Sylvester-Gallai Type Theorems For Quadratic Polynomials

Aeren

March 15, 2021

Sylvester Gallai Theorem

DEFINITION

Let S be a subset of $\mathbb{R}^n$. An **ordinary line** of S is a line passing through exactly two points in S.

Sylvester Gallai Theorem

DEFINITION

Let S be a subset of $\mathbb{R}^n$. An **ordinary line** of S is a line passing through exactly two points in S.

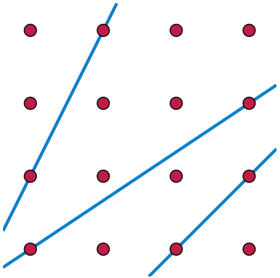

Figure: Three blue ordinary lines of the set of red points

Sylvester Gallai Theorem

THEOREM (Sylvester and Gallai)

A finite subset of $\mathbb{R}^n$ either

- is colinear or
- has an ordinary line.

Sylvester Gallai Theorem

THEOREM (Sylvester and Gallai)

A finite subset of $\mathbb{R}^n$ either

- is colinear or
- has an ordinary line.

THEOREM (Edelstein and Kelly)

Let A, B, and C be finite subsets of $\mathbb{R}^n$ such that $A \cap B \cap C = \emptyset$. Then either

- their span has low dimension or
- there exists a line intersecting with exactly two sets of A, B, and C.

Sylvester Gallai Theorem

QUESTION Why do we care about these theorems in computer science?

Polynomial Identity Testing

DEFINITION

An **arithmetic circuit** over a field F and a set of variables $x_1, \ldots, x_n$ is a labelled directed acyclic graph such that

- nodes with indegree zero is called an **input gate** and is labelled by either x_i or an element of F and
- nodes with non-zero indegree is labelled by either $+$ or $\times$, called **sum gate** and **product gate** respectively.

Polynomial Identity Testing

DEFINITION

An **arithmetic circuit** over a field F and a set of variables $x_1, \ldots, x_n$ is a labelled directed acyclic graph such that

- nodes with indegree zero is called an **input gate** and is labelled by either x_i or an element of F and
- nodes with non-zero indegree is labelled by either $+$ or $\times$, called **sum gate** and **product gate** respectively.

DEFINITION

The **size** of an arithmetic circuit is the number of gates in it.
The **depth** of an arithmetic circuit is the length of the longest path in it.

Polynomial Identity Testing

Each nodes in an arithmetic circuit computes a polynomial over the underlying field.

Polynomial Identity Testing

Each nodes in an arithmetic circuit computes a polynomial over the underlying field.

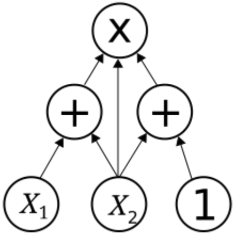

Figure: An arithmetic circuit of size 6 and depth 2

Polynomial Identity Testing

Each nodes in an arithmetic circuit computes a polynomial over the underlying field.

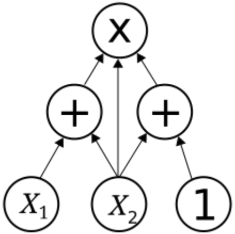

Figure: An arithmetic circuit of size 6 and depth 2

Polynomials computed on each gates

- x_1: x_1
- x_2: x_2
- 1: 1
- left sum gate: $x_1 + x_2$
- right sum gate: $x_2 + 1$
- product gate: $(x_1 + x_2)x_2(x_2 + 1)$

Polynomial Identity Testing

The PIT problem asks for a deterministic algorithm to determine whether the given arithmetic circuit computes a zero polynomial.

Polynomial Identity Testing

The PIT problem asks for a deterministic algorithm to determine whether the given arithmetic circuit computes a zero polynomial.
NOTE $X^7 - X \in \mathbb{F}_7[X]$ is not a zero polynomial even though it evaluates to zero for all substitutions by an element of $\mathbb{F}_7$

Polynomial Identity Testing

DEFINITION

A **homogeneous** $\Sigma^{[k]}\Pi^{[d]}\Sigma$ **circuits in** n **variables** is a depth-3 layered arithmetic circuits in n variables such that

- each arc connects a node to a node in the layer one level higher,
- the first layer contains a single sum gate of indegree k and outdegree 0,
- the second layer contains k product gates of indegree d and outdegree 1,
- the third layer contains $k \times d$ sum gates of outdegree 1, and
- the last layer contains the input gates labelled by a variable.

