Sylvester-Gallai Type Theorems for Quadratic Polynomials

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

ABSTRACT

We prove Sylvester-Gallai type theorems for quadratic polynomials. Specifically, we prove that if a finite collection $\mathcal{Q}$, of irreducible polynomials of degree at most 2, satisfy that for every two polynomials $Q_1, Q_2 \in \mathcal{Q}$ there is a third polynomial $Q_3 \in \mathcal{Q}$ so that whenever Q_1 and Q_2 vanish then also Q_3 vanishes, then the linear span of the polynomials in $\mathcal{Q}$ has dimension $O(1)$. We also prove a colored version of the theorem: If three finite sets of quadratic polynomials satisfy that for every two polynomials from distinct sets there is a polynomial in the third set satisfying the same vanishing condition then all polynomials are contained in an $O(1)$-dimensional space.

This answers affirmatively two conjectures of Gupta [Gup14] that were raised in the context of solving certain depth-4 polynomial identities.

To obtain our main theorems we prove a new result classifying the possible ways that a quadratic polynomial Q can vanish when two other quadratic polynomials vanish. Our proofs also require robust versions of a theorem of Edelstein and Kelly (that extends the Sylvester-Gallai theorem to colored sets).

CCS CONCEPTS

• **Theory of computation → Algebraic complexity theory**; *Randomness, geometry and discrete structures.*

KEYWORDS

Combinatorics, Arithmetic Circuits, polynomial identity testing

ACM Reference Format:
Amir Shpilka. 2019. Sylvester-Gallai Type Theorems for Quadratic Polynomials. In *Proceedings of the 51st Annual ACM SIGACT Symposium on the Theory of Computing (STOC '19), June 23–26, 2019, Phoenix, AZ, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3313276.3316341

1 INTRODUCTION

The Sylvester-Gallai theorem asserts that if a finite set of points 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. Many variants of this theorem were studied: extensions to higher dimensions, colored versions, robust versions and many more. For a survey on the Sylvester-Gallai theorem and its variants see [BM90]. One specific extension that is relevant to our work is the following colored version that was obtained by Edelstein and Kelly: 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, in this case too all the points belong to a low dimensional space.

Another extension of the theorem that is relevant to our work was proved in [BDYW11, DSW14]. There the authors proved the following robust version of the Sylvester-Gallai theorem (along with other robust versions of similar theorems): if a finite set of points satisfies that for every point p in the set there is a δ fraction of other points so that for each of them, the line passing through it and p, spans a third point in the set, then the set is contained in an $O(1/\delta)$-dimensional space.

While these theorems may seem unrelated to computation at first sight they have important consequences for locally decodable and locally correctable codes [BDYW11, DSW14], for reconstruction of certain depth-3 circuits [Shp09, KS09a, Sin16] and for the polynomial identity testing (PIT for short) problem, which we describe next.

The PIT problem asks to give a deterministic algorithm that given 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 both because of its intrinsic importance, its relation to other derandomization problems [KSS15, Mul17, FS13, FGT16, GT17, ST17] and its connections to lower bounds for arithmetic circuits [HS80, Agr05, KI04, DSY09, FSV17, CKS18]. For more on the PIT problem see [SY10, Sax09, Sax14, For14].

The case most relevant to Sylvester-Gallai type theorems is when the input circuit 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 following form

$$\Phi(x_1, \ldots, x_n) = \sum_{i=1}^{k} \prod_{j=1}^{d} \ell_{i,j}(x_1, \ldots, x_n)\,, \tag{1.1}$$

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 1.1 and it has 3 multiplication gates, i.e. $k = 3$. If Φ computes the zero polynomial then we have, for every $j, j' \in [d]$, that

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

As the zero set of two linear functions is an irreducible variety, we get as a consequence that for every $j, j' \in [d]$, the linear functions $\ell_{2,j}$ and $\ell_{3,j'}$ span a linear function in $\{\ell_{1,1}, \ldots, \ell_{1,d}\}$. In other

STOC '19, June 23–26, 2019, Phoenix, AZ, USA

ACM ISBN 978-1-4503-6705-9/19/06…$15.00
https://doi.org/10.1145/3313276.3316341

words, the three sets $\mathcal{T}_i = \{\ell_{i,1}, \ldots, \ell_{i,d}\}$, for $i \in \{1,2,3\}$, satisfy the conditions of the Edelstein-Kelly theorem described above,[1] and hence span a low dimensional space. Thus, if $\Phi \equiv 0$ then we can rewrite the expression for Φ using only constantly many variables (after a suitable invertible linear transformation). This allows efficient PIT algorithms for such $\Sigma^{[3]}\Pi^{[d]}\Sigma$ circuits. The case of more than 3 multiplication gates is more complicated and satisfies a similar higher dimensional condition. This rank-bound approach for PIT of $\Sigma\Pi\Sigma$ circuits was raised in [DS07] and later carried out in [KS09b, SS13].[2]

While such rank-bounds found important applications in studying PIT of depth-3 circuits, it seemed that such an approach cannot work for depth-4 $\Sigma\Pi\Sigma\Pi$ circuits,[3] even in the simplest case where there are only 3 multiplication 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

$$\Phi(\mathbf{x}) = \prod_{j=1}^{d} Q_{1,j}(\mathbf{x}) + \prod_{j=1}^{d} Q_{2,j}(\mathbf{x}) + \prod_{j=1}^{d} Q_{3,j}(\mathbf{x}), \tag{1.2}$$

where each $Q_{i,j}$ is a homogeneous quadratic polynomial. Indeed, we if try to reason as before then we get

$$\prod_{j=1}^{d} Q_{1,j}(\mathbf{x}) = 0 \mod Q_{2,j}, Q_{3,j'}. \tag{1.3}$$

However, unlike the linear case it is not clear what can be concluded now. Indeed, if a product of linear functions vanishes modulo two linear functions, then we know that one function in the product must be in the linear span of those two linear functions. For quadratic polynomials this is not necessarily the case. For example, note that if for a quadratic Q we have that $Q = 0$ and $Q + x^2 = 0$ then also $Q + xy = 0$, and, clearly, we can find Q such that $Q + xy$ is not spanned by Q and $Q + x^2$. An even more problematic difference is that it may be the case that Equation 1.3 holds but that no $Q_{1,j}$ always vanishes when, say, $Q_{2,1}, Q_{3,1}$ vanish. For example, let

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

Then, it is not hard to verify that

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

but neither Q_3 nor Q_4 vanish identically modulo Q_1, Q_2. Thus, the PIT problem for sums of products of quadratics seem much harder than the corresponding problem for depth-3 circuits. Indeed, currently no efficient deterministic PIT algorithm is known for $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuits.

In spite of the above, Beecken et al. [BMS13, Gup14] and Gupta [Gup14] conjectured that perhaps the difference between the quadratic case and the linear case is not so dramatic. In fact, they suggested that this may be the case for any constant degree and not just for quadratics. Specifically, Gupta observed that whenever Equation 1.3 holds it must be the case that there are four polynomials in $\{Q_{1,j}\}$ whose product vanishes identically. That is, 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

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

Gupta then raised the conjecture that whenever this holds for every j, j' and for every two of the multiplication gates, then it must be the case that the *algebraic* rank of the set $\{Q_{i,j}\}$ is $O(1)$. More generally, Gupta conjectured that this is the case for any fixed number of sets.

Conjecture 1.4 (Conjecture 1 in [Gup14]). *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).*

The condition in the conjecture can be stated equivalently as

$$\prod_{i=1}^{c} P_i \in \sqrt{(Q_1, \ldots, Q_{k-1})},$$

where the object on the right hand side is the radical of the ideal generated by $\{Q_i\}_{i=1}^{k-1}$ (see Section 2.1). Note that for $r = 1$ we have also $c = 1$ and by the Edelstein-Kelly theorem λ is ≤ 2 in this case (and we can replace algebraic rank with linear rank).

In [BMS13] 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 this conjecture is weaker than Gupta's as every zero $\Sigma^{[k]}\Pi^{[d]}\Sigma\Pi^{[r]}$ circuit gives rise to a structure satisfying the conditions of Gupta's conjecture, 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.

As an approach towards solving Conjecture 1.4 Gupta set up a collection of conjectures, each of which is a natural extension of a known Sylvester-Gallai type theorem for the case of higher degree polynomials. The first conjecture is a direct analog of the Sylvester-Gallai theorem where we replace the requirement that a line through two points contains a third with a more algebraic condition: that for every two polynomials there is a third one so that whenever the two polynomials vanish then also the third vanishes.

Conjecture 1.5 (Conjecture 2 of [Gup14]). *Let $Q_1, \ldots, Q_m \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible and homogenous polynomials of degree $\leq r$ such that for every pair of distinct Q_i, Q_j there is a distinct Q_k so that whenever Q_i and Q_j vanish then so does Q_k. Then $trdeg_{\mathbb{C}}(Q_1, \ldots, Q_m) \leq \lambda(r)$.*

Note that Sylvester-Gallai's theorem is equivalent to the special case $r = 1$. A more general conjecture in [Gup14] is that a similar phenomenon holds when the polynomials come from different sets.

Conjecture 1.6 (Conjecture 30 of [Gup14]). *Let R, B, G be finite disjoint sets of irreducible homogenous polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ of degree $\leq r$ such that for every pair Q_1, Q_2 from distinct sets there*

[1] The theorem speaks about line through points rather than span of vectors, but it is not hard to see how to translate the Edelstein-Kelly theorem to this setting as well. See Remark 2.7.

[2] The best algorithm for PIT of $\Sigma^{[k]}\Pi^{[d]}\Sigma$ circuits was obtained through a different, yet related, approach in [SS12].

[3] Though we note that 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 [SV11].

is a Q_3 in the remaining set so that whenever Q_1 and Q_2 vanish then also Q_3 vanishes. Then $trdeg_{\mathbb{C}}(R \cup B \cup G) \leq \lambda(r)$.[4]

The case $r = 1$ is the Edelstein-Kelly theorem. Both Conjecture 1.5 and Conjecture 1.6 were open, prior to this work, for any degree $r > 1$.

