



Robust Sylvester-Gallai Type Theorem for Quadratic Polynomials

Shir Peleg  

Tel Aviv University, Israel

Amir Shpilka  

Tel Aviv University, Israel

Abstract

In this work we extend the robust version of the Sylvester-Gallai theorem, obtained by Barak, Dvir, Wigderson and Yehudayoff, and by Dvir, Saraf and Wigderson, to the case of quadratic polynomials. Specifically, we prove that if $\mathcal{Q} \subset \mathbb{C}[x_1, \dots, x_n]$ is a finite set, $|\mathcal{Q}| = m$, of irreducible quadratic polynomials that satisfy the following condition

There is $\delta > 0$ such that for every $Q \in \mathcal{Q}$ there are at least δm polynomials $P \in \mathcal{Q}$ such that whenever Q and P vanish then so does a third polynomial in $\mathcal{Q} \setminus \{Q, P\}$.

then $\dim(\text{span}\{\mathcal{Q}\}) = \text{Poly}(1/\delta)$.

The work of Barak et al. and Dvir et al. studied the case of linear polynomials and proved an upper bound of $O(1/\delta)$ on the dimension (in the first work an upper bound of $O(1/\delta^2)$ was given, which was improved to $O(1/\delta)$ in the second work).

2012 ACM Subject Classification Mathematics of computing \rightarrow Mathematical analysis; Theory of computation \rightarrow Computational geometry

Keywords and phrases Sylvester-Gallai theorem, quadratic polynomials, Algebraic computation

Digital Object Identifier 10.4230/LIPIcs.SoCG.2022.43

Related Version *Full Version:* <http://arxiv.org/abs/2202.04932>

Funding *Shir Peleg:* The research leading to these results has received funding from the Israel Science Foundation (grant number 514/20) and from the Len Blavatnik and the Blavatnik Family foundation.

Amir Shpilka: The research leading to these results has received funding from the Israel Science Foundation (grant number 514/20) and from the Len Blavatnik and the Blavatnik Family foundation.

Independent result

Independently of our work, [18] have also proved the same result. Both works have been presented in a common talk at CG week 2022. For a more detailed comparison between the works, we refer the reader to Subsection 1.2.

1 Introduction

In this paper we prove a robust version of a result of [40]: Let $\mathcal{T} \subset \mathbb{C}[x_1, \dots, x_n]$ be a finite set of polynomials. We say that $Q_1(\vec{x}), Q_2(\vec{x}) \in \mathcal{Q}$ satisfy the *Polynomial Sylvester-Gallai condition* (PSG-condition for short) if there is a third polynomial $Q_3(\vec{x}) \in \mathcal{Q}$ such that $Q_3(\vec{x})$ vanishes whenever $Q_1(\vec{x})$ and $Q_2(\vec{x})$ vanish. We prove that if $\mathcal{T} \subset \mathbb{C}[x_1, \dots, x_n]$ is a finite set containing only irreducible quadratic polynomials, such that for every $Q \in \mathcal{T}$ a δ fraction of the polynomials in \mathcal{T} satisfy the PSG-condition with Q , then $\dim(\text{span}\{\mathcal{T}\}) = \text{Poly}(1/\delta)$.



© Shir Peleg and Amir Shpilka;

licensed under Creative Commons License CC-BY 4.0

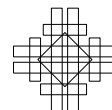
38th International Symposium on Computational Geometry (SoCG 2022).

Editors: Xavier Goaoc and Michael Kerber; Article No. 43; pp. 43:1–43:15

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



The motivation for proving this result, besides its own appeal, is two fold: a similar theorem played an important role in the polynomial identity testing (PIT for short) problem for small depth algebraic circuits, one of the fundamental open problems in theoretical computer science, see [33]; and it is also related to a long line of work extending and generalizing the original Sylvester-Gallai theorem [30, 17]. In particular, our result builds and generalizes a result of [3, 9], that can be viewed as proving an analogous claim for the case of degree-1 polynomials. Such results are useful in discrete geometry [3, 9], in the study of locally correctable codes, for reconstruction of certain depth-3 circuits [39, 25, 42] and more. See the survey of Dvir on incidence geometry for some applications of Sylvester-Gallai type theorems [7].

We next give background on the Sylvester-Gallai theorem, and some of its variants, and then discuss the connection to the polynomial identity testing problem.

Sylvester-Gallai type theorems

The Sylvester-Gallai theorem (SG-theorem) asserts that given a set $S = \{\vec{v}_1, \dots, \vec{v}_m\} \subset \mathbb{R}^n$ such that S is not contained in a line, there must be a line that contains exactly two points from S . It was first conjectured by Sylvester in 1893 [44] and then proved, independently, by Melchior in 1941 [30] and Gallai [17] in 1943 (in an answer to the same question posed by Erdős, who was unaware of Melchior’s result [12]). There are many extensions and generalizations of the theorem. We shall state a few that are related to this work. It is also helpful to think of the contra-positive statement. We say that a set of points is a Sylvester-Gallai configuration (SG-configuration for short) if every line that intersects the set at two points, must contain at least three points from the set. Thus, an SG-configuration in \mathbb{R}^n must be colinear.

In [38] Serre, aware that the original formulation of the theorem is not true over \mathbb{C} asked “Is there a nonplanar version of the Sylvester-Gallai configuration over the field of complex numbers?” Kelly proved that the answer is no, i.e. that every finite set of points in \mathbb{C}^n satisfying the SG-condition is planar [27]. Edelstein and Kelly proved a colorful variant of the problem: if three finite sets of points in \mathbb{R}^n satisfy that every line passing through points from two different sets also contains a point from the third set, then, the points belong to a three-dimensional affine space. This result can be extended to any constant number of sets. Many more extensions and generalizations of the SG-theorem are known, e.g. [22, 8]. The survey by Borwein and Moser [5] is a good resource on the SG-Theorem and some of the different variants that have been studied in the past.

More recently, Barak et al. [3] and Dvir, Saraf and Wigderson [9], motivated by questions on locally decodable codes and construction of rigid matrices, proved a *robust* (or fractional) version of the SG-theorem:

► **Definition 1** (δ -SG configuration). *We say that a set of points $v_1, \dots, v_m \in \mathbb{C}^n$ is a δ -SG configuration if for every $i \in [m]$ there exists at least $\delta(m-1)$ values of $j \in [m]$ such that the line through v_i, v_j contains a third point in the set.*

► **Theorem 2** (Theorem 1.9 of [9]). *Let $V = \{v_1, \dots, v_m\} \subset \mathbb{C}^n$ be a δ -SG configuration. Then $\dim(\text{span}\{v_1, \dots, v_m\}) \leq \frac{12}{\delta} + 1$.*

Algebraic generalizations of Sylvester-Gallai type theorems

Although the Sylvester-Gallai theorem and Theorem 2 are formulated in the setting of discrete geometry, there is a very natural algebraic formulation: If a finite set of pairwise linearly independent vectors, $\mathcal{S} \subset \mathbb{C}^n$, has the property that every two vectors span a third vector in the set, then the dimension of \mathcal{S} is at most 3. The proof is immediate from Kelly's theorem: pick a subspace H of codimension 1, which is in general position with respect to the vectors in \mathcal{S} . The intersection points $p_i = H \cap \text{span}\{s_i\}$, for $s_i \in \mathcal{S}$, satisfy the SG-condition over \mathbb{C} . Therefore, $\dim(S) \leq 3$. An equivalent formulation, in the case of linear functions, is the following: If a finite set of pairwise linearly independent linear forms, $\mathcal{L} \subset \mathbb{C}[x_1, \dots, x_n]$, has the property that for every two forms $\ell_i, \ell_j \in \mathcal{L}$ there is a third $\ell_k \in \mathcal{L}$, such that $\ell_k = 0$ whenever $\ell_i = \ell_j = 0$, then the linear dimension of \mathcal{L} is at most 3. To see the equivalence note that it must be the case that $\ell_k \in \text{span}\{\ell_i, \ell_j\}$ and thus the coefficient vectors of the forms in the set satisfy the condition for the (vector version of the) SG-theorem, and the bound on the dimension follows. Observe that the last example shows that in the case of linear functions the PSG-condition and the SG-condition are equivalent. The last formulation can now be generalized to higher degree polynomials. In particular, the following conjecture was raised by Gupta [20].

