A Generalized Sylvester-Gallai Type Theorem for Quadratic Polynomials

Shir Peleg
Department of Computer Science, Tel Aviv University, Israel
shirpele@tauex.tau.ac.il

Amir Shpilka
Department of Computer Science, Tel Aviv University, Israel
shpilka@tauex.tau.ac.il

Abstract

In this work we prove a version of the Sylvester-Gallai theorem for quadratic polynomials that takes us one step closer to obtaining a deterministic polynomial time algorithm for testing zeroness of $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits. Specifically, we prove that if a finite set of irreducible quadratic polynomials $\mathcal{Q}$ satisfy that for every two polynomials $Q_1, Q_2 \in \mathcal{Q}$ there is a subset $\mathcal{K} \subset \mathcal{Q}$, such that $Q_1, Q_2 \notin \mathcal{K}$ and whenever Q_1 and Q_2 vanish then $\prod_{Q_i \in \mathcal{K}} Q_i$ vanishes, then the linear span of the polynomials in $\mathcal{Q}$ has dimension $O(1)$. This extends the earlier result [33] that showed a similar conclusion when $|\mathcal{K}| = 1$.

An important technical step in our proof is a theorem classifying all the possible cases in which a product of quadratic polynomials can vanish when two other quadratic polynomials vanish. I.e., when the product is in the radical of the ideal generated by the two quadratics. This step extends a result from [33] that studied the case when one quadratic polynomial is in the radical of two other quadratics.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases Algebraic computation, Computational complexity, Computational geometry

Digital Object Identifier 10.4230/LIPIcs.CCC.2020.8

Related Version A full version of the paper is available at `https://arxiv.org/abs/2003.05152`.

Funding The research leading to these results has received funding from the Israel Science Foundation (grant number 552/16) and from the Len Blavatnik and the Blavatnik Family foundation.
Amir Shpilka: Part of this work was done while the author was a visiting professor at NYU.

1 Introduction

This paper studies a problem at the intersection of algebraic complexity, algebraic geometry and combinatorics that is motivated by the polynomial identity testing problem (PIT for short) for depth 4 circuits. The question can also be regarded as an algebraic generalization and extension of the famous Sylvester-Gallai theorem from discrete geometry. We shall first describe the Sylvester-Gallai theorem and some of its many extensions and generalization and then discuss the relation to PIT.

Sylvester-Gallai type theorems

The Sylvester-Gallai theorem asserts that if a finite set of points in $\mathbb{R}^n$ has the property that every line passing through any two points in the set also contains a third point in the set then all the points in the set are colinear. Kelly extended the theorem to points in $\mathbb{C}^n$ and proved that if a finite set of points satisfy the Sylvester-Gallai condition then the points in the set are coplanar. Many variants of this theorem were studied: extensions to higher dimensions, colored versions, robust versions and many more. For a more on the Sylvester-Gallai theorem and some of its variants see [6, 3, 9].

35th Computational Complexity Conference (CCC 2020).
Editor: Shubhangi Saraf; Article No. 8; pp. 8:1–8:33
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
COMPUTATIONAL COMPLEXITY CONFERENCE

There are two extensions that are of specific interest for our work: The **colored** version, proved by Edelstein and Kelly, states that if three finite sets of points satisfy that every line passing through points from two different sets also contains a point from the third set, then, all the points belong to a low dimensional space. This result was further extended to any constant number of sets. The **robust** version, obtained in [3, 9], states that if a finite set of points satisfy that for every point p in the set a δ fraction of the other points satisfy that the line passing through each of them and p spans a third point in the set, then the set is contained in an $O(1/\delta)$-dimensional space.

Although the Sylvester-Gallai theorem is formulated as a geometric question, it can be stated in algebraic terms: If a finite set of pairwise linearly independent vectors, $\mathcal{S} \subset \mathbb{C}^n$, has the property that every two vectors span a third vector in the set then the dimension of $\mathcal{S}$ is at most 3. It is not very hard to see that if we pick a subspace H of codimension 1, which is in general position with respect to the vectors in the set, then the intersection points $p_i = H \cap \operatorname{span}\{s_i\}$, for $s_i \in \mathcal{S}$, satisfy the Sylvester-Gallai condition. Therefore, $\dim(S) \leq 3$. Another formulation is the following: If a finite set of pairwise linearly independent linear forms, $\mathcal{L} \subset \mathbb{C}[x_1, \dots, x_n]$, has the property that for every two forms $\ell_i, \ell_j \in \mathcal{L}$ there is a third form $\ell_k \in \mathcal{L}$, so that whenever ℓ_i and ℓ_j vanish then so does ℓ_k, then the linear dimension of $\mathcal{L}$ is at most 3. To see this note that it must be the case that $\ell_k \in \operatorname{span}\{\ell_i, \ell_j\}$ and thus the coefficient vectors of the forms in the set satisfy the condition for the (vector version of the) Sylvester-Gallai theorem, and the bound on the dimension follows.

The last formulation can now be extended to higher degree polynomials. In particular, the following question was asked by Gupta [17].

▶ **Problem 1.** *Can we bound the linear dimension or algebraic rank of a finite set $\mathcal{P}$ of pairwise linearly independent irreducible polynomials of degree at most r in $\mathbb{C}[x_1, \dots, x_n]$, that has the following property: For any two distinct polynomials $P_1, P_2 \in \mathcal{P}$ there is a third polynomial $P_3 \in \mathcal{P}$, such that whenever P_1, P_2 vanish then so does P_3.*

A robust or colored version of this problem can also be formulated. As we have seen, the case $r = 1$, i.e when all the polynomials are linear forms, follows from the Sylvester-Gallai theorem. For the case of quadratic polynomials, i.e. $r = 2$, [33] gave a bound on the linear dimension for both the non-colored and colored versions. A bound for the robust version is still unknown for $r = 2$ and the entire problem is open for $r \geq 3$. Gupta [17] also raised a more general question of the same form.

▶ **Problem 2.** *Can we bound the linear dimension or algebraic rank of a finite set $\mathcal{P}$ of pairwise linearly independent irreducible polynomials of degree at most r in $\mathbb{C}[x_1, \dots, x_n]$ that has the following property: For any two distinct polynomials $P_1, P_2 \in \mathcal{P}$ there is a subset $\mathcal{I} \subset \mathcal{P}$, such that $P_1, P_2 \notin \mathcal{I}$ and whenever P_1, P_2 vanish then so does $\prod_{P_i \in \mathcal{I}} P_i$.*

As before this problem can also be extended to robust and colored versions. In the case of linear forms, the bound for Problem 1 carries over to Problem 2 as well. This follows from the fact that the ideal generated by linear forms is prime (see Section 2 for definitions). In the case of higher degree polynomials, there is no clear reduction. For example, let $r = 2$ and

$$P_1 = xy + zw \quad , \quad P_2 = xy - zw \quad , \quad P_3 = xw \quad , \quad P_4 = yz.$$

Then, it is not hard to verify that whenever P_1 and P_2 vanish then so does $P_3 \cdot P_4$, but neither P_3 nor P_4 always vanishes when P_1 and P_2 do. The reason is that the radical of the ideal generated by P_1 and P_2 is not prime. Thus it is not clear whether a bound for Problem 1 would imply a bound for Problem 2. The latter problem was open, prior to this work, for any degree $r > 1$.

The Sylvester-Gallai theorem has important consequences for locally decodable and locally correctable codes [3, 9], for reconstruction of certain depth-3 circuits [32, 22, 35] and for the polynomial identity testing (PIT for short) problem, which we describe next.

Sylvester-Gallai type theorems and PIT

The PIT problem asks to give a deterministic algorithm that given an arithmetic circuit as input determines whether it computes the identically zero polynomial. This is a fundamental problem in theoretical computer science that has attracted a lot of attention because of its intrinsic importance, its relation to other derandomization problems [24, 25, 15, 13, 19, 36] and its connections to lower bounds for arithmetic circuits [20, 1, 21, 11, 16, 7]. Perhaps surprisingly, it was shown that deterministic algorithms for the PIT problem for homogeneous depth-4 circuits or for depth-3 circuits would lead to deterministic algorithms for general circuits [2, 18]. This makes small depth circuit extremely interesting for the PIT problem. We next explain how Sylvester-Gallai type questions are directly related to PIT for such low depth circuits. For more on the PIT problem see [34, 28, 29, 14].

The Sylvester-Gallai theorem is mostly relevant for the PIT problem in the setting when the input is a depth-3 circuit with small top fan-in. Specifically, a homogeneous $\Sigma^{[k]}\Pi^{[d]}\Sigma$ circuit in n variables computes a polynomial of the form

$$\Phi(x_1,\ldots,x_n)=\sum_{i=1}^{k}\prod_{j=1}^{d}\ell_{i,j}(x_1,\ldots,x_n)\ , \tag{1}$$

where each $\ell_{i,j}$ is a linear form. Consider the PIT problem for $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuits, i.e., Φ is given as in Equation 1 and $k=3$. In particular,

$$\Phi(x_1,\ldots,x_n)=\prod_{j=1}^{d}\ell_{1,j}(x_1,\ldots,x_n)+\prod_{j=1}^{d}\ell_{2,j}(x_1,\ldots,x_n)+\prod_{j=1}^{d}\ell_{3,j}(x_1,\ldots,x_n)\ . \tag{2}$$

If Φ computes the zero polynomial, then for every $j,j'\in[d]$.

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

This means that the sets $\mathcal{T}_i=\{\ell_{i,1},\ldots,\ell_{i,d}\}$ satisfy the conditions of the colored version of Problem 2 for $r=1$, and therefore have a small linear dimension. Thus, if $\Phi\equiv 0$ then, assuming that no linear form belongs to all three sets, we can rewrite the expression for Φ using only constantly many variables (after a suitable invertible linear transformation). This gives an efficient PIT algorithms for such $\Sigma^{[3]}\Pi^{[d]}\Sigma$ identities. The case of more than three multiplication gates is more complicated but it also satisfies a similar higher dimensional condition. This rank-bound approach for PIT of $\Sigma\Pi\Sigma$ circuits was raised in [10] and later carried out in [23, 31].[2]

As such rank-bounds found important applications in studying PIT of depth-3 circuits it seemed that a similar approach could potentially work for depth-4 $\Sigma\Pi\Sigma\Pi$ circuits as well.[3] In particular, it seemed most relevant for the case where there are only three multiplication

---

[2] The best algorithm for PIT of $\Sigma^{[k]}\Pi^{[d]}\Sigma$ circuits was obtained through a different, yet related, approach in [30].

[3] For multilinear $\Sigma\Pi\Sigma\Pi$ circuits Saraf and Volkovich obtained an analogous bound on the sparsity of the polynomials computed by the multiplication gates in a zero circuit [27].

gates and the bottom fan-in is two, i.e. for homogeneous $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuits that compute polynomials of the form

$$\Phi(x_1,\ldots,x_n) = \prod_{j=1}^{d} Q_{1,j}(x_1,\ldots,x_n) + \prod_{j=1}^{d} Q_{2,j}(x_1,\ldots,x_n) + \prod_{j=1}^{d} Q_{3,j}(x_1,\ldots,x_n)\ . \tag{3}$$

Both Beecken et al. [4] and Gupta [17] suggested an approach to the PIT problem of such identities based on the colored version of Problem 2 for $r = 2$. Both papers described PIT algorithms for depth-4 circuits assuming a bound on the algebraic rank of the polynomials. In fact, Gupta conjectured that the algebraic rank of polynomials satisfying the conditions of Problem 2 depends only on their degree (see Conjectures $1, 2$ and 30 in [17]).

▶ **Conjecture 3** (Conjecture 1 in [17]). *Let $\mathcal{F}_1,\ldots,\mathcal{F}_k$ be finite sets of irreducible homogenous polynomials in $\mathbb{C}[x_1,\ldots,x_n]$ of degree $\leq r$ such that $\cap_i \mathcal{F}_i = \emptyset$ and for every $k-1$ polynomials $Q_1,\ldots,Q_{k-1}$, each from a distinct set, there are $P_1,\ldots,P_c$ in the remaining set such that whenever $Q_1,\ldots,Q_{k-1}$ vanish then also the product $\prod_{i=1}^{c} P_i$ vanishes. Then, trdeg$_{\mathbb{C}}(\cup_i \mathcal{F}_i) \leq \lambda(k,r,c)$ for some function λ, where trdeg stands for the transcendental degree (which is the same as algebraic rank).*

Furthermore, using degree arguments Gupta showed that in Problem 2 we can restrict our attention to sets $\mathcal{I}$ such that $|\mathcal{I}| \leq r^{k-1}$. In particular, if the circuit in Equation (3) vanishes identically, then for every $(j,j') \in [d]^2$ there are $i_{1,j,j'}, i_{2,j,j'}, i_{3,j,j'}, i_{4,j,j'} \in [d]$ so that

$$Q_{1,i_{1,j,j'}} \cdot Q_{1,i_{2,j,j'}} \cdot Q_{1,i_{3,j,j'}} \cdot Q_{1,i_{4,j,j'}} \equiv 0 \mod \langle Q_{2,j}, Q_{3,j'} \rangle\ .$$

In [4] Beecken et al. conjectured that the algebraic rank of simple and minimal $\Sigma^{[k]}\Pi^{[d]}\Sigma\Pi^{[r]}$ circuits (see their paper for definition of simple and minimal) is $O_k(\log d)$. We note that for $k = 3$ this conjecture is weaker than Conjecture 3 as every zero $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[r]}$ circuit gives rise to a structure satisfying the conditions of Conjecture 3, but the other direction is not necessarily true. Beecken et al. also showed how to obtain a deterministic PIT for $\Sigma^{[k]}\Pi^{[d]}\Sigma\Pi^{[r]}$ circuits, assuming the correctness of their conjecture.

1.1 Our Result

Our main result gives a bound on the linear dimension of polynomials satisfying the conditions of Problem 2 when all the polynomials are irreducible of degree at most 2. Specifically we prove the following theorem.

▶ **Theorem 4.** *There exists a universal constant c such that the following holds. Let $\tilde{\mathcal{Q}} = \{Q_i\}_{i\in\{1,\ldots,m\}} \subset \mathbb{C}[x_1,\ldots,x_n]$ be a finite set of pairwise linearly independent homogeneous polynomials, such that every $Q_i \in \tilde{\mathcal{Q}}$ is either irreducible or a square of a linear form. Assume that, for every $i \neq j$, whenever Q_i and Q_j vanish then so does $\prod_{k\in\{1,\ldots,m\}\setminus\{i,j\}} Q_k$. Then, $\dim(\text{span}\{\mathcal{Q}\}) \leq c$.*

While our result still does not resolve Conjecture 3, as we need a colorful version of it, we believe that it is a significant step towards solving the conjecture for $k = 3$ and $r = 2$, which will yield a PIT algorithm for $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuits.

An interesting aspect of our result is that while the conjectures of [4, 17] speak about the algebraic rank we prove a stronger result that bounds that linear dimension (the linear rank is an upper bound on the algebraic rank). As our proof is quite technical it is an interesting question whether one could simplify our arguments by arguing directly about the algebraic rank.

An important algebraic tool in the proof of Theorem 4 is the following result characterizing the different cases in which a product of quadratic polynomials vanishes whenever two other quadratics vanish.

▶ **Theorem 5.** *Let* $\{Q_k\}_{k\in\mathcal{K}}, A, B$ *be homogeneous polynomials of degree* 2 *such that* $\prod_{k\in\mathcal{K}} Q_k \in \sqrt{\langle A, B\rangle}$. *Then one of the following cases hold:*

(i) *There is* $k \in \mathcal{K}$ *such that* Q_k *is in the linear span of* A, B

(ii) *There exists a non trivial linear combination of the form* $\alpha A + \beta B = c \cdot d$ *where* c *and* d *are linear forms.*

(iii) *There exist two linear forms* c *and* d *such that when setting* $c = d = 0$ *we get that* A, B *and one of* $\{Q_k\}_{k\in\mathcal{K}}$ *vanish.*

From now on, to ease notations, we use Theorem 5i, Theorem 5ii or Theorem 5iii to describe different cases of Theorem 5.

The statement of the result is quite similar to Theorem 1.8 of [33] that proved a similar result when $|\mathcal{K}| = 1$. Specifically, in [33] the second item reads “There exists a non trivial linear combination of the form $\alpha A + \beta B = a^2$, where a is a linear form.” This “minor” difference in the statements (which is necessary) is also responsible for the much harder work we do in the paper.

The proof of this theorem can be found in the full version of the paper [26].

1.2 Proof Idea

Our proof has a similar structure to the proofs in [33], but it does not rely on any of the results proved there.

Our starting point is the observation that Theorem 5 guarantees that unless one of $\{Q_k\}$ is in the linear span of A and B then A and B must satisfy a very strong property, namely, they must span a reducible quadratic or they have a very low rank (as quadratic polynomials). The proof of this theorem is based on analyzing the resultant of A and B with respect to some variable. We now explain how this theorem can be used to prove Theorem 4.

Consider a set of polynomials $\mathcal{Q} = \{Q_1, \ldots, Q_m\}$ satisfying the condition of Theorem 4. First, consider the case in which for every $Q \in \mathcal{Q}$, at least, say, $(1/100) \cdot m$ of the polynomials $Q_i \in \mathcal{Q}$, satisfy that there is another polynomial in $\mathcal{Q}$ in $\text{span}\{Q, Q_i\}$. In this case, we can use the robust version of the Sylvester-Gallai theorem [3, 9] (see Theorem 13) to deduce that the linear dimension of $\mathcal{Q}$ is small.

The second case we consider is when every polynomial $Q \in \mathcal{Q}$ that did not satisfy the first case now satisfies that for at least, say, $(1/100) \cdot m$ of the polynomials $Q_i \in \mathcal{Q}$ there are linear forms a_i and b_i such that $Q, Q_i \in \langle a_i, b_i\rangle$. We prove that if this is the case then there is a bounded dimensional linear space of linear forms, V, such that all the polynomials in $\mathcal{Q}$ that are of rank 2 are in $\langle V\rangle$. Then we argue that the polynomials that are not in $\langle V\rangle$ satisfy the robust version of the Sylvester-Gallai theorem (Theorem 13). Finally we bound the dimension of $\mathcal{Q} \cap \langle V\rangle$.

