On Polynomial Identity Testing for depth-4 bounded top & bottom fanin circuits SG approach

Devansh Shringi

Advisor: Prof. Nitin Saxena

December 8, 2020

Contents

Chapter 1

Notation and Definitions

We use $\mathbb{F}$ to represent fields. We will mainly be working with function fields, and the variables will be denoted mainly by $x_1, \ldots, x_n$ with n denoting the number of indeterminants. $\mathbb{F}[x_1, \ldots, x_n]$ will denote the polynomial ring over $\mathbb{F}$. Polynomials are usually denoted by $f_1, \ldots, f_m$, with m denoting the number of polynomials. Arithmetic circuits are the most natural and standard model for computing polynomials and we will be using these to represent polynomials. We use the following definition of Arithmetic circuits

Definition 1.1. (Arithmetic circuits) An arithmetic circuit C over the field $\mathbb{F}$ and the set of variables $x_1, \ldots, x_n$ is a directed acyclic graph as follows. The vertices of C are called gates. Every gate of C of in-degree 0 is labelled by either a variable or a field element. Every other gate is labelled by either $+$ or $\times$. An edge is labelled with field constants, which is 1 by default.

An arithmetic circuit computes a polynomial in a natural way : An input gate labeled by $\alpha \in \mathbb{F} \cup \{x_1, \ldots, x_n\}$ computes the polynomial α. A product gate (gate with label $\times$) computes the product of the polynomials computed by its children. Similarly a sum gate (gate with label $+$) computes the sum of the polynomials computed by its children. An example of an arithmetic circuit is given below.

We define the *size* of an arithmetic circuit to be the number of edges in the graph. We define the *depth* of a gate to be the length of the longest directed path to it. The depth of a circuit is the maximal depth of a gate in it. We refer to the input degree of a gate as its *fanin*, and output degree of a gate as its *fanout*. We can also see an arithmetic circuit as layers of $+$ and $\times$ gates, as consecutive $+$ or consecutive $\times$ gates can be combined just by increasing the fanin. Hence, a depth3 circuit is frequently represented as $\Sigma\Pi\Sigma$ or $\Pi\Sigma\Pi$. The fanins are often written in superscript, for eg., $\Sigma^k\Pi\Sigma$ represents depth3 circuit with top gate fanin k.

As we saw in the model of arithmetic circuits, the two main resources are size and depth. Based on size, we define class VP as the family of circuits $\{C_n\}$ computing polynomials such that n is number of variables , degree and size of the circuit is bounded by $poly(n)$. The class is the arithmetic analog of P. For more details in the algebraic complexity area, refer to the survey [SY10].

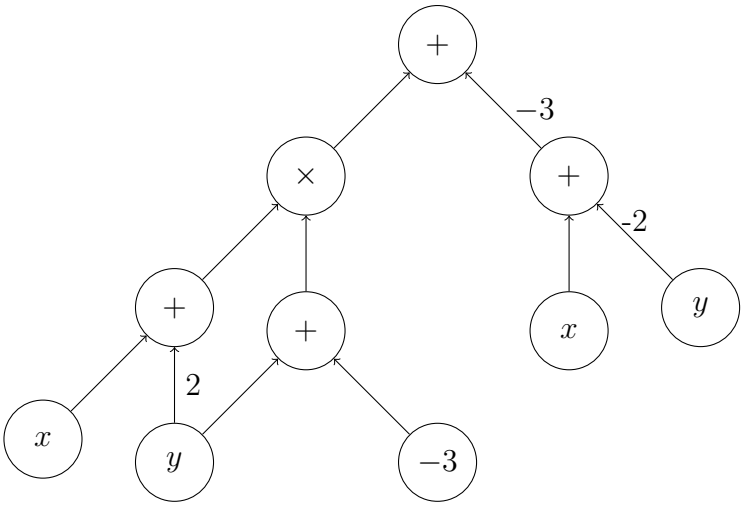

Figure 1.1: Circuit computing $xy + 2y^2$

We will further need a few definitions of a few terms which we give below.

Definition 1.2. (Ideal) The ideal generated by $f_1, \ldots, f_k$ is the set $\{\sum_i h_i \cdot f_i : h_1, \ldots, h_k \in \mathbb{F}[x_1, \ldots, x_n]\}$ and denoted by $\langle f_1, \ldots, f_k \rangle$.

We will denote the quotient ring of an ideal by $\mathbb{F}[x_1, \ldots, x_n]/I$. We will use I_d to denote the polynomials in I of degree d.

Definition 1.3. (Radical) The radical of an ideal I is the set $\{g \in \mathbb{F}[x_1, \ldots, x_n] : g^e \in I \text{ for some integer } e \geq 1\}$ and is denoted by $\sqrt{I}$.

There many different definitions of *variety* but we will be using the following in this report

Definition 1.4. (Variety) The variety of a set of polynomials $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ is the set of all their common zeroes in $\mathbb{F}^n$,i.e. the set $\{(a_1, \ldots, a_n) \in \mathbb{F}^n : f_1(a_1, \ldots, a_n) = \ldots = f_k(a_1, \ldots, a_n) = 0\}$. It is denoted by $V(f_1, \ldots, f_k)$.

Chapter 2

Introduction

2.1 The Problem

In this report we will be studying the problem of Polynomial Identity Testing (PIT). It is the problem in which we are given a polynomial as an arithmetic circuit $C(\mathbf{x})$, over a ring R, to efficiently test whether the C is identically zero. In this report we will focus on the case of R being a field. By efficient we mean the algorithm should run in $poly(size(C))$ many $\mathbb{F}$ operations. The problem is trivial if the polynomial is given as a vector of coefficients, for which we only need to check if any of the coefficient is non-zero. It also has an easy solution for univariate polynomials, which requires it to be evaluated at $degree + 1$ many points, and it is an identity iff all the evaluations are zero. This method doesn't work for multivariate polynomials, as there can be infinite solution for a simple bivariate polynomial (eg. $xy = 0$ over $\mathbb{R}$). There are 2 versions to this problem, Blackbox PIT and Whitebox PIT. In the Blackbox version, we are only allowed evaluations of C at points from $\mathbb{F}^n$, and cannot look inside the computations at inner gates. In the whitebox version we have access to the inner gates of C. Let us give formal definition of the problem

Definition 2.1.1. [For14] **(Polynomial Identity Testing)** Let $\mathcal{C}$ be a class of circuits having $size \leq s$, which computes polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of degree $< d$. The PIT problem for this class $\mathcal{C}$ asks for a deterministic algorithm to test whether a polynomial f_C, computed by a circuit $\mathbb{C} \in \mathcal{C}$, is identically zero or not. The algorithm is considered efficient if it uses only $poly(s, n, d)\mathbb{F}$ operations.

