The Complexity of Hilbert's Nullstellensatz

UG Project (UGP-I) (CS395A) report submitted to

Indian Institute of Technology Kanpur

Bachelor of Technology

in

Computer Science and Engineering

by

Shubhojyoti Nath

(150708)

Under the supervision of

Professor Nitin Saxena

Department of Computer Science and Engineering

Indian Institute of Technology Kanpur

Autumn Semester, 2019-20

November 25, 2019

DECLARATION

I certify that

(a) The work contained in this report has been done by me under the guidance of my supervisor.

(b) The work has not been submitted to any other Institute for any degree or diploma.

(c) I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.

(d) Whenever I have used materials (data, theoretical analysis, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.

Date: November 25, 2019 (Shubhojyoti Nath)
Place: Kanpur (150708)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

KANPUR - 208016, INDIA

CERTIFICATE

This is to certify that the project report entitled "**The Complexity of Hilbert's Nullstellensatz**" submitted by **Shubhojyoti Nath** (Roll No. 150708) to Indian Institute of Technology Kanpur towards no/partial fulfilment of requirements for the award of degree of Bachelor of Technology in Computer Science and Engineering is a record of bona fide work carried out by him under my supervision and guidance during Autumn Semester, 2019-20.

Date: November 25, 2019

Place: Kanpur

Professor Nitin Saxena
Department of Computer Science and
Engineering
Indian Institute of Technology Kanpur
Kanpur - 208016, India

Abstract

Name of the student: **Shubhojyoti Nath** Roll No: **150708**

Degree for which submitted: **Bachelor of Technology**

Department: **Department of Computer Science and Engineering**

Thesis title: **The Complexity of Hilbert's Nullstellensatz**

Thesis supervisor: **Professor Nitin Saxena**

Month and year of thesis submission: **November 25, 2019**

Hilbert's Nullstellensatz is an important theorem in Commutative Algebra and Algebraic Geometry. It connects the notion of ideals (in Commutative Algebra) to that of varieties (in Algebraic Geometry). In this project, we investigate the computational version of this problem (HN) which basically translates to finding how hard it is to decide whether or not 1 lies in the ideal generated by a set of polynomials, say $\{f_1, \cdots, f_k\}$ in $k[x_1, \cdots, x_n]$. In particular, we look at the two most important results pertaining to the complexity of the above problem (for field k of zero-characteristic): $HN \in PSPACE$, and under Generalized Riemann Hypothesis, $HN \in AM$.

Acknowledgements

I am deeply indebted to Prof. Nitin Saxena for giving me this opportunity to work under him; this project would have been nothing short of impossible had he not guided me for the past four months. I thank him for being patient with me and also for the weekly discussions we had, which were extremely edifying. I would also like to thank my colleagues and friends Abhibhav Garg and Diptajit Roy for spending a significant amount of time discussing ideas and pointing me to interesting bodies of work. I am also grateful to Prof. Santosha Pattanayak for giving me some of his valuable time to clarify my doubts. Last but not the least, I would like to thank my parents for the incredible and unconditional support they bestowed upon me during the span of this project.

Contents

Chapter 1

Introduction

In this project, we explore the complexity of determining whether a system of polynomial equations is satisfiable. More precisely, given a set of polynomials $f_1, f_2, \cdots, f_k \in k[x_1, x_2, \cdots, x_n]$ (k is a field), do they have a common zero, i.e. is the following system of equations satisfiable over k?

$$\begin{aligned} f_1(x_1, x_2, \cdots, x_n) &= 0 \\ f_2(x_1, x_2, \cdots, x_n) &= 0 \\ &\vdots \\ f_k(x_1, x_2, \cdots, x_n) &= 0 \end{aligned}$$

The above problem is closely related to the statement of Hilbert's Nullstellensatz, a theorem in Commutative Algebra and Algebraic Geometry. Hence, we define HN to be the decision language consisting of those systems of polynomial equations $\{f_1 = 0, f_2 = 0, \cdots, f_k = 0\}$ which are satisfiable.

In Chapter 2, we see the proof of Hilbert's Nullstellensatz. In Chapter 3, we prove that the above problem (HN) is in $PSPACE$ (due to Jelonek (2005)). In Chapter 4, we prove that HN belongs to the Arthur-Merlin class (AM) for field $k = \mathbb{Q}$ (due to Koiran (1996)), assuming the Generalized Riemann Hypothesis. Finally in Chapter 5, we mention some open problems related to the complexity of HN.

Chapter 2

Proof of Hilbert's Nullstellensatz

Hilbert's Nullstellensatz is a theorem about any ideal in the ring of polynomials $k[x_1, x_2, \cdots, x_n]$ where we assume that k is an algebraically closed field. It's weak form states that such an ideal must either contain 1, or all member polynomials must share a common zero in k^n.

Let's prove the Hilbert's Nullstellensatz for $k = \mathbb{C}$. The following proof is due to Arrondo (2006).

2.1 Points in $\mathbb{C}^n$ correspond to Maximal Ideals in $\mathbb{C}[x_1, x_2, \cdots, x_n]$

Lemma 1. *For $a = (a_1, \cdots, a_n) \in \mathbb{C}^n$ consider the ideal I_a in $\mathbb{C}[z_1, \cdots, z_n]$ generated by $z_1 - a_1, \cdots, z_n - a_n$. Then the ideal I_a is maximal.*

Proof. Consider the evaluation ring homomorphism $\phi_a : \mathbb{C}[z_1, \cdots, z_n] \to \mathbb{C}$ given by $\phi_a(f) = f(a)$. Clearly, ϕ_a is surjective (since $\phi_a(z_0) = z_0$, $\forall z_0 \in \mathbb{C}$). By first isomorphism theorem, $\mathbb{C}[z_1, \cdots, z_n]/kernel(\phi_a)$ is isomorphic to $\mathbb{C}$ which, in turn, is a field. So in order to prove the lemma, it is enough to show that $I_a = kernel(\phi_a) = \{f \in \mathbb{C}[z_1, \cdots, z_n] | \ f(a) = 0\}$, since it's known that quotienting by an ideal produces a field if and only if the ideal is maximal. It's conspicuously evident that $I_a \subseteq kernel(\phi_a)$. Let $w_i = z_i - a_i$, $\forall i = 1, 2, \cdots, n$ and for any $f \in$

$\mathbb{C}[z_1, \cdots, z_n]$, define $g_f \in \mathbb{C}[w_1, \cdots, w_n]$ where $g_f(w_1, \cdots, w_n) = f(w_1+a_1, \cdots, w_n+a_n)$. Clearly, $g_f(0) = 0$ iff $f(a) = 0$. But $g_f(0) = 0$ implies that $g_f(w_1, \cdots, w_n) = \sum_{i=1}^{n} \alpha_i w_i + \sum_{i \leq j=1}^{n} \beta_{ij} w_i w_j + \cdots$, i.e., a polynomial without a non-zero constant term. Therefore, $f(z_1, \cdots, z_n) = \sum_{i=1}^{n} \alpha_i (z_i - a_i) + \sum_{i \leq j=1}^{n} \beta_{ij} (z_i - a_i)(z_j - a_j) + \cdots \in I_a$, i.e. $kernel(\phi_a) \subseteq I_a$. Hence, proved. □

2.2 Maximal Ideals in $\mathbb{C}[x_1, x_2, \cdots, x_n]$ correspond to Points in $\mathbb{C}^n$

In order to make our lives easy, we first prove the following two lemmas, which would be used to finally prove Hilbert's Nullstellensatz.