1.1 Our Results

Our main results give affirmative answers to Conjecture 1.5 and Conjecture 1.6 for the case $r = 2$. This shows that a Sylvester-Gallai type phenomenon holds for degree 2 and we believe this indicates that this might be the case for higher degrees as well. Specifically we prove the following two theorems. The first is an extension of the Sylvester-Gallai theorem to quadratic polynomials. It confirms Conjecture 1.5 for the case $r = 2$.

Theorem 1.7. *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 $O(1)$.*

The second theorem is an extension of the theorem of Edelstein-Kelly to quadratic polynomials, which gives an affirmative answer to Conjecture 1.6 for the case $r = 2$..

Theorem 1.8. *Let $\mathcal{T}_1, \mathcal{T}_2$ and $\mathcal{T}_3$ be finite sets of homogeneous quadratic polynomials over $\mathbb{C}$ satisfying the following properties:*

- *Each $Q \in \cup_i \mathcal{T}_i$ is either irreducible or a square of a linear function.*[5]
- *No two polynomials are multiples of each other (i.e., every pair is linearly independent).*
- *For every two polynomials Q_1 and Q_2 from distinct sets there is a polynomial Q_3 in the third set so that whenever Q_1 and Q_2 vanish then also Q_3 vanishes.*

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

Note that what we proved is even stronger than what was conjectured in Conjectures 1.5 and 1.6. There the conjecture is that there is an upper bound on the algebraic rank whereas our results give an upper bound on the linear rank (which of course trivially implies an upper bound on the algebraic rank).

From the perspective of PIT our results do not imply Conjecture 1.4, even for the case of $k = 3$ and $r = 2$, yet we believe they are a significant step in the direction of resolving this conjecture and obtaining a PIT algorithm for $\Sigma^{[3]}\Pi^{[d]}\Sigma\Pi^{[2]}$ circuits.

An important tool in the proof of Theorem 1.7 is a result of [BDYW11, DSW14] that gives a robust version of the Sylvester-Gallai theorem (see Section 2.2). For the proof of Theorem 1.8 we need the following relaxation of the Edelstein-Kelly theorem. Roughly, three finite sets form a δ-EK configuration if for every point p in one set a δ fraction of the points in a second set satisfy that the line connecting each of them to p passes through a point in the third set.

[4]Here and in Conjectures 1.4 and 1.5 we actually need to assume that the polynomials are pairwise linearly independent.

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

Theorem 1.9. *Let $0 < \delta \leq 1$ be any constant. Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}^n$ be disjoint finite subsets that form a δ-EK configuration. Then* $\dim(\text{span}\{\cup_i \mathcal{T}_i\}) \leq O(1/\delta^3)$.

This theorem is similar in nature to the results proved in [BDYW11, DSW14] (see Theorem 2.5) but it does not seem to directly follow from them.

1.2 Proof Idea

The basic tool in proving Theorems 1.7 and 1.8 is the following result that characterizes the different cases when a quadratic polynomial is in the radical of the ideal generated by two other quadratics, i.e., that is vanishes when the two quadratic polynomials vanish.

Theorem 1.10 (Structure Theorem)**.** *Let Q, Q_1, Q_2 be such that whenever Q_1 and Q_2 vanish then also Q vanishes. Then one of the following cases hold:*

1. *Q is in the linear span of Q_1, Q_2*
2. *There exists a non trivial linear combination of the form $\alpha Q_1 + \beta Q_2 = \ell^2$ where ℓ is a linear function*
3. *There exist two linear functions ℓ_1 and ℓ_2 such that when setting $\ell_1 = \ell_2 = 0$ we get that Q, Q_1 and Q_2 vanish.*

The theorem guarantees that unless Q is in the linear span of Q_1 and Q_2 then Q_1 and Q_2 must satisfy a very strong property, namely, they must span a square of a linear function or they have a very low rank (as quadratic polynomials). The proof of this theorem is based on analyzing the resultant of Q_1 and Q_2 with respect to some variable. We now explain how this theorem can be used to prove Theorem 1.7.

Consider a set of polynomials $\mathcal{T} = \{Q_i\}$ satisfying the condition of Theorem 1.7. If for every $Q \in \mathcal{T}$ for at least, say, $(1/100)\cdot|\mathcal{T}|$ of the polynomials $Q_i \in \mathcal{T}$ there is a another polynomial in $\text{span}(Q, Q_i)$ then the claim follows by the robust version of the Sylvester-Gallai theorem proved in [BDYW11, DSW14] (Theorem 2.5). So let us assume this is not the case. And in fact, let us assume that there are two polynomials $Q_1, Q_2 \in \mathcal{T}$ for which this does not hold. This means that at least 0.98 fraction of the polynomials in $\mathcal{T}$ satisfy Case 2 or Case 3 of Theorem 1.10 with Q_1 and Q_2. This gives very strong restriction on the structure of these $0.98 \cdot |\mathcal{T}|$ polynomials.

To use this structure we first show that the polynomials satisfying Case 2 of Theorem 1.10 with both Q_1 and Q_2 also span a low dimensional space (Claim 5.2). The intuition is that every such polynomial can be represented as both $\alpha Q_1 + \ell_1^2$ and as $\beta Q_2 + \ell_2^2$. This gives rise to many different equations involving Q_1 and Q_2. Analyzing those equations we show that all those ℓ_i span a low dimensional space.

The remaining polynomials must satisfy Case 3 of Theorem 1.10 with either Q_1 or Q_2. We then show (Claim 5.5) that, under the conditions of Theorem 1.7, all the polynomials that satisfy Case 3 of Theorem 1.10 with, say, Q_1 span a low dimensional space. The intuition is that if we map the linear functions in some "minimal" representation of Q_1 to a new variable z, then all these polynomials will be mapped to quadratics of the form $z \cdot \ell_i$. We then show that these ℓ_i's satisfy the usual Sylvester-Gallai condition and hence get a bound on their span.

The proof outline of Theorem 1.8 involves more cases, but it is still similar in spirit and is based on studying the case where our

three sets do not satisfy the robust version of the Edelstein-Kelly theorem (Theorem 1.9).

To prove Theorem 1.9 we would like to reduce to the robust version of the Sylvester-Gallai theorem proved in [BDYW11, DSW14]. For example, if all our sets are of the same size then their union forms a $\delta/3$-SG configuration (see Section 2.2) and we can conclude using the result of [BDYW11, DSW14]. Thus, the main issue is what to do when the sets are of very different sizes. When the largest set has size polynomial in the size of the smallest set then we prove that by sampling a random subset of appropriate size from the largest set and taking its union with the two other sets we again get a $\delta/6$-SG configuration. This implies that the second largest and smallest sets live in an $O(1)$-dimensional space and hence all the sets span an $O(1)$-dimensional space. The proof of the case where the largest set is much larger than the smaller set is different and is based on a completely different covering argument.

1.3 Organization

The paper is organized as follows. Section 2 contains basic facts regarding the resultant and some other basic tools and notation, including the robust version of the Sylvester-Gallai theorem of [BDYW11, DSW14]. In Section 3 we define the notion of a δ-EK configuration and prove Theorem 1.9. Section 4 contains the proof of our structure theorem (Theorem 1.10). In Section 5 we give the proof of Theorem 1.7 and in Section 6 we prove Theorem 1.8. Finally in Section 7 we discuss further directions and open problems. Due to space limitation most proofs are deferred to the full version.

2 PRELIMINARIES

In this section we explain our notation, give some basic facts from algebra that will be useful in our proofs and state a robust version of the Sylvester-Gallai theorem.

We will mostly use the following notation. Greek letters $\alpha, \beta, \ldots$ denote scalars from the field. Uncapitalized letters $a, b, c, \ldots$ denote linear functions and x, y, z denote variables (which are also linear functions). We denote $\mathbf{x} = (x_1, \ldots, x_n)$. Capital letters such as A, Q, F 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 $[n] = \{1, 2, \ldots, n\}$.

We will also need on the following version of Chernoff bound. See e.g. Theorem 4.5 in [MU05].

Theorem 2.1 (Chernoff bound). *Suppose $X_1, \ldots, X_n$ are independent indicator random variables. Let $\mu = E[X_i]$ be the expectation of X_i. Then,*

$$\Pr\left[\sum_{i=1}^{n} X_i < \frac{1}{2}n\mu\right] < \exp(-\frac{1}{8}n\mu).$$

2.1 Facts from Algebra

A notation that will convenient to use is that of a radical ideal. In this work we only consider the ring of polynomials $\mathbb{C}[\mathbf{x}]$. An ideal $I \subseteq \mathbb{C}[\mathbf{x}]$ is an abelian subgroup that is closed under multiplication by ring elements. We will denote with (Q_1, Q_2) the ideal generated by two polynomials Q_1 and Q_2. I.e. $(Q_1, Q_2) = Q_1 \cdot \mathbb{C}[\mathbf{x}] + Q_2 \cdot \mathbb{C}[\mathbf{x}]$. The radical of an ideal I, denoted $\sqrt{I}$, is the set of all ring elements f satisfying that for some natural number m, $f^m \in I$. Hilbert's Nullstellensatz implies that if a polynomial Q vanishes whenever Q_1 and Q_2 vanish then $Q \in \sqrt{(Q_1, Q_2)}$ (see e.g. [CLO07]). We shall often use the notation $Q \in \sqrt{(Q_1, Q_2)}$ to denote this vanishing condition.

A tool that will play an important role in the proof of Theorem 1.10 is the resultant of two polynomials. As we only consider quadratic polynomials in this paper we restrict our attention to resultants of such polynomials. Let $F, G \in \mathbb{C}[\mathbf{x}]$ be quadratic polynomials. View F, G as polynomials in x_1 over $\mathbb{C}(x_2, \ldots, x_n)$. I.e.

$$F = \alpha x_1^2 + a x_1 + F_0 \quad \text{and } G = \beta x_1^2 + b x_1 + G_0 \ .$$

Then, the resultant of F and G with respect to x_1 is the determinant of their Sylvester matrix

$$\mathrm{Res}_{x_1}(F, G) \triangleq \begin{vmatrix} F_0 & 0 & G_0 & 0 \\ a & F_0 & b & G_0 \\ \alpha & a & \beta & b \\ 0 & \alpha & 0 & \beta \end{vmatrix} .$$

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

Theorem 2.2 (See e.g. Proposition 8 in §5 of Chapter 3 in [CLO07]). *Given $F, G \in \mathbb{F}[x]$ of positive degree, the resultant $\mathrm{Res}_x(F, G)$ is an integer polynomial in the coefficients of F, G. Furthermore, F and G have a common factor in $\mathbb{F}[x]$ if and only if $\mathrm{Res}_x(F, G) = 0$.*

Finally, we shall define the rank of a quadratic polynomial as follows.

