# On the Complexity of Hilbert's Nullstellensatz over Positive Characteristic

A Thesis Submitted

in Partial Fulfilment of the Requirements

for the Degree of

**Master of Technology**

*by*

**Ashish Dwivedi**

**Roll No: 15111011**

Under the Guidance of

**Prof. Nitin Saxena**


DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

AUGUST 2017

**Statement of Thesis Preparation**

1. Thesis title: On the Complexity of Hilbert's Nullstellensatz over Positive characteristic
2. Degree for which the thesis is submitted: M. Tech.
3. Thesis Guide was referred to for preparing the thesis. ✓
4. Specifications regarding thesis format have been closely followed. ✓
5. The contents of the thesis have been organized based on the guidelines. ✓
6. The thesis has been prepared without resorting to plagiarism. ✓
7. All sources used have been cited appropriately. ✓
8. The thesis has not been submitted elsewhere for a degree. ✓

(Signature of the student)

Name: ASHISH DWIVEDI

Roll No.: 15111011

Department/~~IDP~~: CSE

# Certificate

It is certified that the work contained in this thesis entitled "On the Complexity of Hilbert's Nullstellensatz over Positive Characteristic" by "Ashish Dwivedi" has been carried out under my supervision and that it has not been submitted elsewhere for a degree.

NSaxena 31 Jul'17

Dr. Nitin Saxena

*July 2017*

(Associate Professor)

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

# Abstract

Hilbert's Nullstellensatz (HN) is a fundamental theorem in Algebraic Geometry. It establishes a fundamental relationship between geometry and algebra. If a given system of polynomial equations $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ has no common zero over $\overline{\mathbb{K}}^n$ then HN gives a certificate $g_1, \ldots, g_m \in \overline{\mathbb{K}}[x_1, \ldots, x_n]$ such that

$$1 = f_1 g_1 + \ldots + f_m g_m$$

We are interested in the complexity of HN. In other words, we want to know how efficiently can we determine the satisfiability of a given system of polynomial equations over a given algebraically closed field.

In this thesis we investigate HN over positive characteristic fields. Current best complexity known for HN over positive characteristic field is PSPACE. We solved some special cases of this problem in NP. Basically we divided the problem in two cases: The first case is when the system of a given polynomial equations is positive dimensional and second case is when the system of a given polynomial equations is zero dimensional.

In positive dimensional case, we show three results in NP,

1. When the zero set of a given affine or projective system is either empty or absolutely irreducible.

2. When the zero set $X$ of a given affine system is either empty or one of its absolutely irreducible component $C$ of same dimension is definable over the coefficient field of $X$.

3. When the zero set $X$ of a given projective system is either empty or one of its absolutely irreducible component $C$ of same dimension is definable over the coefficient field of $X$ and multiple of the degree of defining equations of $C$ is at most the multiple of the degree of given polynomials.

In affine zero dimensional case we give construction of a system which have no small zeros. Further we give a reduction of affine zero dimensional systems to affine positive dimensional systems making general affine positive dimensional case at least as hard as affine zero dimensional case.

# Acknowledgements

I am greatly indebted to my thesis advisor Prof. Nitin Saxena for helping me in learning the first step towards research. One and half year before when I first contacted him, I knew nothing about theoretical computer science. I just had a feeling that I should work in this area and he humbly agreed to advise me. I thank him for all his teachings as an advisor as well as a teacher and for all the treats he has given. In these one and half year I have learnt a lot of algebra from him. I thank him for all his helps and he will always remain a great source of inspiration to me.

I would like to thank my friend Abhishek Rose. Since the very first day at IITK you have always been with me and sometimes even faced troubles just to help me.

Special thanks to my two theory buddies, Kartik Kale and Pranav Bisht. I thank you both for making my stay memorable at IITK. I thank Pranav for always giving me right advices and for his free treats :) Kartik always remained superb in philosophical discussions. You always listened to me and my emotions. Thank you both for being such a great friend. I would also like to thank my other batchmates with whom I enjoyed a lot at IITK.

I thank this great place IITK not only for my academic growth but also for my personal growth. This place is a mini India itself having people from all corners of the country, different languages, diverse thoughts such a great environment is this!

I would also thank my teachers here in CSE department for all your teaching efforts. I have learnt a lot here because of all your efforts.

I will thank my colleague Rajendra Kumar, Sumanta Ghosh and Amit Sinhababu. Thank you for all your precious advises.

At last I will thank my family. They always supported me in my decisions and in tough times. Without their support I would not have been here. Also I will thank my childhood friend Nitesh Tripathi.. friends forever :)

Thank you Gurudev.. Thank you Krishna..

*Dedicated to my Mother ...*
*She is most beautiful and strongest woman in the world*

# Contents

# Chapter 1

# Introduction

## 1.1 Overview

In this thesis we study the complexity of a fundamental problem in algebraic geometry: Checking consistency of a given system of polynomial equations over algebraic closure of a given field. A more general version of this problem, i.e, to find solution of the given system, lead the researchers to develop this giant branch of mathematics. The coefficient field can be a characteristic zero field (like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) or a positive characteristic field (like $\mathbb{Z}/5\mathbb{Z}$) which is also known as finite field. We specifically work on finding the complexity of the problem of consistency checking over a finite field. Today its complexity lie in PSPACE, which is a very higher level class in complexity hierarchy. On the contrary, over zero characteristic the best complexity of the problem known is AM which is a lower level class. Hence we believe that this status can be improved.

## 1.2 The Problem

Formally the problem can be stated as follows:

**Problem 1.** *Given a system $S = \{f_1 = 0, \ldots, f_m = 0\}$ of polynomial equations in $n > 1$ variables over the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$, where $\mathbb{F}_q$ is a finite field of characteristic $p > 0$. The maximum coefficient size of $f_1, \ldots, f_m$ is $\log q$ and maximum total degree $d$. Decide the satisfiability of $S$ over $(\overline{\mathbb{F}}_q)^n$ with complexity better than* PSPACE.

The problem is already known to be NP-hard. There is a polynomial time reduction of 3-SAT to this problem:

- Define $n$ polynomial equations $x_i(1 - x_i) = 0$ for each variable $x_i$ of 3-SAT for $1 \leq i \leq n$.
- Define polynomial equations $(1 - x_i)(1 - x_j)x_k = 0$ for each clause $(x_i \vee x_j \vee \overline{x}_k)$ of 3-SAT for $i, j, k \in [n]$.

Hence the problem is NP-hard. We believe the problem to be NP-complete and so we tried to put it in NP.

## 1.3 Current Status

Currently the problem is known to be in PSPACE over arbitrary characteristic fields. Koiran [Koi96] put the zero characteristic version of this problem in AM under unproven "Generalized Riemann Hypothesis" (GRH). Over positive characteristic, the problem is not known to be in smaller complexity class than PSPACE even conditionally. The following table summarizes the status:

| **Field** | **Complexity** |
|---|---|
| $\mathbb{C}$ | PSPACE |
| $\mathbb{C}$ (under GRH) | AM |
| $\overline{\mathbb{F}}_q$ | PSPACE |

## 1.4 Motivation

Hilbert's Nullstellensatz (HN) is a fundamental theorem in algebraic geometry which establishes a relationship between geometric objects (algebraic sets) and algebraic objects (system of polynomials). So it would be interesting to know the complexity of such a fundamental problem. Also solving system of polynomial equations have wide range of applications. HN is a basic step in decision and quantifier elimination problems in the first order theory of $\mathbb{C}$. It is also useful in applications such as automatic geometric theorem proving and robot motion planning. For example, polynomial equations are used to track the locus of the arms of robots, for more details see the nice book by Cox et. al. [CLO07][Chapter 6] .

As we have shown already that HN is NP-hard and conditionally over $\mathbb{C}$ it is in AM which is just above NP. This gives us evidence that this problem is perhaps NP-complete.

## 1.5 Contribution of the Thesis

In this thesis we divide the problem in two parts: first, when the dimension of zero set of a given system is positive and second when the dimension of the affine zero set is zero.

In the first case we address a promise problem 2: given a system $S$ of polynomial equations which is either inconsistent or its zero set $X$ has dimension $r > 0$ such that $X$ satisfies either of following three constraints:

1. $X$ is an absolutely irreducible affine or projective algebraic set or,
2. $X$ is affine algebraic set and one of its absolutely irreducible component of dimension $r$ is definable in same field in which $X$ is defined or,
3. $X$ is projective algebraic set and one of its absolutely irreducible component $C$ of dimension $r$ is definable in same field in which $X$ is defined such that the multiple of the degree of the equations defining $C$ is at most the multiple of the degree of the equations defining $X$.

check if $X$ is empty with complexity better than PSPACE. Theorem 5.1 shows that this promise problem is actually in NP. To achieve this we use some remarkable results in algebraic geometry.

Secondly we consider the affine zero dimensional case. Here we give example of an affine zero dimensional system which has no small certificate thereby showing that this case is harder than the special positive dimensional cases and HN for affine zero dimensional systems can not be put in NP by the same characterization of certificate as in special positive dimensional cases. Theorem 5.7 proves this claim.

At last we will give a reduction of zero dimensional affine algebraic sets into positive dimensional affine algebraic sets such that existence of a small zero for latter will imply existence of a small zero for former. Hence solving only the HN for affine algebraic sets of positive dimension in NP is sufficient put HN for general affine algebraic sets in NP. This concludes that putting HN for general affine algebraic sets into class NP is not possible by the same characterization of certificate as for special positive dimension cases.

## 1.6 Organization of the Thesis

Chapter 2 presents some ideal theoretic and complexity theoretic background. Chapter 3 and Chapter 4 constitutes the survey part. In Chapter 3 we state the famous "Hilbert's Nullstellensatz" theorem and prove it by simple algebraic techniques and show its significance that it acts as a bridge between algebra and geometry. Also we state its quantitative version which is widely known as "Effective Hilbert's Nullstellensatz". We give sketch of its proof by combinatorial method which is easily understandable to the readers even with little understanding of algebraic geometry. This proof was given by Dubé [Dub93] but it was incomplete and incorrect as was relying on some unproven bounds over Hilbert functions. It was completed and corrected in a paper by Sombra [Som97]. In Chapter 4 we show that over $\mathbb{C}$ our problem is currently known to be in class $\mathsf{AM}$ assuming Riemann Hypothesis is true. This is a result by Koiran [Koi96], based on the observation that a satisfiable system over $\mathbb{C}$ is satisfiable over many prime fields which is not the case with unsatisfiable systems over $\mathbb{C}$. In Chapter 5 we present our work as mentioned in section 1.5 and the last Chapter concludes the work and mentions some related open questions.

# Chapter 2

# Background and Preliminaries

## 2.1 Basic Algebraic Geometry

For a field $k$ and a positive integer $n$, the "affine n-space" over $k$ is defined as,

$$\mathbb{A}^n(k) := k^n = \{(a_1, \ldots, a_n) \mid a_i \in k,\ \forall i \in [n]\}$$

A subset $X \subseteq \mathbb{A}^n$ is called an "affine algebraic set" over $k$ if it is set of common zeros of some finite set of polynomials $\{f_1, \ldots, f_m\}$ in the ring $k[x_1, \ldots, x_n]$, i.e.

$$X = X(k) := \{\overline{a} \in \mathbb{A}^n(k) \mid f_i(\overline{a}) = 0,\ \forall i \in [m]\}$$

An "affine variety" $V \subseteq \mathbb{A}^n(k)$ is an *irreducible* affine algebraic set, i.e. $V$ is not a union of smaller affine algebraic sets over $\mathbb{A}^n(k)$.

From the geometric point of view affine spaces are incomplete in the sense that two lines do not intersect at a point always (parallel lines). We have "projective space" with this and other useful properties. Again for a field $k$ and a positive integer $n$, a "projective n-space" over $k$, denoted as $\mathbb{P}^n(k)$, is defined as

$$\mathbb{P}^n(k) := \frac{k^{n+1} - \overline{0}}{\sim}$$

where $\sim$ is equivalence relation in $k^{n+1}$ and defined as $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ iff there exists non-zero $\lambda \in k$ such that $b_i = \lambda a_i$ for all $i \in [n]$. One can see that $\mathbb{P}^n(k)$ is actually

$\mathbb{A}^n(k)$ added with more points at infinity (where parallel lines meet), in fact,

$$\mathbb{P}^n(k) := \mathbb{A}^n(k) \cup \mathbb{A}^{n-1}(k) \cup \ldots \cup \mathbb{A}^1(k) \cup \mathbb{A}^0(k)$$

These two definitions are equivalent, refer to any text on algebraic geometry or commutative algebra like [CLO07] for more details.

Like affine algebraic sets, "projective algebraic sets" are common zeros in $\mathbb{P}^n(k)$ of some finite set of homogeneous polynomials in $k[x_0, \ldots, x_n]$. Similarly, "projective varieties" are irreducible projective algebraic sets.

There are many definitions of dimension of a variety. The most general definition is, "The dimension of an affine or projective variety $V$ is the maximal length $d$ of the chains $\phi \neq V_0 \subsetneq V_1 \subsetneq V_2 \ldots \subsetneq V_d = V$ of distinct (absolutely irreducible) sub-varieties of $V$".

