

# Robust Radical Sylvester-Gallai Theorem for Quadratics

Abhibhav Garg<sup>\*</sup>      Rafael Oliveira<sup>\*</sup>      Akash Kumar Sengupta<sup>†</sup>

March 10, 2022

## Abstract

We prove a robust generalization of a Sylvester-Gallai type theorem for quadratic polynomials, generalizing the result in [Shp20]. 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  $|\text{rad}(F_i, F_j) \cap \mathcal{F}| \geq 3$ , that is, the radical of  $F_i, F_j$  contains a third polynomial in the set.

In this work, we prove that any  $(\delta, 2)$ -radical Sylvester-Gallai configuration  $\mathcal{F}$  must be of low dimension: that is

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

## 1 Introduction

Suppose  $v_1, \dots, v_m \in \mathbb{R}^n$  is a set of 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 collinear [Sy193]. Independently, this same question was asked by Erdős in 1943 [EBW<sup>+</sup>43]. This was independently proved by [Mel40, Gal44], and this result is known as the Sylvester-Gallai theorem. A set of points satisfying the above property is called a Sylvester-Gallai (SG) configuration.

Sylvester-Gallai theorems depend on the base field. For instance, it is well known that any non-singular planar cubic curve over  $\mathbb{C}$  has nine inflection points, and that any line passing through two such points passes through a third [Dic14]. These nine points are not collinear, 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 [Ser66]. In 1986, Kelly noted that no such configurations can exist, namely, that points in  $\mathbb{C}^n$  that satisfy the Sylvester-Gallai property must be coplanar [Kel86]. Kelly showed that the planarity of Sylvester-Gallai configurations is a simple consequence of Hirzebruch's work on line arrangements which relies on deep results from algebraic geometry [Hir83].

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 in  $\mathbb{F}_p^n$  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 [Dvi12]. In this work, we only focus on fields of characteristic zero, and to make the presentation easier we restrict our attention to  $\mathbb{C}$ .

---

<sup>\*</sup>University of Waterloo, [a65garg@uwaterloo.ca](mailto:a65garg@uwaterloo.ca), [rafael@uwaterloo.ca](mailto:rafael@uwaterloo.ca)

<sup>†</sup>Columbia University, [akashs@math.columbia.edu](mailto:akashs@math.columbia.edu)

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 [BM90] and results therein.

While the above results are mathematically beautiful and interesting in 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 [Han65], a higher dimensional version of the SG 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) [KS09, SS13], a central problem in algebraic complexity theory. The works [KS09, SS13] use the higher dimensional Sylvester-Gallai theorems to bound the “rank” of certain types of depth three circuits.<sup>1</sup> 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  $u_1, \dots, u_k$  in the configuration such that  $v_i$  and  $u_j$  span a third point, for  $1 \leq j \leq k$ . The usual Sylvester-Gallai theorem is the case when  $\delta = 1$ . Such configurations were first studied by Szemerédi and Trotter [ST83], who proved that if  $\delta$  is bigger than an absolute constant close to 1, then the configuration has constant dimension.

In [BDYW11], the authors prove that such a configuration has dimension  $\mathcal{O}(1/\delta^2)$ , for any  $0 < \delta \leq 1$ . This robust version also allows them to prove robust versions of the higher dimensional variants mentioned above. 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 [DSW14], the authors improve the bound on the dimension of robust Sylvester-Gallai configurations to  $\mathcal{O}(1/\delta)$ .

In coding theory, these robust configurations naturally appear in the study of locally decodable codes and locally correctable codes [BDYW11]. These results, as well as similar results, are surveyed in [Dvi12]. Robust SG configurations also have applications in the study of algebraic circuits, in particular in reconstruction of algebraic circuits [Sin16].

**Higher degree generalizations of Sylvester-Gallai configurations:** Also motivated by the PIT problem, Gupta in [Gup14] introduced higher degree generalizations of SG configurations, and asked if they are also “low dimensional.” In his paper, Gupta outlines a series of SG-type conjectures, and gives a deterministic polynomial-time blackbox PIT algorithm for a special class of algebraic circuits<sup>2</sup> assuming that these conjectures hold.

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

---

<sup>1</sup>Algebraic circuits which compute polynomials that can be written as a sum of products of linear forms.

<sup>2</sup>These are circuits computed by a sum of constantly many products of constant degree polynomials.

**Conjecture 1.1** (Conjecture 29, [Gup14]). *Let  $Q_1, \dots, Q_m \in \mathbb{C}[x_1, \dots, x_n]$  be irreducible, homogeneous, and of degree at most  $d$  such that for every pair  $Q_i, Q_j$  there is a  $k$  such that  $Q_k \in \text{rad}(Q_i, Q_j)$ . Then the transcendence degree of  $Q_1, \dots, Q_m$  is  $\mathcal{O}(1)$  (where the constant depends on the degree  $d$ ).*

The case  $d = 2$  of the above conjecture was proved in [Shp20]. 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 in the case when  $d = 2$ .

## 1.1 Main result

In this section, we formally state our main result: robust quadratic radical Sylvester-Gallai configurations must lie in a constant dimensional vector space.<sup>3</sup> In particular, this result implies that the forms 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. As is customary in the literature, we will use *form* to denote homogeneous polynomials. For a polynomial ring  $S = \mathbb{C}[x_1, \dots, x_n]$ , we let  $S_d$  denote the vector space of polynomials of degree  $d$  in  $S$ , and  $(f_1, \dots, f_r)$  denotes the ideal generated by polynomials  $f_1, \dots, f_r$ . We also use  $\text{rad}(f_1, \dots, f_r)$  to denote the radical of this ideal, that is, the set of polynomials  $g$  such that  $g^k \in (f_1, \dots, f_r)$  for some  $k$ .

**Definition 1.2** ( $(\delta, 2)$ -rad-SG configurations). Let  $0 < \delta \leq 1$  and  $\mathcal{F} := \{F_1, \dots, F_m\}$  be a set of irreducible forms in  $\mathbb{C}[x_1, \dots, x_n]$ . 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  $F_i \notin (F_j)$  (forms are “pairwise independent”)
3. for any  $i \in [m]$ , there are  $\delta(m - 1)$  indices  $j \in [m] \setminus \{i\}$  such that  $|\text{rad}(F_i, F_j) \cap \mathcal{F}| \geq 3$ .

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

**Theorem 1.3** ( $(\delta, 2)$ -rad-SG theorem). *If  $\mathcal{F}$  is a  $(\delta, 2)$ -rad-SG configuration, then*

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

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. 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.

---

<sup>3</sup>Our results hold for any algebraically closed field of characteristic zero. However, for simplicity of exposition, we only state our results over  $\mathbb{C}$ .

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 4](#), where we also elaborate on how these algebras behave with SG configurations (where we need the notion of clean algebras). For more intuition about these algebras and about our strategy to prove our main 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  $(\delta, 2)$ -rad-SG configuration is low dimensional (as has also been the first step in the works of [\[Shp20, PS20a\]](#)) 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 neither radical nor prime, then there must be a low-rank quadratic in their span. In [\[Shp20, PS20a\]](#), 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 1.4](#), 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 [\[Shp20, PS20a\]](#) (see [Section 3](#)). 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, as was done in [\[OS22\]](#).

**Proposition 1.4** (Radical Structure Theorem). *Let  $\mathbb{K}$  be an algebraically closed field of characteristic zero and  $Q_1, Q_2 \in S = \mathbb{K}[x_1, \dots, x_n]$  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  $xy \in \text{span}(Q_1, Q_2)$ .*
  - (b) *There exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$ , 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  $\alpha, \beta \in \mathbb{K}$ . In this case, we have  $x^2 \in \text{span}(Q_1, Q_2)$ .*
  - (b)  *$Q_1, Q_2$  do not have a common factor. There exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$  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  $x^2 \in \text{span}(Q_1, Q_2)$ .*
  - (c)  *$Q_1, Q_2$  do not have a common factor and there exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$ , 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 [\[CTSSD87, Section 1\]](#) and [\[HP94, Chapter XIII\]](#). 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 setting of perfect fields, whereas we are concerned with the special case of algebraically closed fields of characteristic zero.

## 1.2 High-level ideas of the proof of Theorem 1.3

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.

Our strategy to prove the robust radical SG theorem is based on the following toy example: suppose our polynomial ring is  $\mathbb{C}[x_1, \dots, x_r, y_1, \dots, y_s]$ , 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  $\mathbb{C}[y_1, \dots, y_s]$ . That is, for each quadratic  $Q$ , there exists a linear form  $x_Q \in \text{span}_{\mathbb{C}}\{x_1, \dots, x_r\}$  such that  $Q \in \mathbb{C}[x_Q, y_1, \dots, y_s]$ . 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 [BDYW11, DSW14].

In general it is not always possible to reduce the general robust radical SG problem for quadratics to the toy example above.<sup>4</sup> However we will be able to construct a small subalgebra of our polynomial ring which is just as good as the small polynomial ring  $\mathbb{C}[y_1, \dots, y_s]$  in the toy example above. Additionally, we will not always be able to reduce the non-linear problem to a robust linear SG configuration, as some forms  $x_Q$  may appear with multiplicity. Instead of a robust linear SG configuration, we will reduce it to a  $\delta$ -LCC configuration of [BDYW11].

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, 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 thought 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 more forms from  $\mathcal{F}$  inside of the larger algebra. We call any vector space which satisfies both conditions above a *clean vector space* with respect to  $\mathcal{F}$ .<sup>5</sup>

<sup>4</sup>For instance if the polynomial  $Q = \sum_{i=1}^s x_i y_i$  is in our SG configuration.

<sup>5</sup>In hindsight, this saturation condition resembles [BDYW11, Theorem 7.7], where they deal with  $\delta$ -LCC configurations. They show that if no element has many repetitions (the trivial case for them), they are able to non-trivially construct a design matrix which annihilates a constant fraction of the elements in the configuration.

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, in [Section 3](#) we prove [Proposition 1.4](#), generalizing the previous structure theorems from [\[Shp20, PS20a\]](#). Additionally, we also assemble results on the structure of minimal primes of these ideals to construct our algebra.

With [Proposition 1.4](#) at hand, we proceed in a similar fashion as in [\[Shp20, PS20a\]](#) by partitioning the quadratics in our SG configuration into subsets, each satisfying a particular case of our structure theorem. The four subsets we have are as follows: if  $\mathcal{F}$  is a  $(\delta, 2)$ -rad-SG configuration, we take  $\varepsilon = \delta/10$  and define

1.  $\mathcal{F}_{\text{span}}$  is the set of quadratics  $Q$  which satisfy a “span dependency” with at least  $\varepsilon$ -fraction of the forms. That is, there exist many quadratics  $F, G \in \mathcal{F}_2$  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 1.4](#) with at least an  $\varepsilon$ -fraction of the other forms. 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  $\geq 2$ .
3.  $\mathcal{F}_{\text{deg}}$  is the set of quadratics  $Q$  with an  $\varepsilon$ -fraction of its SG dependencies with linear forms.<sup>6</sup>
4.  $\mathcal{F}_{\text{square}}$  is the set of quadratics  $Q$  which satisfy case 3 (b) of [Proposition 1.4](#) with at least  $(\delta - 3\varepsilon)$ -fraction of the other forms. That is, there are many quadratics  $F \in \mathcal{F}$  such that there is a linear form  $\ell$  such that  $\ell^2 \in \text{span}_{\mathbb{C}}\{F, Q\}$ .

With this partition, we proceed to 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 form is in the algebra  $\mathbb{C}[V][z]$ .

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. To construct the intermediate subalgebras, we use two strategies: iterative processes similar to the ones used in [\[Shp20, PS20a\]](#), and constructing double covers of the SG dependencies. These two strategies allow us to construct algebras generated by  $\text{poly}(1/\delta)$  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  $\delta$ -LCC configuration.

Once we have our clean subalgebra with respect to the SG configuration, and we have every polynomial in the configuration either in the algebra or univariate over our algebra, 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 make up a  $\delta$ -LCC configuration, and therefore span a vector space of small dimension, concluding our proof.

### 1.3 Related Work

The original motivation for studying higher degree SG configurations comes from [\[Gup14\]](#), in order to give polynomial time PIT for a special class of depth-4 algebraic circuits. The most general

---

<sup>6</sup>Deg stands for the degenerate case.

SG problem/configuration that is needed towards this application is the following conjecture, [Gup14, Conjecture 1], which we term as  $(k, d, c)$ -Sylvester-Gallai conjecture.

**Conjecture 1.5** ( $(k, d, c)$ -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  $\mathcal{F}_{i_i}$ , 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 1.5, [Shp20] studies quadratic SG configurations (Conjecture 1.1). The configurations we study are exactly the fractional versions of these quadratic SG configurations. In [PS20a], the authors extend the result on quadratic SG configurations, weakening the SG condition, only requiring that the radical of the ideal generated by every pair of quadratics contains a product of four other quadratics. In [PS20b], the authors extend this further, by proving Conjecture 1.5 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 [Shp20], [PS20a], [PS20b]. In [Shp20], the author proves a structural result for quadratic forms contained in the radical of the ideal generated by two other quadratic forms. In [PS20a], this result is extended to products of quadratic forms. 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 [Shp20] and [PS20a] 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 [Shp20, PS20a], 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 [Shp20, PS20a]. 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 [Gup14]). In [DDS21], 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 [LST21], which gives a weakly-exponential algorithm for PIT for these circuits via the hardness vs randomness paradigm for constant depth circuits [CKS19]. However, the SG approach of [Gup14] 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 [OS22]:** In [OS22] the authors generalize the radical SG theorem to cubic forms. However, the SG theorem in [OS22] is not robust. Robustness significantly increases the combinatorial complexity of the problem (as it is the case in every setting, even in the linear case).

Some ideas in this paper are motivated by similar constructions in [OS22]. More precisely, the construction of wide algebras motivated our construction of clean vector spaces (Section 4). Wide algebras have stronger algebro-geometric properties and are significantly larger than the algebras generated by clean vector spaces. 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 [PS22]:** Simultaneously and independently from this work, Peleg and Shpilka have also proved that  $(\delta, 2)$ -rad-SG configurations have  $\text{poly}(1/\delta)$  dimension. While the result of [PS22] 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 [PS22] 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 [PS22] is the structure used to control the above sets. In [PS22] 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  $\ell_i$  (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  $\ell_i$  form a LCC configuration, instead of a robust linear SG configuration. This, and the fact that we handle linear forms, are the reasons why our bound is worse than the one in [PS22].

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  $\ell$ , as there is less structure between  $Q, \ell$  and the quadratic in  $\text{rad}(Q, \ell)$  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 establish some notation and preliminary results. In Section 3 we establish the algebro-geometric results we need to prove our structural results on the minimal primes of ideals generated by two quadratics. In this section, we also show how our results generalize previous structural results on SG configurations. In Section 4 we define and prove results that we need about one of the main objects that we develop: clean vector spaces. In Section 5 we prove our main result, that robust radical Sylvester-Gallai configurations must lie in a small dimensional vector space. In Section 6 we conclude and state some open problems and future directions.



## 2 Preliminaries

In this section, we establish the notation which will be used throughout the paper and some important background which we shall need to prove our claims in the next sections.

### 2.1 Notation

Let  $S := \mathbb{C}[x_0, \dots, x_n]$  be our polynomial ring, with the standard grading by degree. We can write  $S = \bigoplus_{d \geq 0} S_d$ , where  $S_d$  is the  $\mathbb{C}$ -vector space of forms of degree  $d$ . For the rest of this paper, we will use the term *form* to refer to a homogeneous polynomial. Given any graded vector space  $V \subset S$ , we use  $V_d$  to denote the subspace of forms of degree  $d$ , that is,  $V_d := V \cap S_d$ .

### 2.2 Rank of quadratic forms

We now define a notion of the rank of quadratic forms, in accordance to [Shp20].

**Definition 2.1** (Rank of a quadratic form). Let  $Q$  be a quadratic form. The rank of  $Q$ , denoted  $\text{rank } Q$  is the smallest  $s$  such that we can write  $Q = \sum_{i=1}^s a_i b_i$  with  $a_i, b_i \in S_1$ . If  $\text{rank } Q = s$ , then such a decomposition  $Q = \sum_{i=1}^s a_i b_i$  with  $a_i, b_i \in S_1$  is called a minimal representation of  $Q$ .

*Remark 2.2.* Let  $Q = \sum_i a_{ii} x_i^2 + \sum_{i < j} 2a_{ij} x_i x_j$  be a quadratic form in  $S$ . Recall that there is an one-to-one correspondence between quadratic forms  $Q \in S_2$  and symmetric bilinear forms. Let  $M$  be the symmetric matrix corresponding to the symmetric bilinear form of  $Q$ . Note that the  $(i, j)$ -the entry of  $M$  is given by  $a_{ij}$ . If  $M$  is of rank  $r$ , then after a suitable linear change of variables, we can write  $Q = x_1^2 + \dots + x_r^2$ . Since the rank of a quadratic form is invariant under a linear change of variables, we have  $\text{rank}(Q) = \lceil r/2 \rceil$ , if  $M$  is of rank  $r$ .

In the next sections, we will need to use the following notion of a vector space of a quadratic form, which is a slight modification on the definition first given in [Shp20]. The only modification that we make is that we preserve the quadratic form if its rank is high enough.

**Definition 2.3** (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:

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

Note that  $\mathbb{L}(Q)$  is always a vector space of  $\mathcal{O}(1)$  dimension (in fact, it is of dimension at most 10), while  $\text{Lin}(Q)$  can have non constant dimension. While a minimal representation  $Q = \sum_{i=1}^s a_i b_i$  is not unique, the vector space  $\text{Lin}(Q)$  is unique and hence well-defined. The following lemma, which appears in [PS20a, Fact 2.15] characterizes  $\text{Lin}(Q)$  as the smallest vector space of linear forms defining the algebras that contain  $Q$ .

We also extend the definition of  $\text{Lin}$  to linear forms in the natural way as follows.

**Definition 2.4.** For a linear form  $\ell \in S_1$  define  $\mathbb{L}(\ell) := \text{span}_{\mathbb{C}}\{\ell\}$ .

**Lemma 2.5.** If  $Q = \sum_{i=1}^r x_i y_i$  with  $x_i, y_i \in S_1$  then  $\text{Lin}(Q) \subseteq \text{span}_{\mathbb{C}}\{x_i, y_j | i, j \in [r]\}$ .

**Proposition 2.6.** Let  $Q_1, Q_2 \in S_2$ . Suppose  $\text{rank}(Q_1) \geq d$  for some  $d$ . Consider the pencil of quadratic forms formed by  $Q_1, Q_2$ , i.e. the set  $\{Q_t = Q_1 + tQ_2 | t \in \mathbb{C}\}$ . Then there are at most  $2d - 1$  values of  $t$  for which the quadratic form  $Q_t$  has  $\text{rank}(Q_t) < d$ .

*Proof.* Let  $M_1, M_2$  be the matrices corresponding to the quadratic forms  $Q_1, Q_2$  respectively. After a linear change of variables, we may assume that the matrix  $M_2$  is a diagonal matrix. Then the matrix corresponding to  $Q_t = Q_1 + tQ_2$  is given by  $M_t = M_1 + tM_2$ . Note that  $\text{rank}(Q_t) < d$  if and only if  $\text{rank}(M_t) < 2d - 1$ . Now  $\text{rank}(M_t) < 2d - 1$  if and only if all the determinants of all the  $(2d - 1) \times (2d - 1)$  minors are zero. Note that each such determinant is a polynomial in  $t$ . Since  $\text{rank}(Q_1) \geq d$ , there exists at least one such determinant that is non-zero at  $t = 0$ , and hence it is a non-zero polynomial in  $t$  of degree  $\leq 2d - 1$ . Thus, there are at most  $2d - 1$  values of  $t$  such that  $\text{rank}(Q_t) < d$ .  $\square$

*Remark 2.7.* If  $Q_1, Q_2$  are irreducible quadratic forms which satisfy the conditions of the previous proposition with  $d = 2$  and there are at least two values of  $t$  for which  $\text{rank}(Q_t) = 1$ , then  $\text{rank}(Q_1) = \text{rank}(Q_2) = 2$ . Further we have  $\mathbb{L}(Q_1) = \mathbb{L}(Q_2)$ , since both  $Q_1$  and  $Q_2$  will be linear combinations of the two reducible polynomials in the pencil defined by  $Q_1, Q_2$ .

**Lemma 2.8.** *If  $V_1 \subset S_1$  and  $x, y, u, v \in S_1$  such that  $xy - uv \in \mathbb{C}[V_1]$  then one of the following holds:*

1. *We have  $x, y, u, v \in V_1$ .*
2. *There exists a linear form  $\ell \in S_1 \setminus V_1$  such that  $x, y, u, v \in \text{span}_{\mathbb{C}}\{V_1, \ell\}$ .*

*Proof.* Let  $P := xy - uv$ . If  $P$  is irreducible, then  $xy - uv$  is a minimal representation of  $P$ . Therefore, we have  $\text{Lin}(P) = \text{span}_{\mathbb{C}}\{x, y, u, v\}$  and [Lemma 2.5](#) implies  $x, y, u, v \in V_1$ .

Thus, we can assume  $P$  factors and  $xy - uv = zw$  for some  $z, w \in S_1$ . Since  $P = zw$  is a minimal representation of  $P$ , [Lemma 2.5](#) implies  $\text{Lin}(P) = \text{span}_{\mathbb{C}}\{z, w\} \subset V_1$ . If  $x, y, u, v \notin V_1$ , we can assume w.l.o.g. that  $x \notin V_1$ , and therefore  $zw \neq 0$  in  $S/(x)$ . By factoriality of  $S/(x)$ , we have that  $-uv \equiv zw \neq 0 \pmod{(x)}$  which implies  $u, v \in \text{span}_{\mathbb{C}}\{x, V_1\}$ . Since  $xy = uv + zw$ , [Lemma 2.5](#) implies that  $\text{Lin}(xy) = \text{span}_{\mathbb{C}}\{x, y\} \subset \text{span}_{\mathbb{C}}\{u, v, z, w\} \subset \text{span}_{\mathbb{C}}\{x, V_1\}$  as we wanted.  $\square$

**Proposition 2.9.** *Let  $Q \in S_2$  be an irreducible quadratic form. If there exists a linear form  $\ell$  such that  $(Q, \ell)$  is not radical, then  $\text{rank } Q = 2$ ,  $\dim \mathbb{L}(Q) = 3$ , and any such  $\ell$  must be in  $\mathbb{L}(Q)$ . Moreover, any three pairwise linearly independent linear forms  $\ell_1, \ell_2, \ell_3$  such that  $(Q, \ell_i)$  is not radical are such that  $\mathbb{L}(Q) = \text{span}_{\mathbb{C}}\{\ell_1, \ell_2, \ell_3\}$ .*

*Proof.* Since  $Q$  is irreducible, we have  $\text{rank}(Q) \geq 2$  and  $\dim \mathbb{L}(Q) \geq 3$ . If  $\text{rank}(Q) \geq 3$  then  $Q$  is irreducible modulo  $\ell$ , for any linear form  $\ell$ . Therefore the ideal  $(Q, \ell)$  is prime, and hence radical for any linear form  $\ell$ . Hence if there exists a linear form  $\ell$  such that  $(Q, \ell)$  is not radical, then we must have that  $\text{rank}(Q) = 2$ . If  $Q$  is reduced modulo a linear form  $\ell$ , then the ideal  $(Q, \ell)$  is radical. Therefore, if  $(Q, \ell)$  is not a radical ideal for some linear form  $\ell$ , then we have  $Q = \ell a + b^2$ , for some  $a, b \in S_1$ . Note that this is a minimal representation of  $Q$ . Therefore, by [\[PS20a, Fact 2.13\]](#) we must have that  $\text{span}_{\mathbb{C}}\{\ell, a, b\} = \mathbb{L}(Q)$ . Hence we have  $\ell \in \mathbb{L}(Q)$ . Therefore  $\dim(\mathbb{L}(Q)) \leq 3$ , which together with  $\dim \mathbb{L}(Q) \geq 3$  implies  $\dim \mathbb{L}(Q) = 3$ .

