ON THE MINIMAL NUMBER OF ELEMENTS GENERATING AN ALGEBRAIC SET

A THESIS

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS

AND THE INSTITUTE OF ENGINEERING AND SCIENCE

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE

By

Mesut Şahin

August, 2002

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Ali Sinan Sertöz (Supervisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Serguei Stepanov

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Hurşit Önsiper

Approved for the Institute of Engineering and Science:

Prof. Dr. Mehmet Baray
Director of the Institute Engineering and Science

ABSTRACT

ON THE MINIMAL NUMBER OF ELEMENTS GENERATING AN ALGEBRAIC SET

Mesut Şahin
M.S. in Mathematics
Supervisor: Assoc. Prof. Dr. Ali Sinan Sertöz
August, 2002

In this thesis we present studies on the general problem of finding the minimal number of elements generating an algebraic set in n-space both set and ideal theoretically.

Keywords: Monomial curves, Complete intersections, Algebraic set.

ÖZET

BİR CEBİRSEL KÜMEYİ ÜRETEN MİNİMAL ELEMAN SAYISI ÜZERİNE

Mesut Şahin
Matematik Bölümü, Master
Tez Yöneticisi: Doç. Dr. Sinan Sertöz
Ağustos, 2002

Bu tezde n boyutlu uzayda bir cebirsel kümenin hem kümesel hem de ideal teorik olarak üretilmesi için gerekli olan minimal eleman sayısının bulunması problemi sunulmuştur.

Anahtar sözcükler: Tek terimli eğriler, Tam kesişimler, Cebirsel küme.

Acknowledgements

I would like to use this opportunity to express my deep gratitude to my supervisor Sinan Sertöz for his guidance, suggestions and invaluable encouragement throughout the development of this thesis.

I would like to thank Hurşit Önsiper and Serguei Stepanov for reading and commenting on the thesis.

I would like to thank to Mefharet Kocatepe, Metin Gürses for their encouragement and help.

I express my special thanks to Halil İbrahim Karakaş and Sefa Feza Arslan for their support, comments and great help.

Finally, many thanks to all of my close friends and my family for their support and love.

Contents

1

INTRODUCTION AND STATEMENT OF RESULTS

In this thesis we will present studies on the general problem of finding the minimal number of elements generating an algebraic set in n space both set and ideal theoretically. This problem may be investigated in algebraic and analytic category; we will deal with algebraic category in this thesis.

Let k be an algebraically closed field of characteristic zero and X be affine or projective n space and $Y \subseteq X$ be an algebraic set. We say that Y *is generated by m elements set theoretically* if we can write

$$Y = Z(f_1, ..., f_m).$$

Let $\mu(Y)$ be the *minimal number of elements generating Y set theoretically.* So $\mu(Y) \leq m$ if Y is generated by m elements set theoretically.

We say that Y *is generated by m elements ideal theoretically* if $I(Y)$ can be generated by m elements. Let $\mu(I(Y))$ be the *minimal number of elements generating Y ideal theoretically.* So $\mu(I(Y)) \leq m$ if Y is generated by m elements ideal theoretically. We define *codimension* of Y as $codim(Y) = n - dimY$. It is easy to see that

$$codim(Y) \leq \mu(Y) \leq \mu(I(Y)).$$

Y is called a *complete intersection set theoretically* if

$$\mu(Y) = codim(Y).$$

If moreover

$$\mu(I(Y)) = codim(Y),$$

then Y is called a *complete intersection ideal theoretically.* If Y is a complete intersection ideal theoretically, i.e. $\mu(I(Y)) = codim(Y)$ then it follows from $codim(Y) \leq \mu(Y) \leq \mu(I(Y))$ that $\mu(Y) = codim(Y)$, i.e Y is a complete intersection set theoretically. But the converse is not true. For example the projective twisted cubic curve is a set theoretic complete intersection even though it is not an ideal theoretic complete intersection.

We present studies on the general problem of finding the minimal number of elements generating an algebraic set in n space both set and ideal theoretically.

We state and give a detailed proof of Eisenbud and Evans' Theorem 2.10 and Theorem 2.13, which suggests the best possible answer known to the problem mentioned above [7].

Although the minimal number $\mu(Y) \leq n$, for an algebraic set Y in the set theoretic case due to Eisenbud and Evans' result, it may be arbitrarily large in the ideal theoretic case due to Bresinsky [6]. So there is no upper bound on the minimal number of elements generating Y ideal theoretically.

It is still an open question to decide whether Eisenbud and Evans' result is best possible in the set theoretic case. We consider curves to solve this problem at least for special cases. A curve C is a complete intersection set theoretically, if

$\mu(C) = n-1$. Hence the open problem turns out to be whether every irreducible (even smooth) space curve is a set theoretic complete intersection of 2 surfaces. The answer of corresponding question in 4 space is negative. Since the surface $S = Z(x,y) \bigcup Z(z,w)$ is not a complete intersection of 2 hypersurfaces. We say a noetherian topological space Y is connected in codimension 1, if the following condition is satisfied "whenever P is a closed subset of Y and $codim(P,Y) > 1$ then $Y - P$ is connected." To show that S is not complete intersection it remains to prove that S is not connected in codimension 1, by a Theorem 3.4 of Hartshorne [11]. Since $P = \{(0,0,0,0)\}$ is a closed subset of S, $codim(P,S) = 2-0 = 2 > 1$ and $S - P = [Z(x,y) - \{(0,0,0,0)\}] \bigcup [Z(z,w) - \{(0,0,0,0)\}]$ is not connected, S is not connected in codimension 1, hence S is not a complete intersection set theoretically.

So the problem mentioned above can be divided into two parts:

(i) Set Theoretic Case

The first general result was given in 1882 by Kronecker [15]. He showed that any radical ideal in a polynomial ring in n variables over k is the radical of an ideal generated by $n+1$ polynomials, i.e. $\mu(Y) \leq n+1$. For a long time, Kronecker's result was believed to be the best possible due to an example of Vahlen [30]. Vahlen's example was a curve in the complex projective 3 space, which he claimed could not be written as an intersection of 3 surfaces. Vahlen's error was noticed in 1942 when Perron [21] gave explicitly 3 surfaces, whose intersection is exactly the curve given by Vahlen. Vahlen's error was that he could not separate the notion and description of ideal and set theoretic complete intersections.

In 1961, Kneser showed that Perron's result is a special case of the fact that indeed every space curve C is an intersection of 3 surfaces, i.e. $\mu(C) \leq 3$ in 3 space [14].

In 1963, Forster generalized affine analogue of Kronecker's result to Noetherian rings, i.e. any radical ideal in an n dimensional Noetherian ring R can be generated by $n+1$ elements up to radical, i.e. any radical ideal in R is the radical of an ideal generated by $n+1$ elements [8].

Eisenbud and Evans generalized Kneser's result in 1973 to n spaces by proving that any radical ideal in an n dimensional Noetherian ring can be generated by n elements up to radical [7]. Storch also generalized independently Kneser's result in 1972, but he only considered the affine case [26].

Let us define affine monomial curves in $\mathbb{A}^n$ and affine monomial space curves.