Dimension of an affine or projective algebraic set is the maximum dimension of its irreducible components. It is then apparent that if $S$ is any affine or projective algebraic set and $S' \subseteq S$ then,

$$dim(S') \leq dim(S)$$

We would like to point out that dimension of an algebraic set does not change when we move from defining field $k$ to some other field extension $\hat{k}$ of $k$. Also let $S$ be an algebraic set defined over some field $k$ then, $dim(S) > 0$ if and only if $S$ has infinitely many points over algebraically closed field $\overline{k}$. Similarly $dim(S) = 0$ if and only if $S$ has finitely many points over $\overline{k}$.

Now we will discuss most important term "degree" of algebraic sets and in particular degree of varieties, which is very useful in proving our result. For the following discussion we refer to excellent book by Hartshorne [Har13a], notes by Vogel and Patil [VP84], and excellent paper by Heintz [Hei83]. These results are also stated at one place in preliminary section of papers by Sombra [Som97] and, Lachaud and Rolland [LR15].

The degree of an affine (resp. projective) variety $V \subseteq \mathbb{A}^n$ $(resp.\ \mathbb{P}^n)$ of dimension $d$ is defined as

$$deg(V) := sup\{\#(V \cap H_1 \cap H_2 \cap \ldots \cap H_d) \mid H_1, \ldots, H_d \subseteq \mathbb{A}^n \ (resp.\ \mathbb{P}^n) \quad \text{are hyperplanes} \quad \text{and} \quad dim(V \cap H_1 \cap H_2 \cap \ldots \cap H_d) = 0\}$$

We can also define the degree of general algebraic sets. Let $X \subseteq \mathbb{A}^n$ $(resp.\ \mathbb{P}^n)$ is some reducible affine (resp. projective) algebraic set of dimension $d$ such that following is the

minimal decomposition of $X$ into its irreducible components,

$$X = \bigcup_{i=1}^{t} V_i$$

then degree of $X$ as defined in [Har13b, Ful13] is,

$$deg(X) = \sum_{\substack{j=1 \\ dim(V_j)=d}}^{t} V_j$$

Hence it is apparent that degree of any irreducible component of an algebraic set is at most degree of that algebraic set.

A "Hypersurface" in $\mathbb{A}^n$ or $\mathbb{P}^n$ is zero set of a single polynomial $f$. The dimension of a hypersurface in $\mathbb{A}^n$ or $\mathbb{P}^n$ is $n-1$ and degree is defined to be the degree of polynomial $f$.

Let $X \subseteq \mathbb{A}^n$ (*resp.* $\mathbb{P}^n$) be any affine (resp. projective) algebraic set defined by polynomials $f_1, \ldots, f_m$ such that degree of $f_i$ is $d_i$ for $i \in [m]$. The following version of Bézout's theorem can be found in [Hei83, VP84] and restated in [Som97, LR15], which gives an upper bound on the degree of $X$.

**Theorem 2.1.** *Let $Z$ be any affine or projective algebraic set and $F_1, \ldots, F_m$ are hypersurfaces respectively in affine or projective space, then*

$$deg(Z \cap F_1 \cap \ldots \cap F_m) \leq deg(Z) \prod_{i=1}^{m} deg(F_i)$$

Taking $Z$ as whole space and let hypersurface $F_i = \mathcal{Z}(f_i)$ for $i \in [m]$, we get that

$$deg(X) \leq \prod_{i=1}^{m} deg(f_i) = \prod_{i=1}^{m} d_i$$

## 2.2 Complexity Theoretic background

In this section we will define some complexity classes mentioned repeatedly in this thesis and also show the order in which they lie in complexity class hierarchy. For more detailed reading we refer to the excellent book by Arora and Barak [AB09].

**Definition 2.2** (Class P)**.** A decision problem $L$ is said to be in class P if any instance $x$ can be correctly decided by a deterministic turing machine in time $O(|x|^c)$ (polynomial), where $c$ is a constant.

**Example 2.1.** *The problems searching, sorting, finding cycle in undirected/directed graph, matrix multiplication lie in class* P*.*

It is always easy to verify a solution rather providing one ( though mathematically its not proven yet). The next class NP captures this notion of *efficiently verifiable problems.* Informally NP is the class of problems which are in class P when their instances are provided with hint ( certificate). Formally,

**Definition 2.3** (Class NP)**.** A decision problem $L$ is said to be in class NP iff there exists polynomials $p$ and $q$ and a deterministic TM M such that,

$$x \in L \Leftrightarrow \exists C, M(x, C) = 1$$

where $|C| = p(|X|)$ and $M$ takes time $q(|x|)$ on $(x, C)$.

**Example 2.2.** *Checking satisfiability of a boolean formula or finding if there is a hamiltonian cycle in a graph etc are the problems in class* NP*. If we are given correct assignment for the given boolean formula or if we are given the nodes of the graph in the order of a hamiltonian cycle then we can decide these problems in polynomial time.*

There is a notion of complete problems for a class. These are the hardest problem of the class in the sense that solving them would solve any other problem in that class. NP-complete problems are those which are of course in class NP and any other problem in class NP is polynomial time reducible to that problem. For example, Boolean satisfiability problem is NP-complete.

Clearly P $\subseteq$ NP. It is a famous open question that, if there is some problem which is in NP but not in P? There are very few such problems in NP but not proven that there is no algorithm for them in P. There was a famous problem, testing a number for prime, which was for long known to be in NP but few years back proved to be in P [AKS04].

Next we give definition of a class, which is mentioned in Chapter4, called "Arthur-Merlin"(AM) class, which is one of those classes following "Interactive proof systems".

**Definition 2.4.** The class AM is set of those problems which can be decided in polynomial time by following Arthur-Merlin protocol: Arthur asks some questions (sends

randomly generated coins) to Merlin, and Merlin accordingly provides answer/proof to Arthur, Arthur then deterministically verifies the proof using only his previously asked questions and accepts or rejects accordingly.

Mathematically, a language $L$ is in AM if there is a deterministic turing machine $M$ and polynomials $p, q$ such for any instance $x$:

- If $x \in L$ then $Pr_{y \in \{0,1\}^{p(|x|)}}[\exists z \in \{0,1\}^{q(|x|)} M(x, y, z) = 1] \geq 2/3$
- If $x \notin L$ then $Pr_{y \in \{0,1\}^{p(|x|)}}[\exists z \in \{0,1\}^{q(|x|)} M(x, y, z) = 1] \leq 1/3$

Where $M$ takes only polynomial amount of time in input size $|x|$. In above, $y$ is question asked by arthur and $z$ is the answer of merlin.

The class NP can be seen to be contained in class AM. Till now we have seen time complexity classes, now we will see a class classified on the basis of space, PSPACE.

**Definition 2.5.** PSPACE is a set of all problems which can be decided by a turing machine using only polynomial amount of extra space. More formally, let we denote by SPACE($s(n)$) the set of all problems that can be solved by a turing machine using only $O(s(n))$ amount of extra space for some function $s : \mathbb{N} \to \mathbb{N}$ of input size $n$ then,

$$\mathsf{PSPACE} = \bigcup_{k \in \mathbb{N}} \mathsf{SPACE}(n^k)$$

Now we give known relation between the classes defined above.

$$\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{AM} \subseteq \ldots \subseteq \mathsf{PH} \subseteq \mathsf{PSPACE}$$

Where dots represents long list of classes in polynomial hierarchy (defined as generalization of NP and coNP) and PH stands for polynomial hierarchy. Clearly class PSPACE is very big in the sense that it contains all of polynomial hierarchy. Currently, unconditionally HN is known to be in this class and it is believed that it actually belongs to some class at lower level in complexity class hierarchy.

# Chapter 3

# Hilbert's Nullstellensatz: Qualitative and Quantitative

## 3.1 Introduction

Hilbert's Nullstellensatz (HN) establishes a fundamental relationship between geometry and algebra. Ideals are basic algebraic objects and algebraic sets are basic geometric objects. HN establishes a bijection between algebraic sets (varieties) and some special kind of ideals known as radical ideals. So that when we talk about polynomials we can always choose between algebraic perspective (ideal) and geometric perspective (algebraic sets). Moreover it tells us about when we can find solution of a system of polynomial equations over an algebraically closed field, which is the question we want to answer efficiently. For reference and more details see [CLO07].

Unless specified explicitly $\mathbb{K}$ stands for an algebraically closed field throughout the Chapter.

## 3.2 Some Definitions

$\mathbb{K}$ is a field and polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ is set of all polynomials over $\mathbb{K}$.

An ideal $I$ of a ring is a subset of the ring and it is closed over addition ($a, b \in I \Rightarrow a+b \in I$) and multiplication by the elements of the ring ($a \in I, r \in \mathbb{K}[x_1, \ldots, x_n] \Rightarrow ra \in I$).

A zero set or an algebraic set $V$ in affine space $\mathbb{K}^n$ is the set of points which are zeroes of some finite set of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. In this Chapter we will use the terms "zero set" and "algebraic set" interchangeably.

If we are given some polynomials explicitly then ideal and zero set can be defined as follows:

**Definition 3.1.** The Ideal of $f_1, \ldots f_m \in \mathbb{K}[x_1, \ldots, x_n]$ denoted as $\langle f_1, \ldots, f_m \rangle$ is the set of polynomials

$$\langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=1}^{m} q_i f_i \mid q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

**Definition 3.2.** The zero set of $f_1, \ldots f_m \in \mathbb{K}[x_1, \ldots, x_n]$ is the set of points in affine space $\mathbb{K}^n$

$$V(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n \mid f_i(a_1, \ldots, a_n) = 0 \ \forall \ 1 \leq i \leq m\}.$$

Further we can define an ideal over a zero set and zero set over an ideal. If we are given a zero set $V \in \mathbb{K}^n$ and an ideal $I \in \mathbb{K}[x_1, \ldots, x_n]$ then:

**Definition 3.3.** The Ideal over zero set $V$ denoted as, $\mathcal{I}(V)$ is

$$\mathcal{I}(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(\boldsymbol{a}) = 0, \ \forall \boldsymbol{a} \in V\}.$$

and

**Definition 3.4.** The zero set over an ideal $I$ denoted as, $\mathcal{V}(I)$ is

$$\mathcal{V}(I) = \{\boldsymbol{a} \in \mathbb{K}^n \mid f(\boldsymbol{a}) = 0 \forall f \in I\}.$$

The radical of an ideal is defined as:

**Definition 3.5.** The Radical of an ideal $I$ denoted as, $\sqrt{I}$ is the set of polynomials

$$\sqrt{I} = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f^m \in I \text{ for some } m \geq 1\}.$$

It can be seen easily that radical of an ideal is itself an ideal.

## 3.3 The Consistency Question

Given some polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$. The Consistency Question is: Does the system of these polynomial equations, say

$$S = \begin{cases} f_1 = 0 \\ f_2 = 0 \\ \cdots \\ f_m = 0 \end{cases}$$

has a solution in $\mathbb{K}$? HN helps in answering this question. In its weak form, also known as Weak Hilbert's Nullstellensatz (WHN), it gives us a certificate when this system has no solution. Precisely,

**Theorem 3.6.** *Let* $f_1, \ldots f_m \in \mathbb{K}[x_1, \ldots, x_n]$. *Then the system*

$$S = \begin{cases} f_1 = 0 \\ f_2 = 0 \\ \cdots \\ f_m = 0 \end{cases}$$

*will have no solution in* $\mathbb{K}$ *iff* $\exists g_1, g_2, \ldots, g_m \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $\sum_{i=1}^{m} f_i g_i = 1$.

Clearly we see that $(g_1, \ldots, g_m)$ is our certificate. The above theorem can be restated in terms of ideal and zero set.

**Theorem 3.7** (WHN)**.** *If* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *and let* $I = \langle f_1, \ldots, f_m \rangle$ *then* $\mathcal{V}(I) = \phi$ *iff* $1 \in I$.

($1 \in I$ iff $I = \mathbb{K}[x_1, x_2, \ldots, x_n]$). Note that in a way, WHN says that when zero set is empty there is only one ideal corresponding to this zero set, the whole ring $\mathbb{K}[x_1, \ldots, x_n]$, i.e., there exists one to one correspondence between ideal and zero set in this case. Does there exists unique ideal to other zero sets? If not then to what kind of ideals zero sets mapped to? Strong Hilbert's Nullstellensatz (SHN) gives answer to these questions which will be discussed in section 3.5.

## 3.4 Proof of WHN

*Proof.* Note that we need to prove only one direction $\mathcal{V}(I) = \phi \Rightarrow 1 \in I$. Other direction is trivial and follows from the fact that $\mathcal{V}(I) \subset \mathcal{V}(1) = \phi$. We will prove by induction on number of variables $n$.

Base case ($n = 1$) follows, since in univariate case the polynomial ring is a PID and so every ideal is generated by a single polynomial, which has to be constant. Otherwise by the fundamental theorem of algebra its zero set will not be empty. Presence of constant ensures presence of 1 in $I$.
Before we proceed further let's state Extension Theorem which will be required in proof of WHN.

**Theorem 3.8** (Extension Theorem)**.** *Let* $I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ *and* $J = I \cap \mathbb{K}[x_2, \ldots, x_n]$. *And for some* $i$,

$$f_i = cx_1^{d_i} + \textit{terms having degree} < d_i,$$

*where constant* $c \neq 0$ *and* $d_i > 0$. *If* $(a_2, \ldots a_n) \in \mathcal{V}(J)$ *then for some* $a_1 \in \mathbb{K}$, $(a_1, \ldots, a_n) \in \mathcal{V}(I)$.