Suppose there exists a linear form  $x$  such that  $(Q, x)$  is not radical. Then, by the above discussion, we may assume that  $Q = xy + z^2$  where  $x, y, z$  are linearly independent forms and  $\mathbb{L}(Q) = \text{span}_{\mathbb{C}}\{x, y, z\}$ . Suppose  $(Q, \ell_i)$  is not radical for three pairwise linearly independent forms  $\ell_1, \ell_2, \ell_3 \in S_1$ . Consider the projective conic defined by  $Q$  in  $\mathbb{P}^2$ . Now  $(Q, \ell_i)$  not radical implies that the line defined by  $\ell_i$  is tangent to the conic  $Q$  at some point  $p_i$ . Since  $\ell_1, \ell_2, \ell_3$  are pairwise linearly independent, the points  $p_1, p_2, p_3$  are distinct. If  $\ell_1, \ell_2, \ell_3$  are linearly dependent then the points  $p_1, p_2, p_3$  are collinear. Then there exists a line passing through  $p_1, p_2, p_3$  which intersects the projective conic  $Q$  at three distinct points. This contradicts Bezout's theorem, and hence  $\ell_1, \ell_2, \ell_3$  are linearly independent.  $\square$

## 2.3 Sylvester-Gallai Configurations and LCC Configurations

We now establish the notation we use for the SG configurations that we will encounter, as well as what is known about the bounds on their dimension. We also define the notion of a  $\delta$ -LCC configuration introduced in [BDYW11], and state a bound on the rank of such configurations.

We start by restating the definition of quadratic robust Sylvester-Gallai configurations.

**Definition 1.2** ( $(\delta, 2)$ -rad-SG configurations). Let  $0 < \delta \leq 1$  and  $\mathcal{F} := \{F_1, \dots, F_m\}$  be a set of irreducible forms in  $\mathbb{C}[x_1, \dots, x_n]$ . 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  $F_i \notin (F_j)$  (forms are “pairwise independent”)
3. for any  $i \in [m]$ , there are  $\delta(m-1)$  indices  $j \in [m] \setminus \{i\}$  such that  $|\text{rad}(F_i, F_j) \cap \mathcal{F}| \geq 3$ .

In the above definition, if  $F_k \in \mathcal{F}$  is such that  $F_k \in \text{rad}(F_i, F_j)$ , then we refer to  $(F_i, F_j, F_k)$  as a SG-triple. Note that the radical condition is not symmetric, i.e. if  $(F_i, F_j, F_k)$  is a SG-triple, it is not necessary that  $(F_i, F_k, F_j)$  or  $(F_k, F_j, F_i)$  is a SG-triple. The general form of the linear SG configurations that we will encounter are as follows:

*Remark 2.10.* If  $\mathcal{F}$  is a  $(\delta, 2)$ -rad-SG configuration where  $\mathcal{F}_2 = \emptyset$ , we obtain the robust linear SG configurations from [BDYW11, DSW14]. Hence, in this case we shall simply denote the robust linear SG configurations as  $\delta$ -linear SG configurations.

**Theorem 2.11** (Rank Bound for Linear SG Configurations [DSW14]). *If  $\mathcal{F}$  be a  $\delta$ -linear SG configuration, then  $\dim(\text{span}_{\mathbb{K}}\{\mathcal{F}\}) \leq 13/\delta$ .*

We now define  $\delta$ -LCC configurations. These are configurations that arise in the study of locally correctable codes, and hence the name. They can be seen as extensions of SG configurations.

**Definition 2.12** ( $\delta$ -LCC configurations, [BDYW11]). Let  $0 < \delta \leq 1$  and let  $\mathcal{F} := \{x_1, \dots, x_m\} \subset S_1$  be a multiset of linear forms, not necessarily distinct. We say that  $\mathcal{F}$  is a  $\delta$ -LCC configuration, if for every  $i \in [m]$  and every subset  $\Gamma \subset [m]$  with  $|\Gamma| \leq \delta m$ , there are indices  $j, k \in [m] \setminus \Gamma$  such that either  $x_i \in \text{span}_{\mathbb{C}}\{x_j\} \cup \text{span}_{\mathbb{C}}\{x_k\}$  or the three linear forms  $x_i, x_j, x_k$  are pairwise independent and satisfy  $x_i \in \text{span}_{\mathbb{C}}\{x_j, x_k\}$ .

In [BDYW11, Theorem 7.6] the authors proved the following bound for  $\delta$ -LCCs.

**Theorem 2.13.** *If  $\mathcal{F}$  is a  $\delta$ -LCC configuration then  $\dim(\text{span}_{\mathbb{C}}\{\mathcal{F}\}) = O(1/\delta^9)$ .*

## 3 Structural Algebro Geometric Results

In this section we establish the necessary definitions and theorems needed from commutative algebra and algebraic geometry. Throughout this section, we will work over an algebraically closed field of characteristic zero  $\mathbb{K}$  and we will denote  $S = \mathbb{K}[x_0, x_1, \dots, x_n]$ .

### 3.1 Algebraic preliminaries

All rings that we consider in this section are commutative rings with unity. We refer to [AM69, Eis95] for general background on commutative algebra, in particular for primary decomposition, Cohen-Macaulay rings and Hilbert-Samuel multiplicities. We briefly recall some of the relevant statements below for convenience.

**Definition 3.1** (Regular sequence). Let  $R$  be ring and  $M$  an  $R$ -module. A sequence of elements  $x_1, x_2, \dots, x_n \in R$  is called an  $M$ -regular sequence if

- (1)  $(x_1, x_2, \dots, x_n)M \neq M$ , and
- (2) for each  $i$ , the element  $x_i$  is a non-zero-divisor in  $M/(x_1, \dots, x_{i-1})M$ .

If  $M = R$ , then we simply call  $x_1, \dots, x_n$  a regular sequence.

*Remark 3.2.* Let  $Q_1, Q_2 \in S_2$ . If  $Q_1, Q_2$  do not have any common factors, then  $Q_1, Q_2$  is a regular sequence. Indeed, if  $Q_1, Q_2$  is not a regular sequence then  $Q_2$  is a zero-divisor in  $S/(Q_1)$ . Therefore,  $PQ_2 = RQ_1$  for some forms  $P \notin (Q_1)$  and  $R \in S$ . Note that  $Q_1$  does not divide  $Q_2$ . Since  $S$  is an UFD, and  $Q_1, Q_2$  do not have any common factors, we conclude that  $Q_1$  divides  $P$ , which is a contradiction. Therefore  $Q_1, Q_2$  is a regular sequence.

The following proposition tells us that ideals generated by  $Q_1, Q_2$  are Cohen-Macaulay, if  $Q_1, Q_2$  do not have a common factor. This is a special case of [Eis95, Proposition 18.13], which states that complete intersections are Cohen-Macaulay.

**Proposition 3.3** (Cohen-Macaulayness [Eis95]). *Let  $Q_1, Q_2 \in S_2$  such that  $Q_1, Q_2$  do not have any common factors, then the ideal  $(Q_1, Q_2)$  is Cohen-Macaulay, i.e. the quotient ring  $S/(Q_1, Q_2)$  is a Cohen-Macaulay ring.*

*Proof.* By Remark 3.2, we know that  $Q_1, Q_2$  is a regular sequence. Therefore co-dimension of the ideal  $(Q_1, Q_2)$  is 2. Since the polynomial ring  $S$  is Cohen-Macaulay, we conclude that  $S/(Q_1, Q_2)$  is Cohen-Macaulay by [Eis95, Proposition 18.13].  $\square$

Cohen-Macaulay ideals are equidimensional and unmixed. Hence, if  $I$  is a Cohen-Macaulay ideal then every associated prime of  $I$  is a minimal prime and the codimension of every minimal prime of  $I$  is the same [Eis95, Corollaries 18.11, 18.14]. An easy consequence is the following result.

**Corollary 3.4** (Unmixedness and Equidimensionality). *If  $Q_1, Q_2 \in S_2$  without any common factors, then the ideal  $(Q_1, Q_2)$  is unmixed and equidimensional. In particular, let  $(Q_1, Q_2) = q_1 \cap \dots \cap q_n$  be an irredundant primary decomposition. Let  $\mathfrak{p}_i = \text{rad}(q_i)$ . Then*

1. every associated prime of  $(Q_1, Q_2)$  is a minimal prime, i.e.  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  are precisely the distinct minimal primes over  $(Q_1, Q_2)$ ,
2. every minimal prime of  $(Q_1, Q_2)$  has codimension 2, i.e.  $\text{ht}(\mathfrak{p}_i) = 2$  for all  $i \in [n]$ .

*Proof.* Note that by Proposition 3.3, the ideal  $(Q_1, Q_2)$  is Cohen-Macaulay. Hence  $(Q_1, Q_2)$  is unmixed and equidimensional.  $\square$

Let  $(R, \mathfrak{m})$  be a local ring and  $M$  be an  $R$ -module. The Hilbert-Samuel function of  $M$  is defined as

$$H_{\mathfrak{m}, M}(n) = \text{length} \left( \frac{\mathfrak{m}^n M}{\mathfrak{m}^{n+1} M} \right).$$

By [Eis95, Proposition 12.2, Theorem 12.4], there exists a polynomial  $P_{\mathfrak{m},M}$  of degree  $\dim(M) - 1$  such that  $P_{\mathfrak{m},M} = H_{\mathfrak{m},M}(n)$  for  $n \gg 0$ . The polynomial  $P_{\mathfrak{m},M}$  is called the Hilbert-Samuel polynomial of  $M$ . Let  $a_d$  be the leading coefficient of  $P_{\mathfrak{m},M}$ , where  $d = \dim(M) - 1$ . The Hilbert-Samuel multiplicity of  $M$  is defined as

$$e(\mathfrak{m}, M) = (d - 1)! a_d.$$

Therefore, the leading coefficient of the Hilbert-Samuel polynomial  $P_{\mathfrak{m},M}$  is  $\frac{e(\mathfrak{m},M)}{(\dim M - 1)!}$ .

Let  $R = S_{\mathfrak{m}}$  be the localization of  $S$  at the irrelevant maximal ideal  $\mathfrak{m} = (x_0, \dots, x_n)$ . Let  $I$  be a homogeneous ideal in  $S$ . Then the localization  $(S/I)_{\mathfrak{m}}$  is an  $R$ -module. We will denote  $e(S/I) := e(\mathfrak{m}, (S/I)_{\mathfrak{m}})$ . Note that by [Eis95, Exercise 12.6], the number  $e(S/I)$  is also equal to the degree of the projective variety defined by  $I$  in  $\mathbb{P}^n$ .

Let  $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$  be an irredundant primary decomposition of  $I$  in  $S$ . Let  $\mathfrak{p}_i = \text{rad}(\mathfrak{q}_i)$  be a minimal prime of  $I$  for some  $i$ . Then the localization  $(S/I)_{\mathfrak{p}_i}$  is an  $S_{\mathfrak{p}_i}$  module of finite length. We define the multiplicity of  $\mathfrak{p}_i$  in the primary decomposition of  $I$  as

$$m(\mathfrak{p}_i) = \text{length}((S/I)_{\mathfrak{p}_i}).$$

*Remark 3.5.* Note that  $m(\mathfrak{p}_i) \geq 1$ . If  $m(\mathfrak{p}_i) = 1$ , then we must have  $\mathfrak{q}_i = \mathfrak{p}_i$ . Indeed,  $\text{length}((S/\mathfrak{q}_i)_{\mathfrak{p}_i}) \leq \text{length}((S/I)_{\mathfrak{p}_i})$  since we have a surjective homomorphism  $(S/I)_{\mathfrak{p}_i} \rightarrow (S/\mathfrak{q}_i)_{\mathfrak{p}_i}$ . Therefore we have  $\text{length}((S/\mathfrak{q}_i)_{\mathfrak{p}_i}) = 1$ . If  $\mathfrak{q}_i \subsetneq \mathfrak{p}_i$ , then we have a strict chain of  $S_{\mathfrak{p}_i}$ -modules given by  $(0) \subsetneq (\mathfrak{p}_i)_{\mathfrak{p}_i} \subsetneq (S/\mathfrak{q}_i)_{\mathfrak{p}_i}$ , which is of length 2. That is a contradiction. Therefore we must have  $\mathfrak{q}_i = \mathfrak{p}_i$ . Hence if we have  $m(\mathfrak{p}_j) = 1$  for all  $j$ , then  $I = \bigcap_j \mathfrak{p}_j$ , and  $I$  is a radical ideal.

Conversely if  $I$  is a radical ideal then  $m(\mathfrak{p}_i) = 1$  for all minimal primes. Indeed for every  $i$  the ideal  $\mathfrak{p}_i (R/I)_{\mathfrak{p}_i}$  is the nilradical of  $(R/I)_{\mathfrak{p}_i}$  by the minimality of  $\mathfrak{p}_i$ . Since  $R/I$  has no nilpotents, we have  $\mathfrak{p}_i (R/I)_{\mathfrak{p}_i} = (0)_{\mathfrak{p}_i}$ , which implies  $(R/I)_{\mathfrak{p}_i}$  is a field, and therefore has length 1.

We recall the basic properties of the Hilbert-Samuel multiplicity below.

**Proposition 3.6.** [Eis95, Exercises 12.7, 12.11] *Let  $I \subset S$  be a homogeneous ideal.*

1. *Let  $J \subset S$  be a homogeneous ideal such that  $I \subset J$ . Then  $e(S/J) \leq e(S/I)$ .*
2. *If  $I = (F)$  for some homogeneous polynomial of degree  $d$ , then  $e(S/I) = d$ .*
3. *If  $I = (F_1, \dots, F_m)$  where  $F_1, \dots, F_m$  is a regular sequence of homogeneous polynomials and  $\deg(F_i) = d_i$ . Then  $e(S/I) = d_1 \cdots d_m$ .*
4. *If  $I = (F_1, \dots, F_m)$  where  $F_1, \dots, F_m$  is a regular sequence of homogeneous polynomials, and  $\mathfrak{p}_1, \dots, \mathfrak{p}_m$  are the minimal primes of  $I$  in  $S$ . Then*

$$e(S/I) = \sum_i m(\mathfrak{p}_i) e(S/\mathfrak{p}_i).$$

### 3.2 Structural Results for Ideals generated by two quadratics

In this section we prove some results on the structure of non-radical ideals and their primary decompositions, which will be used in our proof of the robust Sylvester-Gallai theorem.

**Proposition 3.7.** *Let  $Q_1, Q_2 \in S_2$  be such that they do not have any common factors and  $I = (Q_1, Q_2)$ . Let  $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$  be an irredundant primary decomposition and  $\mathfrak{p}_i = \text{rad}(\mathfrak{q}_i)$ . Then*

1. We have  $e(S/q_i) \leq 4$  for all  $i \in [m]$ .
2. If  $I$  is not a radical ideal, then  $e(S/p_i) \leq 2$  for all  $i \in [m]$ .
3. If  $I$  is not a radical ideal, then for all  $i \in [m]$ , the minimal primes  $p_i$  are of one of the following types :
  - (a) (Linear prime) we have  $p_i = (x, y)$ , for some linearly independent forms  $x, y \in S_1$
  - (b) (Quadratic prime) we have  $p_i = (x, Q)$ , for some  $x \in S_1$  and  $Q \in S_2$  such that  $Q$  is irreducible modulo  $x$ .
4. If  $I$  is a radical ideal that is not prime, then either  $I$  has a minimal prime that is a linear prime, or  $I$  has two minimal primes, both of which are quadratic primes.

*Proof.* Since  $Q_1, Q_2$  is a regular sequence we know that  $e(S/I) = 4$ , by Proposition 3.6. Since  $I$  is a homogeneous ideal, the primary ideals  $q_i$  and the prime ideals  $p_i$  are all homogeneous. Therefore by Proposition 3.6, we see that  $e(S/q_i) \leq 4$  for all  $i$ . By Proposition 3.6, we also have  $\sum_i m(p_i)e(S/p_i) = 4$ .

Suppose first that  $I$  is not radical. We must have  $q_j \subsetneq p_j$  for some  $j$ . Therefore  $m(p_j) > 1$  for some  $j$ . Since  $e(S/p_i) \geq 1$  for all  $i$ , we see that  $e(S/p_i) \leq 2$  for all  $i$ .

Note that  $\text{ht}(p_i) = 2$  for all  $i$ , by Corollary 3.4. By [EG84, Page 112], any height 2 prime ideal  $p$  in  $S$  with multiplicity  $e(S/p) = 1$  is of the form  $(x, y)$  where  $x, y \in S_1$  are linearly independent. By [Eng07, Proposition 11], any height 2 prime ideal  $p$  in  $S$  with  $e(S/p) = 2$  is of the form  $(x, Q)$  where  $x \in S_1, Q \in S_2$  and  $Q$  is irreducible modulo  $x$ .

Suppose next that  $I$  is radical but not prime, so every  $m(p_i) = 1$  and the number of primes  $m$  is greater than 1. Either there is some  $p_i$  such that  $e(S/p_i) = 1$  or we have  $m = 2$  and  $e(S/p_1) = e(S/p_2) = 2$ . In the first case, the ideal  $I$  has a linear minimal prime, and in the second case the ideal  $I$  has two quadratic minimal primes as claimed.  $\square$

As an application we obtain the following structural result for ideals generated by two quadratic forms. This result is a generalization of the structural results in [Shp20, PS20a]. In our result, in addition to providing a new proof of the results in [Shp20, PS20a], we obtain information about the minimal primes of the ideal  $(Q_1, Q_2)$  as well.

**Proposition 1.4** (Radical Structure Theorem). *Let  $\mathbb{K}$  be an algebraically closed field of characteristic zero and  $Q_1, Q_2 \in S = \mathbb{K}[x_1, \dots, x_n]$  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  $xy \in \text{span}(Q_1, Q_2)$ .
  - (b) There exists a minimal prime  $p$  of  $(Q_1, Q_2)$ , such that  $p = (x, y)$  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  $x^2 \in \text{span}(Q_1, Q_2)$ .

- (b)  $Q_1, Q_2$  do not have a common factor. There exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$  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  $x^2 \in \text{span}(Q_1, Q_2)$ .
- (c)  $Q_1, Q_2$  do not have a common factor and there exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$ , 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  $e(S/\mathfrak{q}) \geq 2$ .

*Proof.* Suppose  $(Q_1, Q_2)$  is radical but not prime. If  $Q_1$  is reducible, then it must factor as a product of two linearly independent forms. The ideal then satisfies case 2.(a). The same occurs if  $Q_2$  factors, and therefore we can assume that both  $Q_1, Q_2$  are irreducible. By [Proposition 3.7](#), either  $(Q_1, Q_2)$  has a linear minimal prime, or we have  $(Q_1, Q_2) = (P_1, \ell_1) \cap (P_2, \ell_2)$  with  $(P_i, \ell_i)$  prime and  $P_i \in S_2$ . In the first case, the ideal  $(Q_1, Q_2)$  satisfies 2.(b). Suppose we are in the second case. Then  $Q_i = \alpha_i P_1 + \ell_1 a_i$  for  $\alpha_i \in \mathbb{K}^*$  and  $a_i \in S_1$ , which implies  $\alpha_2 Q_1 - \alpha_1 Q_2 = \ell_1(\alpha_2 a_1 - \alpha_1 a_2)$ . Note that  $\alpha_2 a_1 - \alpha_1 a_2 \notin (\ell_1)$ , otherwise  $(Q_1, Q_2)$  would not be radical. Hence we are in case 2.(a).

Suppose  $(Q_1, Q_2)$  is not a radical ideal. If  $Q_1, Q_2$  have a common factor, then we let  $Q_1 = xy$ ,  $Q_2 = xz$ . If  $x, y, z$  are linearly independent, then we have  $(Q_1, Q_2) = (x) \cap (y, z)$  which is an intersection of prime ideals, hence radical. Since  $(Q_1, Q_2)$  is not radical, we must have that  $x, y, z$  linearly dependent. Therefore  $z = \alpha x + \beta y$  for some  $\alpha, \beta \in k$ . If  $\alpha = 0$ , then  $(Q_1, Q_2) = (xy)$ . Since  $(Q_1, Q_2)$  is not radical, we must have  $x, y$  linearly dependent and then  $x^2 \in \text{span}(Q_1, Q_2)$ . If  $\alpha \neq 0$ , then we see that  $x^2 \in (Q_1, Q_2)$ . Therefore we see that 3.(a) occurs in this case.

Suppose that  $Q_1, Q_2$  do not have a common factor and the ideal  $I = (Q_1, Q_2)$  is not a radical ideal. Let  $I = \bigcap_i \mathfrak{q}_i$  be an irredundant primary decomposition and let  $\mathfrak{p}_i = \text{rad}(\mathfrak{q}_i)$ . Then by [Remark 3.5](#), there exists a minimal prime  $\mathfrak{p}$  such that the multiplicity  $m(\mathfrak{p}) \geq 2$ . Recall that by [Proposition 3.7](#), all the minimal primes of  $I$  are linear or quadratic.

Suppose there exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$ , such that  $\mathfrak{p} = (x, Q)$  for some  $x \in S_1$ ,  $Q \in S_2$  where  $Q$  is irreducible modulo  $x$  and  $m(\mathfrak{p}) \geq 2$ . By [Proposition 3.6](#), we have

$$\sum_i m(\mathfrak{p}_i) e(S/\mathfrak{p}_i) = 4.$$

Note that  $x, Q$  is a regular sequence and hence  $e(S/\mathfrak{p}) = 2$ . Therefore  $m(\mathfrak{p}) \leq 2$ . Hence  $m(\mathfrak{p}) = 2$ , and we must have that  $\mathfrak{p}$  is the only minimal prime and  $I$  is  $\mathfrak{p}$ -primary. Consider the chain of  $S_{\mathfrak{p}}$ -submodules given by  $(0) \subset (x^2) \subsetneq (x) \subsetneq (S/I)_{\mathfrak{p}}$ . Since  $m(\mathfrak{p}) = \text{length}(S/I)_{\mathfrak{p}} = 2$ , we must have  $x^2 = 0$  in  $(S/I)_{\mathfrak{p}}$ . Therefore by [\[AM69, Corollary 10.21\]](#), we conclude that  $x^2 \in I$ . Since  $Q_1, Q_2$  are of degree 2, we must have that  $x^2 \in \text{span}(Q_1, Q_2)$ . In this case, 3.(b) occurs.