Most of the work however (Section 4) goes into studying what happens in the remaining case when there is some polynomial $Q_o \in \mathcal{Q}$ for which at least $0.98m$ of the other polynomials in $\mathcal{Q}$ satisfy Theorem 5ii with Q_o. This puts a strong restriction on the structure of these $0.98m$ polynomials. Specificity, each of them is of the form $Q_i = Q_o + a_i b_i$, where a_i and b_i are linear forms. The idea in this case is to show that the set $\{a_i, b_i\}$ is of low dimension. This is done by again studying the consequences of Theorem 5 for pairs of polynomials $Q_o + a_i b_i, Q_o + a_j b_j \in \mathcal{Q}$. After bounding the dimension of these $0.98m$ polynomials we bound the dimension of all the polynomials in $\mathcal{Q}$. The proof of this case is much more involved than the cases described earlier, and in particular we handle differently the case where Q_o is of high rank and the case where its rank is low.

1.3 On the relation to the proof of [33]

In [33] the following theorem was proved.

▶ **Theorem 6** (Theorem 1.7 of [33]). *Let* $\{Q_i\}_{i\in[m]}$ *be homogeneous quadratic polynomials over* $\mathbb{C}$ *such that each* Q_i *is either irreducible or a square of a linear function. Assume further that for every* $i \neq j$ *there exists* $k \notin \{i, j\}$ *such that whenever* Q_i *and* Q_j *vanish* Q_k *vanishes as well. Then the linear span of the* Q_i*'s has dimension* $O(1)$*.*

As mentioned earlier, the steps in our proof are similar to the proof of Theorem 1.7 in [33]. Specifically, [33] also relies on an analog of Theorem 5 and divides the proof according to whether all polynomials satisfy the first case above or not. However, the fact that case ii of Theorem 5 is different than the corresponding case in the statement of Theorem 1.8 of [33], makes our proof is significantly more difficult. The reason for this is that while in [33] we could always pinpoint which polynomial vanishes when Q_i and Q_j vanish, here we only know that this polynomial belongs to a small set of polynomials. This leads to a richer structure in Theorem 5 and consequently to a considerably more complicated proof. To understand the effect of this on our proof we note that the corresponding case to Theorem 5ii was the *simpler* case to analyze in the proof of [33]. The fact that $a_i = b_i$ when $|\mathcal{K}| = 1$ almost immediately implied that the dimension of the span of the a_is is constant (see Claim 5.2 in [33]). In our case however, this is the bulk of the proof, and Section 4 is devoted to handling this case.

In addition to being technically more challenging, our proof gives new insights that may be extended to higher degree polynomials. The first is Theorem 5. While a similar theorem was proved for the simpler setting of [33], it was not clear whether a characterization in the form given in Theorem 5 would be possible, let alone true, in our more general setting. This gives hope that a similar result would be true for higher degree polynomials. Our second contribution is that we show (more or less) that either the polynomials in our set satisfy the robust version of Sylvester-Gallai theorem (Definition 12) or the linear functions composing the polynomials satisfy the theorem. Potentially, this may be extended to higher degree polynomials.

2 Preliminaries

In this section we explain our notation and present some basic algebraic preliminaries.

We will use the following notation. Greek letters $\alpha, \beta, \ldots$ denote scalars from $\mathbb{C}$. Non-capitalized letters $a, b, c, \ldots$ denote linear forms and x, y, z denote variables (which are also linear forms). Bold faced letters denote vectors, e.g. $\vec{x} = (x_1, \ldots, x_n)$ denotes a vector of variables, $\vec{\alpha} = (\alpha_1, \ldots, \alpha_n)$ is a vector of scalars, and $\vec{0} = (0, \ldots, 0)$ the zero vector. We sometimes do not use a boldface notation for a point in a vector space if we do not use its structure as vector. Capital letters such as A, Q, P denote quadratic polynomials whereas V, U, W denote linear spaces. Calligraphic letters $\mathcal{I}, \mathcal{J}, \mathcal{F}, \mathcal{Q}, \mathcal{T}$ denote sets. For a positive integer n we denote $[n] = \{1, 2, \ldots, n\}$. For a matrix X we denote by $|X|$ the determinant of X.

A *Commutative Ring* is a group that is abelian with respect to both multiplication and addition operations. We mainly use the multivariate polynomial ring, $\mathbb{C}[x_1, \ldots, x_n]$. An *Ideal* $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ is an abelian subgroup that is closed under multiplication by ring elements. For $\mathcal{S} \subset \mathbb{C}[x_1, \ldots, x_n]$, we denote with $\langle \mathcal{S} \rangle$, the ideal generated by $\mathcal{S}$, that is, the smallest ideal that contains $\mathcal{S}$. For example, for two polynomials Q_1 and Q_2, the ideal $\langle Q_1, Q_2 \rangle$ is the set $\mathbb{C}[x_1, \ldots, x_n]Q_1 + \mathbb{C}[x_1, \ldots, x_n]Q_2$. For a linear subspace V, we have that $\langle V \rangle$ is the ideal generated by any basis of V. The *radical* of an ideal I, denoted by $\sqrt{I}$, is the set of all ring elements, r, satisfying that for some natural number m (that may depend on r), $r^m \in I$. Hilbert's Nullstellensatz implies that, in $\mathbb{C}[x_1,\ldots,x_n]$, if a polynomial Q vanishes whenever Q_1 and Q_2 vanish, then $Q \in \sqrt{\langle Q_1, Q_2\rangle}$ (see e.g. [8]). We shall often use the notation $Q \in \sqrt{\langle Q_1, Q_2\rangle}$ to denote this vanishing condition. For an ideal $I \subseteq \mathbb{C}[x_1,\ldots,x_n]$ we denote by $\mathbb{C}[x_1,\ldots,x_n]/I$ the *quotient ring*, that is, the ring whose elements are the cosets of I in $\mathbb{C}[x_1,\ldots,x_n]$ with the proper multiplication and addition operations. For an ideal $I \subseteq \mathbb{C}[x_1,\ldots,x_n]$ we denote the set of all common zeros of elements of I by $Z(I)$.

For $V_1,\ldots,V_k$ linear spaces, we use $\sum_{i=1}^{k} V_i$ to denote the linear space $V_1 + \ldots + V_k$. For two non zero polynomials A and B we denote $A \sim B$ if $B \in \text{span}\{A\}$. For a space of linear forms $V = \text{span}\{v_1,\ldots,v_\Delta\}$, we say that a polynomial $P \in \mathbb{C}[x_1,\ldots,x_n]$ depends only on V if the value of P is determined by the values of the linear forms $v_1,\ldots,v_\Delta$. More formally, we say that P depends only on V if there is a Δ-variate polynomial $\tilde{P}$ such that $P \equiv \tilde{P}(v_1,\ldots,v_\Delta)$. We denote by $\mathbb{C}[v_1,\ldots,v_\Delta] \subseteq \mathbb{C}[x_1,\ldots,x_n]$ the subring of polynomials that depend only on V.

Another notation that we will use throughout the proof is congruence modulo linear forms.

▶ **Definition 7.** *Let $V \subset \mathbb{C}[x_1,\ldots,x_n]$ be a space of linear forms, and $P, Q \in \mathbb{C}[x_1,\ldots,x_n]$. We say that $P \equiv_V Q$ if $P - Q \in \langle V\rangle$.*

▶ **Fact 8.** *Let $V \subset \mathbb{C}[x_1,\ldots,x_n]$ be a space of linear forms and $P, Q \in \mathbb{C}[x_1,\ldots,x_n]$. If $P = \prod_{k=1}^{t} P_k$, and $Q = \prod_{k=1}^{t} Q_k$ satisfy that for all k, P_k and Q_k are irreducible in $\mathbb{C}[x_1,\ldots,x_n]/\langle V\rangle$, and $P \equiv_V Q \not\equiv_V 0$ then, up to a permutation of the indices, $P_k \equiv_V Q_k$ for all $k \in [t]$.*

This follows from the fact that the quotient ring $\mathbb{C}[x_1,\ldots,x_n]/\langle V\rangle$is a unique factorization domain.

2.1 Sylvester-Gallai Theorem and some of its Variants

In this section we present the formal statement the of Sylvester-Gallai theorem and the extensions that we use in this work.

▶ **Definition 9.** *Given a set of points, $v_1,\ldots,v_m$, we call a line that passes through exactly two of the points of the set an* ordinary line.

▶ **Theorem 10** (Sylvester-Gallai theorem)**.** *If m distinct points $v_1,\ldots,v_m$ in $\mathbb{R}^n$ are not collinear, then they define at least one ordinary line.*

▶ **Theorem 11** (Kelly's theorem)**.** *If m distinct points $v_1,\ldots,v_m$ in $\mathbb{C}^n$ are not coplanar, then they define at least one ordinary line.*

The robust version of the theorem was stated and proved in [3, 9].

▶ **Definition 12.** *We say that a set of points $v_1,\ldots,v_m \in \mathbb{C}^n$ is a δ-SG configuration if for every $i \in [m]$ there exists at least δm values of $j \in [m]$ such that the line through v_i, v_j contains a third point in the set.*

▶ **Theorem 13** (Robust Sylvester-Gallai theorem, Theorem 1.9 of [9])**.** *Let $V = \{v_1,\ldots,v_m\} \subset \mathbb{C}^n$ be a δ-SG configuration. Then* $\dim(\text{span}\{v_1,\ldots,v_m\}) \leq \frac{12}{\delta} + 1$.

The following is the colored version of the Sylvester-Gallai theorem.

▶ **Theorem 14** (Theorem 3 of [12]). *Let $\mathcal{T}_i$, for $i \in [3]$, be disjoint finite subsets of $\mathbb{C}^n$ such that for every $i \neq j$ and any two points $p_1 \in \mathcal{T}_i$ and $p_2 \in \mathcal{T}_j$ there exists a point p_3 in the third set that lies on the line passing through p_1 and p_2. Then, any such $\mathcal{T}_i$ satisfy that* $\dim(\mathrm{span}\{\cup_i \mathcal{T}_i\}) \leq 3$.

We also state the equivalent algebraic versions of Sylvester-Gallai.

▶ **Theorem 15.** *Let $\mathcal{S} = \{\vec{s}_1, \ldots, \vec{s}_m\} \subset \mathbb{C}^n$ be a set of pairwise linearly independent vectors such that for every $i \neq j \in [m]$ there is a distinct $k \in [m]$ for which $\vec{s}_k \in \mathrm{span}\{\vec{s}_i, \vec{s}_j\}$. Then* $\dim(\mathcal{S}) \leq 3$.

▶ **Theorem 16.** *Let $\mathcal{P} = \{\ell_1, \ldots, \ell_m\} \subset \mathbb{C}[x_1, \ldots, x_n]$ be a set of pairwise linearly independent linear forms such that for every $i \neq j \in [m]$ there is a distinct $k \in [m]$ for which whenever ℓ_i, ℓ_j vanish so does ℓ_k. Then* $\dim(\mathcal{P}) \leq 3$.

In this paper we refer to each of Theorem 11, Theorem 15 and Theorem 16 as the Sylvester-Gallai theorem. We shall also refer to sets of points/vectors/linear forms that satisfy the conditions of the relevant theorem as satisfying the condition of the Sylvester-Gallai theorem.

2.2 Resultant

A tool that will play an important role in the proof of Theorem 5 is the resultant of two polynomials. We will only define the resultant of a a quadratic polynomial and a linear polynomial as this is the case relevant to our work.[4] Let $A, B \in \mathbb{C}[x_1, \ldots, x_n]$. View A and B as polynomials in x_1 over $\mathbb{C}[x_2, \ldots, x_n]$ and assume that $\deg_{x_1}(A) = 2$ and $\deg_{x_1}(B) = 1$, namely,

$$A = \alpha x_1^2 + a x_1 + A_0 \quad \text{and } B = b x_1 + B_0 \ .$$

Then, the resultant of A and B with respect to x_1 is the determinant of their Sylvester matrix

$$\mathrm{Res}_{x_1}(A, B) =: \left| \begin{bmatrix} A_0 & B_0 & 0 \\ a & b & B_0 \\ \alpha & 0 & b \end{bmatrix} \right| \ .$$

A useful fact is that if the resultant of A and B vanishes then they share a common factor.

▶ **Theorem 17** (See e.g. Proposition 8 in §5 of Chapter 3 in [8]). *Given $F, G \in \mathbb{F}[x_1, \ldots, x_n]$ of positive degree in x_1, the resultant $Res_{x_1}(F, G)$ is an integer polynomial in the coefficients of F and G. Furthermore, F and G have a common factor in $\mathbb{F}[x_1, \ldots, x_n]$ if and only if $Res_{x_1}(F, G) = 0$.*

2.3 Rank of Quadratic Polynomials

In this section we define the rank of a quadratic polynomial, and present some of its useful properties.

▶ **Definition 18.** *For a homogeneous quadratic polynomial Q we denote with* $\mathrm{rank}_s(Q)$ *the minimal r such that there are $2r$ linear forms $\{a_k\}_{k=1}^{2r}$ satisfying $Q = \sum_{k=1}^{r} a_{2k} \cdot a_{2k-1}$. We call such representation a* minimal representation *of Q.*

---

[4] For the general definition of Resultant, see Definition 2 in §5 of Chapter 3 in [8].

This is a slightly different definition than the usual way one defines rank of quadratic forms,[5] but it is more suitable for our needs. We note that a quadratic Q is irreducible if and only if $\text{rank}_s(Q) > 1$. The next claim shows that a minimal representation is unique in the sense that the space spanned by the linear forms in it is unique.

▷ Claim 19. Let Q be a homogeneous quadratic polynomial and let $Q = \sum_{i=1}^{r} a_{2i-1} \cdot a_{2i}$ and $Q = \sum_{i=1}^{r} b_{2i-1} \cdot b_{2i}$ be two different minimal representations of Q. Then $\text{span}\{a_1, \ldots, a_{2r}\} = \text{span}\{b_1, \ldots, b_{2r}\}$.

Proof. Note that if the statement does not hold then, without loss of generality, a_1 is not contained in the span of the b_i's. This means that when setting $a_1 = 0$ the b_i's are not affected on the one hand, thus Q remains the same function of the b_i's, and in particular $\text{rank}_s(Q|_{a_1=0}) = r$, but on the other hand $\text{rank}_s(Q|_{a_1=0}) = r - 1$ (when considering its representation with the a_i's), in contradiction. ◁

This claim allows us to define the notion of *minimal space* of a quadratic polynomial Q, which we shall denote $\text{Lin}(Q)$.

▶ **Definition 20.** *Let Q be a quadratic polynomial, where $\text{rank}_s(Q) = r$, and let $Q = \sum_{i=1}^{r} a_{2i-1} \cdot a_{2i}$ be some minimal representation of Q. Define $Lin(Q) =: \text{span}\{a_1, \ldots, a_{2r}\}$, also denote $Lin(Q_1, \ldots, Q_k) = \sum_{i=1}^{k} Lin(Q_i)$.*

Claim 19 shows that the minimal space is well defined. The following fact is easy to verify.

▶ **Fact 21.** *Let $Q = \sum_{i=1}^{m} a_{2i-1} \cdot a_{2i}$ be a homogeneous quadratic polynomial, then $Lin(Q) \subseteq \text{span}\{a_1, \ldots, a_{2m}\}$.*

We now give some basic claims regarding rank_s.

▷ Claim 22. Let Q be a homogeneous quadratic polynomial with $\text{rank}_s(Q) = r$, and let $V \subset \mathbb{C}[x_1, \ldots, x_n]$ be a linear space of linear forms such that $\dim(V) = \Delta$. Then $\text{rank}_s(Q|_{V=0}) \geq r - \Delta$.

Proof. Assume without loss of generality $V = \text{span}\{x_1, \ldots, x_\Delta\}$, and consider $Q \in \mathbb{C}[x_{\Delta+1}, \ldots, x_n][x_1, \ldots, x_\Delta]$. There are $a_1, \ldots, a_\Delta \in \mathbb{C}[x_1, \ldots, x_n]$ and $Q' \in \mathbb{C}[x_{\Delta+1}, \ldots, x_n]$ such that $Q = \sum_{i=1}^{\Delta} a_i x_i + Q'$, where $Q|_{V=0} = Q'$. As $\text{rank}_s(\sum_{i=1}^{\Delta} a_i x_i) \leq \Delta$, it must be that $\text{rank}_s(Q|_{V=0}) \geq r - \Delta$. ◁

▷ Claim 23. Let $P_1 \in \mathbb{C}[x_1, \ldots, x_k]$, and $P_2 = y_1 y_2 \in \mathbb{C}[y_1, y_2]$. Then $\text{rank}_s(P_1 + P_2) = \text{rank}_s(P_1) + 1$. Moreover, $y_1, y_2 \in \text{Lin}(P_1 + P_2)$.

Proof. Denote $\text{rank}_s(P_1) = r$ and assume towards a contradiction that there are $a_1, \ldots, a_{2r}$ linear forms in $\mathbb{C}[x_1, \ldots, x_k, y_1, y_2]$ such that $P_1 + P_2 = \sum_{i=1}^{r} a_{2i-1} a_{2i}$. Clearly, $\sum_{i=1}^{r} a_{2i-1} a_{2i} \equiv_{y_1} P_1$. As $\text{rank}_s(P_1) = r$ this is a minimal representation of P_1. Hence, for every i, $a_i|_{y_1=0} \in \text{Lin}(P_1) \subset \mathbb{C}[x_1, \ldots, x_k]$. Moreover, from the minimality of r, $a_i|_{y_1=0} \neq 0$. Therefore, as y_1 and y_2 are linearly independent, we deduce that all the coefficients of y_2 in all the a_i's are 0. By reversing the roles of y_1 and y_2 we can conclude that $a_1, \ldots, a_{2r} \subset \mathbb{C}[x_1, \ldots, x_k]$ which means that Q does not depend on y_1 and y_2 in contradiction. Consider a minimal

---

[5] $\text{rank}_s(Q)$ is the minimal t such that there are t linear forms $\{a_k\}_{k=1}^{t}$, satisfying $Q = \sum_{k=1}^{t} a_k^2$.

representation $P_1 = \sum_{i=1}^{2r} b_{2i-1}b_{2i}$, from the fact that $\text{rank}_s(P_1 + P_2) = r + 1$ it follows that $P_1 + P_2 = \sum_{i=1}^{2r} b_{2i-1}b_{2i} + y_1 y_2$ is a minimal representation of $P_1 + P_2$ and thus $\text{Lin}(P_1 + P_2) = \text{Lin}(P_1) + \text{span}\{y_1, y_2\}$. ◁

▶ **Corollary 24.** *Let a and b be linearly independent linear forms. Then, if c, d, e and f are linear forms such that $ab + cd = ef$ then* $\dim(\text{span}\{a, b\} \cap \text{span}\{c, d\}) \geq 1$.