► **Definition 3** (PSG-configuration). *Let $\mathcal{T} \subset \mathbb{C}[x_1, \dots, x_n]$ be a set of polynomials. We say that $Q_1, Q_2 \in \mathcal{T}$ satisfy the Polynomial Sylvester-Gallai condition (PSG-condition for short) if there is a third polynomial $Q_3(\vec{x}) \in \mathcal{T}$ such that Q_3 vanishes whenever Q_1 and Q_2 vanish.*

We say that a set \mathcal{T} is a PSG-configuration if every two polynomials $Q_1, Q_2 \in \mathcal{T}$ satisfy the PSG-condition.

► **Problem 1** (Conjecture 2 of [20]). *There is a function $\lambda : \mathbb{N} \rightarrow \mathbb{N}$ such that for any finite set $\mathcal{T} \subset \mathbb{C}[x_1, \dots, x_n]$ of pairwise linearly independent and irreducible polynomials, of degree at most r , that satisfy the PSG-condition, it holds that the algebraic rank of \mathcal{T} is at most $\lambda(r)$.*

This problem was answered affirmatively, with a stronger conclusion, in the case of quadratic polynomials ($r = 2$) in [40].

► **Theorem 4** (Theorem 1.7 of [40]). *There is a constant λ such that the following holds for every $n \in \mathbb{N}$. Let $\mathcal{T} \subset \mathbb{C}[x_1, \dots, x_n]$ consist of homogeneous quadratic polynomials, such that each $Q \in \mathcal{T}$ is either irreducible or a square of a linear function. If \mathcal{T} satisfies the PSG-condition then $\dim(\text{span}\{\mathcal{T}\}) \leq \lambda$.*

Motivated by applications for the polynomial identity testing problem, Gupta [20] and Beecken, Mittmann and Saxena [4] also raised the following colorful variant, which generalizes the Edelstein-Kelly theorem.

► **Conjecture 5** (Conjecture 30 of [20]). *There is a function $\lambda : \mathbb{N} \rightarrow \mathbb{N}$ such that the following holds for every $r, n \in \mathbb{N}$. Let R, B, G be finite disjoint sets of pairwise linearly independent, irreducible, homogeneous polynomials in $\mathbb{C}[x_1, \dots, x_n]$ 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 so that whenever Q_1 and Q_2 vanish then also Q_3 vanishes. Then the algebraic rank of $(R \cup B \cup G)$ is at most $\lambda(r)$.*

This problem was also answered affirmatively, with the same stronger conclusion, in [40], for the case of quadratic polynomials.

► **Theorem 6** (Theorem 1.8 of [40]). *There is a constant λ such that the following holds for every $n \in \mathbb{N}$. Let $\mathcal{T}_1, \mathcal{T}_2$ and \mathcal{T}_3 be finite sets of homogeneous quadratic polynomials over \mathbb{C} satisfying the following properties:*

- *Each $Q \in \cup_i \mathcal{T}_i$ is either irreducible or a square of a linear function.*
- *No two polynomials are multiples of each other (i.e., every pair is linearly independent).*
- *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 vanish then also Q_3 vanishes.*

Then $\dim(\text{span}\{\cup_i \mathcal{T}_i\})$ has dimension $O(1)$.

PIT and Sylvester-Gallai type theorems

The PIT problem asks to give a deterministic algorithm that given an arithmetic circuit as input determines whether it computes the identically zero polynomial. The circuit can be given either via a description of its graph of computation (white-box model) or via oracle access to the polynomial that it computes (black-box model). This is a fundamental problem in theoretical computer science that has received a lot of attention from researchers in the last two decades. Besides of being a natural and elegant question, the PIT problem is important due its connections to lower bounds for arithmetic circuits (hardness-randomness tradeoffs) [23, 1, 24, 11, 6]; its relation to other derandomization problems such as finding perfect matching deterministically, in parallel, [13, 43], derandomizing factoring algorithms [28], derandomization questions in geometric complexity theory [31, 15]; its role in algebraic natural proofs [16, 19]. In particular, PIT appears to be the most general algebraic derandomization problem. For more on the PIT problem see [41, 34, 35, 14]. For a survey of algebraic hardness-randomness tradeoffs see [29].

A beautiful line of work has shown that deterministic algorithms for the PIT problem for homogeneous depth-4 circuits or for depth-3 circuits would lead to deterministic algorithms for general circuits [2, 21]. This makes small depth circuits extremely interesting for the PIT problem. This is also the setting where Sylvester-Gallai type theorems play an important role. The relation between (colored-versions of the) SG-theorem and deterministic PIT algorithms for depth-3 circuits was observed in [10]. The work of [26, 37] used this relation to obtain polynomial- and quasi-polynomial-time PIT algorithms for depth-3 circuits, depending on the characteristic. Currently, the best algorithm for PIT of depth-3 circuits was obtained through a different yet highly related approach in [36]. As the SG-theorem played such an important role in derandomizing PIT for depth-3 circuits, it was asked whether a similar approach could work for depth-4 circuits. This motivated [4, 20] to raise Problem 1 and Conjecture 5. In [33] we gave a positive answer to Conjecture 5 for the case of degree-2 polynomials ($r = 2$). Interestingly, Theorem 2 played a crucial role in the proof, as well as in the proofs of [40, 32]. Studying the proofs of [40, 32, 33] leads to the conclusion that in order to solve Problem 1 and Conjecture 5 for degrees larger than 2, we must first obtain a result analogous to Theorem 2.

Our results

In this work we prove an analog of Theorem 2 for quadratic polynomials. We hope that this result will lead to an extension of the works [40, 32, 33] to higher degree polynomials.

► **Definition 7** (δ -PSG-configuration). *Let $\mathcal{Q} \subset \mathbb{C}[x_1, \dots, x_n]$ be a set of polynomials. We say that a finite set of polynomials \mathcal{Q} is a δ -PSG configuration if for every $Q \in \mathcal{Q}$ there are at least $\delta \cdot |\mathcal{Q}|$ polynomials $P \in \mathcal{Q}$ such that Q and P satisfy the PSG condition.*

► **Theorem 8.** *Let $\mathcal{Q} \subset \mathbb{C}[x_1, \dots, x_n]$ a finite set of irreducible quadratic polynomials. If \mathcal{Q} is a δ -PSG configuration then $\dim(\text{span}\{\mathcal{Q}\}) = O(1/\delta^{16})$.*

► **Remark 9.** The same conclusion holds even if we allow irreducible polynomials of degree at most 2 (i.e. if we allow linear functions). The proof is similar in nature, with more case analysis, and so we decided to omit it.

Note that this is robust version of Theorem 4 in the same sense that Theorem 2 is a robust version of the SG-theorem.

► **Remark 10.** While the result in Theorem 2 tight (up to the constant in the big Oh), we do not believe that the result of Theorem 8 is tight. In particular, we believe that the upper bound should be $O(1/\delta)$.

1.1 Proof idea

To explain the proof we will use some algebraic notations, $\langle \cdot \rangle$ denotes an ideal, $\sqrt{\langle \cdot \rangle}$ denotes the radical of the ideal, and $\mathbb{C}[V]_2$ denotes the space of all quadratic polynomials defined only using the linear forms in V .

At the heart of all previous work lies an algebraic theorem, classifying the cases in which a quadratic polynomial vanishes when two other quadratics vanish (actually, for [32, 33] a more general result was needed - a characterization of the different cases in which a product of quadratic polynomials vanishes whenever two other quadratics vanish).