Definition 2.1.2. [For14] **(Hitting Set)** Let $\mathcal{C}$ be a class of circuits having $size \leq s$, which compute polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of degree $< d$. A Hitting set $\mathcal{H} \subseteq \mathbb{F}^n$ for the circuit class $\mathcal{C}$ is a set of points such that if a circuit $C \in \mathcal{C}$ computes a non-zero polynomial f_C, then $\exists(\alpha_1, \ldots, \alpha_n) \in \mathcal{H}$ such that $f(\alpha_1, \ldots, \alpha_n) \neq 0$.

From it's definition giving a $poly(s, n, d)$ sized Hitting set for a circuit class $\mathcal{C}$, gives an efficient blackbox PIT for $\mathcal{C}$. It is notable that the problem of PIT has a very simple and elegant randomized solution thanks to the PIT lemma.

Lemma 2.1.1. ***(PIT Lemma)****(Schwartz-Zippel[Sch80]) Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a non-zero polynomial of total degree $d \geq 0$. Let S be any finite subset of $\mathbb{F}$, and let $\alpha_1, \ldots, \alpha_n$ be*

elements selected independently, uniformly and randomly from S. Then,

$$Pr_{\alpha_1,\ldots,\alpha_n \in S}[f(\alpha_1,\ldots,\alpha_n) = 0] \leq \frac{d}{|S|}$$

The above lemma can be easily proved inductively, with the base case being the univariate case. This puts PIT in $coRP$. The problem of derandomizing PIT, so as to put it in P is still open. One trivial derandomization is to check $(d+1)^n$ many points, but is inefficient. It is formally stated below

Lemma 2.1.2. ***(Combinatorial Nullstellensatz)****[AT99] Let $f \in \mathbb{F}[x_1,\ldots,x_n]$ be a non-zero polynomial of individual degree d. Let S be a set of distinct values of size $> d$. Then, there exists $(\alpha_1,\ldots,\alpha_n) \in S^n$ such that $f(\alpha_1,\ldots,\alpha_n) \neq 0$.*

We will look in this report at a special case where the circuits will be have depth 4. As per results in [AV08], solving the problem for depth4 circuits gives us solution for PIT of all circuits in VP. Therefore, we look at an even more restricted case with the top and bottom fanin are also just $O(1)$. The depth 4 circuits can be of two types $\Sigma\Pi\Sigma\Pi$ and $\Pi\Sigma\Pi\Sigma$. The case of $\Pi\Sigma\Pi\Sigma$ is reduced to simply checking the smaller $\Sigma\Pi\Sigma$ circuits which multiply in the final multiplication gate, which itself is a different problem of depth-3 circuits. Hence, we look at only inputs of the form $\Sigma^k\Pi\Sigma\Pi^r$, where $k \geq 3 = O(1)$ and $r \geq 2 = O(1)$. The case of $k = 2$ is solved in whitebox case by division of the common factors in both terms and just comparing the left constants (as $\mathbb{F}[x_1,\ldots,x_n]$ is Unique Factorization Domain). The Blackbox case for the problem is open for even $k = 2$. While, the case of $r = 1$ is the case of depth-3 constant top fanin which is discussed in section 3.1. Let us give a formal definition of the bounded case:

Consider the input circuit be C such that it has a form $C = \Sigma^k\Pi\Sigma\Pi^r$, i.e. the circuit has alternate $+$ and $\times$ gates where the fanin of the top $+$ gate is $\leq k$ and the fanin of the bottom $\times$ gate is $\leq r$. Such a circuit C computes the polynomial of the form

$$C(x_1,\ldots,x_n) = \sum_{i=1}^{k} T_i = \sum_{i=1}^{k} \prod_{j=1}^{d_i} L_{ij}$$

where d_i is the fanin of the i^{th} $\times$ gate on the second level. The circuit is said to be *simple* if $gcd(T_1,\ldots,T_k) = 1$. It is *minimal* if no proper subset of $T's$ sum upto 0, i.e. for every $\phi \subset A \subset [k] : \sum_{i\in A} T_i \neq 0$. We assume the input circuit to be simple and minimal as if it's not simple it breaks into 2 different smaller simpler circuits by taking out the gcd from all terms, and if it's not minimal we can decrease the top fan-in. To even simplify the circuits further we assume that it is a *homogeneous* circuit, i.e. all the $T_i's$ are homogeneous of the same degree (and therefore L_{ij} are homogeneous).

2.2 The Motivation

The problem of PIT has many applications like the problem of deciding existence of perfect matching in a graph efficiently can be seen as a question of finding efficient PIT algorithm

for the determinant polynomial of the graph's Tutte matrix. The idea of PIT was also very useful in the proof of the complexity result $IP = PSPACE$. Even the problem of Primality testing was solved by working with a PIT formulation. It was observed that a positive integer n is prime iff $(x+1)^n = (x^n+1)(mod n)$, which can be considered as checking $P(x) = (x+1)^n - (x^n+1)$ to be identity over $\mathbb{Z}/n\mathbb{Z}$. The problem of derandomizing PIT has relations to complexity results like $PIT \in P \implies NEXP \not\subseteq P/poly$ or $VP \neq VNP$. For more details into PIT and it's application, look at the surveys [Sax09], [Sax14] and [SY10].

The depth reduction results in algebraic complexity have brought the computation of any polynomial in VP to computation by circuits of just depth3. The case of depth3 bounded top fanin case has been solved for both whitebox version in [KS07] and blackbox in [SS12]. Also by results in [AV08], an efficient hsg for $\Sigma^s \wedge^{\omega(1)} \Sigma^s \Pi^{O(\log s)}$ gives an $n^{O(\log n)}$-hsg for VP. Thus, this is one of the open cases near the general case but is also close to already solved cases.

Chapter 3

Previous Work

We will have look at the work done in [Gup14] where he proposes conjectures about Sylvester-Gallai Type theorems that can solve the problem completely. Some of these conjectures have been proven for Quadratic polynomials(case $k = 3$) recently in the papers [Shp19], [PS20a]. Also, proving one such conjecture in [PS20b] gave a poly-time algorithm for the case of $\Sigma^3\Pi\Sigma\Pi^2$ circuits. We will discuss in great details the development of Sylvester Gallai Type theorems in the next section. But, before we will look at how they give us PIT algorithms.