▷ Claim 25. Let a, b, c and d be linear forms, and V be a linear space of linear forms. Assume $\{0\} \neq \text{Lin}(ab - cd) \subseteq V$ then $\text{span}\{a, b\} \cap V \neq \{0\}$.

Proof. As $\text{Lin}(ab - cd) \subseteq V$ it follows that $ab \equiv_V cd$. If both sides are zero then $ab \in \langle V \rangle$ and without loss of generality $b \in V$ and the statement holds. If neither sides is zero then from Fact 8 there are linear forms $v_1, v_2 \in V$, and $\lambda_1, \lambda_2 \in \mathbb{C}^\times$ such that, $\lambda_1\lambda_2 = 1$ and without loss of generality $c = \lambda_1 a + v_1, d = \lambda_2 b + v_2$. Note that not both v_1, v_2 are zero, as $ab - cd \neq 0$. Thus,

$$ab - cd = ab - (\lambda_1 a + v_1)(\lambda_2 b + v_2) = \lambda_1 a v_2 + \lambda_2 b v_1 + v_1 v_2.$$

As $\text{Lin}(ab - cd) \subseteq V$ it follows that $\text{Lin}(\lambda_1 a v_2 + \lambda_2 b v_1) \subseteq V$ and therefore there is a linear combination of a, b in V and the statement holds. ◁

We end this section with claims that will be useful in our proofs.

▷ Claim 26. Let $V = \sum_{i=1}^{m} V_i$ where V_i are linear subspaces, and for every i, $\dim(V_i) = 2$. If for every $i \neq j \in [m]$, $\dim(V_i \cap V_j) = 1$, then either $\dim(\bigcap_{i=1}^{m} V_i) = 1$ or $\dim(V) = 3$.

Proof. Let $w \in V_1 \cap V_2$. Complete it to basis of V_1 and V_2: $V_1 = \text{span}\{u_1, w\}$ and $V_2 = \text{span}\{u_2, w\}$. Assume that $\dim(\bigcap_{i=1}^{m} V_i) = 0$. Then, there is some i for which $w \notin V_i$. Let $x_1 \in V_i \cap V_1$, and so $x_1 = \alpha_1 u_1 + \beta_1 w$, where $\alpha_1 \neq 0$. Similarly, let $x_2 \in V_i \cap V_2$. Since $w \notin V_i$, $x_2 = \alpha_2 u_2 + \beta_2 w$, where $\alpha_2 \neq 0$. Note that $x_1 \notin \text{span}\{x_2\}$, as $\dim(V_1 \cap V_2) = 1$, and w is already in their intersection. Thus, we have $V_i = \text{span}\{x_1, x_2\} \subset \text{span}\{w, u_1, u_2\}$.

Now, consider any other $j \in [m]$. If V_j does not contain w, we can apply the same argument as we did for V_i and conclude that $V_j \subset \text{span}\{w, u_1, u_2\}$. On the other hand, if $w \in V_j$, then let $x_j \in V_i \cap V_j$, it is easy to see that x_j, w are linearly independent and so $V_j = \text{span}\{w, x_j\} \subset \text{span}\{w, V_i\} \subseteq \text{span}\{w, u_1, u_2\}$. Thus, in any case $V_j \subset \text{span}\{w, u_1, u_2\}$. In particular, $\sum_j V_j \subseteq \text{span}\{w, u_1, u_2\}$ as claimed. ◁

2.4 Projection Mappings

In this section we present and apply a new technique which allows us to simplify the structure of quadratic polynomials. Naively, when we want to simplify a polynomial equation, we can project it on a subset of the variables. Unfortunately, this projection does not necessarily preserve pairwise linear independence, which is a crucial property in our proofs. To remedy this fact, we present a set of mappings, which are somewhat similar to projections, but do preserve pairwise linear independence among polynomials.

▶ **Definition 27.** *Let $V = \text{span}\{v_1, \ldots, v_\Delta\} \subseteq \text{span}\{x_1, \ldots, x_n\}$ be a Δ-dimensional linear space of linear forms, and let $\{u_1, \ldots, u_{n-\Delta}\}$ be a basis for $V^\perp$. For $\vec{\alpha} = (\alpha_1, \ldots, \alpha_\Delta) \in \mathbb{C}^\Delta$ we define $T_{\vec{\alpha},V} : \mathbb{C}[x_1, \ldots, x_n] \mapsto \mathbb{C}[x_1, \ldots, x_n, z]$, where z is a new variable, to be the linear map given by the following action on the basis vectors: $T_{\vec{\alpha},V}(v_i) = \alpha_i z$ and $T_{\vec{\alpha},V}(u_i) = u_i$.*

▶ **Observation 28.** *$T_{\vec{\alpha},V}$ is a linear transformation and is also a ring homomorphism. This follows from the fact that a basis for* $\text{span}\{x_1, \ldots, x_n\}$ *is a basis for $\mathbb{C}[x_1, \ldots, x_n]$ as $\mathbb{C}$-algebra.*

▷ Claim 29. Let $V \subseteq \text{span}\{x_1, \ldots, x_n\}$ be a Δ-dimensional linear space of linear forms. Let F and G be two polynomials that share no common irreducible factor. Then, with probability 1 over the choice of $\vec{\alpha} \in [0,1]^\Delta$ (say according to the uniform distribution), $T_{\vec{\alpha},V}(F)$ and $T_{\vec{\alpha},V}(G)$ do not share a common factor that is not a polynomial in z.

Proof. Let $\{u_1, \ldots, u_{n-\Delta}\}$ be a basis for $V^\perp$. We think of F and G as polynomials in $\mathbb{C}[v_1, \ldots, v_\Delta, u_1, \ldots, u_{n-\Delta}]$. As $T_{\vec{\alpha},V} : \mathbb{C}[v_1, \ldots, v_\Delta, u_1, \ldots, u_{n-\Delta}] \to \mathbb{C}[z, u_1, \ldots, u_{n-\Delta}]$, Theorem 17 implies that if $T_{\vec{\alpha},V}(F)$ and $T_{\vec{\alpha},V}(G)$ share a common factor that is not a polynomial in z, then, without loss of generality, their resultant with respect to u_1 is zero. Theorem 17 also implies that the resultant of F and G with respect to u_1 is not zero. Observe that with probability 1 over the choice of $\vec{\alpha}$, we have that $\deg_{u_1}(F) = \deg_{u_1}(T_{\vec{\alpha},V}(F))$ and $\deg_{u_1}(G) = \deg_{u_1}(T_{\vec{\alpha},V}(G))$. As $T_{\vec{\alpha},V}$ is a ring homomorphism this implies that $Res_{u_1}(T_{\vec{\alpha},V}(G), T_{\vec{\alpha},V}(F)) = T_{\vec{\alpha},V}(Res_{u_1}(G,F))$. The Schwartz-Zippel-DeMillo-Lipton lemma now implies that sending each basis element of V to a random multiple of z, chosen uniformly from $(0,1)$ will keep the resultant non zero with probability 1. This also means that $T_{\vec{\alpha},V}(F)$ and $T_{\vec{\alpha},V}(G)$ share no common factor. ◁

▶ **Corollary 30.** *Let V be a Δ-dimensional linear space of linear forms. Let F and G be two linearly independent, irreducible quadratics, such that $Lin(F), Lin(G) \not\subseteq V$. Then, with probability 1 over the choice of $\vec{\alpha} \in [0,1]^\Delta$ (say according to the uniform distribution), $T_{\vec{\alpha},V}(F)$ and $T_{\vec{\alpha},V}(G)$ are linearly independent.*

Proof. As F and G are irreducible they share no common factors. Claim 29 implies that $T_{\vec{\alpha},V}(F)$ and $T_{\vec{\alpha},V}(G)$ do not share a common factor that is not a polynomial in z. The Schwartz-Zippel-DeMillo-Lipton implies that with probability 1, $T_{\vec{\alpha},V}(F)$ and $T_{\vec{\alpha},V}(G)$ are not polynomials in z, and therefore they are linearly independent. ◀

▷ Claim 31. Let Q be an irreducible quadratic polynomial, and V a Δ-dimensional linear space. Then for every $\vec{\alpha} \in \mathbb{C}^\Delta$, $\text{rank}_\text{s}(T_{\vec{\alpha},V}(Q)) \geq \text{rank}_\text{s}(Q) - \Delta$.

Proof. $\text{rank}_\text{s}(T_{\vec{\alpha},V}(Q)) \geq \text{rank}_\text{s}(T_{\vec{\alpha},V}(Q)|_{z=0}) = \text{rank}_\text{s}(Q|_{V=0}) \geq \text{rank}_\text{s}(Q) - \Delta$, where the last inequality follows from Claim 22. ◁

▷ Claim 32. Let $\mathcal{Q}$ be a set of quadratics, and V be a Δ-dimensional linear space. Then, if there are linearly independent vectors, $\{\vec{\alpha}^1, \ldots, \vec{\alpha}^\Delta\} \subset \mathbb{C}^\Delta$, such that, for every i,[6] $\dim(\text{Lin}(T_{\vec{\alpha}^i,V}(\mathcal{Q}))) \leq \sigma$ then $\dim(\text{Lin}(\mathcal{Q})) \leq (\sigma+1)\Delta$.

Proof. As $\dim(\text{Lin}(T_{\vec{\alpha}^i,V}(\mathcal{Q}))) \leq \sigma$, there are ${u^i}_1, \ldots, {u^i}_\sigma \subset V^\perp$ such that $\text{Lin}(T_{\vec{\alpha}^i,V}(\mathcal{Q})) \subseteq \text{span}\{z, {u^i}_1, \ldots, {u^i}_\sigma\}$. We will show that $\text{Lin}(\mathcal{Q}) \subset V + \text{span}\{\{{u^i}_1, \ldots, {u^i}_\sigma\}_{i=1}^\Delta\}$, which is of dimension at most $\Delta + \sigma\Delta$.

Let $P \in \mathcal{Q}$, then there are linear forms, $a_1, \ldots, a_\Delta \subset V^\perp$ and polynomials $P_V \in \mathbb{C}[V]$ and $P' \in \mathbb{C}[V^\perp]$, such that

$$P = P_V + \sum_{j=1}^{\Delta} a_j v_j + P'.$$

---

[6] Recall that $\text{Lin}(T_{\vec{\alpha}^i,V}(\mathcal{Q}))$ is the space spanned by $\cup_{Q\in\mathcal{Q}}\text{Lin}(T_{\vec{\alpha}^i,V}(\mathcal{Q}))$.

Therefore, after taking the projection for a specific $T_{\vec{\alpha}^i,V}$, for some $\gamma \in \mathbb{C}$,

$$T_{\vec{\alpha}^i,V}(P) = \gamma z^2 + \left(\sum_{j=1}^{\Delta} \alpha^i_j a_j\right) z + P'.$$

Denote $b_{P,i} = \sum\limits_{j=1}^{\Delta} \alpha^i_j a_j$. By Corollary 30 if $a_1, \ldots, a_\Delta$ are not all zeros, then, with probability 1, $b_{P,i} \neq \vec{0}$.

If $b_{P,i} \notin \mathrm{Lin}(P')$ then from Claim 23 it follows that $\{z, b_{P,i}, \mathrm{Lin}(P')\} \subseteq \mathrm{span}\{\mathrm{Lin}(T_{\vec{\alpha}^i,V}(P))\}$. If, on the other hand, $b_{P,i} \in \mathrm{Lin}(P')$, then clearly $\{b_{P,i}, \mathrm{Lin}(P')\} \subseteq \mathrm{span}\{z, \mathrm{Lin}(T_{\vec{\alpha}^i,V}(P))\}$. To conclude, in either case, $\{b_{P,i}, \mathrm{Lin}(P')\} \subseteq \mathrm{span}\{z, {u^i}_1, \ldots, {u^i}_\sigma\}$.

Applying the analysis above to $T_{\vec{\alpha}^1,V}, \ldots, T_{\vec{\alpha}^\Delta,V}$ we obtain that $\mathrm{span}\{b_{P,1}, \cdots b_{P,\Delta}\} \subseteq \mathrm{span}\{\{{u^i}_1, \ldots, {u^i}_\sigma\}_{i=1}^{\Delta}\}$. As $\vec{\alpha}^1, \ldots \vec{\alpha}^\Delta$ are linearly independent, we have that $\{a_1, \ldots, a_\Delta\} \subset \mathrm{span}\{b_{P,1}, \cdots b_{P,\Delta}\}$, and thus $\mathrm{Lin}(P) \subseteq V + \{a_1, \ldots, a_\Delta\} + LS(P') \subseteq V + \mathrm{span}\{\{{u^i}_1, \ldots, {u^i}_\sigma\}_{i=1}^{\Delta}\}$. ◁

3 Sylvester-Gallai theorem for quadratic polynomials

In this section we prove Theorem 4. For convenience we repeat the statement of the theorem.

▶ **Theorem** (Theorem 4). *There exists a universal constant c such that the following holds. Let $\tilde{\mathcal{Q}} = \{Q_i\}_{i\in\{1,\ldots,m\}} \subset \mathbb{C}[x_1, \ldots, x_n]$ be a finite set of pairwise linearly independent homogeneous polynomials, such that every $Q_i \in \tilde{\mathcal{Q}}$ is either irreducible or a square of a linear form. Assume that, for every $i \neq j$, whenever Q_i and Q_j vanish then so does $\prod_{k\in\{1,\ldots,m\}\setminus\{i,j\}} Q_k$. Then, $\dim(\mathrm{span}\{\mathcal{Q}\}) \leq c$.*

▶ Remark 33. The requirement that the polynomials are homogeneous is not essential as homogenization does not affect the property $Q_k \in \sqrt{\langle Q_i, Q_j\rangle}$.

▶ Remark 34. Note that we no longer demand that the polynomials are irreducible but rather allow some of them to be square of linear forms, but now we restrict all polynomials to be of degree exactly 2. Note that both versions of the theorem are equivalent, as this modification does not affect the vanishing condition.

We use the following claim of [17].

▷ Claim 35 (Claim 11 in [17]). Let $P_1, \ldots, P_d, Q_1, \ldots, Q_k \in \mathbb{C}[x_1, \ldots, x_n]$ be homogeneous and the degree of each P_i is at most r. Then,

$$\prod_{i=1}^{k} Q_i \in \sqrt{\langle P_1, \ldots, P_d\rangle} \Rightarrow \exists\{i_1, \ldots, i_{r^d}\} \subset [k] \text{ such that } \prod_{j=1}^{r^d} Q_{i_j} \in \sqrt{\langle P_1, \ldots, P_d\rangle}\ .$$

▶ Remark 36. Note that from Claim 35 for $r = d = 2$, it follows that for every $i \neq j$ there exists a subset $\mathcal{K} \subseteq [m] \setminus \{i, j\}$ such that $|\mathcal{K}| \leq 4$ and whenever Q_i and Q_j vanish then so does $\prod_{k\in\mathcal{K}} Q_k$.

In what follows we shall use the following terminology. Whenever we say that two quadratics $Q_1, Q_2 \in \tilde{\mathcal{Q}}$ satisfy Theorem 5i we mean that there is a polynomial $Q_3 \in \tilde{\mathcal{Q}} \setminus \{Q_1, Q_2\}$ in their linear span. Similarly, when we say that they satisfy Theorem 5ii (Theorem 5iii) we mean that there is a reducible quadratic in their linear span (they belong to $\langle a_1, a_2\rangle$ for linear forms a_1, a_2).

Proof of Theorem 4. Partition the polynomials to two sets. Let $\mathcal{L}$ be the set of all squares and let $\mathcal{Q}$ be the subset of irreducible quadratics, thus $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$. Denote $|\mathcal{Q}| = m$, $|\mathcal{L}| = r$. Let $\delta = \frac{1}{100}$, and denote

- $\mathcal{P}_1 = \{P \in \mathcal{Q} \mid$ There are at least δm polynomials in $\mathcal{Q}$ such that P satisfies Theorem 5i but not Theorem 5ii with each of them$\}$.
- $\mathcal{P}_3 = \{P \in \mathcal{Q} \mid$ There are at least δm polynomials in $\mathcal{Q}$ such that P satisfies Theorem 5iii with each of them$\}$.

The proof first deals with the case where $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_3$. We then handle the case that there is $Q \in \mathcal{Q} \setminus (\mathcal{P}_1 \cup \mathcal{P}_3)$.

3.1 The case $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_3$

Assume that $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_3$. For our purposes, we may further assume that $\mathcal{P}_1 \cap \mathcal{P}_3 = \emptyset$, by letting $\mathcal{P}_1 = \mathcal{P}_1 \setminus \mathcal{P}_3$.

▷ Claim 37. There exists a linear space of linear forms, V, such that $\dim(V) = O(1)$ and $\mathcal{P}_3 \subset \langle V \rangle$.

The intuition behind the claim is based on the following observation.

▶ **Observation 38.** *If $Q_1, Q_2 \in \mathcal{Q}$ satisfy Theorem 5iii then $\dim(Lin(Q_1)), \dim(Lin(Q_2)) \leq 4$ and $\dim(Lin(Q_1) \cap Lin(Q_2)) \geq 2$.*

Thus, we have many small dimensional spaces that have large pairwise intersections and we can therefore expect that such a V may exist.

Proof. We prove the existence of V by explicitly constructing it. Repeat the following process: Set $V = \{\vec{0}\}$, and $\mathcal{P}'_3 = \emptyset$. At each step consider any $Q \in \mathcal{P}_3$ such that $Q \notin \langle V \rangle$ and set $V = \mathrm{Lin}(Q) + V$, and $\mathcal{P}'_3 = \mathcal{P}'_3 \cup \{Q\}$. Repeat this process as long as possible, i.e, as long as $\mathcal{P}_3 \not\subseteq \langle V \rangle$. We show next that this process must end after at most $\frac{3}{\delta}$ steps. In particular, $|\mathcal{P}'_3| \leq \frac{3}{\delta}$. It is clear that at the end of the process it holds that $\mathcal{P}_3 \subset \langle V \rangle$.

▷ Claim 39. Let $Q \in \mathcal{Q}$ and $\mathcal{B} \subseteq \mathcal{P}'_3$ be the subset of all polynomials in $\mathcal{P}'_3$ that satisfy Theorem 5iii with $\mathcal{Q}$, then $|\mathcal{B}| \leq 3$.

Proof. Assume towards a contradiction that $|\mathcal{B}| \geq 4$, and that Q_1, Q_2, Q_3 and Q_4 are the first 4 elements of $\mathcal{B}$ that where added to $\mathcal{P}'_3$. Denote $U = \mathrm{Lin}(Q)$, and $U_i = U \cap \mathrm{Lin}(Q_i)$, for $1 \leq i \leq 4$.

