Robust Radical Sylvester-Gallai Theorem for Quadratics

Abhibhav Garg
Cheriton School of Computer Science, University of Waterloo, Canada
Rafael Oliveira[1]
Cheriton School of Computer Science, University of Waterloo, Canada
Akash Kumar Sengupta
Department of Mathematics, Columbia University, New York, NY, USA

Abstract

We prove a robust generalization of a Sylvester-Gallai type theorem for quadratic polynomials. More precisely, given a parameter $0 < \delta \leq 1$ and a finite collection $\mathcal{F}$ of irreducible and pairwise independent polynomials of degree at most 2, we say that $\mathcal{F}$ is a $(\delta, 2)$-radical Sylvester-Gallai configuration if for any polynomial $F_i \in \mathcal{F}$, there exist $\delta(|\mathcal{F}| - 1)$ polynomials F_j such that $|\mathrm{rad}\,(F_i, F_j) \cap \mathcal{F}| \geq 3$, that is, the radical of F_i, F_j contains a third polynomial in the set.
We prove that any $(\delta, 2)$-radical Sylvester-Gallai configuration $\mathcal{F}$ must be of low dimension: that is

$$\dim \mathrm{span}_{\mathbb{C}} \{\mathcal{F}\} = \mathrm{poly}\,(1/\delta)\,.$$

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory; Theory of computation → Computational geometry

Keywords and phrases Sylvester-Gallai theorem, arrangements of hypersurfaces, locally correctable codes, algebraic complexity, polynomial identity testing, algebraic geometry, commutative algebra

Digital Object Identifier 10.4230/LIPIcs.SoCG.2022.42

Related Version *Full Version*: `https://arxiv.org/abs/2203.05532`

Independent result

We would like to remark that, independently and simultaneously to our work, [21] have also proved that $(\delta, 2)$-radical Sylvester-Gallai configurations must be of low dimension. Both works have been presented in a common talk at CG week 2022. For a more detailed comparison between both works, we refer the reader to Section 1.3.

1 Introduction

Suppose $v_1, \ldots, v_m \in \mathbb{R}^n$ is a set of m distinct points, such that the line joining any two points in the set contains a third point. In 1893, Sylvester asked if such configurations of points are necessarily colinear [26]. Independently, this same question was asked by Erdös in 1943 [9]. This was proved by [17], and independently by Gallai [10], where the latter was in response to Erdös. This result is now known as the Sylvester-Gallai theorem. A set of points satisfying the above is called a Sylvester-Gallai (SG) configuration.

Sylvester-Gallai theorems depend on the base field. For instance, it is well known that any nonsingular planar cubic curve over $\mathbb{C}$ has nine inflection points, and that any line passing through two such points passes through a third [5]. These nine points are not collinear,

[1] corresponding author

38th International Symposium on Computational Geometry (SoCG 2022).
Editors: Xavier Goaoc and Michael Kerber; Article No. 42; pp. 42:1–42:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

and therefore form a counterexample to the Sylvester-Gallai theorem when the underlying field is changed from $\mathbb{R}$ to $\mathbb{C}$. In 1966, Serre asked if there are configuration of points in $\mathbb{C}^n$ that satisfy the Sylvester-Gallai that are not coplanar [23]. Kelly [15] proved that no such configurations can exist, or equivalently that points in $\mathbb{C}^n$ that satisfy the Sylvester-Gallai property are always coplanar.

Over finite fields, Sylvester-Gallai configurations do not have bounded dimension. For example, if we are working over the field $\mathbb{F}_p$ (with $p > 2$) and our vector space is $\mathbb{F}_p^n$, then the set of points is $\mathbb{F}_p^n$ is a SG configuration of dimension n, which is not constant. In general, any subgroup of $\mathbb{F}_p^n$ will form a Sylvester-Gallai configuration. Some bounds on the dimension of configurations in this setting can be found in [7]. In this work, we only focus on fields of characteristic zero, and to make presentation easier we restrict our attention to $\mathbb{C}$.

Several variations and generalizations of the Sylvester-Gallai problem defined above have been studied in combinatorial geometry. The underlying theme in all these types of questions is the following:

Are Sylvester-Gallai type configurations always low-dimensional?

In characteristic zero, the answer has always turned out to be yes. For a thorough survey of the earlier works on SG-type theorems, we refer the reader to [2] and results therein.

While the above results are mathematically beautiful and interesting on their own right, it is also interesting and useful in areas such as computer science and coding theory to consider higher-dimensional analogs as well as robust analogs of SG type theorems.

Higher-dimensional analogs of SG configurations. In [12], a higher dimensional version of the theorem was proved, with lines replaced by flats. This variant has applications in the study of algebraic circuits, and in particular in Polynomial Identity Testing (PIT) [14, 22], a central problem in algebraic complexity theory. The works [14, 22] use the higher dimensional Sylvester-Gallai theorems to bound the “rank” of certain types of depth three circuits.[2] In simple terms, if the linear forms of a circuit satisfy the high dimensional SG condition, then in essence the polynomial being computed must depend on a constant number of variables, in which case it is easy to check whether the circuit is computing a non-zero polynomial.

Robust analogs of SG configurations and applications. Robust generalizations of the Sylvester-Gallai theorem have found applications in coding theory and in complexity theory.

In this variant, for every point v_i there are at least $\delta(m-1)$ points $u_1, \dots, u_k$ such that v_i and u_k span a third point. The usual Sylvester-Gallai theorem is the case when $\delta = 1$. Such configurations were first studied by Szemerédi and Trotter [27], who proved that if δ is bigger than an absolute constant close to 1, then the configuration has constant dimension.

In [1], the authors prove that such a configuration has dimension $\mathcal{O}\left(1/\delta^2\right)$, for any $0 < \delta \leq 1$. This robust version also allows them to prove robust versions of the higher dimensional variants, and average case versions of the theorem. They also define the notion of a *LCC*-configuration, which is an extension of the Sylvester-Gallai configuration where points are allowed to occur with multiplicity. In [8], the authors improve the bound on the dimension of robust Sylvester-Gallai configurations to $\mathcal{O}\left(1/\delta\right)$.