3.1 Sylvester-Gallai Theorems

Sylvester-Gallai theorem is a famous theorem in incidence geometry, which is stated below

Theorem 3.1.1. *Given a finite number of non-collinear points S in the plane $\mathbb{R}^2$, there always exists a line which passes through exactly two points in S.*

The above has a simple proof from geometry. It has a higher dimensional generalization that says:

Theorem 3.1.2. *Let S be a finite set of points spanning an affine space $V \subseteq \mathbb{R}^n$ such that $dim(V) \geq 2t$. Then, there exists $(t+1)$ points in S that span a t dimensional affine space $H \subset V$ such that $|H \cap S| = t + 1$.*

The case of depth3 PIT algorithm led to development of lot of new techniques. Karin and Shplika showed that if we have a rank bound of $R(k, d)$ for minimal,simple $\Sigma\Pi\Sigma(n, k, d)$ identities then we have a blackbox PIT algorithm with $poly(n, d^{R(k,d)})$ many field operations. By *rank* of a depth3 circuit we mean the dimension of the vector space spanned by the linear polynomials that appear int he multiplication terms. In [DS07] it was showed that a minimal and simple depth-3 identity has rank at most $\log^k d$. Sylvester-Gallai theorems were used in attempts to get a good bound on the rank of identities. In the case of depth3 circuits The space S is the set of all linear forms that appear in the circuit, hence $dim(V) = rank(C)$. Kayal and Saraf [KS09] used Theorem 3.1.2 to get a bound on the rank of minimal,simple $\Sigma\Pi\Sigma(n, k, d)$ identity.

3.2 SG Theorem relation to depth-4 PIT

We will look at the work done by Gupta in [Gup14] to solve the case of PIT of depth 4 bounded top and bottom fanin circuits. It gives solution to the special case when one of the terms T_i doesn't lie in the radical generated by other terms . For the other cases, which is referred to as the *Sylvester-Gallai* configuration, he proposes conjectures for higher degree polynomials with bounds on transcendence degree similar to the results known for linear polynomials and their rank. We first define the Sylvester-Gallai configuration of the PIT depth4 case.

Definition 3.2.1. (SG-$\Sigma^k\Pi\Sigma\Pi^r$ circuits A simple, minimal, homogeneous $\Sigma^k\Pi\Sigma\Pi^r$ circuit is SG if

$$\forall i \in [k] \bigcap_{j\in[k]\setminus\{i\}} V(T_j) \subseteq V(T_i)$$

By Hilbert's Nullstellensatz, over $\mathbb{C}$ this equivalent to

$$\forall i \in [k] \qquad T_i \in \sqrt{\langle T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_k\rangle}$$

Gupta in his paper gave an algorithm to identify if a depth4 circuit is an SG circuit or not for circuits that work in the Complex field($\mathbb{C}$). If a circuit is an identity the sum of all terms is zero,so we know $\forall i \in [k], T_i \in \langle T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_k\rangle$, and hence definitely lie in it's radical. Thus, all Identities are SG circuits, but the reverse is not true. Gupta gives an algorithm to identify the cases of non-identity in which one of the terms doesn't lie in the radical generated by other terms, i.e. without the loss of generality we have $T_k \notin \sqrt{\langle T_1, \ldots, T_{k-1}\rangle}$. The proof is based on the following proposition:

Proposition 3.2.2. Let $P_1, \ldots, P_d, L_1, \ldots, L_k \in \mathbb{C}[x_1, \ldots, x_n]$ be homogeneous and degree of each L_i is at most r. Then,

$$P_1 \cdots P_d \in \sqrt{\langle L_1, \ldots, L_k\rangle} \iff \exists\{i_1, \ldots, i_{r^k}\} \subseteq [d] : P_{i_1} \cdots P_{i_{r^k}} \in \sqrt{\langle L_1, \ldots, L_k\rangle}$$

Proof: The reverse direction of the proof is obvious from the definition of radical of an ideal. For the forward direction assume, $V_1 \cup V_2 \cup \ldots \cup V_t$ be the minimal decomposition of $V(L_1, \ldots, L_k)$ where V_i's are irreducible. Then by Nullstellensatz,

$$V_1 \cup V_2 \cup \ldots \cup V_t \subseteq V(P_1) \cup \ldots \cup V(P_d)$$

As V_i's are irreducible, we have that for each i there is an $i_j \in [d]$ such that $V_i \subseteq V(P_{i_j})$. Therefore

$$V(L_1, \ldots, L_k) = V_1 \cup V_2 \cup \ldots \cup V_t \subseteq V(P_{i_1}) \cup \ldots \cup V(P_{i_t})$$

which by Nullstellensatz means $P_{i_1} \cdots P_{i_t} \in \sqrt{\langle L_1, \ldots, L_k \rangle}$. The number of irreducible components of a variety is bounded by it's cumulative degree which is the sum of all it's irreducible components. By Bezout's Theorem, cumulative degree of $V(L_1, \ldots, L_k)$ is at most $\Pi_i deg(L_i)$. Hence, $t \leq r^k$. In simpler words the proposition says that if a product of polynomials lies inside the radical generated by k polynomials of degree atmost r, then the product of the elements of a subset of size r^k from the product will also lie in radical. This enables us to create whitebox algorithm straight by checking all r^k subsets, which since both r and k are constant will be polynomial in d and also there products degree will be small$(= r^{k+1})$. For the blackbox algorithm of the same Gupta proves that radical non-membership is preserved under random linear projections, which allows to decrease the number of variables and hence gives us a poly sized hitting set.

For the SG-circuit, he proposes that the transcendence degree $(trdeg)$ is small$(O(1))$. We state the conjecture below

Conjecture 3.2.3. Let $T_1, \ldots, T_k$ be finite sets of irreducible homogeneous polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ of degree $\leq r$ st. $\cap_i T_i = \phi$ and for every $k-1 L_1, \ldots, L_{k-1}$, each from a distinct set T_j being the remaining set st. $T_j \in \sqrt{\langle L_1, \ldots, L_{k-1} \rangle}$. Then, $trdeg_{\mathbb{C}}(\cup_i T_i) \leq \lambda(k, r)$ for some function λ.

The above is true for $r = 1$ and was first proved in [KS09]. He further proposed simpler conjectures to solve in which he proposed instead of product, individual polynomials to lie in the radical, and another one in which he took out the elements being from distinct set(colored version) condition. He says that these could function as stepping stones in proving the main conjecture.

Currently, Sylvester Gallai theorems have only been proved for the case of $k = 3$ and $r = 2$. We will have a look at these theorems and their proof ideas in the next chapter. Then, we will have a look at a possible way to extend these theorems to cubic polynomials.

Chapter 4

Sylvester Gallai Type theorems for Quadratics

4.1 SG Theorem variants known for Quadratics

Here are the basic Sylvester Gallai Type theorems proved for the Quadratic polynomials when $k = 3$ in [Shp19], [PS20a] and [PS20b].