As Q satisfies Theorem 5iii we have that $\dim(U) \leq 4$. Furthermore, for every i, $\dim(U_i) \geq 2$ (by Observation 38). As the Q_is were picked by the iterative process, we have that $U_2 \not\subseteq U_1$. Indeed, since $Q_2 \in \langle U_2 \rangle$, if we had $U_2 \subseteq U_1 \subseteq \mathrm{Lin}(Q_1) \subseteq V$, then this would imply that $Q_2 \in \langle V \rangle$, in contradiction to the fact that $Q_2 \in \mathcal{P}'_3$. Similarly we get that $U_3 \not\subseteq U_1 + U_2$ and $U_4 \not\subseteq U_1 + U_3 + U_3$. However, as the next simple lemma shows, this is not possible.

▶ **Lemma 40.** *Let V be a linear space of dimension ≤ 4, and let $V_1, V_2, V_3 \subset V$ each of dimension ≥ 2, such that $V_1 \not\subseteq V_2$ and $V_3 \not\subseteq V_2 + V_1$ then $V = V_1 + V_2 + V_3$.*

Proof. As $V_1 \not\subseteq V_2$ we have that $\dim(V_1 + V_2) \geq 3$. Similarly we get $4 \leq \dim(V_1 + V_2 + V_3) \leq \dim(V) = 4$. ◀

Thus, Lemma 40 implies that $V = U_1 + U_2 + U_3$ and in particular, $U_4 \subseteq U_1 + U_2 + U_3$ in contradiction. This completes the proof of Claim 39. ◁

For $Q_i \in \mathcal{P}_3'$, define $T_i = \{Q \in \mathcal{Q} \mid Q, Q_i \text{ satisfiy Theorem 5iii}\}$. Since $|T_i| \geq \delta m$, and as by Claim 39 each $Q \in \mathcal{Q}$ belongs to at most 3 different sets, it follows by double counting that $|\mathcal{P}_3'| \leq 3/\delta$. As in each step we add at most 4 linearly independent linear forms to V, we obtain $\dim(V) \leq \frac{12}{\delta}$.

This completes the proof of Claim 37. ◀

So far V satisfies that $\mathcal{P}_3 \subset \langle V \rangle$. Next, we find a small set of polynomials $\mathcal{I}$ such that $\mathcal{Q} \subset \langle V \rangle + \operatorname{span}\{\mathcal{I}\}$.

▷ Claim 41. There exists a set $\mathcal{I} \subset \mathcal{Q}$ such that $\mathcal{Q} \subset \langle V \rangle + \operatorname{span}\{\mathcal{I}\}$ and $|\mathcal{I}| = O(1/\delta)$.

Proof. As before the proof shows how to construct $\mathcal{I}$ by an iterative process. Set $\mathcal{I} = \emptyset$ and $\mathcal{B} = \mathcal{P}_3$. First add to $\mathcal{B}$ any polynomial from $\mathcal{P}_1$ that is in $\langle V \rangle$. Observe that at this point we have that $\mathcal{B} \subset \mathcal{Q} \cap \langle V \rangle$. We now describe another iterative process for the polynomials in $\mathcal{P}_1$. In each step pick any $P \in \mathcal{P}_1 \setminus \mathcal{B}$ such that P satisfies Theorem 5i, but not Theorem 5ii,[7] with at least $\frac{\delta}{3}m$ polynomials in $\mathcal{B}$, and add it to both $\mathcal{I}$ and to $\mathcal{B}$. Then, we add to $\mathcal{B}$ all the polynomials $P' \in \mathcal{P}_1$ that satisfy $P' \in \operatorname{span}\{(\mathcal{Q} \cap \langle V \rangle) \cup \mathcal{I}\}$. Note, that we always maintain that $\mathcal{B} \subset \operatorname{span}\{(\mathcal{Q} \cap \langle V \rangle) \cup \mathcal{I}\}$.

We continue this process as long as we can. Next, we prove that at the end of the process we have that $|\mathcal{I}| \leq 3/\delta$.

▷ Claim 42. In each step we added to $\mathcal{B}$ at least $\frac{\delta}{3}m$ new polynomials from $\mathcal{P}_1$. In particular, $|\mathcal{I}| \leq 3/\delta$.

Proof. Consider what happens when we add some polynomial P to $\mathcal{I}$. By the description of our process, P satisfies Theorem 5i with at least $\frac{\delta}{3}m$ polynomials in $\mathcal{B}$. Any $Q \in \mathcal{B}$, that satisfies Theorem 5i with P, must span with P a polynomial $P' \in \tilde{\mathcal{Q}}$. Observe that $P' \notin \mathcal{L}$ as Q, P do not satisfy Theorem 5ii, and thus $P' \in \mathcal{Q}$. It follows that $P' \in \mathcal{P}_1$ since otherwise we would have that $P \in \operatorname{span}\{\mathcal{B}\} \subset \operatorname{span}\{(\mathcal{Q} \cap \langle V \rangle) \cup \mathcal{I}\}$, which implies $P \in \mathcal{B}$ in contradiction to the way that we defined the process. Furthermore, for each such $Q \in \mathcal{B}$ the polynomial P' is unique. Indeed, if there was a $P \neq P' \in \mathcal{P}_1$ and $Q_1, Q_2 \in \mathcal{B}$ such that $P' \in \operatorname{span}\{Q_1, P\} \cap \operatorname{span}\{Q_2, P\}$ then by pairwise independence we would conclude that $P \in \operatorname{span}\{Q_1, Q_2\} \subset \operatorname{span}\{\mathcal{B}\}$, which, as we already showed, implies $P \in \mathcal{B}$ in contradiction. Thus, when we add P to $\mathcal{I}$ we add at least $\frac{\delta}{3}m$ polynomials to $\mathcal{B}$. In particular, the process terminates after at most $3/\delta$ steps and thus $|\mathcal{I}| \leq 3/\delta$. ◁

Consider the polynomials left in $\mathcal{P}_1 \setminus \mathcal{B}$. As they "survived" the process, each of them satisfies the condition in the definition of $\mathcal{P}_1$ with at most $\frac{\delta}{3}m$ polynomials in $\mathcal{B}$. From the fact that $\mathcal{P}_3 \subseteq \mathcal{B}$ and the uniqueness property we obtained in the proof of Claim 42, we get that $\mathcal{P}_1 \setminus \mathcal{B}$ satisfies the conditions of Definition 12 with parameter $\delta/3$ and thus, Theorem 13 implies that $\dim(\mathcal{P}_1 \setminus \mathcal{B}) \leq O(1/\delta)$. Adding a basis of $\mathcal{P}_1 \setminus \mathcal{B}$ to $\mathcal{I}$ we get that $|\mathcal{I}| = O(1/\delta)$ and every polynomial in $\mathcal{Q}$ is in $\operatorname{span}\{(\mathcal{Q} \cap \langle V \rangle) \cup \mathcal{I}\}$. ◁

We are not done yet as the dimension of $\langle V \rangle$, as a vector space, is not a constant. Nevertheless, we next show how to use Sylvester-Gallai theorem to bound the dimension of $\mathcal{Q}$ given that $\mathcal{Q} \subset \operatorname{span}\{(\mathcal{Q} \cap \langle V \rangle) \cup \mathcal{I}\}$. To achieve this we introduce yet another iterative process: For each $P \in \mathcal{Q} \setminus \langle V \rangle$, if there is quadratic L, with $\operatorname{rank_s}(L) \leq 2$, such that $P + L \in \langle V \rangle$, then we set $V = V + \operatorname{Lin}(L)$ (this increases the dimension of V by at most 4). Since this operation increases $\dim(\langle V \rangle \cap \mathcal{Q})$ we can remove one polynomial from $\mathcal{I}$, and thus decrease its size by 1, and still maintain the property that $\mathcal{Q} \subset \operatorname{span}\{(\mathcal{Q} \cap \langle V \rangle) \cup \mathcal{I}\}$.

---

[7] By this we mean that there are many polynomials that together with P span another polynomial in $\mathcal{Q}$ but not in $\mathcal{L}$.

We repeat this process until either $\mathcal{I}$ is empty, or none of the polynomials in $\mathcal{I}$ satisfies the condition of the process. By the upper bound on $|\mathcal{I}|$ the dimension of V grew by at most $4|\mathcal{I}| = O(1/\delta)$ and thus it remains of dimension $O(1/\delta) = O(1)$. At the end of the process we have that $\mathcal{Q} \subset \text{span}\{(\mathcal{Q} \cap \langle V\rangle) \cup \mathcal{I}\}$ and that every polynomial in $P \in \mathcal{Q} \setminus \langle V\rangle$ has $\text{rank}_s(P) > 2$, even if we set all linear forms in V to zero.

Consider the map $T_{\vec{\alpha},V}$ as given in Definition 27, for a randomly chosen $\vec{\alpha} \in [0,1]^{\dim(V)}$. Each polynomial in $\mathcal{Q} \cap \langle V\rangle$ is mapped to a polynomial of the form form zb, for some linear form b. From Claim 22, it follows that every polynomial in $\mathcal{Q} \setminus \langle V\rangle$ still has rank larger than 2 after the mapping. Let

$$\mathcal{A} = \{b \mid \text{ some polynomial in } \mathcal{Q} \cap \langle V\rangle \text{ was mapped to } zb\} \cup T_{\vec{\alpha},V}(\mathcal{L}) \ .$$

We now show that, modulo z, $\mathcal{A}$ satisfies the conditions of Sylvester-Gallai theorem. Let $b_1, b_2 \in \mathcal{A}$ such that $b_1 \notin \text{span}\{z\}$ and $b_2 \notin \text{span}\{z, b_1\}$. As $\tilde{\mathcal{Q}}$ satisfies the conditions of Theorem 4 we get that there are polynomials $Q_1, \ldots, Q_4 \in \tilde{\mathcal{Q}}$ such that $\prod_{i=1}^{4} T_{\vec{\alpha},V}(Q_i) \in \sqrt{\langle b_1, b_2\rangle} = \langle b_1, b_2\rangle$, where the equality holds as $\langle b_1, b_2\rangle$ is a prime ideal. This fact also implies that, without loss of generality, $T_{\vec{\alpha},V}(Q_4) \in \langle b_1, b_2\rangle$. Thus, $T_{\vec{\alpha},V}(Q_4)$ has rank at most 2 and therefore $Q_4 \in \mathcal{L} \cup (\mathcal{Q} \cap \langle V\rangle)$. Hence, $T_{\vec{\alpha},V}(Q_4)$ was mapped to zb_4 or to b_4^2. In particular, $b_4 \in \mathcal{A}$. Claim 29 and Corollary 30 imply that b_4 is neither a multiple of b_1 nor a multiple of b_2, so it must hold that b_4 depends non-trivially on both b_1 and b_2. Thus, $\mathcal{A}$ satisfies the conditions of Sylvester-Gallai theorem modulo z. It follows that $\dim(\mathcal{A}) = O(1)$.

The argument above shows that the dimension of $T_{\vec{\alpha},V}(\mathcal{L} \cup (\mathcal{Q} \cap \langle V\rangle)) = O(1)$. Claim 32 implies that if we denote $U = \text{span}\{\mathcal{L} \cup \text{Lin}(\mathcal{Q} \cap \langle V\rangle)\}$ then $\dim(U)$ is $O(1)$. As $\mathcal{Q} \subseteq \text{span}\{(\mathcal{Q} \cap \langle V\rangle) \cup \mathcal{I}\}$, we obtain that $\dim(\tilde{\mathcal{Q}}) = \dim(\mathcal{L} \cup \mathcal{Q}) = O(1)$, as we wanted to show.

This completes the proof of Theorem 4 for the case $\mathcal{Q} = \mathcal{P}_1 \cup \mathcal{P}_3$.

3.2 The case $\mathcal{Q} \neq \mathcal{P}_1 \cup \mathcal{P}_3$

In this case there is some polynomial $Q_o \in \mathcal{Q} \setminus (\mathcal{P}_1 \cup \mathcal{P}_3)$. In particular, Q_0 satisfies Theorem 5ii with at least $(1-2\delta)m$ of the polynomials in $\mathcal{Q}$; of the remaining polynomials, at most δm satisfy Theorem 5i with Q_o; and, Q_o satisfies Theorem 5iii with at most δm polynomials. Let

- $\mathcal{Q}_1 = \{P \in \mathcal{Q} \mid P, Q_o \text{ satisfiy Theorem 5ii }\} \cup \{Q_o\}$
- $\mathcal{Q}_2 = \{P \in \mathcal{Q} \mid P, Q_o \text{ do not satisfiy Theorem 5ii }\}$
- $m_1 = |\mathcal{Q}_1|$, $m_2 = |\mathcal{Q}_2|$.

As $Q_o \notin \mathcal{P}_1 \cup \mathcal{P}_3$ we have that $m_2 \le 2\delta m$ and $m_1 \ge (1-2\delta)m$. These properties of Q_o and $\mathcal{Q}$ are captured by the following definition.

▶ **Definition 43.** *Let $\mathcal{Q}_1 = \{Q_o, Q_1, \ldots, Q_{m_1}\}$ and $\mathcal{Q}_2 = \{P_1, \ldots, P_{m_2}\}$ be sets of irreducible homogeneous quadratic polynomials. Let $\mathcal{L} = \{\ell^2{}_1, \ldots, \ell^2{}_r\}$ be a set of squares of homogeneous linear forms. We say that $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$ where $\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$ is a (Q_o, m_1, m_2)-set if it satisfies the following:*

1. *$\tilde{\mathcal{Q}}$ satisfy the conditions in the statement of Theorem 4.*
2. $m_1 > 5m_2 + 2$.
3. *For every $j \in [m_1]$, there are linear forms a_j, b_j such that $Q_j = Q_o + a_j b_j$.*
4. *For every $i \in [m_2]$, every non-trivial linear combination of P_i and Q_o has rank at least 2.*
5. *At most m_2 of the polynomials in $\mathcal{Q}$ satisfy Theorem 5iii with Q_o.*

By the discussion above, the following theorem is what we need in order to complete the proof for the case $\mathcal{Q} \neq \mathcal{P}_1 \cup \mathcal{P}_3$.

▶ **Theorem 44.** *Let $\tilde{\mathcal{Q}}$ satisfy the conditions of Definition 43, then $\dim \tilde{\mathcal{Q}} = O(1)$.*

We prove this theorem in Section 4. This concludes the proof of Theorem 17. ◀

4 Proof of Theorem 44

In this section we prove Theorem 44. The proof is divided to two parts according to whether the polynomial Q_o in Definition 43 is of high rank (Claim 46) or of low rank (Claim 60). Each part is also divided to two – first we consider what happens when $m_2 = 0$ and then the general case where $m_2 \neq 0$. The reason for this split is that when Q_o is of high rank then we know, e.g., that it cannot satisfy Theorem 5iii with any other polynomial. Similarly any polynomial satisfying Theorem 5ii with Q_o is also of high rank and cannot satisfy Theorem 5iii with any other polynomial. The reason why we further break the argument to weather $m_2 = 0$ or not, is that when $m_2 = 0$ all the polynomials are of the form $Q_o + ab$ for some linear forms a, b, which means we have fewer cases to analyse. While this seems a bit restrictive, the general case is not much harder and most of the ideas there already appear in the case $m_2 = 0$.

Throughout the proof we use the notation of Definition 43. In particular, each $Q_i \in \mathcal{Q}_1$ is of the form $Q_i = Q_o + a_i b_i$.

4.1 Q_o is of high rank

In this subsection we assume that $\tilde{\mathcal{Q}}$ is a (Q_o, m_1, m_2)-set for some quadratic Q_o of rank at least 100, this constant is arbitrary, as we just need it to be large enough. The following observation says that for our set $\mathcal{Q}$ we will never have to consider Theorem 5iii.

▶ **Observation 45.** *For $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$ that satisfy Definition 43 with $\text{rank}_s(Q_o) \geq 100$, for every $j \in [m_1]$ the rank of Q_j is at least $100 - 1 > 2$ and so Q_j never satisfies Theorem 5iii with any other polynomial in $\tilde{\mathcal{Q}}$.*

Our goal in this subsection is to prove the next claim.

▷ Claim 46. Let $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$ be a (Q_o, m_1, m_2)-set with $\text{rank}_s(Q_o) \geq 100$. Then $\dim(\text{span}\{\tilde{\mathcal{Q}}\}) = O(1)$.

We break the proof of Claim 46 to two steps. First we handle the case $m_2 = 0$ and then the case $m_2 \neq 0$.

4.1.1 The case $m_2 = 0$

In this subsection we prove the following version of Claim 46 for the case $m_2 = 0$.

▷ Claim 47. Let $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$ be a $(Q_o, m_1, 0)$-set with $\text{rank}_s(Q_o) \geq 100$. Then, for a_i, b_i, ℓ_j as in Definition 43, $\dim(\text{span}\{a_1, \ldots, a_{m_1}, b_1, \ldots, b_{m_1}, \ell_1, \ldots, \ell_r\}) \leq 7$. In particular, $\dim(\text{span}\{\mathcal{Q}\}) \leq 8$.

We first show some properties satisfied by the products $\{a_1 b_1, \ldots, a_{m_1} b_{m_1}\}$.

▶ Remark 48. For $\ell_i^2 \in \mathcal{L}$ we can write $\ell_i^2 = 0 \cdot Q_o + \ell_i \ell_i$. Thus, from now on we can assume that every $Q_i \in \tilde{\mathcal{Q}}$ is of the form $Q_i = \alpha_i Q_o + a_i b_i$, for $\alpha_i \in \{0, 1\}$, and when $\alpha_i = 0$ it holds that $a_i = b_i$. We shall use the convention that for $i \in \{m_1 + 1, \ldots, m_1 + r\}$, $a_i = \ell_{i-m_1}$.

▷ Claim 49. Let $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$ be a $(Q_o, m_1, 0)$-set with $\text{rank}_s(Q_o) \geq 100$, and let $Q_i = Q_o + a_i b_i$ and $Q_j = Q_o + a_j b_j$ be polynomials in $\mathcal{Q} = \mathcal{Q}_1$.