In coding theory, these robust configurations naturally appear in the study of locally decodable codes and locally correctable codes [1]. These results, as well as similar results are surveyed in [7]. They also have applications in the study of algebraic circuits, in particular in reconstruction of algebraic circuits [25].

[2] Algebraic circuits which compute polynomials that can be written as a sum of products of linear forms.

Higher degree generalizations of Sylvester-Gallai configurations. Also motivated by the PIT problem, Gupta in [11] introduced higher degree analogs of Sylvester-Gallai configurations, and asked if they are also "low dimensional." In his paper, Gupta outlines a series of conjectures, and gives a deterministic polynomial-time blackbox PIT algorithm for a special class of algebraic circuits[3] assuming that these conjectures hold.

The first challenge in Gupta's series of conjectures on SG type theorems is the following:

▶ **Conjecture 1** (Conjecture 29, [11])**.** *Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible, homogeneous, and of degree at most d such that for every pair Q_i, Q_j there is a k such that $Q_k \in \operatorname{rad}(Q_i, Q_j)$. Then the transcendence degree of $Q_1, \ldots, Q_m$ is $\mathcal{O}(1)$ (where the constant depends on the degree d).*

The case of $d = 2$ for the above conjecture was proved in [24]. We henceforth refer to the original Sylvester-Gallai theorem (the case $d = 1$) and its variants as the "linear case". As in the linear case of SG type problems, it is natural to consider the robust version of the above lemma as a next step towards the conjectures of Gupta that give an algorithm for a special case of PIT. We resolve the robust version of the above conjecture in the case when $d = 2$.

1.1 Main results

In this section, we formally state our main result: robust quadratic radical Sylvester-Gallai configurations must lie in a constant dimensional vector space.[4] In particular, this result implies that the polynomials must be contained in a small algebra, and also that they have constant transcendence degree. Another important result is a structural result for ideals generated by two quadratic forms.

1.1.1 Robust radical Sylvester-Gallai theorem

We first formally define robust quadratic radical Sylvester-Gallai configurations. Henceforth, as is customary in the literature, we will use *form* to denote homogeneous polynomials. For a polynomial ring $S = \mathbb{C}[x_1, \ldots, x_n]$, we let S_d denote the vector space of polynomials of degree d in S, and the ideal generated by a set of polynomials $f_1, \cdots, f_r$ is denoted as $(f_1, \cdots, f_r)$. We also use $\operatorname{rad}(f_1, \ldots, f_r)$ to denote the radical of this ideal, that is, the set of polynomials g such that $g^k \in (f_1, \ldots, f_r)$ for some k.

▶ **Definition 2** ($(\delta, 2)$-rad-SG configurations)**.** *Let $0 < \delta \leq 1$ and $\mathcal{F} := \{F_1, \ldots, F_m\}$ be a set of irreducible forms in the polynomial ring $S = \mathbb{C}[x_1, \ldots, x_n]$. We say that $\mathcal{F}$ is a $(\delta, 2)$-rad-SG configuration if the following conditions hold:*

1. $\mathcal{F} \subset S_1 \cup S_2$ *(only linear and quadratic forms)*
2. *for any $i \neq j$, we have that $F_i \notin (F_j)$*
3. *for any $i \in [m]$, there are $\delta(m-1)$ indices $j \in [m] \setminus \{i\}$ such that $|\operatorname{rad}(F_i, F_j) \cap \mathcal{F}| \geq 3$.*

We are now ready to formally state the main contributions of our paper. We begin with our main theorem, that robust quadratic radical SG configurations must have small linear span.

▶ **Theorem 3** ($(\delta, 2)$-rad-SG theorem)**.** *If $\mathcal{F}$ is a $(\delta, 2)$-rad-SG configuration, then*

$$\dim(\operatorname{span}_{\mathbb{C}} \{\mathcal{F}\}) = O(1/\delta^{54}).$$

[3] These are circuits computed by a sum of constantly many products of constant degree polynomials.
[4] Our results hold for any algebraically closed field of characteristic zero. However, for simplicity of exposition, we only state our results over $\mathbb{C}$.

To prove the theorem above, we first notice that the theorem would imply that the forms in the configuration are contained in a subalgebra of the polynomial ring of small dimension, namely the subalgebra generated by a linear basis of the given configuration. With this observation at hand, we provide a principled approach to construct small dimensional subalgebras of the polynomial ring which control the configuration (in the sense that all forms in the configuration will become a "univariate form" with coefficients from our subalgebra).

The main property of these algebras is that they allow us to translate non-linear SG dependencies (the radical dependencies) into linear SG dependencies, and therefore we can reduce our non-linear problem to the linear version of the SG problem.

The main principle guiding the construction of our subalgebras is that we would like these subalgebras to look "as free as possible" without increasing the dimension of the algebra by much. The amount of "freeness" that we need is captured by the robust algebras defined in Section 2, where we also elaborate on how these algebras behave with SG configurations (where we need the notion of clean algebras). For more intuition on how we prove the theorem, we refer the reader to Section 1.2.

1.1.2 Results on structure of ideals generated by two quadratics

A key step in our strategy to prove that a SG configuration is low dimensional (as has also been the first step in the works of [24, 19]) is to understand the structure of ideals generated by two quadratic forms.

The general principle at play here is that if the ideal generated by two quadratic forms is not radical or prime, then there must be a low-rank quadratic in their span. In [24, 19], the authors proved similar structural results to determine when a product of quadratic forms is contained in an ideal generated by two quadratic forms. In Proposition 4, we use a different approach to completely characterize when the ideal generated by two quadratic forms is radical or prime, and as corollaries we obtain the structural results in [24, 19]. We use a commutative-algebraic approach to develop a further understanding of the radical of ideals generated by two irreducible quadratics. Indeed, using the standard tools of primary decomposition and Hilbert-Samuel multiplicity we obtain a classification of the possible minimal primes of an ideal generated by two quadratic forms. Consequently we obtain a characterization for such an ideal to be prime or radical. This approach can also be generalized to ideals generated by cubic forms ([18]).