Definition 1.1 *Let k be a field of characteristic zero and $m_1 < \ldots < m_n$ be positive integers such that $gcd(m_1, \ldots, m_n) = 1$. An affine monomial curve $C(m_1, \ldots, m_n)$ in $\mathbb{A}^n$ is given parametrically by*

$$x_1 = t^{m_1}$$
$$x_2 = t^{m_2}$$
$$\vdots$$
$$x_n = t^{m_n}$$

where t is an element of the ground field k. If $n = 3$, then $C(m_1, m_2, m_3)$ is called an affine monomial space curve.

Here are some special results:

in $\mathbb{A}^n$

(1) All monomial space curves in $\mathbb{A}^3$ are the set theoretic complete intersection of two surfaces [3].

(2) The monomial curve $C(m_1, m_2, m_3, m_4)$ is a set theoretic complete intersection in $\mathbb{A}^4$ if and only if $< m_1, m_2, m_3, m_4 >$ is a symmetric semigroup, for the definition of a symmetric semigroup see section 3.3, [4].

(3) For any $n \geq 4$, if some $n-1$ terms of $m_1, \ldots, m_n$ form an arithmetic sequence then the monomial curve $C(m_1, \ldots, m_n)$ is a set theoretical complete intersection [20]. As a corollary to this result: The monomial curve $C(n, an-sd, \ldots, an-d, an+d, \ldots, an+td)$ is a set theoretical complete intersection where a, n, s, d are positive integers with $an > sd$ and $\gcd(n, d) = 1$.

Definition 1.2 *We say a curve C in $\mathbb{P}^3$ is a set theoretic complete intersection on a surface S if there exist another surface T such that C is the intersection of S and T.*

in $\mathbb{P}^n$

(4) Rational normal curves are set theoretic complete intersections in $\mathbb{P}^n$ [22].

The rational normal curve in $\mathbb{P}^n$ is the nth Veronese image of the projective line, i.e. $v_n(\mathbb{P}^1) \subset \mathbb{P}^n$, where Veronese map is defined as follows:

$$v_n : \mathbb{P}^1 \longrightarrow \mathbb{P}^n, v_{i_o, i_1} = x_0^{i_0} x_1^{i_1}$$

where i_0, i_1 are nonnegative integers such that $i_0 + i_1 = n$ and v_{i_o, i_1} denotes homogeneous coordinates of $\mathbb{P}^n$.

(5) All monomial curves in $\mathbb{P}^3$ whose projective coordinate rings are Cohen-Macaulay are set theoretic complete intersections. But the smooth monomial curve $C_4 = (t^4, t^3u, tu^3, u^4)$ whose coordinate ring is not Cohen-Macaulay is not a set theoretic complete intersection on anyone of the three binomial surfaces $f_1 = x_0^2 x_2 - x_1^3$, $f_2 = x_0 x_3 - x_1 x_2$ and $f_3 = x_1 x_3^2 - x_2^3$ even though $Z(C_4) = Z(f_1, f_2, f_3)$. It is an open question whether C_4 is a set theoretic complete intersection [23].

(6) Smooth monomial curves in $\mathbb{P}^3$ of degree > 3 are not set theoretic complete intersections on bihomogeneous surfaces [29]. A bihomogeneous surface in $\mathbb{P}^3$ is a surface defined by a bihomogeneous polynomial F. A polynomial

$$F = \sum a_{v_0 v_1 v_2 v_3} x_0^{v_0} x_1^{v_1} x_2^{v_2} x_3^{v_3} \in k[x_0, x_1, x_2, x_3]$$

is called bihomogeneous of type (d, a_1, a_2) and degree (a, b) if $a_{v_0 v_1 v_2 v_3} = 0$ for all (v_0, v_1, v_2, v_3) with

$$v_0(d, 0) + v_1(a_1, d - a_1) + v_2(a_2, d - a_2) + v_3(0, d) \neq (a, b).$$

(7) Smooth monomial curves in $\mathbb{P}^3$ of degree > 3 are not set theoretic complete intersections on surfaces with at most ordinary nodes as singularities or of degree at most three or cones [13].

(8) Smooth monomial curves in $\mathbb{P}^3$ of degree > 3 are not set theoretic complete intersections on any binomial surfaces [27].

A binomial surface in $\mathbb{P}^3$ is a surface defined by a binomial f of the following form:

$$f = a_{v_0 v_1 v_2 v_3} x_0^{v_0} x_1^{v_1} x_2^{v_2} x_3^{v_3} - a_{\mu_0 \mu_1 \mu_2 \mu_3} x_0^{\mu_0} x_1^{\mu_1} x_2^{\mu_2} x_3^{\mu_3}$$

where $\sum_{i=0}^{3} v_i = \sum_{i=0}^{3} \mu_i$.

(9) All monomial curves in $\mathbb{P}^3$ which are set theoretic complete intersections on two binomial surfaces are exactly those that are ideal theoretic complete intersections [28].

(ii) Ideal Theoretic Case

The minimal number of equations needed to define a space curve can be arbitrarily large due to an example of Macaulay given in 1916 [17]. His example was a curve in $\mathbb{A}^3$ with large number of singularities, so the ideal of curve needs arbitrary large number of generators even locally at these singularities. For any

$r > 1$, Macaulay constructed a curve C in $\mathbb{A}^3$ such that $\mu(I(C)) > r$. For more details see [[9],page 310].

Definition 1.3 *The monomial curve C^n_m is defined parametrically as follows*

$$x_1 = t^{a_1}, x_2 = t^{a_2}, \cdots, x_n = t^{a_n}$$

where $a_1 = 2^{n-4}m(m+1),\ a_2 = 2^{n-4}(m(m+1)+1),\ a_3 = 2^{n-4}(m+1)^2,\ a_4 = 2^{n-4}((m+1)^2+1),\ a_5 = 2^{n-4}(m+1)^2 + 2^{n-5},\ a_i = 2^{n-4}(m+1)^2 + 2^{n-5} + \sum_{j=6}^{i}(-1)^j 2^{n-j}$, *for* $i \geq 6$, *with* $m \geq 2$ *and* $n \geq 4$.

In 1999, Arslan S.F. gave the description of the ideal of the monomial curve C^n_m in his article [2] and showed that $\mu(I(C^n_m)) = 2m + n - 1$.

It is worthwhile to find how many generators are necessary to define a curve locally (which means that in a neighborhood of any point of the curve), and then knowing the answer we can consider the curve globally. This is the so called local global principle; first we prove a theorem on the local ring then, we try to get an analogue of the theorem on the global ring.

In 1963, Forster used this local global principle to show that every smooth curve in $\mathbb{A}^3$ can be defined by 4 equations ideal theoretically [8].

In 1970, Abhyankar proved that 3 equations are enough to define a smooth curve in $\mathbb{A}^3$. Moreover he proved that smooth curves of genus ≤ 1 in $\mathbb{A}^3$ are complete intersections ideal theoretically, if their degree is ≤ 5, [1].

According to Serre all smooth curves of genus ≤ 1 would be ideal theoretically complete intersections, if every projective module of rank 2 over $k[x_1, x_2, x_3]$ would be free [25].

In the same year 1970, Segre claimed that he has found smooth curves of genus

≤ 1 in $\mathbb{A}^3$ which are not complete intersection ideal theoretically (i.e. cannot be defined by 2 equations) [24].