1. If Q_i and Q_j satisfy Theorem 5i then there exists $k \in [m_1 + r]$ such that for some $\alpha, \beta \in \mathbb{C} \setminus \{0\}$

$$\alpha a_i b_i + \beta a_j b_j = a_k b_k. \tag{4}$$

2. If Q_i and Q_j satisfy Theorem 5ii then there exist two linear forms, c and d such that

$$a_ib_i - a_jb_j = cd. \tag{5}$$

The claim only considers Theorem 5i and Theorem 5ii as by Observation 45 we know that Q_i, Q_j do not satisfy Theorem 5iii. Note that the guarantee of this claim is not sufficient to conclude that the dimension of $a_1, \dots, a_{m_1}, b_1, \dots, b_{m_1}$ is bounded. The reason is that c and d are not necessarily part of the set. For example if for every i, $a_ib_i = x_i^2 - x_1^2$. Then every pair, Q_i, Q_j satisfy Theorem 5ii, but the dimension of $a_1, \dots, a_{m_1}, b_1, \dots, b_{m_1}$ is unbounded.

Proof of Claim 49. If Q_i, Q_j satisfy Theorem 5i then there are constants $\alpha, \beta \in \mathbb{C}$ and $k \in [m_1 + r] \setminus \{i, j\}$ such that $\alpha(Q_o + a_ib_i) + \beta(Q_o + a_jb_j) = \alpha Q_i + \beta Q_j = Q_k = \alpha_k Q_o + a_kb_k$. Rearranging we get that

$$\alpha a_ib_i + \beta a_jb_j - a_kb_k = (\alpha_k - (\alpha + \beta))Q_o\ .$$

From the fact that $\text{rank}_\text{s}(Q_o) \geq 100$, it must be that $\alpha_k - (\alpha + \beta) = 0$. Hence,

$$\alpha a_ib_i + \beta a_jb_j = a_kb_k \tag{6}$$

and (4) holds. Observe that $\alpha, \beta \neq 0$ as otherwise we will have two linearly dependent polynomials in $\mathcal{Q}$.

If Q_i, Q_j satisfy Theorem 5ii then there are $\alpha, \beta \in \mathbb{C}$ and two linear forms c and d such that $\alpha(Q_o + a_ib_i) + \beta(Q_o + a_jb_j) = cd$, and again, by the same argument, we get that $\beta = -\alpha$, and that, without loss of generality,

$$a_ib_i - a_jb_j = cd.$$ ◀

Let $V_i =: \text{span}\{a_i, b_i\}$. We next show that the different spaces V_i satisfy some non-trivial intersection properties.

▷ Claim 50. Let $\tilde{\mathcal{Q}}$ be a $(Q_o, m_1, 0)$-set such that $\text{rank}_\text{s}(Q_o) \geq 100$. If for some $i \in [m_1]$ we have $\dim(V_i) = 2$ then for every $j \in [m_1]$ it holds that $\dim(V_j \cap V_i) \geq 1$. In particular it follows that if $dim(V_j) = 1$ then $V_j \subsetneq V_i$.

Proof. This follows immediately from Claim 49 and Corollary 24. ◁

Next we use this fact to conclude some structure on the set of pairs (a_i, b_i).

▷ Claim 51. Let $\tilde{\mathcal{Q}}$ be as in Claim 47. If $\dim(\text{span}\{a_i, b_i\}) > 3$ then there is a linear space of linear forms, V such that $\dim(V) \leq 4$, and for all $i \in [m_1 + r]$, $b_i \in \text{span}\{a_i, V\}$ or $a_i \in \text{span}\{b_i, V\}$.

Proof. Consider the set of all V_i's of dimension 2. Combining Claim 49 and Claim 26 we get that either $\dim(\bigcup_{i=1}^m V_i) \leq 3$ or $\dim(\bigcap_{i=1}^m V_i) = 1$. If $\dim(\bigcup_{i=1}^m V_i) \leq 3$ then $V = \bigcup_{i=1}^m V_i$ is the linear space promised in the claim. If $\bigcap_{i=1}^m V_i) = 1$ there is a linear form, w, such that $\text{span}\{w\} = \dim(\bigcap_{i=1}^m V_i)$. It follows that for every $i \in [m_1]$ there are constants ϵ_i, δ_i such that, with out loss of generality, $b_i = \epsilon_i a_i + \delta_i w$. Note that if $\dim(V_i) = 1$ this representation also holds with $\delta_i = 0$, and thus $V = \text{span}\{w\}$. is the linear space promised in the claim. ◁

From now on we assume there is a linear space of linear forms, V such that $\dim(V) \leq 4$ and for every $i \in [m_1 + r]$ it holds that $b_i = \epsilon_i a_i + v_i$ (we can do this by replacing the roles of a_i and b_i if needed). Indeed, if $\dim(\text{span}\{a_i, b_i\}) > 3$ then this follows from Claim 51 and otherwise we can take $V = \text{span}\{a_i, b_i\}$. Thus, following Remark 48, every polynomial in $\mathcal{Q}$ is of the form $\alpha_i Q + a_i(\epsilon_i a_i + v_i)$ and for polynomials in $\mathcal{L}$ we have that $\alpha_i = 0$, $\epsilon_i = 1$ and $v_i = 0$.

The following claim is the crux of the proof of Claim 47. It shows that, modulo V, the set $\{a_1, \dots, a_{m_1+r}\}$ satisfies the Sylvester-Gallai theorem..

▷ Claim 52. Let $i \neq j \in [m_1 + r]$ be such that $a_i \notin V$ and $a_j \notin \text{span}\{a_i, V\}$. Then, there is $k \in [m_1 + r]$ such that $a_k \in \text{span}\{a_i, a_j, V\}$ and $a_k \notin \text{span}\{a_i, V\} \cup \text{span}\{a_j, V\}$.

Proof. We split the proof to three cases (recall Remark 48): Either

(i) $\alpha_i = \alpha_j = 1$, or
(ii) $\alpha_i = 1, \alpha_j = 0$ (without loss of generality), or
(iii) $\alpha_i = \alpha_j = 0$.

Recall that $\alpha_i = 0$ if and only if $i \in \{m + 1, \dots, m + r\}$.

(i) $\alpha_i = \alpha_j = 1$. Claim 49 implies that there are two linear forms c and d such that cd is a nontrivial linear combination of $a_j(\epsilon_j a_j + v_j), a_i(\epsilon_i a_i + v_i)$. We next show that without loss of generality c depends non-trivially on both a_i and a_j.

▶ **Lemma 53.** *In the current settings, without lost of generality, $c = \mu a_i + \eta a_j$ where $\mu, \eta \neq 0$.*

Proof. Setting $a_i = 0$ gives that, without loss of generality, $cd \equiv_{a_i} a_j(\epsilon_j a_j + v_j)$ and as $a_j \notin \text{span}\{a_i, V\}$ we have that $cd \not\equiv_{a_i} 0$. Thus, without loss of generality $c \equiv_{a_i} \eta a_j$, for some non-zero η. Let μ and η be such that $c = \mu a_i + \eta a_j$. We will now show that $\mu \neq 0$. Indeed, if this was not the case then we would have that $cd = \eta a_j d$. This means that $a_i(\epsilon_i a_i + v_i) \in \text{span}\{a_j(\epsilon_j a_j + v_j), \eta a_j d\}$ (since the linear dependence was non-trivial) setting $a_j = 0$ we see that either a_i, or $\epsilon_i a_i + v_i$ in $\text{span}\{a_j\}$, which contradicts our assumption. ◀

Equation 4 and Lemma 53 show that if Q_i and Q_j satisfy Theorem 5i, i.e. they span Q_k (for $k \notin \{i, j\}$), then one of $a_k, \epsilon_k a_k + v_k$ is a non-trivial linear combination of a_i and a_j. Thus, modulo V, a_k is in the span of a_i and a_j, which is what we wanted to show.

We next handle the case where Q_i and Q_j satisfy Theorem 5ii. Let cd be a product of linear forms in the span of Q_i and Q_j. From Lemma 53 we can assume that $c = \mu a_i + \eta a_j$ with $\mu\eta \neq 0$. In particular, this means that $\sqrt{\langle Q_i, Q_j \rangle} = \sqrt{\langle cd, Q_j \rangle}$.

The assumption that $\text{rank}_s(Q_o) \geq 100$ implies that Q_j is irreducible even after setting $c = 0$. It follows that if a product of irreducible polynomials satisfy $\prod_i A_i \in \sqrt{\langle cd, Q_j \rangle}$ then, after setting $c = 0$, some A_i is divisible by $Q_j|_{c=0}$. Thus, there is a multiplicand that is equal to $\alpha Q_j + ce$ for some linear form e. In particular, there must be a polynomial Q_k, $k \in [m_1 + r] \setminus \{i, j\}$, such that $Q_k = \alpha Q_j + ce$. If $\alpha = 0$ then it holds that $Q_k = a_k^2 = ce$ and therefore a_k satisfies the claim. Otherwise, as before, the rank condition on Q_o implies that $\alpha = 1$ and thus $a_k(\epsilon_k a_k + v_k) = a_j(\epsilon_j a_j + v_j) + (\mu a_i + \eta a_j)e$. Consider what happens when we set $a_j = 0$. We get that $a_k(\epsilon_k a_k + v_k) \equiv_{a_j} \mu a_i e$. Note that it cannot be the case that $e \equiv_{a_j} 0$ as this would imply that $a_k \in \text{span}\{a_j, v_k\}$ and in turn, this implies that $a_i \in \text{span}\{a_j, V\}$ in contradiction to the choice of a_i and a_j. Thus, we get that either a_k or $\epsilon_k a_k + v_k$ are equivalent to a_i modulo a_j. We next show that if either of them depends only on a_i, then we get a contradiction. Thus, we are left in the case that $a_k = \lambda a_i$ (the case $\epsilon_k a_k + v_k = \lambda a_i$ is equivalent). Since $Q_k = Q_o + \lambda a_i\,(\epsilon_k \lambda a_i + v_k) = Q_j + ce$ and we have that $Q_i = Q_o + a_i(\epsilon_i a_i + v_i) = Q_j + cd$ we get by subtracting Q_i from Q_k that

$$a_i\left((\lambda^2\epsilon_k - \epsilon_i)a_i + (\lambda v_k - v_i)\right) = \lambda a_i(\epsilon_k \lambda a_i + v_k) - a_i(\epsilon_i a_i + v_i) = Q_k - Q_i = c(e-d)\ ,$$

and clearly neither side of the equation is zero since $Q_i \neq Q_k$. This implies that $c \in \operatorname{span}\{a_i, V\}$, in contradiction. Thus, in this case too we get that a_k satisfies the claim.

(ii) $\alpha_i = 1, \alpha_j = 0$. In this case, Q_i, Q_j must satisfy Theorem 5ii, as $0 \cdot Q_i + Q_j = a_j^2$. As before, the assumption that $\operatorname{rank_s}(Q_o) \geq 100$ implies that Q_i is irreducible even after setting $a_j = 0$. It follows that if a product of irreducible polynomials satisfy $\prod_t A_t \in \sqrt{\langle a_j^2, Q_i\rangle}$ then, after setting $a_j = 0$, some A_t is divisible by $Q_i|_{a_j=0}$. In our case we get that there is a multiplicand that is equal to $\alpha Q_i + a_j e$ for some linear form e. In particular, there must be a polynomial Q_k, for $k \in [m_1 + r] \setminus \{i, j\}$, such that $Q_k = \alpha Q_i + a_j e$. If $\alpha = 0$ it follows that Q_k is reducible and thus of the form $Q_k = a_k^2 = a_j e$ which is a contradiction to pairwise linear independence (as $Q_k \sim Q_j$). Thus $\alpha = \alpha_k = 1$, and $a_k(\epsilon_k a_k + v_k) = a_i(\epsilon_i a_i + v_k) + a_j e$. As before, we can conclude that $a_k \in \operatorname{span}\{a_i, a_j, V\}$ and that it cannot be the case that $a_k \in \operatorname{span}\{a_i, V\} \cup \operatorname{span}\{a_j, V\}$ (as by rearranging the equation we will get a contradiction to the fact that $a_j \notin \operatorname{span}\{a_i, V\}$), which is what we wanted to show.

(iii) $\alpha_i = \alpha_j = 0$. Then $\sqrt{\langle Q_i, Q_j\rangle} = \langle a_i, a_j\rangle$ is a prime ideal. It follows that there is $k \in [m_1 + r] \setminus \{i, j\}$ such that $Q_k \in \langle a_i, a_j\rangle$ the rank condition on Q_o implies that $\alpha_k = 0$ and therefore a_k is a non-trivial linear combination of a_i and a_j, which is what we wanted to show.

This completes the proof of Claim 52. ◁

We can now prove Claim 47.

Proof of Claim 47. Claim 52 implies that any two linear functions in $\{a_1, \ldots, a_{m_1+r}\}$ that are linearly independent modulo V, span (modulo V) a third function in the set. This implies that if we project all the linear functions to the perpendicular space to V then they satisfy the usual condition of the Sylvester-Gallai theorem and thus the dimension of the projection is at most 3. As $\operatorname{span}\{a_1, \ldots, a_{m_1}, b_1, \ldots, b_{m_1}, a_{m_1+1}, \ldots, a_{m_1+r}\} \subseteq \operatorname{span}\{a_1, \ldots, a_{m_1+r}, V\}$, we get that $\dim(\{a_1, \ldots, a_{m_1}, b_1, \ldots, b_{m_1}, a_{m_1+1}, \ldots, a_{m_1+r}\}) \leq 3 + \dim(V) \leq 7$, as claimed. ◁

Thus far we have proved Claim 47 which is a restriction of Claim 46 to the case $m_2 = 0$. In the next subsection we handle the general case $m_2 \neq 0$.

4.1.2 The case $m_2 \neq 0$

In this subsection we prove Claim 46. We shall assume without loss of generality that $m_2 \neq 0$. We first show that each $P_i \in \mathcal{Q}_2$ (recall Definition 43) is either a rank-2 quadratic, or it is equal to Q_o plus a rank-2 quadratic.

▷ Claim 54. Let $\tilde{\mathcal{Q}}$ be a (Q_o, m_1, m_2)-set such that $\operatorname{rank_s}(Q_o) \geq 100$. Then for every $i \in [m_2]$ there exists $\gamma_i \in \mathbb{C}$ such that $\operatorname{rank_s}(P_i - \gamma_i Q_o)) = 2$.

Proof. Fix $i \in [m_2]$. We shall analyse, for each $j \in [m_1]$, which case of Theorem 5 Q_j and P_i satisfy. From Observation 45 we know that P_i does not satisfy Theorem 5iii with any Q_j. We start by analysing what happens when P_i and Q_j satisfy Theorem 5ii. By definition, there exist linear forms a', b' and non zero constants $\alpha, \beta \in \mathbb{C}$, such that $\alpha P_i + \beta Q_j = a'b'$ and thus,

$$P_i = \frac{1}{\alpha}\left(a'b' - \beta\left(Q_o + a_j b_j\right)\right) = \frac{-\beta}{\alpha} Q_o + \left(\frac{1}{\alpha} a'b' - \frac{\beta}{\alpha} a_j b_j\right) . \tag{7}$$

Hence, the statement holds with $\gamma_i = -\frac{\beta}{\alpha}$. Indeed, observe that the $\mathrm{rank_s}$ of $(\frac{1}{\alpha} a'b' - \frac{\beta}{\alpha} a_j b_j)$ cannot be 1 as this will contradict item 4 in Definition 43.

Thus, the only case left to consider is when P_i satisfies Theorem 5i alone with all the Q_j's. If for some $j \in [m_1]$ there is $j' \in [m_1]$ such that $Q_{j'} \in \mathrm{span}\{Q_j, P_i\}$, then there are $\alpha, \beta \in \mathbb{C} \setminus \{0\}$, for which $P_i = \alpha Q_j + \beta Q_{j'}$ and then

$$P_i = (\alpha + \beta) Q_o + \alpha a_j b_j + \beta a_{j'} b_{j'},$$

and the statement holds with $\gamma_i = \beta + \alpha$. So, let us assume that for every $j \in [m_1]$, there is $t_j \in [m_2]$ such that $P_{t_j} \in \mathrm{span}\{Q_j, P_i\}$. As $5m_2 + 2 < m_1$ there must be $j' \neq j'' \in [m_1]$ and $t' \in [m_2]$ such that $P_{t'} \in \mathrm{span}\{Q_{j'}, P_i\}$ and $P_{t'} \in \mathrm{span}\{Q_{j''}, P_i\}$. Since $\mathcal{Q}$ is a set of pairwise linearly independent polynomials, we can deduce that $\mathrm{span}\{P_i, P_{t'}\} = \mathrm{span}\{Q_{j'}, Q_{j''}\}$. In particular there exist $\alpha, \beta \in \mathbb{C}$, for which $P_i = \alpha Q_j + \beta Q_{j'}$, which, as we already showed, implies what we wanted to prove. ◁

For simplicity, rescale P_i so that $P_i = \gamma_i Q_o + L_i$ with $\mathrm{rank_s}(L_i) = 2$ and $\gamma_i \in \{0, 1\}$. Clearly $\mathcal{Q}$ still satisfies the conditions of Definition 43 after this rescaling, as it does not affect the vanishing conditions or linear independence. The next claim shows that even in the case $m_2 \neq 0$, the linear forms $\{a_1, \ldots, a_{m_1}, b_1, \ldots, b_{m_1}\}$ "mostly" belong to a low dimensional space (similar to Claim 47).

▷ Claim 55. Let $\tilde{\mathcal{Q}}$ be a (Q_o, m_1, m_2)-set such that $\mathrm{rank_s}(Q_o) \geq 100$. Then, there exists a subspace V of linear forms such that $\dim(V) \leq 4$ and that for at least $m_1 - m_2$ indices $j \in [m_1]$ it holds that $a_j, b_j \in V$. Furthermore, there is a polynomial $P \in \mathcal{Q}_2$ such that $P = \gamma Q_o + L$ and $\mathrm{Lin}(L) = V$.

Proof. Let $P_1 = \gamma_1 Q_o + L_1$ where $\mathrm{rank_s}(L_1) = 2$. To simplify notation we drop the index 1 and only talk of P, L and γ. Set $V = \mathrm{Lin}(L)$. As before, Observation 45 implies that P cannot satisfy Theorem 5iii with any $Q_j \in \mathcal{Q}_1$.

Let $Q_j \in \mathcal{Q}_1 \cup \mathcal{L}$. If Q_j, P satisfy Theorem 5iii, then $\alpha_j = 0$ and $Q_j = a_j^2$. By the rank condition on Q_o it follows that $\gamma = 0$ and therefore $a_j \in \mathrm{Lin}(L) = V$.