Definition 2.3. *For a quadratic polynomial we denote with $\mathrm{rank}_s(Q)$ the minimal r such that there are $2r$ linear functions $\{\ell_i\}_{i=1}^{2r}$ satisfying $Q = \sum_{i=1}^{r} \ell_{2i} \cdot \ell_{2i-1}$. We call such a representation a* minimal representation *of Q.* ◊

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

Claim 2.4. *Let Q be an irreducible quadratic polynomial with $\mathrm{rank}_s(Q) = r$. 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 $\mathrm{span}\{a_i\} = \mathrm{span}\{b_i\}$.*

2.2 Robust Sylvester-Gallai Theorem

We will need the following theorem of Dvir et al. [DSW14] that improves on an earlier work of Barak et al. [BDYW11].

We say that the points $v_1, \ldots, v_m$ in $\mathbb{C}^d$ form 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 2.5 (Theorem 1.9 of [DSW14]). *If $v_1, \ldots, v_m \in \mathbb{C}^d$ is a δ-SG configuration then $\dim(\mathrm{span}\{v_1, \ldots, v_m\}) \le 12/\delta$.*

An easy consequence of the theorem is the following.

Corollary 2.6. *Let $0 < \delta < 1$. Assume $v_0, v_1, \ldots, v_m \in \mathbb{C}^d$ are such that 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*

(i.e. the condition holds for all the points except, possibly, v_0). Then $\dim v_0, v_1, ..., v_m < 50/\delta$.

Remark 2.7. *In our application we will have that the span of two points contains a third point. This does not change the theorems much as by picking a random subspace H, of codimension 1, and replacing each point p with $H \cap \text{span}\{p\}$ we get that $p_3 \in \text{span}\{p_1, p_2\}$ iff $H \cap \text{span}\{p_3\}$ is on the line passing through $H \cap \text{span}\{p_1\}$ and $H \cap \text{span}\{p_2\}$.* ◊

3 ROBUST EDELSTEIN-KELLY THEOREMS

In this section we prove Theorem 1.9 as well as some extensions of it, which give robust versions of the following theorem of Edelstein and Kelly [EK66].

Theorem 3.1 (Theorem 3 of [EK66])**.** *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 is on the line passing through p_1 and p_2. Then, any such $\mathcal{T}_i$ satisfy that* $\dim(\text{span}\{\cup_i \mathcal{T}_i\}) \leq 3$.

We would be interested in the case where the requirement in the theorem holds with some positive probability. We say that the sets $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}^n$ form a δ-EK configuration if for every $i \in [3]$ and $p \in \mathcal{T}_i$, for every $j \in [3] \setminus \{i\}$ at least δ fraction of the points $p_j \in \mathcal{T}_j$ satisfy that p and p_j span some point in the third set.[6] To ease the reading we state again Theorem 1.9.

Theorem (Theorem 1.9)**.** *Let $0 < \delta \leq 1$ be any constant. Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}^n$ be disjoint finite subsets that form a δ-EK configuration. Then* $\dim(\text{span}\{\cup_i \mathcal{T}_i\}) \leq O(1/\delta^3)$.

Remark 3.2. *The bound $O(1/\delta^3)$ is probably not tight and we believe that the correct bound should be $O(1/\delta)$ but we did not try to get tight bounds here. The theorem also seems similar in spirit to the results in [BDYW11, DSW14] but as far as we can tell it is not a direct corollary of any of the results there.* ◊

Remark 3.3. *While Theorem 1.9 speaks about lines through points, a similar conclusion holds when we replace the condition that p_3 lies on the line through p_1 and p_2 with the condition $p_3 \in \text{span}\{p_1, p_2\}$.* ◊

Similar to Corollary 2.6 we have the following variant of Theorem 1.9.

Theorem 3.4. *Let $0 < \delta \leq 1$ be any constant. Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}^n$ be disjoint finite subsets. Assume that with the exception of at most c elements from $\cup_{i=1}^3 \mathcal{T}_i$ all other elements in $\cup_{i=1}^3 \mathcal{T}_i$ satisfy the δ-EK property. Then* $\dim(\text{span}\{\cup_i \mathcal{T}_i\}) \leq O_c(1/\delta^3)$.

For the proof of Theorem 1.8 we would actually need the following extension of the theorem. The extension speaks of a situation where some linear combinations fall into a subspace W and not just to one of the sets.

Theorem 3.5. *Let $0 < \delta \leq 1$ be any constant. Let $W \subset \mathbb{C}^n$ be an r-dimensional space and let $W_i \subset W$, for $i \in [3]$, be finite subsets of W. Let $\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3 \subset \mathbb{C}^n \setminus W$ be finite subsets. Let $\mathcal{T}_i = \mathcal{K}_i \cup W_i$. Assume that no two vectors in $\cup_i \mathcal{T}_i$ are linearly dependent.*

Assume that with the exception of at most c elements from $\cup_{i=1}^3 \mathcal{K}_i$ all other elements satisfy the following relaxed EK-property: If $p \in \mathcal{K}_i$ is not one of the c exceptional points then for every $j \in [3] \setminus \{i\}$, for at least δ fraction of the points $q \in \mathcal{T}_j$ the span of p and q contains a point in $\mathcal{T}_k$, for the third index k. Then, there exists a linear subspace V of dimension $\dim(V) = O_c(1/\delta^3)$ such that $\text{span}\{\cup_i \mathcal{T}_i\} \subseteq W + V$. In particular, $\dim(\text{span}\{\cup_i \mathcal{T}_i\}) \leq O_c(r + 1/\delta^3)$.

Note that the theorem assumes nothing about the relation between the size of W_i and $\mathcal{K}_i$. Furthermore, it only asks that points in $\mathcal{K}_i$ satisfy the spanning property with points from $\mathcal{T}_j = \mathcal{K}_j \cup W_j$ and that the spanned point can belong to $\mathcal{T}_k = \mathcal{K}_k \cup W_k$ and not just to $\mathcal{K}_k$.

4 STRUCTURE THEOREM FOR QUADRATICS SATISFYING $Q \in \sqrt{(Q_1, Q_2)}$

An important tool in the proofs of our main results is Theorem 1.10 that classifies all the possible cases in which a quadratic Q is in the radical of two other quadratics, where all quadratics are irreducible.

Before proving the theorem we explain the intuition behind the different cases. We would like to understand when does a quadratic polynomial Q can belong to the radical of two other quadratics. Clearly, if Q is a linear combination of Q_1, Q_2 then it is in their radical (and in fact, in their linear span). Another option is that $Q_2 = \alpha Q_1 + b^2$ and then Q can be of the form $\beta Q_1 + b \cdot a$. This case is clearly different than the linear span case. Finally, another option is the following situation: $Q_1' = xy$, $Q_2' = z(x + z)$ and $Q' = yz$. It is not hard to verify that in this case too, $Q' \in \sqrt{(Q_1', Q_2')}$. All these polynomials are reducible of course, but by defining, e.g., $Q_1 = Q_1' + Q_2'$, $Q_2 = Q_1' - Q_2'$ and $Q = Q' + Q_1' + Q_2'$ we get three irreducible polynomials that do not fall into any of the previous two cases. Thus, all the three cases are distinct and can happen. What Theorem 1.10 shows is that, essentially, these are the only possible cases.

Proof of Theorem 1.10. By applying a suitable linear transformation we can assume that for some $r \geq 1$

$$Q_1 = \sum_{i=1}^{r} x_i^2.$$

We can also assume wlog that x_1^2 appears only in Q_1 as we can replace Q_2 with any polynomial of the form $Q_2' = Q_2 - \alpha Q_1$ without affecting the result. Indeed, $Q \in \sqrt{(Q_1, Q_2)}$ if and only if $Q \in \sqrt{(Q_1, Q_2')}$. Furthermore, all cases in the theorem remain the same if we replace Q_2 with Q_2' and vice versa.

In a similar fashion we can replace Q with $Q' = Q - \beta Q_1$ to get rid of the term x_1^2 in Q. Thus, wlog, the situation is

$$\begin{aligned} Q_1 &= x_1^2 + Q_1' \\ Q_2 &= x_1 \cdot b_2 - A \\ Q &= x_1 \cdot b + B \end{aligned} \tag{4.1}$$

where Q_1', A, B, b_2 and b do not depend on x_1.

The first case we handle is when the "new" Q_2 does not depend on x_1.

Claim 4.2. *If $b_2 = 0$ then Case 2 of the theorem holds.*

[6] Note that here we use the notion of span rather than a line passing through points. However, as noted in Remark 2.7, this does not make any real difference.

Proof. For any assignment satisfying $A = 0$ there are two solutions to $Q_1 = 0$, unless $Q_1' = 0$, whereas Q vanishes for only one value of x_1. Thus, we must have $Q_1' = 0$ modulo A, which means that either A is a square of a linear function and so Q_1 and Q_2 satisfy Case 2 of the theorem (as we assume $b_2 = 0$), or $Q_1 = \alpha \cdot A$ for some nonzero constant α and then x_1^2 is in the span of Q_1 and Q_2, and again Case 2 of the theorem holds. □

We next handle the case where the "new" Q_2 is reducible.