Theorem 4.1.1. ***(Kelly's Theorem for Quadratics)****[Shp19]: 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 $i \neq j, \exists k \neq i and k \neq j$ such that $Q_k \in \sqrt{\langle Q_i, Q_j\rangle}$. Then the linear span of the Q_i's has a dimension $O(1)$.*

Theorem 4.1.2. ***(Coloured Version of Theorem 4.1.1)****[Shp19]: Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ 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 $Q_3 \in \sqrt{\langle Q_1, Q_2\rangle}$*

Then the linear span of the polynomials in $\cup_i T_i$ has dimension $O(1)$.

Theorem 4.1.3. ***(Product in Radical)****[PS20a]: There exists a universal constant c such that the following holds. Let $\{Q_i\}_{i\in[m]} \subset C[x_1, \ldots, x_n]$ be a finite set of pairwise linearly independent irreducible polynomials of degree at most 2. Assume that, for every $i \neq j$, $\prod_{k\in[m]\setminus\{i,j\}} Q_k \in \sqrt{\langle Q_i, Q_j\rangle}$. Then,$dim(span\{Q\}) \leq c$.*

Theorem 4.1.4. ***Coloured Version of theorem 4.1.3*** *[PS20b]: There exists a universal constant Λ such that the following holds. Let $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \subset \mathbb{C}[x_1, ..., x_n]$ be finite sets of pairwise linearly independent homogeneous polynomials satisfying the following properties:*

- *Each $Q \in \bigcup_{j\in[3]} T_j$ is either irreducible quadratic or a square of a linear function*

- *Every two polynomials Q_1 and Q_2 from distinct sets satisfy that whenever they vanish then the product of all the polynomials in the third set vanishes as well. Equivalently, for every two polynomials Q_1 and Q_2 from distinct sets the product of all the polynomials in the third set is in the radical of the ideal generated by Q_1 and Q_2.*

Then $dim(span\{\bigcup_{j\in[3]} T_j\}) \leq \Lambda$

The requirement that the polynomials are homogeneous is not essential as homogenization does not affect the property stated in the theorem.

The Theorem 4.1.4 puts a $O(1)$ bound on the linear dimension of all quadratics in the terms T_1, T_2, T_3 for SG-circuits, thus also bounding their tr-deg. The variable reduction [BMS13] allows us to reduce the number of variables to constant in which case we can simply brute force over all d^k points. Thus, Theorem 4.1.4 gives us a Blackbox PIT algorithm for $\Sigma^3\Pi\Sigma\Pi^2$.

4.2 Required Structure theorems

In proving these, they used the following structural results when quadratics lie in radical of other quadratics.

Theorem 4.2.1. ***(Structural Result 1)****[Shp19] Let $Q \in \sqrt{\langle Q_1, Q_2\rangle}$, then one of the following hold*

1. *Q is in linear span of Q_1, Q_2*
2. *$\exists \alpha, \beta$, and a linear function l such that $\alpha Q_1 + \beta Q_2 = l^2$*
3. *$\exists 2$ linear function l_1, l_2 such that $Q, Q_1, Q_2 \in \sqrt{\langle l_1, l_2\rangle}$*

Theorem 4.2.2. ***(Structural Result 2)****[PS20a] Let $\prod_{i\in K} Q_i \in \sqrt{\langle Q_1, Q_2\rangle}$, then one of the following hold*

1. *$\exists i \in K : Q_i$ is in linear span of Q_1, Q_2*
2. *$\exists \alpha, \beta$, and linear functions l_1, l_2 such that $\alpha Q_1 + \beta Q_2 = l_1 l_2$*
3. *$\exists 2$ linear function l_1, l_2 such that $Q_1, Q_2 \in \sqrt{\langle l_1, l_2\rangle}$*

4.2.1 Proof Idea 4.2.1

The basic idea is to reduce the problem from radical membership in a radical generated by 2 polynomials Q_1, Q_2 to a single polynomial $Res_{x_1}(Q_1, Q_2)$. For this consider

$$Q_1 = x_1^2 + Q_1'$$

$$Q_2 = x_1 a_1 - A$$

$$Q = x_1 q + Q'$$

The easy cases, i.e. of $a_1 = 0$ or $a_1|A$, are handled first. In the first case $a_1 = 0 \implies Q_1 = 0 \mod A$ as for any zero of A, Q_1 has 2 possible assignment of x_1, but Q has only one, which simply results in case 2. For $a_1|A$, we make a variable change to $y = a_1$ and $x_1 - A/a_1 = z$, getting $Q_2 = yz$, and substituting $y = 0$, to get linear forms which make the case 3 true.

Now we work with the main case. Look at the resultant of Q_1, Q_2 wrt x_1

$$Res_{x_1}(Q_1, Q_2) = A^2 + a_1^2 Q_1'$$

If we substitute $x_1 = A/a_1$, we have $Q_2 = 0$, and $Q_1 = (A^2 + a_1^2 Q_1')/a_1^2 = Res_{x_1}(Q_1, Q_2)/a_1^2$. Thus, we have $Q(x_1 = A/a_1) \in \sqrt{Res_{x_1}(Q_1, Q_2)}$.

$$Aq + a_1 Q' \in \sqrt{Res_{x_1}(Q_1, Q_2)}$$

Polynomial on LHS has degree 3, while on RHS has degree 4.Then, we simply look at possible cases of how Resultant can factor and then get lying in radical to one of the cases of the theorem.

Case 1: Resultant is irreducible, or such cases such that $Aq + a_1 Q'$ has to be 0. This means $Q = q/a_1 * Q_2$, i.e. case1 holds as Q multiple of Q_2.

Case 2: Resultant of the form C^2 where C is an irreducible quadratic.

$$A^2 + a_1^2 Q_1' = C^2$$

$$qA + a_1 Q' = bC$$

We have $a_1^2 Q_1' = C^2 - A^2 = (C + A)(C - A)$. If Q_1' is irreducible then $\alpha a_1^2 = (C + A)$ and $Q_1' = \alpha(C - A)$(or opposite), which gives $Q_1' = -2\alpha A + \alpha^2 a_1^2$, which simply gives $Q_1 + 2\alpha Q_2 = (x_1 + \alpha a_1)^2$, i.e. case 2.

If $Q_1' = ef$, either the above holds or $(C - A) = a_1 e$ and $(C + A) = a_1 f$, which gives $a_1|A$, which is already handled.