Let $Q_j \in \mathcal{Q}_1 \cup \mathcal{L}$ be such that Q_j and P satisfy Theorem 5ii. This means that there are two linear forms e, f, and non zero $\alpha, \beta \in \mathbb{C}$ for which $\alpha P - \beta Q_j = ef$, and so,

$$(\alpha\gamma - \beta\alpha_j) Q_o = -\alpha L + \beta a_j b_j + ef \tag{8}$$

As we assumed that $\mathrm{rank_s}(Q_o) \geq 100$ this implies that $\alpha\gamma - \beta\alpha_j = 0$ and thus $\beta a_j b_j + ef = \beta L$. Claim 19 implies that $e, f, a_j, b_j \in V$.

We have shown that V contains all a_j, b_j that come from polynomials satisfying Theorem 5ii with P.

Let $j \in [m_1]$ be such that P and Q_j satisfy Theorem 5i but not Theorem 5ii, i.e, they span another polynomial in $\tilde{\mathcal{Q}} \setminus \mathcal{L}$. If this polynomial is in $\mathcal{Q}_1$, i.e. there exists $j' \in [m_1]$ such that $Q_{j'} \in \mathrm{span}\{P, Q_j\}$ then $P = \alpha Q_j + \beta Q_{j'}$ and as before we would get that $a_{j'}, b_{j'}, a_j, b_j \in V$.

All that is left is to bound the number of $j \in [m_1]$ so that P and Q_j span a polynomial in $\mathcal{Q}_2$. If there are more than m_2 such indices j then, by the pigeonhole principle, for two of them, say j, j' it must be the case that there is some $i \in [m_2]$ such that $P_i \in \text{span}\{P, Q_j\}$ and $P_i \in \text{span}\{P, Q_{j'}\}$. As our polynomials are pairwise independent this implies that $P \in \text{span}\{Q_j, Q_{j'}\}$, and as before we get that $a_{j'}, b_{j'}, a_j, b_j \in V$.

It follows that the only j's for which we may have $a_j, b_j \notin V$ must be such that Q_j and P span a polynomial in $\mathcal{Q}_2$, and no other $Q_{j'}$ spans this polynomial with P. Therefore, there are at most m_2 such "bad" j's and the claim follows. ◁

▶ Remark 56. The proof of Claim 55 implies that if $Q_i = \alpha_i Q_o + a_i b_i \in \mathcal{Q}_1$ satisfies that $\{a_i, b_i\} \not\subseteq V$ then it must be the case that Q_i and P span a polynomial $P_j \in \mathcal{Q}_2$.

▷ Claim 57. Let $\tilde{\mathcal{Q}}$ be a (Q_o, m_1, m_2)-set such that $\text{rank}_\text{s}(Q_o) \geq 100$. Then there exists a 4-dimensional linear space V, such that for every $P_i \in \tilde{\mathcal{Q}}$ either P_i is defined over V, or there is a quadratic polynomial P'_i and a linear form v_i that are defined over V, and a linear form c_i, such that $P_i = Q_o + P'_i + c_i(\epsilon_i c_i + v_i)$, or $P_i = c_i^2$.

Proof. Claim 55 implies the existence of a polynomial $P = \gamma Q_o + L \in \mathcal{Q}_2$ and 4-dimensional linear space $V = \text{Lin}(L)$ such that the set $\mathcal{I} = \{Q_j \mid j \in [m_1] \text{ and } a_j, b_j \in V\}$ satisfies $|\mathcal{I}| \geq m_1 - m_2$. We will prove that V is the space guaranteed in the claim. We first note that every $P_i \in \mathcal{I}$ satisfies the claim with $P'_i = a_i b_i$ and $v_i = c_i = 0$, and clearly for $Q_i \in \mathcal{L}$ the claim trivially holds.

Consider $Q_i \in \mathcal{Q}_1 \setminus \mathcal{I}$. By Remark 56 it must be the case that Q_i and P span a polynomial $P_j \in \mathcal{Q}_2$. Hence, there are $\alpha, \beta \in \mathbb{C} \setminus \{0\}$ such that $P_j = \alpha P + \beta Q_i$. From Claim 54 we get that $P_j = \gamma_j Q_o + L_j$ and thus

$$(\gamma_j - \alpha\gamma - \beta) Q_o = \alpha L + \beta a_i b_i - L_j \ .$$

As $\text{rank}_\text{s}(Q_o) \geq 100$ it follows that $(\gamma_j - \alpha\gamma - \beta) = 0$ and $\alpha L + \beta a_i b_i = L_j$. Claim 23 implies that $\text{span}\{a_i, b_i\} \cap V \neq \{\vec{0}\}$ and therefore there is $v_i \in V$ such that, without loss of generality, $b_i = \epsilon_i a_i + v_i$, for some constant ϵ_i. Thus, the claimed statement holds for Q_i with $c_i = a_i$ and $Q'_i = 0$. I.e., $Q_i = Q_o + 0 + a_i(\epsilon_i a_i + v_i)$.

Consider a polynomial $P_i = \gamma_i Q_o + L_i \in \mathcal{Q}_2$.

If $\gamma_i = 0$ then by rank argument we see that P_i cannot satisfy Theorem 5ii nor Theorem 5iii with any polynomial in $\mathcal{Q}_1$. Hence it must satisfy Theorem 5i with all the polynomials in $\mathcal{Q}_1$. Therefore, by the pigeonhole principle P_i must be spanned by two polynomials in $\mathcal{I}$. Note that in this case we get that $P_i = L_i$ is a polynomial defined over V.

Assume then that $\gamma_i = 1$. If P_i is spanned by Q_j and $Q_{j'}$ such that $j, j' \in \mathcal{I}$, then, as before, $\text{Lin}(L_i) \subseteq \text{span}\{a_j b_j, a_{j'} b_{j'}\}$ and hence L_i is a function of the linear forms in V. Thus, the statement holds with $P'_i = L$ and $v_i = c_i = 0$.

The only case left to consider is when $\gamma_i = 1$ and every polynomial Q_j, for $j \in \mathcal{I}$, that satisfies Theorem 5i with P_i, does not span with P_i any polynomial in $\{Q_j \mid j \in \mathcal{I}\} \cup \mathcal{L}$. Note that in such a case it must hold that Q_j spans with P_i a polynomial in $\{Q_j \mid j \in [m_1] \setminus \mathcal{I}\} \cup \mathcal{Q}_2$. Observe that since our polynomials are pairwise linearly independent, if two polynomials from $\mathcal{I}$ span the same polynomial with P_i then P_i is in their span and we are done. From

$$|\{Q_j \mid j \in [m_1] \setminus \mathcal{I}\} \cup \mathcal{Q}_2| \leq (m_1 - |\mathcal{I}|) + m_2 \leq 2m_2 < m_1 - m_2 - 2 \leq |\mathcal{I}| - 2 \ ,$$

we see that for P_i to fail to satisfy the claim it must be the case that it satisfies Theorem 5ii with at least 2 polynomials whose indices are in $\mathcal{I}$. Let $Q_j, Q_{j'} \in \mathcal{I}$ be two such polynomials. In particular, there are four linear forms c, d, e and f and scalars $\epsilon_j, \epsilon_{j'}$, such that

$$P_i - \varepsilon_j Q_j = cd \quad \text{and} \quad P_i - \varepsilon_{j'} Q_{j'} = ef \ . \tag{9}$$

Equivalently,

$$(1-\varepsilon_j)Q_o = cd + \varepsilon_j a_j b_j - L_i \quad \text{and} \quad (1-\varepsilon_{j'})Q_o = ef + \varepsilon_{j'} a_{j'} b_{j'} - L_i \ .$$

As $\text{rank}_\text{s}(Q_o) \geq 100$ it must hold that $\varepsilon_j = \varepsilon_{j'} = 1$ and hence

$$L_i = cd + a_j b_j \quad \text{and} \quad L_i = ef + a_{j'} b_{j'} \ .$$

It follows that $cd - ef = a_{j'}b_{j'} - a_j b_j$ and therefore $\text{Lin}(cd - ef) \subseteq V$. Claim 25 implies that without loss of generality $d = \epsilon_i c + v_i$. We therefore conclude that

$$P_i = Q_o + L_i = Q_o + a_j b_j + c(\epsilon_i c + v_i)$$

and the statement holds for $P_i' = a_j b_j$ and $c_i = c$. This completes the proof of the Claim 57. ◁

Consider the representation guaranteed in Claim 57 and let

$$\mathcal{S} = \{c_i \mid \text{there is } P_i \in \mathcal{Q} \text{ such that either } P_i = c_i^2 \text{ or, for some } P_i' \text{ defined over } V, \\ P_i = Q_o + P_i' + c_i(\epsilon_i c_i + v_i)\} \ .$$

Clearly, in order to bound the dimension of $\tilde{\mathcal{Q}}$ it is enough to bound the dimension of $\mathcal{S}$. We do so, by proving that $\mathcal{S}$ satisfies the conditions of Sylvester-Gallai theorem modulo V, and thus have dimension at most $3 + \dim(V) = 7$.

▷ Claim 58. Let $c_i, c_j \in \mathcal{S}$ be such that $c_i \notin V$ and $c_j \notin \text{span}\{c_i, V\}$. Then, there is $c_k \in \mathcal{S}$ such that $c_k \in \text{span}\{c_i, c_j, V\}$ and $c_k \notin \text{span}\{c_i, V\} \cup \text{span}\{c_j, V\}$.

Before proving the claim we prove the following simple lemma.

▶ **Lemma 59.** *Let P_V be a polynomial defined over V and let c_i, c_j as in Claim 58. If there are linear forms e, f such that*

$$c_j(\epsilon_j c_j + v_j) + c_i(\epsilon_i c_i + v_i) + ef = P_V$$

then, without loss of generality, $e \in \text{span}\{c_i, c_j, V\}$ and $e \notin \text{span}\{c_i, V\} \cup \text{span}\{c_j, V\}$.

Proof. First note that $e \notin V$ as otherwise we would have that $c_i \equiv_V c_j$ in contradiction.

By our assumption, $ef = P_V$ modulo c_i, c_j. We can therefore assume without loss of generality that $e \in \text{span}\{c_i, c_j, V\}$. Assume towards a contradiction and without loss of generality that $e = \lambda c_i + v_e$, where $\lambda \neq 0$ and $v_e \in V$. Consider the equation $c_j(\epsilon_j c_j + v_j) + c_i(\epsilon_i c_i + v_i) + ef = P_V$ modulo c_i. We have that $c_j(\epsilon_j c_j + v_j) + v_e f \equiv_{c_i} P_V$ which implies that $\epsilon_j = 0$. Consequently, we also have that $f = \mu c_j + \eta c_i + v_f$, for some $\mu \neq 0$ and $v_f \in V$. We now observe that the product $c_i c_j$ has a non zero coefficient $\lambda\mu$ in ef and a zero coefficient in $P_V - c_j(\epsilon_j c_j + v_j) + c_i(\epsilon_i c_i + v_i)$, in contradiction. ◀

Proof of Claim 58. Following the notation of Claim 57, we either have $Q_i = Q_o + Q_i' + c_i(\epsilon_i c_i + v_i)$ or $Q_i = c_i^2$. Very similarly to Claim 52, we consider which case of Theorem 5 Q_i and Q_j satisfy, and what structure they have.

Assume $Q_i = Q_o + Q_i' + c_i(\epsilon_i c_i + v_i)$ and $Q_j = Q_o + Q_j' + c_j(\epsilon_j c_j + v_j)$. As argued before, since the rank of Q_o is large they can not satisfy Theorem 5iii. We consider the remaining cases:

- Q_i, Q_j satisfy Theorem 5i: there is $Q_k \in \mathcal{Q}$ such that $Q_k \in \text{span}\{Q_i, Q_j\}$.
  By assumption, for some scalars α, β we have that

  $$Q_k = \alpha(Q_o + Q_i' + c_i(\epsilon_i c_i + v_i)) + \beta(Q_o + Q_j' + c_j(\epsilon_j c_j + v_j)) \ . \tag{10}$$

  If Q_k depends only on V then we would get a contradiction to the choice of c_i, c_j. Indeed, in this case we have that

  $$(\alpha+\beta)Q_o = Q_k - \alpha(Q_i' + c_i(\epsilon_i c_i + v_i)) - \beta(Q_j' + c_j(\epsilon_j c_j + v_j)) \ .$$

  Rank arguments imply that $\alpha + \beta = 0$ and therefore

  $$\alpha c_i(\epsilon_i c_i + v_i) + \beta c_j(\epsilon_j c_j + v_j) = Q_k - \alpha Q_i' - \beta Q_j' \ ,$$

  which implies that c_i and c_j are linearly dependent modulo V in contradiction.
  If $Q_k = c_k^2$ then by Lemma 59 it holds that c_k satisfies the claim condition.
  We therefore assume that Q_k is not a function of V alone and denote $Q_k = Q_o + Q_k' + c_k(\epsilon_k c_k + v_k)$. Equation 10 implies that

  $$(1-\alpha-\beta)Q_o = \alpha Q_i' + \beta Q_j' - Q_k' + \alpha c_i(\epsilon_i c_i + v_i) + \beta c_j(\epsilon_j c_j + v_j) - c_k(\epsilon_k c_k + v_k) \ .$$

  As $\alpha Q_i' + \beta Q_j' - Q_k'$ is a polynomial defined over V, its rank is smaller than 4 and thus, combined with the fact that $\text{rank}_s(Q_o) \geq 100$, we get that $(1-\alpha-\beta) = 0$ and

  $$Q_k' - \alpha Q_i' - \beta Q_j' = \alpha c_i(\epsilon_i c_i + v_i) + \beta c_j(\epsilon_j c_j + v_j) - c_k(\epsilon_k c_k + v_k) \ .$$

  We now conclude from Lemma 59 that c_k satisfies the claim.
- Q_i, Q_j satisfy Theorem 5ii: There are linear forms e, f such that for non zero scalars α, β, $\alpha Q_i + \beta Q_j = ef$. In particular,

  $$(\alpha+\beta)Q_o = ef - \alpha Q_i' - \beta Q_j' - \alpha c_i(\epsilon_i c_i + v_i) - \beta c_j(\epsilon_j c_j + v_j).$$

  From rank argument we get that $\alpha + \beta = 0$ and from Lemma 59 we conclude that, without loss of generality, $e = \mu c_i + \eta c_j + v_e$ where $\mu, \eta \neq 0$. We also assume without loss of generality that $Q_i = Q_j + ef$.
  By our assumption that $\text{rank}_s(Q_o) \geq 100$ it follows that Q_j is irreducible even after setting $e = 0$. It follows that if a product of irreducible quadratics satisfy

  $$\prod_k A_k \in \sqrt{\langle Q_i, Q_j \rangle} = \sqrt{\langle ef, Q_j \rangle}$$

  then, after setting $e = 0$, some A_k is divisible by $Q_j|_{e=0}$. Thus, there is a multiplicand that is equal to $\gamma Q_j + ed$ for some linear form d and scalar γ. In particular, there must be a polynomial $Q_k \in \tilde{\mathcal{Q}} \setminus \{Q_1, Q_2\}$, such that $Q_k = \gamma Q_j + ed$. If $\gamma = 0$ then it must hold that $Q_k = a_k^2 = ed$ and thus $a_k \sim e$, and the statment holds. If $\gamma = 1$ then we can assume without loss of generality that $Q_k = Q_j + ed$. Thus,

  $$Q + Q_k' + c_k(\epsilon_k c_k + v_k) = Q_k = Q_j + ed = Q_o + Q_j' + c_j(\epsilon_j c_j + v_j) + (\mu c_i + \eta c_j + v_e)d \ .$$

  Setting $c_j = 0$ we get that

  $$Q_k' + c_k(\epsilon_k c_k + v_k) \equiv_{c_j} Q_j' + (\mu c_i + v_e)d \ . \tag{11}$$

  Note that it cannot be the case that $d \equiv_{c_j} 0$. Indeed, if $d = 0$ then we get that Q_j and Q_k are linearly dependent in contradiction. If $d \sim c_j$ then (11) implies that $c_k \in \text{span}\{c_j, V\}$.

From the equality $Q_k = Q_j + ed$ and the fact that e depends non trivially on c_i, it now follows that $c_i \in \mathrm{span}\{c_j, V\}$ in contradiction to the choice of c_i and c_j. As $d \not\equiv_{c_j} 0$, we deduce from (11) that, modulo c_j, $c_k \in \mathrm{span}\{c_i, V\}$. We next show that if c_k depends only on c_i and V then we reach a contradiction and this will conclude the proof. So assume towards a contradiction that $c_k = \lambda c_i + v'_k$, for a scalar λ and $v'_k \in V$. Since

$$Q_j + ed = Q_k = Q_o + Q'_k + c_k(\epsilon_k c_k + v_k) = Q_o + Q'_k + (\lambda c_i + v'_k)\,(\epsilon_k(\lambda c_i + v'_k) + v_k)$$

and

$$Q_j + ef = Q_i = Q_o + Q'_i + c_i(\epsilon_i c_i + v_i)$$

we get by subtracting Q_i from Q_k that

$$e(d - f) = Q_k - Q_i = Q'_k - Q'_i + (\lambda c_i + v'_k)\,(\epsilon_k(\lambda c_i + v'_k) + v_k) - c_i(\epsilon_i c_i + v_i)$$

and clearly neither side of the equation is zero since $Q_i \neq Q_k$. This implies that $e \in \mathrm{span}\{c_i, V\}$. This however contradicts the fact that $e = \mu c_i + \eta c_j + v_e$ where $\mu, \eta \neq 0$.

Now let us consider the case where without loss of generality, $Q_i = Q_o + Q'_i + c_i(\epsilon_i c_i + v_i)$ and $Q_j = c_j^2$. In this case the polynomials satisfy Theorem 5ii as $0 \cdot Q_i + Q_j = c_j^2$. Similarly to the previous argument, it holds that there is Q_k such that $Q_k = \gamma Q_i + c_j e$. If $\gamma = 0$ it holds that Q_k is reducible, and therefore a square of a linear form, in contradiction to pairwise linear independence. Thus $\gamma \neq 0$. If Q_k is defined only on the linear functions in V then it is of rank smaller then $\dim(V) \leq 4$, which will result in a contradiction to the rank assumption on Q_o. Thus $Q_k = Q_o + Q'_k + c_k(\epsilon_k c_k + v_k)$ and $\gamma = 1$. Therefore, we have

$$Q_o + Q'_k + c_k(\epsilon_k c_k + v_k) = Q_k = Q_i + c_j e \ = Q_o + Q'_i + c_i(\epsilon_i c_i + v_i) + c_j e.$$

Hence,

$$Q'_k - Q'_i - c_i(\epsilon_i c_i + v_i) - c_j e = -c_k(\epsilon_k c_k + v_k).$$

Looking at this equation modulo c_j implies that $c_k \in \mathrm{span}\{V, c_i, c_j\}$. and $c_k \notin \mathrm{span}\{V, c_j\}$, or we will get a contradiction to the fact that $c_i \notin \mathrm{span}\{c_j, V\}$. Similarly it holds that $c_k \notin \mathrm{span}\{V, c_i\}$, as we wanted to show.

