The Complexity of Algebraic Geometry and Commutative Algebra

Charles Denis Xavier

Contents

CHAPTER 1

Mathematical Background

In this chapter we will give a self contained presentation of all the mathematical ideas which are involved in the following discussion.

1. Ideals

If R is a ring and $I \subseteq R$ then I is an ideal if it satisfies :

1. $a \in I, b \in I \Rightarrow a - b \in I$.
2. $a \in I, r \in R \Rightarrow ra \in I$.

Let $A = \{a_1, \cdots, a_k\} \subseteq R$, the ideal generated by A denoted $\langle a_1, \cdots, a_k \rangle$ is the intersection of all the ideals containing A. If R is a commutative ring with identity then $\langle a_1, \cdots, a_k \rangle = \{r_1 a_1 + r_2 a_2 + \cdots + r_k a_k \mid r_i \in R, a_i \in A\}$.

Definition 1.1. An $\mathbb{N}$-*graded ring* S is a ring together with a (internal) direct sum decomposition $S = S_0 \oplus S_1 \oplus \cdots$, such that $S_d S_e \subseteq S_{d+e}$. The component S_d is called the d-degree homogeneous component of S.

The ring $\mathbb{F}[x_1, \cdots, x_n]$ can be given a graded structure by setting S to be $\mathbb{F}[x_1, \cdots, x_n]$ and

$$S_d = \{f \ : \ f \in \mathbb{F}[x_1, \cdots, x_n], \deg(f) = d \text{ and } f \text{ is homogeneous}\}$$

It is easy to see that every element p of a graded ring S can be expressed uniquely as a finite sum of elements from S_d, these are called the homogeneous components of p.

Definition 1.2. If $\mathcal{A}$ is the polynomial ring we define a subset of $\mathcal{A}$ called the set of power products of $\mathcal{A}$ denoted $PP_{\mathbb{F}}[x_1, \cdots, x_n]$:

1. $1 \in PP_{\mathbb{F}}[x_1, \cdots, x_n]$.
2. For $1 \leq i \leq n$, $x_i \in PP_{\mathbb{F}}[x_1, \cdots, x_n]$.
3. For $1 \leq i \leq n$, $m \in PP_{\mathbb{F}}[x_1, \cdots, x_n] \Rightarrow m x_i \in PP_{\mathbb{F}}[x_1, \cdots, x_n]$.

Let I be an ideal, then $\sqrt{I} \equiv \{f \mid \exists m \in \mathbb{N}, m \geq 1 \ : \ f^m \in I\}$, is called the *radical* of I. If $I = \sqrt{I}$ then I is called a radical ideal. An ideal I is called *prime* if $fg \in I \Rightarrow (f \in I \vee g \in I)$. An ideal I is called *primary* if $fg \in I \Rightarrow (f \in I \vee g^m \in I)$ for some $m \in \mathbb{N}, m \geq 1$.

We are primarily interested in ideals in the ring of multivariate polynomials.

Definition 1.3. A total ordering $\succ$ on the monomials of $\mathbb{F}[x_1, \cdots, x_n]$ is called **admissible**, if the following hold :

1. For monomials m_1, m_2, m_3, $m_1 \succ m_2 \Rightarrow m_1 m_3 \succ m_2 m_3$.
2. For all variables x_i, $x_i \succ 1$.

Definition 1.4. Let $f \in \mathbb{F}[x_1, \cdots, x_n]$ and let $\succ$ be an admissible ordering on the monomials of $\mathbb{F}[x_1, \cdots, x_n]$. Then if $f = a_0 m_0 + a_1 m_1 + \cdots + a_k m_k$ where m_i's are monomials and $a_i \in \mathbb{F}$, and $m_0 \succ m_1 \succ \cdots \succ m_k$. Then

1. LT $(f) \equiv a_0 m_0$.
2. LM $(f) \equiv m_0$.

3. Terms $(f) \equiv \{a_0 m_0, a_1 m_1, \cdots, a_k m_k\}$.

We fix an admissible ordering in the following discussion.
Let $H \subseteq \mathbb{F}[x_1, \cdots, x_n]$. A polynomial $f \in \mathbb{F}[x_1, \cdots, x_n]$ is said to be H-*reducible* if there is a monomial $m \in \mathbb{F}[x_1, \cdots, x_n]$, and a polynomial $h \in H$, such that $\mathrm{LT}(ch) \in$ Terms (f). The polynomial $g = f - ch$ is called a *reduct* of f. We denote this relationship by $f \xrightarrow{H} g$. The transitive closure $f \xrightarrow[*]{H} g$ means that there is a sequence of polynomials $h_1, \cdots, h_l$ such that $h_1 = f, h_l = g$ and for all $i < l \ : \ h_i \xrightarrow{H} h_{i+1}$. We say that g is a H-normal form of f if :

1. $f \xrightarrow[*]{H} g$, and
2. g is not H-reducible.

If $f_1, \cdots, f_k \in \mathbb{F}[x_1, \cdots, x_n]$, and let $I = \langle f_1, \cdots, f_k \rangle$ then a set $G \subseteq I$ forms a Gröbner basis if any of the following equivalent conditions are satisfied :

1. $\forall h \in I \ \exists g \in G \ : \ \mathrm{LT}\ (g) \setminus \mathrm{LT}\ (h)$.
2. $f \in I \Leftrightarrow f \xrightarrow[*]{G} 0$.
3. $\langle \mathrm{LT}\ (f) \mid f \in I \rangle = \langle \mathrm{LT}\ (g) \mid g \in G \rangle$.

DEFINITION 1.5 (S-Polynomial). If $f, g \in I \subseteq \mathbb{F}[x_1, \cdots, x_n]$ then

$$S(f,g) = \frac{\mathrm{lcm}\ (\mathrm{LM}\ (f), \mathrm{LM}\ (g))}{\mathrm{LT}\ (f)} f - \frac{\mathrm{lcm}\ (\mathrm{LM}\ (f), \mathrm{LM}\ (g))}{\mathrm{LT}\ (g)} g$$

THEOREM 1.6 (Buchberger's Criterion). *If* $G \subseteq \mathbb{F}[x_1, \cdots, x_n]$*, then* G *is a Gröbner basis iff*

$$\forall f, g \in G \ : \ S(f,g) \xrightarrow[*]{G} 0$$

In many cases it turns out that shifting attention to *homogeneous ideals* simplifies the analysis of the structure of the ideals.

DEFINITION 1.7. (Homogenizing ring) We define $\mathbb{F}^{(h)}[y, x_1, \cdots, x_n]$ as the ring obtained by the homogenization of the polynomial ring $\mathbb{F}[x_1, \cdots, x_n]$. $f = \sum_i a_i m_i \in \mathbb{F}[x_1, \cdots, x_n] \Rightarrow f^{(h)} \in \mathbb{F}^{(h)}[y, x_1, \cdots, x_n]$ where

$$f^{(h)} = \sum_i a_i m_i y^{\deg(f) - \deg(m_i)}$$

Notation : We sometimes use $\mathcal{A}$ for $\mathbb{F}[x_1, \cdots, x_n]$ and $\mathcal{A}^{(h)}$ for $\mathbb{F}^{(h)}[y, x_1, \cdots, x_n]$.

2. Algebraic Geometry

2.1. Algebraic Sets.

DEFINITION 2.1. Let $S \subseteq \mathbb{F}^n$, if there are polynomials $f_1, \cdots, f_k \in \mathbb{F}[x_1, \cdots, x_n] = \mathcal{A}$, such that $S = \{x \mid \forall i \ : \ 1 \leq i \leq k \ (f_i(x) = 0)\}$, then S is called an *algebraic set.* $\frac{\mathbb{F}[x_1, \cdots, x_n]}{\langle f_1, \cdots, f_k \rangle}$ is called the *coordinate ring* of S, and denoted $\mathcal{A}(S)$.

Taking the algebraic sets as closed sets, we can impose a natural topology on $\mathbb{F}^n$. A closed set V in a topological space is said to be *irreducible* if there are no proper closed subsets V_1, V_2 of V, such that $V = V_1 \cup V_2$. We call the irreducible algebraic sets *algebraic varieties.*

DEFINITION 2.2. If $U \subseteq \mathbb{F}^n$ is an algebraic set, we denote the ideal of polynomials which vanish on all points of U by $\mathbf{I}(U) \equiv \{f \in \mathcal{A} \mid \forall x \in U \ : \ f(x) = 0\}$. If I is an ideal in $\mathcal{A}$ then we denote the algebraic set $U \equiv \{x \in \mathbb{F}^n \mid \forall f \in I \ : \ f(x) = 0\}$, by $\mathbf{V}(I)$, or by $\mathbf{Z}(I)$.

2.2. Schemes.

DEFINITION 2.3 (Presheaf). Let X be a topological space. A **presheaf** $\mathcal{F}$ of abelian groups (rings, sets) on X consists of

1. For every open subset $U \subseteq X$, an abelian group (rings, sets) $\mathcal{F}(U)$ is associated.
2. For every inclusion $V \subseteq U$, of open subsets of X a morphism of abelian groups (rings, sets) $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ which satisfies
   (a) $\mathcal{F}(\emptyset) = 0$, where $\emptyset$ is the empty set.
   (b) ρ_{UU} is the identity map $\mathcal{F}(U) \to \mathcal{F}(U)$
   (c) If $W \subseteq V \subseteq U$, are three open subsets then $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$.

If $\mathcal{F}$ is a presheaf on X, we refer to $\mathcal{F}(U)$ as the *sections* of the presheaf $\mathcal{F}$ over the open set U. The notation $\Gamma(U, \mathcal{F})$ is used to denote the group $\mathcal{F}(U)$. We call the maps ρ_{UV} *restriction* maps, and if $s \in \mathcal{F}(U)$ we write $s|_V$ instead of ρ_{UV}.

DEFINITION 2.4 (Sheaf). A presheaf $\mathcal{F}$ on a topological space X is a **sheaf** if it satisfies the following conditions

1. If U is an open set, with $U = \bigcup_{i \in I} V_i$, where each V_i is an open set, and $s \in \mathcal{F}(U)$ is an element such that $\forall i \in I \, : \, s|_{V_i} = 0$, then $s = 0$.
2. If U is an open set, with $\{V_i \mid i \in I\}$ an open covering of U, and if we have for each $i \in I$, $s_i \in \mathcal{F}(V_i)$ such that $\forall i, j \in I \, : \, s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$, then $\exists s \in \mathcal{F}(U)$ such that $\forall i \in I \, : \, s|_{V_i} = s_i$.

DEFINITION 2.5 (Stalk). If $\mathcal{F}$ is a presheaf on X, and $P \in X$, the **stalk** $\mathcal{F}_P$ of $\mathcal{F}$ at P is defined as the set $\{\langle U, s\rangle \mid U \in \text{Nbd}(P), s \in \mathcal{F}(U)\}$. $\langle U, s\rangle \equiv \langle V, t\rangle$ iff there is $W \in \text{Nbd}(P)$, with $W \subseteq U \cap V$, such that $s|_W = t|_W$.

DEFINITION 2.6 (Morphisms). If $\mathcal{F}$ and $\mathcal{G}$ are presheaves on X, a **morphism** $\varphi \, : \, \mathcal{F} \to \mathcal{G}$ consists of a morphism of abelian groups $\varphi(U) \, : \, \mathcal{F}(U) \to \mathcal{G}(U)$ for each open set U, such that whenever $V \subseteq U$, the diagram

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\varphi(U)"] \arrow[d, "\rho_{UV}"] & \mathcal{G}(U) \arrow[d, "\rho'_{UV}"] \\
\mathcal{F}(V) \arrow[r, "\varphi(V)"] & \mathcal{G}(V)
\end{tikzcd}$$

is commutative. Where ρ, ρ' are the restriction maps in $\mathcal{F}$ and $\mathcal{G}$. The same definition applies in the case $\mathcal{F}$ and $\mathcal{G}$ are sheaves. An **isomorphism** is a morphism which has a two sided inverse.

DEFINITION 2.7. If A is a ring Spec $A \equiv_{\text{def}} \{\mathfrak{p} \mid \mathfrak{p}$ is a prime ideal of $A\}$. If $\mathfrak{a}$ is any ideal of A,
$V(\mathfrak{a}) \subseteq$ Spec A is the set of all prime ideals which contain $\mathfrak{a}$.

LEMMA 2.8 (Topology on Spec A). *The following are elementary properties of* $V(\mathfrak{a})$

1. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are two ideals of* A*, then* $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.
2. *If* $\{\mathfrak{a}_i\}$ *is any set of ideals of* A*, then* $V(\sum \mathfrak{a}_i) = \bigcap V(\mathfrak{a}_i)$.
3. *If* $\mathfrak{a}$*, and* $\mathfrak{b}$ *are two ideals, then* $V(\mathfrak{a}) \subseteq V(\mathfrak{b})$ *iff* $\sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}}$.

The above lemma allows us to define a topology on Spec A as follows. Subsets of the form $V(\mathfrak{a})$ of Spec A are the closed subsets. We have $V(A) = \phi$ and $V(\langle 0\rangle) =$ Spec A. The lemma shows that finite unions and arbitrary intersections of sets of the form $V(\mathfrak{a})$ are also of that form. Hence they form a topology on Spec A.

We define a sheaf of rings $\mathcal{O}$ on Spec A. For each prime ideal $\mathfrak{p} \subseteq A$, let $A_\mathfrak{p}$ be the localization of A at $\mathfrak{p}$. For an open set $U \subseteq$ Spec A define $\mathcal{O}(U)$ to be the set of functions $s \, : \, U \to \coprod_{\mathfrak{p} \in U} A_\mathfrak{p}$. Such that for each $\mathfrak{p} \in U$, there is a neighborhood V of $\mathfrak{p}$, $V \subseteq U$, and elements $a, f \in A$ such that for each $\mathfrak{q} \in V$, we have $f \notin \mathfrak{q}$ and $s(\mathfrak{q}) = a/f$ in $A_\mathfrak{q}$. $\mathcal{O}(U)$ itself is a commutative ring with identity. If $V \subseteq U$ are two open sets, the natural restriction map $\mathcal{O}(U) \to \mathcal{O}(V)$ is a homomorphism of rings. Thus $\mathcal{O}$ is a presheaf, the local nature given above shows that it is indeed a sheaf.

Definition 2.9. Let A be a ring. The **spectrum** of A is a pair consisting of the topological space Spec A together with the sheaf of rings $\mathcal{O}$ defined as above.

Definition 2.10 (Ringed Space). A **ringed space** is a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and a sheaf of rings $\mathcal{O}_X$ on X. A **morphism** of ringed spaces from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a pair $(f, f^{\#})$ of a continuous map $f : X \to Y$ and a map $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$ of sheaves of rings on Y. The ringed space $(X, \mathcal{O}_X)$ is a **locally ringed space** if for each $P \in X$, the stalk $\mathcal{O}_{X,P}$ is a local ring. Where f_* refers to the direct product cycle of f.

Definition 2.11 (Scheme). An **affine scheme** is a locally ringed space $(X, \mathcal{O}_X)$ which is isomorphic to the spectrum of some ring. A **scheme** is a locally ringed space $(X, \mathcal{O}_X)$ in which every point has an open neighborhood U such that the topological space U, together with the restricted sheaf $\mathcal{O}_X|_U$ is an affine scheme.
X is called the **underlying topological space** of the scheme $(X, \mathcal{O}_X)$, and $\mathcal{O}_X$ is refered to as the **structure sheaf**.

Definition 2.12 (Dimension). The **dimension** of a scheme X, demoted $\dim X$, is its dimension as a topological space. If Z is an irreducible closed subset of X, then the **codimension** of Z in X, denoted codim (Z, X) is the supremum of integers n, such that there is a chain

$$Z = Z_0 \prec Z_1 \prec \cdots \prec Z_n$$

of distinct closed irreducible subsets of X. If $Y \subseteq X$ and Y is closed then, we define

$$\text{codim } (Y, X) = \inf_{Z \subseteq Y} \text{codim } (Z, X)$$

Where the infimum is taken over irreducible Z.

Definition 2.13 (Complete Intersections). A **complete intersection** in $\mathbb{P}^n$, is a closed subscheme $Y \subseteq \mathbb{P}^n$ such that the homogeneous ideal $I = \mathbf{Z}(Y)$ in $S = k[x_0, \cdots, x_n]$ can be generated by $r = \text{codim } (Y, \mathbb{P}^n)$ elements.

Proposition 2.14. *Let Y be a closed subscheme of codimension r in $\mathbb{P}^n$. Then Y is a complete intersection iff there are hypersurfaces (locally principal subschemes of codimension 1) $H_1, \cdots, H_r$, such that $Y = H_1 \cap H_2 \cap \cdots \cap H_r$ as schemes, or $I(Y) = I(H_1) + \cdots + I(H_r)$.*

CHAPTER 2

Effective Nullstellensatz

1. Introduction

We begin our investigations with a discussion on the effectivity results on the *Hilbert's Nullstellensatz.*

THEOREM 1.1 (Hilbert's Nullstellensatz). *Let* k *be an algebraically closed field and let* $\mathfrak{a}$ *be an ideal in* $A = k[x_1, \cdots, x_n]$*, and if* $f \in k[x_1, \cdots, x_n]$ *, such that* $\mathbf{Z}(f) \supseteq \mathbf{Z}(\mathfrak{a})$*, then* $\exists r \in \mathbb{N}, r > 0 \ : \ f^r \in \mathfrak{a}$.

COROLLARY 1.2. *If* $f_1, \cdots, f_k \in \mathbb{C}[x_1, \cdots, x_n]$ *have no common zeros. Then there are polynomials* $g_1, \cdots, g_k \in \mathbb{C}[x_1, \cdots, x_n]$ *such that*

$$(\star) \qquad \sum_{1 \leq i \leq k} g_i f_i = 1$$

The problem of *Effective Nullstellensatz* is to find a bound on the degree of the polynomials g_i. The proof of the theorem being nonconstructive does not yield a direct computation of the degrees. In the following we shall derive a bound on the degrees of the polynomials involved in the Nullstellensatz, and then go on to show that the decision version of this problem can be solved in AM if the Generalized Riemann Hypothesis is true.

2. Sharp Effective Nullstellensatz

In 1926 G. Hermann [**Her26**] gave a bound for the polynomials involved in the expression ($\star$), the bound was obtained by using elimination theory and was doubly exponential in the number of variables[1]. In what follows we shall describe closely the result of *János Kollár* [**Kol88**] which is essentially an optimal bound.