▶ **Proposition 4** (Radical Structure). *Let $\mathbb{K}$ be an algebraically closed field of characteristic zero and $Q_1, Q_2 \in S = \mathbb{K}[x_1, \cdots, x_n]$ be two forms of degree 2. Then one of the following holds:*

1. *The ideal (Q_1, Q_2) is prime.*
2. *The ideal (Q_1, Q_2) is radical, but not prime. Furthermore, one of the following cases occur:*
   - **(a)** *There exist two linearly independent linear forms $x, y \in S_1$ such that $xy \in \mathrm{span}(Q_1, Q_2)$.*
   - **(b)** *There exists a minimal prime $\mathfrak{p} \supset (Q_1, Q_2)$, such that $\mathfrak{p} = (x, y)$ for some linearly independent forms $x, y \in S_1$*
3. *The ideal (Q_1, Q_2) is not radical and one of the following cases occur:*
   - **(a)** *Q_1, Q_2 have a common factor and $Q_1 = xy$, $Q_2 = x(\alpha x + \beta y)$ for some linear forms x, y and $\alpha, \beta \in k$. In this case, we have $x^2 \in \mathrm{span}(Q_1, Q_2)$.*
   - **(b)** *Q_1, Q_2 do not have a common factor. There exists a minimal prime $\mathfrak{p} \supset (Q_1, Q_2)$ such that $\mathfrak{p} = (x, Q)$, where $x \in S_1$, $Q \in S_2$ and Q is irreducible modulo x, and we also have $x^2 \in \mathrm{span}(Q_1, Q_2)$.*

(c) *Q_1, Q_2 do not have a common factor and there exists a minimal prime $\mathfrak{p} \supset (Q_1, Q_2)$, such that $\mathfrak{p} = (x, y)$ for some linearly independent forms $x, y \in S_1$, and the (x, y)-primary ideal $\mathfrak{q}$ has multiplicity $e(S/\mathfrak{q}) \geq 2$.*

The proposition above is not new, and proofs of some of the statements can be found in [4, Section 1] and [13, Chapter XIII]. For completeness, we provide a proof of this proposition using primary decomposition and Hilbert-Samuel multiplicity of an ideal. In the former, the authors study the cycle decomposition of the intersection of two quadric hypersurfaces to obtain results about existence of rational points on intersection of two quadric hypersurfaces and Châtelet surfaces over number fields. Our statements here are slightly simpler to state (and slightly different) since in the works above the authors work in the more general setting of perfect fields, and we are only concerned with algebraically closed fields of characteristic zero.

1.2 Sketch of the proof of Theorem 3

In this section, we give a sketch of the proof of our main theorem. Suppose we are given a $(\delta, 2)$-rad-SG configuration $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$, where $\mathcal{F}_d$ is the set of forms of degree d in our configuration. We will show that there is a small subalgebra of the polynomial ring that contains $\mathcal{F}$. That is, we will construct a subalgebra $\mathbb{C}[y_1, \cdots, y_s, Q_1, \cdots, Q_t]$ generated by linear forms y_i and quadratic forms Q_j, such that $\mathcal{F} \subset \mathbb{C}[y_1, \cdots, y_s, Q_1, \cdots, Q_t]$ and $s + t = O(1/\delta^{27})$. Then it will follow that $\dim(\mathrm{span}_{\mathbb{C}}\{\mathcal{F}\})$ is at most $O(1/\delta^{54})$, since every quadratic form in this algebra is a linear combination of the forms Q_j and pairwise products of the forms y_i.

A motivating special case. Our strategy to prove the robust radical SG theorem is based on the following toy example. Suppose our polynomial ring is $\mathbb{C}[x_1, \ldots, x_r, y_1, \ldots, y_s]$, where one should think of s being constant and $r \gg s$, and every quadratic form Q in our configuration is a polynomial which is "univariate" over the smaller polynomial ring $\mathbb{C}[y_1, \ldots, y_s]$. That is, for each quadratic Q, there exists a linear form $x_Q \in \mathrm{span}_{\mathbb{C}}\{x_1, \ldots, x_r\}$ such that $Q \in \mathbb{C}[x_Q, y_1, \ldots, y_s]$. In this case, one would hope that the *non-linear* SG dependencies involving our configuration $\mathcal{F}$ would imply *linear* SG dependencies for the set of linear forms $\mathcal{F}_1 \cup \{x_Q \mid Q \in \mathcal{F}_2\}$. If we manage to prove that the latter set of linear forms is a *robust linear SG configuration*, we can invoke the robust SG theorem for linear forms of [1, 8] to bound the dimension of $\mathrm{span}_{\mathbb{C}}\{\mathcal{F}_1 \cup \{x_Q \mid Q \in \mathcal{F}_2\}\}$. Thus we may take our small subalgebra to be the subalgebra generated by $y_1, \cdots, y_s$ and $\mathcal{F}_1 \cup \{x_Q \mid Q \in \mathcal{F}_2\}$.

Small subalgebras. In general it is not always possible to reduce the general robust radical SG problem for quadratics to the toy example above.[5] However we will be able to construct a small subalgebra of our polynomial ring which is just as good as the small polynomial ring $\mathbb{C}[y_1, \ldots, y_s]$ in the toy example above. Additionally, we will not always be able to reduce the non-linear problem to a robust linear SG configuration. Instead of a robust linear SG configuration, we will reduce it to a δ-LCC configuration of [1].