Lemma 2. *(Noether Normalization) Suppose that $f \in \mathbb{C}[z_1, \cdots, z_n]$ is of total degree d. Then one can find scalars $\lambda_1, \cdots, \lambda_{n-1} \in \mathbb{C}$ such that the coefficient of z_n^d in $f(z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$ is non-zero. In particular, the mapping $\Lambda : f(z_1, \cdots, z_n) \to f(z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$ is a ring isomorphism from $\mathbb{C}[z_1, \cdots, z_n]$ onto itself.*

Proof. Let f_d be the homogenous part of f of degree d. Since $f_d \neq 0$, $\exists c = (c_1, c_2, \cdots, c_n) \in \mathbb{C}^n$ such that $f_d(c) \neq 0$. Due to continuity of f_d, we can assume that $c_n \neq 0$. Let $\lambda_i = c_i/c_n$, $\forall i = 1, 2, 3, \cdots, n-1$. The coefficient of z_n^d in $f(z_1 + \lambda_1 z_n, \cdots, z_{n-1} + \lambda_{n-1} z_n, z_n)$

$$= f_d(\lambda_1, \cdots, \lambda_{n-1}, 1) = f_d(c_1/c_n, \cdots, c_n/c_n) = f_d(c)/c_n^d \neq 0$$

The second part is easy to see, since the mapping Λ is clearly a bijection (define the inverse mapping to complete the proof). □

(*Note:* The above lemma is true for other fields as well (and not just $\mathbb{C}$), for proof please refer to Atiyah and MacDonald (1994).)

Lemma 3. *Given two polynomials $f, g \in \mathbb{C}[z_1, \cdots, z_{n-1}][z_n]$ of degree d, e with respect to z_n, respectively, such that*

$$f(z) = f_0(z') + f_1(z') z_n + \cdots + f_d(z') z_n^d$$

$$g(z) = g_0(z') + g_1(z')z_n + \cdots + g_e(z')z_n^e$$

where $z = (z_1, \cdots, z_n)$ *and* $z' = (z_1, \cdots, z_{n-1})$. *Define Resultant of* f, g, *i.e.,* $Res(f, g)$ *as the determinant of the following* $(d + e) \times (d + e)$ *matrix:*

$$\begin{bmatrix} f_0 & f_1 & \dots & f_d & 0 & \dots & 0 & 0 & 0 \\ 0 & f_0 & f_1 & \dots & f_d & 0 & \dots & 0 & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \dots & \dots & \vdots \\ 0 & 0 & \dots & 0 & f_0 & f_1 & \dots & \dots & f_d \\ g_0 & g_1 & \dots & g_{e-2} & g_{e-1} & g_e & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & \dots & \dots & g_e & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \dots & \dots & \vdots \\ 0 & 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_e \end{bmatrix}$$

Then, $f, g \in I$ *in* $\mathbb{C}[z_1, \cdots, z_{n-1}, z_n]$ *implies that* $Res(f, g) \in I$. *(The usefulness of* $Res(f, g)$ *is that it's devoid of the variable* z_n, *i.e.,* $Res(f, g) \in \mathbb{C}[z_1, \cdots, z_{n-1}]$*)*

Proof. The determinant of the matrix above would remain unchanged upon performing elementary column operations. Upon applying the following operations sequentially- $C_0 \leftarrow C_0 + z_n^i C_i$, $\forall i = 2, 3, \cdots, (d + e)$, all the elements of the first column become multiples of either $f(z_1, \dots, z_n)$ or $g(z_1, \dots, z_n)$. Upon opening the determinant along the first column, we obtain

$$Res(f, g) = fA + gB$$

for some $A, B \in \mathbb{C}[z_1, \cdots, z_{n-1}, z_n]$. Hence, proved. □

Theorem. *(Hilbert's Nullstellensatz Weak Form) Given any ideal* $I \subseteq \mathbb{C}[z_1, \cdots, z_{n-1}, z_n]$, *either* $1 \in I$ *or all elements of* I *share a common zero.*

Proof. It is enough to show that any maximal ideal in $\mathbb{C}[z_1, \cdots, z_{n-1}, z_n]$ is of the form $\langle z_1 - a_1, z_2 - a_2, \cdots, z_n - a_n \rangle$ for some $(a_1, a_2, \cdots, a_n) \in \mathbb{C}^n$, since any ideal I lies within a maximal ideal. We prove this by induction on the number of variables n to be used in the ring of polynomials $\mathbb{C}[z_1, \cdots, z_n]$. Also, we assume the Hilbert's Basis Theorem which states that any ideal in $\mathbb{C}[z_1, \cdots, z_n]$ is generated by finitely many polynomials. Let J be a maximal ideal in $\mathbb{C}[z_1, \cdots, z_n]$.

Base Case: $n = 1$. We know that every ideal in $\mathbb{C}[z_1]$ is a principle ideal (use GCD algorithm for univariate polynomials to find the generator). Let the generator of

J be $g(z_1)$, which is assumed to be monic without loss of generality, i.e., $J = \langle g \rangle$. Either $g(z_1) = 1$ or g has degree $d > 0$. Since the underlying field is C, g can be broken into d linear factors. Let one of those linear factors be $z_1 - a$ for some $a \in \mathbb{C}$. Then clearly $\langle g \rangle \subseteq \langle z_1 - a \rangle$ (since, any multiple of g is also a multiple of $z - a$). But due to the assumed maximality of J, $\langle z_1 - a \rangle = \langle g \rangle$.

Inductive Step: Assumed true for $n - 1$. By Lemma 2, J contains a polynomial f of total degree, say d, and the coefficient of z_n^d in f is 1, i.e.

$$f(z', z_n) = f_0(z') + \cdots + f_{d-1}(z') z_n^{d-1} + z_n^d$$

where $z' = (z_1, \cdots, z_{n-1})$ and $f_i \in \mathbb{C}[z_1, \cdots, z_{n-1}]$, $\forall i = 1, \cdots, n-1$. Let $J' \subseteq J$ be another ideal such that

$$J' = J \cap \mathbb{C}[z_1, \cdots, z_{n-1}]$$

We observe that $1 \in J$ iff $1 \in J'$. Thus J' is a proper ideal, and therefore $\exists a' = (a_1, \cdots, a_{n-1}) \in \mathbb{C}^{n-1}$ such that all polynomials in J' vanish on a'. Consider the following ideal $J'' \subseteq \mathbb{C}[z_n]$ defined as follows:

$$J'' = \{p(a_1, \cdots, a_{n-1}, z_n) |\ p \in J\}$$

Either $J'' = \langle 1 \rangle$ or by the base case $n = 1$, all elements of J'' vanish on a certain complex number $a_n \in \mathbb{C}$. It is enough to show that $J'' \neq \langle 1 \rangle$. By contrast, let's suppose that $1 \in J''$, i.e. $\exists p \in J$ such that $p(a_1, \cdots, a_{n-1}, z_n) = 1$, i.e.