Case 3: Resultant is for the form

$$A^2 + a_1^2 Q_1' = a^2 C$$

$$qA + a_1 Q' = \lambda a C$$

We know that $a|Res_{x_1}$, therefore $\mod a$, either of Q_1, Q_2 vanish or have a common factor a'. We know as a doesn't have x_1, Q_1' cannot vanish, and for Q_2 to vanish $a_2|A$, which is already handled. For the last case setting the common factor $a' = 0$ and $a = 0$, we have $Q_1 = Q_2 = 0$, and hence $Q = 0$,i.e. case 3. □

4.2.2 Proof Idea 4.2.2

The theorem in PS20 also uses the claim from Gup14 based on Bezout Identity, to get a small product of 4 quadratics to lie in radical, from the whole product. Thus, the initial condition is

$$\prod_{i=1}^{4} L_i \in \sqrt{\langle Q_1, Q_2 \rangle}$$

Applying the same deduction as in Thm 4.2.1, we have for cases when

$$\prod_{i=1}^{4} (Aq_i + a_1 L_i') \in \sqrt{Res_{x_1}(Q_1, Q_2)}$$

Following are the possibilities based on factorization of Res

Case 1 Res is irreducible of deg 4, and all factors in the product have deg 3. Hence there should be one product which is identically 0, which makes the case 1.

Case 2 Res has a linear factor. If the linear factor is a_1, then we a_1 divides A, and case 2 holds. If it is any other factor b, then $\mod b$, either Q_1 or Q_2 zero, which mean $a_1|A$, or they have a common factor a, which if quadratic give case 2, and if linear give case 3.

Case 3 $Res_{x_1}(Q_1, Q_2) = CD$, where C and D are irreducible quadratic polynomials. The basic idea is to consider Q_1, Q_2, C, D as quadratics in a_1. Then, by comparing coefficients in $Res_{x_1}(Q_1, Q_2) = CD$ get structure in Q_1', A and C, D. considering

$$Q_1' = \alpha a_1^2 + p_1 a_1 + A''$$
$$Q_2' = \beta a_1^2 + p_2 a_1 + B''$$
$$C = \gamma a_1^2 + p_3 a_1 + C''$$
$$D = \delta a_1^2 + p_4 a_1 + D''$$

Comparing coefficients in $Res_{x_1}(Q_1, Q_2) = CD$ gives

$$B''^2 = C''D''$$

$$2p_2B'' = p_3D'' + p_4C''$$

These becomes into the case of $C = a_1v + Q_1$ and $D = a_1u + Q_1$, which can be worked to lie in case 2.

The cases that remain are where $a_1 = 0$. This simply means

$$Q_1 = x_1^2 - Q_1'$$

$$Q_2 = x_2^2 - Q_2'$$

where Q_1' and Q_2' are free of x_1, x_2. Represent $(x_3, \ldots, x_n)$ with $\mathbf{z}$. We can remove x_1^2 and x_2^2 terms from Q_i's by subtracting Q_1 and Q_2, hence have

$$Q_i = \alpha_i x_1 x_2 + b_i(\mathbf{z})x_1 + c_i(\mathbf{z})x_2 + L_i'(\mathbf{z})$$

Using the fact that one of the irreducible component of the zeroset of Q_1, Q_2 has it's projection to $\mathbf{z}$ to be dense, it can be shown that either $b_1^2Q_1' = c_1^2Q_2'$ or $L_1^2 = \alpha_1^2Q_1'Q_2'$. Both of these give that either one of Q_1' or Q_2' is a perfect square or $Q_1' = \beta Q_2'$ for some $\beta \in \mathbb{C}$. All the 3 cases result into case 2 of theorem. □

Issues for cubics

- One thing that seems crucial to the structure theorem is the fact that we can diagonalize a quadratic polynomial which allows us to to get a small expression for resultant. But this property doesn't hold for polynomials of higher degree (cubics and further).
- A major issue extending it cubics will be that the degree of resultant will be 9 and hence the number of cases will be larger.
- The expression for Q's after substitution and Resultant are small and hence easy to infer information from. $Q = Aq + a_1Q'$ and $Res = A^2 + a_1^2Q_1'$
- Also getting to a structural result where the problem reduces to lying in radical generated by linear forms seems difficult.

4.3 Bounding dimension of linear space using structure theorem

4.3.1 Proof Idea Theorem 4.1.1

Proof Idea Thm 4.1.1: Let us assume that for every $Q_1 \in \{Q\}$, we have at least a small fraction $\delta \geq 1\%$ of Q's such that the quadratic in their radical $Q_2 \in \sqrt{\langle Q_1, Q_2 \rangle}$ follows case 1 and is in their linear span, then they form a $\delta - SG$ configuration. The points $v_1, \ldots, v_m$ in $\mathbb{C}_d$ form a $\delta - SG$ 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. By Robust version of SG theorem, we can say that they span a $O(1)$ space.

Theorem 4.3.1. ***(Robust SG thm)****: If $v_1, \ldots, v_m$ in $\mathbb{C}_d$ form a $\delta - SG$ configuration then $dim(span\{v_1, \ldots, v_m\}) \leq 12/\delta$*

Now, we move to the other case, i.e. there are 2 polynomials which have less than 1% of quadratics in case1. This means the rest of 98% satisfy case 2 or 3 with either Q_1 or Q_2. This provides a strong structure on these polynomials and hence we bound the dimension on these.

For bounding the dimension in case 2 the fact that it is a square of linear form is very useful as it gives Q_1 in span of 2 products of 2 linear forms. If $F_1, \ldots, F_m$ are quadratic polynomials that satisfy case 2 with Q_1, Q_2, then we can say that all the linear forms involved form a space of dimension 4. The idea is if we have

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

for $i \neq j$ such that $\beta_i \neq \beta_j$, then Q_1, Q_2 lie in span of $\{(l_i - b_i) \cdot (l_i + b_i), (l_j - b_j) \cdot (l_j + b_j)\}$ If there is some other $k \neq i, j$ we have Q_1 in span of $\{(l_k - b_k) \cdot (l_k + b_k), (l_j - b_j) \cdot (l_j + b_j)\}$. This gives us that l_k, b_k in span of $\{l_i, b_i, l_j, b_j\}$. Thus, the dimension is $O(1)$.

Now we bound dimension of polynomials being in case 3. Consider $F_1, \ldots, F_m$ be in case 3 with Q_1. The idea is to write $Q_1 = \sum_{i=1}^{r} a_i b_i$ such that a_i and b_i are linear forms, and r is minimum such r. But, since we know Q_1 is in radical of 2 linear forms, we have for Q_1, $r = 2$. Now we introduce a new variable z and map each of the 4 linear forms $\{a_1, b_1, a_2, b_2\}$ in Q_1 to random multiples of z. Since F_i's also lie in the radical, they are multiples of z, of the form zb_i. Assuming 2 of 3 different b_i's we can say one of them is in span of other 2 as originally Q_3 vanished at $V(Q_1, Q_2)$. This becomes the SG condition exactly and hence, the dimension of $\{b_i\}$ is $O(1)$. It requires a proof why we can substitute z preserving linear independence and radical membership. But, the crucial idea is that since we were able to reduce the problem to lying in radical generated by linear forms, we were able to get a bound on dimension.