► **Theorem 11** (Theorem 1.10 of [40]). *Let A, B and C be n -variate, homogeneous, quadratic polynomials, over \mathbb{C} , such that whenever A and B vanish then so does C . Then, one of the following cases must hold:*

- (i) *C is in the linear span of A and B .*
- (ii) *There exists a non trivial linear combination of the form $\alpha A + \beta B = \ell^2$ for some linear form ℓ .*
- (iii) *There exist two linear forms ℓ_1 and ℓ_2 such that when setting $\ell_1 = \ell_2 = 0$ we get that A and B (and consequently C) vanish.*

The high level idea in the proof of Theorem 4 (which was generalized in [32, 33]), includes two steps; The first step constructs a linear space of linear forms V , and a subset $\mathcal{J} \subset \mathcal{Q}$, both of constant dimension such that a vast majority of the polynomials in \mathcal{Q} are in $\text{span}\{\mathcal{J}, \mathcal{Q} \cap \langle V \rangle\}$.¹ Implementing this idea requires a lot of case analysis, according to Theorem 11. In the second step the dimension of $\mathcal{Q} \cap \langle V \rangle$ is upper bounded.

The idea outlined above heavily relies on the fact that when $\delta = 1$, the set $\mathcal{Q} \cap \langle V \rangle$ is a PSG-configuration in itself. Indeed, let $Q_1, Q_2 \in \mathcal{Q} \cap \langle V \rangle$. When $\delta = 1$ it follows that there is $Q_3 \in \mathcal{Q}$ such that $Q_3 \in \sqrt{\langle Q_1, Q_2 \rangle} \subseteq \langle V \rangle$. In order to bound the dimension of $\mathcal{Q} \cap \langle V \rangle$, [40] “projected” V to a one dimensional space $\text{span}\{z\}$ (where z is a new variable). Every polynomial $Q_i \in \mathcal{Q} \cap \langle V \rangle$ is mapped to a polynomial of the form $z \cdot \ell_i$, for some linear form ℓ_i . Then, it is proved that the ℓ_i ’s form an SG-condition.²

This technique fails when $\delta \in (0, 1)$. First, we cannot expect to prove that $\mathcal{Q} \cap \langle V \rangle$ is a δ' -PSG configuration by itself (even when we allow smaller, yet fixed, $\delta' \leq \delta$). For example, since $\delta < 1$, it may be the case that (many polynomials) $Q \in \mathcal{Q} \cap \langle V \rangle$ have *all* of

¹ [40] had different notations, and $|\mathcal{J}| = 1$.

² The reader should take note that this is a very high-level simplification of one part in the proof. For more details see the “easy-case” in [32, 33].

their neighbors outside $\mathcal{Q} \cap \langle V \rangle$. Furthermore, even if we knew that $\mathcal{Q} \cap \langle V \rangle$ is a δ' -PSG configuration, then it is not clear that by following the lines of [40] and mapping $\langle V \rangle$ to $\text{span}\{z\}$, the resulting ℓ 's, form a δ' -PSG configurations. The reason for that is a bit subtle: note that it may be the case that many polynomials $Q \in \mathcal{Q} \cap \langle V \rangle$ were mapped to $\text{span}\{z^2\}$. Thus, it may be the case that all the neighbors of some $z \cdot \ell$ are in $\text{span}\{z^2\}$, which gives us no information at all about ℓ . In contrast, in [40], since $\delta = 1$, we could get information about ℓ by its interaction with polynomials not in $\text{span}\{z^2\}$.

In order to overcome these issues, we needed to develop new techniques, and improve the characterization given in Theorem 11iii (see Corollary 19). Next, we present the outline of the proof in more details.

We start with the same line of constructing a linear space of linear forms V , and a subset $\mathcal{J} \subset \mathcal{Q}$, both of dimension $O(\text{poly}(\frac{1}{\delta}))$ such that $\mathcal{Q} \subseteq \text{span}\{\mathcal{J}, \langle V \rangle\}$. We partition \mathcal{Q} to four sets: $\mathcal{C}_{[V]} = \mathcal{Q} \cap \mathbb{C}[V]_2$; $\mathcal{C}_{\langle V \rangle} = (\mathcal{Q} \cap \langle V \rangle) \setminus \mathcal{C}_{[V]}$; $\mathcal{J}_{[V]} = \mathcal{Q} \cap \text{span}\{\mathcal{J} \cup \mathbb{C}[V]_2\}$; and the remaining set $\mathcal{J}_{\langle V \rangle} = \mathcal{Q} \cap \text{span}\{\mathcal{J} \cup \langle V \rangle\} \setminus \mathcal{J}_{[V]}$. We already know that $\dim(\mathcal{C}_{[V]} \cup \mathcal{J}_{[V]})$ is small, so we only have to bound the dimension of $\mathcal{C}_{\langle V \rangle} \cup \mathcal{J}_{\langle V \rangle}$.

Let us focus on $\mathcal{C}_{\langle V \rangle}$. We would like to prove that we can add a few linear functions to V to get a subspace U such that $\mathcal{C}_{\langle V \rangle} \subset \mathbb{C}[U]_2$. Let $P \in \mathcal{C}_{\langle V \rangle}$. First we consider the case that many of P 's neighbors (i.e. those polynomials with which P satisfies the PSG-condition) are in $\mathcal{C}_{[V]} \cup \mathcal{C}_{\langle V \rangle}$. To handle this case we strengthen Theorem 11iii and use it to show that if $Q \in \mathcal{C}_{[V]}$ is a neighbor of P then the polynomial $Q' \in \sqrt{\langle P, Q \rangle}$ is unique (see Corollary 18). This means that by moving the linear functions on which P depends to U , we move many polynomials from $\mathcal{C}_{\langle V \rangle}$ to $\mathbb{C}[V + U]_2$.

Next we consider the case where P has “many” neighbors in $\mathcal{J}_{[V]} \cup \mathcal{J}_{\langle V \rangle}$. To handle this case we first prove that P can only satisfy Theorem 11i with polynomials in $\mathcal{J}_{[V]} \cup \mathcal{J}_{\langle V \rangle}$. We prove that under this condition, there is a “large” subset of $\mathcal{C}_{\langle V \rangle}$ that is of constant dimension. Thus, by adding a few linear functions to U , we move many polynomials from $\mathcal{C}_{\langle V \rangle}$ to $\mathbb{C}[V + U]_2$ (see Claim 29). We can continue this process as long as $\mathcal{C}_{\langle V \rangle}$ is large enough, as the amount of polynomials that we move at any step depends on $|\mathcal{C}_{\langle V \rangle}|$. Therefore, when this process terminates we still have to deal with a set $\mathcal{C}_{\langle V \rangle}$ that is not large but not too small either (it is of size $\Omega(\delta m)$). Now, we turn our attention to $\mathcal{J}_{\langle V \rangle}$. Using similar arguments, and relying on the fact that $|\mathcal{C}_{\langle V \rangle}|$ is small, we prove that we can add a few linear functions to U and make $|\mathcal{J}_{\langle V+U \rangle}|$ small. Having achieved that, we prove that if both $|\mathcal{C}_{\langle V+U \rangle}|$ and $|\mathcal{J}_{\langle V+U \rangle}|$ are small then they are in fact, empty (see Claim 28).

1.2 The work of [18]

Independently from this work, Garg, Oliveira and Sengupta have also proved that δ -PSG configurations have dimension bounded by $\text{Poly}(\frac{1}{\delta})$.

While our result, in its current form, holds when the configuration is assumed to contain only irreducible quadratics, [18] also allow linear forms in the configuration. Our techniques are good enough to deduce the more general case, but since it adds more technical details that do not give more insight into the problem, we decided to omit that part of the proof.

There are a number of parallels between the methods used in [18] and the ones used in our paper. Both proofs use structure theorems that analyze the situation in which there is a quadratic polynomial in the radical of an ideal generated by two other quadratics. Basically those theorems prove that the involved quadratics must satisfy certain structural conditions. Further, both results partition the δ -PSG configuration to “special” sets based on the different cases of the structure theorem, and analyze each of these sets separately.

One key technical difference between our approach and that of [18] is the definition of these special sets. While we construct \mathcal{J}, V using our iterative process, [18] define the notion of clean vector spaces, which generate “special algebras” (in their terminology) that have similar properties, but are also saturated in the sense that adding a few linear forms to the vector space cannot bring too many polynomials from the configuration “closer” to the vector space. This is the analog of moving many polynomials from $\mathcal{J}_{(V)} \cup \mathcal{C}_{(V)}$ to $\mathcal{J}_{[V]} \cup \mathcal{C}_{[V]}$, until this cannot be done anymore, in our work.