DEFINITION 2.1. If K is a field and $n, d_1, \cdots, d_k \in \mathbb{N}$ let

$$N(n, d_1, \cdots, d_k) = \min\{s \mid \forall f_1, \cdots, f_k \in K[x_1, \cdots, x_n], \deg f_i = d_i, \mathbf{Z}(\langle f_1, \cdots, f_k \rangle) = \phi,$$
$$\exists g_1, \cdots, g_k \in K[x_1, \cdots, x_n] : \sum_i g_i f_i = 1, \max_i\{\deg(f_i g_i)\} \leq s\}.$$

However we will find it easier to estimate the following quantity, and the relevance to the original problem will be shown as a corollary.

DEFINITION 2.2. If K is a field and $n, d_1, \cdots, d_k \in \mathbb{N}$ let

$$N'(n, d_1, \cdots, d_k) = \min\Big\{ s \mid \forall \overline{f_1}, \cdots, \overline{f_k}(\text{homogeneous}) \in K[x_0, x_1, \cdots, x_n],$$
$$\deg \overline{f_i} = d_i, \text{ and } \left(\sqrt{\langle \overline{f_1}, \cdots, \overline{f_k} \rangle}\right)^s \subseteq \langle \overline{f_1}, \cdots, \overline{f_k} \rangle \Big\}.$$

In some sense, the above quantity refers to how far a given ideal is, from being a radical ideal. We will require the following result in the proof of the main theorem.

LEMMA 2.3. *Let* $Z \subseteq \mathbb{P}^n$ *be a zero dimensional subscheme, and let* $h \in K[x_1, \cdots, x_n]^{(d)}$ *so that* $\deg h = d$*, such that* $\forall z \in Z \ : \ h(z) \neq 0$*. Let* $\mathcal{I}$ *be the homogeneous ideal of* Z*.*
If one of the following conditions is satisfied

1. $k \geq \text{length } Z$

[1] The bound was actually given for the more general situation of polynomial membership in an ideal.

2. *There are hypersurfaces $F_1, \cdots, F_n$ of degrees $d_1, \cdots, d_n$ such that their intersection is T is zero dimensional, Z is the union of some connected components of T, and $k \geq \sum_i (d_i - 1)$.*

then

$$\langle x_0, \cdots, x_n \rangle^{k+d} \subseteq \langle \mathcal{I}, h \rangle$$

Proof : We have,

$$\mathcal{O}_{\mathbb{P}^n}(k) \longrightarrow \mathcal{O}_Z(k) \longrightarrow 0$$

since the k-th twist of the sheaf of regular functions on $\mathbb{P}^n$ are also regular functions on Z. Let S be the graded ring of $K[x_0, \cdots, x_n]$. We have that $S = \bigoplus_{k \in \mathbb{Z}} H^0(\mathcal{O}_{\mathbb{P}^n}(k))$.

$$H^0(\mathcal{O}_{\mathbb{P}^n}(k)) = \langle x_0^{m_1} \cdots x_n^{m_n} \mid \sum_i m_i = k \rangle$$
$$H^0(\mathcal{O}_Z(k)) = \frac{\text{Ker } [\mathcal{O}_Z(k) \longrightarrow 0]}{\text{Im } [\mathcal{O}_{\mathbb{P}^n}(k) \longrightarrow \mathcal{O}_Z(k)]} = \frac{\mathcal{I}(k)}{\mathcal{O}_{\mathbb{P}^n}(k)}$$

Let,

$$M_Z(k) = \text{Im}[H^0(\mathcal{O}_{\mathbb{P}^n}(k)) \longrightarrow H^0(\mathcal{O}_Z(k))]$$

And consider the multiplication map

$$m_k \ : \ M_Z(k) \xrightarrow{h} M_Z(k+d)$$

which causes a twist change of d as $\deg h = d$.
Now observe that $\langle x_0, \cdots, x_n \rangle^{k+d} \subseteq \langle \mathcal{I}, h \rangle$ iff m_j is surjective for $j \geq k$.
If m_j is surjective for all $j \geq k$, then for $f \in \langle x_0, \cdots, x_n \rangle^{k+d}$
there are $f_1, \cdots, f_{k+d}, f_i \in \langle x_0, \cdots, x_n \rangle \ : \ f = f_1 \cdots f_{k+d}$. Clearly $\deg f \geq (k+d)$, so we can split it up into homogeneous components of degrees ranging from $k+d$ to $\deg f$. So there are polynomials $g_1, \cdots, g_l \in H^0(\mathcal{O}_{\mathbb{P}^n}(\deg g_i)) \subseteq H^0(\mathcal{O}_Z(\deg g_i))$, such that $f = g_1 + g_2 \cdots + g_l + \alpha$, where $\alpha \in \mathcal{I}$.
But as m_j is surjective we have $g_i = h \times p_i$ for some p_i polynomials of smaller degree, so $\sum_i g_i \in \langle h \rangle$. Thus we have $f \in \langle \mathcal{I}, h \rangle$. The other direction can be done similarly.

Now as h is not zero on Z it is injective since otherwise $h \times a = h \times b \Rightarrow h(a-b) = 0$, with $a - b$ nonzero on Z. So we have that m_k is surjective if $M_Z(k) = H^0(\mathcal{O}_Z(k))$.

In case (1), let S be a connected component of Z, and let m be the ideal of the closed point of S. Recall that a closed point of S is a minimal closed subset of S in the Zariski space. Since we can find a hypersurface of degree (length S) such that it is zero on S and not zero at the other points of Z. We have $m^{\text{length } S} \ \mathcal{O}_S = 0$. So the following sequence of maps becomes surjective,

$$H^0(\mathcal{O}_{\mathbb{P}^n}(k)) \longrightarrow H^0(\mathcal{O}_{\mathbb{P}^n}/m^{k+1}(k)) \longrightarrow H^0(\mathcal{O}_S(k))$$

is surjective for $k \geq$ length S. Now multiplying such polynomials together we get the surjectivity of $M_Z(k)$.

In case (2), we have by Macaulay *[Reference to be added.]* that the map

$$H^0(\mathcal{O}_{\mathbb{P}^n}(k)) \longrightarrow H^0(\mathcal{O}_T(k))$$

is surjective in the required range. Hence the map for Z is also such a map. □

Theorem 2.4 (Main Theorem). *Given a field K and $n, d_1, \cdots, d_k \in \mathbb{N}$ with $d_1 \geq d_2 \geq \cdots \geq d_k$, and $1 \leq i \leq k, d_i \neq 2$. Then*

$$N'(n, d_1, \cdots, d_k) = \begin{cases} d_1 d_2 \cdots d_k & \textit{if}\, k \leq n \\ d_1 d_2 \cdots d_{n-1} d_k & \textit{if}\, k > n > 1 \\ d_1 + d_k - 1 & \textit{if}\, k > n = 1 \end{cases}$$

Proof : Consider the polynomials f_i, we rearrange them so that $d_1 = \min\{d_1, \cdots, d_k\}$, and also $d_2 \geq d_3 \geq \cdots \geq d_k$.
Let $F_i = \mathbf{Z}(f_i)$.
Let $R = F_1 \cap F_2 \cap \cdots \cap F_k$, and $\mathcal{R}$ be the homogeneous ideal of R.
Let $U = \mathbb{P}^n - R$, which is an open set.
And let $Z_i = \overline{(U \cap F_1 \cap \cdots \cap F_i)}$ which is the topological closure in the Zariski topology.

Now $Z_i \cap U \subset Z_{i-1} \cap U \subset \cdots \subset Z_1 \cap U$. So $Z_i \cap U$ is a complete intersection of codimension i.

As $\langle f_1, \cdots, f_i \rangle \supset Z_i \cap U$, and since we can express f_i's as general linear combinations of $f_1, \cdots, f_i$, we can arrange that $\langle f_1, \cdots, f_i \rangle \supset \langle f_1, \cdots, f_{i-1} \rangle$. Further by assumption $\langle f_1, \cdots, f_k \rangle = \langle 1 \rangle$, and also polynomials in each of these ideals vanish over the set. So the conclusion is obvious.
We can write $\langle f_1, \cdots, f_i \rangle = \mathbf{I}(Z_i) \cap I_i$, where $\mathbf{I}(Z_i)$ is the homogeneous ideal of Z_i and I_i is a homogeneous ideal whose cosupport is in R. I_i may not be unique.

Let $a_i = \min\{s \,:\, \mathcal{R}^s$ annihilates $\frac{\mathbf{I}(Z_i)}{\langle f_1, \cdots, f_k \rangle}\}$.
By assumption $\mathbf{I}(Z_k)$ is the whole ring, and so a_k tells us which power of h is in the ideal of the f_i.
So we have to estimate the a_i.

[**Inductive Step**] Consider the following decomposition :

$$\langle \mathbf{I}(Z_i), f_{i+1} \rangle = \mathbf{I}(Z_{i+1}) \cap \mathcal{K}_{i+1} \cap \mathcal{E}_{i+1}$$

where $\mathcal{K}_{i+1}$ is the intersection of the primary components of codimension $i+1$ whose cosupport is in R, and $\mathcal{E}_{i+1}$ is the intersection of the primary components whose cosupport has codimension $\geq i+2$. Support of $\mathcal{E}_{i+1}$ is also in R. Further $\mathcal{K}_{i+1}$ is uniquely defined.

Let

$$k_{i+1} = \min\{s \mid \mathcal{R}^s \subseteq \mathcal{K}_{i+1}\}$$

and let

$$e_{i+1} = \min\left\{s \,:\, \mathcal{R}^s \text{ annihilates } \frac{\mathbf{I}(Z_{i+1}) \cap \mathcal{K}_{i+1}}{\langle \mathbf{I}(Z_i), f_{i+1} \rangle}\right\}$$

hence $\mathcal{R}^{k_{i+1}+e_{i+1}}$ annihilates $\frac{\mathbf{I}(Z_{i+1})}{\langle \mathbf{I}(Z_i), f_{i+1} \rangle}$.

As $f \in \frac{\mathbf{I}(Z_{i+1})}{\langle \mathbf{I}(Z_i), f_{i+1} \rangle} \to f = \alpha + \beta$, where $\alpha \in \mathbf{I}(Z_{i+1}), \beta \in \langle \mathbf{I}(Z_i), f_{i+1} \rangle$

$$\text{let } \gamma \in \mathcal{R}^{k_{i+1}}$$
$$\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta,$$
$$\text{now }, \gamma\alpha \in \mathbf{I}(Z_{i+1}) \cap K_{i+1}, \text{ and so }, \gamma\alpha + \gamma\beta \in \frac{\mathbf{I}(Z_{i+1}) \cap \mathcal{K}_{i+1}}{\langle \mathbf{I}(Z_i), f_{i+1} \rangle}$$

which is annihilated by $\mathcal{R}^{e_{i+1}}$, so the conclusion follows.
Also clearly $\mathcal{R}^{a_i}$ annihilates

$$\frac{\langle \mathbf{I}(Z_i), f_{i+1} \rangle}{\langle f_1, \cdots, f_i, f_{i+1} \rangle} \Rightarrow \mathcal{R}^{a_i} \langle \mathbf{I}(Z_i), f_{i+1} \rangle \subseteq \langle f_1, \cdots, f_i, f_{i+1} \rangle$$

So we have $\mathcal{R}^{k_{i+1}+e_{i+1}+a_i}$ annihilates

$$\frac{\mathbf{I}(Z_{i+1})}{\langle f_1, \cdots, f_i, f_{i+1}\rangle}$$

Thus we have $a_{i+1} \leq k_{i+1} + e_{i+1} + a_i$, also $k_{i+1} \leq$ the degree of the scheme defined by $\mathcal{K}_{i+1}$, and e_{i+1} is due to the embedded primes. In what follows we will bound these terms.

Definition 2.5. If S is a scheme and $\mathcal{R}$ is an ideal we define

$$\operatorname{nil}(\mathcal{R}, S) = \min\{t \mid \forall Z \subseteq \mathbf{Z}(\mathcal{R}), \forall i < \operatorname{codim}_Z(S) \ : \ \mathcal{R}^t H_Z^i(\mathcal{O}_S) = 0\}.$$

Lemma 2.6. *Let* X *be a pure dimensional affine scheme. Let* f *be a nonzero divisor, and let* $\mathcal{R}$ *be an ideal. Let* $R = \operatorname{Spec} \mathcal{O}_X/\mathcal{R}$. *Let*

$$\langle f \rangle = I \cap K \cap E$$

where I *is the intersection of isolated primary ideals whose cosupport is not in* R, K *is the intersection of isolated primary ideals whose cosupport is in* R, *and* E *is the intersection of embedded primary ideals.*

Further let X' *be the scheme defined by* I.

If $\mathcal{R}^k \subseteq K$, *and* cosupp $E \subseteq R$, *then*

$$\operatorname{nil}(\mathcal{R}, X') \leq 3\operatorname{nil}(\mathcal{R}, K) + k.$$

Proof : Consider the exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_X \arrow[r, "f"] & \mathcal{O}_X \arrow[r] & \frac{\mathcal{O}_X}{\langle f \rangle} \arrow[r] & 0 \\
0 \arrow[r] & \frac{I}{\langle f \rangle} \arrow[r] & \frac{\mathcal{O}_X}{\langle f \rangle} \arrow[r] & \mathcal{O}_{X'} \arrow[r] & 0
\end{tikzcd}$$

these give rise to the homological sequences

$$\begin{tikzcd}
H_Z^i(\mathcal{O}_X) \arrow[r] & H_Z^i(\frac{\mathcal{O}_X}{\langle f \rangle}) \arrow[r] & H_Z^{i+1}(\mathcal{O}_X) \\
H_Z^i(\frac{\mathcal{O}_X}{\langle f \rangle}) \arrow[r] & H_Z^i(\mathcal{O}_{X'}) \arrow[r] & H_Z^{i+1}(\frac{I}{\langle f \rangle})
\end{tikzcd}$$

Now

$$H_Z^i\left(\frac{\mathcal{O}_X}{\langle f \rangle}\right) = \frac{\operatorname{Ker}\left(\frac{\mathcal{O}_X}{\langle f \rangle} \to 0\right)}{\operatorname{Im} \mathcal{O}_X} = \frac{\langle f \rangle}{\operatorname{Im} \mathcal{O}_X}$$

Now

$$\mathcal{R}^{\operatorname{nil}(\mathcal{R}, X)}$$

annihilates $H_Z^i(\mathcal{O}_X)$,

$$g \in H_Z^i\left(\frac{\mathcal{O}_X}{\langle f \rangle}\right) \Rightarrow g = \alpha + \beta \ : \ \alpha \in \langle f \rangle, \beta \in \operatorname{Im} \mathcal{O}_X$$

So $\mathcal{R}^{2\operatorname{nil}(\mathcal{R}, X)}$ annihilates $H_Z^i\left(\frac{\mathcal{O}_X}{\langle f \rangle}\right)$. We have to estimate the power of $\mathcal{R}$ which will annihilate $H_Z^{i+1}\left(\frac{I}{\langle f \rangle}\right)$. We first determine which power of $\mathcal{R}$ annihilates $\frac{I}{\langle f \rangle}$. We have

$$\begin{tikzcd}
0 \arrow[r] & \frac{I \cap K}{\langle f \rangle} \arrow[r, "\subseteq"] & \frac{I}{\langle f \rangle} \arrow[r, "\subseteq"] & \frac{I}{I \cap K} \arrow[r] & 0
\end{tikzcd}$$

Now $\mathcal{R}^k$ annihilates $\frac{I}{I \cap K}$. If Z is the support of $\frac{I \cap K}{\langle f \rangle}$, then $\frac{I \cap K}{\langle f \rangle} = H_Z^0\left(\frac{I \cap K}{\langle f \rangle}\right) = H_Z^0(\frac{\mathcal{O}_X}{\langle f \rangle}) \hookrightarrow H_Z^1(\mathcal{O}_X)$.
As $0 \leq i$, we have $\mathcal{R}^{\operatorname{nil}(\mathcal{R}, X)}$ annihilates $\frac{I \cap K}{\langle f \rangle}$, and as $\mathcal{R}^k \subseteq K$, $\mathcal{R}^{\operatorname{nil}(\mathcal{R}, X)+k}$ annihilates $\frac{I}{\langle f \rangle}$. Hence $\mathcal{R}^{3\operatorname{nil}(\mathcal{R}, X)+k}$ annihilates $H_Z^{i+1}(\mathcal{O}_S)$.

□

Here we assume that $k \geq n$. Now consider the sequence of hypersurfaces as defined earlier $F_i, 1 \leq i \leq n$. Z_i are the schemes as defined. We also have a well defined sequence of integers $k_1, \cdots, k_n$. As Z_1 is a hypersurface we have $\mathrm{nil}(\mathcal{R}, Z_1) = 0$.
Thus we inductively get upper bounds for $\mathrm{nil}(\mathcal{R}, Z_i)$ as follows. To get estimates for the numbers a_j consider

$$\frac{I_j \cap K_j}{\langle f_j \rangle} = H^0_Z\left(\frac{I_j \cap K_j}{\langle f_j \rangle}\right) \hookrightarrow H^1_Z\left(\mathcal{O}_{Z_{j-1}}\right)$$

so we have $e_j \leq \mathrm{nil}(\mathcal{R}, Z_{j-1})$, thus from the bound in the inductive case we have

$$\begin{aligned} a_n &\leq \sum_{1 \leq i \leq n} \left(k_i + \mathrm{nil}(R, Z_{i-1})\right) \\ &\leq \sum_{1 \leq i \leq n} \left(k_i + \sum_{1 \leq j \leq i-1} k_j 3^{i-1-j}\right) \\ &= \sum_{1 \leq i \leq n} k_i \left(1 + \sum_{i+1 \leq j \leq n} 3^{j-i-1}\right) \\ &= \sum_{1 \leq i \leq n} k_i \frac{3^{n-i}+1}{2}. \end{aligned}$$

Z_n is a zero dimensional subscheme and we have to compute its degree. $\deg Z_{i+1} = d_{i+1} \deg Z_i - \deg \mathcal{O}_{\mathcal{P}^n}/K_{i+1}$. $h \in \sqrt{K_{i+1}}$, and this ideal is unmized. Thus we have

$$\mathcal{R}^{\deg \mathcal{O}_{\mathcal{P}^n}/K_{i+1}} \subseteq K_{i+1}$$

$$\text{in particular } k_{i+1} \leq \deg \mathcal{O}_{\mathcal{P}^n}/K_{i+1}$$

$$\text{thus we get } \deg Z_{i+1} \leq d_{i+1} \deg Z_i - k_{i+1}$$

$$\text{so } \deg Z_n \leq \prod_{1 \leq i \leq n} d_i - \sum_{1 \leq i \leq n} k_i \prod_{i+1 \leq j \leq n} d_j$$

$$\text{as } d_j \geq 3, \text{ we have } \deg Z_n \leq \prod_{1 \leq i \leq n} d_i - \sum_{1 \leq i \leq n} k_i 3^{n-i-1} d_n$$

Now we have a straightforward lemma :

LEMMA 2.7.

$$k_i \frac{3^{n-i}+1}{2} \leq k_i 3^{n-i-1} d_n$$

$$\textit{and } d_n + k_i \frac{3^{n-i}+1}{2} \leq k_i 3^{n-i-1} d_n$$

unless $i = n-1$ *and* $k_i = 1$ *or* 2.