In 1971, Murthy has shown that, in the polynomial ring $k[x_1, x_2, x_3]$, over a field k, any ideal of height 2 which is locally a complete intersection can be generated by 3 elements [18]. This means that if C is a curve in $\mathbb{A}^3$ which is generated by 2 elements in a neighborhood of any point of C, then $I(C)$ is generated by 3 elements. We give an example to show that any prime ideal of height 2 need not be generated by 2 polynomials, for details see Remark 4.1. Murthy also gives an example to show that the ideal corresponding even to a nonsingular curve in 3 space need not be generated by 2 elements.

In 1974, Murthy and Towber [19] proved that every projective module of rank 2 over $k[x_1, x_2, x_3]$ is free. Hence it follows from this result together with Serre's result that every smooth curve in $\mathbb{A}^3$ of genus ≤ 1 can be defined by 2 equations ideal theoretically, which shows that the Segre's claim is false.

Here are some special results:

in $\mathbb{A}^n$

(1) Herzog proved that for the monomial curve $C(m_1, m_2, m_3)$, $I(C)$ is generated by 2 elements iff $< m_1, m_2, m_3 >$ is a symmetric semigroup [12].

(2) Bresinsky showed that there are some monomial curves needing arbitrarily large minimal number of equations to define them ideal theoretically [6].

(3) Bresinsky also showed that for the monomial curve

$$C(m_1, m_2, m_3, m_4)$$

if

$$< m_1, m_2, m_3, m_4 >$$

is symmetric then $I(C)$ is generated by 3 or 5 elements [5].

For higher dimensions the question, whether the symmetry implies existence of a finite upper bound for the minimal number of elements generating a monomial curve $C(m_1, \ldots, m_n)$ ideal theoretically, is open.

In projective case the situation is completely different since the local global principle doesn't hold.

2

$\mu(Y) \leq n$ FOR AN ALGEBRAIC SET Y IN AN n SPACE

In this chapter, we will state theorems which are the answers of the following question. What is the minimal number of elements generating an algebraic set? First we state and prove the theorem of Kronecker, which says that $\mu(Y) \leq n+1$, for an algebraic set in n space and then we present Forster's theorem, which is the affine generalization of Kronecker's result to any Noetherian ring. Finally we state and give a detailed proof of Eisenbud and Evans' theorem, which suggests the best possible answer so far to the question above.

2.1 Theorem of Kronecker

Let us first state the theorem of Kronecker and then prove it for projective n space, since affine case follows from projective case. We use Geyer's notes [9] in this section.

Theorem 2.1 (Kronecker,[15]) *Every algebraic set in n space is defined by $n+1$ elements set theoretically.*

For projective n space the theorem above can be stated as follows:

Theorem 2.2 *Every algebraic set in $\mathbb{P}^n$ is defined by $n+1$ homogeneous polynomials set theoretically.*

To prove Theorem 2.2 we need a lemma:

Lemma 2.3 ([16], Lemma 3.2, page 49) *If ϕ is a homogeneous polynomial of degree m in the polynomial ring $k[x_1, \ldots, x_{n+2}]$ over an algebraically closed field k, then making a linear transformation $y_i = x_i + \lambda_i x_{n+2}$, for all $i = 1, \ldots, n+1$ and $\lambda_i \in k$, ϕ takes of the following form*

$$\phi^*(y_1, \ldots, y_{n+1}, x_{n+2}) = \phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1)x_{n+2}^m + \sum_{j=0}^{m-1} \psi_j(y_1, \ldots, y_{n+1})x_{n+2}^j$$

where $\phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1) \neq 0$ and ψ_j's are homogeneous of degree $m-j$, for all $j = 0, \ldots, m-1$.

Proof: First assume that ϕ is a homogeneous polynomial of degree 2 in the polynomial ring $k[x_1, x_2]$. Let $\phi(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ and $y = x_1 + \lambda x_2$. Defining $\phi^*(y, x_2) = \phi(x_1, x_2)$ we get

$$\phi^*(y, x_2) = \phi(y - \lambda x_2, x_2) = a(y - \lambda x_2)^2 + b(y - \lambda x_2)x_2 + cx_2^2$$

$$= (a\lambda^2 - b\lambda + c)x_2^2 + (by - 2a\lambda y)x_2 + (ay^2)$$

$$= \phi(-\lambda, 1)x_2^2 + \psi_1(y)x_2 + \psi_0(y)$$

where $\psi_1(y) = (b - 2a\lambda)y$ is homogeneous of first degree and $\psi_0(y) = ay^2$ is homogeneous of second degree. Since k is an infinite field, we may choose λ so that $\phi(-\lambda, 1) \neq 0$. This is because every nonzero polynomial in one variable may have at most finitely many zeroes.

Therefore, we have proved for $n = 0$ and $m = 2$ that

$$\phi^*(y_1, \ldots, y_{n+1}, x_{n+2}) = \phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1)x_{n+2}^m + \sum_{j=0}^{m-1} \psi_j(y_1, \ldots, y_{n+1})x_{n+2}^j$$

where ψ_j's are homogeneous of degree $m - j$, for all $j = 0, \ldots, m-1$.

Now letting

$$\phi = \sum_{v_1+\ldots+v_{n+2}=m} a_{v_1\ldots v_{n+2}} x_1^{v_1} \ldots x_{n+1}^{v_{n+1}} x_{n+2}^{v_{n+2}},$$

and putting $y_i - \lambda_i x_{n+2}$ instead of x_i in the above expression for all $i = 1, \ldots, n+1$ we get

$$\phi^* = \sum_{v_1+\ldots+v_{n+2}=m} a_{v_1\ldots v_{n+2}} (y_1 - \lambda_1 x_{n+2})^{v_1} \ldots (y_{n+1} - \lambda_{n+1} x_{n+2})^{v_{n+1}} x_{n+2}^{v_{n+2}}.$$

Thus by binomial expansion we get

$$\phi^* = \sum_{v_1+\ldots+v_{n+2}=m} a_{v_1\ldots v_{n+2}} (y_1 k_1 - \lambda_1^{v_1} x_{n+2}^{v_1}) \ldots (y_{n+1} k_{n+1} - \lambda_{n+1}^{v_{n+1}} x_{n+2}^{v_{n+1}}) x_{n+2}^{v_{n+2}},$$

and

$$\phi^* = x_{n+2}^m \sum_{v_1+\ldots+v_{n+2}=m} a_{v_1\ldots v_{n+2}} (-\lambda_1)^{v_1} \ldots (-\lambda_{n+1})^{v_{n+1}} + \cdots.$$

Here the last $\cdots$ is used instead of terms in which x_{n+2} has power less than m. Hence

$$\phi^*(y_1, \ldots, y_{n+1}, x_{n+2}) = \phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1)x_{n+2}^m + \sum_{j=0}^{m-1} \psi_j(y_1, \ldots, y_{n+1})x_{n+2}^j$$

where ψ_j's are homogeneous of degree $m - j$, for all $j = 0, \ldots, m-1$. To accomplish the proof we need to show that $\lambda_1, \ldots, \lambda_{n+1}$ can be chosen so that $\phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1) \neq 0$. This is a consequence of the following fact:

If k is an infinite field and $F \in k[x_1, \ldots, x_r]$ is a nonzero polynomial then there exist $\lambda_1, \ldots, \lambda_r \in k$ so that $F(\lambda_1, \ldots, \lambda_r) \neq 0$. This can be proven by induction on r. If $r = 1$ then F can have at most finitely many zeroes. Since k is infinite we may choose λ_1 such that $F(\lambda_1) \neq 0$. If $r > 1$ then assume that the claim is true for $r - 1$. Let $F(x_1, \ldots, x_r) \in k[x_1, \ldots, x_r]$ be a nonzero polynomial. Then we can write F in the following form

$$F(x_1, \ldots, x_r) = \sum_{i=0}^{N} G_i(x_1, \ldots, x_{r-1}) x_r^i.$$

Since F is a nonzero polynomial, there exist i such that G_i is a nonzero polynomial in $k[x_1, \ldots, x_{r-1}]$. By induction hypothesis, for this fixed i, there exist $\lambda_1^{(i)}, \ldots, \lambda_{r-1}^{(i)} \in k$ such that $G_i(\lambda_1^{(i)}, \ldots, \lambda_{r-1}^{(i)}) \neq 0$. Thus $F(\lambda_1^{(i)}, \ldots, \lambda_{r-1}^{(i)}, x_r)$ is a nonzero polynomial in one variable and by the first case there exist $\lambda_r^{(i)} \in k$ so that $F(\lambda_1^{(i)}, \ldots, \lambda_r^{(i)}) \neq 0$.

Proof of Theorem 2.2: [[9],page 215] Since every algebraic set is defined by a finite number of polynomials due to Hilbert's basis theorem, it suffices to show that any algebraic set defined by $n + 2$ homogeneous polynomials is defined by $n + 1$ homogeneous polynomials, set theoretically. In this way we can decrease the number of defining polynomials by one, so this step can be iterated. We can suppose that the degrees of polynomials are the same, since $f = 0$ is equivalent to the following system of equations

$$x_0^r f = \ldots = x_n^r f = 0$$

where $[x_0 : \ldots : x_n] \in \mathbb{P}^n$, that is, $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$. The transcendence degree of $k[x_0, \ldots, x_n]$ over k is $n + 1$. If we take $n + 2$ homogeneous polynomials $f_1, \ldots, f_{n+2}$ of the same degree d in the polynomial ring $k[x_0, \ldots, x_n]$, then these polynomials must be algebraically dependent, since their number is greater than the transcendence degree of the polynomial ring $k[x_0, \ldots, x_n]$. Algebraically dependent means $(f_1, \ldots, f_{n+2})$ is a zero of some nonzero polynomial ϕ of degree m, that is,

$$\phi(f_1, \ldots, f_{n+2}) \equiv 0$$

Since $\phi = 0$ is equivalent to $\phi_i = 0$, where ϕ_i is the homogeneous component of ϕ of degree i, we may suppose that ϕ is homogeneous of degree m.

By making a linear transformation $g_i = f_i + \lambda_i f_{n+2}$, for all $i = 1, \ldots, n+1$ and $\lambda_i \in k$, we get another polynomial equation by using Lemma 2.3:

$$\phi^*(g_1, \ldots, g_{n+1}, f_{n+2}) = 0$$

where the coefficient of f_{n+2}^m in ϕ^* is $\phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1)$. Since k is an infinite field (k is algebraically closed) and $\phi(x_0, \ldots, x_n)$ is a nonzero polynomial we can choose λ_i so that $\phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1) \neq 0$. Hence we get the following

$$0 = \phi^*(g_1, \ldots, g_{n+1}, f_{n+2}) = \phi(-\lambda_1, \ldots, -\lambda_{n+1}, 1) f_{n+2}^m + \sum_{j=0}^{m-1} \psi_j(g_1, \ldots, g_{n+1}) f_{n+2}^j$$

Since g_i's are homogeneous of the same degree d in $x_0, \ldots, x_n$ we can assume that the polynomials ψ_j's are homogeneous of degree $m - j$ in $g_1, \ldots, g_{n+1}$. Since $j < m$, ψ_j's have positive degree, thus $\psi_j(g_1, \ldots, g_{n+1})$ vanishes whenever g_i's vanish for all $i = 1, \ldots, n+1$. In this case f_{n+2} vanishes by the equality above. It follows from $g_i = f_i + \lambda_i f_{n+2} = 0$ that $f_i = 0$, for all $i = 1, \ldots, n+1$. Therefore we have shown that

$$Z(f_1, \ldots, f_{n+2}) \supseteq Z(g_1, \ldots, g_{n+1}).$$

Conversely if $f_i = 0$, for all $i = 1, \ldots, n+2$ then by $g_i = f_i + \lambda_i f_{n+2}$ we get $g_i = 0$, for all $i = 1, \ldots, n+1$. Hence

$$Z(f_1, \ldots, f_{n+2}) = Z(g_1, \ldots, g_{n+1}).$$

□

Remark 2.4 *Let R be a Noetherian ring and $N = Rad(0)$ be the nilradical ideal of R. If $\overline{R} = R/N$, $\overline{I} = (I + N)/N, \overline{f_i} = f_i + N$ and $Rad(\overline{I}) = Rad(\overline{f_1}, \ldots, \overline{f_n})$ then*

$$Rad(I) = Rad(f_1, \ldots, f_n).$$

Proof: Since $f_i \in I$, it suffices to show that $Rad(I) \subseteq Rad(f_1, \ldots, f_n)$. Take any $h \in Rad(I)$, i.e., $h^r \in I$, for some positive integer r. This implies that

$$h^r + N = (h+N)^r \in \overline{I} \Rightarrow h + N \in Rad(\overline{I}) = Rad(\overline{f_1}, \ldots, \overline{f_n})$$

Then by the definition of a radical ideal we have

$$h^s + N \in (\overline{f_1}, \ldots, \overline{f_n}) = (f_1 + N, \ldots, f_n + N)$$

for some positive integer s. It means that

$$h^s + N = (k_1 + N)(f_1 + N) + \ldots + (k_n + N)(f_n + N)$$

where $k_i \in R$. By the multiplication and summation in R/N we have

$$h^s + N = (\sum_{i=1}^{n} k_i f_i) + N$$

which means that

$$h^s - (\sum_{i=1}^{n} k_i f_i) \in N.$$

Thus we have

$$(h^s - \sum_{i=1}^{n} k_i f_i)^t = 0$$

for some positive integer t. By Binomial expansion we have the following

$$h^{st} - \sum_{i=1}^{n} k_i' f_i = 0$$

where $k_i' \in R$. Thus we end up with

$$h^{st} = \sum_{i=1}^{n} k_i' f_i \in (f_1, ..., f_n) \Rightarrow h \in Rad(f_1, ..., f_n)$$

$\square$

Proposition 2.5 ([16], Prop.1.5, page41) *Let S be a reduced ring with only finitely many minimal prime ideals and let $dim S = 0$. Then S is isomorphic to a finite direct product of fields.*