Therefore we may assume that all quadratic minimal primes have multiplicity 1. Hence  $\mathfrak{q}_i = \mathfrak{p}_i$  for all quadratic primes  $\mathfrak{p}_i$ . If we have that  $\mathfrak{q}_j = \mathfrak{p}_j$  for all linear primes  $\mathfrak{p}_j$ , then the ideal  $I$  would be a radical ideal. Therefore there exists a linear prime  $\mathfrak{p}_j$  such that the  $\mathfrak{p}_j$ -primary ideal  $\mathfrak{q}_j$  is properly contained in  $\mathfrak{p}_j$ . Then  $(0) \subsetneq \mathfrak{p}_j \subsetneq (S/\mathfrak{q}_j)_{\mathfrak{p}_j}$  is a strict chain of  $S_{\mathfrak{p}_j}$ -submodules. Therefore we have  $\text{length}((S/\mathfrak{q}_j)_{\mathfrak{p}_j}) \geq 2$  and hence,  $e(S/\mathfrak{q}_j) = \text{length}((S/\mathfrak{q}_j)_{\mathfrak{p}_j}) \cdot e(S/\mathfrak{p}_j) \geq 2$ . Thus we see that in case 3, if (a) or (b) do not occur then case (c) must occur.  $\square$

As immediate corollaries of [Proposition 1.4](#), we obtain the structural results proved in [\[Shp20, PS20a\]](#). Note that, unlike in the results of [\[Shp20, PS20a\]](#), in our [Proposition 1.4](#) we do not use the existence of a third quadratic or a product of quadratics in the radical of  $(Q_1, Q_2)$ .

**Corollary 3.8** (Theorem 29 in [\[Shp20\]](#)). *Let  $Q_1, Q_2, Q_3$  be quadratic forms such that  $Q_3 \in \text{rad}(Q_1, Q_2)$ . One of the following holds:*

1. The polynomial  $Q_3$  is in the linear span of  $Q_1$  and  $Q_2$ .

2. There exists a linear form  $\ell$  such that  $\ell^2$  is in the linear span of  $Q_1$  and  $Q_2$ .
3. There exist linear forms  $x$  and  $y$  such that  $Q_1, Q_2, Q_3$  all belong to the ideal  $(x, y)$ .

*Proof.* If  $Q_1, Q_2$  satisfy condition 1 or 2 of Theorem 1.4, then we see that  $Q_3 \in \text{rad}(Q_1, Q_2) = (Q_1, Q_2)$ . Since  $Q_1, Q_2, Q_3$  are all degree 2 forms, we must have  $Q_3 \in \text{span}(Q_1, Q_2)$ . If  $Q_1, Q_2$  satisfy conditions 3.(a) or 3.(b) of Theorem 1.4, then we see that case 2 above holds. Otherwise, condition 2.(c) must hold, and there is a prime ideal  $(x, y)$  such that  $(Q_1, Q_2) \subset (x, y)$ . Then we also have  $Q_3 \in \text{rad}(Q_1, Q_2) \subset (x, y)$ .  $\square$

**Corollary 3.9** (Theorem 3.1 in [PS20a]). *Let  $Q_1, Q_2, P_1, \dots, P_k$  be quadratic forms such that  $\prod_i P_i \in \text{rad}(Q_1, Q_2)$ . Then one of the following cases holds:*

1. There exists  $i \in [k]$  such that  $P_i \in \text{span}(Q_1, Q_2)$ .
2. There exists a non-trivial linear combination of the form  $\alpha Q_1 + \beta Q_2 = xy$  where  $x, y$  are linearly independent linear forms.
3. There exist two linear forms  $x, y$  such that  $Q_1, Q_2, \prod_i P_i \in (x, y)$ .

*Proof.* If  $Q_1, Q_2$  satisfy condition 1 of Theorem 1.4, then  $(Q_1, Q_2)$  is a prime ideal. Hence we have  $P_i \in (Q_1, Q_2)$  for some  $i$ . Since  $P_i$  is of degree 2, we see that in this case we must have  $P_i \in \text{span}(Q_1, Q_2)$ . If  $Q_1, Q_2$  satisfy one of the conditions 2.(a), 3.(a) or 3.(b), then we see that case 2 above holds. Otherwise,  $Q_1, Q_2$  must satisfy one of conditions 2.(b) or 3.(c), then we see that case 3 above occurs.  $\square$

We now prove some structural results for quadratics with linear minimal primes.

**Proposition 3.10** (Structure of  $(x, y)$ -primary ideals of  $(Q_1, Q_2)$ ). *Let  $Q_1, Q_2 \in S_2$  be two irreducible forms such that  $\mathbb{L}(Q_1) \neq \mathbb{L}(Q_2)$ . Suppose  $(Q_1, Q_2)$  is not a radical ideal and  $\text{span}(Q_1, Q_2)$  does not contain the square of any linear form. Then the following holds.*

1. There exists a linear minimal prime  $(x, y)$  of  $(Q_1, Q_2)$  where  $x, y \in S_1$  are linearly independent forms, and  $(x, y^2)$  is the  $(x, y)$ -primary component of  $(Q_1, Q_2)$ .
2. There exist  $a, b \in S_1$  such that  $\dim(\text{span}_{\mathbb{C}}\{x, y, a, b\}) = 4$  and

$$Q_1 = ax + y^2, \quad Q_2 = bx + y^2.$$

*Proof.* By our assumption the cases 1, 2.(a), 2.(b) of Theorem 1.4 cannot occur. Therefore case 2.(c) must occur and hence there exists a minimal prime  $\mathfrak{p}$  of  $(Q_1, Q_2)$ , 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  $e(S/\mathfrak{q}) \geq 2$ . Note that by Proposition 3.6, we have  $e(S/\mathfrak{q}) \leq 4$ . By checking the classification of  $(x, y)$ -primary ideals of multiplicity  $\leq 4$  from [MM18], we see that the only case in which  $\mathfrak{q}$  can contain two irreducible quadratics  $Q_1, Q_2$  with  $\mathbb{L}(Q_1) \neq \mathbb{L}(Q_2)$  is case 1 of [MM18, Proposition 1.1]. Thus, after a linear change of variables we must have  $\mathfrak{q} = (x, y^2)$  and since  $\mathbb{L}(Q_1) \neq \mathbb{L}(Q_2)$  we must have (up to scalar multiplication)  $Q_1 = ax + y^2$  and  $Q_2 = bx + y^2$  where  $a, b, x, y$  are linearly independent. This concludes this proof.  $\square$

**Proposition 3.11.** *If  $a, b, x, y \in S_1$  are linearly independent forms and  $Q_1 = ax + y^2, Q_2 = bx + y^2$ , then*

$$\text{rad}(Q_1, Q_2) = (Q_1, Q_2, y(a - b))$$



*Proof.* We claim that the minimal primes of the ideal  $(Q_1, Q_2)$  are  $(x, y)$  and  $(Q_1, a - b)$ . We first show that these ideals are prime, and then show that they are the minimal primes.

That  $(x, y)$  is prime follows from the fact that it is generated by two linear forms. To show that  $(Q_1, a - b)$  is prime, it suffices to show that  $Q_1$  is irreducible in the ring  $S/(a - b)$ , since the latter is isomorphic to a polynomial ring.

If  $Q_1$  factors in  $S/(a - b)$ , then  $ax + y^2 = cd$  in  $S/(a - b)$ , for linear forms  $c, d$ . Quotienting further by  $c$ , we get that  $a, x \in (y)$  in  $S/(a - b, c)$ . This implies  $\text{span}_{\mathbb{K}}\{a, b, x, y\} \subset \text{span}_{\mathbb{K}}\{a, x, y, a - b, c\} = \text{span}_{\mathbb{K}}\{y, a - b, c\}$ , contradicting  $\dim \text{span}_{\mathbb{K}}\{a, b, x, y\} = 4$ . This shows that  $(Q_1, a - b)$  is prime.

Suppose  $P$  is a minimal prime containing  $(Q_1, Q_2)$ . The ideal  $P$  contains  $aQ_2 - bQ_1 = y^2(a - b)$ . Since  $P$  is prime, it must contain either  $y$  or  $(a - b)$ . If  $P$  contains  $a - b$ , then  $P$  clearly contains  $(Q_1, a - b)$  and by minimality we must have  $P = (Q_1, a - b)$ . If  $P$  contains  $y$ , then  $P$  must also contain  $ax = Q_1 - y^2$  and  $bx = Q_2 - y^2$ . If  $P$  contains  $x$ , then  $P$  contains  $(x, y)$  and by minimality we have  $P = (x, y)$ . If  $P$  does not contain  $x$ , then  $P$  contains both  $a, b$  which contradicts  $\text{ht } P = 2$ . This shows that the minimal primes of  $(Q_1, Q_2)$  are  $(x, y)$  and  $(Q_1, a - b)$ .

The radical of any ideal is the intersection of its minimal primes, and therefore  $\text{rad}(Q_1, Q_2) = (x, y) \cap (Q_1, a - b)$ . Suppose  $f$  is an arbitrary polynomial in the intersection. We have  $f = g_1x + g_2y = g_3Q_1 + g_4(a - b)$  for polynomials  $g_1, \dots, g_4$ . Since  $Q_1$  is in the ideal  $(x, y)$ , so is  $g_4(a - b)$ . Since  $a, b, x, y$  are linearly independent,  $g_4$  is in the ideal  $(x, y)$ . This shows that  $f$  is in the ideal  $(Q_1, x(a - b), y(a - b))$ . Conversely, every element of this ideal is in the intersection of  $(x, y)$  and  $(Q_1, a - b)$ . This shows that  $\text{rad}(Q_1, Q_2) = (Q_1, x(a - b), y(a - b)) = (Q_1, Q_2, y(a - b))$ .  $\square$

## 4 Clean vector spaces

In this section, we define clean vector spaces and prove some useful properties about them, which will be used in our robust Sylvester-Gallai proof.

### 4.1 Closeness and robust vector spaces

For any quadratic form  $P \in S$  we would like to measure how far  $P$  is from a subalgebra  $\mathbb{C}[V]$  generated by a vector space of forms in  $S$ . The next definition quantifies the notion of distance from a subalgebra generated by a vector space.

**Definition 4.1** (Forms 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 form  $P$  is  $s$ -close to  $V$  if there is a form  $Q \in \mathbb{C}[V]$  such that  $\text{rank}(P - Q) = s$ , and for any form  $Q' \in \mathbb{C}[V]$ , we have that  $\text{rank}(P - Q') \geq s$ . If a form  $P$  is not  $r$ -close to  $V$ , for any  $r \leq s$ , we say that  $P$  is  $s$ -far from  $V$ .

Given a linear form  $\ell$ , we say  $\ell$  is 1-close to  $V$  if  $\ell \notin V_1$ .

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 4.2** (Robust vector spaces). A vector space  $V = V_1 + V_2$  where  $V_i \subseteq S_i$  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 an  $r$ -robust generating set  $V_1 + V_2$ , we say that  $I$  is an  $r$ -robust ideal.

*Remark 4.3.* Note that if  $Q \notin (V_1)$ , then condition 2 implies condition 1 for  $Q$ . Indeed, suppose  $\text{rank}(Q - F) < r$  for some degree 2 form  $F \in \mathbb{C}[V_1]$ . Then  $\text{rank}(\bar{Q}) < r$ , since  $\bar{F} = 0$  modulo  $(V_1)$ . This is a contradiction to condition 2, therefore we must have  $\text{rank}(Q - F) \geq r$  for any degree 2 form  $F \in \mathbb{C}[V_1]$ . Therefore, in order to check that a vector space  $V = V_1 + V_2$  is  $r$ -robust, it is enough to ensure that condition 1 holds for all  $Q \in V_2 \cap (V_1)$  and condition 2 holds for all  $Q \in V_2 \setminus (V_1)$ .

**Example 4.4.** (a) Let  $V_1$  be any subspace of  $S_1$ , and  $V_2 = (0)$ , then  $V = V_1 + V_2$  is an  $r$ -robust vector space for any  $r$ .

(b) Suppose  $Q_1, \dots, Q_m$  are quadratic forms such that  $\text{rank}(Q) \geq r$  for any  $Q \in \text{span}(Q_1, \dots, Q_m)$ . Let  $V_1 = (0)$ ,  $V_2 = \text{span}(Q_1, \dots, Q_m)$ . Then  $V = V_1 + V_2$  is an  $r$ -robust vector space.

(c) Let  $S = \mathbb{C}[x_1, \dots, x_r, y_1, \dots, y_r, u_1, \dots, u_r]$  and  $Q_1 = x_1 y_1 + \dots + x_r y_r$ ,  $Q_2 = u_1 y_1 + \dots + u_r y_r$ . Let  $V_1 = \text{span}(x_1, \dots, x_r)$ ,  $V_2 = \text{span}(Q_1, Q_2)$ . Then we can show that  $V_1 + V_2$  is a  $r$ -robust vector space.

Let  $Q = aQ_1 + bQ_2 \in V_2$  for some  $a, b \in \mathbb{C}$ . Note that  $Q \in (V_1)$  if and only if  $b = 0$ . Suppose,  $Q \notin (V_1)$ . Then  $\bar{Q} = b\bar{u}_1\bar{y}_1 + \dots + b\bar{u}_r\bar{y}_r$  where  $\bar{u}_i, \bar{y}_j$  denote the images of  $u_i, y_j$  modulo  $(V_1)$ . Hence  $\text{rank}(\bar{Q}) = r$ . Therefore condition 2, and consequently condition 1, holds if  $Q \in V_2 \setminus (V_1)$ .

Now suppose  $Q \in V_2 \cap (V_1)$ . Then  $Q = ax_1 y_1 + \dots + ax_r y_r$ . Let  $F = \sum_i a_{ii} x_i^2 + \sum_{i < j} 2a_{ij} x_i x_j$ , and  $A$  be the  $r \times r$  matrix with the  $(i, j)$ -th entry given by  $a_{ij}$ . Let  $M$  and  $N$  denote the matrices corresponding to the quadratic forms  $Q, F$  in  $S$ . Note that we have

$$M = \begin{pmatrix} 0 & \frac{a}{2} I_{r \times r} & 0 \\ \frac{a}{2} I_{r \times r} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, N = \begin{pmatrix} A & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where  $I_{r \times r}$  denotes the  $r \times r$  identity matrix. Note that the matrix corresponding to  $Q - F$  is given by  $M - N$ . Note that  $\text{rank}(M - N) = \text{rank } M$ , and hence  $\text{rank}(Q - F) \geq r$ .

**Claim 4.5.** Suppose  $V := V_1 + V_2$  is  $r$ -robust with  $V_i \subset S_i$ . If  $Q \in \mathbb{C}[V]$  is a quadratic form of rank less than  $r$ , then  $Q \in \mathbb{C}[V_1]$ . If  $P \in (V)$  is a quadratic form of rank less than  $r$ , then  $P \in (V_1)$ .

*Proof.* Since  $Q \in \mathbb{C}[V]$ , and since  $Q$  has degree 2, we have  $Q = Q_1 + Q_2$  with  $Q_2 \in V_2$  and  $Q_1 \in \mathbb{C}[V_1]$ . If  $Q_2 \neq 0$ , then  $Q_2 - (-Q_1)$  has rank less than  $r$ , which contradicts the robustness of  $V$ . Therefore we have  $Q_2 = 0$ . If  $P = P_1 + P_2$  with  $P_1 \in (V_1)$  and  $P_2 \in V_2$ , then  $\bar{P}_2$  has rank at most  $\text{rank } P < r$  in  $S/(V_1)$ , and therefore  $P_2 \in (V_1)$ .  $\square$

**Proposition 4.6.** If  $V := V_1 + V_2$  is a 5-robust vector space and  $x, y, u, v \in S_1$  such that  $xy - uv \in \mathbb{C}[V]$  then one of the following holds:

1. We have  $x, y, u, v \in V_1$ .
2. There exists a linear form  $\ell \in S_1 \setminus V_1$  such that  $x, y, u, v \in \text{span}_{\mathbb{C}}\{V_1, \ell\}$ .

*Proof.* Let  $P := xy - uv$ . Note that  $\text{rank}(P) \leq 2$ . Since  $P$  is of degree 2, we have  $P \in \mathbb{C}[V_1]$  by Claim 4.5. Since  $P \in \mathbb{C}[V_1]$ , we know that  $\text{Lin}(P) \subset V_1$  by [PS20a, Fact 2.14]. Now, Lemma 2.8 applies and we are done.  $\square$

Another important property of robust vector spaces is that we can get a good control on the vector spaces  $\mathbb{L}(P)$  whenever  $P$  is almost in the algebra. This is captured by the following proposition, which motivates the subsequent definition of relative space of linear forms.

**Proposition 4.7** (Quadratics close to robust vector spaces). *Let  $V = V_1 + V_2$  be an  $r$ -robust vector space and  $s < r/2$ . If  $P$  is  $s$ -close to  $V$ , then for any  $Q, Q' \in \mathbb{C}[V]$  such that  $\text{rank}(P - Q) = \text{rank}(P - Q') = s$ , we have that*

$$\text{Lin}(P - Q) + V_1 = \text{Lin}(P - Q') + V_1.$$

*In other words,  $(\text{Lin}(P - Q) + V_1)/V_1 = (\text{Lin}(P - Q') + V_1)/V_1$  for any two decompositions.*

*Proof.* Let  $R = P - Q$  and  $R' = P - Q'$ . Thus, we have that  $R - R' = Q' - Q \in \mathbb{C}[V]$  and we have  $\text{rank}(Q' - Q) = \text{rank}(R - R') \leq \text{rank}(R) + \text{rank}(R') \leq 2s < r$ . Hence, by Remark 4.5, we have that  $Q' - Q \in \mathbb{C}[V_1]$ . Now, from  $R = R' + (Q' - Q)$  and  $Q' - Q \in \mathbb{C}[V_1]$ , we have that  $\text{Lin}(R) \subseteq \text{Lin}(R') + V_1$ , and similarly, we have that  $\text{Lin}(R') \subseteq \text{Lin}(R) + V_1$ .  $\square$

The above proposition motivates us to define the relative space of linear forms with respect to a robust algebra.

**Definition 4.8** (Relative space of linear forms). Let  $r \geq 9$  be an integer. If  $V$  is an  $r$ -robust vector space and  $P$  is  $s$ -close to  $V$  for  $s < r/2$  we can define

$$\mathbb{L}_V(P) := \begin{cases} \mathbb{L}(P) + V_1, & \text{if } P \in S_1 \\ \mathbb{L}(P - Q) + V_1, & \text{if } P \in S_2, s \leq 4 \\ \text{span}_{\mathbb{C}}\{P\}, & \text{otherwise} \end{cases}$$

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

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

## 4.2 Clean vector spaces

We are now ready to define the main object of this section: Clean vector spaces.

**Definition 4.9** (Clean vector spaces). Let  $r \geq 17$  be an integer and  $\varepsilon \in (0, 1)$ . Let  $\mathcal{F} := \{Q_1, \dots, Q_m\} \subset S_{\leq 2}$  be a set of forms. Let  $V = V_1 + V_2$  be a vector space with  $V_i \subset S_i$ . We say that  $V$  is an  $(r, \varepsilon)$ -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 less than  $\varepsilon m$  forms  $Q_j \in \mathcal{F}$  such that  $Q_j$  is  $s$ -close to  $V$  for  $1 \leq s \leq 4$  and

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

*Remark 4.10.* The vector space  $V + U_1$  is  $r - 8$  robust, since  $U_1$  consists only of linear forms and has dimension at most 8. Since  $r - 8 \geq 9$ , the space  $\dim(\bar{\mathbb{L}}_{V+U_1}(Q_j))$  is well defined.

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

*Remark 4.11.* Condition 2 in Definition 4.9 simply captures the concept that  $Q_j$  becomes closer to being in the algebra  $\mathbb{C}[V, U_1]$ . Thus, a clean ideal is one where no small dimensional vector space would bring many forms in our set closer to being in the augmented algebra.

The following lemma proves that one can clean up ideals over a set of quadratic forms without increasing the number of generators by much.

**Lemma 4.12** (Cleaning up vector spaces). *Let  $\mathcal{F}$  be a set of forms,  $J = J_1 + J_2$  be a vector space, and  $d_i = \dim(J_i)$ . Given  $r \in \mathbb{Z}$  such that  $r \geq 17$  and  $0 < \varepsilon < 1$ , there exists an  $(r, \varepsilon)$ -clean vector space  $I = I_1 + I_2$  over  $\mathcal{F}$  such that:*

1.  $\mathbb{C}[J] \subset \mathbb{C}[I]$
2.  $I_2 \subset J_2$  and  $J_1 \subset I_1$
3.  $\dim(I_1) = \frac{128}{\varepsilon} + d_1 + 4 \cdot d_2 \cdot r$

*Proof.* Let  $\mathcal{F} = \{Q_1, \dots, Q_m\}$ . Starting with the given vector space  $J$ , we will iteratively construct a vector space  $I$  that satisfies the desired properties. Our proof consists of three steps. First, we will define the iterative process to clean up a vector space. Second, we will show that this iterative process actually terminates after at most  $16/\varepsilon$  steps. Finally, we will show that the final output of the iterative process satisfies all the desired properties.

*The iterative processes.* We will devise two processes to clean up the initial vector space  $J$ , and the final iterative process will be a combination of these two. The first process helps us achieve robustness and the second process helps us clean up the vector space. In order to obtain the vector space  $I$ , we will apply both these processes repeatedly.

- **Robustness process:** Let  $V' = V'_1 + V'_2$  be a vector space with  $V'_i \subset S_i$ . Start with the vector spaces  $V_1 := V'_1$ ,  $V_2 := V'_2$  and  $V := V_1 + V_2$ . Perform the following two steps till it is not possible to perform either of them:
  - If there exists a non-zero form  $P \in V_2$  such that  $\text{rank}(P - R) < r$  for some  $R \in \mathbb{C}[V_1]$ , set  $V_1 := V_1 + \text{Lin}(P - R)$ , and replace  $V_2$  by a codimension 1 subspace of  $V_2$  that does not contain  $P$ .
  - If there exists a non-zero form  $P \in V_2 \setminus (V_1)$  such that  $P = P_1 + Q'$  with  $P_1 \in (V_1)$  and  $\text{rank}(Q') < r$ , set  $V_1 := V_1 + \text{Lin}(Q')$ .

The above two steps correspond to the two conditions in the definition of robustness. If we cannot perform either of the above two steps, then the vector space  $V$  that we end up with is  $r$ -robust. We have  $V_2 \subseteq V'_2$  and  $V'_1 \subseteq V_1$ . It is also easy to see that both steps above maintain the inclusion  $\mathbb{C}[V'] \subseteq \mathbb{C}[V]$ .

We now control how many times the above steps can be performed. Each time we perform the first step, we decrease  $\dim V_2$  by 1, and therefore the first step can be performed a total of  $\dim(V'_2)$  times. Each time we perform the second step, we decrease  $\dim \overline{V_2}$  by 1, where  $\overline{V_2}$  is the space  $V_2$  quotiented by the vector space  $(V_1) \cap V_2$ . Therefore, the second step can also be performed at most  $\dim(V'_2)$  times. Hence, this iterative process always halts, and it does so in at most  $2 \dim(V'_2)$  steps. Further, each time we perform either step, we increase the dimension of  $V_1$  by at most  $2r$ .

- **Clean-up process:** Let  $V' = V'_1 + V'_2$  be a vector space with  $V'_i \subset S_i$ . Start with the vector spaces  $V_1 := V'_1$ ,  $V_2 := V'_2$  and  $V = V_1 + V_2$ . While there exists  $U_1 \subseteq S_1$  such that  $U_1$  violates the condition that  $V$  is  $(r, \varepsilon)$ -clean (i.e. condition 2 of [Definition 4.9](#)), update  $V_1 := V_1 + U_1$ .