We can get that the remaining 2% polynomials form either case 2 or 3 with the remaining set of polynomials. Thus, we can get an $O(1)$ bound on them as well using the results proved

above.

4.3.2 Proof Idea Theorem 4.1.2

The basic theme remains the same as Theorem 4.1.1. The dimension bound we got for the case 2 and 3 is still useful as all those polynomials that follow it have $O(1)$-space. To handle the case 1, we will need the following robust coloured version of the Sylvester Gallai theorem.

Theorem 4.3.2. *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 $\delta-$EK configuration, i.e. if for every $i \in [3]$ and $p \in \mathcal{T}_i$, for every $j \in [3] \setminus \{i\}$ at least a δ fraction of the points $p_j \in \mathcal{T}_j$ satisfy that p and p_j span some point in the third set. Then $dim(span\{\cup_i \mathcal{T}_\setminus\}) \leq O(1/\delta^3)$.*

For the case when they don't form a SG condition, we bound the dimension of each of $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ one by one assuming existence of polynomials in the other set which have most $> 98\%$ of the polynomials in this set in case 2 or 3, using results discussed for theorem 1.

Issues Extending it to cubics

- The first case dimension bound of cubic lying in the linear span of other cubics will remain same. The robust version of SG theorem should bound the dimension for significant amount of case 1.
- The dimension bound for case 2 and 3 come from the fact that they represent reduction to problem where radical is generated by linear forms and hence easy to handle. Even if we get a structure theorem for cubics it is unlikely that they will reduce to membership in radicals generated by linear forms, so for getting a bound on the dimension we might have to try something else.

Chapter 5

Extending SG theorems to cubics

To extend it to cubics, the first step naturally is to develop structure theorems similar to the ones we had for quadratics.

5.1 Creating a structure theorem cubics

The breaking of the big product to a smaller one remains similar to the one in [PS20a], except for it would be product of 9 cubics instead of 4 quadratics lying in the radical. It comes from the same claim from [Gup14]. We will first look at trying to develop a structure similar to theorem 4.2.1, and hence assume $\mathcal{Q}$ to be a set of linearly independent cubic polynomials such that any $Q_1, Q_2 \in \mathcal{Q}$, there is a $Q \in \mathcal{Q}$, such that $Q \in \sqrt{\langle Q_1, Q_2 \rangle}$.

An initial issue we face as soon as we get into cubics from quadratics is we cannot diagonalize the polynomial Q_1 anymore. We though can make it's coefficient of x_1^2 zero,for $Q_1 = x_1^3 + a_2x_1^2 + a_1x_1 + a_0$ by substituting $x_1 = x_1 - a_2/3$. We can also remove coefficient of x_1^3 from Q_2 and Q by replacing them with $Q_2' = Q_2 - \alpha Q_1$ and $Q' = Q - \beta Q_1$ for appropriate α, β.Thus we have

$$Q_1 = x_1^3 + a_1x_1 + a_0$$
$$Q_2 = b_2x_1^2 + b_1x_1 + b_0$$
$$Q = q_2x_1^2 + q_1x_1 + q_0$$

We consider the Resultant of Q_1, Q_2, wrt x_1, which we have as

$$Res_{x_1}(Q_1, Q_2) = b_0b_2^2a_1^2 + b_0^3 - 2b_0^2b_2a_1 + b_2^3a_0^2 - b_2^2b_1a_1a_0 + 3b_0b_2a_0b_1 + b_0b_1^2a_1 - b_1^3a_0$$

The Resultant is big and hence inferring something from it being zero in itself is tough. So we go $\mod \langle b_2 \rangle$. Consider the radical generated by $\langle Res_{x_1}(Q_1, Q_2), b_2 \rangle$.Let a common

root they have be $\alpha \in \mathbb{C}^{n-1}$. We have

$$b_2(\alpha) = 0, Res_{x_1}(Q_1, Q_2)(\alpha) = 0$$

$$Res_{x_1}(Q_1, Q_2)(\alpha) = (b_0(\alpha))^3 + b_0(\alpha)a_1(\alpha)(b_1(\alpha))^2 - a_0(\alpha)(b_1(\alpha))^3$$

Since both Res and b_2 are independent of x_1, we can substitute x_1 anything without change in α. We substitute $x_1 = -b_0(\alpha)/b_1(\alpha)$. This makes

$$Q_2(x_1, \alpha) = b_2(\alpha)x_1^2 + b_1(\alpha)x_1 + b_0(\alpha) = b_1(\alpha)x_1 + b_0(\alpha)$$

$$Q_2(x_1 = -b_0(\alpha)/b_1(\alpha), \alpha) = 0$$

Similarly in $Q_1(x_1 = -b_0(\alpha)/b_1(\alpha), \alpha)$, we have

$$Q_1(x_1 = -b_0(\alpha)/b_1(\alpha), \alpha) = Res_{x_1}(Q_1, Q_2)/b_1(\alpha)^3 = 0$$

Hence, we have Q_2, Q_1 vanishing at $x_1 = -b_0(\alpha)/b_1(\alpha)$ and $(x_2, \ldots, x_n) = \alpha$, and since $Q \in \sqrt{\langle Q_1, Q_2 \rangle}$, by Nullstellensatz, we have Q vanishing on this too. Hence

$$(q_2 b_0^2 - q_1 b_0 b_1 + q_0 b_1^2) \in \sqrt{\langle Res_{x_1}(Q_1, Q_2), b_2 \rangle}$$

We currently have a similar result to claim 3.4 in PS20. Now if we substitute $x_2 = -b_{20}/b_{21}$, i.e. simply $b_2 = 0$ and for this substitution we have

$$Q|_{x_1=-b_0/b_1, x_2=-b_{20}/b_{21}} \in \sqrt{\langle Res_{x_1}(Q_1, Q_2)|_{x_2=-b_{20}/b_{21}} \rangle}$$

Thus, **we have reduced the problem to a single generator**, but since the degree is 9, it's factorization is difficult. Also, explicitly calculating it seems tedious.