Since the main counterexample to the above toy example are quadratics of large rank, the small subalgebras that we construct will have both linear and quadratic forms as generating elements. Therefore, it is natural to consider the vector space of forms generating the algebra,

[5] For instance if the polynomial $Q = \sum_{i=1}^{s} x_i y_i$ is in our SG configuration.

which we denote by $V := V_1 + V_2$, where V_1 is the vector space of linear forms in the algebra and V_2 is the vector space of quadratic *generators* of the algebra. The main idea here is that the quadratic generators will be composed only of quadratics of high rank, which can essentially be though of as "free variables." As it turns out, intuitively and informally, the only properties that we need from the vector space above are that:

1. the quadratics in V_2 are "robust" against the linear forms in V_1. That is, we would like each quadratic in V_2 to be of very high rank even if we subtract from it polynomials from the algebra $\mathbb{C}[V_1]$
2. V is in a sense "saturated" with respect to our configuration $\mathcal{F}$. That is, there exists no small vector space of linear forms that we can add to V_1 that would add many polynomials of $\mathcal{F}$ to the algebra $\mathbb{C}[V]$, or "make them closer to being in $\mathbb{C}[V]$."

The first condition ensures that any quadratic from our set $\mathcal{F}$ which "depends" on a form from V_2 must be of high rank, while the second condition ensures that there is no trivial way to increase the algebra slightly in order to have a lot more forms from $\mathcal{F}$ inside of the larger algebra. We call any vector space which satisfies the conditions above a *clean vector space* with respect to $\mathcal{F}$. The formal definition of these vector spaces and the results needed can be found on Section 2.

Univariate over an intermediate small subalgebra. First we construct an intermediate small subalgebra $\mathbb{C}[V]$ such that any polynomial in $\mathcal{F}$ is either contained in $\mathbb{C}[V]$ or it is univariate over $\mathbb{C}[V]$. To construct the subalgebra above, we need to understand in a bit more detail the structure of the radical of an ideal generated by two quadratic forms. To this end, we prove Proposition 4, generalizing the previous structure theorems from [24, 19]. Additionally, we also assemble results on the structure of minimal primes of these ideals to construct our algebra.

With Proposition 4 (our main structural result) at hand, we proceed similarly to [24, 19] by partitioning the quadratics in our $(\delta, 2)$-rad-SG configuration $\mathcal{F}$ into four subsets, each satisfying a particular case of our structure theorem. Taking $\varepsilon = \delta/10$, we define

1. $\mathcal{F}_{\text{span}}$ is the set of quadratics Q which satisfy a "span dependency" with at least ε-fraction of the polynomials. That is, there exist many quadratics $F, G \in \mathcal{F}$ such that $G \in \text{span}_{\mathbb{C}}\{Q, F\}$.
2. $\mathcal{F}_{\text{linear}}$ is the set of quadratics Q which satisfy case 3 (c) of Proposition 4 with at least an ε-fraction of the other polynomials. That is, there are many quadratics $F \in \mathcal{F}$ and linear forms x, y such that $(Q, F) \subset (x, y)$, and this minimal prime has multiplicity ≥ 2.
3. $\mathcal{F}_{\text{deg}}$ is the set of quadratics Q which have an ε-fraction of its SG dependencies with linear forms.[6]
4. $\mathcal{F}_{\text{square}}$ is the set of quadratics Q which satisfy case 3 (b) of Proposition 4 with at least $(\delta - 3\varepsilon)$-fraction of the other polynomials. That is, there are many quadratics $F \in \mathcal{F}$ such that there is a linear form ℓ such that $\ell^2 \in \text{span}_{\mathbb{C}}\{F, Q\}$.

With this partition, we construct a small clean vector space V such that $\mathcal{F}_{\text{square}}$ and $\mathcal{F}_{\text{linear}}$ are entirely contained in the algebra $\mathbb{C}[V]$, and the forms in the remaining subsets are either in $\mathbb{C}[V]$, or are univariate over $\mathbb{C}[V]$. Here, by univariate over $\mathbb{C}[V]$, we mean that there is a linear form $z \notin V_1$ such that the polynomial is in the algebra $\mathbb{C}[V][z]$.

[6] Deg stands for the degenerate case.

Construction of the intermediate small subalgebra. We construct the subalgebra above in four steps, where in each step we construct intermediate subalgebras which handle one of the subsets of quadratics defined above. We use two strategies in the construction: iterative processes similar to the ones in [24, 19], and double covers of the SG dependencies. These two strategies allow us to construct algebras generated by poly $(1/\delta)$ many elements with the desired properties for each of the subsets above. The iterative processes allow us to tightly control $\mathcal{F}_{\text{square}}$ and obtain some control over $\mathcal{F}_{\text{linear}}$ and $\mathcal{F}_{\text{span}}$, whereas the double covers allow us to handle $\mathcal{F}_{\text{deg}}$ and also to prove that the remaining linear forms will become a δ-LCC configuration.

The final small subalgebra. Once we have our clean subalgebra with respect to $\mathcal{F}$, and every polynomial in $\mathcal{F}$ either in the subalgebra or univariate over our subalgebra, we proceed to prove that the "additional linear forms" that arise in this way, together with the linear forms from our configuration, span a vector space of small dimension. While these linear forms satisfy linear relations, the linear forms corresponding to different quadratics in our set might be the same, and therefore the set of linear forms might not form a robust linear Sylvester-Gallai configuration. However, the fact that the vector space V is saturated implies that not too many quadratics have the same linear form: if they did, then we could add that linear form to V_1 and add many polynomials of $\mathcal{F}$ to $\mathbb{C}[V]$. This saturation allows us to show that the linear forms form a δ-LCC configuration, and therefore span a vector space of small dimension. We extend our algebra $\mathbb{C}[V]$ by adjoining the generators of this small vector space to obtain the final small subalgebra containing $\mathcal{F}$ as desired.

1.3 Related work

The original motivation for studying higher degree SG configurations comes from [11], in order to give polynomial time PIT for a special class of depth-4 algebraic circuits. The most general SG problem/configuration that is needed towards this application is the following conjecture. As we mentioned earlier, Conjecture 1 is a first step towards the proof of this conjecture. The most general form of Gupta's conjecture [11, Conjecture 1], which we term as (k, d, c)-Sylvester-Gallai conjecture, is stated below.