$$p(z', z_n) = p_0(z') + \cdots + p_{e-1}(z') z_n^{e-1} + p_e(z') z_n^e$$

where $p_0(a') = 1$ and $p_i(a') = 0, \forall i = 1, 2, \cdots, e$. We have $Res(f, p) \in J'$ (since it's devoid of z_n by definition), from which it follows that $Res(f, p)$ vanishes at a', but this is a contradiction (evaluating the resultant determinant of Lemma 3. at a', we get $Res(f, p)(a') = 1$). Hence, proved. □

Theorem. *(Hilbert's Nullstellensatz) Given any ideal $I \subseteq \mathbb{C}[z_1, \cdots, z_{n-1}, z_n]$, define $Z(I)$ to be the zero set of I, i.e.,*

$$Z(I) = \{a \in \mathbb{C}^n |\ p(a) = 0\ \forall p \in I\}$$

Suppose $f \in \mathbb{C}[z_1, \cdots, z_{n-1}, z_n]$ *vanishes on* $Z(I)$*, then* $\exists r \in \mathbb{N}$ *such that* $f^r \in I$*.*

Proof. (Using Rabinowitsch trick) Let $f_1, \ldots, f_k$ be the generators of I (existence due to Hilbert's Basis Theorem). Then $1 - z_0 f$ and $f_1, \ldots, f_k$ have no zero in common, where z_0 is a newly added free variable. The weak form of Hilbert's Nullstellensatz (previous theorem) states that $\exists g_0, g_1, \ldots g_k \in \mathbb{C}[z_0, z_1, \cdots, z_{n-1}, z_n]$ such that

$$g_0(1 - z_0 f) + \sum_{i=1}^{k} g_i f_i = 1$$

Since z_0 is a free variable, putting $z_0 = 1/f$, we get

$$\sum_{i=1}^{k} g_i(1/f, z_1, \cdots, z_n) f_i(z_1, \cdots, z_n) = 1$$

which can be simplified further by multiplying by the lowest power of f, say r, to get rid of f's from the denominators of every term in the sum. We finally obtain,

$$\sum_{i=1}^{k} h_i(z_1, \cdots, z_n) f_i(z_1, \cdots, z_n) = f^r(z_1, \cdots, z_n)$$

Thus $f^r \in \langle f_1, \cdots, f_k \rangle = I$. Hence, proved. □

Chapter 3

Effective Nullstellensatz

This chapter is much more mathematically involved than the previous chapter, and also, most likely, as compared to any of the subsequent chapter.

3.1 Algebraic Geometry Preliminaries

In this section, we are going to introduce certain terminologies/definitions from the fields of Commutative Algebra and Algebraic Geometry.

Let k be any field; for convenience, we assume k is algebraically closed. We define the *affine space* $\mathbb{A}_k^n$ as follows

$$\mathbb{A}_k^n = \{(c_1, \cdots, c_n) |\ c_i \in k\ \forall i = 1, \cdots, n\}$$

Basically $\mathbb{A}_k^n$ is the same as k^n, but we use different notations for them since k^n usually refers to the n-dimensional k-vector space, and $\mathbb{A}_k^n$ is devoid of such vector space-like structure.

Let $S \subseteq k[x_1, \cdots, x_n]$ be a set of n-variate polynomials. Denote the ideal generated by the polynomials in S by I_S. Let $V(S) \in \mathbb{A}_k^n$ be the set of points such that all polynomials in S vanish on any point in $V(S)$, i.e.,

$$V(S) = \{c \in \mathbb{A}_k^n |\ p(c) = 0\ \forall p \in S\}$$

. It is easy to see that

$$V(S) = V(I_S)$$

Since algebraic geometry is the study of the common zeroes of a set of polynomials, then due to the above equality, it is only natural to assume that such sets of polynomials are ideals in $k[x_1, \cdots, x_n]$.

For any ideal $I \subseteq k[x_1, \cdots, x_n]$, we call $V(I)$ to be the *affine variety* corresponding to I. Similarly, we can define the polynomial *ideal for any subset* T of $\mathbb{A}^n_k$ as follows.

$$I(T) = \{p \in k[x_1, \cdots, x_n] | \ p(t) = 0 \ \forall t \in T\}$$

Let's now define the *radical* $\sqrt{I}$ of an ideal I in a commutative ring R (for our purposes, $R = k[x_1, \cdots, x_n]$). We say that

$$\sqrt{I} = \{x \in R | \ \exists r \in \mathbb{N} \ x^r \in I\}$$

Hilbert's Nullstellensatz (Strong Version) proved in the previous chapter can be translated in terms of the notation we just learnt: For any ideal $I_0 \subseteq k[x_1, \cdots, x_n]$, we have-

$$\sqrt{I_0} = I(V(I_0))$$

This is the relation that connects polynomial ideals to affine varieties. We call a variety *irreducible* if it can't be written as the union of 2 strictly smaller non-empty varieties. Every variety can be expressed as the union of a finite number of irreducible varieties (components) (proof follows from primary decomposition of ideals, refer Atiyah and MacDonald (1994)).

Now we consider the notion of dimension of a variety. For simplicity and ease in visualisation, we take $k = \mathbb{R}, n = 2$. Consider the polynomial $p(x, y) = x^2 + y^2 - 1$. We know that $V(\{p\})$ is the unit circle around $(0, 0)$ which is a curve of dimension 1. For our next example, take $k = \mathbb{R}, n = 3$ and let $p(x, y, z) = x+y+z$. Then we know that $V(\{p\})$ is a plane passing through the point $(0, 0, 0)$ and is of dimension 2. Next take $q(x, y, z) = x - y$. Then $V(\{p, q\})$ is the line given by the parameterization (using t) $(t, t, -2t)$ of dimension 1. Now consider the variety $V(\{xz, yz\})$; it is easy to see that it is the union of the $xy-$plane (which is 2-dimensional) and the $z-$axis (which is 1-dimensional). In this case, dimension of the variety is taken to

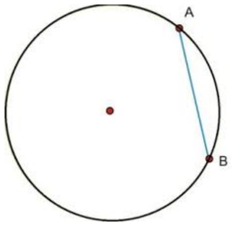

Figure 3.1: Circle

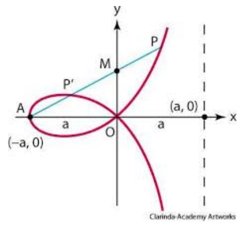

Figure 3.2: Strophoid

be $max(1,2) = 2$. In general, the dimension of a variety is defined as the maximum among the dimensions of its irreducible components. (For a more detailed theory on dimension of varieties, please refer Cox et al. (2015))

For a variety V of dimension d in the affine space $\mathbb{A}^n_k$, the *codimension* of V is defines as $n - d$. Now let's investigate how to define the *degree* of a variety. First we look at the degree of curves defined by a single polynomial. We say that the degree of a curve (zero-set) of a polynomial $f \in k[x_1, \cdots, x_n]$ is equal to the total-degree of the polynomial itself. For example, a *circle* given by $x^2 + y^2 = 1$ should have degree 2 by the above definition. See that any line in general position cuts the circle at maximum 2 points (Fig. 3.1). Next see a *strophoid* given by the equation $(a - x)y^2 = x^2(a + x)$ (Fig. 3.2). Any line in general position cuts it at 3 points (max.) and 3 is also the degree of the curve upon inspection of the defining equation. Also, similarly in $\mathbb{R}^3(\mathbb{C}^3)$, the hyperplane defined by $x + y + z = 1$ has degree 1 and the unit sphere $x^2 + y^2 + z^2 = 1$ has degree 2. And it is evident that a line (in $\mathbb{R}^3$) in general position cuts the above curves in 1 and 2 points (max.), respectively.