[18] also uses the notion of univariate polynomials over clean vector spaces, whereas we work with the ideal generated by the vector space V . They show that there is a clean vector space W , of dimension at most $\text{Poly}(\frac{1}{\delta})$, such that the polynomials in each special set are univariate over W . In other words, each Q_i in the configuration can be represented as a polynomial in the space $\mathbb{C}[W, \ell_i]_2$ for some linear form ℓ_i . They then show that these ℓ_i 's form a LCC configuration (see [3, 18] for definition), instead of a robust linear SG configuration, which is what we use in our work. This in turn is also the reason why the bound in [18] is slightly worse than the one in our work.

1.3 Discussion

There are two distinct goal to the line of work [40, 32, 33], including this paper. The first is obtaining higher degree geometric extensions of the Sylvester-Gallai and Edelman-Kelley theorems. From the complexity theoretic point of view, the goal is to eventually obtain PIT algorithms for $\Sigma^{[k]}\Pi^{[d]}\Sigma\Pi^{[r]}$ circuits, for any $k, r = O(1)$. Currently we have a polynomial time PIT algorithm only for the case $k = 3$ and $r = 2$ [33]. To understand such a difficult question one has to start somewhere, and the case $k = 3$ and $r = 2$ was a natural starting point for the investigation (especially as no subexponential time PIT algorithm, even for $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuits, was known prior to [33]). Since so little is known, we believe that a natural approach for advancing is to first extend the results of [33] to higher degrees (i.e. higher values of r), and then for a higher top fan-in (i.e. higher values of k). Before we explain the difficulties in going to higher degrees we recall that [33] needed the following strengthening of Theorem 6 for their PIT algorithm.

► **Theorem 12** (Theorem 1.6 in [33]). *There exists a universal constant λ such that the following holds. Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}[x_1, \dots, x_n]$ be finite sets of pairwise linearly independent homogeneous polynomials satisfying the following properties:*

- *Each $Q \in \cup_{j \in [3]} \mathcal{T}_j$ is either irreducible quadratic or a square of a linear function.*
- *Every two polynomials Q_1 and Q_2 from distinct sets satisfy that whenever they vanish then the product of all the polynomials in the third set vanishes as well.*

Then, $\dim(\text{span}\{\cup_{j \in [3]} \mathcal{T}_j\}) \leq \lambda$.

There are several difficult hurdles in going from $r = 2$ to general r , or even to $r = 3$, if we wish to continue working in the framework of [40, 32, 33] (and this paper). The first is understanding what is the correct generalization of Theorem 11 to higher degrees, as this theorem lies at the heart of all these papers. A second hurdle is obtaining a robust version of Theorem 12. First for $r = 2$ and then for higher degrees.

For extending Theorem 11 to higher degrees it seems natural to find an extension to $r = 3$. While it seems that such an approach could last forever and lead nowhere (as we will then have to prove a result for $r = 4$ etc.), we believe that understanding the case $r = 3$ can shed more light on the general case, as sometimes going from degree 2 to 3 is as difficult as the general case.

Once we prove such a structural theorem, we will need to extend Theorem 12 to higher values of r . An important tool in the proof of Theorem 12 was a robust version of the EK-theorem.

► **Definition 13** (δ -EK configuration). *We say that the sets $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}^n$ form a δ -EK configuration if for every $i \in [3]$ and $p \in \mathcal{T}_i$ a δ fraction of the vectors q in the union of the two other sets satisfy that p and q span some vector in the third set (the one not containing p and q). We refer to a 1-EK configuration as simply an EK-configuration.*

► **Theorem 14** (Theorem 3.9 of [33]). *Let $0 < \delta \leq 1$ be any constant. Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}^n$ be disjoint finite sets that form a δ -EK configuration. Then, $\dim(\text{span}\{\cup_i \mathcal{T}_i\}) = O(1/\delta^3)$.*

Thus, a natural continuation would be to prove a robust version of Theorem 14 for quadratic polynomials (i.e. a robust version of Theorem 6) and then to extend it to a robust version of Theorem 12 and to higher degrees. While in this paper we only prove a robust version of Theorem 4, we believe that with some more technical work this can be extended to a robust version of Theorem 6 as well. Hence, the next immediate challenge would be to obtain a robust version of Theorem 12 (or even of the main result of [32]). If we obtain such an extension and, in addition extend Theorem 11 to higher values of r , then we expect that a PIT algorithm for the case $k = 3$ and $r = 3$ would follow. More importantly, we believe that this will let us gain important understanding on how to generalize the results for arbitrary values of r .

2 Robust-SG theorems in \mathbb{C}^n

We shall need the following generalizations of Theorem 2. The proofs of this section appear in the full version.

► **Theorem 15.** *Let $0 < \delta \leq 1$ be any constant. Let $W \subset \mathbb{C}^n$ be an r -dimensional space. Let $\mathcal{W} \subset W$ and $\mathcal{K} \subset \mathbb{C}^n \setminus W$ be finite subsets such that no two vectors in $\mathcal{T} = \mathcal{K} \cup \mathcal{W}$ are linearly dependent. Assume further that all the elements in \mathcal{K} satisfy the following relaxed EK-property: For every $p \in \mathcal{K}$, for at least δ fraction of the points $q \in \mathcal{T}$ the span of p and q contains a point in $\mathcal{T} \setminus \{p, q\}$. Then, $\dim(\text{span}\{\mathcal{T}\}) \leq O(r + \frac{1}{\delta})$.*

We also use the following bi-partitive version of [9, Corollary 1.11] this is a slight variation of the formulation presented in their paper.

► **Claim 16.** Let $V = v_1, \dots, v_n \subset \mathbb{C}^d$ be a set of n distinct points. Suppose that there is $\mathcal{B} \subseteq V$ such that there are at least δn^2 pairs in $\mathcal{B} \times (V \setminus \mathcal{B})$ that lie on a special line. Then there exists a subset $\mathcal{B}' \subseteq \mathcal{B}$ such that $|\mathcal{B}'| \geq (\delta/6)n$ and $\text{affine-dim}(\mathcal{B}') \leq O(1/\delta)$.

The important difference between Claim 16 and [9, Corollary 1.11] is that Claim 16 guarantees the existence of a low-dimensional subspace that contains a constant fraction of the points in \mathcal{B} , whereas from [9, Corollary 1.11] we do not get any guarantee about the fraction of points from \mathcal{B} in the low-dimensional space.

3 Strengthening Case iii of Theorem 11

The following claim strengthens Theorem 11iii by providing more information on the polynomial in the radical.

▷ **Claim 17.** Let P, Q and T be irreducible homogeneous quadratic polynomials, such that $T \in \sqrt{\langle P, Q \rangle}$. Furthermore, assume that they satisfy Theorem 11iii and not any other case, that is, there are linear forms v_1, v_2 such that $T, P, Q \in \langle v_1, v_2 \rangle$. Finally, assume $\text{Lin}(P) \not\subseteq \text{Lin}(Q)$. Then there are linear forms $v'_1, v'_2 \in \text{span}\{v_1, v_2\}$ such that the following holds:

- $P = v'_1 \ell + v'^2_2$ for some linear form ℓ .
 - $Q = v'_1 u - v'^2_2$ for some linear form u .
 - $T = v'_2(\ell + u) + \alpha P + \beta Q$ for some constants $\alpha, \beta \in \mathbb{C}$,
- where the qualities holds up to a constant non zero factor.

We provide the proof of Claim 17 in the full version. As a consequence of the claim we can deduce the following uniqueness property.