▶ **Conjecture 5** ((k, d, c)-Sylvester-Gallai conjecture). *Let $k, d, c \in \mathbb{N}^*$ be parameters, and let $\mathcal{F}_1, \dots, \mathcal{F}_k$ be finite sets of irreducible polynomials of degree at most d such that*

- $\cap_i \mathcal{F}_i = \emptyset$,
- *for every $Q_1, \dots, Q_{k-1}$ each from a distinct set $\mathcal{F}_{i_j}$, there are polynomials $P_1, \dots, P_c$ in the remaining set such that $\prod P_i \in \text{rad}(Q_1, \dots, Q_{k-1})$.*

Then the transcendence degree of the union $\cup_i \mathcal{F}_i$ is a function of k, d, c, independent of the number of variables or the size of the sets $\mathcal{F}_i$.

As a step towards the proof of Conjecture 5, [24] studies quadratic Sylvester-Gallai configurations (Conjecture 1). The configurations we study are exactly the fractional versions of these quadratic Sylvester-Gallai configurations. In [19], the authors extend the result on quadratic Sylvester-Gallai configurations, weakening the Sylvester-Gallai condition, only requiring that the radical of the ideal generated by every pair of quadratics contains a product of four other quadratics. In [20], the authors extend this further, by proving Conjecture 5 for the case of $k = 3, d = 2$ and $c = 4$, which gives a polynomial time blackbox PIT for algebraic circuits computing a sum of three products of quadratic polynomials.

Our proof techniques and intermediate results generalise some of those of [24], [19], [20]. In [24], the author proves a structural result for quadratic forms contained in the radical of the ideal generated by two other quadratic forms. In [19], this result is extended to products of quadratics. Our structure result directly classifies the radical of the ideal generated by two quadratics based on the number and degree of the minimal primes of the ideal. Both structure theorems of [24] and [19] follow as immediate corollaries.

Further, our definition of clean vector spaces and the clean up procedure is a generalisation of part of the strategy in the above works. In [24, 19], the authors construct two vector spaces: one of linear forms and another of quadratic forms, and then they prove that most polynomials in the configuration can be written as the sum of a quadratic polynomial in the second vector space, and a polynomial "close" to the algebra generated by the first vector space. Our definition of clean vector spaces formalizes this strategy, giving us more structure which helps us unify the case analysis in these previous works.

Another important point to notice is that in this paper we do not make use of the projection trick used in [24, 19]. While the parameters become slightly worse for not using the projection trick, as we now have to account for repetitions in the set of linear forms not in the algebra, we believe that getting rid of the projection trick will make this strategy more amenable to generalizations to higher degree.

Progress on Polynomial Identity Testing. Recently, there has been remarkable progress on the PIT problem for depth 4 circuits (the same algebraic circuits considered in [11]). In [6], the authors give a quasi-polynomial time algorithm for blackbox PIT for depth 4 circuits with bounded top and bottom fanins. Their approach involves considering the logarithmic derivative of circuits, and is analytic in nature, which allows them to bypass the need of Sylvester-Gallai configurations. Another PIT result in this setting comes from the lower bound against low depth algebraic circuits proved by [16], which gives a weakly-exponential algorithm for PIT for these circuits via the hardness vs randomness paradigm for constant depth circuits [3]. However, the SG approach of [11] is the only one so far which could yield polynomial-time blackbox PIT algorithms for the subclass of depth-4 circuits with constant top and bottom fanins.

Comparison with [18]. In [18] the authors prove the radical SG theorem for cubic forms (not the robust version). Their work is on one hand more general, since they are now handling cubic forms as well, but it is less general in that their SG theorem is not robust, and the robustness - as we have seen, significantly increases the complexity of the problem (as it is the case in every setting, even in the linear case). In their work, the authors proceed with a similar strategy as the previous works and this one, by proving a structure theorem for ideals generated by two cubics, and then constructing a "robust algebra" where the forms become "univariate" with respect to it. Some of the ideas in this paper are motivated by similar constructions done in their work. More precisely, their construction of wide algebras motivated our construction of clean vector spaces, where the difference between the constructions is that in their work they need stronger algebro-geometric properties of their algebras, but to achieve that their algebras must be significantly larger than the ones we construct in this paper. Apart from this motivation, both works are distinct in their techniques, since in our case the robustness severely constrains our choice of dependencies.

Simultaneous result [21]. Simultaneously and independently from this work, Peleg and Shpilka have also proved that $(\delta, 2)$-rad-SG configurations have $\mathrm{poly}(1/\delta)$ dimension. While the result of [21] in its current form works when the configuration only has irreducible quadratics, in our work we also allow linear forms in our configurations.

There are a number of parallels between the methods used in [21] and the ones used in our paper. Both use structure theorems for ideals generated by quadratics, and structure theorems for (x, y)-primary ideals. Further, both results divide the configuration into special sets based on the cases of the structure theorem, and control each of these sets separately.

One key technical difference between our approach and [21] is the structure used to control the above sets. In [21] they use an algebra generated by linear forms and quadratics with the property that linear combinations of quadratics are high rank even after taking quotients with the linear forms. We define the notion of clean vector spaces, which generate "special algebras" which apart from having the above property (what we call robustness) are also saturated in the sense that adding a few linear forms cannot bring too many polynomials in our configuration "closer" to the vector space. We also use the notion of univariate polynomials over clean vector spaces, and prove the existence of a small clean vector space V such that the polynomials in each special set is univariate over V. Once we have such structure, we can assign to each univariate polynomial a linear form ℓ_i (the "extra variable" from this polynomial), and we then show that the set of linear forms $\{\ell_i\}$ corresponding to each polynomial forms a LCC configuration.