Note that we have  $V'_1 \subset V_1 \subset S_1$  and  $V_2 = V'_2$ . Thus,  $V' \subset \mathbb{C}[V]$  by our construction. The space  $U_1$  has dimension at most 8, and therefore the dimension of  $V_1$  increases by at most 8 whenever we apply this procedure.

Now, we can design our main iterative process:

1. Start with our vector space  $W^{(0)} := J$
2. Apply the robustness process to  $W^{(0)}$  to obtain  $U^{(0)}$
3. While  $U^{(k)}$  is not  $(r, \varepsilon)$ -clean vector space over  $\mathcal{F}$ 
  - Let  $W^{(k+1)}$  be a vector space that we obtain after applying the clean-up process once to  $U^{(k)}$
  - Let  $U^{(k+1)}$  be the space we obtain after applying the robustness process to  $W^{(k+1)}$

*Termination.* We will now show that the iterative process must terminate after at most  $16/\varepsilon$  steps. We define the following potential function for  $U := U_1 + U_2$  a  $r$ -robust vector space:

$$\Phi(\mathcal{F}, U) = \sum_{i=1}^m \dim \bar{\mathbb{L}}_U(Q_i).$$

Note that this potential function is always non-negative and upper bounded by  $8 \cdot m$ .

Let  $\Phi_k := \Phi(\mathcal{F}, U^{(k)})$  be the potential function that we defined above applied to the robust vector space  $U^{(k)}$ . If  $U^{(k)}$  violates condition 2 of [Definition 4.9](#) (clean vector space), there exists  $L_1 \subset S_1$  and there are at least  $\varepsilon m$  forms  $Q_j \in \mathcal{F}$  such that  $Q_j$  is  $s$ -close to  $U^{(k)}$ , for  $1 \leq s \leq 4$  and

$$\begin{aligned} \dim \bar{\mathbb{L}}_{U^{(k)}}(Q_j) &= \dim \left( \mathbb{L}_{U^{(k)}}(Q_j) / U_1^{(k)} \right) \\ &> \dim \left( \mathbb{L}_{U^{(k)}+L_1}(Q_j) / (U_1^{(k)} + L_1) \right) \\ &\geq \dim \left( \mathbb{L}_{U^{(k+1)}}(Q_j) / U_1^{(k+1)} \right) = \dim \bar{\mathbb{L}}_{U^{(k+1)}}(Q_j). \end{aligned}$$

If we denote by  $\mathcal{B}_k$  be the set of such  $Q_j$ 's, we have  $|\mathcal{B}_k| \geq \varepsilon m$ .

Let  $\mathcal{N}_k$  be the set of forms  $Q_j \in \mathcal{F}$  that are 4-far from  $U^{(k)}$  but are at most 4-close to  $U^{(k+1)}$ . For any  $Q_j \in \mathcal{N}_k$ , we have that  $\dim \bar{\mathbb{L}}_{U^{(k)}}(Q_j) = 0$  and  $\dim \bar{\mathbb{L}}_{U^{(k+1)}}(Q_j) \leq 8$ . Moreover, note that  $\mathcal{N}_a \cap \mathcal{N}_b = \emptyset$  for any  $a < b$ , since  $\mathbb{C}[U^{(k)}] \subset \mathbb{C}[U^{(k+1)}]$ . Also,  $\mathcal{N}_k \cap \mathcal{B}_k = \emptyset$ .

Then, we have

$$\begin{aligned} \Phi_k - \Phi_{k+1} &= \sum_{i=1}^m (\dim \bar{\mathbb{L}}_{U^{(k)}}(Q_i) - \dim \bar{\mathbb{L}}_{U^{(k+1)}}(Q_i)) \\ &\geq \sum_{Q_i \in \mathcal{B}_k} (\dim \bar{\mathbb{L}}_{U^{(k)}}(Q_i) - \dim \bar{\mathbb{L}}_{U^{(k+1)}}(Q_i)) - \sum_{Q_i \in \mathcal{N}_k} \dim (\bar{\mathbb{L}}_{U^{(k+1)}}(Q_i)) \\ &\geq |\mathcal{B}_k| - 8|\mathcal{N}_k| \\ &\geq \varepsilon m - 8|\mathcal{N}_k|, \end{aligned}$$

where the first inequality holds because for any term not in  $\mathcal{N}_k$ , we have that  $\dim \bar{\mathbb{L}}_{U^{(k)}}(Q_i) \geq \dim \bar{\mathbb{L}}_{U^{(k+1)}}(Q_i)$ . The second inequality holds because for the elements in  $\mathcal{B}_k$  the dimension drops by at least 1. The last inequality holds because we know that  $|\mathcal{B}_k| \geq \varepsilon m$ .

Now, if our iterative process runs for  $t$  iterations, we have that

$$\begin{aligned}\Phi_0 - \Phi_t &= \sum_{k=0}^{t-1} \Phi_k - \Phi_{k+1} \\ &\geq t\epsilon m - 8 \cdot \sum_{k=0}^{t-1} |\mathcal{N}_k| \\ &\geq t\epsilon m - 8m\end{aligned}$$

where the last inequality holds because the sets  $\mathcal{N}_k$  are pairwise disjoint and contained in  $\mathcal{F}$ . Since  $0 \leq \Phi_k \leq 8m$  by the discussion in the first paragraphs of the proof, we have that  $t\epsilon m \leq 16m$ , which implies  $t \leq 16/\epsilon$ . In particular, this shows that our process will terminate.

*Desired properties.* Let  $I := \mathcal{U}^{(t)}$  be the final vector space we obtained at the end of this process. By the above, we have that  $I$  is  $(r, \epsilon)$ -clean over  $\mathcal{F}$ , as the process terminated. Moreover, note that  $\mathbb{C}[J] \subseteq \mathbb{C}[I]$ , as the inclusion  $\mathbb{C}[\mathcal{U}^{(k)}] \subseteq \mathbb{C}[\mathcal{U}^{(k+1)}]$  is preserved throughout the process, and  $\mathbb{C}[J] \subseteq \mathbb{C}[\mathcal{U}^{(0)}]$  by construction. We also have that  $I_2 \subseteq J_2$ , since the robustness process preserves  $\mathcal{U}_2^{(k+1)} \subseteq \mathcal{U}_2^{(k)}$ , and the clean-up process preserves  $\mathcal{U}_2^{(k+1)} = \mathcal{U}_2^{(k)}$ , and  $\mathcal{U}^{(0)} \subset J_2$ . Additionally, we have that  $J_1 \subseteq I_1$ , as both processes only increase the size of  $\mathcal{U}^{(k)}$ .

Now, all we have left is to bound the dimension of  $I_1$ . For this, note that each run of the clean-up process adds a space of linear forms of dimension at most 8, and therefore the total contribution from the clean-up process is  $128/\epsilon$ . To see that the total contribution of the robustness process is at most  $4r \cdot d_2$ , note that the first step of the process strictly decreases  $\dim(\mathcal{U}_2^{(k)})$ , whereas the second step of the process strictly increases  $\dim(\mathcal{U}_2^{(k)} \cap (\mathcal{U}_1^{(k)}))$ . Moreover, if  $\dim(\mathcal{U}_2^{(k)} \cap (\mathcal{U}_1^{(k)})) = \dim(\mathcal{U}_2^{(k)})$  from this point on we can only apply the first step of the process. Finally, note that the clean-up process does not change the degree two part of the vector space. Hence, we can apply the first step of the process at most  $d_2$  times, and the second process at most  $d_2$  times throughout the entire iterative process. Note that each time we apply the foregoing steps, we increase the dimension of the linear piece by at most  $2r$ . Putting everything together, we have that  $\dim(I_2) \leq d_1 + 128/\epsilon + 4r \cdot d_2$ , as we wanted.  $\square$

*Remark 4.13.* Note that in the process above, if  $\mathcal{F} \subset (J)$ , then  $\mathcal{F} \subset (I)$ .

The clean up process is similar to a process used in [PS20a] and [PS20b], where they find an ideal  $V$  generated by linear forms, and a subset  $\mathcal{J}$  of quadratic forms such that every quadratic in their configuration is in the span of elements of  $\mathcal{J}$ , and elements of  $\mathcal{F} \cap (V)$ . They then iteratively find quadratic forms in  $\mathcal{F}$  that have rank 2 in  $S/(V_1)$ . If such a form is found, they add the linear forms to  $V_1$ , and remove a quadratic from  $\mathcal{J}$ . This iterative process does not preserve the algebra generated by  $V$  and  $\mathcal{J}$ . In other words, a form  $Q \in \mathcal{F}$  that lies in  $\mathbb{C}[V, \mathcal{J}]$  might not be in the algebra after one step of the iterative process (although  $Q$  is still guaranteed to be in the ideal generated by  $V, \mathcal{J}$ , and  $Q$  satisfies the stronger property that it is spanned by elements of  $\mathcal{J}$  and  $\mathcal{F} \cap (V)$ ). We require that all forms remain in the algebra, and therefore our clean up process is more involved.

### 4.3 Univariate forms over clean vector spaces

We now turn our attention to a special case of forms which are 1-close to a robust vector space.

**Definition 4.14** (Univariate forms 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  $\dim(\overline{\mathbb{L}}_V(P)) = 1$ . Moreover, we define  $z_P \in S_1/V_1$  to be the linear form such that  $\overline{\mathbb{L}}_V(P) := \text{span}_{\mathbb{C}}\{z_P\}$ .<sup>7</sup>

Once again, given a 3-robust vector space  $V$ , we will also say that a form  $P$  is univariate over the algebra  $\mathbb{C}[V]$  if  $P$  is univariate over  $V$  as in the definition above.

*Remark 4.15.* An immediate consequence of the definition above is that if  $P$  is a quadratic form univariate over  $V$ , then  $P \in \mathbb{C}[V, z_P]$ . Moreover, we can write  $P = Q + z(\alpha z + v)$  where  $Q \in \mathbb{C}[V]$ ,  $\alpha \in \mathbb{C}$  and  $v \in V_1$ . Thus,  $P \in (V) \iff \alpha = 0$ .

Having univariate forms over a clean vector space is desirable because if our SG configuration only has univariate forms over a clean vector space, one would expect the ‘‘extra variables’’ to behave as a LCC configuration. As mentioned in the proof outline, this is indeed the case, and in the next section we will formalize this intuition about the extra variables.

## 5 Proof of the robust Sylvester Gallai theorem

In this section we prove our main theorem:  $(\delta, 2)$ -rad-SG configurations (Definition 1.2) have constant dimension as a  $\mathbb{C}$ -vector space. Throughout this section, we will assume  $\varepsilon := \delta/10$ .

**Theorem 1.3** ( $(\delta, 2)$ -rad-SG theorem). *If  $\mathcal{F}$  is a  $(\delta, 2)$ -rad-SG configuration, then*

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

Before we prove the theorem above, we need some definitions. Let  $\mathcal{F}$  be our  $(\delta, 2)$ -rad-SG configuration, where we write  $\mathcal{F} = \mathcal{F}_1 \sqcup \mathcal{F}_2$  such that  $\mathcal{F}_i = \mathcal{F} \cap S_i$  and let  $m := |\mathcal{F}|$ . We will assume that  $m > 1/\delta^{54}$ , since the statement trivially holds if it is not.

For a form  $Q \in \mathcal{F}_2$ , define the sets

$$\begin{aligned} \mathcal{F}_2(Q) &:= \{Q' \in \mathcal{F}_2 \mid |\text{rad}(Q, Q') \cap \mathcal{F}| \geq 3\} \\ \mathcal{F}_1(Q) &:= \{x \in \mathcal{F}_1 \mid |\text{rad}(Q, x) \cap \mathcal{F}| \geq 3\}. \end{aligned}$$

The sets above account for the quadratic and linear Sylvester-Gallai pairs related to  $Q$ . We also partition  $\mathcal{F}_2(Q)$  into three sets,  $\mathcal{F}_{\text{span}}(Q)$ ,  $\mathcal{F}_{\text{linear}}(Q)$  and  $\mathcal{F}_{\text{square}}(Q)$ . These are the sets of forms in  $\mathcal{F}$  that satisfy the span case, linear case, and the square case of Proposition 1.4 with  $Q$ . The formal definitions of the sets are as follows.

$$\begin{aligned} \mathcal{F}_{\text{span}}(Q) &= \{Q' \in \mathcal{F}_2(Q) \mid |(Q, Q') \cap \mathcal{F}| \geq 3\} \\ \mathcal{F}_{\text{square}}(Q) &= \{Q' \in \mathcal{F}_2(Q) \setminus \mathcal{F}_{\text{span}}(Q) \mid \exists \ell \in S_1, \ell^2 = \alpha Q + \beta Q'\} \\ \mathcal{F}_{\text{linear}}(Q) &= \{Q' \in \mathcal{F}_2(Q) \setminus (\mathcal{F}_{\text{span}}(Q) \cup \mathcal{F}_{\text{square}}(Q)) \mid \exists x, y \in S_1, Q, Q' \in (x, y)\} \end{aligned}$$

Since  $\mathcal{F}$  is a  $(\delta, 2)$ -SG configuration, for each  $Q \in \mathcal{F}_2$  we have

$$|\mathcal{F}_{\text{span}}(Q) \sqcup \mathcal{F}_{\text{linear}}(Q) \sqcup \mathcal{F}_{\text{square}}(Q) \sqcup \mathcal{F}_1(Q)| \geq \delta m.$$

We define sets  $\mathcal{F}_{\text{span}}, \mathcal{F}_{\text{linear}}, \mathcal{F}_{\text{square}}$  and  $\mathcal{F}_{\text{deg}}$  that partition  $\mathcal{F}_2$  as follows.

---

<sup>7</sup>More precisely, we can take  $z_P$  in the  $S$  canonically simply by identifying the quotient polynomial ring with a polynomial ring in less variables. For simplicity, we will abuse notation in this setting.

$$\begin{aligned}
\mathcal{F}_{\text{span}} &= \{Q \in \mathcal{F}_2 \mid |\mathcal{F}_{\text{span}}(Q)| \geq \varepsilon m\} \\
\mathcal{F}_{\text{linear}} &= \{Q \in \mathcal{F}_2 \setminus \mathcal{F}_{\text{span}} \mid |\mathcal{F}_{\text{linear}}(Q)| \geq \varepsilon m\} \\
\mathcal{F}_{\text{deg}} &= \{Q \in \mathcal{F}_2 \setminus \mathcal{F}_{\text{span}} \cup \mathcal{F}_{\text{linear}} \mid |\mathcal{F}_1(Q)| \geq \varepsilon m\} \\
\mathcal{F}_{\text{square}} &= \{Q \in \mathcal{F}_2 \setminus (\mathcal{F}_{\text{span}} \cup \mathcal{F}_{\text{linear}} \cup \mathcal{F}_{\text{deg}}) \mid |\mathcal{F}_{\text{square}}(Q)| \geq (\delta - 3\varepsilon)m\}
\end{aligned}$$

By [Proposition 1.4](#), every form in  $\mathcal{F}_2$  belongs to one of the above sets. We will now begin constructing small algebras which control the sets defined above.

### 5.1 Controlling $\mathcal{F}_{\text{square}}$

The following lemma from [[Shp20](#), Corollary 43] controls the vector space dimension of the set of forms satisfying the square case with two quadratic forms.

**Lemma 5.1.** *Let  $Q_1, Q_2 \in S_2$  be linearly independent and  $F_1, \dots, F_m \in S_2$  such that*

$$F_i = Q_1 + \ell_i^2 = \beta_i Q_2 + b_i^2$$

where  $\ell_i, b_i \in S_1$  and  $\beta_i \in \mathbb{C}$ . Then, there is a vector space  $V$  of dimension at most 4 that contains every  $\ell_i$  and  $b_i$ . In particular, every  $F_i \in \mathbb{C}[Q_1, V]$ , which implies  $\dim \text{span}_{\mathbb{C}}\{Q_1, Q_2, F_1, \dots, F_m\} \leq 7$ . We will denote this vector space  $V$  as  $V(Q_1, Q_2)$ .

If  $P_1, P_2, \dots, P_b$  are the forms in  $\mathcal{F}_{\text{square}}$ , [Lemma 5.1](#) implies that for every  $i, j$  there exists  $V(P_i, P_j) \subset S_1$  with  $\dim(V(P_i, P_j)) \leq 4$  such that

$$\mathcal{F}_{\text{square}}(P_i) \cap \mathcal{F}_{\text{square}}(P_j) \subset \mathbb{C}[\mathbb{L}(P_i) + V(P_i, P_j)].$$

We use these spaces in order to control  $\mathcal{F}_{\text{square}}$ . We begin by proving an auxiliary lemma.

**Lemma 5.2.** *Suppose  $P_1, P_2, P_3 \in \mathcal{F}_2$  satisfy*

$$|\mathcal{F}_{\text{square}}(P_1) \cap \mathcal{F}_{\text{square}}(P_2) \cap \mathcal{F}_{\text{square}}(P_3)| \geq 2.$$

Then  $P_3 \in \mathbb{C}[\mathbb{L}(P_1), V(P_1, P_2)]$ .

*Proof.* Let  $R_1$  and  $R_2$  be two distinct forms in the intersection. After scaling  $R_1, R_2$  appropriately, we have the equations

$$\begin{aligned}
R_1 &= P_1 - \ell_1^2 = \alpha_1 P_2 - g_1^2 = \beta_1 P_3 - h_1^2 \\
R_2 &= P_1 - \ell_2^2 = \alpha_2 P_2 - g_2^2 = \beta_2 P_3 - h_2^2.
\end{aligned}$$

By [Lemma 5.1](#) each of the linear forms  $\ell_1, \ell_2, g_1$  and  $g_2$  is contained in  $V(P_1, P_2)$ . Further, we have  $\beta_1 P_3 = P_1 - \ell_1^2 + h_1^2$ , whence  $P_3 \in \mathbb{C}[\mathbb{L}(P_1), V(P_1, P_2), h_1]$ . It therefore suffices to show that  $h_1 \in \mathbb{C}[\mathbb{L}(P_1), V(P_1, P_2)]$ . We perform a case analysis based on the coefficients  $\beta_i$ .

Suppose first that  $\beta_1 = \beta_2 = \beta$ . We then have  $P_1 - \beta P_3 = \ell_1^2 - h_1^2 = \ell_2^2 - h_2^2$ , which implies

$$(\ell_1 - \ell_2)(\ell_1 + \ell_2) = (h_1 - h_2)(h_1 + h_2),$$

which implies that  $h_1, h_2 \in \text{span}_{\mathbb{C}}\{\ell_1, \ell_2\}$ , proving the result in this case.



Suppose then that  $\beta_1 \neq \beta_2$ . We have

$$(\beta_2 - \beta_1)P_1 + \beta_1\ell_2^2 - \beta_2\ell_1^2 = h_1^2 - h_2^2.$$

Note that in this case, we must have  $\text{rank}(P_1) \leq 4$ . Therefore,  $\mathbb{L}(P_1) = \text{Lin}(P_1)$ . Now  $h_1^2 - h_2^2 = (h_1 + h_2)(h_1 - h_2)$  is a minimal representation. By [Lemma 2.5](#)

$$\text{span}_{\mathbb{C}}\{h_1, h_2\} \subset \mathbb{L}(P_1) + \text{span}_{\mathbb{C}}\{\ell_1, \ell_2\}.$$

This in particular shows that  $h_1 \in \mathbb{C}[\mathbb{L}(P_1), V(P_1, P_2)]$ . □

With the lemma above, we can show that  $\mathcal{F}_{\text{square}}$  is contained in a small subalgebra.

**Lemma 5.3.** *There exist vector spaces  $V_1 \subseteq S_1$  and  $V_2 \subseteq S_2$  of dimensions at most  $O(1/\delta^2)$  such that  $\mathcal{F}_{\text{square}} \in \mathbb{C}[V_1, V_2]$ .*

*Proof.* Let  $\mathcal{F}_{\text{square}} := \{F_1, \dots, F_t\}$ . Set  $\mathcal{U} = \mathcal{F}_2$  and  $S_i = \mathcal{F}_{\text{square}}(F_i)$  for  $i \in [t]$ . In this case, we have  $|\mathcal{U}| \leq m$ , each  $|\mathcal{F}_{\text{square}}(F_i)| \geq \varepsilon m$ , and therefore we can apply [Lemma B.2](#) to these sets with parameter  $\varepsilon$  to obtain a collection of subsets of  $\mathcal{F}_{\text{square}}$  given by  $\mathcal{H}, \mathcal{H}_1, \dots, \mathcal{H}_r$ , where  $r := |\mathcal{H}| \leq 2/\varepsilon$  and  $r_i := |\mathcal{H}_i| \leq 8/\varepsilon$ .

Letting  $\mathcal{H} := \{P_1, \dots, P_r\}$ , and  $\mathcal{H}_i := \{Q_{i1}, \dots, Q_{ir_i}\}$ , we define our vector space  $V$  as

$$V := \sum_{i=1}^r \left( \mathbb{L}(P_i) + \sum_{j=1}^{r_i} V(P_i, Q_{ij}) \right)$$

Define  $V_1$  and  $V_2$  to be  $V \cap S_1$  and  $V \cap S_2$  respectively. The dimension of  $V$  is  $\mathcal{O}(1/\varepsilon^2)$ , since  $\mathbb{L}(P), \mathbb{L}(Q)$  and  $V(P_i, Q_{ij})$  each have dimension  $\leq 8$ .

By construction, every  $P_i$  and  $Q_{ij}$  is contained in the algebra  $\mathbb{C}[V]$ . Suppose  $R \in \mathcal{F}_{\text{square}}$  is not in  $\mathcal{H}$  or  $\mathcal{H}_i$ . By [Lemma B.2](#), there are  $i, j$  such that

$$|\mathcal{F}_{\text{square}}(R) \cap \mathcal{F}_{\text{square}}(P_i) \cap \mathcal{F}_{\text{square}}(Q_{ij})| \geq \varepsilon^3 m / 4^3 \geq 2$$

Thus, [Lemma 5.2](#) implies that  $R \in \mathbb{C}[\mathbb{L}(P_i), V(P_i, Q_{ij})]$ , and therefore in  $\mathbb{C}[V]$ . □

## 5.2 Controlling $\mathcal{F}_{\text{linear}}$

The following lemma, proved in [\[PS20a, Claim 4.4\]](#), shows the existence of a small ideal generated by linear forms containing  $\mathcal{F}_{\text{linear}}$ .

**Proposition 5.4.** *There exists  $V \subseteq S_1$  such that  $\mathcal{F}_{\text{linear}} \subseteq (V)$  and  $\dim V = \mathcal{O}(1/\delta)$ .*

We strengthen the above lemma in two key ways. First, we show that every form in  $\mathcal{F}_{\text{linear}}$  is *univariate* over the algebra of any clean vector space  $W$  such that  $\mathcal{F}_{\text{linear}} \subseteq (W)$ . If we further assume that every form in  $\mathcal{F}$  is univariate over  $\mathbb{C}[W]$ , then  $\mathcal{F}_{\text{linear}} \subseteq \mathbb{C}[W]$ .