The last structure we have to consider is the case where $Q_i = c_i^2, Q_j = c_j^2$. In this case, the ideal $\sqrt{\langle c_i^2, c_j^2\rangle} = \langle c_i, c_j\rangle$ is prime and therefore there is $Q_k \in \langle c_i, c_j\rangle$ this means that $\mathrm{rank_s}(Q_k) \leq 2$. If $\mathrm{rank_s}(Q_k) = 1$ then $Q_k = c_k^2$ and the statement holds. $\mathrm{rank_s}(Q_k) = 2$ then Q_k is defined on the linear function of V, which implies $c_i, c_j \in V$ in contradiction to our assumptions. ◁

We are now ready to prove Claim 46.

Proof of Claim 46. Claim 58 implies that if we project the linear forms in $\mathcal{S}$ to $V^{\perp}$ then, after removing linearly dependent forms, they satisfy the conditions of the Sylvester-Gallai theorem. As $\dim(V) \leq 4$ we obtain that $\dim(\mathrm{span}\{\mathcal{S} \cup V\}) \leq 7$. By Claim 57 every polynomial $P \in \mathcal{Q}$ is a linear combination of Q_o and a polynomial defined over $\mathrm{span}\{\mathcal{S} \cup V\}$ which, by the argument above, implies that $\dim(\mathrm{span}\{\mathcal{Q}\}) \leq 8$. ◁

This completes the proof of Theorem 44 when Q_o has high rank. We next handle the case where Q_o is of low rank.

4.2 Q_o is of Low Rank

In this section we prove the following claim.

▷ Claim 60. Let $\tilde{\mathcal{Q}}$ be a (Q_o, m_1, m_2)-set such that $2 \leq \text{rank}_s(Q_o) < 100$. Then, $\dim(\text{span}\{\tilde{\mathcal{Q}}\}) = O(1)$.

Before we start with the proof of the main claim, let us prove a similar claim but for a more specific structure of polynomials. We will later see that, essentially, this structure holds when $2 \leq \text{rank}_s(Q_o) < 100$.

▷ Claim 61. Let $\tilde{\mathcal{Q}}$ be a set of quadratics polynomials that satisfy the conditions in the statement of Theorem 4. Assume farther that there is a linear space of linear forms, V such that $\dim(V) = \Delta$ and for each polynomial $Q_i \in \tilde{\mathcal{Q}}$ one of the following holds: either $Q_i \in \langle V \rangle$ or there is a linear form a_i such that $\text{Lin}(Q_i) \subseteq \text{span}\{V, a_i\}$. Then $\dim(\tilde{\mathcal{Q}}) \leq 8\Delta^2$.

Proof. Note that by the conditions in the statement of Theorem 4, no two polynomials in $\tilde{\mathcal{Q}}$ share a common factor.

Let $\vec{\alpha} \in \mathbb{C}^\Delta$ be such that if two polynomials in $T_{\vec{\alpha},V}(\tilde{\mathcal{Q}})$ (recall Definition 27) share a common factor then it is a polynomial in z. Note that by Claim 29 such $\vec{\alpha}$ exists. Thus, each $P \in \tilde{\mathcal{Q}}$, satisfies that either $T_{\vec{\alpha},V}(P) = \alpha_P z^2$ or $\text{Lin}(T_{\vec{\alpha},V}(P)) \subseteq \text{span}\{z, a_P\}$ for some linear form a_P independent of z. It follows that every polynomial in $T_{\vec{\alpha},V}(\tilde{\mathcal{Q}})$ is reducible. We next show that $\mathcal{S} = \{a_P \mid P \in \tilde{\mathcal{Q}}\}$ satisfies the conditions of Sylvester-Gallai theorem modulo z.

Let $a_1, a_2 \in \mathcal{S}$ such that $a_2 \notin \text{span}\{z, a_1\}$. Consider Q_1 such that $\text{Lin}(T_{\vec{\alpha},V}(Q_1)) \subseteq \text{span}\{z, a_1\}$ yet $\text{Lin}(T_{\vec{\alpha},V}(Q_1)) \not\subseteq \text{span}\{z\}$. Similarly, let Q_2 be such that $\text{Lin}(T_{\vec{\alpha},V}(Q_2)) \subseteq \text{span}\{z, a_2\}$ and $\text{Lin}(T_{\vec{\alpha},V}(Q_2)) \not\subseteq \text{span}\{z\}$. Then there is a factor of $T_{\vec{\alpha},V}(Q_1)$ of the form $\gamma_1 z + \delta_1 a_1$ where $\delta_1 \neq 0$. Similarly there is a factor of $T_{\vec{\alpha},V}(Q_2)$ of the form $\gamma_2 z + \delta_2 a_2$ where $\delta_2 \neq 0$.

This implies that $\sqrt{\langle T_{\vec{\alpha},V}(Q_1), T_{\vec{\alpha},V}(Q_2) \rangle} \subseteq \langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle$. Indeed, it is clear that for $i \in \{1, 2\}$, $T_{\vec{\alpha},V}(Q_i) \in \langle \gamma_i z + \delta_i a_i \rangle$. Hence, $\sqrt{\langle T_{\vec{\alpha},V}(Q_1), T_{\vec{\alpha},V}(Q_2) \rangle} \subseteq \sqrt{\langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle} = \langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle$, where the equality holds since $\langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle$ is a prime ideal.

We know that, there are $Q_3, Q_4, Q_5, Q_6 \in \mathcal{Q}$ such that

$$Q_3 \cdot Q_4 \cdot Q_5 \cdot Q_6 \in \sqrt{\langle Q_1, Q_2 \rangle}.$$

As $T_{\vec{\alpha},V}$ is a ring homomorphism it follows that,

$$T_{\vec{\alpha},V}(Q_3) \cdot T_{\vec{\alpha},V}(Q_4) \cdot T_{\vec{\alpha},V}(Q_5) \cdot T_{\vec{\alpha},V}(Q_6) \in \sqrt{\langle T_{\vec{\alpha},V}(Q_1), T_{\vec{\alpha},V}(Q_2) \rangle},$$

and

$$\sqrt{\langle T_{\vec{\alpha},V}(Q_1), T_{\vec{\alpha},V}(Q_2) \rangle} \subseteq \langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle .$$

Since $\langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle$ is prime it follows that, without loss of generality, $T_{\vec{\alpha},V}(Q_3) \in \langle \gamma_1 z + \delta_1 a_1, \gamma_2 z + \delta_2 a_2 \rangle$. It cannot be the case that $T_{\vec{\alpha},V}(Q_3) \in \langle \gamma_i z + \delta_i a_i \rangle$ for any $i \in \{1, 2\}$, because otherwise this will imply that $T_{\vec{\alpha},V}(Q_3)$ and $T_{\vec{\alpha},V}(Q_i)$ share a common factor that is not a polynomial in z, in contradiction to our choice of $T_{\vec{\alpha},V}$. This means that there is a factor of $T_{\vec{\alpha},V}(Q_3)$ that is in $\text{span}\{a_1, a_2, z\} \setminus (\text{span}\{a_1, z\} \cup \text{span}\{a_2, z\})$. Consequently, $a_3 \in \text{span}\{a_1, a_2, z\} \setminus (\text{span}\{a_1, z\} \cup \text{span}\{a_2, z\})$ as we wanted to prove. This shows that $\mathcal{S}$ satisfies the conditions of Sylvester-Gallai theorem, and therefore $\dim(\mathcal{S}) \leq 3$. Repeating the analysis above for linearly independent $\vec{\alpha}_1, \ldots, \vec{\alpha}_\Delta$, we can use Claim 32 and obtain that $\dim(\text{Lin}(\tilde{\mathcal{Q}})) \leq (3+1)\Delta$, and thus $\dim(\tilde{\mathcal{Q}}) \leq \binom{4\Delta}{2} + \Delta \leq 8\Delta^2$. ◁

Back to the proof of Claim 60. As before we first prove the claim for the case $m_2 = 0$ and then we prove the general case.

4.2.1 The case $m_2 = 0$

Similarly to the high rank case, in this subsection we prove the following claim.

▷ Claim 62. Let $\tilde{\mathcal{Q}} = \mathcal{Q} \cup \mathcal{L}$ be a$(Q_o, m_1, 0)$-set such that $2 \leq \text{rank}_\text{s}(Q_o) < 100$, then $\dim(\text{span}\{a_1, \ldots, a_{m_1}, b_1, \ldots, b_{m_1}, \ell_1, \ldots, \ell_r\}) = O(1)$.

The proof is similar in structure to the proof of Claim 47. As before, we consider a polynomial $\ell_i^2 \in \mathcal{L}$ as $0 \cdot Q_o + \ell_i \ell_i$. We start by proving an analog of Claim 49. The claims are similar but the proofs are slightly different as we cannot rely on Q_o having high rank.

▷ Claim 63. Let $\tilde{\mathcal{Q}}$ satisfy the assumptions of Claim 62. Let $i \in [m_1]$ be such that $dim(a_i, b_i) = 2$ and $\text{span}\{a_i, b_i\} \cap \text{Lin}(Q_o) = \{\vec{0}\}$. Then, for every $j \in [m_1]$ the following holds:

1. Q_i and Q_j do not satisfy Theorem 5iii.
2. If Q_i and Q_j satisfy Theorem 5i then there exists $\alpha, \beta \in \mathbb{C} \setminus \{0\}$ such that for some $k \in [m_1] \setminus \{i, j\}$
$$\alpha a_i b_i + \beta a_j b_j = a_k b_k \ . \tag{12}$$
3. If Q_j is irreducible and Q_i and Q_j satisfy Theorem 5ii then there exist two linear forms, c and d such that
$$a_i b_i - a_j b_j = cd \ . \tag{13}$$

Proof. Assume Q_i and Q_j satisfy Theorem 5i, i.e., there are $\alpha, \beta \in \mathbb{C}$ and $k \in [m_1] \setminus \{i, j\}$ such that

$$\alpha(Q_o + a_i b_i) + \beta(Q_o + a_j b_j) = \alpha Q_i + \beta Q_j = Q_k = \alpha_k Q + a_k b_k$$

This implies that $\alpha a_i b_i + \beta a_j b_j - a_k b_k = (\alpha_k - (\alpha + \beta))Q_o$. We next show that it must be the case that $\alpha_k - (\alpha + \beta) = 0$.

Indeed, if $\alpha_k - (\alpha + \beta) \neq 0$ we get that $\beta a_j b_j - a_k b_k = (\alpha_k - (\alpha + \beta))Q_o - \alpha a_i b_i$. However, as we assumed $\text{span}\{a_i, b_i\} \cap \text{Lin}(Q_o) = \{\vec{0}\}$, we get by Claim 23 that

$$\text{rank}_\text{s}(\alpha_k - (\alpha + \beta))Q_o - \alpha a_i b_i) = \text{rank}_\text{s}(Q_o) + 1 > 2 \geq \text{rank}_\text{s}(\beta a_j b_j - a_k b_k)$$

in contradiction. We thus have that $\alpha_k - (\alpha + \beta) = 0$ and hence

$$\alpha a_i b_i + \beta a_j b_j = a_k b_k \tag{14}$$

and Equation 12 is satisfied. Observe that since our polynomials are pairwise independent $\alpha, \beta \neq 0$.

A similar argument to the one showing $\alpha_k - (\alpha + \beta) = 0$ also implies that Q_i and Q_j do not satisfy Theorem 5iii. If this was not the case then we would have that $\text{rank}_\text{s}(Q_o + a_i b_i) = 2$ which would again contradict Claim 23.

If Q_j is irreducible, the only case left is when $Q_o + a_i b_i, Q_o + a_j b_j$ satisfy Theorem 5ii. In this case there are $\alpha, \beta \in \mathbb{C}$ and two linear forms c and d such that $\alpha(Q_o + a_i b_i) + \beta(Q_o + a_j b_j) = cd$, and again, by the same argument we get that $\beta = -\alpha$ and so (after rescaling c)

$$a_i b_i - a_j b_j = cd \ .$$

This completes the proof of Claim 63. ◁

For each $i \in [m_1]$ let $V_i =: \text{span}\{a_i, b_i\}$. The next claim is analogous to Claim 50.

▷ Claim 64. Let $\tilde{\mathcal{Q}}$ satisfy the assumption in Claim 62. If for some $i \in [m_1]$ it holds that $\dim(V_i) = 2$ and $\text{Lin}(Q_o) \cap V_i = \{\vec{0}\}$ then for every $j \in [m_1]$ it is the case that $\dim(V_j \cap V_i) \geq 1$. In particular, if $dim(V_j) = 1$ then $V_j \subsetneq V_i$.

Proof. The proof of this claim follows immediately from Claim 63 and Corollary 24. ◁

the next claim is an analogous to Claim 51.

▷ Claim 65. Under the assumptions of Claim 62 there exists a subspace V of linear forms such that $\dim(V) \leq 2 \cdot 100 + 3$ and for every $i \in [m_1]$ there exists $v_i \in V$ and a constant $\epsilon_i \in \mathbb{C}$ such that $b_i = \epsilon_i a_i + v_i$ (or $a_i = \epsilon_i b_i + v_i$).

Proof. Let $\mathcal{I} = \{i \in [m_1] \mid \dim(V_i) = 2 \text{ and } \text{Lin}(Q_o) \cap V_i = \{\vec{0}\}\}$. If $\dim(\bigcup_{i \in \mathcal{I}} V_i) \leq 3$ then we set $V = \text{span}\{\text{Lin}(Q_o) \cup (\bigcup_{i \in \mathcal{I}} V_i)\}$. Clearly $\dim(V) \leq 2 \cdot \text{rank}_s(Q) + 3 \leq 2 \cdot 100 + 3$. Claim 64 implies that V has the required properties.

If $\dim(\bigcup_{i \in \mathcal{I}} V_i) > 3$ then from Claim 64 and Claim 26 it follows that $\dim(\bigcap_{i \in \mathcal{I}} V_i) = 1$. Let w be such that $\text{span}\{w\} = \bigcap_{i \in \mathcal{I}} V_i$ and set $V = \text{span}\{\text{Lin}(Q_o), w\}$. In this case too it is easy to see that V has the required properties. ◁

From now on we assume, without loss of generality that for every $i \in [m_1]$, $b_i = \epsilon_i a_i + v_i$. This structure also holds for the polynomials in $\mathcal{L}$.

Proof of Claim 62. Claim 65 implies that there is a linear space of linear forms, V, with $\dim(V) \leq 2 \cdot 100 + 3$, with the property that for every $Q_i \in \tilde{\mathcal{Q}}$ there is a linear form a_i such that $\text{Lin}(Q_i) \subseteq \text{span}\{V, a_i\}$. Thus $\tilde{\mathcal{Q}}$ satisfies the conditions of Claim 61, and $\dim(\tilde{\mathcal{Q}}) = O(1)$, as we wanted to show. ◁

We next consider the case $m_2 \neq 0$.

4.2.2 The case $m_2 \neq 0$

In this subsection we prove Claim 60, we can assume without loss of generality that $m_2 \neq 0$, as the case that $m_2 = 0$ was proved in the previous subsection. To handle this case we prove the existence of a subspace V of linear forms, of dimension $O(1)$, such that every polynomial in $\tilde{\mathcal{Q}}$ is in $\langle V \rangle$, and then, like we did before, we bound the dimension of $\tilde{\mathcal{Q}}$. The first step is proving an analog of Claim 54.

▷ Claim 66. Let $\tilde{\mathcal{Q}}$ be a (Q_o, m_1, m_2)-set such that $\text{rank}_s(Q_o) < 100$. Then for every $i \in [m_2]$ there exists $\gamma_i \in \mathbb{C}$ such that $\text{rank}_s(P_i - \gamma_i Q_o) = 2$.

Proof. Consider $i \in [m_2]$. If P_i satisfies Theorem 5iii with any $Q_j \in \mathcal{Q}_1$, then the claim holds with $\gamma_i = 0$. If P_i satisfies Theorem 5ii with any $Q_j \in \mathcal{Q}$ then there exist linear forms c and d and non zero $\alpha, \beta \in \mathbb{C}$, such that $\alpha P_i + \beta Q_j = cd$. Therefore, $P_i = \frac{1}{\alpha}(cd - \beta(Q + a_j b_j))$ and the statement holds with $\gamma_i = -\frac{\beta}{\alpha}$. Observe that the rank of $cd - \beta a_j b_j$ cannot be 1 by Definition 43.

Thus, the only case left to consider is when P_i satisfies Theorem 5i with all the Q_j's in $\mathcal{Q}_1$. We next show that in this case there must exist $j \neq j' \in [m_1]$ such that $Q_{j'} \in \text{span}\{Q_j, P_i\}$. Indeed, since $m_1 > 5m_2 + 2$ there must be $j, j' \in [m_1]$ and $i' \in [m_2]$ such that $P_{i'} \in \text{span}\{Q_{j'}, P_i\}$ and $P_{i'} \in \text{span}\{Q_j, P_i\}$. As we saw before this implies that $P_i \in \text{span}\{Q_j, Q_{j'}\}$, which is what we wanted to show.

Let $j \neq j' \in [m_1]$ be as above and let $\alpha, \beta \in \mathbb{C}$ be such that $P_i = \alpha Q_j + \beta Q_{j'}$. It follows that

$$P_i = (\alpha + \beta) Q_o + \alpha a_j b_j + \beta a_{j'} b_{j'} \ .$$

Let $\gamma_i = \alpha + \beta$. Property 4 in Definition 43 implies that $\text{rank}_\text{s}(\alpha a_j b_j + \beta a_{j'} b_{j'}) = 2$ and the claim follows. ◁

As before, whenever $\gamma_i \neq 0$ let us replace P_i with $\frac{1}{\gamma_i} P_i$. Thus, from now on we shall assume $\gamma_i \in \{0, 1\}$. We next prove an analog of Claim 55.

▷ Claim 67. Let $\tilde{\mathcal{Q}}$ be a (Q_o, m_1, m_2)-set such that $\text{rank}_\text{s}(Q_o) < 100$. Then there is a subspace V of linear forms such that $\dim(V) \leq 2 \cdot 100 + 4$, $\text{Lin}(Q_o) \subseteq V$ and for at least $m_1 - 2m_2$ of the indices $j \in [m_1]$ it holds that $a_j, b_j \in V$.