Another key technical difference is that in our work, we **do not** make use of the *projection method*, as we believe that in higher degrees such method may not be amenable to generalization without generalizing the SG conjectures as well. This is one of the main reasons why we can only prove that the univariate polynomials ℓ_i form a LCC configuration, instead of a robust linear SG configuration. This in turn is also the reason that our bound is worse than the one in [21].

Handling the linear forms presents an extra technical challenge. The main difficulty arises when a quadratic Q satisfies the SG condition with many linear forms ℓ, as there is less structure between Q, ℓ and the quadratic in $\mathrm{rad}\,(Q, \ell)$ than when the configurations just consist of quadratics. This lack of structure makes our analysis significantly more intricate.

1.4 Organization

In Section 2 we state the formal definitions of robust and clean vector spaces. In Section 3 we state the condition we want our small algebra (as described in Section 1.2) to satisfy, and how this implies the main theorem. Finally, in Section 4 we state some concluding remarks, and list a number of open problems and further directions. Due to space limitations, all proofs and detailed discussions are omitted from this article, and can be found in the full version on arxiv.

2 Clean vector spaces

In this section we formally define the notions of robust and clean vector spaces as described in the introduction. We refer to the full version for examples, further details and related statements. We begin with a definition of polynomials which are close to being in the algebra generated by a vector space of forms. Recall that $S = \mathbb{C}[x_1, \ldots, x_n]$, and that S_d refers to the vector space of polynomials of degree d.

▶ **Definition 6** (Polynomials close to a vector space). *Given a vector space $V = V_1 + V_2$ where $V_i \subseteq S_i$ we say that a quadratic P is s-*close *to V if there is a polynomial $Q \in \mathbb{C}[V]$ such that $\mathrm{rank}(P - Q) = s$, and for any polynomial $Q' \in \mathbb{C}[V]$, we have that $\mathrm{rank}(P - Q') \geq s$. If a polynomial P is not r-close to V, for any $r \leq s$, we say that P is s-*far *from V.*

With the definition above in hand, we are ready to define robust vector spaces. These are vector spaces whose quadratic forms are in a sense far from the ideal generated by the linear forms.

▶ **Definition 7** (Robust vector spaces). *A vector space $V = V_1 + V_2$ where $V_i \subset S_i$ is said to be r-robust if, for any nonzero $Q \in V_2$, the following conditions hold:*

1. *Q is $(r-1)$-far from V_1*
2. *if $Q \notin (V_1)$, then $\text{rank}(\overline{Q}) \geq r$, where $\overline{Q} \in S/(V_1)$ denotes the image of Q in the quotient ring $S/(V_1)$.*

If a homogeneous ideal I has a generating set $V_1 + V_2$ which is r-robust, we say that I is an r-robust ideal.

In the above definition, we use the fact that the quotient ring $S/(V_1)$ is isomorphic to a polynomial ring, in order to define $\text{rank}(\overline{Q})$. Next we define the relative vector space of a quadratic form and the notion of a polynomial being univariate over a vector space. We refer to the full version for statements regarding well-definedness of these notions.

▶ **Definition 8** (Vector space of a quadratic form). *Let Q be a quadratic form of rank s, so that $Q = \sum_{i=1}^{s} a_i b_i$. Define the vector space $\text{Lin}(Q) := \text{span}_{\mathbb{C}}\{a_1, \dots, a_s, b_1, \dots, b_s\}$. Define $\mathbb{L}(Q)$ as:*

$$\mathbb{L}(Q) = \begin{cases} \text{span}_{\mathbb{C}}\{Q\}, & \textit{if } s \geq 5 \\ \text{Lin}(Q), & \textit{otherwise.} \end{cases}$$

▶ **Definition 9** (Relative space of linear forms). *If V is an r-robust vector space and P is s-close to V for $s < r/2$ we can define*

$$\mathbb{L}_V(P) := \begin{cases} \mathbb{L}(P-Q) + V_1, & \textit{if } s \leq 4 \\ \text{span}_{\mathbb{C}}\{P\}, & \textit{otherwise} \end{cases}$$

where $Q \in \mathbb{C}[V]$ is a polynomial such that $\text{rank}(P-Q) = s$. We also define the quotient space

$$\overline{\mathbb{L}}_V(P) := \begin{cases} \mathbb{L}_V(P)/V_1, & \textit{if } s \leq 4 \\ 0, & \textit{otherwise} \end{cases}$$

▶ **Definition 10** (Univariate polynomials over robust vector spaces). *Let $V := V_1 + V_2$ be an r-robust vector space, where $r \geq 3$ and $V_i \subseteq S_i$, for $i \in \{1, 2\}$. We say that a form P is* univariate over *V if P is 1-close to V and $\dim\left(\overline{\mathbb{L}}_V(P)\right) = 1$. Moreover, we define $z_P \in S_1/V_1$ to be the linear form such that $\overline{\mathbb{L}}_V(P) := \text{span}_{\mathbb{C}}\{z_P\}$.*

We are now ready to define the main object of this section: *clean vector spaces*. The subalgebras that we construct in the proof of the Theorem 3 will be algebras generated by clean vector spaces. The cleanliness conditions imply that the quadratic generators are of high rank and that one can not add a small number of linear forms to a clean vector space V to increase the algebra $\mathbb{C}[V]$ such that the new algebra contains a lot of new polynomials from $\mathcal{F}$. The second condition will be the key to reduce the radical-SG-condition to a linear-SG condition once we show that our polynomials are univariate over a clean vector space.