Suppose the theorem holds till $n-1$ variables. Assume degree of each $f_i$ is $d_i$ and each $f_i$ is a non-constant polynomial otherwise we are done. To exploit extension theorem we need to make each $f_i$ in a proper format. Choose some $z_2, \ldots, z_n \in \mathbb{K}$ and apply the linear transformation,

$$\begin{aligned} x_1 &= y_1, \\ x_2 &= y_2 + z_2 y_1, \\ &\ldots \\ x_n &= y_n + z_n y_1. \end{aligned}$$

So that for $1 \leq i \leq m$, $f_i(x_1, \ldots, x_n) = f_i(y_1, y_2 + z_2 y_1, \ldots, y_n + z_n y_1)$

$= g_i(z_2, \ldots, z_n) y_1^{d_i} +$ terms having degree of $y_1 < d_i$

$= f_i^{'}(y_1, \ldots, y_n)(say)$.

Since every algebraically closed field is infinite, we can always choose value of $z$'s such that for some $i$, $g_i$ is a non-zero constant, say $c$. And suppose $I^{'} = \langle f_1^{'}, \ldots, f_m^{'} \rangle \subset \mathbb{K}[y_1, \ldots, y_n]$. Since linear transformation does not alter constants, $1 \in I \Leftrightarrow 1 \in I^{'}$. Suppose $J = I^{'} \cap \mathbb{K}[y_2, \ldots, y_n]$.

Now It is clear that, $\mathcal{V}(I) = \phi \Rightarrow \mathcal{V}(I^{'}) = \phi$.
$\mathcal{V}(I^{'}) = \phi \Rightarrow \mathcal{V}(J) = \phi$ because if not then by using extension theorem we can extend the point in $\mathcal{V}(J)$ to a point in $\mathcal{V}(I^{'})$ contradicting the fact that $\mathcal{V}(I^{'})$ is empty.
By Induction hypothesis, $\mathcal{V}(J) = \phi \Rightarrow 1 \in J$.
$1 \in J \Rightarrow 1 \in I^{'}$ (since $J \subset I^{'}$).
and $1 \in I^{'} \Rightarrow 1 \in I$. Hence Proved. □

### 3.4.1 Proof of Extension Theorem

*Proof.* Proof of this theorem involves use of resultants. Resultants are tools used in elimination theory. First we will see some of their properties for our use.
Given two multivariate polynomials $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. We take resultant with respect to some variable, say $x_1$, and denote it as $Res_{x_1}(f, g)$. $Res_{x_1}(f, g)$ has following properties:

- $Res_{x_1}(f, g) \in I = \langle f, g \rangle$ and in particular $Res_{x_1}(f, g) \in \mathbb{K}[x_2, \ldots, x_n]$.
- $Res_{x_1}(f, g) = 0 \Rightarrow$ there is a common factor $h \in \mathbb{K}[x_1, \ldots, x_n]$ of $f$ and $g$, or say $f$ and $g$ shares a common root in $\mathbb{K}$.
- If $a = (a_2, \ldots, a_n) \in \mathbb{K}^{n-1}$ and $f^{'} = f(x_1, a), g^{'} = g(x_1, a)$, then $Res_{x_1}(f, g) = l^{cd(g)}$ $Res_{x_1}(f^{'}, g^{'})$, where $l$ is leading coefficient of $f$ wrt $x_1$ and $cd(g)$ =cumulative degree of $g = deg_{x_1}(g) - deg_{x_1}(g^{'})$.

To read more about resultants see Chapter 3 of [CLO07].
Denote $(a_2, \ldots, a_n)$ by $\boldsymbol{a}$.
Consider the homomorphism $\mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1]$ defined by $f(x_1, \ldots, x_n) \longmapsto f(x_1, \boldsymbol{a})$.
Let $I^{'} = \{f(x_1, \boldsymbol{a}) \mid f \in I\}$. Clearly $I^{'}$ is Ideal in $\mathbb{K}[x_1]$. Since $I^{'}$ is PID, let $I^{'} = \langle f(x_1) \rangle$.
There are two cases.
When $f$ is not a non-zero constant then for some $a_1 \in \mathbb{K}$, $f(a_1) = 0$ and hence $(a_1, a_2, \ldots, a_n)$ $\in \mathcal{V}(I)$.
Consider the case when $f$ is some constant, say $b$. Given that leading coefficient of $f_i$ wrt $x_1$ is constant $c \neq 0$ and there must be some $f^{'} \in I$ st $f^{'}(x_1, \boldsymbol{a}) = f(x_1) = b$ . Now let $r(x_2, \ldots, x_n) = Res_{x_1}(f_i, f^{'})$. Since $r \in I$ and $r \in \mathbb{K}[x_2, \ldots, x_n]$, $r \in J$. Hence $r(\boldsymbol{a}) = 0$ since $\boldsymbol{a} \in \mathcal{V}(J)$ .
But by properties of resultant $r(\boldsymbol{a}) = c^{deg_{x_1}(f^{'})} Res_{x_1}(f_i(x_1, \boldsymbol{a}), b)$, since $b$ is constant so $cd(f^{'}) = deg_{x_1}(f^{'})$. But $Res_{x_1}(f_i(x_1, \boldsymbol{a}), b)$ is non-zero constant ($b$ is constant so it has no common root with $f_i(x_1, \boldsymbol{a})$). Hence $r(\boldsymbol{a})$ is non-zero constant, a contradiction. Thus the assumption that $f(x_1)$ is a non-zero constant is false. This proves the theorem. □

## 3.5 Correspondence between Radical Ideals and Algebraic Sets

Recall that WHN says that in an algebraically closed field, there is only one ideal which have empty solution set, the Ring itself. But it is not true for other ideals. There can be many different ideals having same zero set. For eg, $\langle x^2, y^3\rangle$ and $\langle x, y^4\rangle$ are two different ideals in $\mathbb{C}[x, y]$ but their zero sets are same $\{(0, 0)\} \subset \mathbb{C}^2$. Other simple example is $\langle x^5\rangle$ and $\langle x^2\rangle$ in $\mathbb{C}[x, y]$, having same zero set $\{(0, b) \mid \forall b \in \mathbb{C}\} \subset \mathbb{C}^2$. Note that $\mathcal{V}(\mathcal{I}(f_1, \ldots, f_m))$ is same as $\mathcal{V}(f_1, \ldots, f_m)$ but $\mathcal{I}(\mathcal{V}(\mathcal{I}(f_1, \ldots, f_m)))$ is not necessarily same as $\mathcal{V}(f_1, \ldots, f_m)$. In fact if $I = \langle f_1, \ldots, f_m\rangle$, then $I \subseteq \mathcal{I}(\mathcal{V}(I))$. From above examples we observe that the extra polynomials in $I(V(\mathcal{I}))$ are those $f$ such that $f^m \in I$ for some positive $m$, i.e., $\mathcal{I}(\mathcal{V}(I))$ will be at least $\sqrt{I}$. SHN answers this question and states that such polynomials are the only extra polynomials. Hence $\mathcal{I}(\mathcal{V}(\mathcal{I}(...I...)))$ converges at $\sqrt{I}$.

**Theorem 3.9** (SHN)**.** *If $I$ be some ideal in $\mathbb{K}[x_1, \ldots, x_n]$, then*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

This establishes a one to one correspondence between algebraic sets and radical ideals.

### 3.5.1 Proof of SHN

*Proof.* We will show that SHN and WHN are equivalent statements, which will ultimately prove SHN.
It is easy to see that SHN $\Rightarrow$ WHN. $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\phi) = \mathbb{K}[x_1, \ldots, x_n]$(Since $\phi = \mathcal{V}(\langle 1\rangle)$ so $\mathcal{I}(\phi) = \mathcal{I}(\mathcal{V}(\langle 1\rangle)) \supseteq \langle 1\rangle = \mathbb{K}[x_1, \ldots, x_n]$).
Hence $\sqrt{I} = \mathbb{K}[x_1, \ldots, x_n]$
$\Rightarrow 1 \in \sqrt{I}$
$\Rightarrow 1 \in I$.
To prove WHN $\Rightarrow$ SHN we will use Rabinowitsch trick. We need to prove only $\mathcal{I}(\mathcal{V}(I)) \subseteq \sqrt{I}$. So if $f \in \mathcal{I}(\mathcal{V}(I))$ then we need to show that $f \in \sqrt{I}$. By Hilbert basis theorem every ideal is finitely generated. So suppose $I = \langle f_1, \ldots, f_m\rangle$, and also another ideal $J = \langle f_1, \ldots, f_m, 1 - yf\rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$.
It is easy to see that $V(J) = \phi$ because whenever $f_i$'s are zero on some point then since $f \in I$, $f$ also vanishes on that point so $1 - yf = 1 \neq 0$. By WHN, $1 \in J$, hence $\exists g_1, \ldots, g_m, h \in \mathbb{K}[x_1, \ldots, x_n, y]$ such that $1 = \sum_{i=1}^{m} f_i g_i + h(1 - yf)$. This equation also

holds in $\mathbb{K}(x_1, \ldots, x_n)[y]$ and since $f$ is nonzero, put $y = 1/f$ in equation and multiply both sides by $f^m$ for some large enough $m$ to cancel $f$ from denominator of the right side of the equation. We get, $f^m = \sum_{i=1}^{m} f_i g_i^{'} \in I$. Hence $f \in \sqrt{I}$. This proves SHN. □

## 3.6 Effective Hilbert's Nullstellensatz (EHN)

In this section we sketch proof of Dube [Dub93] and Sombra [Som97] for Effective Nullstellensatz. In the previous section we saw a non-constructive proof of HN which says that there exists a certificate $\{g_1, \ldots, g_m\}$, when given system of equations $\{f_1 = 0, \ldots, f_m = 0\}$ is not satisfiable. The next question naturally arises is how big are the degree and the coefficients of $g_i$'s? It is easy to see that only the information about degree of $g_i$'s is sufficient. This question is special version of the "Ideal Membership Problem"(IMP), which asks whether a polynomial $f \in \langle f_1, \ldots, f_m \rangle$? HN asks whether $1 \in \langle f_1, \ldots, f_m \rangle$? Since a long time we knew only doubly exponential upper bound on the degree for IMP. In 1987, a breakthrough came by Brownawaell [Bro87] that EHN is a weak question than IMP. He proved a singly exponential upper bound on the degree in positive characteristic. Later Kollar [Kol88] proved asymptotically same bound but in any characteristic, and thereby proving that consistency checking question is in PSPACE. Dube [Dub93] gave another proof by combinatorial method in 1993, but his proof was incomplete and relying on some unproven bounds on Hilbert functions which was completed and corrected by Sombra [Som97]. We will mainly follow Sombra [Som97] (for the sake of correctness) and occasionally refer to work of Dube [Dub93] . Our objective here is to provide overview and approach of the proof so that reader can get a broad understanding of the proof and can easily refer to the original papers for specific details.

### 3.6.1 Some Background

We present some definitions and notations to be used later in sections ahead.

A *prime sequence* is a sequence of polynomials $\{f_1, \ldots, f_m\}$ in the ring $\mathcal{A} = K[x_1, \ldots, x_n]$, such that for $i = 2, \ldots, m$, $f_i$ is not a zero divisor in the quotient ring $\mathbb{A}/(f_1, \ldots, f_{i-1})$. In other words we can say, $f_i$ is not in any associated prime ideal of $(f_1, \ldots, f_{i-1})$. Most of the prime sequences are *regular sequence* because "a prime sequence whose ideal is not the whole ring $\mathcal{A}$ is defined to be regular sequence".

In the case of above mentioned ring $\mathcal{A}$ ( ring of polynomials over a field) the *height* of an ideal $I$ is the length of the longest regular sequence contained in $I$.

An ideal $I$ is said to be unmixed of height $h$, if all its associated prime ideals have the same height $h$. For a regular sequence $f_1, \ldots, f_m$, the ideal $(f_1, \ldots, f_m)$ is known to be unmixed of height $m$.

### 3.6.2 Overview and Main Idea

Let $\mathcal{A} := K[x_1, \ldots, x_n]$ be a polynomial ring over which the ideal $I$ is defined by the set of polynomials $\{f_1, \ldots, f_s\}$. Degree of each $f_i$ is upper bounded by $d$. If $g \in I$ then there exists some $g_1, \ldots, g_s \in \mathcal{A}$ such that

$$g = g_1 f_1 + \ldots + g_s f_s$$

Now, some term $a_j f_j$ will have degree of the form $deg(g)+D$. We are interested in minimal upper bound on $D$ in the case when $g = 1$, over all possible $\{g_1, \ldots, g_s\}$s. The proof given by Dube considers broader class of ideals, the ideals generated by a prime sequence, and provides exponential bound on $D$. An ideal $I$ generated by $\{f_1, \ldots, f_s\}$ is also generated by a prime sequence if either of the two cases are true:

- $1 \in I$, or
- $I$ is unmixed of height $s$.

Clearly it covers the case we are interested in. The idea is to use homogeneous polynomials instead of the given affine polynomials. Let $I$ be the ideal generated by the given polynomials $f_1, \ldots, f_s$ in the affine ring $k[x_1, \ldots, x_n]$. Let $\hat{f}_1, \ldots, \hat{f}_s$ are corresponding homogeneous polynomials in the ring $k[x_0, \ldots, x_n]$. Let $H$ be the ideal generated by these homogeneous polynomials and $\hat{I}$ is the homogeneous ideal obtained by the homogenization of $I$. Clearly if $g \in I \Rightarrow \hat{g} \in \hat{I}$ but it is not necessary that $\hat{g} \in H$ always. For some $d \geq 0$ we have $x_0^d \hat{g} \in H$. The use of homogenization is that the minimum such $d$ will be equal to the degree $D$ we want to bound.