▶ **Corollary 18.** Let P, Q, Q', T be pairwise linearly independent irreducible quadratics such that $T \in \sqrt{\langle P, Q \rangle}$. Let T' be such that $T' \not\sim P, Q, Q'$ and such that $T' \in \sqrt{\langle P, Q' \rangle}$. Assume further that $P \in \langle \text{Lin}(Q) + \text{Lin}(Q') \rangle$ but $\text{Lin}(P) \not\subseteq \text{Lin}(Q) + \text{Lin}(Q')$. Then $T \neq T'$. In addition, $\text{Lin}(T), \text{Lin}(T') \not\subseteq \text{Lin}(Q) + \text{Lin}(Q')$.

The proof of Corollary 18 appears in the full version.

We finish this section by formulating the improvement for Theorem 11 which follows immediately from Claim 17

▶ **Corollary 19 (Improvement of Theorem 1.10 of [40]).** Let A, B and C be n -variate, homogeneous, quadratic polynomials, over \mathbb{C} , such that $C \in \sqrt{\langle A, B \rangle}$. Then, one of the following cases must hold:

- (i) C is in the linear span of A and B .
- (ii) There exists a non trivial linear combination of the form $\alpha A + \beta B = \ell^2$ for some linear form ℓ .
- (iii) If none of the above hold, then there exist two linear forms ℓ_1 and ℓ_2 such that $A, B, C \in \langle \ell_1, \ell_2 \rangle$. Furthermore, we have that either $\text{Lin}(P) \subseteq \text{Lin}(Q)$ or
 - $A = \ell_1 a + \ell^2_2$ for some linear form a .
 - $B = \ell_1 b - \ell^2_2$ for some linear form b .
 - $C = \ell_2(a + b) + \alpha A + \beta B$ for some constants $\alpha, \beta \in \mathbb{C}$.

4 Robust Sylvester-Gallai theorem for quadratic polynomials

We divide $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{Q}_3$ as following:

$$\mathcal{Q}_1 = \left\{ Q \in \mathcal{Q} \mid \begin{array}{l} Q \text{ satisfies Theorem 11i with at least} \\ \delta/100 \text{ fraction of the polynomials in } \mathcal{Q} \end{array} \right\}, \tag{1}$$

$$\mathcal{Q}_2 = \left\{ Q \in \mathcal{Q} \mid \begin{array}{l} Q \text{ satisfies Theorem 11ii with at least} \\ \delta/100 \text{ fraction of the polynomials in } \mathcal{Q} \end{array} \right\}, \tag{2}$$

$$\mathcal{Q}_3 = \left\{ Q \in \mathcal{Q} \mid \begin{array}{l} Q \text{ satisfies Theorem 11iii with at least} \\ \delta/100 \text{ fraction of the polynomials in } \mathcal{Q} \end{array} \right\}. \tag{3}$$

We will also use the following notation: Let $Q \in \mathcal{Q}$, and $t \in \{(i), (ii), (iii)\}$ we denote

$$\Gamma_t(Q) = \{P \in \mathcal{Q} \mid Q, P \text{ satisfy case } t \text{ of Theorem 11}\}.$$

Finally we set $\mathcal{Q}_1 = \mathcal{Q}_1 \setminus (\mathcal{Q}_2 \cup \mathcal{Q}_3)$. This implies that if $P \in \mathcal{Q}_1$ then at least a $\delta/100$ fraction of the polynomials in \mathcal{Q} satisfy Theorem 11i with P and no other case.

43:10 Robust Sylvester-Gallai Type Theorem for Quadratic Polynomials

► **Observation 20.** *The definition of Γ_t naturally defines an undirected graph with an edge between P and Q if for some t , $Q \in \Gamma_t(P)$ (which is equivalent to saying $P \in \Gamma_t(Q)$). Thus, when we speak of “edges” and “neighbors” this graph is the one that we refer to.*

Throughout the proof, we will use the following simple claim.

▷ **Claim 21.** Let $P, T \in \mathcal{Q}$. Removing T from \mathcal{Q} , causes the removal of at most two polynomials from $\Gamma_{(i)}(P)$, and this happens only in the case that $P \in \Gamma_{(i)}(T)$ and $|\mathcal{Q} \cap \text{span}\{P, T\}| = 3$.

Proof. First, note that for $Q_1, Q_2, Q_3 \in \mathcal{Q}$ if $Q_3 \in \text{span}\{Q_1, Q_2\}$, then for every $k \neq j \in [3]$, $Q_k \in \Gamma_{(i)}(Q_j)$. In particular, if $P \notin \Gamma_{(i)}(T)$, then removing T from \mathcal{Q} does not affect $\Gamma_{(i)}(P)$.

Let $P \in \Gamma_{(i)}(T)$. By the argument above, if $|\mathcal{Q} \cap \text{span}\{P, T\}| > 3$ then removing T does not affect $\Gamma_{(i)}(P)$. Thus, the only case the $\Gamma_{(i)}(P)$ is affected is when $|\mathcal{Q} \cap \text{span}\{P, T\}| = 3$ and in this case the third polynomial in the span is removed from $\Gamma_{(i)}(P)$. ◁

The proof of Theorem 8 is organized as follows. In the full version we bound the dimension of \mathcal{Q}_2 . Specifically, we prove the following claim.

▷ **Claim 22.** There exist a subset $\mathcal{I} \subseteq \mathcal{Q}_2$ of size $|\mathcal{I}| = O(1/\delta)$, and a linear space of linear forms V' such that $\dim(V') = O(1/\delta^2)$ such that $\mathcal{Q}_2 \subset \text{span}\{\mathcal{I}, \mathbb{C}[V']_2\}$.

In the full version prove that for some small dimensional space V'' , it holds that $\mathcal{Q}_3 \subset \langle V'' \rangle$.

▷ **Claim 23.** There exists a linear space of linear forms, V'' , such that $\dim(V'') = O(1/\delta)$ and $\mathcal{Q}_3 \subset \langle V'' \rangle$.

Set $V = V' + V''$. So far it holds that $\mathcal{Q}_2 \in \text{span}\{\mathcal{I}, \mathbb{C}[V]_2\}$ and $\mathcal{Q}_3 \subset \langle V \rangle$. Next, we find a small set of polynomials \mathcal{J} such that $\mathcal{Q} \subset \langle V \rangle + \text{span}\{\mathcal{J}\}$.

▷ **Claim 24.** There exists a set $\mathcal{J} \subseteq \mathcal{Q}$, of size $|\mathcal{J}| = O(1/\delta)$, such that $\mathcal{Q} \subset \text{span}\{(\mathcal{Q} \cap \langle V \rangle), \mathcal{J}, \mathbb{C}[V]_2\}$. Furthermore, if $P \in \mathcal{Q} \setminus \langle V \rangle$ then there is no quadratic L such that $P + L \in \langle V \rangle$ and $\text{rank}_s(L) \leq 2$.

Given the claims above we have that $\mathcal{Q} \subset \text{span}\{(\mathcal{Q} \cap \langle V \rangle), \mathcal{J}, \mathbb{C}[V]_2\}$, where $|\mathcal{J}| = O(1/\delta)$ and $\dim(V) = O(1/\delta^2)$. We are not done yet as the dimension of $\langle V \rangle$, as a vector space, is not a constant. To bound this dimension we partition \mathcal{Q} to four sets and study the subgraphs induced by any two of the sets.

$$\mathcal{C}_{[V]} = \{Q \in \mathcal{Q} \mid Q \in \mathbb{C}[V]_2\} \tag{4}$$

$$\mathcal{C}_{\langle V \rangle} = \{Q \in \mathcal{Q} \mid Q \in \langle V \rangle\} \setminus \mathcal{C}_{[V]} \tag{5}$$

$$\mathcal{J}_{[V]} = \{Q \in \mathcal{Q} \mid Q \in \text{span}\{\mathcal{J}, \mathbb{C}[V]_2\} \setminus \mathbb{C}[V]_2\} \tag{6}$$

$$\mathcal{J}_{\langle V \rangle} = \{Q \in \mathcal{Q} \mid Q \in \text{span}\{\mathcal{J}, \langle V \rangle\} \setminus \langle V \rangle\} \setminus \mathcal{J}_{[V]} . \tag{7}$$

In words, $\mathcal{C}_{[V]}$ is the set of all quadratics in \mathcal{Q} that only depend on linear functions in V . $\mathcal{C}_{\langle V \rangle}$ is the set of polynomials that are in $\langle V \rangle$ but not in $\mathcal{C}_{[V]}$, etc.