▶ **Definition 11** (Clean vector spaces). *Let $\mathcal{F} := \{Q_1, \dots, Q_m\} \subset S_1 \cup S_2$ be a set of forms and $r \geq 17$ be an integer. Let $V = V_1 + V_2$ be a vector space with $V_i \subset S_i$. We say that V is an (r, ε)-clean vector space over $\mathcal{F}$ if the following conditions hold:*

1. *V is an r-robust vector space*
2. *For any $U_1 \subset S_1$ such that $\dim(U_1) \leq 8$, there are $< \varepsilon m$ polynomials $Q_j \in \mathcal{F}$ such that Q_j is s-close to V for $1 \leq s \leq 4$ and*

$$\dim\left(\mathbb{L}_V(Q_j)\right) > \dim\left(\mathbb{L}_{V+U_1}(Q_j)\right).$$

If $V = V_1 + V_2$ is an (r, ε)-clean vector space over $\mathcal{F}$, then we say that the ideal (V) is an (r, ε)-clean ideal over $\mathcal{F}$, and similarly the algebra $\mathbb{C}[V]$ is an (r, ε)-clean algebra over $\mathcal{F}$.

3 Proof of Theorem 3

In this section we formalize the sketch of the proof given in the introduction. We refer to the full version for the formal definitions and proofs of the lemmas below. We use the partition of $\mathcal{F}_2 = \mathcal{F}_{\text{span}} \cup \mathcal{F}_{\text{linear}} \cup \mathcal{F}_{\text{square}} \cup \mathcal{F}_{\text{deg}}$ as defined in the introduction. The first step is to construct an intermediate small algebra such that any polynomial from our configuration $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$ is either in the algebra, or univariate over this algebra (Lemma 12). The second step is to prove that we can augment this algebra slightly to contain all forms from $\mathcal{F}$ (Lemma 13). We achieve this by showing that the extra variables corresponding to the polynomials form a LCC configuration, allowing us to bound their rank.

▶ **Lemma 12** (Reduction to Base Configuration). *Let $0 < \delta \leq 1$ be a constant, and let $\varepsilon := \delta/10$. Let $\mathcal{F}$ be a $(\delta, 2)$-rad-SG configuration. There exists a $(17, \varepsilon^3/4^8)$-clean vector space with respect to $\mathcal{F}$, denoted by V, such that every polynomial in $\mathcal{F}$ is either in $\mathbb{C}[V]$ or univariate over V, and $\dim(V) = O(1/\varepsilon^4)$. Further, $\mathcal{F}_{\text{square}} \cup \mathcal{F}_{\text{linear}} \subseteq \mathbb{C}[V]$. Also, for every polynomial $P \in \mathcal{F}_{\text{deg}} \setminus \mathbb{C}[V]$, if z_P spans $\mathbb{L}_V(P)$ then there are at least $\varepsilon^3 m/4^8$ distinct linear forms $x_1, \dots, x_t$ and distinct linear forms $a_1, \dots, a_t$ such that for every i, the linear forms z_P, x_i, a_i are pairwise linearly independent in S_1/V_1, and $z_P \in \text{span}_{\mathbb{C}}\{x_i, a_i\}$.*

▶ **Lemma 13** (Base Configuration). *Let $0 < \delta \leq 1$, let $\varepsilon := \delta/10$ and let $0 < \gamma \leq \varepsilon^3/4^8$ be constants. If $\mathcal{F}$ is a $(\delta, 2)$-rad-SG configuration, and $V := V_1 + V_2$ is a $(17, \gamma)$-clean vector space with respect to $\mathcal{F}$ that satisfies the conditions of Lemma 12, then there exists $U \subset S_1$ with $\dim(U) = O(1/\varepsilon^{27})$ such that $\mathcal{F} \subset \mathbb{C}[V, U]$.*

▶ **Theorem 3** ($(\delta, 2)$-rad-SG theorem). *If $\mathcal{F}$ is a $(\delta, 2)$-rad-SG configuration, then*

$$\dim(\text{span}_{\mathbb{C}}\{\mathcal{F}\}) = O(1/\delta^{54}).$$

Proof. We use the previous two lemmas to prove the main theorem. Let $\varepsilon := \delta/10$, Given a $(\delta, 2)$-rad-SG, we first apply Lemma 12 to obtain V, a $(17, \varepsilon^3/4^7)$-clean vector space with respect to $\mathcal{F}$. The space V has dimension $\mathcal{O}\left(1/\varepsilon^4\right)$, and is such that every polynomial in $\mathcal{F}$ is either in the algebra $\mathbb{C}[V]$, or univariate over V. We now apply Lemma 13 with parameter $\gamma = \varepsilon^3/4^8$ and vector space V, to obtain a vector space $U \subseteq S_1$. The vector space U has dimension $\mathcal{O}\left(1/\varepsilon^{27}\right)$, and is such that $\mathcal{F} \subseteq \mathbb{C}[V, U]$.

Consider the algebra $\mathbb{C}[V, U]$. Since the generators are homogeneous, the set of linear forms $\mathbb{C}[V, U]_1$ in the vector space $U + V_1$. Further, every quadratic in this algebra is a linear combination of elements of V_2, and products of the form $\ell_1\ell_2$, where $\ell_i \in U + V_1$. Therefore, we have $\mathbb{C}[V, U]_2 = \mathcal{O}\left(1/\varepsilon^{54}\right)$. The vector space $\mathbb{C}[V, U]_1 + \mathbb{C}[V, U]_2$ contains $\mathcal{F}$ and has dimension $\mathcal{O}\left(1/\varepsilon^{54}\right)$. This completes the proof. ◀

4 Conclusion and open problems

In this paper, we prove a robust version of the radical Sylvester-Gallai theorem for quadratics, generalizing [24].

Just as in the linear case of the Sylvester-Gallai problem robustness plays an important role in generalizing Sylvester-Gallai results to higher dimensional variants, such as the flats version in [1], we expect our robust variant to allow us to generalize the Sylvester-Gallai problem to "higher codimension" tuples of quadratic polynomials. For instance, instead of requiring $\text{rad}(F_i, F_j)$ to intersect $\mathcal{F}$ non-trivially, one would only require that for many triples (i, j, k), we would require $\text{rad}(F_i, F_j, F_k)$ to intersect $\mathcal{F}$ non-trivially. Just as in the linear case, properly defining such higher codimension variants requires some careful thought, especially since the non-linear aspect will introduce more subtlety than the linear case.[7] These higher dimensional variants have applications in algebraic complexity, as they can be instrumental in proving the main conjectures posed in [11] about such SG configurations.

