$ is $(2, V)$-radical-SG *configuration, then*

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1 + (\dim V)^2)$$

Our approach

1. Solve $(2, V)$-radical-SG problem

Proposition ([O. Sengupta 2022])

If V is wide AH vector space and $\mathcal{F}$ is $(2, V)$-radical-SG *configuration, then*

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1 + (\dim V)^2)$$

Generalizes **[Shpilka 2020]** main result.

Our approach

1. Solve $(2, V)$-radical-SG problem

Proposition ([O. Sengupta 2022])

If V is wide AH vector space and $\mathcal{F}$ is $(2, V)$-radical-SG configuration, then

$$\dim \operatorname{span}_{\mathbb{C}} \{\mathcal{F}\} = O(1 + (\dim V)^2)$$

2. Now we need to construct V wide such that $\mathcal{F}_3 \subset \mathbb{C}[V]$.

Structure Theorems

Theorem (Structure theorem for cubics **[O. Sengupta 2022]**)

Let F, G be irreducible homogeneous cubics. One of the following must hold:

1. (F, G) *is radical*
2. $(F, G) \subset (x, y)$ *for* x, y *linear forms*
3. $(F, G) \subset (Q, x)$ *for* Q *irreducible quadratic and* x *linear*
4. $xy^2 \in \mathrm{span}_{\mathbb{C}} \{F, G\}$ *for* x, y *linear forms*
5. $(F, G) \subset I_{md}$ *where* I_{md} *cuts out variety of minimal degree*

Example of variety of minimal degree: (twisted cubic)

$$\begin{pmatrix} x & y & z \\ y & z & w \end{pmatrix} \mapsto (y^2 - xz, z^2 - yw, xw - yz)$$

More Structure Theorems

In addition to the above, several new structure theorems which hold for general degree d

More Structure Theorems

In addition to the above, several new structure theorems which hold for general degree d

- Discriminant lemma (decide radical or not)
  - generalizes fact that discriminant of univariate polynomial $p(x)$ is zero $\Leftrightarrow p(x)$ has multiple roots
  - quantitative bounds when combined with wide AH algebras

Key property: Cohen-Macaulayness

More Structure Theorems

In addition to the above, several new structure theorems which hold for general degree d

- Discriminant lemma (decide radical or not)
  - generalizes fact that discriminant of univariate polynomial $p(x)$ is zero $\Leftrightarrow p(x)$ has multiple roots
  - quantitative bounds when combined with wide AH algebras

  Key property: Cohen-Macaulayness

- Transfer principle: generalize several properties of polynomial rings to wide AH algebras
  - elimination theorems in wide AH algebras
  - primality and reducedness criteria in AH algebras
  - more...

  Key property: Intersection Flatness

Proof overview

- $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$ our 3-radical-SG configuration
- Solved $(2, V)$-radical-SG problem over V low dimensional wide AH vector space

Proof overview

- $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$ our 3-radical-SG configuration
- Solved $(2, V)$-radical-SG problem over V low dimensional wide AH vector space
- Need to prove $\mathcal{F}_3 \subset \mathbb{C}[V]$ for some small wide AH vector space V
  1. If $\mathcal{F}_3$ is a δ-linear-SG configuration then $\dim \text{span}_{\mathbb{C}} \{\mathcal{F}_3\} = O(1)$.

     Apply our wide AH process to $\text{span}_{\mathbb{C}} \{\mathcal{F}_3\}$ to get V.

Proof overview

- $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \mathcal{F}_3$ our 3-radical-SG configuration
- Solved $(2, V)$-radical-SG problem over V low dimensional wide AH vector space
- Need to prove $\mathcal{F}_3 \subset \mathbb{C}[V]$ for some small wide AH vector space V
  1. If $\mathcal{F}_3$ is a δ-linear-SG configuration then $\dim \text{span}_{\mathbb{C}} \{\mathcal{F}_3\} = O(1)$.