Proof: Let $\wp_1, ..., \wp_k$ be the minimal prime ideals of S. If $dimS = 0$, then there is no prime ideal other than those. Thus they are maximal ideals and therefore also pairwise relatively prime i.e. $\wp_i + \wp_j = S$, for all $i \neq j$. Chinese Remainder Theorem [[16], Prop.1.7, page41] tells us that if $\wp_1, ..., \wp_k$ are pairwise relatively prime ideals of S then the canonical ring homomorphism

$$\varphi : S \longrightarrow S/\wp_1 \times ... \times S/\wp_k$$

is onto and its kernel is

$$Ker(\varphi) = \bigcap_{i=1}^{k} \wp_i.$$

Since S is reduced, we have

$$N = \bigcap_{i=1}^{k} \wp_i = (0).$$

Thus φ is injective and S is isomorphic to $S/\wp_1 \times ... \times S/\wp_k$ where $S/\wp_i$'s are fields, since $\wp_i$'s are maximal ideals. $\square$

Proposition 2.6 ([16], Lemma1.1, page 123) *Let S be a commutative ring with identity which is isomorphic to a finite direct product of commutative rings with identity $S_1 \times ... \times S_k$. Then S is a Principal Ideal Domain $\Leftrightarrow$ each S_i in the product is a Principal Ideal Domain.*

Proof: Any ideal I of S is of the form $I = I_1 \times ... \times I_k$ where each I_i is the image of I in the ring S_i. $I_i = (f_i) \Leftrightarrow I = (f_1, ..., f_k)$. $\square$

Let us give the following two very well known propositions for completeness:

Proposition 2.7 *Let S be a reduced ring and $\wp_1, \ldots, \wp_k$ be the minimal prime ideals of S. Let $U = S - \{\bigcup_{i=1}^{k} \wp_i\}$ and I be an ideal of S. Then $Rad(I_U) = (Rad(I))_U$.*

Proof: By the definition of the localization we have that

$$\begin{aligned} Rad(I_U) &= \{f/u|(f/u)^r \in I_U, r \geq 1\} \\ &= \{f/u|f^r \in I, u^r \in U, r \geq 1\} \end{aligned}$$

and

$$(Rad(I))_U = \{f/u|f^r \in I, u \in U, r \geq 1\}$$

It follows from $u^r \in U \Leftrightarrow u \in U$ and the definitions of the sets that

$$Rad(I_U) = (Rad(I))_U$$

□

Proposition 2.8 *Let $\wp$ be a prime ideal and I, J some ideals in a commutative ring R with identity. If $\wp \supseteq IJ$, then $\wp \supseteq I$ or $\wp \supseteq J$.*

Proof: Take any $y \in J$ and suppose that $\wp \not\supseteq I$, i.e. $\exists x \in I - \wp$. Now consider $xy \in IJ \subseteq \wp$. Since $\wp$ is a prime ideal, $xy \in \wp \Rightarrow x \in \wp$ or $y \in \wp$. By the assumption on x, we must have $y \in \wp$, which means that $J \subseteq \wp$. □

2.2 Affine generalization to Noetherian rings

Forster generalized Kronecker's Theorem 2.1 to Noetherian rings in the affine case. We state and prove Forster's theorem by a modified version of the proof which is given in [9].

Theorem 2.9 (Forster,[8]) *If R is an n dimensional Noetherian ring and I is a radical ideal in R then there exist elements $f_1, \ldots, f_{n+1} \in I$ such that*

$$I = Rad(f_1, \ldots, f_{n+1})$$

Proof: [[9], page218] We will prove this by using induction on n. Let $n = 0$ and N be the nilradical ideal of R then R/N is a reduced ring. It follows from Proposition 2.5 and Proposition 2.6 that R/N is a principal ideal domain, so there exist $f \in R$ such that $(I+N)/N = (f+N)$. By Remark 2.4, we get $I = Rad(f)$.

Now let $n > 0$ and $\wp_1, ..., \wp_k$ be the minimal prime ideals of R. They are finitely many because in a noetherian ring every proper ideal J is the intersection of finitely many primary ideals $Q_i, i = 1, \ldots, k$, by Theorem 2.17 in [16]. Since radical of a primary ideal is a prime ideal we get that

$$Rad(J) = \bigcap_{i=1}^{k} Rad(Q_i) = \bigcap_{i=1}^{k} \wp_i.$$

Radical of an ideal J is the intersection of minimal prime ideals that contains J, so minimal prime ideals cannot be infinitely many, which can be seen for example by taking $J = (0)$.

Consider the set

$$U = S - \bigcup_{i=1}^{k} \wp_i.$$

Clearly U is a multiplicatively closed set, since $1 \in U$ and $a, b \in U$ implies that $ab \in U$ because of the primeness of $\wp_i$'s. Thus $\wp_i$'s are the maximal ideals of R_U. Therefore R_U is zero dimensional and by the zero dimensional case there exist $f_1 \in R$ such that $I_U = Rad((f_1)_U)$ in R_U. By using Proposition 2.7, we get $I_U = (Rad(f_1))_U$. Since R is a Noetherian ring, I is finitely generated. If $h_1, ..., h_m$ are generators of I, then $h_i \in I$ implies that $h_i/1 \in I_U = (Rad(f_1))_U$. Thus there exist some $u_i \in U$ such that $u_i h_i \in Rad(f_1), i = 1, ..., m$.

Let $u = u_1 ... u_m$. Then $u \in U$, since U is multiplicatively closed. Hence we have

$$uI \subseteq Rad(f_1).$$

Since $u \in U$, no $\wp_i$ contains u, for $i = 1, ..., k$, thus we have $(u) \not\subseteq \wp_i$. Therefore in $R/(u)$, no ideal chain contains prime ideals $\wp_i$, which implies that

$$dim R/(u) \leq n - 1.$$

Let $R^* = R/(u)$ and $I^* = (I + (u))/(u)$. By the induction hypothesis there exist $f_2^*, ..., f_{n+1}^* \in I^*$ such that $I^* = Rad(f_2^*, ..., f_{n+1}^*)$ in R^*. Let $f_2, ..., f_{n+1} \in R$ such that $f_i^* = f_i + (u)$, for all $i = 2, ..., n+1$.

We claim that $I \subseteq Rad(f_1, ..., f_{n+1})$. Since we have

$$I = \bigcap_{\wp \supset I} \wp$$

and

$$Rad(f_1, ..., f_{n+1}) = \bigcap_{\wp \supset (f_1, ..., f_{n+1})} \wp$$

to prove our claim it suffices to show that if $\wp$ is any prime ideal of R such that $\wp \supseteq (f_1, ..., f_{n+1})$ then $\wp \supseteq I$. Since $\wp \supseteq (f_1, ..., f_{n+1}) \supseteq (f_1)$ we have $\wp \supseteq Rad(f_1) \supseteq uI$. By Proposition 2.8, either $\wp \supseteq (u)$ or $\wp \supseteq I$.

In the first case $\wp \supseteq (u)$, $\wp^* = \wp/(u)$ is a prime ideal and $\wp \supseteq (f_1, ..., f_{n+1})$ implies that

$$\wp^* \supseteq (f_2, ..., f_{n+1})/(u) = (f_2^*, ..., f_{n+1}^*)$$

from which follows that

$$\wp^* \supseteq Rad(f_2^*, ..., f_{n+1}^*) = I^*.$$

Thus in this case

$$(\wp + (u))/(u) = \wp/(u) = \wp^* \supseteq I^* = (I + (u))/(u)$$

which implies that $\wp \supseteq I$.