Polynomial Identity Testing

DEFINITION

A **homogeneous** $\Sigma^{[k]}\Pi^{[d]}\Sigma$ **circuits in** n **variables** is a depth-3 layered arithmetic circuits in n variables such that

- each arc connects a node to a node in the layer one level higher,
- the first layer contains a single sum gate of indegree k and outdegree 0,
- the second layer contains k product gates of indegree d and outdegree 1,
- the third layer contains $k \times d$ sum gates of outdegree 1, and
- the last layer contains the input gates labelled by a variable.

A homogeneous $\Sigma^{[k]}\Pi^{[d]}\Sigma$ circuit in n variables computes a polynomial of form

$$P(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{d} l_{i,j}(x_1, \ldots, x_n)$$

for some linear forms $l_{i,j}$.

Polynomial Identity Testing

Consider a homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuit in n variables C with the corresponding polynomial it computes

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} l_{i,j}(x_1, ..., x_n).$$

Polynomial Identity Testing

Consider a homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuit in n variables C with the corresponding polynomial it computes

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} l_{i,j}(x_1, ..., x_n).$$

If P is a zero polynomial, then, for all $j, j' \in [d]$,

$$\prod_{i=1}^{d} l_{1,i} \equiv 0 \mod l_{2,j}, l_{3,j'}.$$

Polynomial Identity Testing

Consider a homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuit in n variables C with the corresponding polynomial it computes

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} l_{i,j}(x_1, ..., x_n).$$

If P is a zero polynomial, then, for all $j, j' \in [d]$,

$$\prod_{i=1}^{d} l_{1,i} \equiv 0 \mod l_{2,j}, l_{3,j'}.$$

This implies that, for all $j, j' \in [d]$, $l_{2,j}$ and $l_{3,j'}$ spans a function in the set $l_{1,1}, ..., l_{1,d}$.

Polynomial Identity Testing

Consequently, by the Edelstein-Kelly theorem, these linear functions span a low dimensional space.

Polynomial Identity Testing

Consequently, by the Edelstein-Kelly theorem, these linear functions span a low dimensional space.

Rewriting C in $\mathrm{O}(1)$ variables forming the basis of the space allows efficient PIT algorithms for $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuits.

Polynomial Identity Testing

Consequently, by the Edelstein-Kelly theorem, these linear functions span a low dimensional space.

Rewriting C in O(1) variables forming the basis of the space allows efficient PIT algorithms for $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuits.

It turns out that a similar but a bit more complicated holds for larger ks.

Polynomial Identity Testing

Consequently, by the Edelstein-Kelly theorem, these linear functions span a low dimensional space.

Rewriting C in $O(1)$ variables forming the basis of the space allows efficient PIT algorithms for $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuits.

It turns out that a similar but a bit more complicated holds for larger ks.

QUESTION Is there a similar relation for higher degree homogeneous polynomials?

Depth-4 Circuits

Let

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} Q_{i,j}(x_1, ..., x_n)$$

be the polynomial computed by a depth-4 homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuit where $Q_{i,j}$s are quadratic forms.

Depth-4 Circuits

Let

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} Q_{i,j}(x_1, ..., x_n)$$

be the polynomial computed by a depth-4 homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuit where $Q_{i,j}$s are quadratic forms.

We can try an approach similar to the depth-3 case.

Depth-4 Circuits

Let

$$P(x_1, \ldots, x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} Q_{i,j}(x_1, \ldots, x_n)$$

be the polynomial computed by a depth-4 homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuit where $Q_{i,j}$s are quadratic forms.

We can try an approach similar to the depth-3 case.