     Apply our wide AH process to $\text{span}_{\mathbb{C}} \{\mathcal{F}_3\}$ to get V.
  2. $\mathcal{F}_3$ not δ-linear-SG configuration, then there are cubics C_1, C_2, C_3 such that most $F_i \in \mathcal{F}_3$ is such that (F_i, C_j) not-radical $(j \in [3])$.

     Most of the wide vector space V comes from C_1, C_2, C_3.

     With a bit of work, transform $\mathcal{F}$ into a $(2, V)$-radical-SG configuration.

Why is 3 important?

Challenges in degree 3 similar to challenges in general case

- geometry is more complex
  - need more general structural lemmas
  - structure theorem for cubics is more involved than for quadratics

Why is 3 important?

Challenges in degree 3 similar to challenges in general case

- geometry is more complex
  - need more general structural lemmas
  - structure theorem for cubics is more involved than for quadratics
- it may not be possible to "linearize" the configuration

Why is 3 important?

Challenges in degree 3 similar to challenges in general case

- geometry is more complex
  - need more general structural lemmas
  - structure theorem for cubics is more involved than for quadratics
- it may not be possible to "linearize" the configuration
- if we want principled approach, need to devise an inductive version of SG
  - reducing from cubic to quadratic is harder than from quadratic to linear

Why is 3 important?

Challenges in degree 3 similar to challenges in general case

- geometry is more complex
  - need more general structural lemmas
  - structure theorem for cubics is more involved than for quadratics
- it may not be possible to "linearize" the configuration
- if we want principled approach, need to devise an inductive version of SG
  - reducing from cubic to quadratic is harder than from quadratic to linear

All of the above (and a little bit more) in **[O. Sengupta 2022]**!

Conclusion

- Proved 3-radical-SG conjecture is true.

Conclusion

- Proved 3-radical-SG conjecture is true.
- Inductive, generalizable SG problem (SG over algebra)

  In previous versions, unclear how to solve SG inductively.

Conclusion

- Proved 3-radical-SG conjecture is true.
- Inductive, generalizable SG problem (SG over algebra)

  In previous versions, unclear how to solve SG inductively.
- Introduced several new algebro-geometric techniques:
  1. wide AH algebras
     - subalgebras "like subpolynomial rings"
     - robust to small augmentations
  2. discriminant-based reducedness testing & quantitative bounds
  3. transfer principle:

     polynomial rings $\to$ algebras generated by prime sequences
  4. Exploration of Cohen-Macaulayness in SG configurations
  5. Structure theorem for intersection of cubics

Open Questions

Open Question (Radical Sylvester-Gallai over an algebra)

There is $\lambda : \mathbb{N}^2 \to \mathbb{N}$ *such that if* $\mathcal{F}$ *is a* (d, V)-radical-SG *configuration, then*

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq \lambda(d, \dim V).$$

Several variants – robust, coloured, higher-codimensional... this is just the beginning of the rabbit hole.

Open Questions

Open Question (Radical Sylvester-Gallai over an algebra)

There is $\lambda : \mathbb{N}^2 \to \mathbb{N}$ *such that if* $\mathcal{F}$ *is a* (d, V)-radical-SG *configuration, then*

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq \lambda(d, \dim V).$$

Several variants – robust, coloured, higher-codimensional... this is just the beginning of the rabbit hole.

Radical Sylvester-Gallai seems instrumental first step towards main conjecture of **[Gupta 2014]**, as in **[Shpilka 2020, Peleg Shpilka 2020]**.

Open Questions

Open Question (Radical Sylvester-Gallai over an algebra)
There is $\lambda : \mathbb{N}^2 \to \mathbb{N}$ *such that if* $\mathcal{F}$ *is a* (d, V)-radical-SG *configuration, then*

$$\dim \mathsf{span}_{\mathbb{C}} \{\mathcal{F}\} \leq \lambda(d, \dim V).$$

Several variants – robust, coloured, higher-codimensional... this is just the beginning of the rabbit hole.

Radical Sylvester-Gallai seems instrumental first step towards main conjecture of **[Gupta 2014]**, as in **[Shpilka 2020, Peleg Shpilka 2020]**.

More generally: can we parametrize cancellations in algebra?