This leads to the following definition: the *degree* of a curve in $\mathbb{A}^n_k$ is equal to the maximum number of points of intersection with any line (1-dimensional linear space in $\mathbb{A}^n_k$) in general position. And the above definition can be generalized as follows: the degree of a variety V in $\mathbb{A}^n_k$ of codimension r is equal to the number of points of intersection of V with a sufficiently general linear subspace of dimension r (Hartshorne (1977)).

It is easy to see that (in $k[x, y, z]$, since $k[x, y, z]$ is an integral domain)

$$V(\{x + y + z\}) = V(\{(x + y + z)^2\}) = V(\{(x + y + z)^3\})$$

and

$$V(\{(x^2+y^2+z^2)(x^2-y^3-3)\}) = V(\{(x^2+y^2+z^2)^2(x^2-y^3-3)^3\})$$

What is worth noting in the above two examples is the fact that if $k[x_1, \cdots, x_n] \ni g = f_1^{r_1} f_2^{r_2} \cdots f_l^{r_l}$ where f_i is irreducible and $r_i \in \mathbb{N}\, \forall i = 1, \cdots l$, then $V(\{g\}) = V(\{\prod_{i=1}^{l} f_i\})$. We say that $\prod_{i=1}^{l} f_i$ is a *reduced polynomial.* In fact, it is also easy to see that

$$V(\{g\}) = V(\{f_1 f_2 \cdots f_l\}) = V(\{f_1\}) \cup V(\{f_2\}) \cdots \cup V(\{f_l\})$$

and $V(\{f_i\})$'s are called the *components* of $V(\{g\})$.

As a corollary of *Bezout's theorem*, given two curves C, D of degrees m, n (these are the *degrees* of the corresponding *reduced* polynomials), respectively, which do not share any *component*, the number of points of in their intersection is less than or equal to mn (In fact, equality holds if the curves are seen in *projective space* and *intersection multiplicities* are accounted for; refer Cox et al. (2015)).

A subset S of $\mathbb{A}_k^n$ is said to be *closed* (as per *Zariski topology*) iff $S = V(I)$ for some ideal $I \in k[x_1, \cdots, x_n]$. The *closure* of $T \in \mathbb{A}_k^n$ (abbreviation $cl(T)$) is defined as the smallest closed set containing T. Let X be a variety in $\mathbb{A}_k^n$, and let $T \subseteq X$, then T is said to be *dense* in X, iff $cl(T) = X$.

Let f be a polynomial in $k[x_1, \cdots, x_n]$ and let P be a point in $X = V(\{f\})$. Point P is said to be singular in X if all the partial derivatives of f, i.e., $f_{x_1}, \cdots, f_{x_n}$ vanish at P. Any point $Q \in X$ which is not singular in X is said to be *non-singular* or *smooth* in X. For example, in the strophoid $s(x, y) = (a - x)y^2 - x^2(a + x) = 0$, $(0, 0)$ is a singular point since $s_x(x, y) = -y^2 - 2ax - 3x^2$ and $s_y(x, y) = 2(a - x)y$ both vanish at $(0, 0)$, in fact, it can be easily checked that $(0, 0)$ is the only singular point in the strophoid, i.e., all other points therein are smooth. Moreover, it can be proved (Shafarevich (1988)) that for any variety, the set of its smooth points is dense in the variety, i.e., ∇f for a reduced polynomial f does not vanish on any of the irreducible components of the variety. This leads to the following characterization of reduced polynomials.

Lemma. A polynomial $f \in k[x_1, \cdots, x_n]$ is reduced if and only if $\nabla f = (f_{x_1}, \cdots, f_{x_n})$ does not vanish on any of the irreducible components of the set $V(\{f\})$.

Proof. (Forward direction proved above) If f is not reduced, then $f = g^2h$ and therefore, $\nabla f = g^2\nabla h + 2gh\nabla g = g(g\nabla h + 2h\nabla g)$ which vanishes on the component given by $g = 0$. □

Let B be a ring and A be its subring such that A contains 1_B. We say that $b \in B$ is *integral* over A if b satisfies the following

$$b^q + a_{q-1}b^{q-1} + \cdots + a_1 b + a_0 = 0$$

for some choice of $a_i \in A$, $\forall i = 1, \cdots, q-1$ and $q \in \mathbb{N}$. Notice that the above polynomial is *monic* in b. We say that B is *integral* over A if every element in B is integral over A.

Let V be a variety in $\mathbb{A}_k^n$. A function $f : V \to k$ is called *regular* if there exists a polynomial $F \in k[x_1, \cdots, x_n]$ such that $f(x) = F(x)\ \forall x \in V$. Then define $k[V] = k[x_1, \cdots, x_n]/I(V)$ to be the *coordinate ring* of V, which is simply the set of all regular functions defined on V.

Now let $X \subseteq \mathbb{A}_k^n$ and $Y \subseteq \mathbb{A}_k^m$ be two varieties. Then a map $f : X \to Y$ is said to be a *regular map* if there exists functions $f_i \in k[X]$ such that $f(x) = (f_1(x) \cdots, f_m(x)), \forall x \in X$ and $i = 1, \cdots, m$. If $f(X)$ is dense in Y then f defines a map f^* from $k[Y] \to k[X]$ as follows:

$$f^*(p) = p \circ f$$

The above map is an embedding of $k[Y]$ in $k[X]$. So one can think of $k[Y]$ as a subring of $k[X]$. Now if $k[X]$ is integral over $k[Y]$, then f is said to be a *finite* map (Shafarevich (1988)).

3.2 Proof Idea for Effective Nullstellensatz

The subsequent proof of Effective Nullstellensatz is due to Jelonek (2005). A first-time reader is strongly advised to go through Section 3.1 before moving forward. We have mentioned the theorems and proofs/ideas in connection with the material presented in Jelonek (2005), with the intention to simplify the complex nature of the paper and make it palatable to new readers, and have neither necessarily replicated the proof as it is, nor given all the rigorous details everywhere. In short, the primary purpose of this section is to build an intuition for the proof of Effective Nullstellensatz.