Case $k \leq n$: We have as $Z_k = \phi$,

$$\begin{aligned} a_k &\leq \sum_{1 \leq i \leq n} k_i \frac{3^{n-i}+1}{2} \leq \sum_{1 \leq i \leq n} k_i 3^{n-i-1} d_n \\ &\leq \prod_{1 \leq i \leq k} d_i - \deg Z_k = \prod_{1 \leq i \leq k} d_i \end{aligned}$$

So we have the required bound in this case.
Case $k_1 = \cdots = k_{n-1} = 0$: In this case the hypersurfaces F_i intersect in a zero dimensional subscheme of $\mathbb{P}^n$. So we can use 2.3 to see that the map

$$M_k \xrightarrow{f_{n+1}} M_{k+d_{n+1}}$$

is surjective for $k \geq \sum_{1\leq i\leq n}(d_i - 1)$.
If we consider the quotient $K[x_0, \cdots, x_n]/\langle f_1, \cdots, f_{n+1}\rangle$ then for $d \geq d_{n+1} + \sum_{1\leq i\leq n}(d_i - 1)$, the degree d graded piece has support in H. By Bezout's theorem, the cosupport of K_n has length at most $\prod_{1\leq i\leq n} d_i$, thus $\mathcal{R}^{\prod_{1\leq i\leq n} d_i} \subseteq K_n$. As $\prod_{1\leq i\leq n} d_i \geq d_{n+1} + \sum_i(d_i - 1)$ we have $\mathcal{R}^{\prod_{1\leq i\leq n} d_i} \subseteq \langle f_1, \cdots, f_{n+1}\rangle$. Which is what we have to show.

Case $k > 0$ *for some* $i \leq (n-1)$: We have $\mathcal{R}^{a_n}$ annihilates $\frac{I_n}{\langle f_1,\cdots,f_n\rangle}$, and so it also annihilates $\frac{I_n, f_{n+1}}{\langle f_1,\cdots,f_n,f_{n+1}\rangle}$, by 2.3 we have $\mathcal{R}^{\deg Z_n + d_{n+1}} \subseteq \langle I_n, f_{n+1}\rangle$. Thus we have $\mathcal{R}^{\deg Z_n + d_{n+1} + a_n} \subseteq \langle I_n, f_{n+1}\rangle$. By the above lemma we have

$$a_n + \deg Z_n + d_{n+1} \leq k_i \frac{3^{n-i}+1}{2} + \prod_{1\leq i\leq n} d_i - \sum_{1\leq i\leq n} k_i 3^{n-i-1} d_n + d_{n+1} \leq \prod_{1\leq i\leq n} d_i$$

unless $k_1 = \cdots = k_{n-2} = 0$, $k_{n-1} = 1$ or 2.
Remaining Cases We have that the hypersurfaces $F_1, \cdots, F_n$ intersect in a curve C of degree c, and in finitely many other points. So $\deg Z_n = \prod_{1\leq i\leq n} d_i - c d_n - \deg \mathcal{O}_{\mathbb{P}^n}/K_n$. so we require the inequality $\deg Z_n + 2k_{n-1} + k_n + d_{n+1} \leq \prod_{1\leq i\leq n} d_i$. This is satisfied if $c \geq 3$. So the final cases are when C has degree 1 or 2. If we have $\deg \mathcal{O}_{\mathbb{P}^n}/K_n \geq k_n + 2$. As C has degree at most two, it is a local complete intersection curve and so we have by *[Reference to Fulton]*

$$|F_1 \cap \cdots \cap F_n| = |C| \cup \left|\left(\prod_i d_i - \left(\sum_i d_i - n - 1\right)c - 2\chi(\mathcal{O}_C)\right)\right|$$

From this we get that Spec $\mathcal{O}_{\mathbb{P}^n}/K_n$ has at least $\left(\sum_i d_i - n - 1\right)c + 2\chi(\mathcal{O}_C) - c d_n$ points as a subscheme of $\mathcal{O}_C$. Thus we have

$$\deg \mathcal{O}_{\mathbb{P}^n}/K_n - k_n \geq \left(\sum_{1\leq i\leq n} d_i - n - 1\right)c + 2\chi(\mathcal{O}_C) - c d_n - c \geq 2$$

if $n \geq 3$. When $n = 2$, the common curve of intersection becomes a common irreducible factor for the f_i and so we are in the reducible case which can be reduced to a simpler case. □

REMARK 2.8. If we have a bound on the degrees then the solution of $h \in \langle f_1, \cdots, f_k\rangle$, is equivalent to solving for the coefficients of polynomials of g_i in $h = \sum_i g_i f_i$, which turns out to be a linear equation for these unknowns. If we have a degree bound then solvability for these coefficients in the extension field implies solvability in the base field. Hence without loss of generality we can assume that the field K is algebraically closed.

COROLLARY 2.9. *Given* $f_1, \cdots, f_k$ *and* $h \in K[x_1, \cdots, x_n]$, *assume that* h *vanishes on all of* $\mathbf{Z}(f_1, \cdots, f_k)$ *(in the algebraic closure of* K*). Let* $d_i = \deg f_i$ *and if* $d_i \neq 2$*. Then we can find* $g_1, \cdots, g_k \in K[x_1, \cdots, x_n]$ *and* $s \in \mathbb{N}$ *such that*

$$\sum_i g_i f_i = h^s$$

and $s \leq N'(n, d_1, \cdots, d_k$ *and* $\deg g_i f_i \leq (1 + \deg h)N'(n, d_1, \cdots, d_k)$.

Proof : We first homogenize f_i to get $\overline{f_i}$ by introducing a new variable x_0, say we have to homogenize the polynomial to degree $d \geq \deg f_i$ then we set $\overline{f_i}(x_0, \cdots, x_n) = x_0^d f_i(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0})$.

Similarly let $\overline{h}$ be the homogenization of h. As h vanishes on all common zeros of f_i, then $\overline{f_i} = 0 \Rightarrow x_0^d f_i(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}) = 0$, as K is a field $x_0 \neq 0 \Rightarrow f_i = 0$. So $\overline{f_i}$ vanishes if $x_0 \neq 0$ and the other coordinates are a zero of the polynomial. So $\overline{h}$ vanishes on all common zeros of $\overline{f_i}$ which do not lie on the hyperplane at infinity $(x_0 = 0)$. Thus $x_0\overline{h}$, vanishes at all common zeros of $\overline{f_i}$.

So $x_0\overline{h}$ is contained in $\langle\overline{f_1},\cdots,\overline{f_k}\rangle$. Thus by 2.4, there are homogeneous polynomials $\overline{g_i}$ such that $\sum_i \overline{f_i}\overline{g_i} = (x_0\overline{h})^s$. We can assume that

$$\deg \overline{f_i}\overline{g_i} = s \deg x_0\overline{h} \leq N'(n, d_1, \cdots, d_k)(1 + \deg h).$$

The dehomogenization of the above now gives the result. □

There are classes of polynomials for which the above degree bound is achieved, so the bounds are tight. For the case of $d = 2$, there is a tighter bound due to *Sombra*.

3. The Complexity of the Nullstellensatz

We investigate the complexity of the following problem :

Problem : Hilbert's Nullstellensatz **(HN)**
Input : $f_1, \cdots, f_s \in \mathbb{C}[x_1, \cdots, x_n]$
Question : Is there $\overline{x} = (x_1, \cdots, x_n) \in \mathbb{C}[x_1, \cdots, x_n]$ such that $\forall 1 \leq i \leq s\ :\ f_i(\overline{x}) = 0$?

Hilbert's Nullstellensatz tells us that this happens iff $1 \notin \langle f_1, \cdots, f_s\rangle$, or it is not possible to find $g_1, \cdots, g_s \in \mathbb{C}[x_1, \cdots, x_n]\ :\ \sum_i g_i f_i = 1$.
In light of the previous result, we have a bound on the degree of the g_i's involved, so we can write $g_1 = \sum_j m_j$, where m_j are monomials, and the sum is over monomials of degree less than the bound given. In the Blum-Shub-Smale model of computation, the resulting set of linear equations obtained by the above sum can be solved using only polynomial amount of space. So **HN** $\in$ PSPACE.

However if we assume the Generalized Riemann Hypothesis, we can show that **HN** is in AM. This result is by *Koiran* [**Koi96**].

Firstly observe that **HN** is NP-hard. We give a many-one reduction from **SAT** to **HN**. If $\phi = \phi_1 \wedge \phi_2 \wedge \cdots \wedge \phi_k$, then consider the polynomials constructed as follows :

$$P_\phi = \begin{cases} x_i & \text{if } \phi = x_i \\ (1 - P_\varphi) & \text{if } \phi = \neg\varphi \\ (P_{\phi_1} + P_{\phi_2} - P_{\phi_1}P\phi_2) & \text{if } \phi = \phi_1 \vee \phi_2 \end{cases}$$

Now $\phi(x_1, \cdots, x_n) = \top \Rightarrow P_\phi(x_1, \cdots, x_n) = 1$, $\phi(x_1, \cdots, x_n) = \perp \Rightarrow P_\phi(x_1, \cdots, x_n) = 0$.
So the ideal $\langle P_{\phi_1} - 1, \cdots, P_{\phi_k} - 1, x_1^2 - x_1, \cdots, x_n^2 - x_n\rangle$, has a common zero iff ϕ was satisfiable. The polynomials $x_i^2 - x_i$, restrict attention to solutions on the Boolean cube.
We make the following notational conventions.

1. Let $S = \{f_1, \cdots, f_s\}, f_i \in \mathbb{Z}[x_1, \cdots, x_n]$.
2. Let $d = \max_i \deg f_i$
3. If $f_i = \sum_j a_{ij}x^j$ then $L = \max_{i,j} \lg |a_{ij}|$, that is L is the maximum size of the coefficients.
4. $\sigma = \deg S \equiv 2 + \sum_{1\leq i\leq s} d_i$.
5. Polynomials are assumed to be in the sparse notation, i.e., the monomials with coefficient zero are not listed.
6. We can assume that by the repeated squaring method, all polynomials have been reduced to have degree 2, and coefficients in $[-2..2]$.
7. $\pi(x) = \{1, 2, \cdots, x\} \cap \mathbf{P}$.
8. $R_S = \{p \mid S \text{ is satisfiable in } F_p = \mathbb{Z}_p\}$.
9. $R_S(x) = R_S \cap \{1, 2, \cdots, x\}$.
10. If $f \in \mathbb{Z}[x]$, then

$$R_f \equiv R_{\{f\}},$$
$$R_f(x) \equiv R_{\{f\}}(x)$$
$$\text{and } \pi_f(x) \equiv \pi_{\{f\}}(x)$$

3.1. Main theorems. Here we list the two main theorems which help us to locate the complexity of the Nullstellensatz.

THEOREM 3.1 (Main Theorem). *If GRH is true then there exist constants* $c_1, c_2, c_3 \in \mathbb{N}$ *such that if*

$$A = d^{c_1 n} s(\lceil \lg s \rceil + L),$$
$$B = 8A(\lg A + 3),$$
$$\text{and } x_0 \geq L^{c_2} 2^{(n \lg \sigma)^{c_3}}$$

then the following two properties hold :

1. *If* S *is not satisfiable in* $\mathbb{C}$ *then* $\pi_S(x_0) \leq A$.
2. *If* S *is satisfiable in* $\mathbb{C}$ *then* $\pi_S(x_0) \geq B$

REMARK 3.2. The dependence on GRH comes from a technical lemma required in the proof.

We can see that **HN** is in $P^{\sharp P^{NP}}$, since to decide whether S is satisfiable, we have to compute $\pi_S(x_0)$, since checking whether a number is prime is an NP predicate, we can compute $\pi_S(x_0)$ in $\sharp$P, using an NP-oracle which given an integer p checks whether p is prime and guesses a solution to S and verifies it in $\mathbb{Z}_p$. The main idea is that since the gap between the two cases is large enough, we need not have exact counting.

LEMMA 3.3 (Sipser's Lemma). **[Sip83]** *There is a* Σ_2^p *predicate* $\text{Hash}(E, m)$ *which has the following property. If* $E \subseteq \{0, 1\}^k$, $|E| \leq 2^{m-2}$ *then* $\text{Hash}(E, m) = \top$, *and if* $|E| \geq m2^m$ *then* $\text{Hash}(E, m) = \bot$.

The statement is that if $h : \Sigma^n \to \Sigma^m$ is a linear transformation given by $R = \{r_{ij}\}_{m \times n}$ picked at random from $\{0, 1\}^{m \times n}$, where $r_{ij} \in \{0, 1\}$, and $h(x) \mapsto \langle (\sum_j r_{ij} \wedge x_j) \mod 2 \rangle_{1 \leq i \leq m}$, then we have the following :

LEMMA 3.4. *For each* $i \leq n$ *and* $x, y \in \Sigma^n, x \neq y$, $\Pr[h(x)_i = h(y)_i] = \frac{1}{2}$

LEMMA 3.5. *For distinct* $x, y \in \Sigma^n$, $\Pr[h(x) = h(y)] = 2^{-m}$

LEMMA 3.6. *Let* $A \subseteq \Sigma^n, |A| = k, m = 1 + \lceil \lg k \rceil$, *then*

$$\forall x \in \Sigma^n \; \Pr[\exists y \in A \; : x \neq y \wedge h(x) = h(y)] \leq k.2^{-m}$$

LEMMA 3.7. *Let* H *be a collection of* m *randomly selected functions* h *as above, then*

$$\Pr[\forall h \in H \; \exists y \in A \; : \; (y \neq x \wedge h(x) \neq h(y))] \leq 2^{-m}$$

LEMMA 3.8.

$$\Pr[\exists x \in A \; : \; \forall h \in H \; : \; \exists y \in A \; : y \neq x \wedge h(x) = h(y)] \leq \frac{1}{2}$$

Let $A, B \subseteq \Sigma^n$ and $x \in \Sigma^n$.
We say that h separates x within A if $\forall y \in A, y \neq x \; h(x) \neq h(y)$.
We say that h separates B within A if it separates each $x \in B$ within A.
H separates B within A if for each $x \in B$ some $h \in H$ separates x within A.

LEMMA 3.9 (Coding Lemma). $A \subseteq \Sigma^n$, $k = |A|$ *and* $m = 1 + \lceil \lg k \rceil$. *If* H *is a collection of* m *randomly chosen linear transformations* $h \; : \; \Sigma^n \to \Sigma^m$ *then*

$$\Pr[H \textit{ separates } A \textit{ within } A] \geq \frac{1}{2}$$

For the above setting we see that as the probability is nonzero such a setting will exist. However if $|A| \geq m2^m$, then as each function cannot work for more than 2^m x's if there are more that $m2^m$ x's then the probability falls off to zero. Thus the result of 3.3 follows, since the middle existential quantifier is ranging over a polynomial sized set and can be removed and then the universal quantifiers are merged together. Thus we have a Σ_2^p predicate which is the claim.

THEOREM 3.10. **HN** $\in$ AM

Proof : We first show that **HN** $\in \Pi_2^P$.
Consider the Π_2^P-predicate $\neg$Hash(E, m), which has the form

$$\forall f_1, \cdots, f_m \; C(f_1, \cdots, f_m)$$

$$\text{where } C(f_1, \cdots, f_m) \equiv \exists x, x_1, \cdots, x_m \in E \bigwedge_{1 \le i \le m} \Big((f_i(x) = f_i(x_i)) \wedge x \ne x_i \Big)$$

Now as before $f_i : \{0,1\}^k \to \{0,1\}^m$ is a linear transformation.

We apply the result to the set $E = R_S(x_0)$, the membership of $x, x_1, \cdots, x_m \in E$ can be coded as a Σ_1^P predicate. Now when these existential quantifiers are merged with those in the Π_2^P predicate for the above predicate we have the result that the satisfaction of the $\neg$Hash(E, m) is equivalent to the satisfiability of S, if $A \le 2^{m-2} \le m2^m \le B$.

Now let m be the integer which satisfies $A \le 2^{m-2} < 2A$, as $m < \lg A + 3$, $m2^m \le B$ is satisfied, if B is as chosen in the main theorem. So **HN** $\in \Pi_2^P$.

From the lemma given above, we see that if $|E| \le 2^{m-2}$ and the functions are chosen at random by selecting the entries of the matrices at random, the probability of a collision $(C(f_1, \cdots, f_m) = \top)$ is at most $\frac{1}{2}$. So the randomized algorithm fails with probability at most $\frac{1}{2}$ for unsatisfiable systems and the algorithm always gives the correct answer if the system was satisfiable. This shows that **HN** $\in$ AM. □

3.2. Proof of the main Theorem.

We have to prove some preliminary results before we can prove the main theorem.

DEFINITION 3.11. Let $P = \sum_{0 \le k \le d} a_k x^k \in \mathbb{Z}[x]$, the norm of the polynomial is $\|P\| = \sqrt{\sum_{0 \le k \le d} a_k^2}$.

We have the following effective version of the primitive element theorem.

THEOREM 3.12. *Let α_1 and α_2 be roots of two squarefree polynomials $P_1, P_2 \in \mathbb{Z}[x]$, of degree d_1 and d_2 and maximum norm N. Let $d = \max\{d_1, d_2\}$. There exists a squarefree polynomial $R \in \mathbb{Z}[x]$ of degree at most $d_1 d_2$ and a root β of R called a primitive element, such that $\alpha_i = Q_i(\beta)/a_i, (i = 1, 2)$ where $Q_i \in \mathbb{Z}[x]$ and $a_i \in \mathbb{Z}$, $|a_i| \le cN^{2d}$. Where c is a universal constant,* $\deg Q_i < d_1 d_2$ *and* $N(R) \le cN^{2d}$.

We have a straightforward generalization of the above theorem to many polynomials as follows.