Claim 4.3. *If b_2 divides A then the conclusion of the theorem holds.*

Proof. If b_2 divides A then $Q_2 = b_2 \cdot b_2'$. Assume that b_2' is not a constant multiple of b_2 (as otherwise Case 2 of the theorem holds). Then, after a suitable invertible linear transformation we have $Q_2 = y \cdot z$. Denote

$$Q_1 = \alpha y^2 + \beta z^2 + y \cdot \ell_1 + z \cdot \ell_2 + Q_1''$$

and

$$Q = \alpha' y^2 + \beta' z^2 + \gamma' yz + y \cdot k_1 + z \cdot k_2 + Q'',$$

where $\ell_1, \ell_2, k_1, k_2, Q_1'', Q''$ do not involve y nor z. Observe that since we can subtract a multiple of Q_2 from Q_1 we can assume that the term yz does not appear in Q_1. Consider the assignment $y = 0$. This simplifies Q_1 and Q to:

$$Q_1|_{y=0} = \beta z^2 + z \cdot \ell_2 + Q_1''$$

and

$$Q|_{y=0} = \beta' z^2 + z \cdot k_2 + Q'',$$

which are two polynomials not depending on y. We now have that any assignment that makes $Q_1|_{y=0}$ vanish, also makes $Q|_{y=0}$ vanish. In other words $Q|_{y=0} \in \sqrt{(Q_1|_{y=0})}$. This means that all irreducible factors of $Q_1|_{y=0}$ divide $Q|_{y=0}$. Thus, either $Q|_{y=0} = \delta \cdot Q_1|_{y=0}$ for some constant δ, or $Q_1|_{y=0} = b_3^2$ and $Q|_{y=0} = b_3 \cdot b_3'$ for some linear functions b_3, b_3'.

Notice that in the second case, if we set $y = b_3 = 0$ then Q_1 and Q_2 vanish and hence Q also vanishes and Case 3 of the theorem holds.

So let us assume that $Q_1|_{y=0}$ divides $Q|_{y=0}$. We repeat the same reasoning when setting $z = 0$ and again assume that $Q_1|_{z=0}$ divides $Q|_{z=0}$. By comparing coefficients we get that there are constants δ, δ' such that $\beta' = \delta\beta, k_2 = \delta\ell_2, Q'' = \delta Q_1''$ and $\alpha' = \delta'\alpha, k_1 = \delta'\ell_1, Q'' = \delta' Q_1''$. It follows that either $\delta = \delta'$ and we obtain that $Q = \delta Q_1 + \gamma' Q_2$, which satisfies Case 1 of the theorem or that $Q_1'' = Q_1 = 0$ in which case Q_1, Q_2, Q all vanish when setting $y = z = 0$ as in Case 3 of the theorem. □

Hence, from now on we assume that b_2 is non-zero and does not divide A. Consider the resultant of Q_1, Q_2 (as given in Equation 4.1) with respect to x_1. It is equal to

$$\mathrm{Res}_{x_1}(Q_1, Q_2) = A^2 + b_2^2 \cdot Q_1'. \tag{4.4}$$

We next study what happens when the resultant vanishes. I.e. when

$$\mathrm{Res}_{x_1}(Q_1, Q_2) = A^2 + b_2^2 \cdot Q_1' = 0\ . \tag{4.5}$$

Claim 4.6. *Whenever $\mathrm{Res}_{x_1}(Q_1, Q_2) = 0$ it holds that $A \cdot b + b_2 \cdot B = 0$.*

Proof. If $\mathrm{Res}_{x_1}(Q_1, Q_2) = 0$ then either $b_2 = 0$, which also implies $A = 0$ and in this case the claim clearly holds, or $b_2 \neq 0$. Consider the case $b_2 \neq 0$ and set $x_1 = A/b_2$ (we are free to select a value for x_1 as $\mathrm{Res}_{x_1}(Q_1, Q_2)$ does not involve x_1). Notice that for this substitution we have that $Q_2 = 0$ and that

$$Q_1|_{x_1 = A/b_2} = (A/b_2)^2 + Q_1' = \mathrm{Res}_{x_1}(Q_1, Q_2)/b_2^2 = 0.$$

Hence, we also have $Q|_{x_1 = A/b_2} = 0$. In other words that

$$A \cdot b + b_2 \cdot B = 0.$$

□

In other words, Claim 4.6 implies that

$$A \cdot b + b_2 \cdot B \in \sqrt{(\mathrm{Res}_{x_1}(Q_1, Q_2))}.$$

Thus, there exists an integer k and a polynomial ψ so that

$$(A \cdot b + b_2 \cdot B)^k = \psi \cdot \mathrm{Res}_{x_1}(Q_1, Q_2) = \psi \cdot (A^2 + b_2^2 \cdot Q_1').$$

This means that all irreducible factors of $A^2 + b_2^2 \cdot Q_1'$ divide $A \cdot b + b_2 \cdot B$. As $\deg(A^2 + b_2^2 \cdot Q_1') = 4$ and $\deg(A \cdot b + b_2 \cdot B) = 3$ it follows, by examining the possible ways that a degree 4 polynomial can factor, that one of the following cases must hold:

(1) There is a quadratic polynomial C and a linear function a such that

$$A^2 + b_2^2 \cdot Q_1' = C^2$$
$$b \cdot A + b_2 \cdot B = a \cdot C$$

(2) For some scalar λ, a linear function a and a quadratic C

$$A^2 + b_2^2 \cdot Q_1' = a^2 \cdot C \tag{4.7}$$
$$b \cdot A + b_2 \cdot B = \lambda \cdot a \cdot C$$

We next handle each of these cases.

Case 1: we have that

$$b_2^2 \cdot Q_1' = C^2 - A^2 = (C + A)(C - A).$$

If Q_1' is irreducible then $\alpha b_2^2 = (C + A)$ and $Q_1' = \alpha(C - A)$, or $\alpha b_2^2 = (C - A)$ and $Q_1' = \alpha(C + A)$ for some $\alpha \neq 0$. In the first case we get that $Q_1' = -2\alpha A + \alpha^2 b_2^2$ and hence $Q_1 + 2\alpha Q_2 = (x + \alpha b_2)^2$. Similarly, in the second case we get $Q_1' = 2\alpha A + \alpha^2 b_2^2$ and thus $Q_1 - 2\alpha Q_2 = (x - \alpha b_2)^2$. In either cases, Case 2 of the theorem holds.

If Q_1' is reducible, i.e. $Q_1' = e \cdot f$, then either the analysis above continues to hold or it must be the case that (w.l.o.g.) $C + A = b_2 \cdot e$ and $C - A = b_2 \cdot f$. It follows that in this case b_2 divides A and we are done by Claim 4.3.

Case 2: From Equation 4.7 we learn that $a^2 | \mathrm{Res}_{x_1}(Q_1, Q_2)$ so in particular, when setting $a = 0$ we get that the resultant is zero. Theorem 2.2 implies that, modulo a, either one of Q_1, Q_2 vanishes, or that Q_1 and Q_2 share a linear factor.

As a does not involve x_1, clearly $Q_1|_{a=0} \neq 0$. Further, for Q_2 to vanish modulo a we need that b_2 is a multiple of a, and vice versa. This implies that b_2 divides A and we are done by Claim 4.3.

We thus have to deal with the case that, modulo a, Q_1 and Q_2 share a linear factor. Let a' be that common linear factor.

We get that by setting $a = a' = 0$ both Q_1 and Q_2 vanish and hence also Q vanishes and Case 3 of the theorem holds.

This concludes the proof of Theorem 1.10. □

5 SYLVESTER-GALLAI THEOREM FOR QUADRATIC POLYNOMIALS

In this section we prove Theorem 1.7. For convenience we repeat the statement of the theorem.

Theorem (Theorem 1.7). *Let $\{Q_i\}_{i\in[m]}$ be homogeneous quadratic polynomials 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 $Q_k \in \sqrt{(Q_i, Q_j)}$. Then the linear span of the Q_i's has dimension $O(1)$.*

Remark 5.1. *The requirement that the polynomials are homogeneous is not essential as homogenization does not affect the property $Q_k \in \sqrt{(Q_i, Q_j)}$.* ◊

5.1 Some Useful Claims

In this section we look at some implications of Theorem 1.10. We do so by considering two irreducible polynomials Q_1 and Q_2 and consider sets of polynomials that satisfy Case 2 or Case 3 of Theorem 1.10 with Q_1 and Q_2.

Claim 5.2. *Let Q_1, Q_2 be two linearly independent quadratic polynomials and let $F_1, \ldots, F_m$ be quadratic polynomials such that for every i there exist linear functions ℓ_i, b_i and a scalar β_i so that*

$$F_i = Q_1 + \ell_i^2 = \beta_i \cdot Q_2 + b_i^2. \tag{5.3}$$

Then, there exists a 4-dimensional space V such that for every i, $\{\ell_i, b_i\} \subseteq V$.

Corollary 5.4. *Under the hypothesis of Claim 5.2, there exist four linear functions a_1, a_2, a_3, a_4 such that every F_i is a linear combination of $Q_1, \{a_i \cdot a_j\}_{i\leq j}$.*

Claim 5.5. *Let $F_1, \ldots, F_{m'}$ be quadratics in our set[7] that satisfy Case 3 of Theorem 1.10 with an irreducible Q. Then there exists an $O(1)$-dimensional space V such that each F_i is a quadratic polynomial in the linear functions in V.*

Proof. As Q satisfies Case 3 of Theorem 1.10 and is irreducible it follows that $\text{rank}_s(Q) = 2$ (recall Definition 2.3). Thus, Q is a quadratic polynomial in at most 4 linear functions. Let V to be the space spanned by the linear functions in a minimal representation of Q. By Claim 2.4 it follows that V is well defined. Clearly $\dim(V) \leq 4$.

Let z be a new variable. Set each basis element of V to a random multiple of z (say by picking the multiples independently uniformly at random from $[0,1]$). Each F_i now becomes $z \cdot b_i$ for some nonzero b_i. Indeed, if we further set $z = 0$ then all linear functions in the representation of Q vanish and hence also F_i vanishes (this again follows from Claim 2.4). Further, $b_i \neq 0$ as we mapped the basis elements to random multiples of z. We next show that unless all linear functions in the minimal representation of F_i, F_j are in V then F_i, F_j remain linearly independent after this restriction.

[7] I.e. they are a subset of the $\{Q_i\}$ from the statement of Theorem 1.7.