Therefore in both cases we show that $\wp \supseteq I$. Thus we have proved that $I \subseteq Rad(f_1, ..., f_{n+1})$. Since $f_1, \ldots, f_{n+1} \in I$ it follows that $Rad(f_1, ..., f_{n+1}) \subseteq I$. Hence $I = Rad(f_1, ..., f_{n+1})$. $\square$

2.3 Eisenbud and Evans' Theorem for affine n space

Theorem 2.10 (Eisenbud and Evans [7]) *Let $R = S[x]$ be a polynomial ring for some Noetherian ring S of dimension $n-1$ and I be an ideal of R. Then there exist n elements $g_1, \ldots, g_n \in I$ such that $Rad(I) = Rad(g_1, ..., g_n)$.*

Proof: We will prove the theorem by induction on $n = dimR$. So first assume that $n = 1$, which means that $dimS = 0$. Let N be the nilradical ideal of S, then S/N is reduced and it follows from Proposition 2.5 that

$$S/N \cong S_1 \times ... \times S_k$$

for some fields S_i, where $i = 1, ..., k$. Since S_i's are fields, $S_i[x]$'s are PID.

Proposition 2.6 implies that $R/N = S/N[x] \cong S_1[x] \times ... \times S_n[x]$ is a PID. Hence there exist $g \in I \subseteq R$ such that $(I+N)/N = (g+N)$. Therefore $Rad(I) = Rad(g)$, by Remark 2.4.

Now assume that $n > 1$. Let $\wp_1, ..., \wp_k$ be the minimal prime ideals of S and let

$$U = S - \bigcup_{i=1}^{k} \wp_i$$

Since the minimal prime ideals $\wp_i$'s are also maximal, the dimension of S_U is zero, hence the dimension of R_U is one. By the one dimensional case there exist $g_1 \in I$ such that $Rad(I_U) = Rad((g_1)_U)$ in R_U. By using Proposition 2.7 we get $(Rad(I))_U = (Rad(g_1))_U$.

Since every ideal in a Noetherian ring is finetely generated, I is a finitely generated ideal of R. Let $h_1, ..., h_m$ be the generators of I. Then $h_i \in Rad(I)$, which implies that $h_i/1 \in (Rad(I))_U = (Rad(g_1))_U$. Thus there exist some $u_i \in U$ such that $u_i h_i \in Rad(g_1)$, for all $i = 1, ..., m$.

Let $u = u_1...u_m$. Then $u \in U$, since U is multiplicatively closed. Thus we have that

$$uI \subseteq Rad(g_1).$$

Since $u \in U$, no $\wp_i$ contains u, for all $i = 1, ..., k$. Hence we have $(u) \nsubseteq \wp_i$. Therefore in $R/(u)$, no ideal chain contains prime ideals $\wp_i$, which implies that

$$dim R/(u) \leq n - 1.$$

Let $R^* = R/(u)$ and $I^* = I + (u)/(u)$. By the induction hypothesis there exist $g_2^*, ..., g_n^* \in I^*$ such that $Rad(I^*) = Rad(g_2^*, ..., g_n^*)$ in R^*. Let $g_2, ..., g_n \in I$ such that $g_i^* = g_i + (u)$, for all $i = 2, ..., n$.

We claim that $Rad(I) \subseteq Rad(g_1, ..., g_n)$. Since we have

$$Rad(I) = \bigcap_{\wp \supset I} \wp$$

and

$$Rad(g_1, ..., g_n) = \bigcap_{\wp \supset (g_1, ..., g_n)} \wp.$$

To prove our claim it suffices to show that if $\wp$ is any prime ideal of R such that $\wp \supseteq (g_1, ..., g_n)$ then $\wp \supseteq I$. Since $\wp \supseteq (g_1, ..., g_n) \supseteq (g_1)$ we have that

$$\wp \supseteq Rad(g_1) \supseteq uI.$$

By Proposition 2.8, either $\wp \supseteq (u)$ or $\wp \supseteq I$.

In the first case $\wp \supseteq (u)$, $\wp^* = \wp/(u)$ is a prime ideal and $\wp \supseteq (g_1, ..., g_n)$ implies that

$$\wp^* \supseteq (g_2, ..., g_n)/(u) = (g_2^*, ..., g_n^*).$$

It follows that

$$\wp^* \supseteq Rad(g_2^*, ..., g_n^*) = Rad(I^*) \supseteq I^*.$$

Thus in this case

$$\wp + (u)/(u) = \wp/(u) = \wp^* \supseteq I^* = I + (u)/(u)$$

which implies that $\wp \supseteq I$.

Therefore in both cases we show that $\wp \supseteq I$. Thus we have proven that $Rad(I) \subseteq Rad(g_1, ..., g_n)$. Since $g_1, \ldots, g_n \in I$ we have $Rad(g_1, ..., g_n) \subseteq Rad(I)$. Hence $Rad(I) = Rad(g_1, ..., g_n)$. □

Corollary 2.11 *Every algebraic set in $\mathbb{A}^n$ can be generated by n polynomials set theoretically.*

Proof: Let k be an algebraically closed field and $S = k[x_1, \ldots, x_{n-1}]$ be the polynomial ring of dimension $n-1$. Let $R = S[x_n]$ and Y be an algebraic set in $\mathbb{A}^n$. By using Theorem 2.10 above, for the ideal $I(Y)$, we get $g_1, \ldots, g_n \in I(Y)$ so that $Rad(I(Y)) = Rad(g_1, \ldots, g_n)$. Therefore we have that

$$Y = Z(I(Y)) = Z(g_1, \ldots, g_n).$$

□

2.4 Eisenbud and Evans' Theorem for projective n space

Let $S = \sum_{i \geq 0} S^{(i)}$ and $S^+ = \sum_{i>0} S^{(i)}$. We assume that S^+ is generated by $S^{(1)}$. **Relevant** prime ideals are prime ideals which do not contain the **irrelevant** prime ideal S^+ of S. **Projective dimension** of S is the length of a maximal chain of relevant prime ideals of S. Note that if S is a noetherian graded ring of projective dimension $n-1$, then the projective dimension of $S[x]$ is greater than or equal to n. For projective analogue of Eisenbud and Evans' theorem we need to give a lemma about division of polynomials.

Lemma 2.12 (Eisenbud and Evans, [7]) *Let S be a ring and $f, g \in S[x]$ some polynomials having degrees d and e respectively, with $d \leq e$. If $u \in S$ is the leading coefficient of f, then for all $N > e - d$ there exist polynomials h and r such that*

$$u^N g = fh + r$$

and the degree of r in x is less than d. Moreover, if S is a graded ring and f and g are homogeneous polynomials then h and r can be chosen homogeneous as well.

Theorem 2.13 (Eisenbud and Evans, [7]) *Let $R = S[x]$ be a graded polynomial ring for some noetherian graded ring S of projective dimension $n - 1$. If $I \subset S^+R$ is a homogeneous ideal then there exist homogeneous elements $g_1, \ldots, g_n \in I$ such that $Rad(I) = Rad(g_1, \ldots, g_n)$.*

Proof: The proof goes by induction on n, as in the proof of Theorem 2.10.

If $n = 0$, S^+ is the nilpotent ideal of S, since $Rad(0)$ is a prime ideal and there is no relevant prime ideal in S, so $S^+ \subseteq Rad(0)$. The converse is always the case. Thus $Rad(I)$ is the nilradical of R which is the radical of the ideal (0), generated by the empty set of elements.