The essence of combinatorics in the proof comes from the involvement of Hilbert functions. The bounds (lower and upper) for the values of the Hilbert functions are known for the homogeneous ideals of regular or prime sequences. So to get to the point where we can get benefit of the properties of Hilbert functions and complete our proof we will first reduce

the given sequence to a prime sequence (because ideal is given as such that it can be generated by a prime sequence). Now we want to homogenize the new sequence in the hope that homogenized sequence will be regular sequence but there is no guarantee that the new homogenized sequence will be a regular sequence. For this we will convert our current affine prime sequence to a new affine prime sequence which when homogenized, produces new homogeneous regular sequence of controlled degree (this degree is not bad for our purpose). Hilbert function bounds are used to make this conversion possible. Now we consider many different homogeneous ideals and see that when $g \in I$ then what is the upper bound on the each of the degree $d$ of $x_0$ such that $x_0^d \hat{g}$ is in those homogeneous ideals. We find connection among these degrees and based on that connection we bound the required degree $D$. While doing this, it requires use of bounds on the Hilbert functions and use of some ideal theoretic techniques.

### 3.6.3 Upper and Lower Bound on Hilbert Function

We will only state some important theorems which gives us required bound and some properties of Hilbert functions to be used in later sections. Interested readers are referred to the paper by Sombra [Som97].

**Lemma 3.10.** *Let $I \subseteq k[x_0, \ldots, x_n]$ be an homogeneous unmixed ideal of dimension 0. Then*

$$h_I(m) \geq m+1 \qquad I-2 \geq m \geq 0$$
$$h_I(m) = degI \qquad m \geq degI - 1$$

**Theorem 3.11.** *Let $I \subseteq k[x_0, \ldots, x_n]$ be an homogeneous ideal of dimension $d \geq 0$. Then*

$$h_I(m) \geq \binom{m+d+1}{d+1} - \binom{m-degI+d+1}{d+1}$$

Now we state the upper bound.

**Theorem 3.12.** *Let $k$ be a perfect field and $I \subseteq k[x_0, \ldots, x_n]$ a homogeneous unmixed radical ideal of dimension $d \geq 0$. Then,*

$$h_I(m) \leq \binom{m+degI+d}{d+1} - \binom{m+d}{d+1} \qquad m \geq 1$$

**Theorem 3.13.** *Let $k$ be a perfect field and $I \subseteq k[x_0, \ldots, x_n]$ a homogeneous unmixed radical ideal of dimension $d \geq 0$, and let $f \in k[x_0, \ldots, x_n]$ be a non zero divisor modulo $I$.*

*Then,*

$$h_{(I,f)}(m) \leq degI \qquad m \geq 1$$
$$h_{(I,f)}(m) = 0 \qquad m \geq degI + degf - 1$$

### 3.6.4 Regular Sequence Construction

In this section we show that a given prime sequence $f_1 \ldots, f_s \in k[x_1, \ldots, x_n]$ of affine polynomials can be replaced by another prime sequence $p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$ of controlled degree (not very big for our purpose), which when homogenized forms a regular sequence $\hat{p_1}, \ldots, \hat{p_s} \in k[x_0, \ldots, x_n]$. We assume $k$ to be an algebraically closed field (though $k$ being perfect and infinite suffices).

We will use following theorem from [Som97],

**Theorem 3.14.** *Let $I \subseteq k[x_0, \ldots, x_n]$ be an unmixed radical ideal of dimension $d \geq 0$, and let $F \in k[x_0, \ldots, x_n]$ be a homogeneous polynomial which is a non-zero divisor in $k[x_0, \ldots, x_n]/I$. Then there exist homogeneous polynomials $f_1, \ldots, f_{n-d} \in I$ such that $F, f_1, \ldots, f_{n-d}$ is a regular sequence such that*

$$deg(f_i) \leq deg(I) + deg(F) - 1 \qquad if\ d = 0$$
$$deg(f_i) \leq (5d)deg(I)deg(F) \qquad if\ d \geq 1$$

This theorem is a result of the upper bounds on hilbert functions proved in the referred paper. If $F, f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ be homogeneous polynomials such that $f_1, \ldots, f_s$ is a prime sequence in $k[x_0, \ldots, x_n]/(F)$, this does not imply always that $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ is a regular sequence. But this sequence can be replaced by another sequence of polynomials $p_1, \ldots, p_s \in k[x_0, \ldots, x_n]$ of degrees not very big such that $\langle p_1, \ldots, p_i \rangle = \langle f_1, \ldots, f_i \rangle$ for $i \in [s]$ and $p_1, \ldots, p_s$ is a regular sequence in $k[x_0, \ldots, x_n]$. This is the result of next theorem by M. Sombra [Som97] which follows the arguments of similar proof (relying on unproved bound on hilbert functions) in T. dube's paper [Dub93].

**Theorem 3.15.** *Let $s \leq n + 1$ and let $F, f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ be homogeneous polynomials, with $F$ non-constant, such that $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]/(F)$ is a prime sequence and $\langle f_1, \ldots, f_i \rangle \subseteq k[x_0, \ldots, x_n]/(F)$ is a radical ideal for $i \in [s-1]$. Let $I_i := \langle f_1, \ldots, f_i \rangle \subseteq k[x_0, \ldots, x_n]/(F)$ and $I_i^c := I_i \cap k[x_0, \ldots, x_n]$ for $i \in [s]$. Then there exist homogeneous polynomials $p_1, \ldots, p_s \in k[x_0, \ldots, x_n]$ satisfying the conditions:*

1. *$p_1 = F^{c_1} f_1, p_2 = F^{c_2} f_2, p_i \equiv F^{c_i} f_i \pmod{I_{i-1}}$ with $c_i \in \mathbb{Z}$ for $i \in [s]$,*

2. $p_1, \ldots, p_s \in k[x_0, \ldots, x_n]$ *is a regular sequence,*

3. $deg(p_i) \leq max\{deg(f_i), 5(n+1-i)deg(F)deg(I_{i-1}^c)\}$ *if* $i \leq n$
   $deg(p_{n+1}) = max\{deg(f_{n+1}), deg(I_n^c) + deg(F) - 1\}$

*Proof.* We will prove it by induction on $s$.

For base case, $s = 2$. Let $f_1 = F^{e_1}a_1$ and $f_2 = F^{e_2}a_2$ where $e_1, e_2$ are maximal power of $F$, i.e, $F \nmid a_1$ and $F \nmid a_2$. Also $a_1$ and $a_2$ must be co-prime since $f_1, f_2$ is a regular sequence in $k[x_0, \ldots, x_n]/(F)$. So $p_1, p_2$ can be taken as,

$$p_1 := F^{-e_1}f_1, p_2 := F^{-e_2}f_2$$

Clearly $p_1, p_2$ is a regular sequence in $k[x_0, \ldots, x_n]$.

Now induction hypothesis is: for $i \geq 3$ there exists homogeneous polynomials $p_1, \ldots, p_{i-1} \in k[x_0, \ldots, x_n]$ for $f_1, \ldots, f_{i-1}$ as stated in theorem. Let $L_{i-1} := \langle p_1, \ldots, p_{i-1} \rangle \subseteq k[x_0, \ldots, x_n]$. Clearly $L_{i-1}$ is unmixed of height $i-1$, i.e, dimension of $L_{i-1}$ is $n-i+1$. Consider the irredundant primary decomposition of $L_{i-1}$,

$$L_{i-1} = \bigcap_{j=1}^{t} q_j$$

Since $F$ is not in $L_i$, let we have,

$$F \notin \sqrt{q_j} \quad for\ 1 \leq j \leq r$$
$$F \in \sqrt{q_j} \quad for\ r+1 \leq j \leq t$$

Suppose $(L_{i-1})$ is a version of $L_{i-1}$ in $k[x_0, \ldots, x_n]/(F)$. Hence $(L_{i-1}) = I_{i-1}$ and so
$I_{i-1}^c = (L_{i-1}) \cap k[x_0, \ldots, x_n]$
$\Rightarrow I_{i-1}^c = \cap_{j=1}^r q_j \subseteq k[x_0, \ldots, x_n]$

The last equality gives a primary decomposition of $I_{i-1}^c$. Since $f_1, \ldots, f_{i-1}$ was a prime sequence, hence either $1 \in I_{i-1}$ or $I_{i-1}$ is unmixed ideal of height $i-1$ in $k[x_0, \ldots, x_n]/(F)$. In other words, either $1 \in I_{i-1}$ or dimension of $I_{i-1}$ is $n-i+1$. So we have either $1 \in I_{i-1}^c$ or $dim(I_{i-1}^c) = n-i+1$. Clearly, $I_{i-1}^c$ is unmixed radiacal ideal, so by applying theorem 3.14 on $I_{i-1}^c$, there exist homogeneous polynomials $b_1, \ldots, b_{i-1} \in I_{i-1}^c$ such that $F, b_1, \ldots, b_{i-1}$ is a regular sequence and such that,

$$deg(b_j) = max\{deg(f_i), 5(n+1-i)deg(F)deg(I_{i-1}^c)\} \qquad 1 \leq j \leq i-1$$

If $i \leq n$ and

$$deg(b_j) = max\{deg(f_{n+1}), deg(F) + deg(I_n^c) - 1\} \qquad 1 \leq j \leq n$$

if $i = n + 1$.

Now let we define $u_i \in I_{i-1}^c$ as, $u_i := \sum_{j=1}^{i-1} \lambda_j b_j$ for a generic choice of $\lambda_1, \ldots, \lambda_{i-1}$. We claim that if $p_i$ is defined as $p_i := F^{c_i} f_i + u_i$ such that $c_i := deg(u_i) - deg(f_i) \geq 0$ then it will satisfy the conditions stated in theorem.

The bound on degree of $p_i$s are then easy to see as, $deg(p_i) = deg(u_i)$ and so,

$$\begin{aligned} deg(p_i) &= max\{deg(f_i), 5(n+1-i)deg(F)deg(I_{i-1}^c)\} && for\ i \leq n,\ and \\ deg(p_{n+1}) &= max\{deg(f_{n+1}), deg(F) + deg(I_n^c) - 1\} && 1 \leq j \leq n \end{aligned}$$

Also $p_i$s follow condition 1 i.e, $p_i \equiv F^{c_i} f_i \pmod{I_{i-1}}$. The only thing left is to prove that $p_i$ does not belong to any associated prime ideal of $L_{i-1}$.

Consider again the primary decomposition of $L_{i-1}$.
Case 1: For $j \in [r]$, we know that $f_i \notin \sqrt{q_j}$ because $(L_{i-1}) = I_{i-1}$ and $f_i$ is a non-zero divisor in $I_{i-1}$. And since $u_i \in I_{i-1}$ so $p_i = F^{c_i} f_i + u_i \notin \sqrt{q_j}$.
Case 2: For $r + 1 \leq j \leq t$. As we said before, $L_{i-1}$ is an unmixed ideal of dimension $n - i + 1$ so each $q_j$ has dimension $n - i + 1$ and it can not conatain a regular sequence of length more than $i - 1$. Since $F \in \sqrt{q_j}$ and if for $i \in [i - 1]$ each $b_l$ is in $\sqrt{q_j}$ then we have a regular sequence of length $i$ which is a contradiction. So some $b_i$ must not be in $\sqrt{q_j}$. And since field $k$ is infinte and perfect, there must be some choice of $\lambda_l$'s such that $u_i = \sum_{l=1}^{i-1} \lambda_l b_l$ must not be in $\sqrt{q_j}$. Hence $p_i \notin \sqrt{q_j}$.

□

Now we can use theorem 3.15 to get the similar result for affine polynomials.

**Corollary 3.16.** *If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ is a prime sequence of affine polynomials and given that $\langle f_1, \ldots, f_i \rangle \subseteq k[x_1, \ldots, x_n]$ is a radical ideal for $i \in [s - 1]$. Also define $I_i$ as the ideal $\langle f_1, \ldots, f_i \rangle \subseteq k[x_1, \ldots, x_n]$ for $i \in [s]$. Then we can find another sequence of affine polynomials $p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$ such that:*

1. *$p_1 = f_1, p_2 = f_2, p_i \equiv f_i \pmod{I_{i-1}}$ for $i \in [s]$,*
2. *$\hat{p}_1, \ldots, \hat{p}_s \in k[x_0, \ldots, x_n]$ is a regular sequence,*

3. $deg(p_i) \leq max\{deg(f_i), 5(n+1-i)deg(\hat{I}_{i-1})\}$ *if* $i \leq n$, *and*
   $deg(p_{n+1}) = max\{deg(f_{n+1}), deg(\hat{I}_n)\}$

*Proof.* Since $f_1, \ldots, f_s$ is prime sequence in $k[x_1, \ldots, x_n]$, $\hat{f}_1, \ldots, \hat{f}_s$ a prime sequence in $k[x_0, \ldots, x_n]/(x_0)$. Similarly $\langle \hat{f}_1, \ldots, \hat{f}_i \rangle$ is a radical ideal in $k[x_0, \ldots, x_n]/(x_0)$ for $i \in [s-1]$. Then on applying theorem 3.15 we get polynomials $P_1, \ldots, P_s \in k[x_0, \ldots, x_n]$ satisfying the properties stated in theorem 3.15.