P being a zero polynomial would imply that, for all $j, j' \in [d]$,

$$\prod_{i=1}^{d} Q_{1,i} \equiv 0 \mod Q_{2,j}, Q_{3,j'}.$$

Depth-4 Circuits

Unfortunately, we can't deduce the same result with the above equation:

Depth-4 Circuits

Unfortunately, we can't deduce the same result with the above equation:

Let $Q_1 = xy + zw, Q_2 = xy - zw, Q_3 = xw, Q_4 = yz$.

Depth-4 Circuits

Unfortunately, we can't deduce the same result with the above equation:

Let $Q_1 = xy + zw, Q_2 = xy - zw, Q_3 = xw, Q_4 = yz$.

Then

$$Q_3 \cdot Q_4 \equiv 0 \mod Q_1, Q_2$$

but neither Q_3 nor Q_4 vanishes modulo Q_1, Q_2.

Definition

Let R be a commutative ring and I an ideal of R.
The **radical of** I, denoted by $\sqrt{I}$, is defined as

$$\sqrt{I} = \{r \in R | r^n \in I \text{ for some } n \in \mathbb{Z}_+\}.$$

Definition

Let R be a commutative ring and I an ideal of R.
The **radical of** I, denoted by $\sqrt{I}$, is defined as

$$\sqrt{I} = \{r \in R | r^n \in I \text{ for some } n \in \mathbb{Z}_+\}.$$

For example, the radical of $24\mathbb{Z}$ as an ideal of $\mathbb{Z}$ is $6\mathbb{Z}$.

Review Of Algebraic Geometry

Definition

Let R be a commutative ring and I an ideal of R.
The **radical of** I, denoted by $\sqrt{I}$, is defined as

$$\sqrt{I} = \{r \in R | r^n \in I \text{ for some } n \in \mathbb{Z}_+\}.$$

For example, the radical of $24\mathbb{Z}$ as an ideal of $\mathbb{Z}$ is $6\mathbb{Z}$.

It is not hard to verify that radical of an ideal is again an ideal, and that $\sqrt{\sqrt{I}} = \sqrt{I}$

DEFINITION

Let K be a field.
The **projective space of dimension** n, denoted by $\mathbb{P}_n(K)$, is the quotient space of the $n+1$ dimensional vector space over K, excluding the origin, under the equivalence relation "$(x_0, ..., x_n) \sim (y_0, ..., y_n)$ if and ony if there exists $c \in K$ with $c(x_0, ..., x_n) = (y_0, ..., y_n)$".
We denote the equivalence class of $(x_0, ..., x_n)$ by $(x_0 : ... : x_n)$.

Review Of Algebraic Geometry

DEFINITION

Let K be a field.
The **projective space of dimension** n, denoted by $\mathbb{P}_n(K)$, is the quotient space of the $n+1$ dimensional vector space over K, excluding the origin, under the equivalence relation "$(x_0, ..., x_n) \sim (y_0, ..., y_n)$ if and ony if there exists $c \in K$ with $c(x_0, ..., x_n) = (y_0, ..., y_n)$".
We denote the equivalence class of $(x_0, ..., x_n)$ by $(x_0 : ... : x_n)$.

Note that for a homogeneous polynomial $p \in K[x_0, ..., x_n]$, it makes sense to argue whether an element in $\mathbb{P}_n(K)$ is a zero of p or not, since, for any $(x_0, ..., x_n) \neq (0, ..., 0)$, if $p(x_0, ..., x_n) = 0$, then $p(c \cdot x_0, ..., c \cdot x_n) = 0$ for all $c \in K$.

Review Of Algebraic Geometry

DEFINITION

Let K be an algebraically closed field.
Given a set $P \subseteq K[x_0, ..., x_n]$ of homogeneous polynomials, denote by $\mathcal{Z}(P)$ the set of common zeroes of polynomials in P in $\mathbb{P}_n(K)$.
Given a set $S \subseteq \mathbb{P}_n(K)$, denote by $\mathcal{I}(S)$ the ideal of $K[x_0, ..., x_n]$ of polynomials vanishing at all points in S.
A subset S of $\mathbb{P}_n(K)$ is a **projective variety** if $S = \mathcal{Z}(P)$ for some $P \subseteq K[x_0, ..., x_n]$.