We know that $Q|_{x_1=-b_0/b_1, x_2=-b_{20}/b_{21}}$ will be a degree ≤ 7 polynomial, while $Res_{x_2}(Res_{x_1}(Q_1, Q_2), b_2)$ will be a degree 9 polynomial. As before, lying in the radical implies that all the irreducible factors of Res will divide Q. So we make the cases as following

- **Case 1** Res is irreducible after the substitution of x_2. This simply means that $Q|_{x_1=-b_0/b_1, x_2=-b_{20}/b_{21}} = 0$ or Q in linear span of Q_1, Q_2.This means that $x_1 = -b_0/b_1$ is a root of Q after the substitution, and since Q cannot have fractional roots $b_1|_{x_2=-b_{20}/b_{21}}$ divides $b_0|_{x_2=-b_{20}/b_{21}}$. We assumed $Res_{x_1}(Q_1, Q_2) = b_0^3 + b_0 a_1 b_1^2 - a_0 b_1^3$($b_2 = 0$ as $x_2 = -b_{20}/b_{21}$) to be irreducible after the substitution, but if $b_1|b_0$ after the substitution, we have a quadratic factor of Res which is a contradiction. Hence, $Res_{x_1}(Q_1, Q_2)|_{x_2=-b_{20}/b_{21}}$ cannot be a irreducible.

- **Case 2** $Res = C^3$ after substitution, where C is an irreducible quadratic and $Q = CF$, where F is a $deg = 4$ polynomial. Since we have made $b_2 = 0$, we have $b_0^3 + b_0 a_1 b_1^2 - a_0 b_1^3|_{x_2=-b_{20}/b_{21}} = C^3$.This means assuming they are not divisible by b_2, $b_1^2(b_0 a_1 - a_0 b_1) = C^3 - b_0^3 = (C - b_0)(C^2 + b_0^2 + C b_0)$. We also know that

$deg(b_1) = 2, deg(b_0a_1 - a_0b_1) = 5, deg(C - b_0) = 3, deg(C^2 + b_0^2 + Cb_0) = 6$. Thus, $b_1|(C - b_0)$ and $b_1|(C^2 + b_0^2 + Cb_0)$ (after substitution of x_2).So either $b_1|b_0 \mod b_2$, but that would mean $b_1|C$, which is contradiction as we assumed C to be irreducible cubic. The other case would be b_1 doesn't divide b_0 and C both, but divides $C - b_0$. Then we have that C and b_0 have same remainder when divided by b_1, i.e. $C = b_1l_1 + r$ and $b_0 = b_1l_2 + r$. But we also have $b_1|C^2 + b_0^2 + Cb_0$, which gives $b_1|r^2$. That simply means r has a factor that divides b_1, but that will give a factor of C, which we assumed to be irreducible cubic, hence also contradiction. That brings us to the case where $b_2|b_1$, in which case $Res_{x_1}(Q_1, Q_2)$ is $b_0^3 \mod b_2$. **Possible candidate for case 2 equivalent**

- **Case 3** $Res = q^2 \cdot p$ after substitution $x_2 = -b_{20}/b_{21}$, where q is a quadratic and p has degree 5, and $Q = qp$.Note that q will be a polynomial in $n - 3$ variables. Consider $\mod (q, b_2)$, $Res_{x_1}(Q_1, Q_2) = 0$ implies that either Q_1 or Q_2 is zero, or Q_1,Q_2 have a common factor.As both q and b_2 are independent of x_1, clearly Q_1 cannot be zero $\mod b_2, q$ as x_1^3 will not vanish. For Q_2 to vanish b_1 will have to divide b_0, we analyse this later. If Q_1, Q_2 have a common factor $l'(deg = 1)$ or $q'(deg = 2)$, we get that Q, Q_1, Q_2, lie in $\sqrt{\langle b_2, l'/q', q\rangle}$. We can easily remove b_2 by setting $x_2 = -b_{20}/b_{21}$. Then, we will have to handle the case where a cubic polynomial lies in radical of 2 quadratic polynomials.

- **Case 4** Res after substitution $x_2 = -b_{20}/b_{21}$ has a linear factor l.Note that l will be a polynomial in $n - 3$ variables. Consider $\mod (l, b_2)$, $Res_{x_1}(Q_1, Q_2) = 0$ implies that either Q_1 or Q_2 is zero, or Q_1,Q_2 have a common factor.As both l and b_2 are independent of x_1, clearly Q_1 cannot be zero $\mod b_2, l$ as x_1^3 will not vanish. For Q_2 to vanish b_1 will have to divide b_0, we will analyse this later. If Q_1, Q_2 have a common factor $l'(deg = 1)$ or $q'(deg = 2)$, we get that Q, Q_1, Q_2, lie in $\sqrt{\langle b_2, l'/q', l\rangle}$. We can easily remove b_2 by setting $x_2 = -b_{20}/b_{21}$. Then, we will have to handle the case where a cubic polynomial lies in radical of a quadratic and a linear polynomials. The case of it lying in radical of 3 linear polynomials seems appropriate.

Combining Case2 and Case3, some of the cases reduce to Q lying in radical of 3 linear, one linear 2 quadratic or 2 linear 1 quadratic polynomials. Thus we have a degree reduction of atleast 1 in the generators of radical case.But in the case the number of generators increase we need to see what can be done. We explore it a bit later.

Following are the cases where the terms we are dividing by are 0, and how to handle those cases,

- $\mathbf{b_1 = 0}$ for this case when $Q_2 = 0$, $x_1^2 = -b_0/b_2$. substituting we have $Q_1 = (a_1 - b_0/b_2)x_1 + a_0$ and $Q = -q_2b_0/b_2 + q_1x_1 + q_0b_2$.When $Q_1 = 0$ in this case, we will

have $Q = 0$. Eliminating x_1 from the 2 equations we have, $q_2 b_0^2 - q_0 b_0 b_2 - q_2 b_0 b_2 a_1 + q_0 b_2^2 a_1 - q_1 b_2^2 a_0 = 0$. Going $\mod b_2$, we have $q_2 b_0^2 = 0$, which means either $q_2 = \lambda b_2$ or $b_2 | b_0$. First when $q_2 = \lambda b_2$, for any substitution that makes $b_2 = 0 (x_2 = -b_{20}/b_{21})$, $Q_2 = b_0|_{x_2 = -b_{20}/b_{21}}$ and $Q = (x_1 q_1 + q_0)|_{x_2 = -b_{20}/b_{21}}$. Now any assignment that makes $b_0 = 0$ will have 3 zeroes for x_1 with Q_1 or $a_1, a_0 = 0 \mod b_2, b_0$, but only 1 for Q as q_2 will also be zero. This will also mean that $q_0 = 0 \mod b_0, b_2$. This means Q will be in linear span of Q_1, Q_2. The other case will be $b_2 | b_0$. This means $Q_2 = b_2 (x_1^2 + b_0')$.Now after substitution $x_2 = -b_{20}/b_{21}$, we have any assignment that satisfies Q_1, satisfies Q. Therefore, all irreducible factors of $Q_1|_{x_2 = -b_{20}/b_{21}}$ must divide $Q|_{x_2 = -b_{20}/b_{21}}$. So, either $Q_1|_{x_2 = -b_{20}/b_{21}}$ divides $Q|_{x_2 = -b_{20}/b_{21}}$. Or $Q_1 = l_1^2 l_2$ and $Q = l_1 l_2 l_3$, which means Q, Q_1, Q_2 lie in radical of b_2, l_1.Now, we are left with $\mod b_2$, $Q_1 | Q$.**Possible candidate for case 2 equivalent**