Theorem 1. *Let $f_1, f_2, \ldots, f_{n+1} \in k[x_1, x_2, \cdots, x_n]$ be $n-$variate polynomials, where k is a field. Then $\exists W \in k[X_1, X_2, \cdots, X_n, X_{n+1}]$ such that $W(f_1, f_2, \ldots, f_{n+1}) = 0$, i.e., $f_1, f_2, \ldots, f_{n+1}$ are algebraically dependent.*

Proof. Let the total degree of f_i be $d_i > 0$, $\forall i = 1, 2, \cdots, n+1$. Let N be a large enough natural number (how large it should be would get clearer consequently). Consider the vector space V of all polynomials in $k[x_1, x_2, \cdots, x_n]$ of total degree $\leq N$, a basis for which could be as follows:

$$B = \{\prod_{i=1}^{n} x_i^{e_i} | \sum_{i=1}^{n} e_i \leq N\}$$

Here, $|B| = {}^{N+n}C_n$ which is a degree n polynomial in N, i.e., $|B| = \Theta(N^n)$. Now consider the following set of polynomials:

$$S = \{\prod_{i=1}^{n+1} f_i^{r_i} | \, r_i \leq \frac{N}{(n+1)d_i}, \ i \in \{0, 1, 2, \cdots, n+1\}\} - 1$$

Here, each $g \in S$ has total degree $\leq N$, i.e., $S \subseteq V$ and there are more than $\frac{N^{n+1}}{(n+1)^{n+1} \prod_{i=1}^{n+1} d_i}$ elements in S, in fact more accurately, $|S| = \Theta(N^{n+1})$. Choose N such that dimension of V (i.e., size of B) becomes smaller than size of S. Then, there are elements in S which have a linear dependency, which leads to an algebraic dependency among f_i's. □

Theorem 2. *Suppose V is an affine variety of degree d in $\mathbb{A}_k^m$. Let $f = (f_1, f_2, \cdots, f_n)$ be a polynomial map, (hence a "morphism of finite type"), from V to a variety $W = cl(f(V)) \subseteq \mathbb{A}_k^n$ such that dim V = dim $W = r$. If the degrees of f_i's are bounded by e, then $deg(W) \leq de^r$.*

Proof. Let $L \subseteq \mathbb{A}_k^n$ be a generic linear subspace of codimension r of W. Then by definition, the cardinality of the (finite) intersection $L \cap W$ is equal to $deg(W)$, and this is bounded above by the (finite) cardinality of $f^{-1}(L \cap W) = f^{-1}(L) \cap f^{-1}(W) = f^{-1}(L) \cap V$, since f is finite and has generically non-empty finite fibres. But $f^{-1}(L) \cap$

V is the intersection of V with the zero loci of r generic linear combinations of the f_i's. Now let's state the following generalisation of the Bezout's theorem: given a closed subset X with degree $deg(X)$ and suppose H is a hypersurface of degree e, then $deg(X \cap H) = e \times deg(X)$. This implies that the degree of $f^{-1}(L) \cap V$, that is, its cardinality, is at most $deg(V) \times deg(f^{-1}(L)) = de^r$, which gives us the desired result. □

Theorem 3. *(Generalized Perron's Theorem) Let k be a field and let $F_1, ..., F_{n+1} \in k[x_1, \cdots, x_m]$ be non-constant polynomials with $deg(F_i) = d_i$. Assume that $X \subseteq \mathbb{A}_k^m$ is an affine variety of dimension n and of degree D. If the mapping $\phi = (F_1, ..., F_{n+1}) : X \to \mathbb{A}_k^{n+1}$ is generically (locally) finite, then there exists a non-zero polynomial $W(T_1, ..., T_{n+1}) \in k[T_1, ..., T_{n+1}]$ such that*

1. *$W(F_1, ..., F_{n+1}) = 0$ on X*
2. *$deg(W(T_1^{d_1}, \cdots, T_{n+1}^{d_{n+1}})) \leq D \prod_{j=1}^{n+1} d_j$*

Proof. Let $W(T_1, ..., T_{n+1}) \in k[T_1, ..., T_{n+1}]$ be an irreducible polynomial such that $W(F_1, ..., F_{n+1}) = 0$ on X, whose existence is due to Theorem 1 and the fact that $k[T_1, ..., T_{n+1}]$ is an integral domain. Let $P(T_1, \cdots, T_{n+1}) = W(T_1^{d_1}, \cdots, T_{n+1}^{d_{n+1}})$. Since W is irreducible, it must be reduced, therefore $\nabla P = \nabla W \cdot (d_1 T^{d_1 - 1} + 1, \cdots, d_{n+1} T^{d_{n+1}-1} + 1) \neq 0$ (where $\cdot$ is the coordinate/component-wise product). Hence by lemma proved in the previous section, P is also reduced. Define $Y = \{y \in k^{n+1} | \ P(y) = 0\}$ where evidently, $deg(Y) = deg(P)$ and dimension of Y is n ($\because$ Y is a hyperplane in k^{n+1}). Form a new set $\widetilde{X} = \{(x, w) \in X \times k^{n+1} | \ F_i(x) = w_i$ if $d_i = 1$; $F_i(x) = w_i^{d_i} + w_i$, otherwise$\}$. Clearly, $dim\ X = dim\ \widetilde{X}$ since each of the $n + 1$ polynomials involving w_i's (used in the definition of $\widetilde{X}$) reduces the dimension of $X \times k^{n+1}$ by 1. And by Bezout's theorem, $deg(\widetilde{X}) \leq D \prod_{j=1}^{n+1} d_j$. Thus, $dim\ \widetilde{X} = n = dim\ Y$ and we consider the following map

$$\pi : \widetilde{X} \ni (x, w) \ \to \ w \ \in \ Y$$

which is clearly a finite map. We therefore apply Theorem 2. on the map π and obtain the following relation

$$deg(Y) \leq deg(\widetilde{X})$$

that is,

$$deg(W(T_1^{d_1},\cdots,T_{n+1}^{d_{n+1}})) = deg(P(T_1,...,T_{n+1})) = deg(Y) \leq deg(\widetilde{X}) \leq D\prod_{j=1}^{n+1} d_j$$

Hence, proved. □

Lemma. *(Noether Normalization) Assume k is an infinite field. Then if $X \subseteq \mathbb{A}_k^m$ be an affine variety of dimension n. Then for sufficiently general $a_{ij} \in k$, the mapping*

$$\alpha:\ X \ni (x_1,\cdots,x_m)\ \rightarrow \left(\sum_{j=1}^{m} a_{1j}x_j, \sum_{j=2}^{m} a_{2j}x_j, \cdots, \sum_{j=n}^{m} a_{nj}x_j\right)\ \in \mathbb{A}_k^n$$

is a finite projection of X on $\mathbb{A}_k^n$.

Proof. Refer Atiyah and MacDonald (1994), and Shafarevich (1988).

Theorem 4. *(Effective Nullstellensatz) Let K be an algebraically closed field and let $f_1,\cdots,f_k \in k[x_1,\cdots,x_m]$ be non-zero polynomials. Let $X \subseteq \mathbb{A}_K^m$ be an affine algebraic variety of dimension n and of degree D. Let $deg(f_i) = d_i$, where $d_1 \geq \cdots \geq d_k$. If $V(\{f_1,\cdots,f_k\}) \cap X = \phi$ then there exist polynomials g_i, such that*

1. $deg(f_i g_i) \leq D\prod_{j=1}^{k} d_j$
2. $1 = \sum_{i=1}^{k} f_i g_i$ *on* X

Proof. Assume $k \leq n$. Consider the mapping

$$\phi : X \times K \ni (x,z)\ \rightarrow\ (x, f_1(x)z,\cdots,f_k(x)z)\ \in K^m \times K^k$$

Since, by Hilbert's Nullstellensatz, $\exists g_i$'s such that $\sum_{i=1}^{k} f_i g_i = 1$, given $(x,w_1,\cdots,w_k) \in X \times K^k$, we can obtain $\phi^{-1}(x,w_1,\cdots,w_k) = (x,\sum_{i=1}^{k} w_i g_i(x))$, that is, ϕ is an embedding (or that $\phi : X \times K \rightarrow \phi(X \times K)$ is a bijection). In particular, the set

$$\phi(X\times K) = \left\{(x,w_1,\cdots,w_k) \in X \times K^k \,\middle|\, x \in X \text{ and } \forall i,\ w_i - f_i(x)\cdot\left(\sum_{j=1}^{k} w_j g_j(x)\right) = 0\right\}$$

is closed of dimension $n+1$, and $\phi : X \times K \rightarrow \phi(X \times K)$ is finite.