Future Directions

A sneak peek into the rabbit hole:

Open Question (Complexity theory for Algebraic Geometry)

Can we pin down the complexity of basic algebro-geometric questions?

- *primary decomposition*
- *radical ideal membership*
- *projective dimension*
- *free resolutions*

Future Directions

A sneak peek into the rabbit hole:

Open Question (Complexity theory for Algebraic Geometry)

Can we pin down the complexity of basic algebro-geometric questions?

- *primary decomposition*
- *radical ideal membership*
- *projective dimension*
- *free resolutions*

[Ananyan Hochster 2020] gives us upper bound (non-explicit) on parametrization of cancellations/relations (and in the above problems).

- can we get explicit (and eventually tight) parametrizations?
- important special cases as complexity classes?

References I

Ananyan, Tigran and Hochster, Melvin (2020)
Small subalgebras of polynomial rings and Stillman's conjecture
Journal of the American Mathematical Society

Barak, Boaz and Dvir, Zeev and Yehudayoff, Amir and Wigderson, Avi (2011)
Rank Bounds for Design Matrices with Applications to Combinatorial Geometry and Locally Correctable Codes
Forty-Third Annual ACM Symposium on Theory of Computing

Brownawell, W. Dale. (1987)
Bounds for the degrees in the Nullstellensatz.
Annals of Mathematics 126.3

Colliot-Thélene, J-L and Sansuc, J-J and Swinnerton-Dyer, P (1987)
Intersections of two quadrics and Châtelet surfaces. I.
Journal für die reine und angewandte Mathematik

References II

Dvir, Zeev and Shpilka, Amir (2007)
Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits
SIAM Journal on Computing

Dvir, Zeev and Saraf, Shubhangi and Wigderson, Avi (2014)
Improved rank bounds for design matrices and a new proof of Kelly's theorem
Forum of Mathematics, Sigma

Garg, Abhibhav and Oliveira, Rafael and Sengupta, Akash K (2022)
Robust Radical Sylvester-Gallai Theorem for Quadratics
SoCG 2022

Gallai, Tibor (1944)
Solution of problem 4065
American Mathematical Monthly

References III

Gupta, Ankit (2014)
Algebraic Geometric Techniques for Depth-4 PIT & Sylvester-Gallai Conjectures for Varieties.
Electron. Colloquium Comput. Complex.

Hansen, Sten (1966)
A generalization of a theorem of Sylvester on the lines determined by a finite point set
Mathematica Scandinavica

Hodge, William Vallance Douglas and Pedoe, Daniel (1994)
Methods of Algebraic Geometry: Volume 2
Cambridge University Press

Hirzebruch, (1983)
Arrangements of lines and algebraic surfaces
Arithmetic and Geometry, pages 113–140.

References IV

Kayal, Neeraj and Saraf, Shubhangi (2009)
Blackbox polynomial identity testing for depth 3 circuits
50th Annual IEEE Symposium on Foundations of Computer Science

Kollár, János. (1988)
Sharp effective nullstellensatz.
Journal of the American Mathematical Society

Mayr, Ernst and Meyer, Albert (1982)
The complexity of the word problems for commutative semigroups and polynomial ideals
Advances in Mathematics, 305-329

Melchior, Eberhard (1940)
Uber vielseite der projektiven ebene
Deutsche Math, volume 5, pages 461–275

References V

Oliveira, Rafael and Sengupta, Akash K (2022)
Radical Sylvester-Gallai theorem for cubics
Manuscript

Peleg, Shir and Shpilka, Amir (2020)
Polynomial time deterministic identity testing algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits via Edelstein-Kelly type theorem for quadratic polynomials
53rd Annual ACM SIGACT Symposium on Theory of Computing

Saxena, Nitin and Seshadhri, Comandur
From Sylvester-Gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits
Journal of the ACM (JACM)

Sinha, Gaurav (2016)
Reconstruction of Real Depth-3 Circuits with Top Fan-In 2
31st Conference on Computational Complexity

References VI

Serre, Jean-Pierre (1966)
Advanced problem 5359
Amer. Math. Monthly, volume 73, number 1, page 89

Shpilka, Amir (2020)
Sylvester-Gallai type theorems for quadratic polynomials
Discrete Analysis

Sylvester, James Joseph (1893)
Mathematical question 11851
Educational Times, volume 59, number 98, page 256

SG configurations in PIT and Reconstruction

- PIT/Reconstruction break down into two cases:
  1. SG circuits: where a lot of cancellations/relations can happen. In this case the circuit may not be unique/have less structure (hard case)
  2. non-SG circuits: few relations can happen. This case is easier, since we can "isolate" the gates.