**Lemma 5.5.** *If  $W = W_1 + W_2$  is any  $(17, \varepsilon/2)$  clean vector space such that  $\mathcal{F}_{\text{linear}} \subseteq (W)$  then every form in  $\mathcal{F}_{\text{linear}}$  that is not in  $\mathbb{C}[W]$  is of the form  $ax + y^2$ , with  $x, y \in W_1$ . In particular  $Q$  is univariate over  $W$  and  $\overline{\mathbb{L}}_W(Q)$  is spanned by  $\bar{a}$ .*

*Proof.* Let  $Q$  be a form in  $\mathcal{F}_{\text{linear}} \setminus \mathbb{C}[W]$ . Since  $W$  is 17-robust, and since  $Q$  has rank 2, we have  $Q \in (W_1)$  by [Claim 4.5](#). We also have  $\mathbb{L}(Q) \not\subset W_1$ , that is  $\dim(\overline{\mathbb{L}}_Q(W)) \geq 1$ . If every  $P \in \mathcal{F}_{\text{linear}}(Q)$  is such that  $\mathbb{L}(Q) = \mathbb{L}(P)$ , then the clean condition is violated, since  $\dim(\overline{\mathbb{L}}_W(P)) \geq 1$  for every such  $P$ , while  $\dim(\overline{\mathbb{L}}_Z(P)) = 0$  where  $Z = \mathbb{L}(Q) + W$ . Hence, there exists  $P \in \mathcal{F}_{\text{linear}}(Q)$  such that  $\mathbb{L}(P) \neq \mathbb{L}(Q)$ , which by [Proposition 3.10](#), implies  $Q = y^2 + ax$  and  $P = y^2 + bx$  for independent linear forms  $a, b, x, y$ .

Consider now the equation  $y^2 + ax = 0$  in the quotient ring  $S/(W_1)$ . Suppose  $y \in W_1$ . In this case,  $ax = 0$  in  $S/(W_1) \Rightarrow x \in W_1$  or  $a \in W_1$ . In either case, after potentially swapping the roles of  $a$  and  $x$  we have the required statement. Suppose now that  $y \notin W_1$ . The equation  $y^2 + ax = 0$  implies that  $\gamma y = a$  in  $S_1/W_1$  for some nonzero constant  $\gamma$ . We then have  $y^2 + ax = y(y + \gamma x) = 0$  in  $S/(W_1)$ . Since  $y \notin W_1$ , we must have  $y + \gamma x \in W_1$ . We can write  $Q = (y + \gamma x)^2 + x(a - 2\gamma y - \gamma x^2)$ . After changing  $y, x, a$ , this is equivalent to the case of  $y \in W_1$ , and the required result holds.  $\square$

**Claim 5.6.** *Let  $U \subset S_1$  be a vector space and  $Q = ax + y^2$  where  $x, y \in U, a \notin U$ . Suppose  $P_1, P_2$  are two distinct forms in  $\mathcal{F}_{\text{linear}}(Q) \cap \mathbb{C}[U]$ , and suppose  $R_1 \in \text{rad}(Q, P_1) \cap \mathcal{F}_2$  and  $R_2 \in \text{rad}(Q, P_2) \cap \mathcal{F}_2$ . Then  $R_1$  and  $R_2$  are distinct elements of  $\mathcal{F}_2$ . Further,  $R_1, R_2 \notin \mathbb{C}[U]$ , and  $R_1, R_2 \in \mathbb{C}[U + \mathbb{L}(Q)]$ .*

*Proof.* Since  $\mathbb{L}(Q) \neq \mathbb{L}(P_i)$  for  $i \in \{1, 2\}$ , we can use [Proposition 3.10](#), to write  $Q = a_i x_i + y_i^2$  and  $P_i = b_i x_i + y_i^2$  for independent linear forms  $a_i, b_i, x_i, y_i$ . We now show that after a linear change of coordinates we can make  $x_i \in (x)$  and  $y_i \in (y)$ , for  $i \in \{1, 2\}$ .

Since  $P_i \in \mathbb{C}[U]$ , we have  $x_i, y_i, b_i \in U$ . From  $Q = xa + y^2 = x_i a_i + y_i^2$ , we have  $y^2 - y_i^2 \equiv x_i a_i \pmod{(x)}$ . If  $x_i \notin (x)$ , then by factoriality of  $S/(x)$  we have  $a_i \in (x, y, y_i) \subset U \Rightarrow \mathbb{L}(Q) \subset U$  which is a contradiction. Hence, we have that  $x_i = \alpha x$  for some  $\alpha \in \mathbb{C}^*$ . This implies  $x(a - \alpha a_i) = y_i^2 - y^2$ , and if  $a \neq \alpha a_i$ , factoriality implies that  $y_i \in \text{span}_{\mathbb{C}}\{x, y\}$ . Moreover, we know that  $y_i \notin (x)$  since  $Q$  is irreducible, so writing  $y_i = \alpha_i x + \beta_i y$  we have  $\beta_i \neq 0$  and hence after a change of coordinates we can map  $y_i \mapsto y$ , as we wanted.

After scaling appropriately, we have  $Q = ax + y^2$ , and  $P_1 = bx + y^2$  and  $P_2 = cx + y^2$ . By [Proposition 3.11](#),  $\text{rad}(P_1, Q) = (P_1, Q, y(a - b))$  and thus  $R_1 \in \text{rad}(P_1, Q) \Rightarrow R_1 = \alpha_1 Q + \beta_1 P_1 + \delta_1 y(a - b)$ . If  $R_1 \in \mathbb{C}[U]$  then  $\alpha_1 ax + \delta_1 ay \in \mathbb{C}[U]$ , which implies that  $a(\alpha_1 x + \delta_1 y) \in \mathbb{C}[U]$ . Since  $x$  and  $y$  are linearly independent, this implies  $a \in U$  which is a contradiction, so  $R_1 \notin \mathbb{C}[U]$ . Similarly, we have  $R_2 = \alpha_2 Q + \beta_2 P_2 + \delta_2 y(a - c)$ . This proves the last part of the claim.

Suppose  $R_1 = \mu R_2$  for some  $\mu \in \mathbb{C}$ . After rescaling  $\alpha_2, \beta_2, \delta_2$  we have

$$\alpha_1 Q + \beta_1 P_1 + \delta_1 y(a - b) = \alpha_2 Q + \beta_2 P_2 + \delta_2 y(a - c).$$

Plugging in the formulae of  $Q, P_1, P_2$  and rearranging, we get  $a((\alpha_1 - \alpha_2)x + (\delta_1 - \delta_2)y) \in \mathbb{C}[U]$ . Since  $a \notin U$ , we must have  $(\alpha_1 - \alpha_2)x + (\delta_1 - \delta_2)y = 0$ , which by the independence of  $x$  and  $y$  implies  $\alpha_1 = \alpha_2$  and  $\delta_1 = \delta_2$ . The equation therefore implies  $\beta_1 P_1 - \beta_2 P_2 = \delta_1 y(b - c)$ . We also have  $\beta_1 P_1 - \beta_2 P_2 = (\beta_1 - \beta_2)y^2 + x(\beta_1 b - \beta_2 c)$ . Equating the two and rearranging, we get

$$x(\beta_1 b - \beta_2 c) = y(\delta_1(b - c) - (\beta_1 - \beta_2)y).$$

If  $(\beta_1 b - \beta_2 c) = (\delta_1(b - c) - (\beta_1 - \beta_2)y) = 0$  then  $b = (\beta_2/\beta_1)c$  and  $\beta_2 \neq \beta_1$  (otherwise  $P_1 = P_2$ ), and  $y \in (b)$ , contradicting irreducibility of  $P_1$ . Otherwise,  $y \in \text{span}_{\mathbb{C}}\{b, c\}$  and  $x \in \text{span}_{\mathbb{C}}\{b, c, y\}$  which together imply that  $x, y \in \text{span}_{\mathbb{C}}\{b, c\}$ . This implies that  $P_1$  is bivariate, contradicting its irreducibility. Therefore,  $R_1 \neq \mu R_2$  for any  $\mu$ , that is,  $R_1$  and  $R_2$  are distinct elements of  $\mathcal{F}_2$ .  $\square$

**Lemma 5.7.** *Let  $W = W_1 + W_2$  be a  $(17, \varepsilon/3)$  clean vector space such that  $\mathcal{F}_{\text{linear}} \subseteq (W)$  and such that every form in  $\mathcal{F}$  is either in  $\mathbb{C}[W]$  or univariate over  $W$ . Then  $\mathcal{F}_{\text{linear}} \subset \mathbb{C}[W_1]$ .*

*Proof.* Assume that there is  $Q \in \mathcal{F}_{\text{linear}} \setminus \mathbb{C}[W_1]$ . By [Lemma 5.5](#), we know that  $Q = \alpha x + y^2$ , with  $x, y \in W_1$  and  $\alpha \notin W_1$ . Let  $Z := \mathbb{L}(Q) + W$ . Every form in  $\mathcal{F}_{\text{linear}}(Q)$  has rank 2, and any such form that is in  $\mathbb{C}[W]$  is also in  $\mathbb{C}[W_1]$ . Also, if a form in  $\mathcal{F}_{\text{linear}}$  has rank 2 and it is univariate over  $W$  then it is univariate over  $W_1$ .

Let  $\{P_1, \dots, P_b\} := \mathcal{F}_{\text{linear}}(Q) \cap \mathbb{C}[W_1]$ . If  $R_i \in \text{rad}(Q, P_i)$ , then by [Proposition 3.11](#)  $R_i \in \mathcal{F}_2$  and [Claim 5.6](#) shows that  $R_1, \dots, R_b$  are distinct. It also shows that  $R_i \notin \mathbb{C}[W_1]$ , that is,  $\dim(\overline{\mathbb{L}}_W(R_i)) > 0$  and that  $R_i \in \mathbb{C}[Z]$ , that is,  $\dim(\overline{\mathbb{L}}_Z(R_i)) = 0$ . By the clean condition, we have  $b < \varepsilon m/3$ .

Hence, we have  $|\mathcal{F}_{\text{linear}}(Q) \setminus \mathbb{C}[W_1]| \geq 2\varepsilon m/3$ . By the clean condition there are at most  $\varepsilon m/3$  forms  $P' \in \mathcal{F}$  such that  $\overline{\mathbb{L}}_W(Q) = \overline{\mathbb{L}}_W(P')$ , since for each such form we have  $\dim(\overline{\mathbb{L}}_W(P')) = 1$  while  $\dim(\overline{\mathbb{L}}_Z(P')) = 0$ . We can therefore find a form  $P \in \mathcal{F}_{\text{linear}}(Q) \setminus \mathbb{C}[W_1]$  and such that  $\overline{\mathbb{L}}_W(Q) \neq \overline{\mathbb{L}}_W(P)$ . Note that this latter condition also implies  $\mathbb{L}(Q) \neq \mathbb{L}(P)$ . Also we must have  $\mathbb{L}(Q) \cap \mathbb{L}(P) \subset \text{span}_{\mathbb{C}}\{x, y\}$ . Indeed, suppose  $u \in \mathbb{L}(Q) \cap \mathbb{L}(P)$ . As  $\mathbb{L}(Q) = \text{span}_{\mathbb{C}}\{\alpha, x, y\}$ , we must have  $\bar{u} = \lambda \bar{u} \in \overline{\mathbb{L}}_W(P)$  for some non-zero  $\lambda$ . This is a contradiction since  $\overline{\mathbb{L}}_W(Q) \neq \overline{\mathbb{L}}_W(P)$  and both are one dimensional.

Since  $\mathbb{L}(P) \cap \mathbb{L}(Q) \subset \text{span}_{\mathbb{C}}\{x, y\}$  and  $\mathbb{L}(Q) \neq \mathbb{L}(P)$ , after a linear change of variables we can write  $Q = y^2 + \alpha x$  and  $P = y^2 + \beta x$  for independent linear forms  $\alpha, \beta, x, y$  by [Proposition 3.10](#).

Let  $R \in \text{rad}(Q, P) \cap \mathcal{F}_2$ . As  $R \in \mathcal{F}_2$ , we have that  $R$  is irreducible and univariate over  $W_1$  or  $R \in \mathbb{C}[W_1]$ . By [Proposition 3.11](#) we have

$$R = \alpha Q + \beta P + \gamma y(a - b) = (\alpha + \beta)y^2 + x(\alpha a + \beta b) + \gamma y(a - b).$$

Let  $R' := x(\alpha a + \beta b) + \gamma y(a - b)$ , so  $R - R' = (\alpha + \beta)y^2 \in \mathbb{C}[W_1]$ . The form  $R$  is either univariate over  $W_1$  or in  $\mathbb{C}[W_1]$  by assumption, and therefore so is  $R'$ . Since  $a, b, x, y$  are independent, if  $\alpha \neq -\beta$  then  $x, y, \alpha a + \beta b, a - b$  are independent, and  $R'$  is irreducible with  $\mathbb{L}(R') = \text{span}_{\mathbb{C}}\{x, y, a, b\}$ . This would imply that  $\dim(\overline{\mathbb{L}}_W(R')) = 2$ , with basis  $a, b$  contradicting the fact that  $R'$  is univariate over  $W_1$  or in  $\mathbb{C}[W_1]$ . Therefore, we have  $\alpha = -\beta$  and we get  $R = (\alpha x + \gamma y)(a - b)$ . This contradicts irreducibility of  $R$  and completes the proof.  $\square$

### 5.3 Controlling $\mathcal{F}_{\text{deg}}$

Now we control  $\mathcal{F}_{\text{deg}}$ . The proof is similar to the proof in [Lemma 5.7](#), where we construct a double cover of the dependencies to be able to find a small vector space of forms to add to our algebra. Before we execute the above plan, we need to clean-up the quadratics in  $\mathcal{F}_{\text{deg}}$ , which is the purpose of the following two propositions.

**Proposition 5.8.** *Let  $\mathcal{N} \subseteq \mathcal{F}_{\text{deg}}$  be the set of quadratics  $Q$  such that there are at least  $\varepsilon^2 m/100$  other forms  $P \in \mathcal{F}$  such that  $\mathbb{L}(Q) = \mathbb{L}(P)$ . There exists  $W \subset S_1$  with  $\dim W = O(1/\delta^2)$  such that  $\mathcal{N} \subset \mathbb{C}[W]$ .*

*Proof.* For each  $Q \in \mathcal{N}$ , we must have  $\text{rank}(Q) \leq 4$ , otherwise  $\mathbb{L}(Q) = \text{span}_{\mathbb{C}}\{Q\}$  and by the SG condition there is no other form  $P \in \mathcal{F}$  such that  $\mathbb{L}(P) = \mathbb{L}(Q)$ , as that would imply  $P \in \text{span}_{\mathbb{C}}\{Q\}$ . Let  $\mathcal{N}(Q)$  be the set of forms  $P \in \mathcal{F}$  such that  $\mathbb{L}(P) = \mathbb{L}(Q)$ .

Start with  $\mathcal{A} = \emptyset$ , and  $W = \{0\}$ . Iterate over the elements of  $\mathcal{N}$ , and whenever  $Q \in \mathcal{N}$  is not in the algebra  $\mathbb{C}[W]$ , we add  $Q$  to  $\mathcal{A}$ , and update  $W \leftarrow W + \mathbb{L}(Q)$ . At the end of the process, we have  $\mathcal{N} \subseteq \mathbb{C}[W]$  by construction.

Since  $\dim(W) \leq 8 \cdot |\mathcal{A}|$ , it is enough for us to bound the size of  $\mathcal{A}$ . Suppose the forms of  $\mathcal{A}$  are  $Q_1, \dots, Q_t$  in the order they were added. Since we add  $Q_i$  to  $\mathcal{A}$ , it must be that  $\mathcal{N}(Q_i) \cap \mathcal{N}(Q_j) = \emptyset$  for every  $j < i$ . We therefore have

$$|\cup_{k \leq i} \mathcal{N}(Q_k)| - |\cup_{k < i} \mathcal{N}(Q_k)| \geq \varepsilon^2 m/100.$$

Since  $|\cup_{k \leq i} \mathcal{N}(Q_k)| \leq |\mathcal{F}| \leq m$ , these equations together with  $\varepsilon = \delta/10$  imply  $t = O(1/\delta^2)$ .  $\square$

**Proposition 5.9.** *Let  $\mathcal{M} \subseteq \mathcal{F}_{\text{deg}}$  be the set of quadratics  $Q$  such that  $(Q, x)$  is not radical for at least  $\varepsilon m/3$  linear forms  $x \in \mathcal{F}_1(Q)$ . There is  $\mathcal{U} \subset S_1$  such that  $\dim(\mathcal{U}) = O(1/\delta)$  and  $\mathcal{M} \subset \mathbb{C}[\mathcal{U}]$ .*

*Proof.* By Proposition 2.9, if two forms  $Q_1, Q_2 \in \mathcal{F}_2$  do not form a radical ideal with at least 3 linear forms from  $\mathcal{F}_1$ , then  $\text{rank}(Q_1) = \text{rank}(Q_2) = 2$  and  $\mathbb{L}(Q_1) = \mathbb{L}(Q_2)$ . Moreover, the same proposition implies that each form in  $\mathcal{M}$  has rank 2. In particular,  $\mathbb{L}(Q) \subset S_1$  for each  $Q \in \mathcal{M}$ .

Denote  $\mathcal{M} := \{P_1, \dots, P_r\}$  and for each  $i \in [r]$ , let

$$\mathcal{H}_i := \{x \in \mathcal{F}_1(P_i) \mid (P_i, x) \text{ not radical}\}.$$

By definition of  $\mathcal{M}$ ,  $|\mathcal{H}_i| \geq \varepsilon m/3$  for each  $i \in [r]$ . Since  $|\mathcal{F}_1| \leq m$ , Proposition B.1 applies. Let  $Q_1, \dots, Q_t$  be the forms from  $\mathcal{M}$  which we obtain from Proposition B.1, where  $t \leq 6/\varepsilon$ .

For any  $Q \in \mathcal{M}$ , there exists  $i \in [t]$  such that  $|\mathcal{F}_1(Q) \cap \mathcal{F}_1(Q_i)| \geq \varepsilon^2 m/36 > 2$ . In particular, the above together with Proposition 2.9 implies that  $\mathbb{L}(Q) = \mathbb{L}(Q_i)$ .

Therefore, if we take  $\mathcal{U} := \sum_{i=1}^t \mathbb{L}(Q_i)$ , we have that  $\dim(\mathcal{U}) \leq 8 \cdot t \leq 48/\varepsilon = O(1/\delta)$  and  $\mathcal{M} \subset \mathbb{C}[\mathcal{U}]$  by the previous paragraph.  $\square$

By the previous two propositions, we are left with the forms  $P \in \mathcal{F}_{\text{deg}}$  such that:

1.  $(P, x)$  is radical with at least  $2\varepsilon m/3$  of the linear forms  $x \in \mathcal{F}_1(P)$
2.  $\mathbb{L}(P) = \mathbb{L}(Q)$  for at most  $\varepsilon^2 m/100$  forms  $Q \in \mathcal{F}_2$ .

Let  $\mathcal{R}$  denote the set of such forms. The next remark shows that for any  $P \in \mathcal{F}_{\text{deg}}$ , we can find many distinct quadratic dependencies corresponding to the linear forms satisfying item 1 above.

*Remark 5.10 (Quadratic dependencies).* For each form  $P \in \mathcal{R}$  and  $x_i \in \mathcal{F}_1(P)$  such that  $(P, x_i)$  is radical, the SG condition implies that there is  $Q_i \in \mathcal{F}_2$  such that  $Q_i \in (P, x_i)$ . By Proposition 2.6 there are at most 6 linear forms  $x_j$  such that  $Q_i \in (P, x_j)$ . Hence, in the set

$$\tau(P) := \{(Q_i, x_i) \in \mathcal{F}_2 \times \mathcal{F}_1(P) \mid Q_i \in (P, x_i) \text{ and } (P, x_i) \text{ radical}\}$$

we have that a quadratic form  $Q \in \mathcal{F}_2$  can appear in at most 6 tuples, and each  $x \in \mathcal{F}_1(P)$  has a  $Q \in \mathcal{F}_2$  such that  $(Q, x) \in \tau(P)$ . Thus, we know that there is a subset

$$\mathcal{G}_{\text{deg}}(P) := \{(Q_1, x_1), \dots, (Q_t, x_t)\} \subset \tau(P)$$

with  $t \geq \varepsilon m/10$  such that for every  $i \in [t]$  we have  $\mathbb{L}(Q_i) \neq \mathbb{L}(P)$  and for  $i \neq j$  we have  $Q_i \notin (Q_j)$  and  $x_i \notin (x_j)$ . With this at hand, we can define the set

$$\mathcal{F}_{\text{deg}}(P) := \{Q \mid \exists x \in \mathcal{F}_1(P) \text{ s.t. } (Q, x) \in \mathcal{G}_{\text{deg}}(P)\}.$$

By the above, we have that  $|\mathcal{F}_{\text{deg}}(P)| \geq \varepsilon m/10$  for any  $P \in \mathcal{R}$ .

Now, to control the forms in  $\mathcal{R}$ , we will construct a small dimensional  $(17, \varepsilon^3/100)$ -clean vector space  $V$  such that every form  $P \in \mathcal{R}$  is either in  $\mathbb{C}[V]$  or  $P$  is univariate over  $V$ . Moreover, if the latter happens, we can prove that all but  $\varepsilon^3 m/100$  of the SG dependencies in  $\mathcal{F}_{\text{deg}}(P)$  are also 1-close to  $V$ . Before we construct this vector space  $V$ , we need the following proposition.

**Lemma 5.11.** *Let  $P_1, P_2, P_3$  be quadratics in  $\mathcal{R}$  such that  $\mathbb{L}(P_i) \neq \mathbb{L}(P_3)$  for  $i \in \{1, 2\}$  and let  $V = V_1 + V_2$  be a  $(17, \gamma)$ -clean vector space with respect to  $\mathcal{F}$  such that  $P_1, P_2 \in \mathbb{C}[V]$ .*

1. If  $P_3 \notin \mathbb{C}[V]$ , then  $|\mathcal{F}_{\deg}(P_3) \cap \mathbb{C}[V]| \leq \gamma m$ .

2. Suppose

$$|\mathcal{F}_{\deg}(P_1) \cap \mathcal{F}_{\deg}(P_2) \cap \mathcal{F}_{\deg}(P_3)| = B > 3\gamma m + 2.$$

Then  $P_3$  is univariate over  $\mathbb{C}[V]$ . Moreover, if  $P_3 \notin \mathbb{C}[V]$ , there exist  $\alpha \in \mathbb{C}^*$ ,  $z \in S_1 \setminus V_1$ ,  $a \in V_1$  such that one of the following holds:

(a)  $P_3 = \alpha P_1 + az$ , and there exist  $t \geq B - 3\gamma m - 2$  forms  $R_1, \dots, R_t \in \mathcal{F}_{\deg}(P_1) \cap \mathcal{F}_{\deg}(P_2) \cap \mathcal{F}_{\deg}(P_3)$ , such that

$$R_i = \alpha P_1 - x_i a = P_3 - a_i a$$

where  $x_i \in \mathcal{F}_1(P_1) \setminus V_1$  and  $a_i \in \mathcal{F}_1(P_3) \setminus V_1$ .

(b)  $P_3 = \alpha P_1 + z(z + a)$ , and there exist  $t \geq B - 3\gamma m - 2$  forms  $R_1, \dots, R_t \in \mathcal{F}_{\deg}(P_1) \cap \mathcal{F}_{\deg}(P_2) \cap \mathcal{F}_{\deg}(P_3)$ , such that

$$R_i = \alpha P_1 - x_i(x_i + \alpha_i a) = P_3 - a_i b_i$$

where  $\alpha_i \in \mathbb{C}$ ,  $x_i \in \mathcal{F}_1(P_1) \setminus V_1$  and  $a_i \in \mathcal{F}_1(P_3) \setminus V_1$ .