Review Of Algebraic Geometry

THEOREM (Hilbert)

For an algebraically closed field K and an ideal I of $K[x_0, ..., x_n]$ of homogeneous polynomials,

$$\sqrt{I} = \mathcal{I}(\mathcal{Z}(I))$$

Generalization

We had a polynomial computed by a depth-4 homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuit

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} Q_{i,j}(x_1, ..., x_n)$$

where $Q_{i,j}$s are quadratic forms.

Generalization

We had a polynomial computed by a depth-4 homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuit

$$P(x_1, ..., x_n) = \sum_{i=1}^{3} \prod_{j=1}^{d} Q_{i,j}(x_1, ..., x_n)$$

where $Q_{i,j}$s are quadratic forms.

P being a zero polynomial would imply that, for all $j, j' \in [d]$,

$$\prod_{i=1}^{d} Q_{1,i} \equiv 0 \mod Q_{2,j}, Q_{3,j'}.$$

Generalization

THEOREM (Gupta)

Let $P_1, \dots, P_d, Q_1, \dots, Q_k \in \mathbb{C}[x_1, \dots, x_n]$ be homogeneous polynomials with degree of each Q_i is at most r. Then,

$$\prod_{i=1}^{d} P_i \in \sqrt{\langle Q_1, \dots, Q_k \rangle} \iff \exists \{i_1, \dots, i_{r^k}\} \subseteq [d] : \prod_{j=1}^{r^k} P_{i_j} \in \sqrt{\langle Q_1, \dots, Q_k \rangle}.$$

Generalization

THEOREM (Gupta)

Let $P_1, \ldots, P_d, Q_1, \ldots, Q_k \in \mathbb{C}[x_1, \ldots, x_n]$ be homogeneous polynomials with degree of each Q_i is at most r. Then,

$$\prod_{i=1}^{d} P_i \in \sqrt{\langle Q_1, \ldots, Q_k \rangle} \iff \exists \{i_1, \ldots, i_{r^k}\} \subseteq [d] : \prod_{j=1}^{r^k} P_{i_j} \in \sqrt{\langle Q_1, \ldots, Q_k \rangle}.$$

By the Hilbert's theorem, the statement is equivalent to

$$\prod_{i=1}^{d} P_i \equiv 0 \mod Q_1, \ldots, Q_k \iff \exists \{i_1, \ldots, i_{r^k}\} \subseteq [d] : \prod_{j=1}^{r^k} P_{i_j} \equiv 0 \mod Q_1, \ldots, Q_k$$

Generalization

Therefore,

$$\prod_{i=1}^{d} Q_{1,i} \equiv 0 \mod Q_{2,j}, Q_{3,j'}$$

$$\iff$$

$$\exists i_{1,j,j'}, i_{2,j,j'}, i_{3,j,j'}, i_{4,j,j'} \in [d] : Q_{i_{1,j,j'}} Q_{i_{2,j,j'}} Q_{i_{3,j,j'}} Q_{4_{1,j,j'}} \equiv 0 \mod Q_{2,j}, Q_{3,j'}$$

Generalization

Therefore,

$$\prod_{i=1}^{d} Q_{1,i} \equiv 0 \mod Q_{2,j}, Q_{3,j'}$$

$$\iff$$

$$\exists i_{1,j,j'}, i_{2,j,j'}, i_{3,j,j'}, i_{4,j,j'} \in [d] : Q_{i_{1,j,j'}} Q_{i_{2,j,j'}} Q_{i_{3,j,j'}} Q_{4_{1,j,j'}} \equiv 0 \mod Q_{2,j}, Q_{3,j'}$$

Similar reasoning also works for higher degree homogeneous polynomials.