Let $\pi : \phi(X \times K) \to K^{n+1}$ be a generic projection and is therefore finite; consider it to be of the form described in the previous lemma. Define $\psi := \pi \circ \phi$ which is finite again. This is because the composition of finite maps is finite (can be easily proved using the fact that if ring A is integral over ring B and B is integral over another ring C, then A is integral over C, refer Atiyah and MacDonald (1994)). In fact, ψ is a generic projection of $X \times K$ on K^{n+1} and is of the form

$$\begin{aligned}\psi : \ X \times K \ni (x, z) \ &\to (\sum_{j=1}^{n} \gamma_{1j} f_j(x) z + l_1(x), \sum_{j=2}^{n} \gamma_{2j} f_j(x) z + l_2(x), \\ &\cdots, \sum_{j=n}^{n} \gamma_{nj} f_j(x) z + l_n(x), l_{n+1}(x)) \ \in \ K^{n+1}\end{aligned}$$

where l_j's are linear polynomials and $f_j := 0$ for $j > k$. Set $\psi = (\psi_1, \cdots, \psi_{n+1})$.

Now we apply the *Generalized Perron's Theorem* on $\psi_1, \cdots, \psi_{n+1} \subseteq K(z)[x_1, \cdots, x_m]$ over field $K(z)$ and the variety X is also considered over $K(z)$. Then there exists a polynomial $W \in K(z)[T_1, \cdots, T_m]$ such that

1. $W(\psi_1, ..., \psi_{n+1}) = 0$ on X
2. $deg(W(T_1^{d_1}, \cdots, T_k^{d_k}, T_{k+1}, \cdots, T_{n+1})) \leq D \prod_{j=1}^{k} d_j$

Here, the coefficients of W are in $K(z)$. Multiplying with the least common multiple of all denominators we get $\widetilde{W} \in K[T_1, \cdots, T_m, Y]$ such that

1. $\widetilde{W}(\psi_1(x, z), ..., \psi_{n+1}(x, z), z) = 0$.
2. $deg_T(\widetilde{W}(T_1^{d_1}, \cdots, T_k^{d_k}, T_{k+1}, \cdots, T_{n+1}, Y)) \leq D \prod_{j=1}^{k} d_j$ where deg_T denotes the degree with respect to the variables $T = (T_1, \cdots, T_{n+1})$.

Since $\psi = (\psi_1, \cdots, \psi_{n+1}) : X \times K \to K^{n+1}$ is a finite mapping, $K[X][z]$ is integral over $K[T_1, \cdots, T_{n+1}]$ (by definition of finite mapping, refer Section 3.1), i.e. for any polynomial $H \in K[X][z]$, there exists a minimal polynomial $P_H \in K[T_1, \cdots, T_{n+1}][Y]$ monic in Y such that

$$P_H(\psi_1, \cdots, \psi_{n+1}, H) = H^r + \sum_{j=1}^{r-1} b_j(\psi_1, \cdots, \psi_{n+1}) H^j = 0$$

.

Take $H = z$. By the minimality of P_z, we get $P_z(T, Y)$ divides $\widetilde{W}(T, Y)$ and therefore

$$deg_T(P_z(T_1^{d_1}, \cdots, T_k^{d_k}, T_{k+1}, \cdots, T_{n+1}, Y)) \leq D \prod_{j=1}^{k} d_j$$

.

Let the degree of P_z with respect to Y be N. Then

$$P_z(\psi_1, \cdots, \psi_{n+1}, z) = z^N + \sum_{j=1}^{N-1} b_j(\psi_1, \cdots, \psi_{n+1}) z^j = 0$$

that is

$$z^N + \sum_{j=1}^{N-1} b_j \left(\sum_{j=1}^{n} \gamma_{1j} f_j(x) z + l_1(x), \ \cdots \ , \sum_{j=n}^{n} \gamma_{nj} f_j(x) z + l_n(x), l_{n+1}(x) \right) z^j = 0$$

The terms involving z^N in the expansion of

$$\sum_{j=1}^{N-1} b_j \left(\sum_{j=1}^{n} \gamma_{1j} f_j(x) z + l_1(x), \ \cdots \ , \sum_{j=n}^{n} \gamma_{nj} f_j(x) z + l_n(x), l_{n+1}(x) \right) z^j$$

must be of the form $z^N U(x) \prod_{j=1}^{k} f_j^{u_j}(x)$ for some polynomial $U \in K[x_1, \cdots, x_m]$ and the powers u_j's are such that $\sum_{j=1}^{k} u_j > 0$. This leads to obtaining polynomials $g_i \in K[x_1, \cdots, x_m]$, $i = 1, \cdots, k$ such that conditions 1. and 2. in the theorem statement hold (the degree bound is sharp in this case, i.e., when $k < n$).

Now consider the case $k > n$; it's known that if now $1 \in \langle f_1, \cdots, f_k \rangle$, then 1 also belongs to the ideal generated by $n + 1$ random linear combinations of these polynomials. Call them $\widetilde{f_1}, \cdots, \widetilde{f_{n+1}}$. Hence, the above proof would work for this case as well, but with a little adjustment - one can increase the dimension of the variety X by 1, by adding another independent coordinate x_{m+1}, so we now have $n + 1$ polynomials and an $n + 1$ dimensional variety. Thus, the case $k > n$ has been reduced to $k = n$ (although the degree bound won't be sharp in this case). □

3.3 $HN \in PSPACE$

$PSPACE$ is defined as the set of all decision problems that can be solved by Turing Machine in polynomial (with respect to input size) space. More precisely,

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

where $SPACE(s(n))$ is the set of all decision problems that can be solved by a Turing Machine in $O(s(n))$ space for some function s of the input size n.

Since we have the degree bound on g_i's, which is exponential in the size of the input, one can form a linear system of equations with the unknowns being the coefficients of g_i's, and solve it in $PSPACE$ (the crux is not to store the linear system, instead one should compute the matrix entries on demand, Berkowitz (1984)).

Chapter 4

HN is in AM under Generalized Riemann Hypothesis

We will divide this chapter into two sections: the first would be concerned with developing a general understanding of the complexity class *AM* (*Arthur-Merlin*) and the second would contain the proof idea for the proposition $HN \in AM$ under Generalized Riemann Hypothesis (GRH). This proof is due to Koiran (1996).