Take $p_i = {}^aP_i$, the affinization of $P_i$ s for $i \in [s]$. Then the first condition follows directly by this affinization.

Now considering the sequence $\hat{p}_1, \ldots, \hat{p}_s \in k[x_0, \ldots, x_n]$, we have $x_0^{r_i}\hat{p}_i = P_i$ where $r_i \geq 0$ for $i \in [s]$. So if $P_1, \ldots, P_s \in k[x_0, \ldots, x_n]$ is a regular sequence then $\hat{p}_1, \ldots, \hat{p}_s \in k[x_0, \ldots, x_n]$ is also a regular sequence and hence condition 2 follows.

It is also clear that $deg(\hat{p}_i) \leq deg(P_i)$ and $I_{i-1}^c$ for $P_i$ s is nothing but homogeneous ideal $\hat{I}_{i-1}$ for $i \in [s]$. Also $deg(F) = deg(x_0) = 1$, hence it proves the bound on degree of $p_i$s. □

### 3.6.5 Effective Hilbert Nullstellensatz

Again we come to our main question. Let $g, f_1 \ldots, f_s$ are given polynomials in affine polynomial ring $k[x_1, \ldots, x_n]$ such that $g \in \langle f_1, \ldots, f_s \rangle$, then by hilbert nullstellensatz,

$$g = a_1 f_1 + \ldots + a_s f_s$$

with $deg(a_i f_i) \leq deg(g) + D$ for $i \in [s]$ if and only if

$$x_0^D \hat{g} \in \langle \hat{f}_1, \ldots, \hat{f}_s \rangle \subseteq k[x_0, \ldots, x_n]$$

So we want an upper bound on $D$ such that $x_0^D \hat{g} \in \langle \hat{f}_1, \ldots, \hat{f}_s \rangle$.

In the previous section we saw that if we are given a prime sequence with some additional property then we can form another prime sequence of bounded degree which when homogenized forms a regular sequence of homogeneous polynomials. This was the core of Sombra's paper [Som97], where the paper of Dube [Dub93] was incorrect. When we have such a regular sequence of homogeneous polynomials we can apply the ideas given in section 6 of Dube's paper with a little modification to get bound on $D$. We will not prove those theorems but refer to them whenever needed and we will follow Sombra's paper.

The notations used here and in Sombra's paper are consistent with that of Dube's paper and so the interested readers who will refer Dube's paper will find it easy to get the flow.

Without loss of generality, field $k$ is assumed to be algebraically closed. For $s \leq n+1$, Let us given an affine prime sequence $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$ such that the ideal $\langle h_1, \ldots, h_i \rangle$ is radical for all $i \in [s-1]$. For $i \in [s]$, definition of some terms from T. Dube are given as follows:

$$\begin{aligned} I_i &:= \langle h_1, \ldots, h_i \rangle \subseteq k[x_1, \ldots, x_n] \\ H_i &:= \langle \hat{h}_1, \ldots, \hat{h}_i \rangle \subseteq k[x_0, \ldots, x_n] \\ \hat{I}_i &:= \langle \{\hat{f} \mid f \in I_i\} \rangle \subseteq k[x_0, \ldots, x_n] \\ J_i &:= \langle \hat{I}_{i-1}, \hat{h}_i \rangle \subseteq k[x_0, \ldots, x_n] \end{aligned}$$

If primary decomposition of $J_i$ is as follows,

$$J_i := \bigcap_{j=1}^{r} Q_j$$

Then $J_i^*$ is defined to be the intersection of those primary ideals of $J_i$ which have height $\leq i$ or dimension $\geq n-i$. This $J_i^*$ is well defined and is always unique. The primary decomposition of $J_i^*$ may not be unique. One other terms defined in T. Dube is $\gamma$. Let we have $\gamma_1 := 0$ and for $i \in [n]$, $\gamma_i := deg(h_i)deg(\hat{I}_{i-1}) - \hat{I}_i$ and $\gamma_{n+1} := deg(h_{n+1}) + deg(\hat{I}_n) - 1$. Then following proposition follows by Sombra [Som97],

**Proposition 3.17.** *If $g \in I_i$ for $1 \leq i \leq s$ . Then $x_0^{\gamma_i} \hat{g} \in J_i^*$.*

We omit proof of this. This proposition is totally technical in nature and just used as a tool to prove bound on $D$, hence we refer the reader to see lemma 5.5 of T. Dube [Dub93] and proposition 4.33 of M. Sombra [Som97].

Now on applying corollary 3.16 to the prime sequence $h_1, \ldots, h_s$ we get new sequence $p_1, \ldots, p_s$ such that,

1. $p_1 = h_1, p_2 = h_2$ and $p_i = h_i + u_i \in I_i$ where $u_i \in I_{i-1}$ for $3 \leq i \leq s$
2. $\hat{p}_1, \ldots, \hat{p}_s \in k[x_0, \ldots, x_n]$ is a regular sequence, and
3. $deg(p_i) \leq max\{deg(h_i), 5(n+1-i)deg(\hat{I}_{i-1})\}$ for $1 \leq i \leq n$, and
   $deg(p_{n+1}) = max\{deg(h_{n+1}), deg(\hat{I}_n)\}$

On homogenizing $p_i$s we have, $p_i = x_0^{c_i} \hat{h}_i + \hat{u}_i$ where $c_1 = c_2 = 0$ and $c_i = max\{0, 5(n+i-1)deg(\hat{I}_{i-1}) - deg(h_i)\}$ for $i \in [n]$ and $c_{n+1} = max\{0, deg(\hat{I}_n) - deg(h_{n+1})\}$.

The following lemma is due to Dube [Dub93][Section 6, lemma 6.1,6.2] and proposition 3.17.

**Lemma 3.18.** *If $g \in I_i$ then $x_0^{D_i}\hat{g} \in H_i$,*

$$D_i = \sum_{j=2}^{i}(i-j+1) + \sum_{j=3}^{i-1}(i-j)c_j$$

*for $2 \leq i \leq s$.*

*Proof.* □

Now we can bound $D$ using the lemma 3.18. Actually $D = max_s\{D_s\}$.

**Proposition 3.19.** *Let $d := max_{1\leq i\leq s} deg(h_i)$. We have following bound on $D_s$,*

1. $D_s \leq s^2(d-1+3n)max_{1\leq i\leq s-1}deg(\hat{I}_i)$ *for $s \leq n$*
2. $D_{n+1} \leq n^2(d-1+3n)max_{1\leq i\leq s-1}deg(\hat{I}_i)$

We omit its proof. It is just a calculative part, to see details see proposition 4.35 of Sombra [Som97].

As mentioned in the start of this section, we are given polynomials $f_i, \ldots, f_s$ whose ideal $I$ have height $\geq s$. $f_i$s do not necessarily form a prime sequence. So how can we apply all our ideas. Well, there are some ways for such kind of polynomials. It is proven that for such kind of polynomials we can find another sequence $h_1, \ldots, h_t$ where $t \leq s$ such that,

1. $h_1, \ldots, h_t$ form a prime sequence,
2. $\langle h_1, \ldots, h_t\rangle = \langle f_1, \ldots, f_s\rangle$
3. $\langle h_1, \ldots, h_t\rangle \subseteq k[x_1, \ldots, x_n]$ is a radical ideal for $1 \leq i \leq t-1$.

Dube [Dub93] section 3 gives a simple proof that linear combination of $f_1, \ldots, f_s$ is enough to form one such $h_1, \ldots, h_t$ in any charactesristic. This result can also be proved using bertini's theorem. Let $d$ be maximum of the degree of $f_i$s and suppose that $deg(f_i) \leq deg(f_{i+1})$ for $1 \leq i \leq s-1$. Then in characteristic zero field we can take $deg(h_i) \leq deg(f_i)$ for $1 \leq i \leq s-1$, and $deg(h_i) \leq (d+1)$ in positive characteristic.

Now we will state the main theorem which gives bound for the degree in effective nullstellensatz,

**Theorem 3.20** (Effective Nullstellensatz)**.** *Let we are given polynomials* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ *of degree st most* $d$ *such that* $1 \in \langle f_1, \ldots, f_s \rangle$*. Then there exists* $a_1, \ldots, a_s \in k[x_1, \ldots, x_n]$ *such that*

$$1 = a_1 f_1 + \ldots + a_s f_s$$

*with* $deg(a_i f_i) \leq m^2(d+3n)(d+1)^{m-1}$*, where* $m = min\{n, s\}$*.*

*Proof.* In proposition 3.19 we can replace $d$ by $d+1$ which is maximum over degree of any $h_i$. And maximum over deg $\hat{I}_i$ can be obtained by maximum over deg $I_i^c$ mentioned in theorem 3.15. This degree bound is proven in a bézout-type lemma in Sombra[Som97][Lemma 3.32]. Hence the theorem follows. □

## 3.7 Conclusion

We saw how ideals and varieties are closely related. One represents algebraic and other represents geometric aspect and HN is the bridge between them. We saw an elementary algebraic proof of HN and also the proof of its quantitative version- Effective HN. In next Chapter we will see the only known result which improves the complexity of HN over zero characteristic than PSPACE.

# Chapter 4

# Hilbert's Nullstellensatz is in Arthur-Merlin Class Under GRH

In this Chapter we will discuss a result about the consistency question stated in the previous Chapter. Koiran [Koi96] proved that Hilbert's Nullstellensatz over characteristic zero is in Arthur-Merlin (AM) class under the assumption of a famous unproven hypothesis known as "Generalized Riemann Hypothesis (GRH)". To achieve this result he used Effective Hilbert's Nullstellensatz only indirectly. We will present here the intuition behind his idea and sketch of his proof. The proof sketch presented here is also inspired by the lecture notes of Madhu Sudan [Sud98].

## 4.1 Problem statement

Input: Given a system of polynomial equations $S = \{f_1 = 0, \ldots, f_m = 0\}$, where $f_i \in \mathbb{Z}[x_1, \ldots, x_n]$ has total degree $d_i$ for $i \in [m]$. Coefficients of these polynomials in $\mathbb{Z}$ are at most $C$ and $d \in \mathbb{N}$ is such that $d = max\{d_1, \ldots, d_m\}$.

Output: Decide if $S \in L$, where $L = \{S \mid S$ is satisfiable system of polynomial equations over $\mathbb{C}\}$.

Clearly we can see that size $|S|$ of this system is $poly(n, m, d, \log C)$.

## 4.2 Some examples

In this section we will see some examples and analyze if they have solution over $\mathbb{C}$ and over $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$.

**Example 4.1.** *Consider the following system $S$ over $\mathbb{Z}[x, y]$,*

$$S = \begin{cases} xy - 6 = 0 \\ x - 2 = 0 \end{cases}$$

*This system is satisfiable over $\mathbb{C}$, in fact over $\mathbb{Z}$, $(2, 3)$. And we can see it is satisfiable in $\mathbb{Z}/p\mathbb{Z}$ for any prime $p$. Actually we know its solution will be $(2 \bmod p, 3 \bmod p)$ in $\mathbb{Z}/p\mathbb{Z}$ for any prime $p$.*

Let's see an example of unsatisfiable system over $\mathbb{C}$.

**Example 4.2.** *Consider the following system $S$ over $\mathbb{Z}[x, y]$,*

$$S = \begin{cases} (xy)^6 - 1 = 0 \\ x - 2 = 0 \\ y - 3 = 0 \end{cases}$$

*Clearly this system has no solution over $\mathbb{C}$ but if we look carefully it has solution $(2 \bmod 5, 3 \bmod 5)$ in $\mathbb{Z}/5\mathbb{Z}$ and $(2 \bmod 7, 3 \bmod 7)$ in $\mathbb{Z}/7\mathbb{Z}$.*

It will soon be clear why we are looking for solution in some $\mathbb{Z}/p\mathbb{Z}$ but for now we can see that a satisfiable system can be unsatisfiable in some $\mathbb{Z}/p\mathbb{Z}$ and an unsatisfiable system can be satisfiable in some $\mathbb{Z}/p\mathbb{Z}$.

## 4.3 Intuition and main idea

We see that satisfiable system of example 1 is satisfiable in $\mathbb{Z}/p\mathbb{Z}$ for any prime $p$ but this will never happen in case of unsatisfiable system. If a given system is unsatisfiable over $\mathbb{C}$ then for any solution $(a_1, \ldots, a_n) \in \mathbb{C}^n$ there will be only bounded number of primes $p$ for which system will be satisfiable in $\mathbb{Z}/p\mathbb{Z}$. This leads us to a guess that a satisfiable system may remain satisfiable for many primes $p \leq x$, for some carefully chosen $x$, in $\mathbb{Z}/p\mathbb{Z}$. On

the contrary, unsatisfiable systems may be satisfiable for significantly lesser number of primes $p$ in $\mathbb{Z}/p\mathbb{Z}$. This is the main idea of this result.

We got the intuition, now we will state the idea more formally. We will fix a number $x$ and check the satisfiability of given system in $\mathbb{Z}/p\mathbb{Z}$ for a randomly chosen prime $p \leq x$. The number $x$ will be chosen large enough so that probability of system being satisfiable in $\mathbb{Z}/p\mathbb{Z}$, when it is actually satisfiable over $\mathbb{C}$, will be much greater than probability of system being satisfiable in $\mathbb{Z}/p\mathbb{Z}$, when it was unsatisfiable over $\mathbb{C}$. This large gap will help us put this problem in class AM.