Generalization

Therefore,

$$\prod_{i=1}^{d} Q_{1,i} \equiv 0 \mod Q_{2,j}, Q_{3,j'}$$

$$\iff$$

$$\exists i_{1,j,j'}, i_{2,j,j'}, i_{3,j,j'}, i_{4,j,j'} \in [d] : Q_{i_{1,j,j'}} Q_{i_{2,j,j'}} Q_{i_{3,j,j'}} Q_{4_{1,j,j'}} \equiv 0 \mod Q_{2,j}, Q_{3,j'}$$

Similar reasoning also works for higher degree homogeneous polynomials.

All that is left to do is finding the corresponding Sylvester-Galllai / Edelstein-Kelly theorem!

Main Theorems

CONJECTURE (Gupta)

Let $\mathcal{F}_1, ..., \mathcal{F}_k$ be finite sets of irreducible homogeneous polynomials in $\mathbb{C}[x_1, ..., x_n]$ of degree $\leq r$ such that $\cap_i \mathcal{F}_i = \emptyset$ and for every $k-1$ polynomials $Q_1, ..., Q_{k-1}$ from distinct sets, there are $P_1, ..., P_c$ from the remaining set such that whenever $Q_1, ..., Q_{k-1}$ vanish, the product $\prod_{i=1}^{c} P_i$ also vanishes. Then, $trdeg_{\mathbb{C}}(\cup_i \mathcal{F}_i) \leq \lambda(k, r, c)$ for some function λ.

Main Theorems

CONJECTURE (Gupta)

Let $\mathcal{F}_1, \ldots, \mathcal{F}_k$ be finite sets of irreducible homogeneous polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ of degree $\leq r$ such that $\cap_i \mathcal{F}_i = \emptyset$ and for every $k-1$ polynomials $Q_1, \ldots, Q_{k-1}$ from distinct sets, there are $P_1, \ldots, P_c$ from the remaining set such that whenever $Q_1, \ldots, Q_{k-1}$ vanish, the product $\prod_{i=1}^{c} P_i$ also vanishes. Then, $trdeg_{\mathbb{C}}(\cup_i \mathcal{F}_i) \leq \lambda(k, r, c)$ for some function λ.

When $r = c = 1$, by the Edelstein-Kelly theorem, $\lambda(k, r, c) \leq 2$.

Main Theorems

In order to approach the previous conjecture, Gupta set up two subsequent conjectures.

Main Theorems

In order to approach the previous conjecture, Gupta set up two subsequent conjectures.

CONJECTURE

Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible and homogeneous polynomials of degree $\leq r$ such that for every pair of distinct Q_i, Q_j, there is a distinct Q_k so that whenever Q_i and Q_j vanish, then so does Q_k. Then $trdeg_{\mathbb{C}}(Q_1, \ldots, Q_m) \leq \lambda(m)$ for some function λ.

Main Theorems

In order to approach the previous conjecture, Gupta set up two subsequent conjectures.

CONJECTURE

Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible and homogeneous polynomials of degree $\leq r$ such that for every pair of distinct Q_i, Q_j, there is a distinct Q_k so that whenever Q_i and Q_j vanish, then so does Q_k. Then $trdeg_{\mathbb{C}}(Q_1, \ldots, Q_m) \leq \lambda(m)$ for some function λ.

Note that $r = 1$ case is implied by the Sylvester-Gallai theorem.

Main Theorems

In order to approach the previous conjecture, Gupta set up two subsequent conjectures.

CONJECTURE

Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible and homogeneous polynomials of degree $\leq r$ such that for every pair of distinct Q_i, Q_j, there is a distinct Q_k so that whenever Q_i and Q_j vanish, then so does Q_k. Then $trdeg_{\mathbb{C}}(Q_1, \ldots, Q_m) \leq \lambda(m)$ for some function λ.

Note that $r = 1$ case is implied by the Sylvester-Gallai theorem.

CONJECTURE

Let R, B, G be finite sets of irreducible homogeneous polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ of degree $\leq r$ such that for every pair Q_1, Q_2 from distinct sets, there is a Q_3 in the remaining set such that whenever Q_1 and Q_2 vanish, so does Q_3. Then $trdeg_{\mathbb{C}}(R \cup B \cup G) \leq \lambda(r)$ for some function λ.