Proof. Let $P = P_1$. Claim 66 implies that $P = \gamma Q_o + L$, for some L of rank 2. Set $V = \text{span}\{\text{Lin}(Q_o) \cup \text{Lin}(L)\}$. Clearly $\dim(V) \leq 2 \cdot 100 + 4$.

Let $j \in [m_1]$. If P and Q_j satisfy Theorem 5iii, then there are two linear forms c and d such that $Q_j, P \in \sqrt{\langle c, d \rangle}$, this implies that $\text{span}\{c, d\} \subset \text{Lin}(P) \subseteq V$. If $Q_o = Q_j - a_j b_j$ is not zero modulo c, d, then we obtain that $Q_o \equiv_{c,d} -a_j b_j$. Thus, there are linear forms $v_1, v_2 \in \text{Lin}(Q_o)$ such that $a_j \equiv_{c,d} v_1$ and $b_j \equiv_{c,d} v_2$. In particular, as $\text{Lin}(Q_o) \cup \{c, d\} \subset V$ it follows that $a_j, b_j \in V$. If Q_o is zero modulo c and d, then Q_j, Q_o satisfy Theorem 5iii and from property 5 of Definition 43 we know that there are at most m_2 such Q_j's. Furthermore, as $c, d \in \text{Lin}(Q_o) \subset V$ we obtain that $Q_j \in \langle V \rangle$. Denote by $\mathcal{K}$ the set of all Q_j that satisfy Theorem 5iii with Q_o. As we mentioned, $|\mathcal{K}| \leq m_2$.

If P and Q_j satisfy Theorem 5ii then there are two linear forms c and d, and non zero $\alpha, \beta \in \mathbb{C}$, such that $\alpha P + \beta Q_j = cd$. Hence,

$$\beta Q_o + \alpha P = -\beta a_j b_j + cd \ .$$

As $\beta Q_o + \alpha P$ is a non trivial linear combination of Q_o and P, we get from property 4 of Definition 43 that $2 \leq \text{rank}_\text{s}((\alpha\gamma + \beta) Q_o + \alpha L)$. It follows that

$$\text{rank}_\text{s}(-\beta a_j b_j + cd) = \text{rank}_\text{s}((\alpha\gamma + \beta) Q_o + \alpha L) = 2$$

and therefore by Fact 21,

$$\{a_j, b_j, c, d\} \subset \text{Lin}(-\beta a_j b_j + cd) = \text{Lin}((\alpha\gamma + \beta) Q_o + \alpha L) \subseteq V \ ,$$

and again $a_j, b_j \in V$.

The last case to consider is when P and Q_j satisfy Theorem 5i. If they span a polynomial $Q_{j'} \in \mathcal{Q}_1 \cup \mathcal{L}$, then $P = \alpha Q_j + \beta Q_{j'}$ and as in the previous case we get that $a_j, b_j \in V$.

Let $\mathcal{J}$ be the set of all indices $j \in [m_1]$ such that P and Q_j span a polynomial in $\mathcal{Q}_2$ but no polynomial in $\mathcal{Q}_1 \cup \mathcal{L}$. So far we proved that for every $j \in [m_1] \setminus (\mathcal{J} \cup \mathcal{K})$ we have that $a_j, b_j \in V$. We next show that $|\mathcal{J}| \leq m_2$ which concludes the proof.

Indeed, if this was not the case then by the pigeonhole principle there would exist a polynomial $P_i \in \mathcal{Q}_2$ and two polynomials $Q_j, Q_{j'} \in \mathcal{Q}_1$ such that $P_i \in \text{span}\{Q_j, P\}$ and $P_i \in \text{span}\{Q_{j'}, P\}$. By pairwise independence this implies that $Q_{j'}$ is in the linear span of P and Q_j which contradicts the definition of $\mathcal{J}$. ◁

Our next claim gives more information about the way the polynomials in $\tilde{\mathcal{Q}}$ relate to the subspace V found in Claim 67.

▷ Claim 68. Let $\tilde{\mathcal{Q}}$ and V be as in Claim 67. Then, every polynomial P in $\tilde{\mathcal{Q}}$ satisfies (at least) one of the following cases:

1. $\mathrm{Lin}(P) \subseteq V$ or
2. $P \in \langle V \rangle$ or
3. $P = P' + c(c+v)$ where P' is a quadratic polynomial such that $\mathrm{Lin}(P') \subseteq V$, $v \in V$ and c is a linear form.

Proof. Let $\mathcal{I} = \{j \in [m_1] \mid a_j, b_j \in V\}$. Claim 67 implies that $|\mathcal{I}| \geq m_1 - 2m_2$. Furthermore, by the construction of V we know that $\mathrm{Lin}(Q_o) \subseteq V$. Observe that this implies that for every $j \in \mathcal{I}$, $\mathrm{Lin}(Q_j) \subseteq V$.

Note that every polynomial in $\mathcal{L}$ satisfies the third item of the claim. Let P be any polynomial in $\mathcal{Q}_2 \cup \{Q_j \mid j \in [m_1] \setminus \mathcal{I}\}$. We study which case of Theorem 5 P satisfies with polynomials whose indices belong to $\mathcal{I}$.

If P_i satisfies Theorem 5iii with any polynomial Q_j, for $j \in \mathcal{I}$, then, as $\mathrm{Lin}(Q_j) \subseteq V$, it follows that $P \in \langle V \rangle$.

If P is spanned by two polynomials $Q_j, Q_{j'}$ such that $j, j' \in \mathcal{I}$, then clearly $\mathrm{Lin}(P) \subseteq V$. Similarly, if P is spanned by a polynomial $Q_j, Q_{j'}$ such that $j \in \mathcal{I}$ and $Q_{j'} \in \mathcal{L}$ then $P = \alpha Q_j + \beta a_{j'}^2$, and hence it also satisfies the claim.

Hence, for P to fail to satisfy the claim, it must be the case that every polynomial Q_j, for $j \in \mathcal{I}$, that satisfies Theorem 5i with P, does not span with P any polynomial in $\{Q_j \mid j \in \mathcal{I}\} \cup \mathcal{L}$. Thus, it must span with P a polynomial in $\{Q_j \mid j \in [m_1] \setminus \mathcal{I}\} \cup \mathcal{Q}_2$. As before, observe that by pairwise linear independent, if two polynomials from $\mathcal{I}$ span the same polynomial with P, then P is in their span and we are done. Thus, since

$$|\{Q_j \mid j \in [m_1] \setminus \mathcal{I}\} \cup \mathcal{Q}_2| \leq (m_1 - |\mathcal{I}|) + m_2 \leq 3m_2 < m_1 - 2m_2 - 2 \leq |\mathcal{I}| - 2 \ ,$$

for P to fail to satisfy the claim it must be the case that it satisfies Theorem 5ii with at least 2 polynomials whose indices are in $\mathcal{I}$.

Let $Q_j, Q_{j'}$ be two such polynomials. There are four linear forms, c, d, e and f and scalars $\epsilon_j, \epsilon_{j'}$ such that

$$P + \varepsilon_j Q_j = cd \qquad \text{and} \qquad P + \varepsilon_{j'} Q_{j'} = ef \ .$$

Therefore

$$\varepsilon_j Q_j - \varepsilon_{j'} Q_{j'} = cd - ef \ . \tag{15}$$

In particular, $\mathrm{Lin}(cd - ef) \subseteq V$. Claim 25 and Equation (15) imply that, without loss of generality, $d = \epsilon c + v$ for some $v \in V$ and $\epsilon \in \mathbb{C}$. Thus, $P = cd - \varepsilon_j Q_j = c(\epsilon c + v) - \varepsilon_j Q_j$ and no matter whether $\epsilon = 0$ or not. P satisfies the claim. Indeed, if $\epsilon = 0$ then $P \in \langle V \rangle$ and we are done. Otherwise, we can normalize c, v to assume that $\epsilon = 1$ and get that $\mathrm{Lin}(P - c^2) \in V$ as claimed. ◁

We can now complete the proof of Claim 60.

Proof of Claim 60. Claim 68 implies that there is a linear space of linear forms, V, such that $\dim(V) \leq 2 \cdot 100 + 4$ and every polynomial $Q_i \in \tilde{\mathcal{Q}}$ satisfies the following. Either $Q_i \in \langle V \rangle$ or, there is a linear form a_i such that $\mathrm{Lin}(Q_i) \subseteq \mathrm{span}\{V, a_i\}$. (It might be that $\mathrm{Lin}(Q_i) \subseteq V$ or that $\mathrm{Lin}(Q_i) \subseteq \mathrm{span}\{a_i\}$). Thus $\tilde{\mathcal{Q}}$ satisfies the conditions of Claim 61, and $\dim(\tilde{\mathcal{Q}}) = O(1)$, as we wanted to show.

◁

Claim 46 together with Claim 60 completes the proof of Theorem 44. ◀

5 Conclusions and future research

In this work we solved Problem 2 in the case where all the polynomials are irreducible and of degree at most 2. This result directly relates to the problem of obtaining deterministic algorithms for testing identities of $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuits. As mentioned in Section 1, in order to obtain PIT algorithms we need a colored version of this result. Formally, we need to prove the following conjecture:

▶ **Conjecture 69.** *Let $\mathcal{T}_1, \mathcal{T}_2$ and $\mathcal{T}_3$ be finite sets of homogeneous quadratic polynomials over $\mathbb{C}$ satisfying the following properties:*

- *Each $Q_o \in \cup_i \mathcal{T}_i$ is either irreducible or a square of a linear form.*[8]
- *No two polynomials are multiples of each other (i.e., every pair is linearly independent).*
- *For every two polynomials Q_1 and Q_2 from distinct sets, whenever Q_1 and Q_2 vanish then also the product of all the polynomials in the third set vanishes.*

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

We believe that tools similar to the tools developed in this paper should suffice to verify this conjecture. Another interesting question is a robust version of this problem, which is still open.

▶ **Problem 70.** *Let $\delta \in (0,1]$. Can we bound the linear dimension (as a function of δ) of a set of polynomials $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ that satisfy the following property: For every $i \in [m]$ there exist at least δm values of $j \in [m]$ such that for each such j there is $\mathcal{K}_j \subset [m]$, where $i, j \notin \mathcal{K}_j$ and $\prod_{k \in \mathcal{K}_j} Q_k \in \sqrt{\langle Q_i, Q_j \rangle}$.*

In this result, we prove that the dimension of a set of quadratic polynomials satisfying the conditions of Theorem 4 is bounded by a constant c. By carefully examining the proof, we get that $c \leq 20,000$. This is a very loose bound, and we believe it can be improved. Thus, it might be interesting to find a tight bound on the dimension, or even presenting examples for which the dimension is larger then 10.

Extending our approach to the case of more than 3 multiplication gates (or more than 3 sets as in the colored version of the Sylvester-Gallai theorem (Theorem 14)) seems more difficult. Indeed, an analog of Theorem 5 for this case seems harder to prove in the sense that there are many more cases to consider which makes it unlikely that a similar approach will continue to work as the number of gates get larger. Another difficulty is proving an analog of Theorem 5 for higher degree polynomials. Thus, we believe that a different proof approach may be needed in order to obtain PIT algorithms for $\Sigma^{[O(1)]}\Pi^{[d]}\Sigma\Pi^{[O(1)]}$ circuits.

In this paper we only considered polynomials over the complex numbers. However, we believe (though we did not check the details) that a similar approach should work over positive characteristic as well. Observe that over positive characteristic we expect the dimension of the set to scale like $O(\log |\mathcal{Q}|)$, as for such fields a weaker version of Sylvester-Gallai theorem holds.

▶ **Theorem 71** (Corollary 1.3 in [5]). *Let $V = \{\vec{v}_1, \ldots, \vec{v}_m\} \subset \mathbb{F}_p^d$ be a set of m vectors, no two of which are linearly dependent. Suppose that for every $i, j \in [m]$, there exists $k \in [m]$ such that $\vec{v}_i, \vec{v}_j, \vec{v}_k$ are linearly dependent. Then, for every $\epsilon > 0$*

$$\dim(V) \leq \text{poly}(p/\epsilon) + (4 + \epsilon) \log_p m .$$

---

[8] We replace a linear form with its square to keep the sets homogeneous of degree 2.

References

1 Manindra Agrawal. Proving lower bounds via pseudo-random generators. In Ramaswamy Ramanujam and Sandeep Sen, editors, *FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science, 25th International Conference, Hyderabad, India, December 15-18, 2005, Proceedings*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105. Springer, 2005. `doi:10.1007/11590156_6`.

2 Manindra Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 67–75. IEEE Computer Society, 2008. `doi:10.1109/FOCS.2008.32`.

3 Boaz Barak, Zeev Dvir, Avi Wigderson, and Amir Yehudayoff. Fractional sylvester–gallai theorems. *Proceedings of the National Academy of Sciences*, 110(48):19213–19219, 2013.

4 Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Inf. Comput.*, 222:2–19, 2013. `doi:10.1016/j.ic.2012.10.004`.

5 Arnab Bhattacharyya, Zeev Dvir, Shubhangi Saraf, and Amir Shpilka. Tight lower bounds for linear 2-query lccs over finite fields. *Combinatorica*, 36(1):1–36, 2016. `doi:10.1007/s00493-015-3024-z`.

6 Peter Borwein and William O. J. Moser. A survey of sylvester's problem and its generalizations. *Aequationes Mathematicae*, 40:111–135, 1990. `doi:10.1007/BF02112289`.

7 Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Hardness vs randomness for bounded depth arithmetic circuits. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*, volume 102 of *LIPIcs*, pages 13:1–13:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. `doi:10.4230/LIPIcs.CCC.2018.13`.

8 David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, 3rd edition, 2007.

9 Zeev Dvir, Shubhangi Saraf, and Avi Wigderson. Improved rank bounds for design matrices and a new proof of kelly's theorem. *CoRR*, abs/1211.0330, 2012. `arXiv:1211.0330`.

10 Zeev Dvir and Amir Shpilka. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM J. Comput.*, 36(5):1404–1434, 2007. `doi:10.1137/05063605X`.

11 Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-randomness tradeoffs for bounded depth arithmetic circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009. `doi:10.1137/080735850`.

12 Michael Edelstein and Leroy M. Kelly. Bisecants of finite collections of sets in linear spaces. *Canadian Journal of Mathematics*, 18:375–280, 1966.

13 Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. A deterministic parallel algorithm for bipartite perfect matching. *Commun. ACM*, 62(3):109–115, 2019. `doi:10.1145/3306208`.

14 Michael A. Forbes. *Polynomial identity testing of read-once oblivious algebraic branching programs.* PhD thesis, Massachusetts Institute of Technology, 2014.

15 Michael A. Forbes and Amir Shpilka. Explicit noether normalization for simultaneous conjugation via polynomial identity testing. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*, pages 527–542. Springer, 2013. `doi:10.1007/978-3-642-40328-6_37`.

16 Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving lower bounds for algebraic circuits. *Theory of Computing*, 14(1):1–45, 2018. `doi:10.4086/toc.2018.v014a018`.

17 Ankit Gupta. Algebraic geometric techniques for depth-4 PIT & sylvester-gallai conjectures for varieties. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:130, 2014. URL: `http://eccc.hpi-web.de/report/2014/130`.

18 Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi. Arithmetic circuits: A chasm at depth three. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 578–587, 2013. `doi:10.1109/FOCS.2013.68`.

19 Rohit Gurjar and Thomas Thierauf. Linear matroid intersection is in quasi-nc. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 821–830. ACM, 2017. `doi:10.1145/3055399.3055440`.

20 Joos Heintz and Claus-Peter Schnorr. Testing polynomials which are easy to compute (extended abstract). In Raymond E. Miller, Seymour Ginsburg, Walter A. Burkhard, and Richard J. Lipton, editors, *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA*, pages 262–272. ACM, 1980. `doi:10.1145/800141.804674`.

21 Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004. `doi:10.1007/s00037-004-0182-6`.

22 Zohar S. Karnin and Amir Shpilka. Reconstruction of generalized depth-3 arithmetic circuits with bounded top fan-in. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 274–285. IEEE Computer Society, 2009. `doi:10.1109/CCC.2009.18`.

23 Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testing for depth 3 circuits. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 198–207. IEEE Computer Society, 2009. `doi:10.1109/FOCS.2009.67`.

24 Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of polynomial identity testing and polynomial factorization. *Computational Complexity*, 24(2):295–331, 2015. `doi:10.1007/s00037-015-0102-y`.

25 Ketan D. Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *J. Amer. Math. Soc.*, 30(1):225–309, 2017.

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

27 Shubhangi Saraf and Ilya Volkovich. Black-box identity testing of depth-4 multilinear circuits. *Combinatorica*, 38(5):1205–1238, 2018. `doi:10.1007/s00493-016-3460-4`.

28 Nitin Saxena. Progress on polynomial identity testing. *Bulletin of EATCS*, 99:49–79, 2009. URL: `https://eccc.weizmann.ac.il/report/2009/101/`.

29 Nitin Saxena. Progress on polynomial identity testing-ii. In M. Agrawal and V. Arvind, editors, *Perspectives in Computational Complexity: The Somenath Biswas Anniversary Volume*, Progress in Computer Science and Applied Logic, pages 131–146. Springer International Publishing, 2014. URL: `https://books.google.co.il/books?id=U7ApBAAAQBAJ`.

30 Nitin Saxena and Comandur Seshadhri. Blackbox identity testing for bounded top-fanin depth-3 circuits: The field doesn't matter. *SIAM J. Comput.*, 41(5):1285–1298, 2012. `doi:10.1137/10848232`.

31 Nitin Saxena and Comandur Seshadhri. From sylvester-gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *J. ACM*, 60(5):33, 2013. `doi:10.1145/2528403`.

32 Amir Shpilka. Interpolation of depth-3 arithmetic circuits with two multiplication gates. *SIAM J. Comput.*, 38(6):2130–2161, 2009. `doi:10.1137/070694879`.

33 Amir Shpilka. Sylvester-gallai type theorems for quadratic polynomials. In Moses Charikar and Edith Cohen, editors, *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019.*, pages 1203–1214. ACM, 2019. `doi:10.1145/3313276.3316341`.

34 Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010. `doi:10.1561/0400000039`.

35 Gaurav Sinha. Reconstruction of real depth-3 circuits with top fan-in 2. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPIcs*, pages 31:1–31:53. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. `doi:10.4230/LIPIcs.CCC.2016.31`.

36 Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-nc. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 696–707. IEEE Computer Society, 2017. `doi:10.1109/FOCS.2017.70`.