Furthermore, in both cases above, we have that  $\bar{z}, \bar{x}_i, \bar{a}_i \in S_1/V_1$  are pairwise linearly independent and  $\dim \text{span}_{\mathbb{C}}\{\bar{z}, \bar{x}_i, \bar{a}_i\} = 2$ .

*Proof.* We begin by proving item 1.

**Proof of item 1:** Suppose  $|\mathcal{F}_{\deg}(P_3) \cap \mathbb{C}[V]| > \gamma m$ . Let  $R_i \in |\mathcal{F}_{\deg}(P_3) \cap \mathbb{C}[V]|$  for  $i \in [\gamma m + 1]$ . In this case, we will show that  $P_3 \in \mathbb{C}[V]$ . After proper scalar multiples, we may assume  $R_i = P_3 - a_i b_i$  where  $a_i \in \mathcal{F}_1(P_3)$  and  $b_i \in S_1$ . Assume for the sake of contradiction that  $P_3 \notin \mathbb{C}[V]$ . Suppose there is  $i \in [\gamma m + 1]$  such that  $a_i \in V_1$ . Without loss of generality we can assume that  $i = 1$ . If  $P_3 \notin \mathbb{C}[V]$  then  $b_1 \notin V_1$ . However, we have  $a_1 b_1 - a_i b_i = R_i - R_1 \in \mathbb{C}[V_1]$ , which implies that  $b_i \in (a_1)$  and  $a_i \in \text{span}_{\mathbb{C}}\{V_1, b_1\} \setminus V_1$ , since  $a_i \notin (a_1)$ . This happens for all  $2 \leq i \leq \gamma m + 1$ . We therefore have  $\dim \bar{\mathbb{L}}_V(P_3) > \dim \bar{\mathbb{L}}_{V+\{b_1\}}(P_3)$  and  $\dim \bar{\mathbb{L}}_V(a_i) > \dim \bar{\mathbb{L}}_{V+\{b_1\}}(a_i)$  for every  $2 \leq i \leq \gamma m$ , which contradicts the clean condition.

We are left with the case where  $a_i \notin V_1$  for each  $i \in [\gamma m + 1]$ . In this case,  $a_1 b_1 - a_i b_i = R_i - R_1 \in \mathbb{C}[V_1]$  and [Proposition 4.6](#) imply that there is  $z_i \in S_1 \setminus V_1$  such that  $a_1, b_1, a_i, b_i \in \text{span}_{\mathbb{C}}\{V_1, z_i\}$ . Since  $a_1 \notin V_1$ , we must have that  $\text{span}_{\mathbb{C}}\{V_1, z_i\} = \text{span}_{\mathbb{C}}\{V_1, a_1\}$ , which implies that  $a_i \in \text{span}_{\mathbb{C}}\{V_1, a_1\}$  for all  $i \in [\gamma m]$ . Equivalently, we have  $\dim \bar{\mathbb{L}}_V(a_i) = 1$  and  $\dim \bar{\mathbb{L}}_{V+\{a_1\}}(a_i) = 0$  or all such  $i$ , which violates the clean condition. Therefore, this case cannot happen.

**Proof of item 2:** We can assume that  $P_3 \notin \mathbb{C}[V]$ , otherwise we are done. Let  $R_i$  be elements in the intersection  $\mathcal{F}_{\deg}(P_1) \cap \mathcal{F}_{\deg}(P_2) \cap \mathcal{F}_{\deg}(P_3)$ , where  $i \in [B]$ . After proper scalar multiples, we have:

$$R_i = \alpha_i P_1 - x_i y_i = \beta_i P_2 - u_i v_i = P_3 - a_i b_i \tag{1}$$

where  $\alpha_i, \beta_i \in \mathbb{C}^*$ ,  $x_i \in \mathcal{F}_1(P_1)$ ,  $u_i \in \mathcal{F}_1(P_2)$  and  $a_i \in \mathcal{F}_1(P_3)$ . Moreover, by [Remark 5.10](#) we know that for any  $i \neq j$  we must have  $x_i \notin (x_j)$ ,  $u_i \notin (u_j)$  and  $a_i \notin (a_j)$ .

By the first item and the fact that  $P_3 \notin \mathbb{C}[V]$ , at least  $B_1 := B - \gamma m$  forms  $R_i$  not in the algebra. (Say  $R_i \notin \mathbb{C}[V]$  for  $i \in [B_1]$ .) Recall also that  $\mathbb{L}(P_3) \neq \mathbb{L}(P_1)$ .

Since  $P_3 - \alpha_i P_1 = x_i y_i - a_i b_i$ , we know that  $\text{rank}(P_3 - \alpha_i P_1) \leq 2$ . For any  $i \in [B_1]$  such that  $\text{rank}(P_3 - \alpha_i P_1) = 2$ , we have that  $P_3 - \alpha_i P_1 = x_i y_i - a_i b_i$  is a minimal representation of

$P_3 - \alpha_i P_1$ , and therefore  $\text{span}_{\mathbb{C}}\{x_i, a_i, y_i, b_i\} = \mathbb{L}(P_3 - \alpha_i P_1)$ . Let  $\mathcal{L} \subseteq [B_1]$  be the indices  $i$  such that  $\text{rank}(P_3 - \alpha_i P_1) = 2$ .

If there were  $i \neq j \in \mathcal{L}$  such that  $\alpha_i \neq \alpha_j$ , w.l.o.g. we can say  $\alpha_1 \neq \alpha_2$ , then  $\mathbb{L}(P_3), \mathbb{L}(P_1) \subset W := \text{span}_{\mathbb{C}}\{x_1, x_2, y_1, y_2, a_1, a_2, b_1, b_2\}$ . For every other  $k \in \mathcal{L}$ , as  $\text{rank}(x_k y_k - a_k b_k) = 2$ , then  $x_i, y_i, a_i, b_i \in W$ . This would imply that  $R_i \in \mathbb{C}[V + W]$ , or equivalently that  $\dim \overline{\mathbb{L}}_V(R_i) > \dim \overline{\mathbb{L}}_{V+W}(R_i) = 0$ . The above cannot happen for more than  $\gamma m$  indices, as it would contradict the clean condition, since  $\dim(W) \leq 8$ .

If  $\alpha_i = \alpha_j$  for all  $i \neq j \in \mathcal{L}$ , we obtain the same conclusion as above, but now with  $W := \text{span}_{\mathbb{C}}\{x_1, y_1, a_1, b_1\}$ . Therefore, we know that  $|\mathcal{L}| \leq \gamma m$ .

We have just proved that there must be at least  $B_2 := B_1 - \gamma m$  indices with  $P_3 - \alpha_i P_1 = x_i y_i - a_i b_i$  being rank 1. Moreover, by [Remark 2.7](#) and  $\mathbb{L}(P_1) \neq \mathbb{L}(P_3)$  there is a unique rank 1 element in the pencil  $P_3 - \lambda P_1$ . In particular, this implies  $\alpha_i = \alpha$  for all  $i \in [B_2]$ .

After rescaling  $P_1$  and reordering the indices, we can assume that  $P_3 - P_1$  is of rank 1, and that  $x_i y_i - a_i b_i$  has rank 1 for every  $i \in [B_2]$ . Hence, [Eq. \(1\)](#) becomes:

$$R_i = P_1 - x_i y_i = \beta_i P_2 - u_i v_i = P_3 - a_i b_i \quad (2)$$

We now have two cases to analyze:

**Case (a):**  $P_3 \in (V)$ .

In this case, we can write  $P_3 = P_1 + za$ , where  $a \in V_1$  and  $z \in S_1 \setminus V_1$ . Since  $x_i y_i - u_i v_i = P_1 - \beta_i P_2 \in \mathbb{C}[V_1]$ , and by our assumption we know that  $x_i y_i \notin \mathbb{C}[V]$ , [Proposition 4.6](#) implies that there is  $z_i \in S_1 \setminus V_1$  such that  $x_i, y_i, u_i, v_i \in \text{span}_{\mathbb{C}}\{V_1, z_i\}$ . By the clean condition on  $V$ , we have that  $z_i \in \text{span}_{\mathbb{K}}\{V_1, z\}$  for at most  $\gamma m$  indices. Thus, if  $B_3 := B_2 - \gamma m$ , we can assume that  $z_i \notin \text{span}_{\mathbb{K}}\{V_1, z\}$ , for  $i \in [B_3]$ .

As  $P_1 - x_i y_i = P_3 - a_i b_i$ , we have that  $a_i b_i - x_i y_i = P_3 - P_1 = za$  for all  $i \in [B_2]$ . Hence,  $a_i b_i \equiv x_i y_i \pmod{(a)}$ . If  $x_i y_i \not\equiv 0 \pmod{(a)}$ , by the factoriality of  $S/(a)$  we have that  $a_i b_i = (x_i + \beta_i a)(y_i + \gamma_i a)$ , which implies that

$$za = a_i b_i - x_i y_i = a(\gamma_i x_i + \beta_i y_i + \beta_i \gamma_i a),$$

which in turn implies that  $z = \gamma_i x_i + \beta_i y_i + \beta_i \gamma_i a$ . Since  $a_i b_i \neq x_i y_i$ , we have that one of  $\beta_i, \gamma_i$  is nonzero, which implies that  $z \in V_1 + \text{span}_{\mathbb{C}}\{x_i, y_i\} = V_1 + \text{span}_{\mathbb{C}}\{z_i\}$ , which implies that  $z_i \in V_1 + \text{span}_{\mathbb{C}}\{z\}$ , contradicting our choice of  $z_i$ . This contradiction implies  $x_i y_i \in (a)$ . Note that for every such  $i$ , we also have  $a_i b_i = za - x_i y_i \in (a)$ .

Since the forms  $x_j, a_k$  for all  $j, k$  are pairwise linearly independent, there can be at most one index with  $x_i \in (a)$  or  $a_i \in (a)$ . Therefore, for  $i \in [B_3 - 2]$ , we have  $y_i, b_i \in (a)$ . In particular, this implies that  $\text{span}_{\mathbb{K}}\{V_1, x_i\} = \text{span}_{\mathbb{K}}\{V_1, z_i\}$  for  $i \in [B_3 - 2]$ , and therefore  $x_i \notin \text{span}_{\mathbb{K}}\{V_1, z\}$ . After rescaling the  $x_i$  and  $a_i$ , this implies

$$R_i = P_1 - x_i a = P_3 - a_i a$$

for each such index, completing the first part of the proof in this case.

For each index satisfying the above, the condition  $za = a_i b_i - x_i y_i$  now implies that  $z = \alpha_i a_i - \beta_i x_i$  for nonzero  $\alpha_i, \beta_i$ . Since  $x_i \notin \text{span}_{\mathbb{K}}\{V_1, z\}$  by our choice of indices, we also have that  $a \notin V_1$ . If  $\bar{z}, \bar{a}_i, \bar{x}_i$  are not pairwise linearly independent, then  $z_i \in V_1 + \text{span}_{\mathbb{C}}\{z\}$ , contradicting the choice of indices. This completes the proof of the moreover part in this case.

**Case (b):**  $P_3 \notin (V)$ .

In this case, we have  $P_3 - P_1 = pq$  with neither  $p$  nor  $q$  in  $V_1$ . Let  $W$  be the space spanned by  $p, q$  in  $S_1/V_1$ . Also, let  $z_i \in S_1 \setminus V_1$  be such that  $x_i, y_i, u_i, v_i \in \text{span}_{\mathbb{C}}\{V_1, z_i\}$  and let  $\mu_i, \nu_i \in \mathbb{C}$  be such that  $x_i = \mu_i z_i$  and  $y_i = \nu_i z_i$  in  $S_1/V_1$ . Since  $R_i \notin \mathbb{C}[V]$ , at most one of  $\mu_i, \nu_i$  can be zero for each  $i$ . We have equation  $pq = P_3 - P_1 = \nu_i \mu_i z_i^2 - \alpha_i b_i$  in the ring  $S_1/(V_1)$ .

Let  $\mathcal{L}_1 \subset [B_2]$  be the set of indices such that  $z_i \in V_1 + W$ . This implies  $R_i \in \mathbb{C}[V, W]$  for  $i \in \mathcal{L}_1$ . By the clean condition, we have that  $|\mathcal{L}_1| \leq \gamma m$ . Let  $\mathcal{L}_2 \subset [B_2] \setminus \mathcal{L}_1$  be the set of indices such that  $\alpha_i$  or  $b_i \in V_1 + W$ . In this case, we have that  $pq - \alpha_i b_i = \mu_i \nu_i z_i^2$ , and since  $z_i \notin V_1 + W$ , we have that  $\mu_i \nu_i = 0$  and thus both  $\alpha_i, b_i \in V_1 + W$ , hence  $R_i \in \mathbb{C}[V, W]$ . However, this implies  $R_i - P_1 = x_i y_i \in \mathbb{C}[V, W] \Rightarrow z_i \in V_1 + W$ , which is a contradiction, so  $\mathcal{L}_2 = \emptyset$ .

Without loss of generality, we can assume that  $[B_3] = [B_2] \setminus \mathcal{L}_1$ . By definition,  $i \in [B_3] \Rightarrow z_i \notin V_1 + W$  and  $\alpha_i b_i \notin (V_1 + W)$ . Since  $x_i y_i = pq - \alpha_i b_i \equiv -\alpha_i b_i \not\equiv 0 \pmod{(V_1 + W)}$ , this also implies that both  $x_i, y_i \notin (V_1 + W)$ . Therefore, for every  $i \in [B_3]$  we have  $x_i, y_i, \alpha_i, b_i \notin V_1 + W$ .

We now show  $\dim W = 1$ . Assume towards a contradiction that  $\dim W = 2$ . For each  $i \in [B_3]$ , let  $W_i := \text{span}_{\mathbb{C}}\{\alpha_i, b_i, z_i\}$  over  $S_1/V_1$ . From  $x_i y_i - \alpha_i b_i = pq$ , we have  $p, q \in W_i \Rightarrow W \subset W_i$ . Since  $z_i, \alpha_i \notin W$ , this inclusion is strict, and  $\dim W_i = 3$ .

For every  $i, j \in [B_3]$  we have  $\alpha_i b_i - \alpha_j b_j = x_i y_i - x_j y_j \in \mathbb{C}[V_1 + \text{span}_{\mathbb{C}}\{z_i, z_j\}]$ . Hence, by [Proposition 4.6](#) there is  $\ell_{ij} \in S_1$  such that  $\alpha_i, b_i, \alpha_j, b_j \in \text{span}_{\mathbb{C}}\{z_i, z_j, \ell_{ij}\} + V_1$ . Therefore,  $\text{span}_{\mathbb{C}}\{\alpha_i, b_i, z_i\} + V_1 = \text{span}_{\mathbb{C}}\{z_i, z_j, \ell_{ij}\} + V_1 = \text{span}_{\mathbb{C}}\{\alpha_j, b_j, z_j\} + V_1 \Rightarrow W_i = W_j$ . This implies that  $R_i \in \mathbb{C}[V + W_1]$  for every  $i \in [B_3]$ , or equivalently that  $\dim \overline{\mathbb{L}}_V(R_i) > \dim \overline{\mathbb{L}}_{V+W_1}(R_i)$ . This contradicts cleanliness, since  $B_3 \geq \gamma m$ .

Therefore, it must be that  $\dim(W) = 1$ , or equivalently (after rescaling) that  $q = p + a$  for some  $a \in V_1$ . Setting  $z = p$ , we get that  $W = \text{span}_{\mathbb{C}}\{z\}$  and the first part of case 1 of the lemma holds, that is  $P_3 = P_1 + z(z + a)$ . For each  $i \in [B_3]$ , we also know that  $y_i, x_i \notin V_1$ , and therefore, we have  $y_i = \alpha_i x_i + f_i$  for some  $\alpha_i \in \mathbb{C}^*$  and  $f_i \in V_1$  (since  $x_i, y_i$  are spanned by  $z_i$  in  $S_1/V_1$ ). Since  $x_i y_i - \alpha_i b_i = z(z + a)$ , by [Proposition 4.6](#) and  $x_i \notin V_1 + W$ , we have  $x_i, y_i, \alpha_i, b_i \in \text{span}_{\mathbb{C}}\{z, a, x_i\}$ . Since  $f_i = y_i - \alpha_i x_i \in \text{span}_{\mathbb{C}}\{z, a, x_i\}$  and  $x_i \notin V_1 + W$ , it must be that  $f_i \in \text{span}_{\mathbb{C}}\{a\}$ .

From  $z(z + a) = x_i(x_i + f_i) - \alpha_i b_i$ , we have  $z^2 - x_i^2 \equiv \alpha_i b_i \pmod{(V_1)} \Rightarrow \alpha_i = \beta_i(x_i \pm z)$  and  $b_i = \beta_i^{-1}(x_i \mp z)$  over  $S/(V_1)$ . Thus,  $\overline{\alpha_i}, \overline{z}$  and  $\overline{x_i}$  form a linear dependence. Combined with the fact that  $\overline{\alpha_i}, \overline{x_i} \notin (\overline{z})$ , we also deduce that  $\overline{\alpha_i}$  and  $\overline{x_i}$  are linearly independent over  $S/(V_1)$ .  $\square$

**Lemma 5.12** (Controlling  $\mathcal{F}_{\text{deg}}$ ). *There exists a  $(17, (\varepsilon/100)^3)$ -clean vector space  $V := V_1 + V_2$ , where  $V_i \subset S_i$  of dimension  $\dim(V) = O(1/\delta^3)$  such that each form in  $\mathcal{F}_{\text{deg}}$  is either in  $\mathbb{C}[V]$  or univariate over  $V$ . Moreover:*

1. When  $P \in \mathcal{F}_{\text{deg}} \setminus \mathbb{C}[V]$ , if  $z_P$  spans  $\overline{\mathbb{L}}_V(P)$  then there is  $t \geq (\varepsilon/100)^3 m$  and distinct linear forms  $x_1, \dots, x_t \in \mathcal{F}_1$ , and distinct linear forms  $\alpha_1, \dots, \alpha_t \in \mathcal{F}_1$  such that for every  $i \in [t]$ , we have  $x_i, \alpha_i \notin V_1$ ,  $z_P, \overline{x_i}, \overline{\alpha_i}$  are pairwise linearly independent in  $S_1/V_1$ , and  $z_P \in \text{span}_{\mathbb{C}}\{\overline{x_i}, \overline{\alpha_i}\}$ .
2. If  $W$  is  $(17, (\varepsilon/100)^3)$ -clean such that  $\mathbb{C}[V] \subseteq \mathbb{C}[W]$ , then the above condition holds with  $W$  too.

*Proof.* Partitioning  $\mathcal{F}_{\text{deg}} = \mathcal{M} \sqcup \mathcal{N} \sqcup \mathcal{R}$  as defined in this subsection, [Proposition 5.9](#) implies that there exists a vector space  $U \subset S_1$  such that  $\dim(U) = O(1/\delta)$  and  $\mathcal{M} \subset \mathbb{C}[U]$ . Similarly, [Proposition 5.8](#) implies that there is a vector space  $W \subset S_1$  such that  $\dim(W) = O(1/\delta^2)$  and  $\mathcal{N} \subset \mathbb{C}[W]$ . Thus, we are only left with the forms in  $\mathcal{R}$ .

[Remark 5.10](#) implies that  $|\mathcal{F}_{\text{deg}}(P)| \geq \varepsilon m/10$  for each  $P \in \mathcal{R}$ . Thus, applying our double cover lemma [Lemma B.2](#) with the sets  $\mathcal{F}_{\text{deg}}(P_i)$ , for  $P_i \in \mathcal{R}$ , and parameter  $\nu = \varepsilon/10$ , we obtain a set of forms  $\mathcal{G} \subset \mathcal{R}$  with  $|\mathcal{G}| \leq (200/\varepsilon)^2$  such that for any form  $P \in \mathcal{R}$ , we have that either  $P \in \mathcal{G}$  or there

exist  $P_1, P_2 \in \mathcal{G}$  such that

$$|\mathcal{F}_{\text{deg}}(P) \cap \mathcal{F}_{\text{deg}}(P_1) \cap \mathcal{F}_{\text{deg}}(P_2)| \geq (\nu/4)^3 m = \varepsilon^3 m / 40^3.$$

Now, letting  $V' := U + W + \text{span}_{\mathbb{C}}\{\mathcal{G}\}$ , and applying the cleanup lemma [Lemma 4.12](#) with robustness parameter  $r = 17$  and clean parameter  $(\varepsilon/100)^3$  to  $V'$  and obtain our  $(17, (\varepsilon/100)^3)$ -clean vector space  $V$ . By part 1 of [Lemma 4.12](#), we have that  $\mathcal{G} \subset \mathbb{C}[V]$  and by part 2 we have  $U+W \subset V_1$ . By [Lemma 5.11](#) applied to  $P_1, P_2$  and  $P$  we deduce that either  $P \in \mathbb{C}[V]$ , or that  $P$  is univariate over  $V$ . In the latter case, the moreover part of [Lemma 5.11](#) gives us the distinct linear forms  $x_1, \dots, x_t$  and  $a_1, \dots, a_t$ . Note that  $t \geq \varepsilon^3 m / 40^3 - 4(\varepsilon/100)^3 m > (\varepsilon/100)^3 m$ . As the choice of  $P$  was arbitrary, the above holds for every  $P \in \mathcal{R}$ , and therefore for every  $P \in \mathcal{F}_{\text{deg}}$ . The last condition follows from the fact that [Lemma 5.11](#) does not depend on how the clean vector space was constructed.

By part 3 of [Lemma 4.12](#), we have  $\dim V = 128 \cdot (100/\varepsilon)^3 + \dim(V'_1) + 4 \cdot 17 \cdot \dim(V'_2)$ , which implies  $\dim(V) = O(1/\varepsilon^3) = O(1/\delta^3)$ , since  $\dim(V'_1) = \dim(U+W) = O(1/\delta)$  and  $\dim(V'_2) = |\mathcal{G}| = O(1/\delta^2)$ . This concludes the proof.  $\square$

## 5.4 Controlling $\mathcal{F}_{\text{span}}$

We now construct a clean vector space  $V$  where any form in  $\mathcal{F}_{\text{span}}$  is either in  $\mathbb{C}[V]$  or is univariate over  $V$ . We shall use the previous vector spaces for  $\mathcal{F}_{\text{square}}, \mathcal{F}_{\text{linear}}$  and  $\mathcal{F}_{\text{deg}}$  to help us in this case.

Before we prove the main lemma of this subsection, [Lemma 5.15](#), we need to understand the structure of the forms in  $\mathcal{F}_{\text{span}}$  relative to the current clean vector space that we have. To that end, throughout this section, we will work with  $W := W_1 + W_2$  being a  $(17, (\varepsilon/100)^3)$ -clean vector space such that  $\mathcal{F}_{\text{square}} \subset \mathbb{C}[W]$ , and the forms in  $\mathcal{F}_{\text{linear}} \cup \mathcal{F}_{\text{deg}}$  are either in the algebra  $\mathbb{C}[W]$  or are univariate over  $W$ . We will also define  $\mathcal{H}$  as the set of forms in  $\mathcal{F}_2$  which are in  $\mathbb{C}[W]$  or univariate over  $W$ , and  $\mathcal{G} = \mathcal{F}_2 \setminus \mathcal{H}$ . Note that by the properties of  $W$  we have that  $\mathcal{G} \subseteq \mathcal{F}_{\text{span}}$ .