Claim 5.6. *Let V be a linear space of linear functions. Let $F = v_1 \cdot \ell_1 + v_2 \cdot \ell_2$ and $G = v_3 \cdot \ell_3 + v_4 \cdot \ell_4$ be two linearly independent irreducible quadratics, where for every i, $v_i \in V$. If $\text{span}\{\ell_1, \ldots, \ell_4\} \not\subseteq V$ then with probability 1, F and G remain linearly independent even after we map the basis elements of V to random multiples of a new variable z (say, by picking the multiples uniformly and independently from the segment $[0,1]$).*

We postpone the proof of Claim 5.6 and continue with the proof of Claim 5.5. We next show that the linear functions $\{b_i\}_i \cup \{z\}$ satisfy the "usual" Sylvester-Gallai condition, i.e., that any two of them span a third function in the set (with the possible exception of z). In fact, we will add to this set all quadratics in our set that are now of the form $z \cdot \ell$ for a linear ℓ.

Consider two quadratics $Q_1 = zb_1, Q_2 = zb_2$ so that neither b_1 nor b_2 is a multiple of z. If $\{b_1, b_2\}$ span z then we are done. Otherwise, assume that Q_3 vanishes when Q_1 and Q_2 vanish. Then clearly z divides Q_3. Thus $Q_3 = zb_3$ and b_3 is in our set. Further, when we set $b_1 = b_2 = 0$ both Q_1 and Q_2 vanish and hence Q_3 vanishes as well. Since $z \notin \text{span}\{b_1, b_2\}$ this implies that $b_3 \in \text{span}\{b_1, b_2\}$ and in this case too b_1 and b_2 span a third linear function in $\{b_i\}_i \cup \{z\}$. Note also that, by Claim 5.6, b_3 is not a multiple of b_1 nor of b_2 as this would imply that Q_3 and Q_1 (or Q_2) are linearly dependent in contradiction to our assumption.

From Corollary 2.6 (recalling Remark 2.7) we get that the dimension of all those $\{b_i\}_i$ is $O(1)$.

We now repeat the same argument again for a different random mapping of the basis elements of V to multiples of z. As before each F_i is mapped to a polynomial of the form $z \cdot b_i'$ and again the dimension of $\{b_i'\}_i$ is $O(1)$. Let U be the subspace containing the span of $V \cup \{b_i\}_i \cup \{b_i'\}_i$. Clearly $\dim(U) = O(1)$. We next show that every F_i is a polynomial in the linear functions in U. Indeed, let $F = v_1 \cdot u_1 + v_2 \cdot u_2$ be arbitrary polynomial from $\{F_i\}_i$, where $v_1, v_2 \in V$. Assume the first mapping mapped $v_i \mapsto \alpha_i \cdot z$ and the second mapping is $v_i \mapsto \beta_i \cdot z$. Then, F was mapped to $z \cdot b$ under the first mapping where $b = \alpha_1 u_1 + \alpha_2 u_2$ and to $z \cdot b'$ under the second mapping where $b' = \beta_1 u_1 + \beta_2 u_2$. As $\alpha_1, \alpha_2, \beta_1, \beta_2$ where chosen uniformly independently at random from $[0,1]$ it follows that the determinant

$$\left\| \begin{bmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{bmatrix} \right\| \neq 0$$

and hence $u_1, u_2 \in \text{span}\{b, b'\} \subseteq U$. As we also have $v_1, v_2 \in V \subseteq U$ the claim follows.

This concludes the proof of Claim 5.5. □

We now give the proof of Claim 5.6.

Proof of Claim 5.6 . Let $x_1, \ldots, x_k$, for some $1 \leq k \leq 4$ be a basis for $\text{span}\{\ell_1, \ldots, \ell_4\}$ such that for some $0 < t \leq k$, $x_{t+1}, \ldots, x_k$ for a basis to $\text{span}\{\ell_1, \ldots, \ell_4\} \cap V$. We can rewrite F and G as

$$F = \sum_{i=1}^{t} x_i u_i + F' \quad \text{and} \quad G = \sum_{i=1}^{t} x_i w_i + G'$$

where $u_i, w_i \in V$ and F', G' are defined over V, and, w.l.o.g., for every i, at least one of u_i and w_i is nonzero. Observe that F and G are linearly independent (over $\mathbb{C}$) if and only if the two vectors

$$u_F = (u_1, \ldots, u_t, F') \quad \text{and} \quad w_G = (w_1, \ldots, w_t, G')$$

are linearly independent over $\mathbb{C}(V)$, the function field generated by adding the linear functions in V to $\mathbb{C}$. Indeed, if F and G are linearly dependent over $\mathbb{C}$ then clearly u_F and w_G are linearly dependent over $\mathbb{C}$, and hence over $\mathbb{C}(V)$. If on the other hand u_F and w_G are linearly dependent over $\mathbb{C}(V)$ then this means that for some polynomials $f(V)$ and $g(V)$ we have

$$f \cdot (u_1, \ldots, u_t, F') = g \cdot (w_1, \ldots, w_t, G').$$

This implies that all the 2×2 determinants vanish, i.e. that $u_i \cdot w_j - u_j \cdot w_i = 0$, for every i and j, and $u_i \cdot G' - w_i \cdot F' = 0$. By unique factorization we get that there are two possible cases:

(1) There is $\alpha \in \mathbb{C}$ so that $u_i = \alpha w_i$ for some i: The equality $u_i \cdot w_j - u_j \cdot w_i = 0$ implies that for every j we actually have $u_j = \alpha w_j$, and the fact that $u_i \cdot G' - w_i \cdot F' = 0$ gives $F' = \alpha G'$ and thus u_F and w_G are linearly dependent over $\mathbb{C}$ and indeed F and G are linearly dependent.
(2) There are constants α_i such that for every i, $u_i = \alpha_i u_1$ and $w_i = \alpha_i w_1$: In this case, since F is irreducible, it holds that u_1 does not divide F'. As $u_1 \cdot G' - w_1 \cdot F' = 0$, by unique factorization it follows that u_1 is a multiple of w_1 and we are thus in the previous case again.

It therefore follows that the matrix

$$M = \begin{bmatrix} u_1 & \ldots & u_j & F' \\ w_1 & \ldots & w_j & G' \end{bmatrix}$$

is full rank over $\mathbb{C}(V)$. Thus the determinant of[8] $M \cdot M^\dagger$ is a nonzero polynomial over V. The Schwartz-Zippel-DeMillo-Lipton lemma now implies that sending each basis element of V to a random multiple of z will make the determinant nonzero with probability 1. This also means that F and G remain linear independent after such mapping. □

5.2 The Proof

We are now ready to prove Theorem 1.7. The proof follows the outline sketched in Section 1.2 and it relies on the claims proved in Section 5.1 and on Corollary 2.6.

Proof of Theorem 1.7. 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. Denote $|\mathcal{Q}| = m_1$.

We next focus on polynomials in $\mathcal{Q}$. We prove that they are contained in an $O(1)$-dimensional space of a special form.

Call a polynomial $Q \in \mathcal{Q}$ bad if there are less than, say, $m_1/100$ pairs $(Q_1, Q_2) \in \mathcal{Q} \times \mathcal{Q}$ so that $Q_2 \in \sqrt{(Q, Q_1)}$ and Q, Q_1 satisfy item 1 of Theorem 1.10 (i.e. Q_2 is in their linear span). If $Q \in \mathcal{Q}$ is not bad then we call it a good polynomial. We handle two cases according to whether there is at most one bad polynomial or more than that.

(1) **There is at most one bad polynomial:**
In this case, from Corollary 2.6 we get that the linear span of the polynomials in $\mathcal{Q}$ has dimension $O(1)$.
Assume $Q_1, \ldots, Q_k$ for some $k = O(1)$ span $\mathcal{Q}$. We now repeat the following process. We start with $\mathcal{I} = \{Q_1, \ldots, Q_k\}$ and $V = \emptyset$. If there is some nontrivial linear combination of the polynomials in $\mathcal{I}$ that is equal to a quadratic of the form $a_1 b_1 + a_2 b_2$, where a_i, b_i are linear functions then we add a_1, a_2, b_1, b_2 to V and remove one of the polynomials that participated in the linear combination from $\mathcal{I}$. We continue doing so according to the following rule. If there exists a linear combination of the polynomials in $\mathcal{I}$ that is equal to a polynomial of the form $F(V) + ab + a'b'$, where $F(V)$ is a quadratic polynomial over linear functions in V, then we add a, b, a', b' to V and remove some polynomial participating in the linear combination from $\mathcal{I}$. We do so until no such linear combination exists or until $\mathcal{I}$ is empty. At the end $|V| \leq 4k = O(1)$. Abusing notation we now think of V as the space spanned by the linear functions in it. Clearly $\dim(V) \leq 4k = O(1)$.
It remains to bound the dimension of $\mathcal{L}$. The next claim guarantees that the space spanned by the linear functions in $\mathcal{L}$ has small dimension, thus completing the proof for the case where there is at most one bad polynomial.

Claim 5.7. *Let $\mathcal{Q} \cup \mathcal{L}$ satisfy the assumption of Theorem 1.7 where*
(a) *$\mathcal{Q}$ consists of irreducible quadratics.*
(b) *There is a set of polynomials $\mathcal{I}$ and an $O(1)$-dimensional space V such that every polynomial in $\mathcal{Q}$ is in the linear span of $\mathcal{I}$ and quadratics over V. Furthermore, no nonzero linear combination of the polynomials in $\mathcal{I}$ can be expressed as $xa + yb + F(V)$ where F is any quadratic over V and x, a, b, y are any four linear forms.*
(c) *$\mathcal{L}$ is a set of squares of linear functions.*
Then, the dimension of the space spanned by the functions whose squares are in $\mathcal{L}$ has dimension $O(1)$.

Note that the conditions in the claim are satisfied by our $\mathcal{I}, V, \mathcal{Q}$ and $\mathcal{L}$.