Our goal is to bound the dimension of each of these sets. In fact, we already know that $\dim(\mathcal{C}_{[V]})$, $\dim(\mathcal{J}_{[V]}) \leq O(1/\delta^4)$ so we only need to bound $\dim(\mathcal{C}_{\langle V \rangle})$ and $\dim(\mathcal{J}_{\langle V \rangle})$. For that we will analyze the edges between the different sets.

We first note that the “furthermore” part of Claim 24, stating that the “rank-distance” between nonzero polynomials in $\text{span}\{\mathcal{J}\}$ and quadratics in $\langle V \rangle$ is larger than 2, implies the following:

► **Observation 25.**

1. If $P \in \mathcal{C}_{\langle V \rangle} \cup \mathcal{C}_{[V]}$ and $Q \in \mathcal{J}_{\langle V \rangle} \cup \mathcal{J}_{[V]}$ satisfy that $P \in \Gamma(Q)$ then P and Q satisfy Theorem 11i.
2. If $P \in \mathcal{J}_{\langle V \rangle}$ and $Q \in \mathcal{C}_{\langle V \rangle} \cup \mathcal{C}_{[V]} \cup \mathcal{J}_{[V]}$ satisfy that $P \in \Gamma(Q)$ then P and Q satisfy Theorem 11i.

Proof. We only prove the first case as the proof of the second case is similar. As $Q \in \mathcal{J}_{\langle V \rangle} \cup \mathcal{J}_{[V]}$, we have that $\text{rank}_s(Q_1) > 2$. In particular, P and Q do not satisfy Theorem 11iii. If P and Q satisfy Theorem 11ii then $Q = \alpha P + \ell^2$ for some linear form ℓ , which contradicts the structure of \mathcal{J} guaranteed in Claim 24. ◀

To bound the dimension of $\mathcal{C}_{\langle V \rangle}$ we note that any edge going from $P \in \mathcal{C}_{\langle V \rangle} \cup \mathcal{J}_{\langle V \rangle}$ to $\mathcal{C}_{[V]} \cup \mathcal{J}_{[V]}$ defines uniquely a third polynomial in $\mathcal{C}_{\langle V \rangle} \cup \mathcal{J}_{\langle V \rangle}$. This uniqueness property guarantees that if we add $\text{Lin}(P)$ to V , then many polynomials move from $\mathcal{C}_{\langle V \rangle} \cup \mathcal{J}_{\langle V \rangle}$ to $\mathcal{C}_{[V]} \cup \mathcal{J}_{[V]}$.

▷ **Claim 26.** Let $P \in \mathcal{C}_{\langle V \rangle}$ then,

1. for every polynomial $Q_1 \in \Gamma(P) \cap \mathcal{J}_{[V]}$ there is a unique polynomial $Q'_1 \in \mathcal{J}_{\langle V \rangle}$ such that $Q'_1 \in \text{span}\{P, Q_1\}$. I.e., there is no other $Q_2 \in \mathcal{J}_{[V]}$ such that $Q'_1 \in \text{span}\{P, Q_2\}$.
2. for every polynomial $Q_1 \in \Gamma(P) \cap \mathcal{C}_{[V]}$ there is a unique polynomial $Q'_1 \in \mathcal{C}_{\langle V \rangle}$ such that $Q'_1 \in \sqrt{\langle P, Q_1 \rangle}$. I.e., there is no other $Q_2 \in \mathcal{C}_{[V]}$ such that $Q'_1 \in \sqrt{\langle P, Q_2 \rangle}$.

Proof.

1. Let $Q_1 \in \Gamma(P) \cap \mathcal{J}_{[V]}$. By Observation 25, P and Q_1 satisfy Theorem 11i. We first prove that they span a polynomial in $\mathcal{J}_{\langle V \rangle}$ and then prove its uniqueness. Any polynomial in $T \in \text{span}\{P, Q_1\} \setminus (\text{span}\{P\})$ has $\text{rank}_s(T) > 2$, even when setting the linear forms in V to 0. Hence, P and Q_1 span a polynomial $Q'_1 \in \mathcal{J}_{[V]} \cup \mathcal{J}_{\langle V \rangle}$. As $P \notin \mathcal{C}[V]_2$ we can conclude that $Q'_1 \in \mathcal{J}_{\langle V \rangle}$. To prove that Q'_1 is unique assume that $Q'_1 \in \text{span}\{P, Q_2\}$ for some $Q_2 \in \mathcal{J}_{[V]}$. Pairwise linear independence implies that $P \in \text{span}\{Q_1, Q_2\}$ which implies that $P \in \mathcal{C}_{[V]}$, in contradiction.
2. Follows from Corollary 18. ◀

▷ **Claim 27.** Let $P \in \mathcal{J}_{\langle V \rangle}$. Then for every polynomial $Q_1 \in \Gamma(P) \cap (\mathcal{J}_{[V]} \cup \mathcal{C}_{[V]})$ there is a unique polynomial $Q'_1 \in \mathcal{J}_{\langle V \rangle} \cup \mathcal{C}_{\langle V \rangle}$ such that $Q'_1 \in \text{span}\{P, Q_1\}$. By “unique” we mean that there is no other $Q_2 \in \mathcal{J}_{[V]}$ such that $Q'_1 \in \text{span}\{P, Q_2\}$.

Proof. We first consider the case $Q_1 \in \Gamma(P) \cap \mathcal{C}_{[V]}$. Observation 25 implies that P and Q_1 satisfy Theorem 11i. By construction of \mathcal{J} , any polynomial in $T \in \text{span}\{P, Q_1\} \setminus (\text{span}\{Q_1\})$ has $\text{rank}_s(T) > 2$, even when setting the linear forms in V to 0. Hence, P and Q_1 span a polynomial $Q'_1 \in \mathcal{J}_{[V]} \cup \mathcal{J}_{\langle V \rangle}$. As $P \notin \mathcal{J}_{[V]}$ we conclude that $Q'_1 \in \mathcal{J}_{\langle V \rangle}$. To prove that Q'_1 is unique assume that $Q'_1 \in \text{span}\{P, Q_2\}$ for some $Q_2 \in \mathcal{J}_{[V]} \cup \mathcal{C}_{[V]}$. As before, pairwise linear independence shows that $P \in \text{span}\{Q_1, Q_2\}$, which implies that $P \in \mathcal{J}_{[V]}$, in contradiction.

Consider the case $Q_1 \in \Gamma(P) \cap \mathcal{J}_{[V]}$. As before, P and Q_1 must satisfy Theorem 11i. Any polynomial in $T \in \text{span}\{P, Q_1\} \setminus (\text{span}\{Q_1\})$ is not in $\mathcal{J}_{[V]} \cup \mathcal{C}_{[V]}$. Hence, P and Q_1 span a polynomial $Q'_1 \in \mathcal{C}_{\langle V \rangle} \cup \mathcal{J}_{\langle V \rangle}$. Uniqueness follows exactly as in the first case. ◀

We next show that the uniqueness property proved in Claims 26 and 27 imply that $\mathcal{J}_{\langle V \rangle}$ and $\mathcal{C}_{\langle V \rangle}$ cannot be “too small,” unless they are empty.

▷ **Claim 28.** If $|\mathcal{J}_{\langle V \rangle}|, |\mathcal{C}_{\langle V \rangle}| \leq (\delta/10) \cdot m$, then $\mathcal{J}_{\langle V \rangle} = \mathcal{C}_{\langle V \rangle} = \emptyset$.