4.1 Arthur-Merlin Class

The class *Arthur-Merlin* (AM) (Arora and Barak (2009)) is the set of those languages L for which membership can be ascertained with the help of an *Arthur-Merlin game* having *constant* number of rounds. An *Arthur-Merlin game* is simply an interactive protocol involving public coins where *Merlin* is an all-powerful *prover* and is trying to prove to *Arthur*, a probabilistic polynomial-time *verifier* that a certain element x is in the language L. In the beginning, *Arthur* produces *random bits* (say, by flipping truly random coins) and gives them to *Merlin*, hence the name public coins (since they are visible to *Merlin*). These random coins are like challenges to *Merlin* who has to provide a response to *Arthur*, and the response is usually trying to convince *Arthur* about the membership of x in L. Lastly, *Arthur*, using the random bits he generated and Merlin's responses, *verifies* the claims made by *Merlin* by doing certain polynomial time computations (very much like NP). *Merlin* can make *Arthur* accept with probability at least 2/3 for a *yes*-instance x and with probability at most 1/3 for a *no*-instance x, no matter what *Merlin* does (that is, even if he tries to cheat).

AM is most useful in identifying a language L where proving membership of x in L leads to the following scenario. Assume that there is a universe U and every candidate x for membership in L defines a *"good"* set $Good(x) \subseteq U$ such that membership of some $y \in U$ in $Good(x)$ is a problem in NP, i.e., given an appropriate (polynomial-sized) certificate, membership in $Good(x)$ can be verified in polynomial-time and also the set $Good(x)$ is such that if x is a *yes*-instance ($x \in L$), then $|Good(x)| \geq P_1$ and if x is a *no*-instance ($x \notin L$), then $|Good(x)| \leq P_2$, where $P_1 > 4P_2$. For the explicit AM protocol and the proof of $L \in AM$, refer *Sudan* (1998).

Let's build on the terminology introduced in the previous paragraph. In the subsequent section, we take $L = HN$ and $x = S = \{f_1, \cdots, f_m\}$, $f_i \in \mathbb{Z}[x_1. \cdots, x_n]$ of degree at most d. We have $S \in HN$ iff $\exists c \in \mathbb{C}^n$ such that $f(c) = 0$, $\forall f \in S$. For any $b \in \mathbb{N}$, define $[b]$ to be the set $\{1, \cdots, b\}$. Let $U = [N]$ for some $N \in \mathbb{N}$. We define

$$Good(S) := \{p \in [N] |\ p \text{ is a prime and } S \text{ has a solution in } \mathbb{Z}_p\}$$

Clearly, membership in $Good(S) \subseteq [N]$ is in NP, because one can provide a certificate $c_p \in \mathbb{Z}_p^n$ such that $f(c_p) = 0$ in $\mathbb{Z}_p$ for all $f \in S$. Also, the size of S, i.e., $|S| = poly(n, m, d, \log C)$ where C is the bound on the coefficients of $f \in S$.

4.2 Proof of $HN \in AM$ under GRH

At this point, it only remains to show why we defined $Good(S)$ the way we defined it and the bounds P_1 and P_2 on its size when S is a *yes*-instance or *no*-instance, respectively. When S is a *yes*-instance, it means that the system of equations $f = 0$ for $f \in S$ is satisfiable (we say S is *satisfiable*) and has a solution in $\mathbb{C}^n$. On the other hand, when S is a *no*-instance, the system of equations $f = 0$ for $f \in S$ is unsatisfiable (we say S is *unsatisfiable*) and has no solution in $\mathbb{C}^n$. The following two theorems precisely state that the fact that when S is satisfiable, the number of primes p for which the system of equations $f = 0 \pmod{p}$ for $f \in S$ has a solution, is far greater than the the case when S is not sastisfiable. In fact, the number of such primes is infinite in the former case and finite in the latter.

Theorem 1. *In case S is unsatisfiable over $\mathbb{C}$, there are at most $P_2 = exp(|S|)$ primes p such that S is satisfiable over $\mathbb{Z}_p$.*

Theorem 2. *In case S is satisfiable over $\mathbb{C}$, there exists two constants N_2, N_3 such that are at least $P_1 = \dfrac{\pi(N)}{N_2} - N_3 - O(\sqrt{N}\log N)$ primes $p \leq N$ such that S is satisfiable over $\mathbb{Z}_p$. Moreover, N_2, N_3 are $exp(|S|)$. (Here, $O(\sqrt{N}\log N)$ is the error term, and π is the prime-counting function, i.e., $\pi(N) :=$ number of primes $\leq N$ and it's known that $\pi(N) \approx N/\log N$.)*

We take N to be sufficiently large so that $P_1 > 4P_2$ (as discussed in the previous section). In the following subsections we present the proof idea for the above theorems.

4.2.1 Unsatisfiable System of Equations

If S is unsatisfiable, then due to Chapter 2, there exist polynomials $g_1, \cdots, g_m$ such that

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

The degrees of g_i's are bounded by $exp(|S|)$ due to Effective Nullstellensatz, and the above equation, therefore, reduces to a linear system with $exp(|S|)$ unknowns, i.e., the coefficients of g_i's. Since the coefficients of f_i's belong to $\mathbb{Q}$, so do those of g_i's, a proof of which is apparent using Cramer's rule. In fact, more can be said using Cramer's rule. The denominators of g_i's coefficients are determinants of $exp(|S|)$-sized matrices, and the denominators, in worst case, are exponential in the size of them matrix. Therefore, the denominators of g_i's are bounded by $exp(exp(|S|))$. If we take the LCM of the denominators of the coefficients of g_i, call it α (which is also bounded by $exp(exp(|S|))$), then the above equation becomes

$$f_1 G_1 + \cdots + f_m G_m = \alpha$$

where G_i's are polynomials with integer coefficients.

Let p be a prime such that S is satisfiable over $\mathbb{Z}_p$, i.e., there exists a solution (mod p) for S in $\mathbb{Z}^n$. Putting that solution in the above equation we get

$$\alpha = 0 \pmod{p}$$

that is, p divides α and the number of such p's is bounded by $\log_2 \alpha$. In order to prove Theorem 1., it remains to show that $\alpha = O(\exp(\exp(|S|))) = P_2$ which has been already proved in the preceding paragraph.

4.2.2 Satisfiable System of Equations

The case where S is satisfiable, is harder of the two cases. In order to develop more intuition about what is happening in this situation, we start with a few motivating examples.

Example 1. Consider the following system of equations in $\mathbb{Z}[x, y]$

$$\begin{aligned} xy - 30 &= 0 \\ x - 5 &= 0 \\ y - 6 &= 0 \end{aligned}$$

This has a solution $x = 5, y = 6$. In fact, for every prime p, there is a solution modulo p to the above system of equations, namely $x = 5 \pmod{p}, y = 6 \pmod{p}$

Example 2. Consider the following system of equations in $\mathbb{Z}[x, y, z]$

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

This has a solution $(x, y, z) = (1/2, 1/18, \pm 1/6) = (9/18, 1/18, \pm 3/18)$. Observe that unlike the previous example this equation has no solution modulo $p = 2$. Since $0 \neq 1 = -1 = 2x - 1 \pmod{2}$ for any $x \in \mathbb{Z}_2$. But there exists a solution modulo 5, namely $(x, y, z) = (3 \pmod{5},\ 2 \pmod{5},\ \pm 1 \pmod{5})$. In fact, it is easy to check that for every prime $p \neq 2, 3$, there is a solution modulo p to the above system of equations, namely $(x, y, z) = (18^{-1} \pmod p) \cdot (9,\ 1,\ \pm 3)$. Observe that 2,3 are the only primes that divide 18, the least common denominator of the components of the common solution over $\mathbb{Q}$.