Proof. Denote $\mathcal{L}' = \mathcal{L} \setminus V$. We shall prove that the linear functions in $\mathcal{L}'$ satisfy the Sylvester-Gallai condition and hence their span has dimension $O(1)$ as claimed.
Let $x, y \in \mathcal{L}'$. Let Q be such that $Q \in \sqrt{(x, y)}$. Thus, there exist linear functions a, b so that $Q = xa + yb$. We next consider two cases for Q.
If $Q \in \mathcal{Q}$ then $Q = Q' + G(V)$, where Q' is a linear combination of the polynomials in $\mathcal{I}$. In particular, $Q' = xa + yb - G(V)$. This implies that $Q' = 0$ as otherwise we get a contradiction to the assumptions on $\mathcal{I}$ and V. Hence, $xa + yb = Q = G(V)$. As Q is irreducible it must hold that $x, y \in V$ (by Claim 2.4). This is in contradiction to the definition of $\mathcal{L}'$.
The remaining case is when $Q \in \mathcal{L}$. Thus, $Q = \ell^2$ for some linear ℓ, and it follows that $\ell \in \text{span}\{x, y\}$. Note however that we may have $\ell \in V$. To overcome this we apply a random projection to the linear functions in V so that they are all equal to some multiple of a new variable z. As before it is not hard to see that even after this projection any two linear functions from $\mathcal{L}'$ are projected to linearly independent linear functions. Hence, in the case above, there is a third linear function in $\mathcal{L}' \cup \{z\}$ that is spanned by x, y. It follows that $\mathcal{L}' \cup \{z\}$ satisfy the conditions of Corollary 2.6 (with, say, $\delta = 1/2$) and hence $\dim(\mathcal{L}') = O(1)$ as claimed. □

[8] $M^\dagger$ is the conjugate transpose of M.

This completes the proof for the case when there is at most one bad polynomial. We handle the other case next.

(2) **There are at least two bad polynomials:**

Claim 5.8 (At least two bad polynomials)**.** *If $\mathcal{Q}$ contains at least two bad polynomials, Q_1 and Q_2, then there is a space V of linear functions of dimension $O(1)$ so that every polynomial in $\mathcal{Q}$ is a linear combination of Q_1 and a quadratic over V.*

Proof. Notice that for Q_1 there are $0.99m_1$ polynomials in $\mathcal{Q}$ that even together with Q_1 do not span any other polynomial in $\mathcal{Q}$. The same holds for Q_2. Consider a polynomial Q_j so that Q_1 and Q_j do not span any other polynomial in $\mathcal{Q}$. We conclude that Q_1 and Q_j satisfy Case 2 or Case 3 of Theorem 1.10. Indeed, if Q_1 and Q_j satisfy item 1 of Theorem 1.10 then they span some polynomial in $\mathcal{L}$ and in particular they span a square, but this means that they also satisfy Case 2 of Theorem 1.10.

From the discussion above it follows that there are at least $0.98m_1$ polynomials in $\mathcal{Q}$ satisfying Case 2 or Case 3 of the theorem with Q_1 and Q_2. Let $\mathcal{F}$ be the set of these polynomials. Partition $\mathcal{F}$ to three sets $\mathcal{I}, \mathcal{J}, \mathcal{K}$ so that those polynomials in $\mathcal{I}$ satisfy Case 3 of Theorem 1.10 with with Q_1, those in $\mathcal{J}$ satisfy Case 3 of Theorem 1.10 with Q_2 and those in $\mathcal{K}$ satisfy Case 2 of Theorem 1.10 with both Q_1 and Q_2. From Corollary 5.4 and Claim 5.5 we conclude that there is a an $O(1)$-dimensional space V' of linear functions such that all those $0.98m_1$ polynomials are in the linear span of quadratics over V' and Q_1.
To simplify things further, if it is the case that $Q_1 = F(V') + aa' + bb'$, i.e. that Q_1 can be written as a quadratic over V' plus two products of linear forms, then we add a, a', b, b' to V' and we do not consider Q_1 any more.[9]
We now consider the remaining $0.02m_1$ polynomials in $\mathcal{Q}$. In fact, consider those polynomials that cannot be spanned by quadratics over V' and Q_1 and call this set $\mathcal{F}^c$ (abusing notation).

Claim 5.9. *For each $Q \in \mathcal{F}^c$ there are at least $0.96m_1$ polynomials in $\mathcal{F}$ that satisfy either Case 2 or Case 3 of Theorem 1.10 with Q.*

Proof. If Q and $F \in \mathcal{F}$ span a polynomial in $\mathcal{L}$ then we say that Q satisfies Case 2 with F. Thus, if Q and $F \in \mathcal{F}$ satisfy item 1 of Theorem 1.10 then the third polynomial is not in $\mathcal{F}$ (as by switching sides we will get that Q is also in $\mathcal{F}$). Hence, this polynomial must be in $\mathcal{F}^c$. Assume that Q' is this polynomial. Notice that there is no other $F' \in \mathcal{F}$ that together with Q spans Q' as in such a case Q would be in $\mathcal{F}$. Indeed, let $\alpha_1 Q + F = Q'$ and $\alpha_2 Q + F' = Q'$. Since F and F' are linearly independent we get that $0 \neq (\alpha_1 - \alpha_2)Q = F' - F$ in contradiction to the assumption that Q is in $\mathcal{F}^c$. Thus, Q can satisfy item 1 of Theorem 1.10 with at most $|\mathcal{F}^c| \leq 0.02m_1$ polynomials. It follows that there are at least $0.96m_1$ polynomials in $\mathcal{F}$ that satisfy either Case 2 or Case 3 of Theorem 1.10 with Q. □

[9] This step is not crucial at this point, it just makes some later argument a bit simpler.

Let $\mathcal{I}'$ be the set of all $Q \in \mathcal{F}^c$ that satisfy Case 3 of Theorem 1.10 with any polynomial in $\mathcal{F}$. Let $\mathcal{J}'$ be the remaining polynomials in $\mathcal{F}^c$. I.e. $\mathcal{J}'$ are those polynomials in $\mathcal{F}^c$ that satisfy Case 2 of Theorem 1.10 with all polynomial in $\mathcal{F}$.
Consider a polynomial $Q \in \mathcal{J}'$. Let $F_1, F_2 \in \mathcal{F}$. Then, after rescaling, there are a_1, a_2 so that $Q + a_1^2 = F_1$ and $Q + a_2^2 = F_2$. Hence, $a_1^2 - a_2^2 = F_2 - F_1$. As $F_2 - F_1$ is a linear combination of Q_1 and quadratics over V', it must be the case that $F_2 - F_1$ are defined over V' alone as otherwise we would have replaces Q_1 with two linear functions as described above. Thus, $a_1^2 - a_2^2 = F(V')$ and it follows that $a_1, a_2 \in V'$ and hence $Q \in \mathcal{F}$ in contradiction.
We now deal with the polynomials in $\mathcal{I}'$. By an argument similar to the proof of Claim 5.5 it follows that there is an $O(1)$-dimensional space of linear functions, V'' such that all polynomials in $\mathcal{I}'$ are quadratics over V'': We send V' to a random multiple of a new variable z. This makes all polynomials in $\mathcal{I}'$ to be of the form zb_i and as before the linear functions $\{b_i\}_i \cup \{z\}$ satisfy the usual Sylvester-Gallai condition and we conclude using Corollary 2.6 (as in the proof of Claim 5.5 we repeat this twice for two independent mappings etc.). Set V be the span of $V'' \cup V'$. This completes the proof of Claim 5.8 □

It remains to bound the dimension of $\mathcal{L}$. This however, follows immediately from Claim 5.7.
This concludes the proof of the case of two bad polynomials and with it the proof of Theorem 1.7.

□

6 EDELSTEIN-KELLY THEOREM FOR QUADRATIC POLYNOMIALS

In this section we prove Theorem 1.8. We repeat its statement for convenience.

Theorem (Theorem 1.8)**.** *Let $\mathcal{T}_1, \mathcal{T}_2$ and $\mathcal{T}_3$ be finite sets of homogeneous quadratic polynomials over $\mathbb{C}$ satisfying the following properties:*

- *Each $Q \in \cup_i \mathcal{T}_i$ is either irreducible or a square of a linear function.*
- *No two polynomials are multiples of each other (i.e., every pair is linearly independent).*
- *For every two polynomials Q_1 and Q_2 from distinct sets there is a polynomial Q_3 in the third set such that $Q_3 \in \sqrt{(Q_1, Q_2)}$.*

Then the linear span of the polynomials in $\cup_i \mathcal{T}_i$'s has dimension $O(1)$.

Remark 6.1. *As before, the requirement that the polynomials are homogeneous is without lost of generality as homogenization does not affect the property $Q_k \in \sqrt{(Q_i, Q_j)}$.* ◊

The proof follows a similar outline to the proof of Theorem 1.7.

Proof of Theorem 1.8. Partition the polynomials in each $\mathcal{T}_i$ to two sets. Let $\mathcal{L}_i$ be the set of all squares and $\mathcal{Q}_i$ be the rest. Denote $|\mathcal{Q}_i| = m_i$.

Call a polynomial $Q \in \mathcal{Q}_1$ bad for $\mathcal{Q}_2$ if there are less than $m_2/100$ polynomials $Q_2 \in \mathcal{Q}_2$ so that $\text{span}\{Q, Q_2\}$ contains a polynomial from $\mathcal{Q}_3$, i.e., Q and Q_2 satisfy Case 1 of Theorem 1.10 (but not

Case 2). We say that $Q \in \mathcal{Q}_1$ is bad for $\mathcal{Q}_3$ if the equivalent condition is satisfied. We say $Q \in \mathcal{Q}_1$ is bad if it is bad for both $\mathcal{Q}_2$ and $\mathcal{Q}_3$. We call the polynomials in $\mathcal{Q}_2, \mathcal{Q}_3$ bad and good in a similar way.

We handle two cases according to whether there is at most one bad polynomial for each $\mathcal{Q}_i$ or not.