In order to approach the previous conjecture, Gupta set up two subsequent conjectures.

CONJECTURE

Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible and homogeneous polynomials of degree $\leq r$ such that for every pair of distinct Q_i, Q_j, there is a distinct Q_k so that whenever Q_i and Q_j vanish, then so does Q_k. Then $trdeg_{\mathbb{C}}(Q_1, \ldots, Q_m) \leq \lambda(m)$ for some function λ.

Note that $r = 1$ case is implied by the Sylvester-Gallai theorem.

CONJECTURE

Let R, B, G be finite sets of irreducible homogeneous polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ of degree $\leq r$ such that for every pair Q_1, Q_2 from distinct sets, there is a Q_3 in the remaining set such that whenever Q_1 and Q_2 vanish, so does Q_3. Then $trdeg_{\mathbb{C}}(R \cup B \cup G) \leq \lambda(r)$ for some function λ.

Again, $r = 1$ case is implied by the Edelstein-Kelly theorem.

Main Theorems

This paper confirms the previous two conjectures for $r = 2$. More specifically,

Main Theorems

This paper confirms the previous two conjectures for $r = 2$. More specifically,

THEOREM (Sylvester-Gallai Theorem For Quadratic Polynomials)

Let $Q_1, \ldots, Q_n$ be homogeneous quadratic polynomials over $\mathbb{C}$ such that each Q_i is either irreducible or square of a linear function, and for every $i \neq j$, there exists $k \neq i, j$ such that whenever Q_i and Q_j vanish, Q_k vanishes as well. Then the linear span of Q_is has dimension $O(1)$

Main Theorems

This paper confirms the previous two conjectures for $r = 2$. More specifically,

THEOREM (Sylvester-Gallai Theorem For Quadratic Polynomials)

Let $Q_1, \ldots, Q_n$ be homogeneous quadratic polynomials over $\mathbb{C}$ such that each Q_i is either irreducible or square of a linear function, and for every $i \neq j$, there exists $k \neq i, j$ such that whenever Q_i and Q_j vanish, Q_k vanishes as well. Then the linear span of Q_is has dimension $O(1)$

THEOREM (Edelstein-Kelly Theorem For Quadratic Polynomials)

Let $\mathcal{T}_1, \mathcal{T}_2$, and $\mathcal{T}_3$ be finite sets of homogeneous quadratic polynomials over $\mathbb{C}$ such that

- each $\cup_i \mathcal{T}_i$ is either irreducible or square of a linear function,
- no two polynomials are linearly dependent, and
- for every two polynomials Q_1 and Q_2 from distinct sets there is a polynomial Q_3 in the third set so that whenever Q_1 and Q_2 vanishes, Q_3 vanishes as well.

Then the linear span of the polynomials in $\cup_i \mathcal{T}_i$ has dimension $O(1)$.

Proof Outline

The following theorem gives the general structure of quadratic forms satisfying $Q \in \sqrt{\langle Q_1, Q_2 \rangle}$.

Proof Outline

The following theorem gives the general structure of quadratic forms satisfying $Q \in \sqrt{\langle Q_1, Q_2 \rangle}$.

THEOREM (Structure Theorem)

Let Q, Q_1, and Q_2 be homogeneous quadratic polynomials such that whenever Q_1 and Q_2 vanish, Q vanishes as well. Then one of the followings hold:

1. Q is in the linear span of Q_1, Q_2.
2. There exists a non trivial linear combinations of the form $\alpha Q_1 + \beta Q_2 = \mathcal{L}^2$ where $\mathcal{L}$ is a linear form.
3. There exist two linear forms $\mathcal{L}_1$ and $\mathcal{L}_2$ such that whenever they vanish, Q, Q_1 and Q_2 vanish as well.

Proof Outline

DEFINITION

We say that a set of points $S = v_1, ..., v_m \subseteq \mathbb{C}^d$ forms a δ-**SG configuration** if for every $i \in [m]$, there exists at least $\delta \cdot m$ values of $i \neq j \in [m]$ such that the line through v_i and v_j passes through a third point in the set.