Example 3. Consider the following system of equations in $\mathbb{Z}[x, y, z]$

$$\begin{aligned} x^3 - 2 &= 0 \\ y - 1 &= 0 \\ z - 3xy &= 0 \end{aligned}$$

This has a solution $(x, y, z) = (\sqrt[3]{2}, 1, 3\sqrt[3]{2})$. Observe that the methodology used to find solutions modulo p in the previous example fails to apply in this one.

So now that we have enough motivation about the kinds of scenario we might end up in if S is satisfiable, let's take a more general approach. Let $a = (a_1, \cdots, a_n) \in \overline{\mathbb{Q}}^n$ such that a is a zero of all the polynomials in S. If all a_i's are in $\mathbb{Z}$ or $\mathbb{Q}$, then we take approaches similar to those in Examples 1 and 2. Otherwise, we do the following. Obviously, a_i belongs to the field extension $\mathbb{Q}(a_i)$ for each i. Therefore each a_i belongs to the field extension $\mathbb{Q}(a_i, \cdots, a_n)$, which is equal to $\mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$ due to the Primitive Element Theorem (for an elementary proof, refer Brown (2010)). Let $R(x) \in Z[x]$ be the minimal annihilator of α. Since $a_i, \cdots, a_n \in \mathbb{Q}(\alpha)$, a_i can be written as a polynomial in α over $\mathbb{Q}$, i.e., $a_i = p_i(\alpha)/q$ for all i (q is the least natural number such that $p_i(x) \in \mathbb{Z}[x]$ for all i). The following lemma helps us in getting upper bounds on q and the degree and coefficients of R.

Lemma. *If $a = (a_1, \cdots, a_n)$ (the common zero of polynomials in S) is chosen appropriately, then the degree of R is $exp(|S|)$ and q and the coefficients of R are $exp(exp(|S|)$.*

Proof. Sudan (1998) □

Let for each $i = 1, \cdots, m$

$$g_i(x) = q^d \times f_i\left(\frac{p_1(x)}{q}, \cdots, \frac{p_n(x)}{q}\right)$$

Notice that each of the g_i's is a univariate (in x).

We have $g_i(\alpha) = q^d \times f_i\left(\frac{p_1(\alpha)}{q}, \cdots, \frac{p_n(\alpha)}{q}\right) = q^d \times f_i(a_1 \cdots, a_n) = 0$. Hence, R divides g_i for each i, since $R(x)$ is the minimal polynomial in $\mathbb{Q}[x]$ one of whose zeroes is α.

If p is a prime $\leq N$ not dividing q such that $R(x)$ has a zero modulo p, say $\alpha_p \in \mathbb{Z}_p$, then α_p is also a zero of every g_i, and by the technique used in Example 2., we obtain a common zero $\left(\frac{p_1(\alpha_p)}{q}, \cdots, \frac{p_n(\alpha_p)}{q}\right)$. The number of such primes p is what we desire to count (this is exactly equal to the size of $\mathit{Good}(S)$).

Suppose R has degree D and $\Delta = \mathit{Res}(f, f')$ where Res was defined in Chapter 2. Define $\mathcal{N}_p$ as follows

$$\mathcal{N}_p := |\{b \in \mathbb{Z}_p | \ R(b) = 0 \pmod p\}|$$

Theorem 3. *(Effective Chebotarev Density Theorem, Adleman and Odlyzko (1983)) Under Generalized Riemann Hypothesis,*

$$\left(\sum_{p \,\in\, \mathbb{P} \,\cap\, [N]} \mathcal{N}_p\right) = \left(\sum_{\substack{p \,\in\, \mathbb{P} \,\cap\, [N] \\ p \,\nmid\, \Delta}} 1\right) - O(\sqrt{N}\log(\Delta N))$$

where $\mathbb{P}$ is the set of primes.

We want $|\mathit{Good}(S)| = \sum_{\substack{p \,\in\, \mathbb{P} \,\cap\, [N] \\ p \,\nmid\, q \\ R \text{ has zero over } \mathbb{Z}_p}} 1$ which is greater than $\frac{\sum_{p \,\in\, \mathbb{P} \,\cap\, [N]} \mathcal{N}_p}{D} - \log q$ (since there are at most D zeros of R in $\mathbb{Z}_p$) which in turn equals

$$P_1 = \frac{(\pi(N) - \log\Delta) - O(\sqrt{N}\log(\Delta N))}{D} - \log q$$

(due to the Theorem 3.). We have repeatedly used the fact the number of prime factors of $M \in \mathbb{N}$ is $O(\log M)$.

Hence, Theorem 2. has been proved (use the preceding lemma as well for bounds on D and Δ).

Chapter 5

Conclusion and Future Scope

In Chapter 3, we saw that the computational version of the Hilbert's Nullstellensatz, HN, is in $PSPACE$. In Chapter 4, we saw that HN is in AM when the polynomials are considered over the ring of integers and Generalized Riemann Hypothesis is assumed. The following problems are open for the future. Can one put HN in AM for integer polynomials without assuming the Generalized Riemann Hypothesis? Can one put HN in AM for polynomials over all fields (particularly those having positive characteristic)? Is it possible to put HN in $NP \subseteq AM$? These questions are yet to be answered.

Bibliography

Adleman, L. M. and Odlyzko, A. M. (1983). *Irreducibility testing and factorization of polynomials.* Mathematics of Computation, 41(164):699–709.

Arora, S. and Barak, B. (2009). *Computational Complexity: A Modern Approach.* Cambridge University Press, Princeton University.

Arrondo, E. (2006). *Another Elementary Proof of the Nullstellensatz.* The Mathematical Association of America.

Atiyah, M. F. and MacDonald, I. G. (1994). *Introduction To Commutative Algebra.* Avalon Publishing, University of Oxford.

Berkowitz, S. J. (1984). *On computing the determinant in small parallel time using a small number of processors.* Elsevier Science Publishers, Array Systems Computing, Downsview. Ontario M3H 5T5, Canada.

Brown, K. (2010). *The Primitive Element Theorem.* Mathematics 6310, Fall 2011, Algebra, Cornell University.

Cox, D. A., Little, J., and O'Shea, D. (2015). *Ideals, Varieties, and Algorithms.* Springer International Publishing.

Dwivedi, A. (2017). *On the Complexity of Hilbert's Nullstellensatz over Positive Characteristic.* Indian Institute of Technology Kanpur.

Hartshorne, R. (1977). *Algebraic Geometry.* Springer, Berkeley, California.

Jelonek, Z. (2005). *On the effective Nullstellensatz.* Inventiones mathematicae - Springer, Instytut Matematyczny, Polska Akademia Nauk, Poland.

Koiran, P. (1996). *Hilbert's Nullstellensatz is in the Polynomial Hierarchy.* DIMACS, LIP, Ecole Normale Supérieure de Lyon - CNRS.

Shafarevich, I. R. (1988). *Basic Algebraic Geometry.* Springer, Moscow State University.

Sudan, M. (1998). *Algebra and Computation Lecture Notes.* MIT.