(1) **There is at most one bad polynomial for each Q_j:** In this case, in a similar fashion to the first case of Theorem 1.7, we get from Theorem 3.4 that the linear span of the polynomials in $\mathcal{Q} \triangleq \mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{Q}_3$ has dimension $O(1)$.
As in the proof of Theorem 1.7 we next extend the bound to also include the linear functions in $\cup_i \mathcal{T}_i$. Assume $Q_1, \ldots, Q_k$ for some $k = O(1)$ span $\mathcal{Q}$. We now repeat the following process. We start with $\mathcal{I} = \{Q_1, \ldots, Q_k\}$ and $V = \emptyset$. If there is some nontrivial linear combination of the polynomials in I that is equal to a quadratic of the form $F(V) + a_1 b_1 + a_2 b_2$, where a_i, b_i are linear functions then we add a_1, a_2, b_1, b_2 to V and remove one of the polynomials that participated in the linear combination from $\mathcal{I}$. We continue doing so until no such linear combination exists or until $\mathcal{I}$ is empty. At the end $|V| \leq 4k = O(1)$. As before we abuse notation and think of V as the linear space spanned by the linear functions in it. It remains to bound the dimension of $\mathcal{L} \triangleq \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$. We do so in a similar fashion to the proof of Claim 5.7. Denote $\mathcal{L}' = \mathcal{L} \setminus V$.
First, we apply a random projection to the linear functions in V so that they are all equal to some multiple of z. We next show that the set $\mathcal{L}' \cup \{z\}$ satisfies the Sylvester-Gallai condition and hence its dimension is $O(1)$ as needed (we abuse notation and denote with $\mathcal{L}'$ the projection of $\mathcal{L}'$, which, as before, still consists of pairwise independent linear functions).
Let $x, y \in \mathcal{L}'$ come from two different $\mathcal{L}_i$. Let Q be such that $Q \in \sqrt{(x, y)}$. If $Q \in \mathcal{Q}$ then $Q = Q' + G(z)$, where Q' is a linear combination of the polynomials in $\mathcal{I}$. Note however, that by definition of V, Q' must be zero as otherwise we would have a linear combination of small rank and then the set $\mathcal{I}$ would be different. Hence, $Q = G(z)$. It follows that $z \in \text{span}\{x, y\}$ and so x, y, z are linearly dependent as required. If, on the other hand, $Q \in \mathcal{L}$ then $Q = \ell^2$ and it follows that $\ell \in \text{span}\{x, y\}$. In either case, there is a third linear function in $\mathcal{L}' \cup \{z\}$ that is spanned by x, y as claimed. Note that if $\mathcal{L} \subseteq \mathcal{L}_i$ for some i then we easily conclude this case by picking any $x \in \mathcal{L}$ and any Q in a different set and as above conclude that $x \in \text{span}\{z\}$.

(2) **There are at least two bad polynomial for some Q_j:** To ease notation assume w.l.o.g. that there are at least two bad polynomials for $\mathcal{Q}_3$. The next claim gives something similar to the first part in the proof of Claim 5.8.

Claim 6.2. *Assume $Q_1, Q_2 \in \mathcal{Q}_1 \cup \mathcal{Q}_2$ are bad for $\mathcal{Q}_3$, then there is a space V of linear functions of dimension $O(1)$ so that at least $0.98m_3$ of the polynomials in $\mathcal{Q}_3$ are in the linear span of Q_1 and quadratic polynomials over V.*

Proof. Notice that for Q_1 there are $0.99m_3$ polynomials in $Q' \in \mathcal{Q}_3$ that even together with Q_1 do not span any other polynomial in $\mathcal{Q}_2$. The same holds for Q_2. Consider a polynomial $Q' \in \mathcal{Q}_3$ so that Q_1 and Q' do not span any other polynomial in $\mathcal{Q}_2$. We conclude that Q_1, Q' satisfy Case 2 or Case 3 of Theorem 1.10. Indeed, if Q_1 and Q' satisfy item 1 of Theorem 1.10 then they span some polynomial in $\mathcal{L}_2$ and in particular they span a square of a linear function, but this means that they also satisfy Case 2 of Theorem 1.10.

From the discussion above it follows that there are at least $0.98m_3$ polynomials in $\mathcal{Q}_3$ satisfying Case 2 or Case 3 of the theorem with Q_1 and Q_2. Let $\mathcal{F}_3$ be the set of these polynomials in $\mathcal{Q}_3$. We partition $\mathcal{F}_3$ to three sets $\mathcal{I}_3, \mathcal{J}_3, \mathcal{K}_3$ so that those polynomials in $\mathcal{I}_3$ satisfy Case 3 of Theorem 1.10 with Q_1, those in $\mathcal{J}_3$ satisfy Case 3 of Theorem 1.10 with Q_2 and those in $\mathcal{K}_3$ satisfy Case 2 of Theorem 1.10 with both Q_1 and Q_2. As before we would like to apply Corollary 5.4 and Claim 5.5 to conclude that there is a an $O(1)$-dimensional space V' of linear functions such that all those $0.98m_3$ polynomials of $\mathcal{F}_3$ are in the linear span of quadratics over V' and Q_1. The only problem is that the proof of Claim 5.5 should be tailored to the colored case, which is what we do next (indeed, Claim 5.2 can be applied without any changes and therefore also Corollary 5.4).
Note that if $Q \in \mathcal{Q}_1$ satisfies Case 3 of Theorem 1.10 with some polynomial in $\mathcal{Q}_3$ then it also satisfies the same case with a polynomial in $\mathcal{Q}_2$.

Claim 6.3. *Let $\mathcal{I}_2 \subseteq \mathcal{Q}_2$ and $\mathcal{I}_3 \subseteq \mathcal{Q}_3$ be irreducible quadratics that satisfy Case 3 of Theorem 1.10 with an irreducible $Q \in \mathcal{Q}_1$. Then, there exists an $O(1)$-dimensional space V such that all polynomials in $\mathcal{I}_2 \cup \mathcal{I}_3$ are quadratic polynomials in the linear functions in V.*

We defer the proof of the claim to the full version of the paper and continue with the proof of Claim 6.2. By applying Claim 6.3 first to $\mathcal{I}_3$ and then to $\mathcal{J}_3$ we conclude that $\mathcal{I}_3 \cup \mathcal{J}_3$ are quadratics over a set of $O(1)$ linear functions V. Corollary 5.4 implies that every quadratic in $\mathcal{K}_3$ is in the linear span of Q_1 and quadratics over an $O(1)$-sized set V'. combining V and V' the claim follows. This completes the proof of Claim 6.2. □

Let V be the $O(1)$-dimensional space and $\mathcal{F}_3 \subseteq \mathcal{Q}_3$ the set of polynomials guaranteed by Claim 6.2.
To continue we again have to consider two cases. The first is when there are two polynomials that are bad for $\mathcal{Q}_1$ or for $\mathcal{Q}_2$ (so far we assumed there are at least two bad polynomials for $\mathcal{Q}_3$). The second case is when at most one polynomial is bad for $\mathcal{Q}_1$ and at most one polynomial is bad for $\mathcal{Q}_2$.

(a) **There are two bad polynomials for some $\mathcal{Q}_i$, $i \in [2]$:** Assume w.l.o.g. that $i = 2$. As before Claim 6.2 implies that there is a polynomial Q_2 and an $O(1)$-dimensional space U such that $0.98m_2$ of the polynomials in $\mathcal{Q}_2$ are in the linear span of Q_2 and quadratics over U. Call those polynomials $\mathcal{F}_2$. Let $W = U + V$ be an $O(1)$-dimensional space containing both U and V.
We now check whether there is any nontrivial linear combination of Q_1 and Q_2 that is of the form $a \cdot b + a' \cdot b' + F(W)$. If such a combination exists then we add a, a', b, b' to W

(and abusing notation call the new sets W as well) and replace one polynomial that appeared in this combination with the other. I.e. if Q_2 appeared in such a combination then we think of the space that is spanned by Q_1 and W rather than by Q_2 and W. We continue to do so once again if necessary.

Assume further, w.l.o.g., that $|\mathcal{Q}_2| \geq |\mathcal{Q}_3|$. Partition the set $\mathcal{Q}_1$ to three sets $\mathcal{I}, \mathcal{J}, \mathcal{K}$ so that:

$$\text{Each } Q \in \mathcal{I} \text{ satisfies Case 3 of Theorem 1.10 with at least one polynomial in } \mathcal{F}_2. \tag{6.4}$$

$$\text{Each } Q \in \mathcal{J} \text{ satisfies Case 2 of Theorem 1.10 with at least two polynomials in } \mathcal{F}_2. \tag{6.5}$$

$$\text{Each } Q \in \mathcal{K} \text{ satisfies Case 1 of Theorem 1.10 with all except possibly one polynomial in } \mathcal{F}_2. \tag{6.6}$$

Claim 6.7. *With the notation above we prove the following claims.*

(i) *The linear span of all polynomials in $\mathcal{I}$ has dimension $O(1)$.*
(ii) *All polynomials in $\mathcal{J}$ are polynomials over W.*
(iii) *All polynomials in $\mathcal{K}$ are in the linear span of Q_1, Q_2 and quadratics over W.*

Proof. The proof of item 2(a)i follows exactly as in Claim 6.3.

To show item 2(a)ii we proceed as in the discussion following the proof of Claim 5.9. Consider a polynomial $Q \in \mathcal{J}$. Let $F_1, F_2 \in \mathcal{Q}_2$ satisfy Case 2 of Theorem 1.10 with Q. Then, after rescaling, there are a_1, a_2 so that $Q + a_1^2 = F_1$ and $Q + a_2^2 = F_2$. Hence, $a_1^2 - a_2^2 = F_2 - F_1$. As $F_2 - F_1$ is a linear combination of Q and quadratics over W, it must be the case that $F_2 - F_1$ are defined over W alone as otherwise we would have replaced Q_2 with two linear functions as described above. Thus, $a_1^2 - a_2^2 = F(W)$ and it follows that $a_1, a_2 \in W$ and hence Q is a polynomial over W.