We state here two theorems which give us bound for various parameters. These will be proved later in section 4.5.

**Theorem 4.1.** *If given system $S$ is unsatisfiable over $\mathbb{C}$, then there are at most $x_1 = exp(|S|)$ number of primes $p \in \mathbb{Z}$ such that $S$ is satisfiable over $\mathbb{Z}/p\mathbb{Z}$.*

**Theorem 4.2.** *If given system $S$ is satisfiable over $\mathbb{C}$, then there are at least $x_2 = (|\pi(x)|/c_1 - c_2 - O(\sqrt{x}\log x))$ number of primes $p \in [x]$ such that $S$ is also satisfiable over $\mathbb{Z}/p\mathbb{Z}$. Where $\pi(x)$ is the set of all primes $\leq x$ and $c_1, c_2 = exp(|S|)$ are constants.*

Note that $O(\sqrt{x}\log x)$ is error term. So for big enough $x$, $|\pi(x)| = x/\log x \gg \sqrt{x}\log x$. On picking $x = exp(|S|)$ suffices for $x_2 \gg x_1$.

## 4.4 Putting HN in AM

Now that we have all the setup, in this section we will prove that deciding the existence of a solution for a system of multivariate polynomial equations over $\mathbb{C}$ is indeed in class AM. Our simple algorithm can be: let Arthur pick a random prime number $p$ from $\pi(x)$ and give it to Merlin. Merlin then finds a solution $(a_1, \ldots, a_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ and pass it to Arthur. Arthur verifies if it is indeed a solution for the system. Since $x$ is exponential in size of the system, $p$ can also be at most exponential in system size and hence solution given by Merlin will be of polynomial size. So Arthur can check in polynomial time whether it is a solution or not.

The only problem is that $|\pi(x)|$ can be much larger than $x_1$ and $x_2$ so it will give bad probability even for yes input. Good thing is that relatively $x_2$ is much larger than $x_1$ (we can take $x_2 > 4x_1$) so we can map the space $\pi(x)$ to another compact space and

then calculate the probability. This is a complexity theoretic technique. To learn more we suggest reader to read book by Arora and Barak [AB09][Chapter 8].

Denote space $\pi(x)$ as $U$. Now we will use a universal family of hash function $H$ to map space $U$ to another compact space $V$. Let $|V| = x_2$. For any $W \subset U$ with $|W| = \alpha|V|$ for $\alpha \leq 1$. Then for a randomly chosen $h \in H$ and $v \in V$,

$$\alpha - \alpha^2/2 \leq Pr(v \in h(W)) \leq \alpha$$

when we have $W$ as set of those primes $p$ of $U$ such that system is satisfiable in $\mathbb{Z}/p\mathbb{Z}$, then $|W| = x_2$ for satisfiable system and $|W| = x_1$ for unsatisfiable system. Hence in case of unsatisfiable system probability is at most $\alpha \leq 1/4$ and for satisfiable system probability is at least $\alpha - \alpha^2/2 = 1 - 1/2 = 1/2$.

Now we can give our new algorithm.

- Arthur picks a random hash function $h \in H$ and random $v \in V$ and pass it to merlin.
- Merlin returns $t$, such that $h(t) = v$ and also gives solution $(a_1, \ldots, a_n) \in (\mathbb{Z}/t\mathbb{Z})^n$.
- Arthur verifies that $h(t) = v$ and also verifies that $(a_1, \ldots, a_n)$ is indeed a solution $\in (\mathbb{Z}/t\mathbb{Z})^n$.

As calculated before Arthur does all calculation in randomized polynomial time with probability for yes instance at least $1/2$ and for no instance at most $1/4$. So our question is in AM.

## 4.5 Proof Sketch for Bounds

In this section we will prove our previously stated theorems in section 4.3 which provide bound for various parameters. First we will see easy one, unsatisfiable case, then harder one, satisfiable case. We will only discuss the crucial part of the proof to make the idea clear. We will omit proof of some details which we think will not distract the reader.

### 4.5.1 Unsatisfiable case

If the given system of equations $\{f_1, \ldots, f_m\} \subset \mathbb{Q}[x_1, \ldots, x_n]$ is unsatisfiable over $\mathbb{C}$ then by Hilbert's Nullstellensatz $1 \in \langle f_1, \ldots, f_m \rangle$ or in other words $\exists g_1, \ldots, g_m \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$

such that

$$f_1g_1 + f_2g_2 + \ldots + f_mg_m = 1. \tag{4.1}$$

We can see easily see that coefficients of $g_i$s are in $\mathbb{Q}$. Since coefficients of $f_1, \ldots, f_m$ are actually in $\mathbb{Z}$ we can multiply by suitable integer $a$ on both side of equation 4.1 so that coefficients of $g_i$'s are now in $\mathbb{Z}$. We can rewrite equation 4.1 as

$$f_1g_1 + f_2g_2 + \ldots + f_mg_m = a. \tag{4.2}$$

where $g_1, \ldots, g_m \in \mathbb{Z}[x_1, \ldots, x_n]$. If this system is to be satisfiable in some $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$ then $p$ must divide $a$. By elementary number theory, we know there can be at most $\log a$ such primes. Theorem 4.1 says that there are at most $exp(|S|)$ primes $p$ such that $S$ is satisfiable in $\mathbb{Z}/p\mathbb{Z}$, so to prove the theorem, $a$ should be $exp(exp(|S|))$ which we claim next.

**Claim 4.3.** *The constant $a$ satisfying equation 4.2 can be at most doubly exponential in $|S|$.*

*Proof.* To get information about $a$ we first need to get information about the rational coefficients of $g_i$'s in equation 4.1. Since coefficients of $f_i's$ are known, we can form a system of linear equations out of equation 4.1 whose coefficients are coefficients of $f_i$'s and unknowns are coefficients of $g_i$'s. Since coefficients of $f_i$'s are in $\mathbb{Z}$, solution to this linear system is in $\mathbb{Q}$ and LCM of the denominator of this solution will be our $a$.

By Effective Hilbert's Nullstellensatz as done in Chapter 3, degree of each $g_i$ is at most $exp(|S|)$, hence the number of unknowns are also $exp(|S|)$ and the size of linear system is also $exp(|S|)$.

Now we solve the linear system by cramer's rule [CG50]. So in solution value of every unknown has denominator which is a determinant of exponential size and value of a determinant in worst case can be exponential in its size, hence the denominator of each unknown is a constant of value $exp(exp(|S|))$. So the LCM $a$ can be at most $exp(exp(|S|))$. Hence the claim follows. □

Above argument proves the Theorem 4.1 which gives us bound on the number of $p$'s for which an unsatisfiable system is satisfiable in $\mathbb{Z}/p\mathbb{Z}$. Next we will prove bound given by theorem 4.2 for satisfiable case.

### 4.5.2 Satisfiable case

Proof in this section is more involved and requires use of diverse areas such as basic field theory, results in analytical number theory and quantifier elimination. Our objective is to make proof understandable to reader so where ever required we will go in detail and in some cases elaborate by examples but in other cases we will just state the theorems without providing proofs.

We saw in example 4.1 that it is possible for a satisfiable system to remain satisfiable in $\mathbb{Z}/p\mathbb{Z}$s for every prime $p$. That example gave us clue about unboundedness on the number of primes in satisfiable case. If we fix some number $N$ then there are $\pi(N)$ primes $\leq N$. Whenever there is a zero $\overline{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, the system will be satisfiable for all primes $p \in \pi(N)$ with the corresponding zero $(a_1 \pmod p, \ldots, a_n \pmod p)$ in $(\mathbb{Z}/p\mathbb{Z})^n$. So this case follows theorem 4.2 with the maximum possible number of primes in $[N]$.

We next see another example which will give us the idea why the number of good primes can not be $\pi(N)$ every time.

**Example 4.3.** *Consider the given system of equation over* $\mathbb{Z}[x, y, z]$

$$S = \begin{cases} xy - z^2 = 0 \\ 2x - 1 = 0 \\ x - 9y = 0 \end{cases}$$

*This system is satisfiable over* $\mathbb{C}$ *and the solutions of this system are* $(1/2, 1/18, \pm 1/6)$ *or after normalizing the denominator* $(9/18, 1/18, \pm 3/18)$ *over* $\mathbb{C}^3$. *In* $\mathbb{Z}/2\mathbb{Z}$ *this system is not satisfiable because second equation gives* $1 = 0$, *and also in* $\mathbb{Z}/3\mathbb{Z}$ *this system is unsatisfiable because second equation gives* $x = 2$ *and third equation gives* $x = 0$, *two inconsistent values for* $x$. *But in* $\mathbb{Z}/5\mathbb{Z}$ *it has a solution* $(3, 2, 1) \equiv (9.18^{-1} \pmod 5, 1.18^{-1} \pmod 5, 3.18^{-1} \pmod 5)$. *Indeed this system is satisfiable in* $\mathbb{Z}/p\mathbb{Z}$ *for any prime* $p$ *except* 2 *and* 3. *Because as we saw in* $\mathbb{Z}/5\mathbb{Z}$ *the denominator* 18 *has inverse but since* 2 *and* 3 *are only prime factors of* 18 *so it doesn't have inverse in those two prime fields. So this system will be satisfiable in* $\pi(N) - 2$ *prime fields for* $N \geq 3$.

The above example shows us that satisfiable system will be unsatisfiable in $\mathbb{Z}/p\mathbb{Z}$ for some primes $p$ because those primes divide common denominator of the solution in $\mathbb{Q}^n$. This way we have solution for fewer than maximum possible number of primes $\pi(N)$. As a general rational-zero example we can show that common denominator $b$ can not be more

than $exp(exp(|S|))$, hence number of primes diving $b$ can be at most $exp(|S|)$. So the system will be satisfiable for at least $\pi(N) - exp(|S|)$ primes $p$ again following theorem 4.2.

Example 4.3 also directs our proof for any general zero $\overline{a} = (a_1, \ldots, a_n) \in \overline{\mathbb{Q}}^n$. We will try to form new zero in rational form as in example 4.3. To achieve this, we will use some tricks of *Galois Theory*.

Suppose $\overline{a} = (a_1, \ldots, a_n) \in \overline{\mathbb{Q}}^n$ is a zero of given system. If $\overline{a}$ is actually over $\mathbb{Q}^n$ then we can apply the previous trick for rational-zeros. But if $\overline{a}$ is not rational then each coordinate $a_i$ is in some field extension $\mathbb{Q}(a_i)$ or collectively they are in field extension $\mathbb{Q}(a_1, \ldots, a_n)$. Clearly this exrension of $\mathbb{Q}$ is a finite extension so by primitive element theorem in galois theory, this extension is actually isomorphic to an extension by only one element $\mathbb{Q}(\alpha)$, for some $\alpha \in \overline{\mathbb{Q}}$. So there must be a minimal polynomial $R(x) \in \mathbb{Q}[x]$ for $\alpha$. On multiplying $R(x)$ by the common denominator of its coefficients, we can see $R(x)$ in $\mathbb{Z}[x]$. Also, since $a_1, \ldots, a_n \in \mathbb{Q}(\alpha)$, so $a_1, \ldots, a_n$ are actually polynomials in $\alpha$ over $\mathbb{Q}$. We can also represent $a_i$ as $p_i(\alpha)/q$, where $p_i(x) \in \mathbb{Z}[x]$ and $q \in \mathbb{Z}$, for $i \in [n]$. The following lemma follows from the results in galois theory about primitive elements and quantifier elimination. We are omitting its proof, for more details see [Koi96][Theorem 4,6,7].

**Lemma 4.4.** *For an appropriate choice of the zero $\overline{a}$, degree of $R$ is $exp(|S|)$ and $q$ and coefficients of $R$ are $exp(exp(|S|))$.*

Now consider a univariate system $\{g_1(x) = 0, \ldots, g_m(x) = 0\}$, where

$$g_i(x) = q^d f(p_1(x)/q, \ldots, p_n(x)/q).$$

for $i \in [m]$. Hence $g_i(\alpha) = q^d f(p_1(\alpha)/q, \ldots, p_n(\alpha)/q) = q^d f(a_1, \ldots, a_n) = 0$. Now since $R$ is minimal polynomial for $\alpha$ and $\alpha$ is also a zero of all $g_i$'s, $R$ must divide $g_i$ for $i \in [m]$. We now have simplified the things. What we want is: count of all those primes $p \leq N$ which doesn't divide $q$ and $R$ has some solution $\gamma$ over $\mathbb{Z}/p\mathbb{Z}$. Solution of $R$ will ensure solution of $g_i$'s and that ensures solution of original system in $\mathbb{Z}/p\mathbb{Z}$. So this count will actually give the required count $x_2$.

Suppose $R$ has degree $D$ and let $\Delta$ be the discriminant of $R$ ie, $\Delta = Res(R, R')$, where $R'$ is first order derivative of $R$. Also we know that $R$ is irreducible. Then for a prime $p$

$$W(p) := |\{k \mid R(k) \equiv 0 \pmod{p}, 0 \leq k \leq p-1\}|$$

is the number of zeros of $R$ in $\mathbb{Z}/p\mathbb{Z}$. Adleman and Odylzko [AO83] gave the following bound

**Theorem 4.5.**

$$|S(N)| = O(\sqrt{N}\log(\Delta N^D))$$

*where* $S(N) := \Sigma'_{p\leq N}(1 - W(p))$. $\Sigma'$ *means summation over those* $p$*'s which do not divide* $\Delta$.