LEMMA 3.13. *Let $\alpha_1, \cdots, \alpha_n$ be roots of n squarefree polynomials $P_1, \cdots, P_n \in \mathbb{Z}[x]$ of degree $2 \le d_i \le d$, and norm $N(P - i) \le N$. There is a squarefree polynomial $R_n \in \mathbb{Z}[x]$ of degree at most d^n and a root β_n of R_n such that $\alpha_i = \frac{Q_{in}(\beta_n)}{\alpha_{in}}$, where $Q_{in} \in \mathbb{Z}[x]$ and $a_{in} \in \mathbb{Z}, |a_{in}| = N^{d^{O(n^2)}}$,* $\deg Q_{in} < d^{\sum_{1 \le i \le n} i}$ *and*

$$\|R_n\| \le c' N^{2^{n-1} d^{\frac{n(n-1)}{2}}}, \; c' \textit{ is a universal constant.}$$

THEOREM 3.14. *Let $x_1, \cdots, x_n$ be n algebraic numbers which are roots of polynomials $A_i \in \mathbb{Z}[x]$ of degree at most d with coefficients of size at most L. There is a primitive element r for $x_1, \cdots, x_n$ which is a root of an irreducible polynomial $B \in \mathbb{Z}[x]$ of degree at most d^n. The coefficients of B are of size at most $L.d^{n^{O(1)}}$. Further, each x_i can be represented as $x_i = Q_i(r)/a_i$ where $Q_i \in \mathbb{Z}[x]$ and* $\lg |a_i| = Ld^{n^{O(1)}}$.

Proof : The primitive element is obtained as follows :

1. Let A_i' be the derivative of A_i. A_i is made squarefree by computing $P_i = \frac{A_i}{\gcd(A_i, A_i')}$.
2. Applying the 3.13 to $P_1, \cdots, P_n$, this gives a_i, Q_i and a polynomial $R \in \mathbb{Z}[x]$.
3. The primitive element r is a root of R. So B is an irreducible factor of R.

The bounds on the coefficients follow from the results of Mignotte. □

Now we consider solutions modulo p, for the system of equations S.

3.2.1. *Unsatisfiable Systems.* If the system we unsatifiable then S has no common zeros in $\mathbb{C}$ so by the Nullstellensatz we can write for some $a \neq 0 \ \in \mathbb{Z}, g_i \in \mathbb{Z}[x_1, \cdots, x_n]$

$$a = g_1 f_1 + \cdots + g_s f_s. \tag{1}$$

We need a bound on the size of a which can be obtained if we have a bound on the degrees D_i of the g_i's. We showed earlier that we can take $D_i = \max\{3, d\}^n$. Given the bound on the the degrees we have to find the coefficients by comparison in the above identity. The linear system contains as many variables as monomials of degree at most $\max\{3, d\}^n$, and a is the determinant of a maximal minor of the system matrix. This leads to an exponential number of coefficients in the dense representation sd^{n^2} of binary size $d^{O(n^2)}L^{O(1)}$, thus the determinant value is upper bounded by $s^{O(1)}d^{O(n^2)}L^{O(1)}$. It turns out that we can get a better upper bound on the size of a, as from [**Kri96**] we have $\lg|a| \leq d^{O(n)}s(\lg s + L)$.

THEOREM 3.15. *If the system S has no common zero in $\mathbb{C}$, then R_S is finite and $|R_S| \leq d^{O(n)}s(\lg s + L)$.*

Proof : If S has no solution in $\mathbb{C}$ then **(1)** holds in $\mathbb{C}$ and hence also in $\mathbb{Z}_p$. So S has no solution in $\mathbb{Z}_p$ if $a \mod p \neq 0$. The result follows as a cannot have more than $\lg a$ prime factors, and the above bound on the size of a. □

3.2.2. *Satisfiable Systems.* We have to show that if the system is satisfiable, then it has algebraic solutions which have small enough descriptions. First we require a quantifier elimination result.

THEOREM 3.16 (Fichtas, Galligo). *Let Φ be a prenex formula in the first-order theory of $\mathbb{C}$. Let r be the number of quantifier blocks, n the total number of variables, and $\sigma(\Phi)$ the total degree of Φ, defined as :*

$$\sigma(\Phi) = 2 + \sum_{1 \leq i \leq s} \deg F_i$$

where $F_1, \cdots, F_s$ are the polynomials occuring in Φ. Φ is equivalent to a quantifier-free formula Ψ in which all polynomials have degree at most

$$2^{n^{O(r)}(\lg \sigma(\Phi))^{O(1)}}.$$

The number of polynomials occuring in Ψ is $O(\sigma(\Phi)^{n^{O(r)}})$. Further if the coefficients in the polynomials of Φ are integers of size at most L, the constants in Ψ are integers of size at most $L2^{n^{O(r)}(\lg \sigma(\Phi))^{O(1)}}$.

THEOREM 3.17. *There are absolute constants c_1 and c_2 such that if S has a solution over $\mathbb{C}$, then there is a solution $x = (x_1, \cdots, x_n)$ such that each x_i is a root of a polynomial of degree at most $2^{(n \lg \sigma)^{c_1}}$ with coefficients of size at most $L2^{(n \lg \sigma)^{c_2}}$.*

We first show a special case of the above.

LEMMA 3.18. *3.17 Holds for the case where $\mathbf{Z}(S)$ is finite.*

Proof : Let T be the solution set of S, and $T_i \subseteq \mathbb{C}$ be the projection of T onto the i-th coordinate axis. By 3.16, S_i can be defined by a quantifier-free formula in which polynomials $P_{i1}, \cdots, P_{im_i}$ of degree at most $2^{(n \lg \sigma)^{c'_1}}$ and coefficients of size at most $L2^{(n \lg \sigma)^{c'_2}}$. If T is finite then each S_i is also finite. Hence each element of S_i is a root of some P_{ij}. The result follows as the components of any solution $x \in T$ must be in one of $T_1, \cdots, T_n$. □

Proof :3.17 The proof is by induction on n. The constants will satisfy $c_1 = c'_1$ and $c_2 \geq c'_2$.
If S has finitely many solutions then the result holds by above lemma.
Now if S has infinitely many solutions. Then at least one of the T_i must be infinite. Thus $\mathbb{C} - T_i$ is finite, since the variety on the i-th axis is defined by the vanishing of polynomials which can exclude only finitely many points if it is infinite. As its elements are among the roots of $m_i = \sigma^{n^{O(1)}}$ polynomials of degree at most $2^{(n \lg \sigma)^{c_1}}$. So we have $|\mathbb{C} - T_i| \leq 2^{(n \lg \sigma)^{c_3}}$ for some absolute constant c_3.
This implies that there is an integer $\alpha \in T_i$, with $0 \leq \alpha \leq 2^{(n \lg \sigma)^{c_3}}$, by a similar analysis as in the case of the unsatisfiable system. As α is polynomial in size, this integer can be substituted for x_i in the system, to obtain an new satisfiable sytem in $n - 1$ variables, where the polynomials are of degree at most d, and have coefficients of size at most $L + d \lg \alpha \leq L + d(n \lg \sigma)^{c_3}$.

By induction hypothesis this system has a solution whose components are roots of polynomials of degree at most $2^{((n-1)\lg\sigma)^{c_1}}$.
They have coefficients of size bounded by

$$B = \left(L + d(n\lg\sigma)^{c_3}\right)2^{((n-1)\lg\sigma)^{c_2}}.$$

To complete the proof we have to show that $B \leq L2^{(n\lg\sigma)^{c_2}}$. If we assume that L and $d(n\lg\sigma)^{c_3}$ are bigger than 2, we have :

$$B \leq L2^{((n-1)\lg\sigma)^{c_2}+\lg(d(n\lg\sigma)^{c_3})}$$

Now as $d \leq \sigma$, it suffices to show

$$(n\lg\sigma)^{c_2} - ((n-1)\lg\sigma)^{c_2} \geq \lg\sigma + c_3\lg(n\lg\sigma)$$

Which holds if we chose c_2 large enough. □

LEMMA 3.19. *Let* $x = (x_1, \cdots, x_n)$ *be a vector of algebraic numbers which are a solution of* S. *Let* r *be a primitive element for* $x_1, \cdots, x_n$ *there exists polynomials* $Q_1, \cdots, Q_n \in \mathbb{Z}[x]$ *and* $a \in \mathbb{N}$ *such that* $x_i = Q_i(r)/a$. *Let* $R \in \mathbb{Z}[x]$ *be an irreducible polynomial such that* $R(r) = 0$. *If* R *has a root in* $\mathbb{Z}_p$ *and* $a \mod p \neq 0$, *then* S *is satisfiable in* $\mathbb{Z}_p$.

Proof : For $i \in \{1, \cdots, s\}$, let

$$g_i(x) = a^{d_i}f_i\left(\frac{Q_1(x)}{a}, \cdots, \frac{Q_n(x)}{a}\right), g_i \in \mathbb{Z}[x] \tag{2}$$

These polynomials must be multiples of R as R is irreducible and $g_i(r) = 0$. So there are polynomials $A_1, \cdots, A_2 \in \mathbb{Z}[x]$ such that

$$g_i(x) = R(x)A_i(x) \tag{3}$$

If $a \mod p \neq 0$ then **(2), (3)** must hold in $\mathbb{Z}_p$. Thus x_0 is a root of R in $\mathbb{Z}_p$, $(\frac{Q_1(x_0)}{a}, \cdots, \frac{Q_n(x_0)}{a})$ is a solution of S in $\mathbb{Z}_p$. □

Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree n, and let $\Delta = \prod_{i\neq j}(x_i - x_j)^2$, (where x_i are the roots of the polynomial) be the discriminant of f. For a prime p

$$W(p) = |\{f : 0 \leq k \leq p-1 \ f(k) \equiv_p 0\}|$$

denotes the number of roots of f in $\mathbb{Z}_p$. Let $S(x) = \sum'_{p\leq x}(1 - W(p))$, where the summation $\sum'$ is over primes p which do not divide Δ.
The following theorem depends on the Generalized Riemann Hypothesis.

THEOREM 3.20.

$$|S(x)| = O(x^{\frac{1}{2}}\lg(\Delta x^n))$$

COROLLARY 3.21. *There is an absolute constant* c *such that*

$$\pi_f(x) \geq \frac{1}{n}\left(\pi(x) - \lg\Delta - cx^{1/2}\lg(\Delta x^n)\right).$$

THEOREM 3.22. *There are absolute constants* c_4, c_5, c_6 *such that if* S *is satisfiable,*

$$\pi_S(x) \geq \frac{\pi(x) - c_6nx^{\frac{1}{2}}\lg x}{L2^{(n\lg\sigma)^{c_4}}} - L2^{(n\lg\sigma)^{c_5}}x^{\frac{1}{2}}$$

Proof : We need explicit estimates on a and the Q_i's to apply 3.19. The algebraic numbers $x_1, \cdots, x_n$ are roots of polynomials $P_1, \cdots, P_n$ whose degree and coefficient size can be bounded using 3.17. The primitive element r's complexity can be estimated using 3.14. The number of primes p in $\pi_R(x)$ can now be estimated using 3.21, and that the discriminant of a polynomial is polynomially bounded in its degree and the bit size of its coefficients. From this estimate we have to subtract the prime factors of a of which there are at most

$\lg a$. □

Now it is straightforward to prove the main theorem.

CHAPTER 3

Polynomial Ideal Membership

1. Introduction

In this chapter we will explore the complexity of a generalization of the Nullstellensatz. We showed that determining whether 1 was an element of a polynomial ideal is equivalent to determining whether the system of polynomials had no solutions. Here we will be concerned with the following problem :

Problem : Polynomial Ideal Membership (**PIM**).
Input : $f, f_1, \cdots, f_k \in \mathbb{F}[x_1, \cdots, x_n]$.
Question : $f \in \langle f_1, \cdots, f_k \rangle$.

It turns out that the above problem is EXPSPACE-complete when $f, f_1, \cdots, f_k \in \mathbb{Q}[x_1, \cdots, x_n]$. We will however concentrate on showing that the general problem is EXPSPACE hard. The results are from Mayr, Meyer [**MM82**].

2. Background

The proof shows that a problem called the *word problem for commutative semigroups* is EXPSPACE-complete and then shows a reduction from this problem to **PIM**.

We begin with a few elementary definitions.

Definition 2.1 (Semi-Thue system). Let Σ be a finite alphabet set, and Σ^* be the set of all finite words on this alphabet. A *Semi-Thue system* over Σ is a finite set $P \equiv \{l_i \to r_i \mid 1 \leq i \leq n \ : \ l_i, r_i \in \Sigma^*\}$. The elements of this set are called productions.

Definition 2.2. Let P be a semi-Thue system over Σ^*, we define a relation $\underset{P}{\longrightarrow}$ on Σ^* as follows:

$$\alpha \underset{P}{\longrightarrow} \beta \ \Leftrightarrow \ \exists \gamma, \delta \in \Sigma^*, l_i \to r_i \in P \ : \ (\alpha = \gamma l_i \delta \wedge \beta = \gamma r_i \delta).$$

Let $\overset{*}{\underset{P}{\longrightarrow}}$ be the reflexive transitive closure of the above relation.
A sequence $(\alpha_0, \cdots, \alpha_n)$ of words $\alpha_i \in \Sigma^*$ with $\alpha_i \underset{P}{\longrightarrow} \alpha_{i+i}$ for $0 \leq i \leq n-1$ is called a *derivation* of *length* n of α_n from α_0.

Definition 2.3 (Thue System). A *semigroup presentation* or *Thue System* is a semi-Thue system P which satisfies $(l \to r) \in P \Rightarrow (r \to l) \in P$.

If P is a Thue system then the relation on Σ^* defined by

$$\alpha \equiv_P \beta \Leftrightarrow \alpha \overset{*}{\underset{P}{\longrightarrow}} \beta$$

then becomes an equivalence relation on Σ^*.
We say that a semi-Thue system P is *commutative* if $\forall s, s' \in \Sigma \ : \ (ss' \longrightarrow s's \in P)$. If it is understood that the system is commutative these relations are not included in the set of productions.
We define a function $\Phi \ : \ \Sigma^* \times \Sigma \to \mathbb{N}$ is a mapping with $\Phi(\alpha, s) =$ The number of occurrences of s in α.
So we have the following natural problem for Commutative Semigroups.

Problem : Word Problem for Commutative Semigroups (**CSG**).
Input : P a commutative semigroup presentation over Σ, $\alpha, \beta \in \Sigma^*$.

Question : $\alpha \equiv_P \beta$.

3. Relation between CSG and PIM

Let $X = \{x_1, \cdots, x_v\}$ and $\mathbb{Q}[X] = \mathbb{Q}[x_1, \cdots, x_v]$.
Let $P = \{\alpha_i \equiv \beta_i \mid 1 \leq i \leq w\}$, be a finite commutative semigroup presentation, with $\alpha_i, \beta_i \in X^*$, $1 \leq i \leq w$.
We identitfy any $\alpha \in X^*$ with the monomial $\alpha = x_1^{\Phi(\alpha,x_1)} \cdots x_v^{\Phi(\alpha,x_v)}$.
Let $I_R[P] = \langle \beta_1 - \alpha_1, \cdots, \beta_w - \alpha_w \rangle$. R is either $\mathbb{Q}$ or $\mathbb{Z}$.

LEMMA 3.1. *If $\alpha \equiv_P \beta$ then $\beta - \alpha \in I_{\mathbb{Z}}[P]$.*

Proof : Suppose $\alpha = \gamma_0 \xrightarrow[P]{} \cdots \xrightarrow[P]{} \gamma_n = \beta$, let $n \geq 1$ without loss of generality.
Then for $1 \leq m \leq n$ there are $\delta_m \in X^*, i_m \in \{1, \cdots, w\}$, such that

$$\gamma_{m-1} = \alpha_{i_m}\delta_m$$
$$\gamma_m = \beta_{i_m}\delta_m$$
$$\text{so } \beta - \alpha = \sum_{1 \leq m \leq n} (\beta_{i_m} - \alpha_{i_m})\delta_m \in I_{\mathbb{Z}}[P].$$

□

The converse holds if we consider $I_{\mathbb{Q}}[X]$.

LEMMA 3.2. *If $\beta - \alpha \in I_{\mathbb{Q}}[P]$ then $\alpha \equiv_P \beta$.
In paritcular if $\beta - \alpha = \sum_{1 \leq i \leq w}(\beta_i - \alpha_i)g_i$ for $g_i \in \mathbb{Q}[X]$ there is a derivation $\alpha = \gamma_0 \xrightarrow[P]{} \cdots \xrightarrow[P]{} \gamma_n = \beta$ of β from α in P, such that for $1 \leq j \leq n$*

$$\operatorname{length}(\gamma_j) \leq \max_{1 \leq i \leq w} \deg \beta_i g_i.$$

Proof : Let $d \in \mathbb{N}$, be the least common multiple of all the denominators involved in the rational coefficients of the polynomials (g_i) in the expression for $\beta - \alpha$.

We can assume without loss of generality that $\alpha \neq \beta$.
Now we can expand out the polynomials g_i and repeat terms such that every coefficient in the following expansion is $+1$.

$$d\beta - d\alpha = \sum_{1 \leq m \leq n} (\beta_{i_m} - \alpha_{i_m})g'_m, \text{ for some } n \geq 1.$$

where $g'_m \in \mathbb{Z}[X]$, are all monomials with coefficient $+1$ and $\deg g'_m \leq \deg g_{i_m}$.

As α appears on the left side of the above identity and as it is a monomial, and also $\alpha \neq \beta$ so there should be a term on the right hand side for some $r : 1 \leq r \leq n$ such that $\alpha = \alpha_{i_r} g'_r$. As the coefficient of α is negative it cannot be one of the β_{i_m}'s.

So we have

$$d\beta - (d-1)\alpha - \beta_{i_r} g'_r = \sum_{1 \leq m \leq n, m \neq r} (\beta_{i_m} - \alpha_{i_m})g'_m$$
$$\alpha \xrightarrow[P]{} \beta_{i_r} g'_r$$

If $\beta_{i_r} g'_r = \beta$ we are done otherwise we repeat the argument and by induction on n obtain a derivation

$$\alpha \xrightarrow[P]{} \gamma_1 \xrightarrow[P]{} \cdots \xrightarrow[P]{} \gamma'_n = \beta, \text{ with } n' \leq n.$$

Where each γ_k is of the form $\beta_{i_r} g'_r$ sor some $r \in \{1, \cdots, n\}$. □

Thus we have that **CSG** $\leq_m^{lg}$ **PIM**.

PROPOSITION 3.3 ([**Her26**]). *Let* $X = \{x_1, \cdots, x_v\}, p_1, \cdots, p_w \in \mathbb{Q}[X]$.
Let $d = \max_i \deg p_i$.
If $p \in \langle p_1, \cdots, p_w\rangle$ *there exist* $g_1, \cdots, g_w \in \mathbb{Q}[X]$ *such that*

1. $p = \sum_i g_i p_i$;
2. $\deg g_i \leq \deg p + (wd)^{2^v}$.

REMARK 3.4. Note that we cannot use *Kollár*'s bound here since there we dealt with the case of the membership of a power of the polynomial to the ideal. This made no difference when membership of 1 is concerned, but in this case we need the more general bound.