- $\mathbf{b_1 | b_0} \mod \mathbf{b_2}$ This happens in case 2 and case 3 when Q_2 could be zero $\mod b_2$ and some other function without x_1, x_2. We again go $\mod b_2$.So $\mod b_2$, we have $Q_2 = b_1 (x_1 + b_0')$ where b_0' is a linear. Thus, after substituting $x_2 = -b_{20}/b_{21}$ and $x_1 = b_0'$, we have $Q'' \in \sqrt{\langle Q_1'' \rangle}$, where Q'', Q_1'' are Q, Q_1 after the 2 substitutions. Since both are $deg = 3$ either Q_1'' divides Q'', or $Q_1'' = l_1^2 l_2$ and $Q'' = l_1 l_2 l_3$, which means Q, Q_1, Q_2 lie in radical of $b_2, (x_1 - b_0'), l_1$ all of which are linear. We are left with the case $\mod b_2, (x_1 - b_0')$, Q_1 divides Q. **Possible candidate for case 2 equivalent**

- $\mathbf{b_{21} = 0}$ This means b_2 isn't a linear form rather just a constant, which breaks the homogeneity condition on Q's. The other case would be $b_2 = 0$ simply, which will be easier to handle as wherever we don't need to go $\mod b_2$, giving result much simplified.

Thus, after the analysis of all the cases we arrive that the conditions become very similar to the quadratic case. We still need to derive an equivalent of case 2 in theorem 4.2.1 for our structural theorem for cubics.

5.2 Progress on Structure Theorem till now

As we saw in previous section, we were able to break the radical of 2 generators for cubics using the resultant(similar to quadratics) and get the problem to an ideal-membership problem for single generator. As the degree is higher and the expression is bigger, along with the fact that we are looking $\mod b_2$ in most part, the analysis has a lot more cases. But, eventually most of them converge to either Q lies in linear span of Q_1, Q_2 or Q lies in radical of p_1, p_2, l where p_1, p_2 are linear or quadratic forms and l is a linear form. Even, without it, the result is a degree reduction. Thus, very similar to cases 1 and 3 for quadratics. We believe that rest of cases can be compressed to an equivalent of case 2 from theorem 4.2.1.

5.3 Future work direction for cubics

- The first idea should be to complete the Structure Theorem by simplifying the left cases for an equivalent of case 2.

- It does seem that the case of p_1, p_2, l where p_1, p_2 are quadratics can simplified further to linear polynomials again using resultant, as we go $\mod l$ by substituting a variable and getting the problem of a cubic lying in radical of 2 quadratics.
- Once we are done with the structure theorem, we can start getting a bound on linear dimension. The first case majority should remain same as for quadratics and can be bound using the robust version of Sylvester-Gallai theorem. Bounding dimension for rest of the cases still needs to be done.

Chapter 6

Conclusion and Future Scope

We saw in this report at the approach of using Sylvester-Gallai type theorems in solving the problem of PIT for depth-4 circuits of constant top and bottom fan-in. We looked at the Sylvester-Gallai type theorems known for quadratic theorems and their proof ideas using structure theorems. We also looked at the proof ideas of these structure theorems that develop structure when a quadratic or product of quadratics lie in radical of 2 quadratic polynomial. We saw how the use of resultant helps us tackle this problem. Then, we tried developing a similar structure theorem for cubics.

In future, we aim at completing the structure theorem for cubics and then bounding dimension using the structure theorem. After that we can try working on lifting this approach to constant bottom fan-in. The idea being to tackle the radical generated by 2 polynomials using resultant, possibly by going $\mod b_r, \ldots, b_2$. Again the cases, will be more, but possibly we can find a more general structure once we complete the result for cubics. Thus, extension for bottom fan-in seems possible, but there is no clear way on how to handle increase in top fan-in as number of generators of radical increase. The next step to it would be allowing multiplicity of the polynomials more than 1 in the terms.

Bibliography

[AT99] Noga Alon and M Tarsi. Combinatorial nullstellensatz. *Combinatorics Probability and Computing*, 1999.

[AV08] Manindra Agrawal and V Vinay. Arithmetic circuits: A chasm at depth four. *In Foundations of Computer Science*, 2008.

[BMS13] M. Beecken, J. Mittmann, and N. Saxena. Algebraic independence and blackbox identity testing. *Information and Computation*, 222:2 – 19, 2013. 38th International Colloquium on Automata, Languages and Programming (ICALP 2011).

[DS07] Z. Dvir and Amir Shpilka. Locally decodable code with 2 queries and polynomial identity testing for depth-3 circuits. *SIAM Journal on Computing, 36(5):1404–1434*, 2007.

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

[Gup14] Ankit Gupta. Algebraic geometric techniques for depth-4 pit and sylvester-gallai conjectures for varieties. *Electronic Colloquium on Computational Complexity (ECCC),21:130*, 2014.

[KS07] Neeraj Kayal and Nitin Saxena. Polynomial identity testing for depth 3 circuits. *Computational Complexity, 16(2):115–138*, 2007.

[KS09] Neeraj Kayal and Shubhangi Saraf. Blackbox polynomial identity testingfor depth 3 circuits. *In Foundations of Computer Science, 2009. FOCS'09.50th Annual IEEE Symposium on, pages 198–207*, 2009.

[PS20a] Shir Peleg and Amir Shpilka. A generalized Sylvester-Gallai type theorem for quadratic polynomials. *arXiv e-prints*, page arXiv:2003.05152, March 2020.

[PS20b] Shir Peleg and Amir Shpilka. Polynomial time deterministic identity testingalgorithm for $\Sigma^{[3]}\Pi\Sigma\Pi^{[2]}$ circuits via Edelstein-Kelly type theorem for quadratic polynomials. *arXiv e-prints*, page arXiv:2006.08263, June 2020.

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

[Sax14] Nitin Saxena. Progress on polynomial identity testing- ii. *In Perspectives in Computational Complexity, volume 26 of Progress in Computer Science and Applied Logic, pages 131–146. Springer International Publishing*, 2014.

[Sch80] Jacob T Schwart. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM (JACM)*, 1980.

[Shp19] 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*, 2019.

[SS12] Nitin Saxena and C. Seshadhri. Blackbox identity testing for bounded top-fan in depth-3 circuits: The field doesn't matter. *SIAM Journal on Computing, 41(5):1285–1298*, 2012.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science: Vol. 5*, 2010.