Proof Outline

DEFINITION

We say that a set of points $S = v_1, ..., v_m \subseteq \mathbb{C}^d$ forms a δ-**SG configuration** if for every $i \in [m]$, there exists at least $\delta \cdot m$ values of $i \neq j \in [m]$ such that the line through v_i and v_j passes through a third point in the set.

THEOREM (Qualitative Sylvester-Gallai Theorem)

Suppose $S \subseteq \mathbb{C}^d$ is a δ-SG configuration. Then $\dim(\mathrm{span}(S)) \in O(1/\delta^2)$

Proof Outline

DEFINITION

We say that three finite sets of points $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subseteq \mathbb{C}^d$ form a δ-**EK configuration** if for every point in one set and δ fractions of point in another set, the line connecting each of them passes through a point in the third set.

Proof Outline

DEFINITION

We say that three finite sets of points $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subseteq \mathbb{C}^d$ form a δ-**EK configuration** if for every point in one set and δ fractions of point in another set, the line connecting each of them passes through a point in the third set.

THEOREM (Qualitative Edelstein-Kelly Theorem)

Suppose $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subseteq \mathbb{C}^d$ is a δ-EK configuration. Then $\dim(\mathrm{span}(\mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3)) \in O(1/\delta^3)$.

Proof Outline

1. Let $Q_1, \ldots, Q_n$ be polynomials satisfying the condition in the Sylvester-Gallai theorem for quadratic polynomials.

Proof Outline

1. Let $Q_1, ..., Q_n$ be polynomials satisfying the condition in the Sylvester-Gallai theorem for quadratic polynomials.
2. If for every Q_i, there exists at least $n/100$ polynomials Q_j where $\mathrm{span}(Q_i, Q_j)$ contains another polynomial, the theorem follows from the qualitative Sylvester-Gallai theorem.

Proof Outline

1. Let $Q_1, ..., Q_n$ be polynomials satisfying the condition in the Sylvester-Gallai theorem for quadratic polynomials.
2. If for every Q_i, there exists at least $n/100$ polynomials Q_j where $\mathrm{span}(Q_i, Q_j)$ contains another polynomial, the theorem follows from the qualitative Sylvester-Gallai theorem.
3. The proof is now just casework depending on how many polynomials violate the condition.

Proof Outline

1. Let $Q_1, ..., Q_n$ be polynomials satisfying the condition in the Sylvester-Gallai theorem for quadratic polynomials.
2. If for every Q_i, there exists at least $n/100$ polynomials Q_j where $\mathrm{span}(Q_i, Q_j)$ contains another polynomial, the theorem follows from the qualitative Sylvester-Gallai theorem.
3. The proof is now just casework depending on how many polynomials violate the condition.
4. More specifically, if there exists two polynomial violating the condition, we can use the structure theorem to put some heavy restriction on the remaining polynomials.

Proof Outline

1. Let $Q_1, ..., Q_n$ be polynomials satisfying the condition in the Sylvester-Gallai theorem for quadratic polynomials.
2. If for every Q_i, there exists at least $n/100$ polynomials Q_j where $\mathrm{span}(Q_i, Q_j)$ contains another polynomial, the theorem follows from the qualitative Sylvester-Gallai theorem.
3. The proof is now just casework depending on how many polynomials violate the condition.
4. More specifically, if there exists two polynomial violating the condition, we can use the structure theorem to put some heavy restriction on the remaining polynomials.

The proof outline for the Edelstein-Kelly theorem goes similarly, except that it has more cases.

Conclusion

- Unfortunately, these results don't directly lead to an PIT algorithm for $\Sigma^{[k]}\Pi\Sigma\Pi^{[2]}$ circuits, even for $k = 3$.
- However, the author published a subsequent paper presenting the polynomial time deterministic PIT algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits.
- Currently, lots of variants of Sylvester-Gallai theorem are known, including the colored version(Edelstein-Kelly theorem) and the quadratic polynomial version presented in this paper. It could be the case that there exists a common generalization of the theorem which contains all these variants.

The End