Using the above results we can derive the following :

LEMMA 3.5. *Let* $\Sigma = \{a_1, \cdots, a_v\}$ *and* $P = \{\alpha_i \equiv \beta_i \mid 1 \leq i \leq w\}$ *be a commutative semigroup presentation over* Σ.
Then for $\alpha, \beta \in \Sigma^*$, $\alpha \equiv_P \beta$ *iff there is a derivation* $\alpha = \gamma_0 \xrightarrow[P]{} \gamma_1 \xrightarrow[P]{} \cdots \xrightarrow[P]{} \gamma_n = \beta$ *of* β *from* α *such that*

$$\text{length}(\gamma_i) \leq 2^{2^{c\text{size}(\alpha,\beta,P)}}, \textit{ for } 0 \leq i \leq n$$

where $c > 0$ *is a universal constant independent of* $\alpha, \beta,$ *and* P, *and* $\text{size}(\alpha, \beta, P)$ *is the length of a resonable encoding of the objects.*

Proof : Clearly $\deg(\beta - \alpha)$ and $\deg(\beta_i - \alpha_i)$ are all bounded by $2^{\text{size}(\alpha,\beta,P)}$. Further w the number of generators are bounded above by $2^{\text{size}(\alpha,\beta,P)}$. Thus the upper bound follows from the above bound. □

THEOREM 3.6. *There is a deterministic Turing Machine* M *and a constant* $d > 0$, *such that for any instance* (α, β, P), M *decides whether* $\alpha \equiv_P \beta$ *using space at most* $2^{d\ \text{size}(\alpha,\beta,P)}$.

4. Bounded Counter Machines

DEFINITION 4.1. A 3-counter machine C is a 4-tupe (Q, q_0, q_a, δ), where

1. Q is a finite set of states.
2. $q_0, q_a \in Q$.
3. $\delta : (Q - \{q_a\}) \to (Q \times \{0, \pm 1\} \times \{1, 2, 3\}) \cup (Q \times Q \times \{1, 2, 3\})$.

The *computation* of C is given by the sequence $c^0, c^1, \cdots$ of *instantaneous descriptions* $c^i \in Q \times \mathbb{Z}^3$ where

1. $c^0 = (q_0, 0, 0, 0)$ all the three registers start with zero value and the machine starts in state q_0.
2. If $i \in \mathbb{N}, c^i = (q, z_1, z_2, z_3)$ with $q \neq q_a$ and
   (a) $\delta(q) = (q', d, k) \in Q \times \{0, \pm 1\} \times \{1, 2, 3\}$, then
   $$c^{i+1} = (q', z_1', z_2', z_3'),$$
   $$\text{where } z_i' = \begin{cases} z_i + d & \text{if } i = k \\ z_i & \text{otherwise.} \end{cases}$$
   The last component of the instruction gives the address of the register to be changed.
   (b) $\delta(q) = (q', q'', k) \in Q \times Q \times \{1, 2, 3\}$ this is a branch instruction then
   $$c^{i+1} = \begin{cases} (q', z_1, z_2, z_3) & \text{if } z_k = 0. \\ (q'', z_1, z_2, z_3) & \text{otherwise.} \end{cases}$$

c^i_{1+k} is the component which stores the value in the kth counter after i steps for $1 \leq k \leq 3$.

We say that C *terminates with empty counters* iff there is a computation of C which contains the 4-tuple $(q_a, 0, 0, 0)$. We shall simply refer to this as *termination.*
We define the *size* of C to be $|Q|$. The computation of a 3-counter machine C is said to be *bounded* by $n \in \mathbb{N}$ iff the contents of all three counters c^i_{1+k} satisfy $0 \leq c^i_{1+k} \leq n$ for every computation step i.
We have the following result from [**FMR68**].

LEMMA 4.2. *The language*

$$\mathbf{ESC} \equiv_{\mathrm{def}} \{C \mid C \textit{ is a terminating 3-counter machine whose computation is bounded by } 2^{2^{\mathrm{size}(C)}}\}.$$

is EXPSPACE-*complete under* log-*space reductions.*

5. Reduction of ESC to CSG.

Now from a given 3-counter machine C, we construct a commutative semigroup presentation of size $O(\mathrm{size}(C))$ such that **ESC** reduces to **CSG**.

As a first approximation we construct a finitely presented commutative semigroup to which **ESC** reduces but which is too large to be a log-space reduction. Then we will show how this presentation can be embedded in a more succinct one giving us the desired result.

Let $e_n = 2^{2^n}$. Consider the representation of a configuration of C, say $c = (q, z_1, z_2, z_3)$ by a word of the form $qh_1^{z_1}h_2^{z_2}h_3^{z_3}$, where h_i are distinct symbols from some alphabet. The representation is fine as long as we do not have to deal with the *branch on zero* instruction. However since the register sizes are bounded we can use new symbols which model the value stored in the register and the unused amount left i.e $e_n - z_k$ simultaneously so that we can branch if the other hits the maximum value. We are not able to use other representations such as $qh_1^{z_1+1}h_2^{z_2+1}h_3^{z_3+1}$ since we cannot check for the presence of exactly one symbol in the underlying problem.

Now let $n = \mathrm{size}(C)$.
Now the commutative semigroup presentation P'_C over an alphabet set

$$\overline{Q} = Q \,\dot{\cup}\, \{g_1, h_1, g_2, h_2, g_3, h_3\}$$

We encode the configuration (q, z_1, z_2, z_3) of $C = (Q, \delta)$ into the word in $\overline{Q}^*$ by setting $w(q, z_1, z_2, z_3) = qg_1^{e_n - z_1}h_1^{z_1}g_2^{e_n - z_2}h_2^{z_2}g_3^{e_n - z_3}h_3^{z_3}$.

Now the equivalences in P'_C are defined as the following :
For every $q \in Q, \delta(q) = (q', d, k) \in Q \times \{0, +1, -1\} \times \{1, 2, 3\}$.

(A) $q \equiv q'$ if $d = 0$

(B) $qg_k \equiv q'h_k$ if $d = 1$

(C) $qh_k \equiv q'g_k$ if $d = -1$

For every $q \in Q, \delta(q) = (q', q'', k) \in Q \times Q \times \{1, 2, 3\}$.

(D) $qh_k \equiv q''h_k$ Counter is not zero

(E) $qg_k^{e_n} \equiv q'g_k^{e_n}$ Counter is zero

Let $W = \{w(q, z_1, z_2, z_3) \mid q \in Q, 0 \le z_1, z_2, z_3 \le e_n\}$. Now by definition we have that $\Phi(\alpha, g_k) + \Phi(\alpha, h_k) = e_n$. Further if $\beta \equiv_{P'_C} \alpha$, we can easily show using induction in the length of derivation of $\beta \in W$ that $\Phi(\beta, g_k) + \Phi(\beta, h_k) = e_n$.
Now we can see that if $C \in \mathbf{ESC}$ then $w(q_0, 0, 0, 0) \equiv_{P'_C} w(q_a, 0, 0, 0)$ as the computation of C is simulated step-wise by the corresponding derivation in the commutative semigroup presentation starting from $w(q_0, 0, 0, 0)$. The converse can also be proved using techniques from [**Po47**] that the reverse implication also holds.
Hence we can conclude the following:

LEMMA 5.1. $w(q_0, 0, 0, 0) \equiv_{P'_C} w(q_a, 0, 0, 0) \Leftrightarrow C \in \mathbf{ESC}$.

Now from the above we see that the only problem arises when we consider branch instructions since their encoding results in space usage which is exponential (to output the degree). To tackle this case we need to implicitize the representation of the high degrees encoding them into smaller words. In what follows for

$n \in \mathbb{N}$ we construct a commutative semigroup P_n of size $O(n)$ containing generators S, F and B such that FB^{e_n} is the only word containing F that is derivable from S in P_n.

We define both the presentation P_n and G_n the generator set by induction. We will actually use $B_1, \cdots, B_4$ to represent the single symbol B the reason for which will become clear as we proceed.

$$\text{Let } G_0 \equiv_{def} \{s, f, c_1, c_2, c_3, c_4, b_1, b_2, b_3, b_4\}$$
$$P_0 \equiv_{def} \{sc_i \equiv fc_i b_i^2 \mid 1 \le i \le 4\}.$$

For $m > 0$ let $\{S, Q_1, Q_2, Q_3, Q_4, F, C_1, C_2, C_3, C_4, B_1, B_2, B_3, B_4\}$ be distinct symbols not in G_{m-1}. We define

$$G_m \equiv_{def} G_{m-1} \dot{\cup} \{S, Q_1, Q_2, Q_3, Q_4, F, C_1, C_2, C_3, C_4, B_1, B_2, B_3, B_4\}$$

We call the elements of G_0 as *level* 0 elements and, for $m > 0$ the elements of $G_m - G_{m-1}$ as elements of *level* m. In what follows we shall use upper case letters $S, \cdots, B_4$ to represent elements at level $n (> 0)$, and the lower case letters $s, \cdots, b_4$ to represent the generators at level $n - 1$.
Let

(a) $$S \equiv Q_1 s c_1$$
(b) $$Q_1 f c_1 b_1 \equiv Q_2 s c_2$$
(c) $$Q_2 f c_2 \equiv Q_3 f c_3$$
(d) $$Q_3 s c_3 b_1 \equiv Q_2 s c_2 b_4$$
(e) $$Q_3 s c_3 \equiv Q_4 f c_4 b_4$$
(f) $$Q_4 s c_4 \equiv F$$
(G) $$Q_2 C_i f b_2 \equiv Q_2 C_i B_i f b_3 \text{ for } 1 \le i \le 4.$$

LEMMA 5.2. *Let* S, F, C_i, B_i *be of level* n. *Then*

$$SC_i \equiv_{P_n} FC_i B_i^{e_n} \textit{ for } 1 \le i \le 4.$$

Proof : The proof is by induction on n.
For $n = 0$, P_0 contains exactly the claimed equivalences.
For $n > 0$ we have for $1 \le i \le 4$

$$\begin{aligned}
SC_i &\equiv C_i Q_1 s c_1 && \text{by (a)}\\
&\equiv C_i Q_1 f c_1 b_1^{e_{n-1}} && \text{by Induction Hypothesis}\\
&\equiv C_i b_1^{e_{n-1}-1} Q_2 s c_2 && \text{by (b)}\\
&\equiv C_i b_1^{e_{n-1}-1} Q_2 f c_2 b_2^{e_{n-1}} && \text{by Induction Hypothesis}\\
&\equiv C_i b_1^{e_{n-1}-1} Q_2 f c_2 b_3^{e_{n-1}} B_i^{e_{n-1}} && \text{by (G)}\\
&\equiv C_i B_i^{e_{n-1}} b_1^{e_{n-1}-1} Q_3 f c_3 b_3^{e_{n-1}} && \text{by (c)}\\
&\equiv C_i B_i^{e_{n-1}} b_1^{e_{n-1}-1} Q_3 s c_3 && \text{by Induction Hypothesis}\\
&\equiv C_i B_i^{e_{n-1}} b_1^{e_{n-1}-2} b_4 Q_2 s c_2 && \text{by (d)}\\
&\equiv \cdots \equiv C_i B_i^{e_{n-1} \dot{e}_{n-1}} b_4^{e_{n-1}-1} Q_3 s c_3 && \text{By iterating the relevant parts of above argument}\\
&\equiv C_i B_i^{e_n} Q_4 f c_4 b_4^{e_{n-1}} && \text{by (e)}\\
&\equiv C_i B_i^{e_n} Q_4 s c_4 && \text{by Induction Hypothesis}\\
&\equiv FC_i B_i^{e_n} && \text{by (f).}
\end{aligned}$$

□

Let S, C_i be of level n and $\alpha \in G_n^*$ such that $\alpha \equiv_{P_n} SC_i$. We define the *height* $h(\alpha)$ as follows

$$h(\alpha) \equiv_{def} \min\{m \in \mathbb{N} \mid \Phi(\alpha, c_i) > 0 \text{ for some } c_i \text{ of level } m\}.$$

The following lemma can be proved by induction on the length of the derivation.

LEMMA 5.3. *Let* $SC_i = \gamma_0 \rightarrow_{P_n} \gamma_1 \rightarrow_{P_n} \cdots \rightarrow_{P_n} \gamma_r = \alpha$ *be a derivation of* α *in* P_n. *Then*

1.

$$\sum_{1 \leq i \leq 4} \Phi(\alpha, c_i) = 1 \textit{ if } c_1, \cdots, c_4 \textit{ are of level } m \textit{ with } h(\alpha) \leq m \leq n.$$
$$= 0 \textit{ otherwise };$$

2.

$$\sum_{1 \leq i \leq 4} \Phi(\alpha, q_i) = 1 \textit{ if } q_1, \cdots, q_4 \textit{ are of level } m \textit{ with } h(\alpha) < m \leq n.$$
$$= 0 \textit{ otherwise };$$

3.

$$\Phi(\alpha, s) + \Phi(\alpha, f) = 1 \textit{ if } s, f \textit{ are of level } h(\alpha) \qquad = 0 \textit{ otherwise };$$

4.

$$|h(\gamma_i) - h(\gamma_{i-1})| \leq 1 \textit{ for } 1 \leq i \leq r;$$

5. Only the equivalences in $P_{h(\alpha)+1} - P_{h(\alpha)-1}$ *are applicable to* α *(with* $P_{-1} = \phi$*), and the height decreases iff an equivalence in* $P_{h(\alpha)}$ *is applied.*

We can then show the important lemma:

LEMMA 5.4. *Let* S, F, C_i, B_i *be of level* n*, and let* $\alpha \in FG_n^*$. *If* $SC_i \equiv_{P_n} \alpha$ *and* α *contains an occurrence of* S *or* F*, then either* $\alpha = SC_i$ *or* $\alpha = FC_iB_i^{e_n}$.

Now given a 3-counter machine $C = (Q, \delta)$ of size n, we construct the commutative semigroup presentation P_C as follows:
We can assume that the equivalences $(A) - (D)$ of P'_C are over a disjoint alphabet from the alphabet G_n of P_n except that $g_k = b_k$ for $1 \leq k \leq 3$. Then P_C is defined to contain all the equivalences in P_n and P'_C now we replace every equivalence of the form $qg_k^{e_n} \equiv q'g_k^{e_n}$ by the following new equivalences. Let $q_r, q_e \notin \overline{Q} \cup G_n$ be two new symbols. Then the replacement equivalences instead of the one above are :

(k)	$q \equiv q_rFC_k$
(l)	$q_rSC_k \equiv q_eSC_k$
(m)	$q_eFC_k \equiv q'$
(n)	$q_{01} \equiv q_{02}SC_1$
(o)	$q_{02}FC_1 \equiv q_{03}SC_2$
(p)	$q_{03}FC_2 \equiv q_{04}SC_3$
(q)	$q_{04}FC_3 \equiv q_0$
(r)	$q_a \equiv q_{a4}FC_3$
(s)	$q_{a4}SC_3 \equiv q_{a3}FC_2$
(t)	$q_{a3}SC_2 \equiv q_{a2}FC_1$
(u)	$q_{a2}SC_1 \equiv q_{a1}$

This completes the description of P_C.
Note that intuitively we reduce $w(q_a, 0, 0, 0)$ to q_{a1} and $w(q_0, 0, 0, 0)$ to q_{01} using these series of checks that every one of the register has hit the maximum value.
Now if $W = \{w(q, z_1, z_2, z_3) \mid q \in Q, 0 \leq z_1, z_2, z_3 \leq e_n\}$. Let $\mathcal{W}$ be the subset of the commutative semigroup presented by P'_C which is given by words in W. We can then show that:

LEMMA 5.5. *There is a semigroup homomorphism from the commutative semigroup presented by* P'_{C} *into the one presented by* P_{C} *which is injective on* $\mathcal{W}$.

The proof proceeds by showing that the natural map taking g_{k} to B_{k} and the indentity mapping on $\overline{\mathsf{Q}}$ has the desired property.
As a result of the above lemma we have:

LEMMA 5.6. *Let* C *be a* 3*-counter machine and* P_{C} *the finite commutative semigroup presentation constructed above. Then*

$$\mathsf{C} \in \mathbf{ESC} \Leftrightarrow \mathsf{q}_{01} \equiv_{\mathsf{P}_{\mathsf{C}}} \mathsf{q}_{a1}.$$

THEOREM 5.7. **CSG** *is* EXPSPACE*-complete with respect to* log *space reductions.*

Since we showed that **CSG** reduces to **PIM**, we also have:

COROLLARY 5.8. **PIM** *is* EXPSPACE*-hard.*

CHAPTER 4

Gröbner Bases

In the previous chapter we saw that the ideal membership problem is EXPSPACE-hard. In this chapter we will deal with the problem of solving **PIM**. This effort will yield a very useful solution which not only solves **PIM** but a host of different important problems. We will begin with a description of Gröbner bases which solves the **PIM** and the *Buchberger*'s algorithm which computes the Gröbner basis for an ideal, following which we will consider the problem of finding an upper bound on the resource requirements of the algorithm.

1. Buchberger's Algorithm

Theorem 1.6 suggests a simple algorithm to compute a Gröbner basis for a given polynomial ideal.

Algorithm 1.1 Simple Buchberger Algorithm

```
Input : $I = \langle f_1, \cdots, f_k \rangle \subseteq \mathbb{F}[x_1, \cdots, x_n]$
Output : G a Gröbner basis for I.
Steps :
$G \leftarrow \{f_1, \cdots, f_k\}$
while( $\exists f, g \in G \ : \ \overline{S(f,g)}^G \neq 0$)
 {
 $G \leftarrow G \cup \{\overline{S(f,g)}^G\}$
 }
return(G)
```

Author's Note : More material will be added on improvements and applications of Buchberger's algorithm.

In the following sections we shall investigate the question of bounding the size of the Gröbner basis produced by the above algorithm. The results and the presentation we follow are from [**Dub90**].

2. Cone decompositions of a polynomial ring

Since the Hilbert function contains information which bounds the size of a Gröbner basis. We take as our first task to produce a decomposition of an ideal I into subsets which have a simple Hilbert function.

Let $U \subseteq X = \{x_1, \cdots, x_n\}$.

Definition 2.1. If h is a homogeneous polynomial, we define the cone of h with respect to U as the set

$$C(h, U) \equiv \{ah \mid a \in \mathbb{F}[U]\}$$

The rationale behind this definition is that this set has a particularly simple form of the Hilbert function, which is dependent only on the degree of h and $|U|$.