If $n > 0$, then assume that $P_1, \ldots, P_k$ are the minimal relevant prime ideals of S. We will show that there exist elements $u \in S^+$ and $g_1 \in I$ such that $u \notin \bigcup_{i=1}^k P_i$ and

$$uI \subseteq Rad(g_1).$$

For this let us define for all $i = 1, \ldots, k$

$$I_i = (I + P_iR)/P_iR \subseteq R/P_iR.$$

For $h_i \in I$, let $h_i^* \in I_i$ be a homogeneous polynomial having the lowest possible degree in x such that $h_i = h_i^* + P_iR$, for all $i = 1, \ldots, k$. Choose a homogeneous element, $s_i \in S$ such that

$$s_i \in (\bigcup_{j=1}^{k} P_j) - P_i$$

and choose $s \in S^{(1)} - \bigcup_{i=1}^{k} P_i$; here we must show that $S^{(1)} - \bigcup_{i=1}^{k} P_i \neq \emptyset$, if it is empty, then $S^{(1)} \subseteq \bigcup_{i=1}^{k} P_i$ which implies that $S^{+} \subseteq (\bigcup_{i=1}^{k} P_i) \bigcup (\sum_{i>1} S^{(i)})$. This gives a contradiction $S^{+} \subseteq P_i$, for some i. If $h_i^* = 0$ then choose $u_i \in S^{+}$ to be any homogeneous element such that $u_i \notin P_i$. If $h_i^* \neq 0$ and u_i^* is the leading coefficient of h_i^* then choose $u_i \in S^{+}$ to be a homogeneous element such that $u_i = u_i^* + P_i$. Multiplying each h_i, u_i and s_i by a suitable power of s we can assume that for all i and j,

$$deg(h_i) = deg(h_j)$$

$$deg(u_i) = deg(u_j)$$

$$deg(s_i) = deg(s_j).$$

Let $g_1 = \sum_{i=1}^{k} s_i h_i$ and $u = (s(\sum_{i=1}^{k} s_i u_i))^N$ where N is sufficiently large. Clearly $u \in S^{+}$ since $u_i \in S^{+}$. Since P_i is a prime ideal, $s_i \notin P_i$ and $u_i \notin P_i$ implies that $s_i u_i \notin P_i$. Thus

$$(\sum_{i=1}^{k} s_i u_i) \notin \bigcup_{i=1}^{k} P_i$$

on the other hand $s \notin \bigcup_{i=1}^{k} P_i$ hence

$$u \notin \bigcup_{i=1}^{k} P_i.$$

We claim that $uI \subseteq Rad(g_1)$; to see this let us fix i and define the following:

$$g_1 = g_1^* + P_i R$$

$$u = u^* + P_i R$$

$$s_i = s_i^* + P_i R$$

then $g_1^* \in I_i$ is $s_i^* h_i^*$ since it is the image of g_1 in $R/P_i R$, i.e.

$$g_1 = \sum_{i=1}^{k} s_i h_i = \sum_{i=1}^{k} (s_i^* h_i^* + P_i R)$$

Therefore the degree of g_1^* is the minimal among the degrees in x of elements of I_i. By definition of u,

$$u = (s(\sum_{i=1}^{k} s_i u_i))^N = (s^* + P_i R)^N (\sum_{i=1}^{k} s_i^* u_i^* + P_i R)^N.$$

We have that $u^* = (s^*)^N (s_i^* u_i^*)^N$ is a multiple of a large power of the leading coefficient $s_i^* u_i^*$ of g_1^*, thus by Lemma 2.12 we get $u^* k = l g_1^* + r$, for all $k \in I_i$ with the degree of r in x is less than the degree of g_1^* in x. So $r = 0$, since degree of g_1^* is the minimal. Therefore we conclude that $u^* I_i \subseteq (g_1^*)$. Because $u \in S^+$ it follows that $uI \subseteq S^+ R$. On the other hand $u^* I_i \subseteq (g_1^*)$ implies that $uI \subseteq ((g_1) + P_i R)$, for all i, therefore we get

$$uI \subseteq (S^+ R) \bigcap ((g_1) + P_i R). \tag{2.1}$$

Every prime ideal of R contains either $S^+ R$ or some $P_i R$. Let P be any prime ideal of R such that $P \supseteq (g_1)$. If $P \supseteq S^+ R$ then we have $P \supseteq uI$ by Equation 2.1. If $P \supseteq P_i R$, for some i, then we have $P \supseteq uI$ again by Equation 2.1. So $P \supseteq (g_1)$ implies that $P \supseteq uI$ which means that $uI \subseteq Rad(g_1)$ as desired. □

Corollary 2.14 *Every algebraic set in $\mathbb{P}^n$ can be generated by n homogeneous polynomials set theoretically.*

Proof: Let k be an algebraically closed field and $S = k[x_0, \ldots, x_{n-1}]$ be the homogeneous polynomial ring of projective dimension $n - 1$. Let $R = S[x_n]$ and Y be an algebraic set in $\mathbb{P}^n$. Without loss of generality we may assume that $[0 : \cdots : 0 : 1] \in Y \subset \mathbb{P}^n$. Then $I(Y) \subseteq S^+ R = (x_0, \ldots, x_{n-1})$. By using Theorem 2.13 above, for the ideal $I(Y)$, we get $g_1, \ldots, g_n \in I(Y)$ so that $Rad(I(Y)) = Rad(g_1, \ldots, g_n)$. Therefore we have that

$$Y = Z(I(Y)) = Z(g_1, \ldots, g_n)$$

□

3

Monomial Curves that are complete intersection

3.1 Introduction and monomial curves

In this chapter we will prove that all monomial space curves in $\mathbb{A}^3$ are set theoretic complete intersection of two surfaces [3]. This gives a partial answer to the well known question of whether every monomial curve in $\mathbb{A}^n$ is a set theoretic complete intersection.

Later we will give an example of a monomial curve which is a set theoretic complete intersection in $\mathbb{A}^4$.

Let us first define affine monomial curves in $\mathbb{A}^n$ and then prove that all affine monomial space curves are set theoretic complete intersection in the next section.

Definition 3.1 *Let k be a field of characteristic zero and $m_1 < \ldots < m_n$ be positive integers such that $gcd(m_1, \ldots, m_n) = 1$. An affine monomial curve $C =$*

$C(m_1, \ldots, m_n)$ in $\mathbb{A}^n$ is given parametrically by

$$x_1 = t^{m_1}$$
$$x_2 = t^{m_2}$$
$$\vdots$$
$$x_n = t^{m_n}$$

where t is an element of the ground field k.