Another important open problem is to generalize the above result to prove a robust version of the "product version" of the Sylvester-Gallai problem - a robust version of [11, Conjecture 1] with $k = 3$ and $r = 2$. In this work, we made a somewhat strong use of the fact that we have an extra polynomial in the radical ideal, and having a product of polynomials in the ideal instead seems to require a strengthening of several arguments in this paper to address it. Just as in [19], we believe that our general structure theorem, which gives us a deeper look in the minimal primes, could shed some light into a different way to construct robust algebras.

It is important to remark that higher codimension variants of the Sylvester-Gallai problem, even for quadratics, involves the study of schemes which are not equidimensional, which may require stronger structural results on the structure of such ideals. However, one could hope that our structure theorems might suffice, just as in [1] the robust linear Sylvester-Gallai theorem was sufficient to induct on the higher-dimensional analogs.

Lastly, another interesting direction and potential application of robust SG configurations is in the study of non-linear locally correctable codes (LCCs) over fields of characteristic zero. While lower bounds for linear LCCs have been out of reach for current techniques even over characteristic zero,[8] it would be interesting to know if robust non-linear SG configurations have bounded transcendence degree. If a robust form of Gupta's general conjecture is false, it could yield the first constructions of non-linear LCCs over characteristic zero, which are not known to exist. Moreover, we currently do not know of any construction of such codes with constant queries over characteristic zero.

References

1 Boaz Barak, Zeev Dvir, Amir Yehudayoff, and Avi Wigderson. Rank bounds for design matrices with applications to combinatorial geometry and locally correctable codes. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 519–528, New York, NY, USA, 2011. Association for Computing Machinery. doi:10.1145/1993636.1993705.

2 Peter Borwein and William OJ Moser. A survey of sylvester's problem and its generalizations. *Aequationes Mathematicae*, 40(1):111–135, 1990.

3 Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Closure results for polynomial factorization. *Theory of Computing*, 15(1):1–34, 2019.

[7] In [1] had to account for sub-flats intersecting $\mathcal{F}$ non-trivially.

[8] Aside from 2-query LCCs where optimal lower bounds are known for both linear and non-linear codes.

4 J-L Colliot-Thélene, J-J Sansuc, and P Swinnerton-Dyer. Intersections of two quadrics and châtelet surfaces. i. *Journal für die reine und angewandte Mathematik*, 373:37–107, 1987.

5 Leonard Eugene Dickson. The points of inflexion of a plane cubic curve. *The Annals of Mathematics*, 16(1/4):50–66, 1914.

6 Pranjal Dutta, Prateek Dwivedi, and Nitin Saxena. Deterministic identity testing paradigms for bounded top-fanin depth-4 circuits. In *Proceedings of the 36th Computational Complexity Conference*, CCC '21, Dagstuhl, DEU, 2021. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. `doi:10.4230/LIPIcs.CCC.2021.11`.

7 Zeev Dvir. Incidence theorems and their applications. *arXiv preprint*, 2012. `arXiv:1208.5073`.

8 Zeev Dvir, Shubhangi Saraf, and Avi Wigderson. Improved rank bounds for design matrices and a new proof of kelly's theorem. In *Forum of Mathematics, Sigma*, volume 2. Cambridge University Press, 2014.

9 Paul Erdos, Richard Bellman, Hubert S Wall, James Singer, and Victor Thébault. Problems for solution: 4065-4069. *The American Mathematical Monthly*, 50(1):65–66, 1943.

10 Tibor Gallai. Solution of problem 4065. *American Mathematical Monthly*, 51:169–171, 1944.

11 Ankit Gupta. Algebraic geometric techniques for depth-4 pit & sylvester-gallai conjectures for varieties. In *Electron. Colloquium Comput. Complex.*, volume 21, page 130, 2014.

12 Sten Hansen. A generalization of a theorem of sylvester on the lines determined by a finite point set. *Mathematica Scandinavica*, 16(2):175–180, 1965.

13 William Vallance Douglas Hodge and Daniel Pedoe. *Methods of Algebraic Geometry: Volume 2*. Cambridge University Press, 1994.

14 Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 198–207. IEEE, 2009.

15 Leroy Milton Kelly. A resolution of the sylvester-gallai problem of j.-p. serre. *Discrete & Computational Geometry*, 1(2):101–104, 1986.

16 Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Electron. Colloquium Comput. Complex.*, page 81, 2021. URL: `https://eccc.weizmann.ac.il/report/2021/081`.

17 Eberhard Melchior. Uber vielseite der projektiven ebene. *Deutsche Math*, 5:461–475, 1940.

18 Rafael Oliveira and Akash Sengupta. Radical sylvester-gallai theorem for cubics. *Manuscript*, 2021.

19 Shir Peleg and Amir Shpilka. A generalized sylvester-gallai type theorem for quadratic polynomials. *CoRR*, abs/2003.05152, 2020. `arXiv:2003.05152`.

20 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`.

21 Shir Peleg and Amir Shpilka. Robust sylvester-gallai type theorem for quadratic polynomials. *CoRR*, abs/2202.04932, 2022. `arXiv:2202.04932`.

22 Nitin Saxena and Comandur Seshadhri. From sylvester-gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *Journal of the ACM (JACM)*, 60(5):1–33, 2013.

23 Jean-Pierre Serre. Advanced problem 5359. *Amer. Math. Monthly*, 73(1):89, 1966.

24 Amir Shpilka. Sylvester-gallai type theorems for quadratic polynomials. *Discrete Analysis*, page 14492, 2020.

25 Gaurav Sinha. Reconstruction of real depth-3 circuits with top fan-in 2. In *31st Conference on Computational Complexity (CCC 2016)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

26 James Joseph Sylvester. Mathematical question 11851. *Educational Times*, 59(98):256, 1893.

27 Endre Szemerédi and William T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3(3):381–392, 1983.