This result assumes *Generalized Riemann Hypothesis* and comes through effective version of *Chebotarev Density Theorem*. Cleary we can see that

$$\Sigma'_{p\leq N}W(p) \geq \Sigma'_{p\leq N}1 - O(\sqrt{N}\log(\Delta N^D))$$

Now we want $(1/D)\Sigma'_{p\leq N}W(p)$, since $R$ can have at most $D$ roots in $\mathbb{Z}/p\mathbb{Z}$. Also we know that $\Sigma'_{p\leq N}1 = \pi(N) - \log\Delta$. Hence

$$x_2 = (1/D)[\pi(N) - \log\Delta - c.\sqrt{N}\log(\Delta N^D)] - \log q$$

Following the bounds of lemma 4.4 we can easily see that it follows the theorem 4.2.

## 4.6 Conclusion

Looking at the proof we can see that riemann hypothesis is assumed only in the satisfiable case and indirectly just to give some bounds on number of primes for a univariate polynomial $R$. It is an interesting open question whether this proof can be made unconditional? Also it is proved in case of unsatisfiable system that the upper bound on the number of primes is exponential. This bound can't be improved. In fact koiran gave an example

$$S = \begin{cases} x^{\pi_n} - 1 = 0 \\ x - \pi_n = 0 \end{cases}$$

This system is unsatisfiable over $\mathbb{C}$ but he showed that it is satisfiable in $\mathbb{Z}/p\mathbb{Z}$ for exponential number of primes $p$. For proof we refer to his paper [Koi96].

# Chapter 5

# Hilbert's Nullstellensatz Over Positive Characteristic

In this Chapter we will present our work. We started attacking the problem aiming to put it in NP. We divide the problem in two cases: one when the zero set defined by the system is positive dimensional and the one when the zero set is zero dimensional.

In the first case, we will solve three special cases of positive dimensional systems in NP. These cases are formally stated in a single promise problem 2. The general affine algebraic sets of positive dimension do not behave well and we will see an example for this in section 5.3.

Next case is for affine zero dimensional algebraic sets. We don't have any special result about them but we will show that by using the same characterization of certificate as in section 5.1, affine zero dimensional systems can not be put in NP.

Further in section 5.3 we give a reduction of affine zero dimensional systems to affine positive dimensional systems, which indicates that affine positive dimensional case is more hard than affine zero dimensional case. Unless mentioned the space of algebraic sets is assumed to be affine.

## 5.1 Positive Dimensional Systems

In this section we will see that if the zero set generated by given system of polynomial equations over $\mathbb{F}_q$ has positive dimension then the problem of deciding the consistency of

this system actually falls in class NP provided that zero set follows any one of the three constraints explained in problem 2.

We will address the following promise problem:

**Problem 2.** *Given a system $S$ of $m \geq 1$ affine (or homogeneous) polynomials $f_1, \ldots, f_m$ in the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ (or respectively $\mathbb{F}_q[x_0, \ldots, x_n]$) over a finite field $\mathbb{F}_q$ such that $deg(f_i) \leq d$, for $i \in [m]$. Let $X \subseteq \mathbb{A}^n(\overline{\mathbb{F}}_q)$ (or resp. $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$) is zero set of the system $S$. Also it is promised that,*

1. *either $X$ is empty or,*
2. *$X$ has positive dimension $r$ and follows either of the following conditions,*
   (a) *$X$ is absolutely irreducible affine (or resp. projective) variety or,*
   (b) *$X$ is reducible affine algebraic set but one of its absolutely irreducible component of dimension $r$ is $\mathbb{F}_q$-definable or,*
   (c) *$X$ is reducible projective algebraic set but one of its absolutely irreducible component of dimension $r$ is $\mathbb{F}_q$-definable by $m' \geq 1$ polynomials of degree at most $\delta$ such that $\delta^{m'} \leq d^m$.*

*Decide if $X = \phi$ over $\mathbb{A}^n(\overline{\mathbb{F}}_q)$ (or resp. $\mathbb{P}^n(\overline{\mathbb{F}}_q)$)?*

We assume that input is given in form of usual sparse representation (coefficient degree pair for each non-zero term) of $m$ polynomials. Hence $|S| = O(m(n \log d + \log q)\#M)$, where $\#M$ is the maximum number of non-zero terms in a polynomial, i.e. maximum sparsity of a polynomial which can be at most $d^n$.

The theorem 5.1 solves the promise problem 2.

**Theorem 5.1.** *The promise problem 2 is in* NP.

*Proof.* We first present an algorithm 1 and then prove that it actually puts the promise problem 2 in NP.

The correctness of algorithm is obvious except in step 2 where we are not sure whether we can always get some $\overline{a}$ of bit-size polynomial in $|S|$. We will prove that small zeros always exist for a system as described above.

Consider a field extension of base field $\mathbb{F}_q$ of finite degree $k$, i.e, $\mathbb{F}_{q^k}$. For notational convenience denote $q^k$ by $\hat{q}$. We would like to know the least value of $k$ such that this

**Algorithm 1** Algorithm for promise problem 2

1. Verifier gets the data as stated in promise problem, and asks prover for certificate.
2. Prover gives verifier a zero of system $S$ as a certificate, $\overline{a} \in \mathbb{A}^n(\overline{\mathbb{F}}_q)$ or $\overline{a} \in \mathbb{P}^n(\overline{\mathbb{F}}_q)$.
3. Verifier verifies $\overline{a}$ by checking whether $f_i(\overline{a}) = 0$, for all $i \in [m]$.
4. If the answer is yes in step 3 then output "**Yes**" else output "**No**".

extension will have at least one zero of $X$. If $\hat{q}$ is at most exponential in $|S|$ then we are done since bit-size of $\overline{a}$ will then be $O(n \log \hat{q})$ which is polynomial in $|S|$.

Fortunately we have the following inequality in a remarkable result by Lang and Weil [LW54] for number of points of an absolutely irreducible projective variety over a finite field. We will present the effective version of their result given by Ghorpade and Lachaud [GL02] who also extended the result for affine variety as well,

**Theorem 5.2.** *If $V$ is an absolutely irreducible projective variety in $\mathbb{P}^n$ or absolutely irreducible affine variety in $\mathbb{A}^n$ defined over finite field $\mathbb{F}_q$, such that $dim(V) = r$ and $deg(V) = d$, then*

$$\begin{aligned} ||V(\mathbb{F}_q)| - \pi_r| &\leq (d-1)(d-2)q^{r-\frac{1}{2}} + Aq^{r-1} && \text{when } V \text{ is projective variety} \\ ||V(\mathbb{F}_q)| - q^r| &\leq (d-1)(d-2)q^{r-\frac{1}{2}} + Aq^{r-1} && \text{when } V \text{ is affine variety} \end{aligned}$$

*where $\pi_r$ is the cardinality of $r$-projective space over $\mathbb{F}_q$ which is $|\mathbb{P}^r(\mathbb{F}_q)| = q^r + q^{r-1} + \ldots + q + 1 = \theta(q^r)$ and $A$ is constant with respect to underlying field $\mathbb{F}_q$ and depends only on $n, d'$ and $r$. Also if $V$ is $\mathbb{F}_q$-definable by $m$ polynomials of degree at most $\delta$ then,*

$$A \leq \begin{cases} 9 \times 2^m(m\delta + 3)^{n+1} & \text{when } V \text{ is projective variety} \\ 6 \times 2^m(m\delta + 3)^{n+1} & \text{when } V \text{ is affine variety} \end{cases}$$

The above inequality simply means that the number of points of $V$ in $\mathbb{P}^n(\mathbb{F}_q)$ (or $\mathbb{A}^n(\mathbb{F}_q)$) differs with $\pi_r$ (or $q^r$) at most by the error term $(d-1)(d-2)q^{r-\frac{1}{2}} + Aq^{r-1}$. If $q$ is such that $q^{r-\frac{1}{2}} \gg (d-1)(d-2)$ and $q^{r-1} \gg A$ then the error term is dominated by the quantity $q^{r-\frac{1}{2}}$ which is much smaller than $\theta(q^r)$ for sufficiently large $q$. Hence as we move to higher extension fields, we start getting zeros of the $V$.

Coming to the promise problem, consider part (a). Since $X$ is absolutely irreducible, we can apply theorem 5.2 directly. By the bézout's theorem 2.1 we get that degree of $X$, $\deg X \leq d^m$. Without loss of generality suppose $X(\mathbb{F}_q) = \phi$ otherwise we have a

point $\overline{a} \in (\mathbb{F}_q)^n$ of bit-size $O(n \log q)$ which is polynomial in $|S|$. Now consider some field extension $\mathbb{F}_{\hat{q}}$. For $X$ to have a point in $(\mathbb{F}_{\hat{q}})^n$,

$$\hat{q}^{r-\frac{1}{2}} \gg (d^m)^2 \text{ and } \hat{q}^{r-1} \gg 9 \times 2^m (md+3)^{n+1}$$

$$\Rightarrow \log \hat{q} = O(\max\{m \log d, m + n(\log d + \log m)\})$$

This implies that $\log(\hat{q})$ is polynomial in input size $|S|$ which implies the existence of small certificate $\overline{a}$ for part (a) in both affine and projective case.

Part (c) also follows easily by the arguments of part (a). We just need to apply the theorem 5.2 over absolutely irreducible component $V$ of $X$. We know by the definition of degree of reducible algebraic sets, $\deg V \leq \deg X$ or $\deg V \leq d^m$. Hence on applying theorem 5.2 we have,

$$\hat{q}^{r-\frac{1}{2}} \gg (d^m)^2 \text{ and } \hat{q}^{r-1} \gg 6 \times 2^{m'} (m'\delta+3)^{n+1}$$

The second inequality is crucial. We have,

| | |
|---|---|
| $\Rightarrow \hat{q} = O(2^{m'} \times m'^n \times \delta^n)$ | ignoring first inequality |
| $\Rightarrow \hat{q} = O(2^{m'+n \log m'} \times \delta^n)$ | |
| $\Rightarrow \hat{q} = O(\delta^{m'} \times \delta^{m'})$ | *considering* $\delta > 2$ *and* $m' > n$ |
| $\Rightarrow \hat{q} = O(d^{2m})$ | *by the assumption in part* (b) *that* $\delta^{m'} \leq d^m$ |
| $\Rightarrow \log \hat{q} = O(m \log d)$ | |

So again we have small certificate for part (c) of promise problem.

Now we consider the part (b). We have following estimate by Cafure and Matera [CM06] for the number of points of an absolutely irreducible affine variety over a finite field,

**Theorem 5.3.** *Let $V \subseteq \mathbb{A}^n$ is an absolutely irreducible affine $\mathbb{F}_q$-definable variety of dimension $r > 0$ and degree $\delta$. If $q > 2(r+1)\delta^2$ then,*

$$||V(\mathbb{F}_q)| - q^r| \leq (\delta-1)(\delta-2)q^{r-\frac{1}{2}} + 5\delta^{\frac{13}{3}} q^{r-1}$$

Hence by the assumption in part (b), let $V \subset X$ be a $\mathbb{F}_q$-definable affine absolutely irreducible component of $X$ of dimension $r$. Again by the definition of degree for reducible algebraic sets, the degree of $V$, (say) $\delta \leq d^m$. By the similar arguments as for part (a), it is easy to see that the degree of field extension, where existence of a point of $V$ and hence $X$ is guaranteed, is not more than $poly(|S|)$. This proves the part (b) of promise problem.

Note that the bound given by Cafure and Matera [CM06] could have been applied to part (a) as well but these bounds are given only for affine varieties while the one given by Ghorpade and Lachaud [GL02] works for affine as well as projective varieties.

□

## 5.2 Zero Dimensional Affine Systems

We work here in affine space only. In this section we will analyze zero-dimensional systems. We will see that zero-dimensional case is harder than positive dimensional special case of section 5.1 and for this we provide some examples to support our claim.

Suppose the polynomials in our system are given as arithmetic circuits. We know that degree of a polynomial represented by a circuit can be exponential in the size of the circuit. As we are trying to put "HN for zero-dimensional ideals over a finite field" in class NP, we again are considering that prover will provide a zero of the polynomial system as certificate to verifier. Our main concern is in proving that we can have at least one such certificate of polynomial size for this kind of systems. We will give some counter examples here to show that this problem can not be put in class NP, at least with the assumption that certificate is a zero of the system.

**Observation 5.4.** *Given a univariate system of only one equation over* $\mathbb{F}_{p^m}[x]$

$$S = \{x^b - a = 0\}$$

*In this setup* $b$ *is a prime and* $m$ *is such that* $b|(p^m - 1)$*. Also, since we know that* $p$ *is exponential in input size (coefficients are of* $O(\log p)$ *size) we can assume that* $b \geq 2^s$ *where* $s$ *is system's size. And* $a \in \mathbb{F}_{p^m}$ *is* $b$*-th non-residue.*

*Clearly* $x^b - a$ *is an irreducible polynomial in* $\mathbb{F}_{p^m}[x]$ *and its zeros are in at least* $b$*-th degree extension of* $\mathbb{F}_{p^m}$*, i.e. over* $\mathbb{F}_{p^{mb}}$*. Hence size of certificate is* $\Omega(mb \log p)$ *which is not polynomial in input size.*

Now we will consider other representation of polynomials such as dense representation or sparse representation. There also we will see some zero-dimensional systems which have no zero of polynomial size. But before that we will prove a claim in number theory and then we will show some observations. Finally we will prove a theorem about the badness of the observation for any (sparse or dense) representation.