**Proposition 5.13.** *If  $Q \in \mathcal{F}_{\text{span}}$  is 2-far from  $W$ , then one of the following holds:*

1. *there are at least  $\varepsilon m/3$  linear SG triples  $(Q, F_i, G_i)$  where  $F_i \in \mathcal{H}$  and  $G_i \in \mathcal{G}$ , where all forms  $F_i, G_j$  are distinct*
2. *there are at least  $\varepsilon m/3$  distinct linear SG triples  $(Q, F_i, G_i)$ , where  $F_i, G_j \in \mathcal{G}$*

*Proof.* Since  $Q$  is 2-far from  $W$ ,  $\text{rank}(Q - P) \geq 3$  for any  $P \in \mathbb{C}[W]$ . Let  $F \in \mathcal{F}_{\text{span}}(Q)$  and  $G \in \text{span}_{\mathbb{C}}\{F, Q\} \cap \mathcal{F}_2$ . Both  $F$  and  $G$  cannot be in  $\mathcal{H}$ : if that was the case, there would exist  $P_F, P_G \in \mathbb{C}[W]$  with  $\text{rank}(F - P_F) \leq 1$  and  $\text{rank}(G - P_G) \leq 1$ , which implies  $\text{rank}(Q - (P_F + P_G)) \leq 2$ , contradicting  $Q$  being 2-far from  $W$ . Thus, either  $F$  and  $G$  are both in  $\mathcal{G}$ , or one of them is in  $\mathcal{H}$  and the other is in  $\mathcal{G}$ .

Suppose we have  $F_1, F_2 \in \mathcal{H} \cap \mathcal{F}_{\text{span}}(Q)$  and  $G \in \text{span}_{\mathbb{C}}\{Q, F_1\} \cap \text{span}_{\mathbb{C}}\{Q, F_2\} \cap \mathcal{F}_2$ . In this case, we would have  $\text{span}_{\mathbb{C}}\{G, Q\} = \text{span}_{\mathbb{C}}\{F_1, F_2\}$ , which implies  $Q \in \text{span}_{\mathbb{C}}\{F_1, F_2\}$ , which contradicts  $Q$  being 2-far from  $W$ . Thus, if there are at least  $\varepsilon m/3$  forms  $F_1, \dots, F_t$  in  $\mathcal{F}_{\text{span}}(Q) \cap \mathcal{H}$ , then there are at least  $\varepsilon m/3$  distinct forms  $G_1, \dots, G_t \in \mathcal{G}$  such that  $(Q, F_i, G_i)$  is a linear SG triple.

We are now left with the case where  $|\mathcal{F}_{\text{span}}(Q) \cap \mathcal{H}| \leq \varepsilon m/3$ . Hence,  $|\mathcal{F}_{\text{span}}(Q) \cap \mathcal{G}| \geq 2\varepsilon m/3$ . Let  $P_1, \dots, P_a$  be the forms in  $\mathcal{F}_{\text{span}}(Q) \cap \mathcal{G}$  such that  $\text{span}_{\mathbb{C}}\{Q, P_i\}$  does not contain a third form in  $\mathcal{F}_{\text{span}}(Q) \cap \mathcal{G}$ . If  $R_i$  is the form spanned by  $Q$  and  $P_i$ , we must have  $R_i \in \mathcal{H}$ , and further it must be that  $R_i \notin (R_j)$ : if not then  $P_i$  and  $Q$  span  $P_j$ , contradicting our assumption on the  $P_i$ 's.

By the pigeon hole principle, and by the assumption that  $\mathcal{F}_{\text{span}}(Q) \cap \mathcal{H}$  has less than  $\varepsilon m/3$  forms, it must be that  $a \leq \varepsilon m/3$ , and therefore that there are at least  $\varepsilon m/3$  forms in  $\mathcal{F}_{\text{span}}(Q) \cap \mathcal{G}$  such that the form they span with  $Q$  also lies in  $\mathcal{G}$ .  $\square$



**Proposition 5.14.** *If  $Q \in \mathcal{F}_{\text{span}}$  is either 1-close or 2-close to  $W$  and satisfies  $\dim(\overline{\mathbb{L}}_Q(W)) \geq 2$  then there are at least  $(\varepsilon - 2(\varepsilon/100)^3)m$  distinct linear SG triples  $(Q, F_i, G_i)$  with  $F_i, G_i \in \mathcal{G}$ .*

*Proof.* Let  $Q = F_Q + E_Q$  with  $F_Q \in \mathbb{C}[W]$  and  $\text{rank}(E_Q) \leq 2$ . We have  $\overline{\mathbb{L}}_W(Q) = \overline{\mathbb{L}}_W(E_Q)$ . Let  $P \in \mathcal{F}_{\text{span}}(Q)$  and let  $R \in \mathcal{F}_2 \cap \text{span}_{\mathbb{C}}\{Q, P\}$ . Let  $Z := \mathbb{L}(E_Q) + W$ , so  $Z_1 = W_1 + \mathbb{L}(E_Q)$ .

Assume both  $P$  and  $R$  are in  $\mathcal{H}$ . If either  $P$  or  $R$  is in  $\mathbb{C}[W]$ , then  $Q$  is a univariate over  $W$  which is a contradiction, so we have  $\dim(\overline{\mathbb{L}}_P(W)) = \dim(\overline{\mathbb{L}}_W(R)) = 1$ . We can write  $P = F_P + y_P z_P$  and  $R = F_R + y_R z_R$  with  $F_P, F_R \in \mathbb{C}[W]$ . Let  $R = \alpha P + \beta Q$  for some  $\alpha, \beta \in \mathbb{C}^*$ . We have  $F_Q + \alpha F_P - \beta F_R = \beta y_R z_R - \alpha y_P z_P - E_Q$ , and this form is in  $\mathbb{C}[W]$ . Since the rank of  $\beta y_R z_R - \alpha y_P z_P - E_Q$  is bounded by 4, this form is in  $\mathbb{C}[W_1]$ . Combining this with the fact that  $y_P, y_R$  are spanned by  $z_P, z_R$  in  $S_1/W_1$  we get  $E_Q \in \mathbb{C}[W_1, z_P, z_R]$  and  $\mathbb{L}(E_Q) \subseteq W_1 + \langle z_P, z_R \rangle$ . Since  $\dim(\overline{\mathbb{L}}_W(Q)) \geq 2$ , the image of  $\mathbb{L}(E_Q)$  in  $S_1/W_1$  has dimension at least 2, and therefore is spanned by  $z_P, z_R$ . We then get  $z_P, z_R \in \overline{\mathbb{L}}_W(Q)$ , and that  $\dim(\overline{\mathbb{L}}_Z(P)) = \dim(\overline{\mathbb{L}}_Z(R)) = 0$ .

Suppose now that  $P \in \mathcal{H}$  and  $R \in \mathcal{G}$ . We again write  $P = F_P + y_P z_P$ , where  $y_P = z_P = 0$  if  $P \in \mathbb{C}[W]$ . Since  $Q$  is at most 2-close and since  $P$  is at most 1-close, the form  $R$  is at most 3-close from  $W$ . We can therefore write  $R = F_R + E_R$ , with  $F_R \in \mathbb{C}[W]$  and  $\text{rank}(E_R) \leq 3$ . Since  $R \notin \mathcal{H}$  we have  $\dim(\overline{\mathbb{L}}_W(R)) \geq 2$ . Combining the equations again we get  $E_R - E_Q - y_P z_P \in \mathbb{C}[W_1]$ , and therefore  $E_Q \in \mathbb{C}[W_1, z_P, \mathbb{L}(E_R)]$ . This implies that  $\overline{\mathbb{L}}_W(Q) \subseteq \langle z_P \rangle + \overline{\mathbb{L}}_W(R)$ . Combining this with the facts that  $\dim(\overline{\mathbb{L}}_W(R)), \dim(\overline{\mathbb{L}}_W(Q)) \geq 2$  we get that  $\dim((\overline{\mathbb{L}}_W(Q)) \cap (\overline{\mathbb{L}}_W(R))) \geq 1$ . This in turn implies that  $\dim(\overline{\mathbb{L}}_W(R)) > \dim(\overline{\mathbb{L}}_Z(R))$ . In the case when  $P \in \mathcal{G}$  and  $R \in \mathcal{H}$ , we can repeat the above analysis to deduce  $\dim(\overline{\mathbb{L}}_W(P)) > \dim(\overline{\mathbb{L}}_Z(P))$ .

We now use the clean condition to bound how many times the above two cases can occur. Let  $P_1, \dots, P_a$  be the forms in  $\mathcal{F}_{\text{span}}(Q)$ , and let  $R_i \in \mathcal{F}_2 \cap \text{span}_{\mathbb{C}}\{Q, P_i\}$ . Let  $P_1, \dots, P_b$  be the forms such that  $P_i \in \mathcal{H}$  and  $R_i \in \mathcal{G}$ . For every  $i \leq b$  we have  $\dim(\overline{\mathbb{L}}_W(R_i)) > \dim(\overline{\mathbb{L}}_Z(R_i))$  by the above. If  $R_i = R_j$  then  $Q \in \text{span}_{\mathbb{C}}\{P_i, P_j\}$ . From the above analysis, this implies  $\dim(\overline{\mathbb{L}}_W(P_i)) = \dim(\overline{\mathbb{L}}_W(P_j)) = 1$ , while  $\dim(\overline{\mathbb{L}}_Z(P_i)) = \dim(\overline{\mathbb{L}}_Z(P_j)) = 0$ . Therefore, among the  $2b$  forms  $P_1, \dots, P_b, R_1, \dots, R_b$ , there are at least  $b$  distinct forms whose relative space of linear forms with respect to  $Z$  has lower dimension than that with respect to  $W$ , and by the clean condition  $b \leq (\varepsilon/100)^3 m$ . Let  $P_{b+1}, \dots, P_{b'}$  be the forms with  $R_i \in \mathcal{H}$ . By the above analysis, for every such  $i$  we have  $\dim(\overline{\mathbb{L}}_W(P_i)) > \dim(\overline{\mathbb{L}}_Z(P_i))$ , whence  $b' - b \leq (\varepsilon/100)^3 m$ . For every  $P_i$  with  $i > b'$  we must have  $P_i, R_i \in \mathcal{G}$ , completing the proof.  $\square$

**Lemma 5.15.** *Let  $W := W_1 + W_2$  be a  $(17, (\varepsilon/100)^3)$ -clean vector space such that  $\mathcal{F}_{\text{square}} \subset \mathbb{C}[W]$ , and the forms in  $\mathcal{F}_{\text{deg}} \cup \mathcal{F}_{\text{linear}}$  are either in  $\mathbb{C}[W]$  or are univariate over  $W$ . Then there exists a  $(17, (\varepsilon/100)^3)$ -clean vector space  $U := U_1 + U_2$  with  $\mathbb{C}[W] \subset \mathbb{C}[U]$  such that every form in  $\mathcal{F}_{\text{span}}$  is either in  $\mathbb{C}[U]$  or is univariate over  $U$ . Moreover,  $\dim U_2 = \dim W_2 + \mathcal{O}(1/\varepsilon)$  and  $\dim U_1 = \dim W_1 + \mathcal{O}(\dim W_2/\varepsilon + 1/\varepsilon^4)$ .*

*Proof.* We use an iterative process to construct  $U$ . Start by setting  $U^{(0)} := W$ . Let  $\mathcal{H}^{(0)}$  consist of all forms univariate over  $U^{(0)}$  and  $\mathcal{G}^{(0)} := \mathcal{F}_2 \setminus \mathcal{H}^{(0)}$ . Suppose  $Q \in \mathcal{G}^{(0)}$  satisfies case 1 of Proposition 5.13, that is, there are at least  $\varepsilon m/3$  linear SG triples  $(Q, F_i, G_i)$  with  $F_i \in \mathcal{H}^{(0)}$  and  $G_i \in \mathcal{G}^{(0)}$ . We then set  $U'^{(1)} := U^{(0)} + \text{span}_{\mathbb{C}}\{Q\}$ , and set  $U^{(1)}$  to be the result of applying the clean up procedure (Lemma 4.12) to  $U'^{(1)}$  with parameters  $r, (\varepsilon/100)^3$ . We also set  $\mathcal{H}^{(1)}$  to be the subset of  $\mathcal{F}_2$  that is univariate over  $U^{(1)}$ , and set  $\mathcal{G}^{(1)} := \mathcal{F}_2 \setminus \mathcal{H}^{(1)}$ . The form  $Q$  is in  $\mathbb{C}[U^{(1)}]$ , and the forms  $G_i$  are univariate over  $U^{(1)}$ , and therefore  $|\mathcal{H}^{(1)}| - |\mathcal{H}^{(0)}| \geq \varepsilon m/3$ . By Lemma 4.12, we have  $\dim U_2^{(1)} \leq \dim U_2^{(0)} + 1$  and

$$\dim U_1^{(1)} \leq \dim U_1^{(0)} + 128 \cdot (100/\varepsilon)^3 + 68 \cdot (\dim U_2^{(0)} + 1).$$

We repeat the above process as long as we can find such a form  $Q$ . After  $t$  steps, we have vector space  $U^{(t)}$  and subset  $\mathcal{H}^{(t)}$  such that  $|\mathcal{H}^{(t)}| - |\mathcal{H}^{(0)}| \geq \epsilon t m / 3$ , and  $\dim U_2^{(t)} \leq \dim U_2^{(0)} + t$ , and

$$\dim U_1^{(t)} \leq \dim U_1^{(0)} + 128 \cdot (100/\epsilon)^3 \cdot t + 68 \cdot t \cdot \dim U_2^{(0)} + 68 \cdot \frac{t(t+1)}{2}.$$

Since  $|\mathcal{H}^{(t)}| \leq m$ , the process must stop after  $t = 3/\epsilon$  steps.

Once we can no longer find such a form  $Q$ , every form in  $\mathcal{G}^{(t)}$  satisfies either case 2 of [Proposition 5.13](#) or [Proposition 5.14](#), and therefore  $\mathcal{G}^{(t)}$  is a robust linear SG configuration with parameter  $\epsilon/6$ . By [Theorem 2.11](#) there are forms  $P_1, \dots, P_b$  with  $b \leq 78/\epsilon$  such that  $\mathcal{G}^{(t)} \subseteq \text{span}_{\mathbb{C}}\{P_1, \dots, P_b\}$ . We set  $U' := U^{(t)} + \text{span}_{\mathbb{C}}\{P_1, \dots, P_b\}$ , and set  $U$  to be the result of the clean up procedure ([Lemma 4.12](#)) to  $U'$  with parameters  $r, \epsilon^3/4^8$ . By construction, every form in  $\mathcal{F}_{\text{span}}$  is either in  $\mathbb{C}[U]$  or univariate over  $U$ . Since  $\mathbb{C}[W] \subseteq \mathbb{C}[U]$ , every form in  $\mathcal{F}$  is also either in  $\mathbb{C}[U]$  or univariate over  $U$ . Finally, using the bound on  $\dim U^{(t)}$  and  $b$  we get  $\dim U_2 \leq \dim W_2 + C/\epsilon$  and

$$\dim U_1 \leq \dim W_1 + C \cdot \frac{\dim W_2}{\epsilon} + C \cdot \frac{1}{\epsilon^4}$$

for some universal constant  $C$ . □

## 5.5 Proof of Theorem 1.3

We now prove our main theorem:  $(\delta, 2)$ -rad-SG configurations must lie in a constant dimensional vector space. We prove our result by first constructing an auxiliary algebra where the forms of our configuration  $\mathcal{F}$  are either in the algebra, or are univariate over this algebra, and then prove that we can augment this algebra slightly to contain all forms from  $\mathcal{F}$ . The first step follows from the lemmas we have proved in the last four subsections. The second step is to show that extra variables corresponding to the forms form a LCC configuration, allowing us to bound their rank.

**Lemma 5.16** (Reduction to Base Configuration). *Let  $0 < \delta \leq 1$  be a constant, and let  $\epsilon := \delta/10$ . Let  $\mathcal{F}$  be a  $(\delta, 2)$ -rad-SG configuration. There exists a  $(17, (\epsilon/100)^3)$ -clean vector space with respect to  $\mathcal{F}$ , denoted by  $V$ , such that:*

1. every form in  $\mathcal{F}$  is either in  $\mathbb{C}[V]$  or univariate over  $V$ , and  $\dim(V) = O(1/\epsilon^4)$ .
2.  $\mathcal{F}_{\text{square}} \cup \mathcal{F}_{\text{linear}} \subseteq \mathbb{C}[V]$ .
3. For every form  $P \in \mathcal{F}_{\text{deg}} \setminus \mathbb{C}[V]$ , if  $\overline{\mathbb{L}}_V(P) = \text{span}_{\mathbb{C}}\{z_P\}$  then there are at least  $(\epsilon/100)^3$  distinct linear forms  $x_1, \dots, x_t \in \mathcal{F}_1$  and distinct linear forms  $a_1, \dots, a_t \in \mathcal{F}_1$  such that for every  $i$ , the linear forms  $z_P, \overline{x}_i, \overline{a}_i$  are pairwise linearly independent in  $S_1/V_1$ , and  $z_P \in \text{span}_{\mathbb{C}}\{\overline{x}_i, \overline{a}_i\}$ .

*Proof.* Let  $V^{(1)}$  be the vector space obtained by applying [Lemma 5.3](#) to  $\mathcal{F}$ . Let  $V^{(2)}$  be the vector space obtained by applying [Proposition 5.4](#) to  $\mathcal{F}$ . Let  $V^{(3)}$  be the vector space obtained by applying the clean up procedure ([Lemma 4.12](#)) to  $V^{(2)}$ , with parameters  $17, (\epsilon/100)^3$ . We have  $\dim V_1^{(3)} = O(1/\epsilon^3)$  and  $\dim V_2^{(3)} = O(1/\epsilon^2)$ . By [Lemma 5.3](#) we have  $\mathcal{F}_{\text{square}} \subseteq \mathbb{C}[V^{(3)}]$ , and by [Lemma 5.5](#) every form in  $\mathcal{F}_{\text{linear}}$  is either in  $\mathbb{C}[V^{(3)}]$  or univariate over  $V^{(3)}$ .

Now let  $V^{(4)}$  be the  $(17, (\epsilon/100)^3)$ -clean vector space obtained by applying [Lemma 5.12](#) to  $\mathcal{F}_{\text{deg}}$ . Let  $V^{(5)}$  be the result of applying the clean up procedure ([Lemma 4.12](#)) to  $V^{(3)} + V^{(4)}$  with parameters  $17, (\epsilon/100)^3$ . We have  $\dim V_1^{(5)} = O(1/\epsilon^3)$  and  $\dim V_2^{(5)} = O(1/\epsilon^3)$ . Every form in  $\mathcal{F}_{\text{deg}}$  is now either in  $\mathbb{C}[V^{(5)}]$  or univariate over  $V^{(5)}$ . The conditions on  $\mathcal{F}_{\text{square}}, \mathcal{F}_{\text{linear}}$  still hold with  $V^{(5)}$  in place of  $V^{(3)}$ .

Finally, let  $V$  be the result of applying [Lemma 5.15](#) to  $V^{(5)}$ . Every form in  $\mathcal{F}_{\text{span}}$  is either in  $\mathbb{C}[V]$  or univariate over  $V$ . The vector space  $V$  is  $(17, (\varepsilon/100)^3)$ -clean, and we have  $\dim V_1 = \mathcal{O}(1/\varepsilon^4)$  and  $\dim V_2 = \mathcal{O}(1/\varepsilon^3)$ .

By construction, we have  $\mathcal{F}_{\text{square}} \subseteq \mathbb{C}[V]$  and that every form in  $\mathcal{F}$  is either in  $\mathbb{C}[V]$  or univariate over  $V$ . Note that this condition trivially holds for the forms in  $\mathcal{F}_1$ . We can now apply [Lemma 5.7](#) to deduce that  $\mathcal{F}_{\text{linear}} \subseteq \mathbb{C}[V]$ . Since  $\mathbb{C}[V^{(5)}] \subseteq \mathbb{C}[V]$ , the condition for forms in  $\mathcal{F}_{\text{deg}} \setminus \mathbb{C}[V]$  holds by the last statement of [Lemma 5.12](#).  $\square$

**Lemma 5.17 (Base Configuration).** *Let  $0 < \delta \leq 1$ ,  $\varepsilon := \delta/10$  be constants. If  $\mathcal{F}$  is a  $(\delta, 2)$ -rad-SG configuration, and  $V := V_1 + V_2$  is  $(17, (\varepsilon/100)^3)$ -clean vector space with  $\mathcal{F}$  that satisfies the conditions of [Lemma 5.16](#), then there exists  $U \subset S_1$  with  $\dim(U) = \mathcal{O}(1/\delta^{27})$  such that  $\mathcal{F} \subset \mathbb{C}[V, U]$ .*

*Proof.* For every  $Q \in \mathcal{F}_2$ , we use  $z_Q$  to denote the linear form in  $S_1/V_1$  that spans  $\overline{\mathbb{L}}_V(Q)$ . For linear forms  $\ell \in \mathcal{F}_1$ , we use  $z_\ell$  to denote the image of  $\ell$  in  $S_1/V_1$ . If a form is in  $\mathbb{C}[V]$  then  $z_Q = 0$ , and if a linear form is in  $V_1$  then  $z_\ell = 0$ . Let  $\lambda := \frac{1}{4} \cdot (\varepsilon/100)^3$ . We now show that the set of nonzero linear forms  $z_Q, z_\ell$  form a  $\lambda$ -LCC configuration, which allows us to bound their dimension.

Let  $\mathcal{F}'$  be the subset of  $\mathcal{F}$  that consists of forms not in  $\mathbb{C}[V]$ . Define  $\mathcal{F}'_1 := \mathcal{F}' \cap S_1$  and  $\mathcal{F}'_2 = \mathcal{F}' \cap S_2$ . Let  $P_1, \dots, P_b$  be the forms in  $\mathcal{F}'_2$  and let  $\ell_{b+1}, \dots, \ell_c$  be the forms in  $\mathcal{F}'_1$ . By definition, the linear forms  $z_{P_i}$  and  $z_{\ell_j}$  are all nonzero, although they might not all be distinct. In order to show that these linear forms form a  $\lambda$ -LCC configuration, we have to show the following: given a form  $P \in \mathcal{F}'$  and a subset  $\Gamma \subset \mathcal{F}'$  of size at most  $\lambda m$ , there are forms  $F, G \in \mathcal{F}' \setminus \Gamma$  such that  $z_P \in \text{span}_{\mathbb{C}}\{z_F, z_G\}$ .

Suppose  $P \in \mathcal{F}'_2$ . Since  $\mathcal{F}_{\text{linear}}, \mathcal{F}_{\text{square}} \subseteq \mathbb{C}[V]$  we have  $P \in \mathcal{F}_{\text{span}} \cup \mathcal{F}_{\text{deg}}$ . We handle each of these two cases separately. Let  $Z := V + z_P$ .