If $U = \emptyset$ we have

$$\varphi_{C(h,\emptyset)}(z) = \begin{cases} 0, & \text{if } z \neq \deg(h) \\ 1, & \text{if } z = \deg(h) \text{ Only LT } (h) \text{ is present in LT } (C(h,\emptyset))_{(z)}. \end{cases}$$

If $|U| > 0$ then

$$\varphi_{C(h,U)}(z) = \begin{cases} 0, & \text{if } z < \deg(h) \\ \binom{z-\deg(h)+|U|-1}{|U|-1}, & \text{if } z \geq \deg(h). \end{cases}$$

DEFINITION 2.2 (Cone Decomposition). Let $h_1, \cdots, h_r$ be homogeneous polynomials of $\mathcal{A}$, Let $U_1, \cdots, U_r$ be subsets of X. A finite set $P = \{\langle h_1, U_1\rangle, \cdots, \langle h_r, U_r\rangle\}$ is a cone decomposition of $T \subseteq \mathcal{A}$ if

$$T = \bigoplus_{1 \leq i \leq r} C(h_i, U_i).$$

The pairs $\langle h_i, U_i\rangle \in P$ with $U_i = \emptyset$ form a finite part of T which does not contribute to the Hilbert Polynomial of the set T.
The remaining cases for which $U_i \neq \emptyset$ is the portion we are interested in. This part of the decomposition represents a set which at large degrees is equivalent to T. We adopt the following notation for this portion of the decomposition.

$$P^+ = \{\langle h, U\rangle \in P \mid U \neq \emptyset\}$$

Since we are interested in degree bounds on the basis for an ideal we form a notion of the same for cones.

DEFINITION 2.3. A cone decomposition P for T is said to be k-standard ($k \in \mathbb{N}$) if the following two conditions hold:

1. There is no pair $\langle h, U\rangle \in P^+$ with $\deg(h) < k$.
2. $\forall \langle g, V\rangle \in P^+ \ \forall d \ : \ k \leq d \leq \deg(g) \ \exists \ \langle h, U\rangle \in P^+ \ : \ (\deg(h) = d) \wedge (|U| \geq |V|)$.

If $P^+ = \emptyset$ then P is k-standard for every $k \in \mathbb{N}$. If $P^+ \neq \emptyset$, then the only possible value for k is $\min\{\deg(h) \mid \langle h, U\rangle \in P^+\}$.

We have the following properties for cone decompositions and k-standard cone decompositions :

1. $\emptyset$ is a 0-standard cone decomposition for $\emptyset$.
2. $\{\langle h, U\rangle\}$ is a $\deg(h)$-standard decomposition of $C(h, U)$.
3. $\{\langle 1, X\rangle\}$ is a 0-standard decomposition of $\mathcal{A}$.
4. Let $T = S_1 \oplus S_2$ and let P_1, P_2 be cone decompositions of S_1 and S_2 respectively. Then $P_1 \cup P_2$ is a cone decomposition of T. If P_1 and P_2 are k-standard cone decompositions then so is $P_1 \cup P_2$.
5. If $P = \{\langle h_1, U_1\rangle, \cdots, \langle h_s, U_s\rangle\}$ is a k-standard cone decomposition for T, then for any homogeneous polynomial c, the set $P' = \{\langle ch_1, U_1\rangle, \cdots, \langle ch_s, U_s\rangle\}$ is a $(k + \deg(c))$-standard cone decomposition for cT.

DEFINITION 2.4. Let $U = \{x_{j_1}, \cdots, x_{j_m}\} \subseteq X$.

$$E(h, U) \equiv \{\langle h, \emptyset\rangle\} \cup \{\langle x_{j_i} h, \{x_{j_i}, \cdots, x_{j_m}\}\rangle \mid 1 \leq i \leq m\}.$$

$E(h, U)$ is a $(\deg(h) + 1)$-standard decomposition of $C(h, U)$. We make use of this property to prove the following result.

LEMMA 2.5. *Let P be a k-standard cone decomposition for T. For any $d \geq k$, there is a d-standard cone decomposition P_d for T.*

Proof : If $P^+ = \emptyset$, then the result holds trivially.
If $P^+ \neq \emptyset$, then we show that a $(k + 1)$-standard cone decomposition exists for T. The result follows by induction. Let $R = \{\langle h, U\rangle \mid \deg(h) = k\}$ and $S = P - R$. It is clear the S is $(k + 1)$-standard. Now R is k-standard. The set spanned by R has a $(k + 1)$-standard cone decomposition given by

$$R' = \bigcup_{\langle h, U\rangle \in R} E(h, U)$$

Now by the observations preceding the lemma, we have that $R' \cup S$ is a $(k+1)$-standard decomposition of T. □

Corollary 2.6. *Let* $S_1, \cdots, S_r$ *be a direct decomposition of* T, *where for each* S_i *there is a* k_i*-standard cone decomposition* P_i. *Then there is a* k*-standard cone decomposition* P *of* T *with* $k = \max\{k_1, \cdots, k_r\}$.

3. Splitting decompositions

Let $I \subseteq \mathcal{A}$ be an ideal and f a polynomial, a useful operation is to compute the basis for the quotient ideal $I : \langle f \rangle \equiv \{g \in \mathcal{A} \mid fg \in I\}$ [1]. It is clear that in the ideal $I \cap \langle f \rangle$ every polynomial is a multiple of f and also belongs to I (and also every polynomial which is in I and a multiple of f belongs to $I \cap \langle f \rangle$), so dividing out f from its generators we get the generators for the quotient ideal.

We are interested in the case where f is a monomial and in particular when $f = x_i$ where x_i is one of the indeterminates of the polynomial ring, and I is a monomial ideal. The above idea results in the following algorithm. For convenience we write $I : x_i$ instead of $I : \langle x_i \rangle$.

Algorithm 3.1 Algorithm for computing the basis for $I : x_i$

```
Quotient-Basis($F, x_j$)
**Input :** $F$ a monomial basis for $I \subseteq \mathcal{A}$, $x_j \in X$ a variable.
**Output :** $F'$ a monoial basis for $I : x_j$.
**Steps :**
$F' \leftarrow \emptyset$
for ($f_i \in F$)
 {
 if ($f_i \in \mathbb{F}[X - \{x_j\}]$)
   $F' \leftarrow F' \cup \{f_i\}$
 else
   $F' \leftarrow F' \cup \{x_j^{-1} f_i\}$
 }
```

Definition 3.1. Let $P \cup Q$ be a cone decomposition for $T \subseteq \mathcal{A}$, and let $I \subseteq \mathcal{A}$ be an ideal. Then P and Q are said to *split* T *relative to* I, if $\langle h, U \rangle \in P \Rightarrow C(h, U) \subseteq I$ $(h \in I)$, and $\langle h, U \rangle \in Q \Rightarrow C(h, U) \cap I = \{0\}$.

It is clear that in the above case P is a cone decomposition for $T \cap I$. However under some restrictions Q forms a cone decomposition for $T \cap N_I$.

Lemma 3.2. *Let* $P = \{\langle g_1, U_1 \rangle, \cdots, \langle g_r, U_r \rangle\}$, *and* $Q = \{\langle h_1, V_1 \rangle, \cdots, \langle h_s, V_s \rangle\}$ *split* T *relative to a monomial ideal* I, *where for each* $\langle h_i, V_i \rangle \in Q$, h_i *is a monomial. Then* Q *is a cone decomposition for* $T \cap N_I$.

Proof : If I is a monomial ideal, then for a fixed Gröbner basis G, and an admissible ordering we have,

$$f \in N_I \Leftrightarrow (\forall m \in \text{Terms } (f) \; : \; m \notin I)$$

Further if h_i is a monomial then,

$$f \in C(h_i, V_i) \Leftrightarrow (h_i \setminus f) \Leftrightarrow (\forall m \in \text{Terms } (f) \; : \; m \in C(h_i, V_i))$$

Since the above sets for a split of T with respect to I we have $C(h_i, V_i) \cap I = \{0\}$, so

$$f \in C(h_i, V_i) \leftrightarrow (\forall m \in \mathsf{Terms}(f) \; : \; m \notin I).$$

Let $f \in T \cap N_I$, since P and Q are a cone decomposition for T we can write it as

$$f = f_{P_1} + f_{P_2} + \cdots + f_{P_r} + f_{Q_1} + \cdots + f_{Q_s}$$

Now $f_{\overline{P}} = f_{P_1} + f_{P_2} + \cdots + f_{P_r} \in I$ and is a sum of monomials which themselves are in I, since no such monomials can appear in $C(h_i, V_i)$, all the monomials of $f_{\overline{P}}$ also appear in f (i.e., there are no cancellations of these monomials). But $f \in N_I$ and so cannot have any monomial of I. Hence $f_{\overline{P}} = 0$ and f can be written

[1] $0 \in I : \langle f \rangle$, $g, h \in I : \langle f \rangle \Rightarrow hf \in I \Rightarrow \forall p \in \mathcal{A}\; phf \in I \Rightarrow ph \in I : \langle f \rangle$ and finally $fg \in I, fh \in I \Rightarrow (g+h)f \in I \Rightarrow (g+h) \in I : \langle f \rangle$. Actually the definition of the quotient ideal is slightly different, but for the case of a taking quotients with a principal ideal both the definitions coincide.

uniquely as $f = f_{Q_1} + \cdots + f_{Q_s}$. So Q forms a cone decomposition of $T \cap N_I$. □

Now to test whether $C(h, U)$ can belong to a split $P \cup Q$ decomposition of T with respect to I, only if $C(h, U) \subseteq I$ or $C(h, U) \cap I = \emptyset$. We show now that if I is a monomial ideal and h is a monomial then we can test this condition. This provides an algorithm to split $\mathcal{A}$ with respect to a monomial ideal I.

Lemma 3.3. *Let* I *be a monomial ideal,* $h \in PP_{\mathbb{F}}[X]$, $U \subseteq X$, *and let* F *be a power product basis (monic monomials) for* $I : h$. *Then*

1. $C(h, U) \subseteq I \Leftrightarrow (1 \in F)$.
2. $C(h, U) \cap I = \emptyset \Leftrightarrow (F \cap PP_{\mathbb{F}}[U] = \emptyset)$.

Proof :

1. $1 \in F \Leftrightarrow 1 \in I : h \Leftrightarrow h \in I \Leftrightarrow C(h, X) \subseteq I$.
2. $(\Rightarrow)$ If $C(h, U) \cap I = \emptyset$. Then for $g \in PP_{\mathbb{F}}[U]$,

$$\begin{aligned} hg \in C(h, U) &\Rightarrow hg \in I \\ &\Rightarrow g \notin I : h \\ &\Rightarrow g \notin F. \end{aligned}$$

$(\Leftarrow)$ If $F \cap PP_{\mathbb{F}}[U] = \emptyset$. Then for $g \in PP_{\mathbb{F}}[U]$, $g \notin I : h$ since otherwise F would have a divisor of g and this divisor would be in $PP_{\mathbb{F}}[U]$. So $g \notin I : h \Rightarrow hg \notin I$. By the definition of $C(h, U)$, every polynomial contained in the cone is of the form hg with $g \in P_{\mathbb{F}}[U]$ and hence not in I.

□

Algorithm 3.2 The algorithm for splitting $C(h, U)$ relative to a monomial ideal I.

```
Split(h, U, F)
Input :  $h \in PP_{\mathbb{F}}[X]$, $U \subseteq X$ is a set of variables, $F$ a power product basis for $I : h$.
Output :  $(P, Q)$ which splits $C(h, U)$ relative to I.
Steps :
If $(1 \in F)$ then return $(P \leftarrow \{\langle h, U\rangle\}, Q \leftarrow \emptyset)$
If $F \cap PP_{\mathbb{F}}[U] = \emptyset$ then return $(P = \emptyset, Q \leftarrow \{\langle h, U\rangle\})$
else
  {
  Select $S \subseteq U$ a maximal subset such that $F \cap PP_{\mathbb{F}}[S] = \emptyset$.
  Select $x_j \in U - S$ (Algorithm halts before this if $S = U$.)
  $(P_0, Q_0) \leftarrow$ Split$(h, U - \{x_j\}, F)$
  $F' \leftarrow$ Quotient-Basis$(F, x_j)$
  $(P_1, Q_1) \leftarrow$ Split$(x_j h, u, F')$
  return $(P \leftarrow P_0 \cup P_1, Q \leftarrow Q_0 \cup Q_1)$
  }
```

Lemma 3.4. *The algorithm* Split *terminates.*

Proof : For a set of arguments h, U, and F, we define the rank of the arguments as $|U| + \sum_{f \in F} \deg(f)$. We have to show that if Split is invoked with arguments of rank r, then the two recursive calls have rank $\leq (r-1)$.

For the first call it is clear since the variable set decreases in cardinality.

Now for the second call, U remains the same, so we have to show $\sum_{f \in F'} \deg(f)$ decreases. Since F' is a basis for $I : x_j$, now by the operation of the Quotient-Basis algorithm the degree of such a basis decreases if there is a polynomial in $f_i \in F$ but $f \notin PP[X - \{x_j\}]$.

Now suppose every $f_i \in F$ also belonged to $PP[X - \{x_j\}]$ then $F \cap K[S \cup \{x_j\}] = \emptyset$ since all the polynomials do not involve the variable x_j, but this contradicts the choice of S and hence of x_j. □

LEMMA 3.5. *The algorithm* Split *is correct.*

Proof : The correctness of the algorithm can be proved using the depth of the recursion. The basis case follows from 3.3. Otherwise, the cone $C(h, U)$ is decomposed into

$$C(h, U) = C(h, U - \{x_j\}) \oplus C(x_j h, U)$$

As F is a power product basis for $I : h$, the procedure Quotient-Basis produces a power product basis F' for the ideal $I : x_j h$. By inductive hypothesis Split returns

1. (P_0, Q_0), which splits $C(h, U - \{x_j\})$ relative to I, and
2. (P_1, Q_1), which splits $C(x_j h, U)$ relative to I.

The decomposition for $C(h, U)$ is clearly the union of these two componentwise. □

The choice of $S \subseteq U$, such that $F \cap PP_{\mathbb{F}}[S] = \emptyset$ as a maximal subset is not necessary for the correctness of the algorithm, but however this results in the set Q having the property of being $\deg(h)$-standard. In the following we prove this result.

LEMMA 3.6. *Let* h, U, I *and* F *be the arguments for the algorithm* Split. *Then for any* $V \subseteq X$,

$$C(h, V) \subseteq C(h, U) \cap N_I \Leftrightarrow (V \subseteq U) \wedge (F \cap PP_{\mathbb{F}}[V] = \emptyset).$$

Proof : $(\Rightarrow)$ $C(h, V) \subseteq C(h, U)$ implies that $V \subseteq U$. Now we need too show $F \cap PP[V] = \emptyset$. Consider any nonzero element of $\mathbb{F}[V]$. Then $hf \in C(h, V) \subseteq N_I$. But $I \cap N_I = \{0\}$ and neither f not h is zero so $hf \notin I$. Then,

$$\begin{aligned} hf \notin I &\Rightarrow f \notin I : h \\ &\Rightarrow f \notin F. \end{aligned}$$

$(\Leftarrow)$ $V \subseteq U$ implies that $C(h, V) \subseteq C(h, U)$, so we have to show that $C(h, V) \subseteq N_I$. This is the same as showing no monomial of $C(h, V)$ belongs to I. Each monomial of $C(h, V)$ is of the form hf with f a monomial in $\mathbb{F}[V]$. Then

$$\begin{aligned} F \cap PP[V] = \emptyset &\Rightarrow f \notin I : h \\ &\Rightarrow hf \notin I. \end{aligned}$$

□

LEMMA 3.7. *Let* $h, U, I,$ *and* F *be the arguments for* Split, *and let* $(P, Q) \leftarrow \text{Split}(h, U, F)$. *Then for any power product* g, $C(g, V) \subseteq C(h, U) \cap N_I \Rightarrow (\exists \ \langle h, S\rangle \in Q \ : \ |S| \geq |V|)$.

Proof : Using the above lemma

$$\begin{aligned} C(g, V) \subseteq C(h, U) \cap N_I &\Rightarrow C(h, V) \subseteq C(h, U) \cap N_I \\ &\Rightarrow V \subseteq U, F \cap PP[V] = \emptyset \end{aligned}$$

We proceed by induction on $|U| - |V|$. If $U = V$ the algorithm returns $Q = \{\langle h, U\rangle\}$, satisfying the lemma. Otherwise, S is a maximal subset such that $F \cap PP[S] = \emptyset \Rightarrow |S| \geq |V|$, we now apply the previous lemma to get $C(h, S) \subseteq C(h, U - \{x_j\}) \cap N_I$. By inductive hypothesis, Q_0 formed by the recursive call $\text{Split}(h, U - \{x_j\}, F)$ contains a pair $\langle h, W\rangle$ with $|W| \geq |S| \geq |V|$. The lemma follows as $Q_0 \subseteq Q$. □

A basis $F = \{f_1, \cdots, f_k\}$ for an ideal I is *reduced* if each f_i satisfies $f_i \notin \langle F - \{f_i\}\rangle$. It is clear that any basis contains a reduced basis for the same ideal.

LEMMA 3.8. *Let* R *be a reduced power product basis for a monomial ideal* I, *and let* $P = \{\langle h_1, U_1\rangle, \cdots, \langle h_r, U_r\rangle\}$ *be any cone decomposition of* I *where the* h_i*'s are power products. Then* $\forall f \in R \ : \ \exists \langle f, U\rangle \in P$.

Proof : Let $f \in R$ as $f \in I\ \exists \langle h, U \rangle \in P\ :\ f \in C(h, U)$. But $h \in I$, so $h = bg$ for some $g \in R$, so we have $f = ah = abg$, as R is reduced $ab = 1$, so $h = bf$, where b is a unit but since the entries are power products we have $h = f$. □

Lemma 3.9. *Let* F *be a power product basis for* $I \neq \mathbb{F}[x_1, \cdots, x_n]$, $(P, Q) \leftarrow \text{Split}(1, X, F)$, *and let* $R \subseteq F$ *be a reduced basis for* I. *Then* $\forall f \in R\ \exists \langle h, U \rangle \in Q\ :\ \deg(h) = \deg(f) - 1$.

Proof : Let $f \in R$. By the above lemma we have a $\langle f, V \rangle \in P$. Now we consider how this pair entered P by the execution of Split. As $\deg(f) > 0$, we must have had a recursive call to $\text{Split}(f, V, F')$ where F' is a basis for $I : f$. This must have come from either

1. $\text{Split}(x_j^{-1} f, V, F'')$ or
2. $\text{Split}(f, V \cup \{x_j\}, F')$

Tracing backward through the execution using alternative (1) as the basis we can find an invocation of $\text{Split}(x_j^{-1} f, V, F'')$ with $V' \supseteq V$. $C(x_j^{-1} f, V') \nsubseteq I$ as otherwise a recursive call would not have been generated. Thus if $(P', Q') \leftarrow \text{Split}(x_j^{-1} f, V', F'')$ then $Q' \neq \emptyset$ then by 3.7 we have a pair $\langle x_j^{-1} f, S \rangle \in Q'$, as $\deg(x_j^{-1} f) = \deg(f) - 1$ and since $Q' \subseteq Q$ the lemma follows. □

Corollary 3.10. *Let* F *be a power product basis for* I, *and let* $(P, Q) \leftarrow \text{Split}(1, X, F)$. *Then if* $d = 1 + \max\{\deg(h)\ :\ \langle h, U \rangle \in Q\}$. *I can be generated by the set* $\{f \in F \mid \deg(f) \leq d\}$.