43:12 Robust Sylvester-Gallai Type Theorem for Quadratic Polynomials

Proof. Assume towards a contradiction that there is $P \in \mathcal{C}_{\langle V \rangle} \cup \mathcal{J}_{\langle V \rangle}$. As $|\Gamma(P)| \geq \delta m$ it follows that $|\Gamma(P) \cap (\mathcal{C}_{[V]} \cup \mathcal{J}_{[V]})| \geq (8\delta/10) \cdot m$. Claims 26 and 27 imply that there are at least $|\Gamma(P) \cap (\mathcal{C}_{[V]} \cup \mathcal{J}_{[V]})| \geq 8\delta/10$ polynomials in $\mathcal{J}_{\langle V \rangle} \cup \mathcal{C}_{\langle V \rangle}$ in contradiction to the assumption that there are at most $(2\delta/10) \cdot m$ polynomials in $\mathcal{J}_{\langle V \rangle} \cup \mathcal{C}_{\langle V \rangle}$. \triangleleft

Thus, if we can make $|\mathcal{J}_{\langle V \rangle}|, |\mathcal{C}_{\langle V \rangle}| \leq (\delta/10) \cdot m$ without increasing $\dim(V)$ and $|\mathcal{J}|$ too much then Claim 28 would imply that $\mathcal{Q} \in \text{span}\{\mathcal{J}, \mathbb{C}[V]_2\}$, from which the theorem would follow. We first show how to reduce $|\mathcal{C}_{\langle V \rangle}|$ and then we reduce $|\mathcal{J}_{\langle V \rangle}|$. We will need the following easy observation.

\triangleright **Claim 29.** There is a linear subspace $V \subseteq V'$, of dimension $\dim(V') \leq 1/\delta^4 \cdot \dim(V) \leq 1/\delta^6$, such that $|\mathcal{C}_{\langle V' \rangle}| \leq \delta/10 \cdot m$.

The proof of Claim 29 appears in the full version. Note that it may now be the case that some linear combination of polynomials in \mathcal{J} is now “close” to V' . We therefore perform the following simple process: if $Q \in \text{span}\{\mathcal{J}\}$ is such that for some quadratic L of $\text{rank}(L) = 2$ we have that $P + L \in \langle V' \rangle$ then we can add $\text{Lin}(L)$ to V' and remove one polynomial from \mathcal{J} while still maintaining that $\mathcal{Q} \subset \text{span}\{(\mathcal{Q} \cap \langle V' \rangle), \mathcal{J}, \mathbb{C}[V']_2\}$. As $|\mathcal{J}| = O(1/\delta)$, this does not have much affect on the dimension of V' , which is still $O(1/\delta^4 \cdot \dim(V))$.

To simplify notation, we denote with V the linear space guaranteed by Claim 29. As V may have changed, we update the sets $\mathcal{C}_{[V]}, \mathcal{C}_{\langle V \rangle}, \mathcal{J}_{[V]}$ and $\mathcal{J}_{\langle V \rangle}$ accordingly. By construction of $V = V'$, we now have that $|\mathcal{C}_{\langle V \rangle}| \leq \delta/100m$.

We now complete the proof of Theorem 8 by bounding the dimension of $\mathcal{J}_{\langle V \rangle}$.

\triangleright **Claim 30.** There is a set $\mathcal{J} \subseteq \mathcal{J}' \subset \mathcal{Q}$ such that $|\mathcal{J}'| \leq |\mathcal{J}| + O(1/\delta)$ and $\dim(\mathcal{J}'_{\langle V \rangle}) \leq O(1/\delta + \dim(V)^2)$.

Proof. Denote $\mathcal{T}_1 = \{Q \in \mathcal{J} \mid |\Gamma_{(ii)}(Q)| \geq 0.1\delta m\}$ and $\mathcal{T}_2 = \mathcal{J}_{\langle V \rangle} \setminus \mathcal{T}_1$. For every polynomial in $Q \in \mathcal{J}_{\langle V \rangle}$, denote $Q = Q_{\mathcal{J}} + Q_{\langle V \rangle}$ where $Q_{\mathcal{J}} \in \text{span}\{\mathcal{J}\}$ and $Q_{\langle V \rangle} \in \langle V \rangle$. Note that neither $Q_{\mathcal{J}}$ nor $Q_{\langle V \rangle}$ can be zero as this would imply $Q \in \mathcal{J}_{[V]} \cup \mathcal{C}_{\langle V \rangle}$.

\triangleright **Claim 31.** There is a subset $\mathcal{T}'_1 \subseteq \mathcal{T}_1$ of size at most $10/\delta$ such that $\mathcal{T}_1 \subset \text{span}\{\mathcal{T}'_1, \mathcal{J}, \mathbb{C}[V]_2\}$.

We prove Claim 31 in the full version. Set $\mathcal{T}_2 = \mathcal{T}_2 \setminus \text{span}\{\mathcal{T}_1, \mathcal{J}, \mathbb{C}[V]_2\}$. Every $Q \in \mathcal{T}_2$ must now satisfy that $|\Gamma_i(Q)| \geq 0.9\delta m$. Indeed, this follows from the fact that $Q \notin \mathcal{T}_1$ and that it cannot satisfy Theorem 11iii with any polynomial. Remove from $\Gamma_i(Q)$ all the polynomials in \mathcal{B}_1 , this removes at most $2|\mathcal{B}_1| \leq 2/10\delta m$ polynomials from $\Gamma_i(Q)$ (using an argument similar to Claim 21), leaving $|\Gamma_{(i)}(Q)| \geq 0.7\delta m$. This implies that $\mathcal{K} = \mathcal{T}_2$, $W = \text{span}\{\mathcal{T}_1, \mathcal{J}, \mathbb{C}[V]_2\}$ and $\mathcal{W} = \mathcal{Q} \cap \text{span}\{\mathcal{T}_1, \mathcal{J}, \mathbb{C}[V]_2\}$ satisfy the conditions of Theorem 15. As $\dim(W) \leq O(\dim(V)^2)$ it follows that $\dim(\mathcal{J}_{\langle V \rangle}) \leq O(1/\delta + \dim(V)^2)$.

Setting $\mathcal{J}' = \mathcal{T}'_1 \cup \mathcal{J}$ completes the proof. \triangleleft

We now put everything together and prove Theorem 8.

Proof of Theorem 8. Claims 22, 23 and 24 imply that there exists a set $\mathcal{J} \subseteq \mathcal{Q}$, of size $|\mathcal{J}| = O(1/\delta)$, and a subspace of linear functions V of dimension $\dim(V) = O(1/\delta^2)$ such that $\mathcal{Q} \subset \text{span}\{(\mathcal{Q} \cap \langle V \rangle), \mathcal{J}, \mathbb{C}[V]_2\}$.

By Claims 29 and 30 there are $\mathcal{J} \subseteq \mathcal{J}'$ and $V \subseteq V'$ such that $\dim(V') \leq 1/\delta^4 \cdot \dim(V) \leq 1/\delta^6$ and $|\mathcal{J}'| = O(1/\delta)$, for which it holds that $|\mathcal{C}_{\langle V' \rangle}| \leq \delta/10 \cdot m$ and $\dim(\mathcal{J}'_{\langle V \rangle}) \leq O(1/\delta + \dim(V)^2) = O(1/\delta^8)$. We now set $\mathcal{J} = \mathcal{J}'$, $V = V'$ and, if needed, we add $O(|\mathcal{J}|)$ linear functions to V to make sure that no non-trivial linear combination of polynomials in

\mathcal{J} is of the form $L + F(V)$ where $\text{rank}_s(L) \leq 2$ and $F \in \mathbb{C}[V]_2$, we obtain that $\mathcal{J}_{\langle V \rangle} = \emptyset$ and $|\mathcal{C}_{\langle V \rangle}| \leq \delta m/10$. Claim 28 now guarantees that we also have that $\mathcal{C}_{\langle V \rangle} = \emptyset$. Hence, $\mathcal{Q} = \mathcal{C}_{[V]} \cup \mathcal{J}_{[V]}$ and it follows that $\dim(\text{span}\{\mathcal{Q}\}) \leq |\mathcal{J}| + \dim(V)^2 = O(1/\delta^{16})$. \blacktriangleleft