**Claim 5.5.** *If $p$ is a prime such that $p \equiv 1 \pmod 4$ and $a \in \mathbb{F}_p$ is a quadratic non-residue (qnr) then $a^{1/2^n}$ is a quadratic non-residue in $\mathbb{F}_{p^{2^n}}$ for any positive integer $n$.*

*Proof.* We prove our claim by induction over $n$. We know the qnr criteria over $\mathbb{F}_p$ is

$$a \in \mathbb{F}_p \text{ is qnr if } a^{(p-1)/2} \equiv -1 \pmod p$$

. Suppose $a \in \mathbb{F}_p$ is qnr then $\sqrt{a} \in \mathbb{F}_{p^2}$. For base case we need to show that $\sqrt{a}$ is qnr in $\mathbb{F}_{p^2}$, i.e,

$$\sqrt{a}^{(p^2-1)/2} \equiv -1 \pmod p$$

We have

$$\begin{aligned}
&\sqrt{a}^{(p^2-1)/2} \equiv (\sqrt{a}^p.\sqrt{a})^{(p-1)/2} \pmod p \\
&\equiv (-\sqrt{a}.\sqrt{a})^{(p-1)/2} \pmod p \\
&\equiv (-a)^{(p-1)/2} \pmod p \\
&\equiv -1 \pmod p.
\end{aligned}$$

The last equivalence follows because of the assumption $p \equiv 1 \pmod 4$ and by the criteria of qnr of $a \in \mathbb{F}_p$. Hence $\sqrt{a}$ is qnr in $\mathbb{F}_{p^2}$.

Now our induction hypothesis is: over $\mathbb{F}_{p^{2^{n-1}}}$, $a^{1/2^{n-1}}$ is qnr. It means

$$(a^{1/2^{n-1}})^{(p^{2^{n-1}}-1)/2} \equiv -1 \pmod p$$

. Hence over $\mathbb{F}_{p^{2^n}}$, we have

$$\begin{aligned}
&(a^{1/2^n})^{(p^{2^n}-1)/2} \equiv (a^{1/2^n}.(a^{1/2^n})^{p^{2^{n-1}}})^{(p^{2^{n-1}}-1)/2} \pmod p \\
&\equiv (a^{1/2^n}.(-a^{1/2^n}))^{(p^{2^{n-1}}-1)/2} \pmod p \\
&\equiv (-a^{1/2^{n-1}})^{(p^{2^{n-1}}-1)/2} \pmod p \\
&\equiv -1 \pmod p
\end{aligned}$$

Again last equivalence follows by induction hypothesis and qnr criteria and the fact that $(p-1)|(p^{2^m}-1)$ for any positive $m$, hence $(p^{2^{n-1}}-1)/2$ is even. Hence the claim follows. □

Now let's have a look at the following observation.

**Observation 5.6.** *Consider the zero-dimensional system*

$$S = \begin{cases} x_1^2 - a = 0 \\ x_2^2 - x_1 = 0 \\ x_3^2 - x_2 = 0 \\ \dots \\ x_n^2 - x_{n-1} = 0 \end{cases}$$

*over* $\mathbb{F}_p[x_1, \dots, x_n]$. *Its zero set is*

$$\mathcal{Z}(S) = \{(\pm\sqrt{a}, \pm\sqrt{x}_1, \pm\sqrt{x}_2, \dots, \pm\sqrt{x}_{n-1})\}$$

*over* $(\overline{\mathbb{F}}_p)^n$.

*Clearly it has finite number of solutions. By the claim proved above if* $a$ *is picked as qnr in* $\mathbb{F}_p$ *and* $p$ *is such as* $p \equiv 1 \pmod 4$, *then* $\sqrt{a}$ *will be qnr in* $\mathbb{F}_{p^2}$ *and* $a^{1/4}$ *will be qnr in* $\mathbb{F}_{p^4}$ *and so on. Hence any zero of this system will lie in the field extension* $\mathbb{F}_{p^{2^n}}$ *and not in any smaller degree field extension, so that the certificate size returned by the prover will be* $\Omega(n2^n \log p)$.

Now we will present theorem 5.7 which concludes that the HN for any arbitrary zero-dimensional system over positive characteristic is not in NP, under the assumption that certificate provided by prover is a zero of the given system.

**Theorem 5.7.** *There exists a system* $S$ *defining affine algebraic set* $V$ *over some* $\overline{\mathbb{F}}_q$, *such that* $\dim(V) = 0$ *and irrespective of the representation of the system* $S$ *(sparse or dense), its any zero will have bit-size* $exp(|S|)$, *where* $|S|$ *is the size of system* $S$.

*Proof.* Proof is divided into two parts. First part is for sparse representation and second part is for dense representation. Consider the example in observation 5.6.

In case of sparse representation, each polynomial of ideal has constant sparsity 2 and constant degree 2, so system's size would be $O(n(\log p + n))$. But as we pointed out in observation 5.6 that the certificate size returned by prover is $\Omega(n2^n \log p)$, which is clearly exponential in system's size.

In case of dense representation, a total degree $d$ multivariate polynomial over $n$ variables can have at most $\binom{n+d}{d}$ different terms, which is approximately $O(d^n)$. So it seems that certificate size would be polynomial in input size, but again same observation 5.6 is bad for this case too. Since degree in observation 5.6 is constant $d = 2$, hence $\binom{n+d}{d}$ will be

approximated as $O(n^2)$, so the size of system in dense representation will be $O(nn^2 \log p) = O(n^3 \log p)$. Hence again size of a zero of this system $\Omega(n2^n \log p)$ is exponential in system's size. □

The theorem 5.7 concludes that it is hard to put "HN for zero-dimensional system over $\overline{\mathbb{F}}_q$" in class NP, under the assumption that certificate is a zero of the system.

## 5.3 A Reduction of Zero Dimensional Affine Systems into Positive Dimensional Affine Systems

In this concluding section, we will point out that solving HN for positive dimensional affine systems is at least as hard as for zero dimensional affine systems. We will also put out some crucial points with the help of examples.

The following theorem gives us reduction of zero dimensional affine systems into positive dimensional affine systems.

**Theorem 5.8.** *Given an affine algebraic set $S$ over $\overline{\mathbb{F}}_q$ in form of system of polynomial equations $\{f_1(\overline{x}) = 0, \ldots, f_m(\overline{x}) = 0\}$ over $\mathbb{F}_q[x_1, \ldots, x_n]$ and a promise that either $S$ is empty or $S$ has dimension zero. For every such $S$ there exists an affine algebraic set $S'$ over $\overline{\mathbb{F}}_q$ with its defining equations over $\mathbb{F}_q[x_1, \ldots, x_{n+2}]$ such that,*

1. *If $S = \phi$ then $S' = \phi$ and,*
2. *If $S \neq \phi$ then dimension of $S'$ is 1 and for any zero $\overline{a} = (a_1, \ldots, a_n, a_{n+1}, a_{n+2})$ in $S' \subseteq (\overline{\mathbb{F}}_q)^{n+2}$ there exists a zero $(a_1, \ldots, a_n)$ in $S \subseteq (\overline{\mathbb{F}}_q)^n$.*

*Proof.* Simply consider a new system $F$ over $\mathbb{F}_q[x_1, \ldots, x_{n+2}]$ as

$$F := \{f_1(\overline{x}) = 0, \ldots, f_m(\overline{x}) = 0\} \cup \{f(x_{n+1}, x_{n+2}) = 0\}$$

where $f$ is a non constant bivariate polynomial. It is clear that $S' = \mathcal{Z}(F)$ has dimension 1 and its any zero provides a zero for $S$ as stated in the theorem. □

Now we will see an example which shows that there are no small certificate for a positive dimensional affine algebraic set.

**Example 5.1.** *Consider again the system $S$ in observation 5.6 over $\mathbb{F}_p[x_1, \ldots, x_n]$. Now consider the system $S'$ defined as*

$$S' := S \cup \{y_2 - y_1 = 0\}$$

*over $\mathbb{F}_p[x_1, \ldots, x_n, y_1, y_2]$. This system $S'$ is 1-dimensional and it has no small certificate.*

We would like to remind here that all the arguments presented in this section and in section 5.2 are for affine algebraic sets. The example 5.1 is not bad for the projective algebraic sets. In case of projective algebraic sets, we have small zero $(0, 0, \ldots, 0, 1, 1)$ of the analogous homogeneous system.

# Chapter 6

# Conclusion and Open Questions

In this thesis we addressed the question of complexity of checking consistency of system of polynomial equations defined over a field of positive characteristic. This is a particular case of the more general problem of checking consistency of polynomial equations defined over any characteristic field. This problem is very well known as "Hilbert's Nullstellensatz". The current best complexity for this problem is PSPACE over arbitrary characteristic fields. Over zero characteristic fields, P. Koiran [Koi96] solved this problem in class AM but under the assumption that generalized riemann hypothesis (GRH) is true. We gave a brief sketch of his proof in Chapter 4. It is important to note that GRH is being used in his proof only to give some count on the number of primes modulo which some univariate polynomial has solution. It is interesting to know whether we can remove this restriction,

**Open Question 1.** *Under the assumption of GRH, best complexity known for Hilbert's Nullstellensatz is* AM *over zero characteristic fields. Can this be said unconditionally?*

The problem over positive characteristic fields seems more hard and it is not known to be in some class better than PSPACE even conditionally. Even this result came after some excellent research on effective nullstellensatz. In Chapter 3 we gave proof for hilbert's nullstellensatz and a brief sketch of the proof of effective nullstellensatz by Dube and Sombra [Dub93, Som97]. Since PSPACE is very higher level class and over zero characteristic better results are known though conditionally, the following open question naturally arises,

**Open Question 2.** *Over positive characteristic fields, Can we put Hilbert's Nullstellensatz in polynomial hierarchy, or in particular in class AM or NP?*

We tried to put this problem over positive characteristic in class NP. We divided the problem in two cases: when the solution set is positive dimensional and when solution set

is zero dimensional. For positive dimensional case we solved 3 more special cases in class NP. We solved a problem which promises that either the system is inconsistent or,

- the affine or projective zero set of system is absolutely irreducible,
- the projective zero set is reducible but one of its absolutely irreducible component is definable in base field by some polynomials whose degree product is not bigger than the degree product of input polynomials,
- the affine zero set is reducible but one of its absolutely irreducible component is definable in base field.

We used some estimates on the number of points of a variety to achieve our result. Next for zero dimensional case we constructed some examples which are bad in the sense that they have no small solutions. Further we reduced the zero dimensional case to positive dimensional case for affine algebraic sets. This concludes that either checking consistency of general affine algebraic sets is not in NP or there is some other characterization of certificate to put the problem in class NP. Though we believe there must be some charcterization. Finally we ask the following question,

**Open Question 3.** *Is the complexity of Hilbert's Nullstellensatz in class* NP *over arbitrary characteristic fields?*

# Bibliography


[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Annals of Mathematics*, pages 781–793, 2004.

[AO83] Leonard M Adleman and Andrew M Odlyzko. Irreducibility testing and factorization of polynomials. *Mathematics of Computation*, 41(164):699–709, 1983.

[Bro87] W Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Annals of Mathematics*, 126(3):577–591, 1987.

[CG50] Cramer and Gabriel. *Introduction a l'analyse des lignes courbes algebriques par Gabriel Cramer...* chez les freres Cramer & Cl. Philibert, 1750.

[CLO07] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[CM06] Antonio Cafure and Guillermo Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields and Their Applications*, 12(2):155–185, 2006.

[Dub93] Thomas Dubé. A Combinatorial Proof of the Effective Nullstellensatz. *J. Symb. Comput.*, 15:277–296, 1993.

[Eis13] David Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[Ful13] William Fulton. *Intersection theory*, volume 2. Springer Science & Business Media, 2013.

[GL02] Sudhir R Ghorpade and Gilles Lachaud. Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Moscow Mathematical Journal*, 2(3):589–631, 2002.

[Har13a] Joe Harris. *Algebraic geometry: a first course*, volume 133. Springer Science & Business Media, 2013.

[Har13b] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[Hei83] Joos Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz is in the Polynomial Hierarchy. *J. Complexity*, 12(4):273–286, 1996.

[Kol88] János Kollár. Sharp Effective Nullstellensatz. *Journal of the American Mathematical Society*, 1(4):963–975, 1988.

[LR15] Gilles Lachaud and Robert Rolland. On the number of points of algebraic sets over finite fields. *Journal of Pure and Applied Algebra*, 219(11):5117–5136, 2015.

[LW54] Serge Lang and Andre Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4):819–827, 1954.

[SH94] Igor Rostislavovich Shafarevich and Kurt Augustus Hirsch. *Basic algebraic geometry*, volume 2. Springer, 1994.

[Som97] Martin Sombra. Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz. *Journal of Pure and Applied Algebra*, 117:565–599, 1997.

[Sud98] Madhu Sudan. Lecture notes on Algebra and Computation. 1998.

[VP84] Wolfgang Vogel and Dilip P Patil. *Lectures on results on Bezout's theorem*, volume 74. Springer Berlin Heidelberg New York, 1984.