We can finally show the following:

Lemma 3.11. *Let* $(P, Q) \leftarrow \text{Split}(h, U, F)$, *then* Q *is a* $\deg(h)$-*standard cone decomposition.*

Proof : If Q is either $\emptyset$ or $\{\langle h, U \rangle\}$ the lemma holds. Otherwise we proceed by induction on the number of recursions and we assume that Q_0, Q_1 satisfy the lemma. Q_0 is $\deg(h)$-standard and Q_1 is $(\deg(h) + 1)$-standard.
To show that Q is $\deg(h)$-standard cone decomposition we have to show

$$\forall \langle g, V \rangle \in Q\ :\ \forall d\ :\ \deg(h) \leq d \leq \deg(g)\ :\ \exists\ \langle p, T \rangle \in Q\ :\ (\deg(p) = d) \wedge |T| \geq |V|.$$

As $Q = Q_0 \cup Q_1$ we have two cases:

1. $\langle g, V \rangle \in Q_0$. As Q_0 itself is $\deg(h)$-standard, Q_0 contains all pairs to satisfy the criterion, and $Q_0 \subseteq Q$.
2. $\langle g, V \rangle \in Q$. As Q_1 is a $(\deg(h) + 1)$-standard cone decomposition, Q_1 contains all the pairs needed to satisfy the criterion for $\langle g, V \rangle$ for $\deg(h) + 1 \leq d \leq \deg(g)$. For $d = \deg(h)$ by 3.7 we have that Q contains such a pair.

□

Theorem 3.12. *Let* G *be a Gröbner basis for* I *with respect to an admissible ordering. Let* $(P, Q) \leftarrow \text{Split}(1, X, \text{LT}\ (G))$. *The* Q *is a* 0-*standard cone decomposition of* N_I *with respect to this Gröbner basis. Further if* $d = 1 + \max\{\deg(h) \mid \langle h, U \rangle \in Q\}$, *then* $G' = \{g \in G\ :\ \deg(g) \leq d\}$ *is also a Gröbner basis for* I.

Proof : $\text{LT}\ (G)$ is a basis for $\text{LT}\ (I)$. Thus the Split algorithm returns a 0-standard cone decomposition for $N_{\text{LT}\ (I)} = N_I$.
By Corollary 3.10 the set $\{h \in \text{LT}\ (G) \mid \deg(h) \leq d\} \subseteq \text{LT}\ (G')$, is also a basis for $\text{LT}\ (I)$ and so G' is a Gröbner basis for I. □

To use this theorem we have to bound the degrees in the cone decomposition. This will be the focus of our attention in the next few sections.

4. Splitting a homogeneous ideal

It turns out that for homogeneous ideals we can find a cone decomposition.

LEMMA 4.1. *For an ideal* $J \subseteq \mathcal{A}$ *and* $h \in \mathcal{A}$, *let*

$$\begin{aligned} I &= \langle J, f\rangle = J + \langle f\rangle \\ L &= J : f \\ S &= \{af \mid a \in N_L\} \end{aligned}$$

then $I = J \oplus S$

Proof : Let G be the Gröbner basis for L used to form N_L and $S = fN_L$. $J \subseteq I, S \subseteq I$, so it suffices to show that every $h \in I$ can be written uniquely as $h = h_J + h_S$. We first show that such a decomposition exists.

Every polynomial $h \in I$ can be written as $h = a_J + a_f f, a_J \in J$ by the definition of the sum of two ideals.

Claim : $h = h_J + h_S$, $h_J = h - \overline{(a_f)}^G f$ and $h_S = \overline{(a_f)}^G f$, is the desired decomposition.

$$\begin{aligned} a_f - \overline{a_f}^G &\in L \\ (a_f - \overline{a_f}^G)f &\in J \\ h_J = a_J + (a_f - \overline{a_f}^G)f &\in J \end{aligned}$$

so $h_J \in J$ and clearly $h_S \in S$.
Now consider any two decompositions of h

$$\begin{aligned} h &= a_1 + \overline{b_1}^G f = a_2 + \overline{b_2}^G f, \ a_1, \ a_2 \in J \\ &\Rightarrow (\overline{b_1}^G - \overline{b_2}^G)f = a_2 - a_1 \in J \\ &\Rightarrow \overline{b_1}^G - \overline{b_2}^G \in L \\ &\Rightarrow \overline{b_1}^G - \overline{b_2}^G = 0 \text{ as G is a Gröbner basis for L.} \end{aligned}$$

□

COROLLARY 4.2. *Let* $F = \langle f_1, \cdots, f_r\rangle$ *be a basis for an ideal* I. *Let* S_1 *be the principal ideal* $\langle f_1\rangle$, *and for each* $2 \leq i \leq r$, *let*

$$\begin{aligned} L_i &= \langle f_1, \cdots, f_{i-1}\rangle : f_i \\ S_i &= \{hf_i \mid h \in N_{L_i}\}. \end{aligned}$$

Then $I = S_1 \oplus S_2 \oplus \cdots \oplus S_r$.

LEMMA 4.3. *Let* $F = \{f_1, \cdots, f_r\}$ *be a homogeneous basis for an ideal* I, *then there is a* k*-standard cone decomposition* P *for* I *with*

$$k = \max\{\deg(f_i) \mid 1 \leq i \leq r\}$$

Proof : Let $S_1 = \langle f_1\rangle$, and for $2 \leq i \leq r$

$$\begin{aligned} J_i &= \langle f_1, \cdots, f_{i-1}\rangle \\ L_i &= J_i : f_i \end{aligned}$$

and $S_i = \{cf_i \mid c \in N_{L_i}\} = f_i N_{L_i}$. The sets S_i form a direct decomposition of I (from the above corollary). S_1 is a principal ideal that has a $\deg(f_1)$-standard cone decomposition $P_1 = \{\langle f_1, X\rangle\}$. Using the algorithm Split, we form a 0-standard decomposition Q_i for each N_{L_i}. If $Q_i = \{\langle h_1, U_1\rangle, \cdots, \langle h_s, U_s\rangle\}$, then clearly from the definition of the sets $P_i = \{\langle f_i h_1, U_1\rangle, \cdots \langle f_i h_s, U_s\rangle\}$ forms a $\mathtt{deg}(f_i)$-standard cone decomposition for S_i. The lemma follows from 2.6. □

It is useful to exclude the set P_1 from this decomposition as follows:

Corollary 4.4. *Let $F = \langle f_1, \cdots, f_r \rangle$ be a homogeneous basis for an ideal* I *with $r > 0$, and let $S_1, \cdots, S_r$ be as above. Then there is a direct decomposition of* I *consisting of the principal ideal $S_1 = \langle f_1 \rangle$, and a* k*-standard cone decomposition* P *for $S_2 \oplus S_3 \oplus \cdots \oplus S_r$, with*

$$k = \max\{\deg(f_i) \mid 1 \leq i \leq r\}$$

5. Exact cone decompositions

Definition 5.1. For $T \subseteq \mathbb{F}[X]$, Q is called an *exact* cone decomposition of T if Q is a k-standard cone decomposition of T for some k, and in addition $\forall d \ : \ |\{\langle h, U \rangle \in Q \mid \deg(h) = d\}| \leq 1$.

Notation : We define $\bar{a}_Q$ to be the least k such that Q is k-standard.
For $0 \leq i \leq (n+1)$ (n is the size of the variable set), let

$$b_i = \min\{d \geq \bar{a}_Q \mid \langle h, U \rangle \in Q, |U| \geq i \Rightarrow (\deg(h) < d)\}$$

In other words it is the least (strict) upper bound on the degree of entries in Q whose variable sets have cardinality greater than i.

As a result of the above definition $b_0 \geq b_1 \geq b_2 \geq \cdots \geq b_{n+1} = \bar{a}_Q$.

Further note that,

$$b_1 = \begin{cases} 1 + \max\{\deg(h) \mid \langle h, U \rangle \in Q^+\}, & Q^+ \neq \emptyset, \\ 0, & Q^+ = \emptyset. \end{cases}$$

The following lemma summarizes the information content of these numbers for an exact cone decomposition.

Lemma 5.2. *Let* Q *be an exact cone decomposition, and let $b_0, \cdots, b_{n+1}$ be defined as above. Then for each $1 \leq i \leq n$ and degree* d *with $b_{i+1} \leq d < b_i$, there is exactly one pair $\langle h, U \rangle \in q^+$ with* $\deg(h) = d$ *and in that pair $|U| = i$.*

Proof : If $Q^+ = \emptyset$, then $b_i = 0$ and the lemma holds. Otherwise for each $1 \leq i \leq n$, the definition of b_i requires that $b_i - 1$ be the largest degree such that Q contains a pair $\langle g, V \rangle$, with $|V| \geq i$. As Q is b_{n+1} standard, each degree $d \in [b_{n+1} \cdots (b_i - 1)]$ must have a pair $\langle h_d, U_d \rangle \in Q$, with $\deg(h_d) = d$ and $|U_d| \geq |V| \geq i$. Since Q is an exact cone decomposition any such pair is unique. If $b_i = b_{i+1}$ then the range $[b_{i+1} \cdots (b_i - 1)]$ is empty. If $b_i \neq b_{i+1}$, for each d in this range $|U_d| = i$, since $|U_d| > i \Rightarrow b_{i+1} \leq d$, and a contradiction arises. □

Lemma 5.3. *Let* Q *be a* k*-standard cone decomposition of* T*, and let $\langle f, S \rangle, \langle g, V \rangle \in Q$ such that* $\deg(f) = \deg(g)$*, and $|V| \geq |S| > 0$. Then for any $x_j \in S$,*

$$Q' = (Q - \{\langle f, S \rangle\}) \cup \{\langle f, S - \{x_j\} \rangle, \langle x_j f, S \rangle\}$$

is also a k*-standard cone decomposition of* T.

Proof : We have to show that for every pair $\langle l, W \rangle \in Q'$ and degree $d \in [k \cdots \deg(l)]$ there is a pair $\langle h, U \rangle \in Q'$ with $\deg(h) = d$ and $|U| \geq |W|$. For $\langle l, W \rangle \in Q \cap Q'$, Q' has all the pairs required from Q itself. For the two new pairs, $\langle g, V \rangle \in Q'$ satisfies the requirements. □

The above lemma can be used to shift off pairs from sharing the same degree. In what follows we call a k-standard cone decomposition P m-exact if for each degree d there is at most one pair $\langle h, U \rangle \in P$ such that $\deg(h) = d$ and $|U| > m$. A cone decomposition is exact iff it is 0-exact.

Lemma 5.4. *The algorithm* Shift *is correct.*

Proof : If Q is a k-standard decomposition, then it follows from the previous lemma we find that Q' is also k-standard. Further, the action of the algorithm assures that for each degree $d < k + c$, Q' contains at most one pair $\langle h, U \rangle$ with $\deg(h) = d$ and $|U| \geq m$. The main point is that degrees $\geq k + c$ need not be considered. First note that at the location where Q' is modified $|\{\langle h, U \rangle \in Q' \mid |U| \geq m\}|$ remains c. now as Q' is a k-standard a pair $\langle g, V \rangle \in Q'$ with $|V| \geq m$ requires that Q' also contain a pair $\langle h_d, U_d \rangle$ with $|U_d| \geq |V|$,

Algorithm 5.1 Algorithm to shift pairs in a standard cone decomposition

```
Shift(Q,k,m)
Input :  $Q$ a $k$-standard $m$-exact cone decomposition for $T$
Output :  $Q'$ a $k$-standard $(m-1)$-exact cone decomposition for $T$
Steps :
$Q' \leftarrow Q$
If $(\{\langle h, U\rangle \in Q \mid |U| \geq m\} = \emptyset)$ then return$(Q')$
$c \leftarrow |\{\langle h, U\rangle \in Q \mid |U| \geq m\}|$
For$(d \leftarrow k;\ d \leq k+c-1)$
 {
 $B \leftarrow \{\langle h, U\rangle \in Q' \mid \deg(h) = d, |U| \geq m\}$
 While$(|B| > 1)$
  {
   Select $\langle h, U\rangle \in B$ with $|U| = m$
   Select $x_j \in U$
   $B \leftarrow B - \{\langle h, U\rangle\}$
   $Q' \leftarrow (Q' - \{\langle h, U\rangle\}) \cup \{\langle h, U - \{x_j\}\rangle, \langle x_j h, U\rangle\}$
  }
 }
return(Q')
```

and $\deg(h_d) = d$, for every degree $d \in [k \cdots \deg(g)]$. Thus the c pairs in the set $\{\langle h, U\rangle \in Q' \mid |U| \geq m\}$ must then include the $\deg(g) - k + 1$ pairs of the form $\langle h_d, U_d\rangle$. Thus $\deg(g) \leq k + c - 1$. □

Repeating the action of Shift we get the following algorithm for producing an exact cone decomposition. The action of the algorithm shows that if $Q' \leftarrow \text{Exact}(Q, k)$, then b_0 for Q' satisfies :

$$b_0 \geq 1 + \max\{\deg(h) \mid \langle h, U\rangle \in Q\}.$$

Algorithm 5.2 Algorithm for producing an exact partition

```
Exact(Q,k)
Input :  $Q$ a $k$-standard cone decomposition for $T$
Output :  $Q'$ an exact cone decomposition for $T$
Steps :
$Q_n \leftarrow Q$
For$(m \leftarrow n; m \geq 1; m \leftarrow m-1)$
 {
 $Q_{m-1} \leftarrow$ Shift$(Q_m, k, m)$
 }
return$(Q_0)$
```

6. Hilbert function of exact cone decompositions

In this section we shall find expressions for the hilbert function of a cone decomposition for a set T. It turns out that this function depends on the value of b_0, and we shall be able to show that this quantity is a bound on the degree of the polynomials in a Gröbner basis. As a result using elementary techniques from dimension theory we can find a bound on this quantity. This will conclude our quest for a bound on the degree of the entries is a Gröbner basis for an ideal.

We know that for a cone decomposition P of a set T. The Hilbert function is just the sum of the Hilbert functions of the individual cones in P.

$$\varphi_T(z) = \sum_{\langle h,U\rangle \in P} \varphi_{C(h,U)}(z)$$

From an elementary counting argument we can show that if the degrees exceed the maximum degree of polynomials involved in a cone decomposition, then the value of the Hilbert function is simply the number of leading terms possible in the cone which is the number of monomials which can be formed of a given degree which are multiples of the base of the cone. More precisely,

$$\text{If } z' = \max\{\deg(h) \mid \langle h,U\rangle \in P\}$$
$$\text{then for } z \geq z' \ \varphi_{C(h,U)}(z) = \overline{\varphi}_{C(h,U)}(z) = \binom{z - \deg(h) + |U| - 1}{|U| - 1}$$

so we have

$$\overline{\varphi_T}(z) = \sum_{\langle h,U\rangle \in P^+} \binom{z - \deg(h) + |U| - 1}{|U| - 1}.$$

If P is exact the information about the degrees and the cardinalities of the sets involved are all contained in the constants b_i, so rephrasing the above expression for this case we have,

$$\overline{\varphi}_T(z) = \sum_{1 \leq j \leq n} \sum_{b_{j+1} \leq d \leq b_i - 1} \binom{z - d + j - 1}{j - 1}$$

By a comparison of definitions it is clear that $z' = b_0$, so the Hilbert function matches the polynomial form for $z \geq b_0$. Now making use of the fact that

$$\sum_{b_{j+1} \leq d \leq b_j - 1} \binom{z - d + j - 1}{j - 1} = \binom{z - b_{j+1} + j}{j} - \binom{z - b_j + j}{j}$$

we can write the Hilbert function of T in the form

$$\begin{aligned}
\varphi_T(z) &= \sum_{1 \leq j \leq n} \left\{ \binom{z - b_{j+1} + j}{j} - \binom{z - b_j + j}{j} \right\} \\
&= \binom{z - b_{n+1} + n}{n} - \binom{z - b_1 + 1}{1} + \sum_{1 \leq j \leq n-1} \left\{ \binom{z - b_{j+1} + j}{j} - \binom{z - b_{j+1} + j + 1}{j + 1} \right\} \\
&= \binom{z - b_{n+1} + n}{n} - 1 - \binom{z - b_1}{1} - \sum_{1 \leq j \leq n-1} \binom{z - b_{j+1} + j}{j + 1} \\
&= \binom{z - b_{n+1} + n}{n} - 1 - \sum_{0 \leq j \leq n-1} \binom{z - b_{j+1} + j}{j + 1}
\end{aligned}$$

Changing indices in the summation accoring to $i \leftarrow j + 1$ we get

$$(\star) \qquad \varphi_T(z) = \binom{z - b_{n+1} + n}{n} - 1 - \sum_{1 \leq i \leq n} \binom{z - b_i + i - 1}{i}$$

We noted that $(\star)$ becomes valid as soon as $z \geq b_0$, however in the range $b_1 \leq z < b_0$, though the cones in P^+ have their Hilbert function described by $(\star)$, there are some cones in $P - P^+$, these cones are isolated monomials and they contribute to the Hilbert function in this range. Thus for $z \geq b_1$ the following form of the function is valid

$$\begin{aligned}\varphi_T(z) &= \overline{\varphi_T}(z) + \sum_{\langle h,\emptyset\rangle \in P} \varphi_{C(h,\emptyset)}(z)\\ &= \overline{\varphi_T}(z) + |\{\langle h,\emptyset\rangle \in P \mid \deg(h) = z\}|.\end{aligned}$$

LEMMA 6.1. *Let P be an exact cone decomposition for a set T. Once $b_{n+1} = \overline{a}_Q$ is fixed, the constants $b_0, \cdots, b_n$ are uniquely determined.*

Proof : The Hilbert polynomial of T can be written as

$$\overline{\varphi_T}(z) = a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_1 z + a_0.$$

The degree $n-1$ comes about from the expression $(\star)$, as the degree n term cancels. We assume inductively that the constants $b_{j+1}, \cdots, b_{n+1}$ have been uniquely determined such that the Hilbert function given by $(\star)$ agrees with the coefficients $a_{n-1}, \cdots, a_j$. The binomial coefficient

$$\binom{z - b_i + i - 1}{i}$$

is a degree i monic polynomial in z. So the coefficients $b_{j-1}, \cdots, b_1$ do not affect the coefficient of z^{j-1} in the Hilbert polynomial. Thus to match the coefficient of a_{j-1} we require a unique choice for b_j.
We can also set b_0 to be unique as

$$b_0 = \min\{d \geq b_1 \mid \forall z > d \;:\; \overline{\varphi_T}(z) = \varphi_T(z)\}$$

□

LEMMA 6.2. *Let I be a homogeneous ideal, then the Hilbert function of N_I is described by a unique set of constants $b_0 \geq b_1 \geq \cdots \geq b_{n+1} = 0$. Further, for any admissible ordering the degree of polynomials in a reduced Gröbner basis for I with respect to the ordering is bounded by b_0 .*

Proof : N_I has a 0-standard cone decomposition, so we can find an exact cone decomposition for N_I for which $b_{n+1} = 0$. Once b_{n+1} is fixed the other constants are determined uniquely.
Let G be a Gröbner basis for I under the ordering. Then N_I admits a 0-standard cone decomposition Q which can be found using $\text{Split}(1, X, \text{LT}\ (G))$. Let $d = 1 + \max\{\deg(h) \mid \langle h, U\rangle \in Q\}$. By Theorem 3.12, $\{g \in G \mid \deg(g) \leq d\}$ is also a Gröbner basis for I. The operation of the algorithm Exact shows that $b_0 \geq d$, so the result follows. □

7. Bounds on the Gröbner basis degree

In the following $F = \{f_1, \cdots, f_r\}$ be a homogeneous basis for an ideal I. We assume that $\deg(f_1) = d$ is the largest degree in the basis. We showed earlier that for any ideal I there is an exact decomposition Q for N_I for which $\overline{a}_Q$ is zero. Further for $z \geq b_0$ (where b_i are as defined earlier), the Hilbert function of N_I attains the polynomial form

$$\varphi_{N_I}(z) = \binom{z+n}{n} - 1 - \sum_{1\leq i\leq n} \binom{z - b_i + i - 1}{i}$$

And we also know that I itself has a direct decomposition consisting of the principal ideal $\langle f_1\rangle$ and an exact decomposition P with $\overline{a}_P = d$. Let $a_0 \geq a_1 \geq \cdots a_{n+1} = d$, be the constants associated with the decomposition P of I. For degrees $z \geq a_0$ the Hilber function of I is:

$$\varphi_I(z) = \binom{z - d + n - 1}{n-1} + \binom{z - d + n}{n} - 1 - \sum_{1\leq i\leq n} \binom{z - a_i + i - 1}{i}$$

where the first term is the contribution to the Hilbert polynomial from the principal ideal.