References

- 1 Manindra Agrawal. Proving lower bounds via pseudo-random generators. In Ramaswamy Ramanujam and Sandeep Sen, editors, *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science, 25th International Conference, Hyderabad, India, December 15-18, 2005, Proceedings*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105. Springer, 2005. doi:10.1007/11590156_6.
- 2 Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 67–75. IEEE Computer Society, 2008. doi:10.1109/FOCS.2008.32.
- 3 Boaz Barak, Zeev Dvir, Avi Wigderson, and Amir Yehudayoff. Fractional Sylvester–Gallai theorems. *Proceedings of the National Academy of Sciences*, 110(48):19213–19219, 2013.
- 4 Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Inf. Comput.*, 222:2–19, 2013. doi:10.1016/j.ic.2012.10.004.
- 5 Peter Borwein and William O. J. Moser. A survey of Sylvester’s problem and its generalizations. *Aequationes Mathematicae*, 40:111–135, 1990. doi:10.1007/BF02112289.
- 6 Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Hardness vs Randomness for Bounded Depth Arithmetic Circuits. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, volume 102 of *LIPICs*, pages 13:1–13:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPICs.CCC.2018.13.
- 7 Zeev Dvir. Incidence theorems and their applications. *Found. Trends Theor. Comput. Sci.*, 6(4):257–393, 2012. doi:10.1561/04000000056.
- 8 Zeev Dvir and Guangda Hu. Sylvester-Gallai for Arrangements of Subspaces. *Discrete & Computational Geometry*, 56(4):940–965, 2016. doi:10.1007/s00454-016-9781-7.
- 9 Zeev Dvir, Shubhangi Saraf, and Avi Wigderson. Improved rank bounds for design matrices and a new proof of Kelly’s theorem. *Forum of Mathematics, Sigma*, 2, 2014. arXiv:1211.0330.
- 10 Zeev Dvir and Amir Shpilka. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM J. Comput.*, 36(5):1404–1434, 2007. doi:10.1137/05063605X.
- 11 Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009. doi:10.1137/080735850.
- 12 Paul Erdős. Problems for Solution: 4065. *The American Mathematical Monthly*, 50(1):65, 1943. URL: <http://www.jstor.org/stable/2304011>.
- 13 Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. A deterministic parallel algorithm for bipartite perfect matching. *Commun. ACM*, 62(3):109–115, 2019. doi:10.1145/3306208.
- 14 Michael A. Forbes. *Polynomial identity testing of read-once oblivious algebraic branching programs*. PhD thesis, Massachusetts Institute of Technology, 2014.
- 15 Michael A. Forbes and Amir Shpilka. Explicit noether normalization for simultaneous conjugation via polynomial identity testing. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*, pages 527–542. Springer, 2013. doi:10.1007/978-3-642-40328-6_37.

- 16 Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct Hitting Sets and Barriers to Proving Lower Bounds for Algebraic Circuits. *Theory of Computing*, 14(1):1–45, 2018. doi:10.4086/toc.2018.v014a018.
- 17 Tibor Gallai. Solution to Problem 4065. *The American Mathematical Monthly*, 51:169–171, 1944.
- 18 Abhibhav Garg, Rafael Oliveira, and Akash Kumar Sengupta. Robust Radical Sylvester-Gallai Theorem for Quadratics. Personal communication, 2021.
- 19 Joshua A. Grochow, Mrinal Kumar, Michael E. Saks, and Shubhangi Saraf. Towards an algebraic natural proofs barrier via polynomial identity testing. *CoRR*, abs/1701.01717, 2017. arXiv:1701.01717.
- 20 Ankit Gupta. Algebraic Geometric Techniques for Depth-4 PIT & Sylvester-Gallai Conjectures for Varieties. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:130, 2014. URL: <http://eccc.hpi-web.de/report/2014/130>.
- 21 Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Satharishi. Arithmetic circuits: A chasm at depth 3. *SIAM J. Comput.*, 45(3):1064–1079, 2016. doi:10.1137/140957123.
- 22 Sten Hansen. A generalization of a theorem of Sylvester on the lines determined by a finite point set. *Mathematica Scandinavica*, 16:175–180, 1965.
- 23 Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute (extended abstract). In Raymond E. Miller, Seymour Ginsburg, Walter A. Burkhard, and Richard J. Lipton, editors, *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA*, pages 262–272. ACM, 1980. doi:10.1145/800141.804674.
- 24 Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004. doi:10.1007/s00037-004-0182-6.
- 25 Zohar S. Karnin and Amir Shpilka. Reconstruction of generalized depth-3 arithmetic circuits with bounded top fan-in. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 274–285. IEEE Computer Society, 2009. doi:10.1109/CCC.2009.18.
- 26 Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 198–207. IEEE Computer Society, 2009. doi:10.1109/FOCS.2009.67.
- 27 Leroy Milton Kelly. A resolution of the Sylvester-Gallai problem of J.-P. Serre. *Discrete & Computational Geometry*, 1(2):101–104, 1986.
- 28 Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of polynomial identity testing and polynomial factorization. *Computational Complexity*, 24(2):295–331, 2015. doi:10.1007/s00037-015-0102-y.
- 29 Mrinal Kumar and Ramprasad Satharishi. Hardness-Randomness Tradeoffs for Algebraic Computation. *Bull. EATCS*, 129, 2019. URL: <http://bulletin.eatcs.org/index.php/beatcs/article/view/591/599>.
- 30 Eberhard Melchior. Über Vielseite der Projektive Ebene. *Deutsche Mathematik*, 5:461–475, 1941.
- 31 Ketan D. Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *J. Amer. Math. Soc.*, 30(1):225–309, 2017.
- 32 Shir Peleg and Amir Shpilka. A Generalized Sylvester-Gallai Type Theorem for Quadratic Polynomials. In Shubhangi Saraf, editor, *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*, volume 169 of *LIPICs*, pages 8:1–8:33. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPICs.CCC.2020.8.

- 33 Shir Peleg and Amir Shpilka. Polynomial time deterministic identity testing algorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits via edelstein-kelly type theorem for quadratic polynomials. *CoRR*, abs/2006.08263, 2020. [arXiv:2006.08263](https://arxiv.org/abs/2006.08263).
- 34 Nitin Saxena. Progress on polynomial identity testing. *Bulletin of EATCS*, 99:49–79, 2009. URL: <https://eccc.weizmann.ac.il/report/2009/101/>.
- 35 Nitin Saxena. Progress on polynomial identity testing-ii. In M. Agrawal and V. Arvind, editors, *Perspectives in Computational Complexity: The Somenath Biswas Anniversary Volume*, Progress in Computer Science and Applied Logic, pages 131–146. Springer International Publishing, 2014. URL: <https://books.google.co.il/books?id=U7ApBAAAQBAJ>.
- 36 Nitin Saxena and Comandur Seshadhri. Blackbox identity testing for bounded top-fan-in depth-3 circuits: The field doesn't matter. *SIAM J. Comput.*, 41(5):1285–1298, 2012. doi:10.1137/10848232.
- 37 Nitin Saxena and Comandur Seshadhri. From sylvester-gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *J. ACM*, 60(5):33, 2013. doi:10.1145/2528403.
- 38 Jean-Pierre Serre. Advanced Problems: 5359. *The American Mathematical Monthly*, 73(1):89, 1966. URL: <http://www.jstor.org/stable/2313941>.
- 39 Amir Shpilka. Interpolation of depth-3 arithmetic circuits with two multiplication gates. *SIAM J. Comput.*, 38(6):2130–2161, 2009. doi:10.1137/070694879.
- 40 Amir Shpilka. Sylvester-Gallai type theorems for quadratic polynomials. *Discrete Analysis*, 13, 2020.
- 41 Amir Shpilka and Amir Yehudayoff. Arithmetic Circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010. doi:10.1561/04000000039.
- 42 Gaurav Sinha. Reconstruction of Real Depth-3 Circuits with Top Fan-In 2. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPICs*, pages 31:1–31:53. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. doi:10.4230/LIPICs.CCC.2016.31.
- 43 Ola Svensson and Jakub Tarnawski. The Matching Problem in General Graphs Is in Quasi-NC. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 696–707. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.70.
- 44 James Joseph Sylvester. Mathematical question 11851. *Educational Times*, pages 59–98, 1893.