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:

$$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F, G) = 9$, since F, G cubics with $\gcd(F, G) = 1$

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F, G) = 9$, since F, G cubics with $\gcd(F, G) = 1$
  4. if $m(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ then (F, G) is radical

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F,G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F,G) = 9$, since F, G cubics with $\gcd(F,G) = 1$
  4. if $m(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ then (F, G) is radical
  5. if $(F,G) \subset (x,y)$ we are done, so assume this is not the case. Then $\deg(\mathfrak{p}) \geq 2$ for all $\mathfrak{p}$.

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F, G) = 9$, since F, G cubics with $\gcd(F, G) = 1$
  4. if $m(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ then (F, G) is radical
  5. if $(F, G) \subset (x, y)$ we are done, so assume this is not the case. Then $\deg(\mathfrak{p}) \geq 2$ for all $\mathfrak{p}$.
  6. $9 = \{2, 3\} \cdot d +$ "stuff of degree ≥ 2" so $d \in \{2, 3\}$

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F, G) = 9$, since F, G cubics with $\gcd(F, G) = 1$
  4. if $m(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ then (F, G) is radical
  5. if $(F, G) \subset (x, y)$ we are done, so assume this is not the case. Then $\deg(\mathfrak{p}) \geq 2$ for all $\mathfrak{p}$.
  6. $9 = \{2, 3\} \cdot d +$ "stuff of degree ≥ 2" so $d \in \{2, 3\}$
  7. $d = 2 \Rightarrow \mathfrak{p} = (Q, x)$ for Q quadratic and x linear

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F, G) = 9$, since F, G cubics with $\gcd(F, G) = 1$
  4. if $m(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ then (F, G) is radical
  5. if $(F, G) \subset (x, y)$ we are done, so assume this is not the case. Then $\deg(\mathfrak{p}) \geq 2$ for all $\mathfrak{p}$.
  6. $9 = \{2, 3\} \cdot d +$ "stuff of degree ≥ 2" so $d \in \{2, 3\}$
  7. $d = 2 \Rightarrow \mathfrak{p} = (Q, x)$ for Q quadratic and x linear
  8. $d = 3$ and (F, G) degenerate $\Rightarrow \mathfrak{p} = (F, x)$ for x linear

Proving structure theorem

- Look at primary decomposition (minimal primes + multiplicity)
  1. (F, G) is Cohen-Macaulay $\Rightarrow$ unmixed (and much more)
  2. From primary decomposition:
  $$\deg(F, G) = \sum_{\mathfrak{p}} m(\mathfrak{p}) \cdot \deg(\mathfrak{p})$$
  3. $\deg(F, G) = 9$, since F, G cubics with $\gcd(F, G) = 1$
  4. if $m(\mathfrak{p}) = 1$ for all $\mathfrak{p}$ then (F, G) is radical
  5. if $(F, G) \subset (x, y)$ we are done, so assume this is not the case. Then $\deg(\mathfrak{p}) \geq 2$ for all $\mathfrak{p}$.
  6. $9 = \{2, 3\} \cdot d +$ "stuff of degree ≥ 2" so $d \in \{2, 3\}$
  7. $d = 2 \Rightarrow \mathfrak{p} = (Q, x)$ for Q quadratic and x linear
  8. $d = 3$ and (F, G) degenerate $\Rightarrow \mathfrak{p} = (F, x)$ for x linear
  9. $d = 3$ and (F, G) non-degenerate $\Rightarrow \mathfrak{p}$ defines variety of minimal degree