- Suppose  $P \in \mathcal{F}_{\text{span}}$ , and suppose  $(P, F_i, G_i)$  are the SG triples corresponding to  $P$ . If  $F_i \in \mathbb{C}[V]$ , then  $z_P \in (z_{G_i})$ . If  $G_i = G_j$  then  $P \in \text{span}_{\mathbb{C}}\{F_i, F_j\}$ , contradicting  $P \notin \mathbb{C}[V]$ . This implies that  $G_i$  and  $G_j$  are distinct if  $F_i, F_j \in \mathbb{C}[V]$ . Therefore, by the clean condition there are at most  $(\varepsilon/100)^3 m$  SG triples with  $F_i \in \mathbb{C}[V]$  since for each of these triples we have  $\dim \overline{\mathbb{L}}_V(G_i) = 1$  and  $\dim \overline{\mathbb{L}}_Z(G_i) = 0$ . The clean condition also implies that there are at most  $(\varepsilon/100)^3 m$  SG triples with  $z_{F_i} \in (z_P)$ , since for each of these we have  $\dim \overline{\mathbb{L}}_V(F_i) = 1$  and  $\dim \overline{\mathbb{L}}_Z(F_i) = 0$ .

We only consider the remaining  $(\varepsilon - 2(\varepsilon/100)^3)m$  triples, where we have  $z_{F_i} \neq 0$  and  $z_{F_i} \notin (z_P)$ . The latter condition also implies  $G_i \notin \mathbb{C}[V]$ . Therefore, every triple we consider satisfies  $F_i, G_i \in \mathcal{F}'$ . Let  $\Gamma$  be any subset of  $\mathcal{F}'$  of size at most  $\lambda m$ . After removing at most  $\lambda m$  SG triples, since  $\varepsilon - 2(\varepsilon/100)^3 - \lambda > 2\lambda$  there are still  $2\lambda m$  triples with  $F_i \notin \Gamma$ . If  $G_i = G_j$ , for two of such triples, then  $P \in \text{span}_{\mathbb{C}}\{F_i, F_j\}$  and we are done. If the forms  $G_i$  are all distinct for these  $2\lambda m$  triples, then after removing at most  $\lambda m$  more triples we can also assume that  $G_i \notin \Gamma$  for any triple. In either case,  $P$  is spanned by two forms  $Q_1, Q_2 \in \mathcal{F}' \setminus \Gamma$ , and  $z_P$  is spanned by  $z_{Q_1}, z_{Q_2}$ . Hence  $z_P$  satisfies the condition of the  $\lambda$ -LCC configuration.

- Suppose now that  $P \in \mathcal{F}_{\text{deg}}$ . By assumption, there are at least  $(\varepsilon/100)^3 m$  linear forms  $x_1, \dots, x_t \in \mathcal{F}'_1$ , and linear forms  $a_1, \dots, a_t \in \mathcal{F}'_1$  such that  $z_P \in \text{span}_{\mathbb{C}}\{z_{x_i}, z_{a_i}\}$ . [Lemma 5.11](#) also guarantees that each of the  $x_i$  are distinct, and that each of the  $a_i$  are distinct. Let  $\Gamma \subset \mathcal{F}'$  of size at most  $\lambda m$ . Since the  $x_i$  are distinct, and since the  $a_i$  are distinct, there are at most  $2\lambda m$  indices with either  $x_i \in \Gamma$  or  $a_i \in \Gamma$ . Since  $(\varepsilon/100)^3 m - 2\lambda m > 0$ , we can find an index  $i$  such that  $z_P \in \text{span}_{\mathbb{C}}\{z_{x_i}, z_{a_i}\}$  with  $x_i, a_i \in \mathcal{F}'_1 \setminus \Gamma$ , proving that  $z_P$  satisfies the  $\lambda$ -LCC criterion.

Now let  $\ell \in \mathcal{F}'_1$  and  $\Gamma \subset \mathcal{F}'$  such that  $|\Gamma| \leq \lambda m$ .

- Suppose  $\ell$  satisfies the SG condition with at least  $\varepsilon m/2$  linear forms, that is, there are at least  $\varepsilon m/2$  SG triples  $(\ell, g_i, H_i)$  with  $g_i \in \mathcal{F}_1$ . If  $H_i \in \mathcal{F}_2$ , then  $\ell \in \mathbb{L}(H_i)$ , and since  $H_i$  is univariate over  $V$  we get  $z_{H_i} \in (z_\ell)$ . By the clean condition, there can be at most  $(\varepsilon/100)^3 m$  triples with  $H_i \in \mathcal{F}_2$ , since  $\dim \overline{\mathbb{L}}_V(H_i) > \dim \overline{\mathbb{L}}_{V+\{z_\ell\}}(H_i)$ . We therefore restrict our attention to the  $\varepsilon m/2 - (\varepsilon/100)^3 m$  triples  $(\ell, g_i, H_i)$  where  $H_i$  is a linear form. By the same argument as the case of  $P \in \mathcal{F}_{\text{span}}$  above we get either  $\ell \in \text{span}_{\mathbb{C}}\{g_i, g_j\}$  with  $g_i, g_j \in \mathcal{F}'_1 \setminus \Gamma$  or  $\ell \in \text{span}_{\mathbb{C}}\{g_i, H_i\}$  with  $g_i, H_i \in \mathcal{F}'_1 \setminus \Gamma$ . This step requires  $(\varepsilon/2 - 3(\varepsilon/100)^3 - 2\lambda)m > 0$  which holds by the choice of  $\lambda$ .
- Finally suppose  $\ell$  satisfies the SG condition with at least  $\varepsilon m/2$  quadratics, that is, there are at least  $\varepsilon m/2$  triples  $(\ell, F_i, H_i)$  with  $F_i \in \mathcal{F}_2$ . By [Proposition 2.9](#), the ideal  $(\ell, F_i)$  is not radical only if  $\ell \in \mathbb{L}(F_i)$ . Since  $F_i$  is univariate over  $V$ , and since  $\ell \notin V_1$ , this condition implies  $z_{F_i} \in (z_\ell)$ . By the clean condition, this can happen for at most  $(\varepsilon/100)^3 m$  triples, since  $\dim \overline{\mathbb{L}}_V(F_i) > \dim \overline{\mathbb{L}}_{V+\{z_\ell\}}(F_i)$ . For the remaining triples, we have  $H_i = F_i + \ell h_i$  for some linear form  $h_i$ . If  $F_i \in \mathbb{C}[V]$ , then  $\overline{\mathbb{L}}_V(H_i)$  is spanned by  $\ell, h_i$ , and since  $H_i$  is univariate over  $V$ , we get  $z_{H_i} \in (z_\ell)$ . If  $F_i, F_j \in \mathbb{C}[V]$ , then  $H_i \neq H_j$ , otherwise  $0 \neq \ell(h_i - \mu h_j) \in \mathbb{C}[V_1]$  for some constant  $\mu \in \mathbb{C}$ , contradicting  $\ell \notin V_1$ . Therefore, by the clean condition, there are at most  $(\varepsilon/100)^3 m$  triples with  $F_i \in \mathbb{C}[V]$ , since for each such index we have  $\dim \overline{\mathbb{L}}_V(H_i) > \dim \overline{\mathbb{L}}_{V+\{z_\ell\}}(H_i)$ . For every other triple we have  $\ell h_i + z_{F_i} y_{F_i} - z_{H_i} y_{H_i} \in \mathbb{C}[V_1]$ , whence  $z_\ell \in \text{span}_{\mathbb{C}}\{z_{F_i}, z_{H_i}\}$ . By the same argument as the case of  $P \in \mathcal{F}_{\text{span}}$  above we get either  $z_\ell \in \text{span}_{\mathbb{C}}\{z_{F_i}, z_{F_j}\}$  with  $F_i, F_j \in \mathcal{F}'_2 \setminus \Gamma$  or  $z_\ell \in \text{span}_{\mathbb{C}}\{z_{F_i}, z_{H_i}\}$  with  $F_i, H_i \in \mathcal{F}'_2 \setminus \Gamma$ . This step also requires  $(\varepsilon/2 - 3(\varepsilon/100)^3 - 2\lambda)m > 0$  which holds by the choice of  $\lambda$ .

Therefore, the set  $\{z_{P_i}, z_{\ell_j} \mid P_i, \ell_j \in \mathcal{F}'\}$  forms a  $\lambda$ -LCC configuration. By [Theorem 2.13](#), there is a vector space  $U$  of  $S_1/V_1$  of dimension  $\mathcal{O}(\lambda^9)$  such  $z_{P_i}, z_{\ell_j} \in U$ . Since  $z_P = 0$  for every  $P \in \mathcal{F} \setminus \mathcal{F}'$ , we can say  $z_P \in U$  for every  $P \in \mathcal{F}$ . Finally, since every form  $P \in \mathcal{F}$  is univariate over  $V$ , we have  $P \in \mathbb{C}[V, z_P]$ , whence  $P \in \mathbb{C}[V, U]$  as required.  $\square$

**Theorem 1.3** ( $(\delta, 2)$ -rad-SG theorem). *If  $\mathcal{F}$  is a  $(\delta, 2)$ -rad-SG configuration, then*

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

*Proof.* Let  $\varepsilon := \delta/10$ . Given a  $(\delta, 2)$ -rad-SG, apply [Lemma 5.16](#) to obtain  $V$ , a  $(17, (\varepsilon/100)^3)$ -clean vector space with respect to  $\mathcal{F}$  such that  $\dim V = \mathcal{O}(1/\varepsilon^4)$ , and every form in  $\mathcal{F}$  is either in  $\mathbb{C}[V]$ , or univariate over  $V$ . We now apply [Lemma 5.17](#) with vector space  $V$ , to obtain a vector space  $U \subseteq S_1$  such that  $\dim(U) = \mathcal{O}(1/\delta^{27})$ , and  $\mathcal{F} \subseteq \mathbb{C}[V, U]$ .

Since the generators of  $\mathbb{C}[V, U]$  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,  $\dim \mathbb{C}[V, U]_2 = \mathcal{O}(1/\delta^{54})$ . The vector space  $\mathbb{C}[V, U]_1 + \mathbb{C}[V, U]_2$  contains  $\mathcal{F}$  and has dimension  $\mathcal{O}(1/\delta^{54})$ .  $\square$

## 6 Conclusion and Open Problems

In this paper, we prove a robust version of the radical Sylvester-Gallai theorem for quadratics, generalizing [\[Shp20\]](#). 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 [\[BDYW11\]](#). We similarly 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. These higher dimensional variants have applications in algebraic complexity, as they can be instrumental in proving the main conjectures posed in [Gup14] 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 [Gup14, 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 [PS20a], 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 [BDYW11] the robust linear Sylvester-Gallai theorem was sufficient to induct on the higher-dimensional analogs.

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,<sup>8</sup> 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 with non-constant dimension over characteristic zero, which are not known to exist.

## Bibliography

- [AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison Wesley Publishing Company, 1969. [12](#), [15](#)
- [BDYW11] 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*, page 519–528, New York, NY, USA, 2011. Association for Computing Machinery. [2](#), [5](#), [11](#), [36](#), [37](#)
- [BM90] Peter Borwein and William OJ Moser. A survey of sylvester’s problem and its generalizations. *Aequationes Mathematicae*, 40(1):111–135, 1990. [2](#)
- [CKS19] Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Closure results for polynomial factorization. *Theory of Computing*, 15(1):1–34, 2019. [7](#)
- [CTSSD87] J-L Colliot-Thélène, 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. [4](#)

---

<sup>8</sup>Aside from 2-query LCCs where optimal lower bounds are known for both linear and non-linear codes

- [DDS21] Pranjali Dutta, Prateek Dwivedi, and Nitin Saxena. Deterministic identity testing paradigms for bounded top-fan-in depth-4 circuits. In *Proceedings of the 36th Computational Complexity Conference, CCC '21*, Dagstuhl, DEU, 2021. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. 7
- [Dic14] Leonard Eugene Dickson. The points of inflexion of a plane cubic curve. *The Annals of Mathematics*, 16(1/4):50–66, 1914. 1
- [DSW14] 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. 2, 5, 11
- [Dvi12] Zeev Dvir. Incidence theorems and their applications. *arXiv preprint arXiv:1208.5073*, 2012. 1, 2
- [EBW<sup>+</sup>43] 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. 1
- [EG84] D. Eisenbud and S. Goto. Linear free resolutions and minimal multiplicity. *J.Algebra*, 88:89–133, 1984. 14
- [Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Theory*. Springer-Verlag, New York, 1995. 12, 13
- [Eng07] B. Engheta. On the projective dimension and the unmixed part of three cubics. *J.Algebra*, 316:715–734, 2007. 14
- [Gal44] Tibor Gallai. Solution of problem 4065. *American Mathematical Monthly*, 51:169–171, 1944. 1
- [Gup14] Ankit Gupta. Algebraic geometric techniques for depth-4 PIT & Sylvester-Gallai conjectures for varieties. In *Electron. Colloquium Comput. Complex.*, volume 21, page 130, 2014. 2, 3, 6, 7, 37
- [Han65] 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. 2
- [Hir83] Friedrich Hirzebruch. Arrangements of lines and algebraic surfaces. In *Arithmetic and geometry*, pages 113–140. Springer, 1983. 1
- [HP94] William Vallance Douglas Hodge and Daniel Pedoe. *Methods of Algebraic Geometry: Volume 2*. Cambridge University Press, 1994. 4
- [Kel86] Leroy Milton Kelly. A resolution of the Sylvester-Gallai problem of J.-P. Serre. *Discrete & Computational Geometry*, 1(2):101–104, 1986. 1
- [KS09] 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. 2
- [LST21] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Electron. Colloquium Comput. Complex.*, page 81, 2021. 7

- [Mel40] Eberhard Melchior. Uber vielseite der projektiven ebene. *Deutsche Math*, 5:461–475, 1940. 1
- [MM18] Paolo Mantero and Jason McCullough. A finite classification of  $(x, y)$ -primary ideals of low multiplicity. *Collectanea Mathematica*, 69(1):107–130, 2018. 16, 39, 40
- [OS22] Rafael Oliveira and Akash Sengupta. Radical sylvester-gallai theorem for cubics. *Manuscript*, 2022. 4, 8
- [PS20a] Shir Peleg and Amir Shpilka. A generalized sylvester-gallai type theorem for quadratic polynomials. *CoRR*, abs/2003.05152, 2020. 4, 6, 7, 9, 10, 14, 15, 16, 18, 22, 25, 37
- [PS20b] 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. 7, 22
- [PS22] Shir Peleg and Amir Shpilka. Robust sylvester-gallai type theorem for quadratic polynomials. *CoRR*, abs/2202.04932, 2022. 8
- [Ser66] Jean-Pierre Serre. Advanced problem 5359. *Amer. Math. Monthly*, 73(1):89, 1966. 1
- [Shp20] Amir Shpilka. Sylvester-gallai type theorems for quadratic polynomials. *Discrete Analysis*, page 14492, 2020. 1, 3, 4, 6, 7, 9, 14, 15, 24, 36
- [Sin16] 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. 2
- [SS13] 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. 2
- [ST83] Endre Szemerédi and William T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3(3):381–392, 1983. 2
- [Syl93] James Joseph Sylvester. Mathematical question 11851. *Educational Times*, 59(98):256, 1893. 1

## A Elaborating on the proof of Proposition 3.10

The results of [MM18] classify the low degree parts of  $(x, y)$  primary ideals of degrees at most 4. We are interested in the ideals primary to  $(x, y)$  that can contain two irreducible quadratics  $Q_1, Q_2$  such that  $\mathbb{L}(Q_1) \neq \mathbb{L}(Q_2)$ . Suppose  $J$  is an ideal primary to  $(x, y)$  that contains  $Q_1$  and  $Q_2$ . The degree of  $(Q_1, Q_2)$  is at most 4, and therefore the same is true of  $J$ . Since  $Q_1, Q_2$  have degree two, and since  $J$  is homogeneous, we are only interested in the generators of  $J$  of degree at most 2. Note that every irreducible homogeneous forms in two variables is reducible.

Suppose  $J$  has degree 2. It then satisfies either case 1 or case 2 of Proposition 1.1 from [MM18]. We can rule out case 2, since if  $a, b$  have degrees higher than 2 then  $J$  contains only reducible polynomials, and if  $a, b$  have degree 1 then  $\mathbb{L}(Q_1) = \mathbb{L}(Q_2)$ , and these are spanned by  $a, b, x, y$ .

Suppose  $J$  has degree 3. It satisfies one of the eight cases from Theorem 2.1 of [MM18]. We can rule out case 1 and case 2, since quadratic polynomials in these ideals cannot be irreducible. We can rule out case 3 since every irreducible polynomial in such ideals have the same linear space. For the remaining cases, we focus only on the generators of degree at most 2. Cases 4 and 5 are ruled out by irreducibility. The other cases are ruled out since they have no generators of degree less than 3.

Suppose  $J$  has degree 4, so it satisfies one of the 23 cases of Theorem 3.1 in [MM18]. We can rule out cases 1, 2, 3, 4 by irreducibility. We can rule out case 5 since our polynomials satisfy  $\mathbb{L}(Q_1) \neq \mathbb{L}(Q_2)$ . The other cases have generators of higher degree, so we focus on the low degree parts. In each of the cases, the degree two parts are either empty, or can only contain reducible polynomials. This rules out all the cases.

## B Covering Lemmas

In this section, we state and prove the combinatorial covering lemmas that we will need in the Sylvester-Gallai proof in Section 5.

We begin with an easy proposition on the basic covering of a set. The following lemma states that given a family of large subsets, we can find a small subfamily such that every subset has large intersection with some element of the subfamily.

**Proposition B.1.** *Let  $\mathcal{U}$  be a set of size at most  $n$ , and let  $0 < \nu < 1$  be a constant. Let  $S_1, \dots, S_t \subset \mathcal{U}$  be a family of subsets of  $\mathcal{U}$  such that for each  $i \in [t]$ , we have  $|S_i| \geq \nu n$ . There exists a subset  $\mathcal{H} \subset [t]$  satisfying  $|\mathcal{H}| \leq 2/\nu$  such that for any  $i \in [t]$ ,*

$$\left| S_i \cap \bigcup_{j \in \mathcal{H}} S_j \right| \geq \nu n / 2.$$

*In particular, there exists  $j \in \mathcal{H}$  such that  $|S_i \cap S_j| \geq \nu^2 n / 4$ .*

*Proof.* We construct the subset  $\mathcal{H}$  greedily. Start with  $\mathcal{H} := \emptyset$ . As long as there is an index  $i \in [t] \setminus \mathcal{H}$  such that the intersection of  $S_i$  and  $\bigcup_{j \in \mathcal{H}} S_j$  is less than  $\nu n / 2$ , we add  $i$  to  $\mathcal{H}$ . Each time we add an index to  $\mathcal{H}$ , we increase the size of  $\bigcup_{i \in \mathcal{H}} S_i$  by at least  $\nu n / 2$ , thus we have at any point of the process above we have

$$|\mathcal{H}| \cdot \nu n / 2 \leq \left| \bigcup_{i \in \mathcal{H}} S_i \right| \leq n \Rightarrow |\mathcal{H}| \leq 2/\nu.$$

Therefore this iterative process must end after at most  $2/\nu$  steps, and at the end of the process we must have  $|\mathcal{H}| \leq 2/\nu$ . Further, at the end of the process, for every  $i \notin \mathcal{H}$ , we must have that

$$\left| S_i \cap \bigcup_{j \in \mathcal{H}} S_j \right| \geq \nu n / 2.$$

By the pigeonhole principle, there is an index  $j \in \mathcal{H}$  such that  $|S_i \cap S_j| \geq \frac{\nu n}{2|\mathcal{H}|} \geq \nu^2 n / 4$ .  $\square$

We now apply the above lemma to obtain a larger subfamily of sets that form a “double cover” of the elements of the universe, that is, such that every subset in our family has large simultaneous intersection with two elements of the subfamily.



**Lemma B.2** (Double covering lemma). *Let  $\mathcal{U}$  be a set of size at most  $n$ , and let  $0 < \nu < 1$  be a constant. Let  $S_1, \dots, S_t \subset \mathcal{U}$  be a family of subsets of  $\mathcal{U}$  such that for each  $i \in [t]$ , we have  $|S_i| \geq \nu n$ . There exist  $h \leq 2/\nu$  and subsets  $\mathcal{H}, \mathcal{H}_1, \dots, \mathcal{H}_h \subset [t]$  such that the following properties hold:*

- $|\mathcal{H}| = h$  and  $\mathcal{H}$  satisfies the properties of [Proposition B.1](#)
- $|\mathcal{H}_i| \leq 8/\nu$
- $\mathcal{H} \cap \bigcup_{j \in [h]} \mathcal{H}_j = \emptyset$
- for any  $k \in [t]$  such that  $k \notin \mathcal{H} \cup \bigcup_{i \leq h} \mathcal{H}_i$ , there exist  $i \in \mathcal{H}$  and  $j \in \mathcal{H}_i$  such that

$$|S_i \cap S_j \cap S_k| \geq \nu^3 n / 4^3$$

*Proof.* For every  $i$ , define  $S'_i$  to be a subset of  $S_i$  of size exactly  $\nu n$ . For any  $i, j, k$  we have  $|S_i \cap S_j \cap S_k| \geq |S'_i \cap S'_j \cap S'_k|$ . If the result is proved for the family  $S'_1, \dots, S'_t$ , then the result also holds for the original family  $S_1, \dots, S_t$ , with the same  $\mathcal{H}$  and  $\mathcal{H}_i$  acting as witnesses. We can thus assume that the original family consists of sets of size exactly  $\nu n$ .

In order to obtain  $\mathcal{H}$ , we apply [Proposition B.1](#) to the family. After relabelling the subsets  $S_i$ , we can assume that  $\mathcal{H} = \{1, 2, \dots, h\}$ .

We now partition the remaining subsets  $S_{h+1}, \dots, S_t$  as follows. For each  $i > h$ , let  $g_i$  be an index between 1 and  $h$  such that  $|S_i \cap S_{g_i}| \geq \nu^2 n / 4$ . The construction of  $\mathcal{H}$  guarantees the existence of at least one such index for every  $i$ , and if there are multiple such indices, we pick one arbitrarily. Define  $\mathcal{G}_k := \{i \mid g_i = k\}$ , so each  $\mathcal{G}_k$  is a collection of subsets that has large intersection with  $S_k$ .

In order to construct  $\mathcal{H}_1, \dots, \mathcal{H}_h$ , we apply [Proposition B.1](#) to each of the families  $\mathcal{G}_1, \dots, \mathcal{G}_h$ . We will show how to construct  $\mathcal{H}_1$ , as the construction of the other  $\mathcal{H}_i$ 's are analogous.

In this case, the set  $\mathcal{U}$  is  $S_1$ , which is of size  $|S_1| = \nu n$ . The sets that make up the family are  $S_j \cap S_1$  for every  $j$  in  $\mathcal{G}_1$ , which have size at least  $\nu^2 n / 4$ . The parameter is  $\nu/4$ . Applying [Proposition B.1](#) we obtain  $\mathcal{H}_1$ , a subset of  $\mathcal{G}_1$  of size at most  $8/\nu$ . For any  $j \in \mathcal{G}_1$ , either  $j \in \mathcal{H}_1$  or there is a  $k \in \mathcal{H}_1$  such that  $|S_j \cap S_k \cap S_1| \geq \nu^3 n / 4^3$ . We similarly get  $\mathcal{H}_2, \dots, \mathcal{H}_h$ .

The first, second, and third claimed properties follow by construction. The fourth property follows by the argument in the previous paragraph, and the fact that the  $\mathcal{G}_i \setminus \mathcal{H}_i$  cover the indices  $\{h+1, \dots, n\}$  that are not in any  $\mathcal{H}_i$ .  $\square$