The main point is that I and N_I form a direct decomposition of $\mathbb{F}[X]$, thus the sum of these two Hilbert functions must equal the Hilbert function of $\mathbb{F}[X]$ which has the simple expression:

$$\varphi_{\mathbb{F}[X]}(z) = \binom{z+n-1}{n-1}$$

Thus for $z \geq \max\{a_0, b_0\}$ we have the equality

$$\begin{aligned} \binom{z+n-1}{n-1} &= \binom{z-d+n-1}{n-1} + \binom{z-d+n}{n} + \binom{z+n}{n} - 2 \\ &\quad - \sum_{1 \leq i \leq n} \left\{ \binom{z-a_i+i-1}{i} + \binom{z-b_i+i-1}{i} \right\} \end{aligned} \tag{1}$$

Recall that $\nabla F(z) \equiv_{def} F(z) - F(z-1)$ for any function $F(z)$, and $\nabla^j F(z) = \nabla(\nabla^{j-1}F(z))$ For the binomial coefficients this has a simple form given below which follows directly from the recurrence for $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, namely :

$$\nabla \binom{z+k}{n} = \binom{z+k-1}{n-1}$$
$$\text{and } \nabla^j \binom{z+k}{n} = \binom{z+k-j}{n-j}$$

It is clear that if $F_1(z) = F_2(z)$ for $z > k$ then $\nabla^j F_1(z) = \nabla^j F_2(z)$ for $z > k + j$. Now applying ∇^j for $0 \leq j \leq n-1$ to (1). This yields the following set of equations which are valid if z is large enough:

$$\begin{aligned} \binom{z+n-j-1}{n-j-1} &= \binom{z-d+n-j-1}{n-j-1} + \binom{z-d+n-j}{n-j} + \binom{z+n}{n} - 2 \\ &\quad - \sum_{j+1 \leq i \leq n} \left\{ \binom{z-a_i+i-j-1}{i-j} + \binom{z-b_i+i-j-1}{i-j} \right\} \end{aligned}$$

As both sides are polynomials in z, they must agree for each power of z. In particular they must have the same constant term. Now the constant term of $\binom{z+k}{n}$ is given by

$$\binom{0+k}{n} = \begin{cases} \binom{k}{n}, & k \geq 0 \\ (-1)^n \binom{n-1-k}{n}, & k < 0 \end{cases}$$

Now computing the constant terms of the previous set of equations, we get

$$\begin{aligned} 1 &= (-1)^{n-j-1} \binom{d-1}{n-j-1} + (-1)^{n-j} \binom{d-1}{n-j} - 1 \\ &\quad - \sum_{j+1 \leq i \leq n} (-1)^{i-j} \left\{ \binom{a_i}{i-j} + \binom{b_i}{i-j} \right\} \end{aligned}$$

At $j = n-1$ this implies,

$$1 - \binom{d-1}{1} - 1 + a_n + b_n = 1 \Rightarrow a_n + b_n = d.$$

We know that $a_n \geq d$, and $b_n \geq 0$, this implies that $a_n = d$. Thus with these values substituted, the series of equations becomes:

$$2(-1)^{n-j-1} \binom{d-1}{n-j-1} - 1 - \sum_{j+1 \leq i \leq n-1} (-1)^{i-j} \left\{ \binom{a_i}{i-j} - \binom{b_i}{i-j} \right\} = 1.$$

If we set $c_{j+1} = a_{j+1} + b_{j+1}$. Solving for this from the above yields

$$c_{j+1} = 2 + 2(-1)^{n-j}\binom{d-1}{n-j-1} + \sum_{j+2\leq i\leq n-1} (-1)^{i-j}\left\{\binom{a_i}{i-j} + \binom{b_i}{i-j}\right\}$$

Now the summation disappears for $j = n-2$ and so $c_{n-1} = 2 + 2(d-1) = 2d$. Further since

$$\binom{a_{i+1}}{k} + \binom{b_{i+1}}{k} \leq \binom{c_{i+1}}{k} \tag{2}$$

holds for all i, we have for $j = n-3$ in the above,

$$c_{n-2} \leq 2 - 2\binom{d-1}{2} + \binom{2d}{d} = d^2 + 2d.$$

For $j < n-3$, the equations contain the expression

$$2 + (-1)^{n-j}\left\{2\binom{d-1}{n-j-1} - \binom{a_{n-1}}{n-j-1} - \binom{b_{n-1}}{n-j-1}\right\}$$

the magnitude of which is bounded by $\binom{c_{n-1}}{n-j-1}$.
So we have the inequality:

$$c_{j+1} \leq \binom{c_{n-1}}{n-j-1} + \sum_{j+1\leq i\leq n-2} (-1)^{i-j}\left\{\binom{a_i}{i-j} + \binom{b_i}{i-j}\right\}$$

Ther term in the sum becomes negative for $i = j+3$ so can be discarded. Retaining all remaining terms and ignoring sign changes we get the weaker inequality:

$$\begin{aligned} c_{j+1} &\leq \binom{c_{n-1}}{n-j-1} + \binom{a_{j+2}}{2} + \binom{b_{j+2}}{2} = \sum_{j+4\leq i\leq n-2}\left\{\binom{a_i}{i-j} + \binom{b_i}{i-j}\right\} \\ &\leq \binom{c_{j+2}}{2} + \sum_{j+4\leq i\leq n-1}\binom{c_i}{i-j} \end{aligned}$$

Changing the indices by $j \to j-1$ we have

$$c_j \leq \binom{c_{j+1}}{2} + \sum_{j+3\leq i\leq n-1}\binom{c_i}{i-j+1}$$

Now we can use this inequality to find the bound:

LEMMA 7.1. *For $j \leq n-2$, the value c_j satisfies the inequality $c_j \leq D_j$, where*

$$D_j = 2\left(\frac{d^2}{2} + d\right)^{2^{n-j-1}}$$

From this we conclude that both a_1 and b_1 are each less than $D_1 = 2(\frac{d^2}{2} + d)^{2^{n-2}}$. But we need a bound on b_0. To obtain that we observe that for $\max\{a_1, b_1\} < z \leq \max\{a_0, b_0\}$, we have:

$$\varphi_I(z) + \varphi_{N_I}(z) = \varphi_{\mathbb{F}[X]}(z)$$

to get

$$\overline{\varphi}_I(z) + |\{\langle h, \emptyset\rangle \in P \mid \deg(h) = z\}| + \overline{\varphi}_{N_I}(z) + |\{\langle h, \emptyset\rangle \in Q \mid \deg(h) = z\}| = \varphi_{\mathbb{F}[X]}(z)$$

Now consider the space $\mathbb{F}[X]$ if the monomial degrees are greater than $\max\{a_1, b_1\}$, then such a monomial would have to belong to either the cones of P^+ or of $Q+$ we conclude that $\overline{\varphi}_I(z) + \overline{\varphi}_{N_I}(z) = \varphi_{\mathbb{F}[X]}(z)$ holds for $z \geq \max\{a_1, b_1\}$. This implies that $P \cup Q$ has no pair of the form $\langle h, \emptyset\rangle$ for $\deg(h) > \max\{a_1, b_1\}$. Thus the value of D_1 also provides a bound for b_0. Using this and Lemma 6.2 we have the following theorem.

THEOREM 7.2. *Let* I *be an ideal in* $\mathbb{F}[x_1, \cdots, x_n]$*, generated by the homogeneous basis* $F = \{f_1, \cdots, f_r\}$*. Let* $d = \max\{\deg(f) \mid f \in F\}$*. Then for any admissible ordering the degree of polynomials required in a Gröbner basis for* I *with respect to the ordering is bounded above by*

$$2\left(\frac{d^2}{2} + d\right)^{2^{n-2}}$$

Using the idea of homogenizing an ideal discussed in Chapter 1, we have the following Corollary.
Let $X = \{x_1, \cdots, x_n\}$.

COROLLARY 7.3. *Let* $F \subseteq \mathbb{F}[X]$*, and let* I *be ideal generated by* F*, and let* $d = \max\{\deg(f) \mid f \in F\}$*. Then for any admissible ordering, the degree of polynomials required in a Gröbner basis for* I *with respect to the ordering is bounded by*

$$2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}$$

In light of the fact that Gröbner bases solve the **PIM**, we conclude that the above bound is essentially optimal - in the sense that there are classes of ideals for which the degree in the Gröbner basis grows doubly exponentially.

CHAPTER 5

Primary Decomposition

We show that every ideal can be expressed as a finite intersection of *primary ideals*, and then discuss the computational aspect of this problem. We begin with the study of properties of *prime ideals*.

1. Prime Ideals

Recall that if I is an ideal then $\sqrt{I}$ is the set $\{f \mid \exists m \in \mathbb{N} \ : \ f^m \in I\}$. Since $f^m \in I,\ g^n \in I \Rightarrow (f-g)^{m+n-1} \in I$, we see that $\sqrt{I}$ is also an ideal. This ideal is called the *radical* of I. If I is an ideal for which $I = \sqrt{I}$, then I is called a *radical ideal*. Hilbert's Nullstellensatz shows that the algebraic sets in $\mathbb{F}^n$ (where $\mathbb{F}$ is algebraically closed), and the radical ideals are in bijection.

If X is a Noetherian topological space i.e., every sequence of closed subsets $Y_1 \supseteq Y_2 \supseteq \cdots \supseteq Y_r \supseteq Y_{r+1} \supseteq \cdots$ stabilizes ($Y_k = Y_{k+1}$ for some k), then every closed set can be expressed as a finite union of irreducible closed sets of the space (uniquely). The space defined above is Noetherian since $Y_1 \supseteq Y_2 \supseteq \cdots$ leads to an ascending chain $\mathbf{I}(Y_1) \subseteq \mathbf{I}(Y_2) \subseteq \cdots$, and as $\mathcal{A}$ is Noetherian the conclusion follows.

We defined an ideal I to be *prime* if $x \notin I, y \notin I \Rightarrow xy \notin I$. From this definition it is clear that I is prime iff $\mathcal{A}/I$ is an integral domain. Further we can show that I is prime iff $\mathbf{V}(I)$ is irreducible. It is too much to expect that every ideal can be expressed as an intersection of prime ideals, however from the correspondence of radical ideals with algebraic sets and irreducible algebraic sets with prime ideals we have:

THEOREM 1.1. *If* I *is a radical ideal then*

$$I = \bigcap_{\mathfrak{p} \text{ a prime ideal, } \mathfrak{p} \supseteq I.} \mathfrak{p}.$$

The set $\{\mathfrak{p} \mid \mathfrak{p} \supseteq I, \mathfrak{p}$ *is a prime ideal.*$\}$ *is a finite set.*

If I is a maximal ideal of $\mathcal{A}$, then clearly $\mathcal{A}/I$ is a field which is also an integral domain, which implies that all maximal ideals are also prime. We might pose the following natural problem:

Problem : Ideal Primality (**IP**)
Input : $f_1, \cdots, f_k \in \mathcal{A}$
Question : Is $\langle f_1, \cdots, f_k \rangle$ a prime ideal?

THEOREM 1.2. **IP** *is* coNP *hard.*

Proof : Let 1-**SAT** $\equiv \{\phi \mid \exists_1 \sigma \in \{\bot, \top\}^n \ : \ \phi(\sigma) = \top\}$ (boolean formulas with exactly one satisfying assignment). Note that this problem is coNP hard, since we can reduce the complement of **SAT** to this language simply by adding a new variable say y and using the distributive properties of $\vee$ over $\wedge$ to add one more satisfying assignment to ϕ by setting $\phi' \leftarrow (\phi \wedge y) \vee (\neg y \wedge \neg x_1 \cdots \neg x_n)$. Now ϕ' has exactly one satisfying assignment iff ϕ was unsatisfiable which gives the reduction[1].

Claim : 1-**SAT** $\leq^p_m$ **IP**.
We use the same construction in (2.§3) to associate a natural ideal I to the given boolean formula. We observe that $\mathbf{V}(I)$ is a zero-dimensional variety, and the only such irreducible varieties are those which have

[1] By Valiant-Vazirani this language is hard for NP under polytime randomized reductions.

exactly one point (minimal irreducible sets). So the associated ideal is prime iff the orginal boolean formula had exactly one satisfying assignment. □

The known algorithms for **IP** involve Gröbner bases, and so the upper bound for this problem is EXPSPACE.

Actually we can prove a slightly stronger claim.

PROPOSITION 1.3. **HN** $\leq_m$ **IP**

Proof : The version of **HN**we shall use, is the following.
Instance : $I = \langle p_1, \cdots, p_k \rangle \subseteq \mathcal{A}$.
Question : Is $1 \in I$?

Consider the reduction which given the above instance outputs the generators for the ideal $I' =_{def} I.\langle x \rangle \subseteq \mathbb{F}[x_1, \cdots, x_n, x]$. Now If 1 in I then $I' = \langle x \rangle$ which is clearly prime.
If $1 \notin I$, then $\mathbf{V}(I') = \mathbf{V}(I) \cup \mathbf{V}(\langle x \rangle)$, and clearly $\mathbf{V}(I) \neq \mathbf{V}(\langle x \rangle)$, so the ideal I' is not prime since the corresponding variety is not irreducible. We have assumed that $I \neq 0$, which is trivial to check - if I has any non-zero generators then $I \neq 0$. □

Consider the following problem :
Radical Ideal Membership Problem (RIM) :
Instance : $I = \langle f_1, \cdots, f_k \rangle \subseteq \mathcal{A}$ with $I = \sqrt{I}$ and $h \in \mathcal{A}$.
Question : $h \in I$?

It is interesting to observe that:

PROPOSITION 1.4. **RIM** $\leq_m^p$ **HN**

Proof : The proof follows from the fact that :

$$\begin{aligned} f \in I &\Leftrightarrow \mathbf{V}(I) - \mathbf{V}(f) = \emptyset \quad \text{as } I = \sqrt{I} \\ &\Leftrightarrow \mathbf{V}(I + \langle 1 - xf \rangle) = \emptyset.\ x \text{ is a new variable.} \end{aligned}$$

Whenever f does not vanish we can find $x \in \mathbb{F}$ such that $1 - xf = 0$. So $\mathbf{V}(I) - \mathbf{V}(f)$ in the ring $\mathbb{F}^{(n+1)}$ is given by the algebraic set of the ideal sum as given. □

It is interesting to note that if we define the radical ideal membership problem to be as follows :
Radical Ideal Membership Problem (RIM) :
Instance : $I = \langle f_1, \cdots, f_k \rangle \subseteq \mathcal{A}$ and $h \in \mathcal{A}$.
Question : $h \in \sqrt{I}$?

Then we have the following theorem which easily follows from the above :

THEOREM 1.5. **RIM** *and* **HN** *are equivalent under polynomial time many-one reductions.*

In essence what we have shown is that the so called weak version of the Nullstellensatz and the strong version are computationally equivalent.

Bibliography

[Dub90] Thomas W. Dubé, *The Structure of Polynomial Ideals and Gröbner Bases*, SIAM J. Comput. (1990), Vol. 19, No. 4, 750-773.

[FMR68] P. C. Fischer, A. R. Meyer, and A. L. Rosenberg. *Counter machines and counter languages*, Math. Systems Theory **2**(3) (1968), 265-283.

[Ful98] William Fulton, *Intersection Theory*, Springer-Verlag (1998).

[Har77] Robin Hartshorne, *Algebraic Geometry.* Springer-Verlag GTM 52 (1977).

[Her26] Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale* (1926). Math. Ann. **95**, 736-788.

[Koi96] Pascal Koiran, *Hilbert's Nullstellensatz is in the Polynomial Hierarchy.* DIMACS Technical Report 96-27 (1996) (http://www.dimacs.rutgers.edu/).

[Kol88] János Kollár, *Sharp Effective Nullstellensatz.* J. Amer. Math. Soc. **1** (1988), no. 4,963-975.

[Kri96] Teresa Krick, Luis M. Pardo, *A Computational Method for Diophantine Approximation.* Algorithms in Algebraic Geometry and Applications (1996), Vol **143** Progess in Mathematics, Birkhäuser Verlag, 193-254.

[Mat80] Hideyuki Matsumura, *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics (1980), Cambridge University Press.

[MM82] Ernst W. Mayr, Albert R. Meyer, *The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals.* Adv. Math. (1982), **46**,305-329.

[Po47] Emil Post, *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic (1947), **12** 1-11.

[Sip83] Michael Sipser, *A Complexity Theoretic Approach to Randomness.* Proc. 15th ACM Symposium on Theory of Computing (1983), 330-335.