Finally, to prove item 2(a)iii we note that for every $Q \in \mathcal{K}$ there are at least $0.98m_2 - 1$ polynomials $Q_2 \in \mathcal{F}_2$ so that for each of them there is $Q_3 \in \mathcal{Q}_3 \cap \text{span}\{Q, Q_2\}$. If there exists such a combination where $Q_3 \in \mathcal{F}_3$ then it follows that Q is a linear combination of Q_1, Q_2 and quadratics over W (as all polynomials in $\mathcal{F}_2$ and $\mathcal{F}_3$ are). If we always get $Q_3 \notin \mathcal{F}_3$ then as $|\mathcal{Q}_3 \setminus \mathcal{F}_3| \leq 0.02m_3 \leq 0.02m_2 < (1/2) \cdot |\mathcal{F}_2|$ there exist $Q_2, Q_2' \in \mathcal{F}_2$ and $Q_3 \in \mathcal{Q}_3$ so that $Q_3 \in \text{span}\{Q, Q_2\}, \text{span}\{Q, Q_2'\}$. As every two polynomials in our set are linearly independent this implies that $Q \in \text{span}\{Q_2, Q_2'\}$, and in particular it is in the span of Q_2 and quadratics over W, as claimed. □

A similar argument will now show that $\mathcal{Q}_2$ and $\mathcal{Q}_3$ are also contained in an $O(1)$-dimensional space. We thus showed that there is an $O(1)$-dimensional space containing all polynomials in $\mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{Q}_3$. It remains to bound the dimension of the linear functions in $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$. This can be done at exactly the same way as before. This concludes the proof of Theorem 1.8 in this case.

(b) **At most one polynomial is bad for $\mathcal{Q}_1$ and at most one polynomial is bad for $\mathcal{Q}_2$**

In this case we reduce to the extended robust Edelstein-Kelly theorem (Theorem 3.5).

For each $i \in [2]$ partition $\mathcal{Q}_i$ to $\mathcal{I}_i, \mathcal{J}_i$ and $\mathcal{K}_i$ as in Equation 6.4 except that we now consider $\mathcal{F}_3$ instead of $\mathcal{F}_2$ when partitioning. It follows, exactly as in the proof of Claim 6.7, that there is an $O(1)$-dimensional space U that all polynomials in $\mathcal{I}_1 \cup \mathcal{J}_1 \cup \mathcal{I}_2 \cup \mathcal{J}_2$ are in the linear span of Q_1 and quadratics over U.

Let W be the space spanned by Q_1 and quadratics over U. Clearly $\dim(W) = O(1)$.

For $i \in [2]$ let $\mathcal{K}_i' \subset \mathcal{K}_i$ be those polynomials in $\mathcal{K}_i$ that are not in W. Similarly, define $K_3' \subset \mathcal{Q}_3$. Let $W_i = W \cap \mathcal{Q}_i$, for $i \in [3]$.

We now observe that the sets $\mathcal{Q}_1 = \mathcal{K}_1' \cup W_1, \mathcal{Q}_2 = \mathcal{K}_2' \cup W_2, \mathcal{Q}_3 = \mathcal{K}_3' \cup W_3$ satisfy the conditions in the statement of Theorem 3.5 (where the $\mathcal{K}_i$ in the statement of the theorem is our $\mathcal{K}_i'$), with parameters $r = O(1)$, $c = 2$ and $\delta = 1/100$, when we identify our quadratic polynomials with their vectors of coefficients.

Indeed, as we are in the case where there is at most one bad polynomial for $\mathcal{Q}_1$ and at most one bad polynomial for $\mathcal{Q}_2$ we see that there are at most 2 "exceptional" vectors defined that way. Furthermore, from the definition of $\mathcal{K}_1', \mathcal{K}_2'$ (Equation 6.4) no point in them is "exceptional" when considering $\mathcal{Q}_3$.

Thus, Theorem 3.5 guarantees the existence of a space Y of dimension $O_c(r + 1/\delta^3) = O(1)$ that spans all vectors in the set $\mathcal{Q}_1 \cup \mathcal{Q}_2 \cup \mathcal{Q}_3$. We are almost done - we still have to deal with the linear function in $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$. This however is done exactly as before.

This completes the proof of Theorem 1.8 (modulo the proof of Claim 6.3 that we give next). □

7 CONCLUSIONS AND FUTURE RESEARCH

In this work we proved analogs of theorems of Sylvester-Gallai and Edelstein-Kelly for quadratic polynomials. These results directly relate 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 even stronger extensions of these results - something in the line of Conjecture 1.4 that was proposed by Gupta [Gup14].

It is quite likely that Theorems 1.7 and 1.8 could be extended to obtain a positive answer to Conjecture 1.4 for $r = 2$ and $k = 3$. Indeed, there is an analog of Theorem 1.10 that suits the condition of the conjecture (for $r = 2$ and $k = 3$). Peleg [Pel19] used this extension of Theorem 1.10 to extend the result of Theorem 1.7 to the case that for every Q_i and Q_j it holds that whenever they vanish the product of the other Q_k's vanishes as well. This is a significant step towards resolving Conjecture 1.4 (for $r = 2$ and $k = 3$).

However, extending our approach to the case of more than 3 multiplication gates (or more than 3 sets as in Theorem 1.8) seems more challenging. Indeed, the structure theorem gets more complicated in the sense that there are many more cases to consider and it seems unlikely that a similar approach will work for "higher values

of 3". Similarly, while proving a structural theorem for degree 3 polynomials is possible, it seems that extending the exact same approach to significantly higher degrees may be less easy. 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.

Another interesting question is, stated vaguely, understanding the conditions under which we get a Sylvester-Gallai kind of behavior. By now many variants of the theorem are known: The original Sylvester-Gallai theorem, the colored version of it (Edelstein-Kelly theorem), robust versions of it (by [BDYW11, DSW14]), extensions to subspaces [DH16], k-wise dependencies [Han65, BDYW11], our results for quadratic polynomials and more. It is an intriguing question whether there is a common generalization of all these cases or some framework that contain all these different results.

ACKNOWLEDGEMENTS

I would like to thank Shir Peleg for helpful discussions and Ankit Gupta for commenting on an earlier version of the paper. Part of this work was done while the author was visiting NYU. 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.

REFERENCES

[Agr05] 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.

[BDYW11] Boaz Barak, Zeev Dvir, Amir Yehudayoff, and Avi Wigderson. Rank bounds for design matrices with applications toc ombinatorial geometry and locally correctable codes. In Fortnow and Vadhan [FV11], pages 519–528.

[BM90] Peter Borwein and William O. J. Moser. A survey of Sylvester's problem and its generalizations. *Aequationes Mathematicae*, 40:111–135, 1990.

[BMS13] Malte Beecken, Johannes Mittmann, and Nitin Saxena. Algebraic independence and blackbox identity testing. *Inf. Comput.*, 222:2–19, 2013.

[CKS18] 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 fuer Informatik, 2018.

[CLO07] 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.

[DH16] Zeev Dvir and Guangda Hu. Sylvester-Gallai for Arrangements of Subspaces. *Discrete & Computational Geometry*, 56(4):940–965, 2016.

[DS07] 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.

[DSW14] Zeev Dvir, Shubhangi Saraf, and Avi Wigderson. Improved rank bounds for design matrices and a new proof of Kelly's theorem. *Forum of Mathematics, Sigma*, 2, 2014. Pre-print available at `arXiv:1211.0330`.

[DSY09] Zeev Dvir, Amir Shpilka, and Amir Yehudayoff. Hardness-Randomness Tradeoffs for Bounded Depth Arithmetic Circuits. *SIAM J. Comput.*, 39(4):1279–1293, 2009.

[EK66] Michael Edelstein and Leroy M. Kelly. Bisecants of finite collections of sets in linear spaces. *Canadanian Journal of Mathematics*, 18:375–280, 1966.

[FGT16] Stephen A. Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite perfect matching is in quasi-NC. In Daniel Wichs and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 754–763. ACM, 2016.

[For14] Michael A. Forbes. *Polynomial identity testing of read-once oblivious algebraic branching programs*. PhD thesis, Massachusetts Institute of Technology, 2014.

[FS13] 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.

[FSV17] Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving algebraic circuits lower bounds. In Hatami et al. [HMK17], pages 653–664.

[FV11] Lance Fortnow and Salil P. Vadhan, editors. *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*. ACM, 2011.

[GT17] Rohit Gurjar and Thomas Thierauf. Linear matroid intersection is in quasi-NC. In Hatami et al. [HMK17], pages 821–830.

[Gup14] Ankit Gupta. Algebraic Geometric Techniques for Depth-4 PIT & Sylvester-Gallai Conjectures for Varieties. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:130, 2014.

[Han65] Sten Hansen. A generalization of a theorem of Sylvester on the lines determined by a finite point set. *Mathematica Scandinavica*, 16:175–180, 1965.

[HMK17] 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*. ACM, 2017.

[HS80] Joos Heintz and Claus-Peter Schnorr. Testing Polynomials which Are Easy to Compute (Extended Abstract). In *Proceedings of the 12th annual STOC*, pages 262–272, 1980.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[KS09a] Zohar Shay 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.

[KS09b] 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.

[KSS15] Swastik Kopparty, Shubhangi Saraf, and Amir Shpilka. Equivalence of Polynomial Identity Testing and Polynomial Factorization. *Computational Complexity*, 24(2):295–331, 2015.

[MU05] Michael Mitzenmacher and Eli Upfal. *Probability and Computing – Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

[Mul17] Ketan D. Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *J. Amer. Math. Soc.*, 30(1):225–309, 2017.

[Pel19] Shir Peleg. Sylvester-Gallai type theorem for quadratic polynomials. Master's thesis, Tel Aviv University, 2019.

[Sax09] Nitin Saxena. Progress on polynomial identity testing. *Bulletin of EATCS*, 99:49–79, 2009.

[Sax14] 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.

[Shp09] Amir Shpilka. Interpolation of Depth-3 Arithmetic Circuits with Two Multiplication Gates. *SIAM J. Comput.*, 38(6):2130–2161, 2009.

[Sin16] 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.

[SS12] Nitin Saxena and C. Seshadhri. Blackbox Identity Testing for Bounded Top-Fanin Depth-3 Circuits: The Field Doesn't Matter. *SIAM J. Comput.*, 41(5):1285–1298, 2012.

[SS13] Nitin Saxena and C. Seshadhri. From Sylvester-Gallai configurations to rank bounds: Improved blackbox identity test for depth-3 circuits. *J. ACM*, 60(5):33, 2013.

[ST17] 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.

[SV11] Shubhangi Saraf and Ilya Volkovich. Black-box identity testing of depth-4 multilinear circuits. In Fortnow and Vadhan [FV11], pages 421–430.

[SY10] 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.