3.2 All monomial space curves are complete intersection set theoretically

By [12], the prime ideal $I(C) \subseteq k[x_1, x_2, x_3]$ corresponding the monomial space curve $C = C(n_1, n_2, n_3)$ is given by

$$I(C) = (f_1 = x_1^{m_1} - x_2^{m_{12}} x_3^{m_{13}}, f_2 = x_2^{m_2} - {x_1}^{m_{21}} x_3^{m_{23}}, f_3 = x_3^{m_3} - x_1^{m_{31}} x_2^{m_{32}})$$

where all components are positive integer satisfying the following relations

$$m_1 = m_{21} + m_{31}$$
$$m_2 = m_{12} + m_{32}$$
$$m_3 = m_{13} + m_{23}.$$

Lemma 3.2 (Bresinsky,[3]) $J = (f_1, f_2, f_3) \bigcap (x_1^{m_{21}}, x_2^{m_{12}}) = (f_1, f_2, x_1^{m_{21}} f_3, x_2^{m_{12}} f_3)$

Proof: $\supseteq$ is trivial as

$$f_1, f_2, x_1^{m_{21}} f_3, x_2^{m_{12}} f_3 \in (f_1, f_2, f_3)$$

and

$$x_1^{m_{21}} f_3, x_2^{m_{12}} f_3 \in (x_1^{m_{21}}, x_2^{m_{12}}).$$

So we only need to show that $f_1, f_2 \in (x_1^{m_{21}}, x_2^{m_{12}})$ but these are evident from the following equalities

$$\begin{aligned} f_1 = x_1^{m_1} - x_2^{m_{12}} x_3^{m_{13}} &= x_1^{m_{21}} x_1^{m_{31}} - x_2^{m_{12}} x_3^{m_{13}} \in (x_1^{m_{21}}, x_2^{m_{12}}) \\ f_2 = x_2^{m_2} - x_1^{m_{21}} x_3^{m_{23}} &= x_2^{m_{12}} x_2^{m_{32}} - x_1^{m_{21}} x_3^{m_{23}} \in (x_1^{m_{21}}, x_2^{m_{12}}). \end{aligned}$$

For the converse inclusion consider the polynomial

$$f = \sum_{i=1}^{3} g_i f_i \in I$$

then

$$g_3 f_3 \in (x_1^{m_{21}}, x_2^{m_{12}})$$

since f_1 and f_2 are already in $(x_1^{m_{21}}, x_2^{m_{12}})$. It is easy to see that $(x_1^{m_{21}}, x_2^{m_{12}})$ is irreducible and primary. Since f_3 is not in

$$(x_1, x_2) = Rad(x_1^{m_{21}}, x_2^{m_{12}})$$

by the definition of primary ideal g_3 must be in the ideal $(x_1^{m_{21}}, x_2^{m_{12}})$, which implies that

$$g_3 = p_1 x_1^{m_{21}} + p_2 x_2^{m_{12}}$$

where $p_1, p_2 \in k[x_1, x_2, x_3]$.

Hence

$$f = \sum_{i=1}^{3} g_i f_i = g_1 f_1 + g_2 f_2 + (p_1 x_1^{m_{21}} + p_2 x_2^{m_{12}}) f_3 \in (f_1, f_2, x_1^{m_{21}} f_3, x_2^{m_{12}} f_3).$$

□

Lemma 3.3 (Bresinsky,[3]) *We have* $(f_1, f_2, x_1^{m_{21}} f_3, x_2^{m_{12}} f_3) = (f_1, f_2)$

Proof: $\supseteq$ is trivial. $\subseteq$ can be deduced by the equalities

$$x_1^{m_{21}} f_3 = -x_2^{m_{32}} f_1 - x_3^{m_{12}} f_2,$$

$$x_2^{m_{12}} f_3 = -x_1^{m_{31}} f_2 - x_3^{m_{23}} f_1.$$

□

Corollary 3.4 *$Z(f_1, f_2) = C \bigcup L$, where the line L is the x_3 -axis.*

Proof: It follows from Lemma 3.2 and Lemma 3.3 that $J = (f_1, f_2)$ thus $Z(f_1, f_2) = Z(J) = Z(f_1, f_2, f_3) \bigcup Z(x_1, x_2) = C \bigcup L$. □

Indeed we can prove Corollary 3.4 directly as follows:

Proof of Corollary 3.4: Take a point $p = (a, b, c) \in Z(f_1, f_2)$. We may have two cases, either $a = 0$ or not. If $a = 0$ then $b = 0$ by $f_2(p) = 0$. Hence $p = (0, 0, c) \in L$.

If $a \neq 0$ then $b \neq 0$ and $c \neq 0$ by $f_1(p) = 0$. Hence a,b and c are all nonzero which follows that

$$f_1(p) = 0 \Rightarrow a^{m_1} = b^{m_{12}} c^{m_{13}} \Rightarrow c^{m_{13}} = a^{m_1} b^{-m_{12}}$$

$$f_2(p) = 0 \Rightarrow b^{m_2} = a^{m_{21}} c^{m_{23}} \Rightarrow c^{m_{23}} = a^{-m_{21}} b^{m_2}$$

Therefore we get

$$c^{m_3} = c^{m_{13}} c^{m_{23}} = a^{m_1 - m_{21}} b^{m_2 - m_{12}} = a^{m_{31}} b^{m_{23}}$$

which means that $f_3(p) = 0$, i.e. , $p \in C$. □

Theorem 3.5 (Bresinsky, [3]) *If $g \in I(C)$ such that $f_2 \in Rad(g, f_1)$ and $g = \pm x_3^{\alpha} + h$, where $h \in (x_1, x_2)$ and α is a positive integer, then $C = Z(g, f_1)$.*

Proof: It is immediate from $(g, f_1) \subseteq I(C)$ that

$$C = Z(I(C)) \subseteq Z(g, f_1).$$

For the converse, we take a point $p = (a, b, c) \in Z(g, f_1)$ and show that $p \in C$. Either $a = 0$ or $a \neq 0$. In the first case $a = 0$, we get $b = 0$ and $c = 0$, from $f_2(p) = 0$ and $g(p) = 0$, respectively. So $p = (0, 0, 0) \in C$ in this case. In the second case if we assume that $b = 0$ or $c = 0$ then we get $a = 0$, by $f_1(p) = 0$, which is a contradiction. So a, b and c are all nonzero in the second case. Consider the following facts

$$f_1(p) = 0 \Rightarrow a^{m_1} = b^{m_{12}} c^{m_{13}} \Rightarrow c^{m_{13}} = a^{m_1} b^{-m_{12}},$$

$$f_2(p) = 0 \Rightarrow b^{m_2} = a^{m_{21}} c^{m_{23}} \Rightarrow c^{m_{23}} = a^{-m_{21}} b^{m_2}.$$

Therefore we get

$$c^{m_3} = c^{m_{13}} c^{m_{23}} = a^{m_1 - m_{21}} b^{m_2 - m_{12}} = a^{m_{31}} b^{m_{23}}$$

which means that $f_3(p) = 0$, i.e. $p \in C$. $\square$

According to above Theorem 3.5, to show that C is the set theoretic complete intersection of the surfaces $g = 0$ and $f_1 = 0$, the only thing we need is to construct a polynomial $g \in I(C)$ such that $f_2 \in Rad(g, f_1)$ and $g = \pm x_3^{\alpha} + h$ where $h \in (x_1, x_2)$. To construct such a polynomial g we first take

$$f_2^{m_1} = (x_2^{m_2} - x_1^{m_{21}} x_3^{m_{23}})^{m_1} = x_2^{m_2} k \pm x_1^{m_{21} m_1} x_3^{m_{23} m_1}$$

where $k \in (x_1, x_2)$, and then subtract or add

$$x_1^{m_{21} m_1} x_3^{m_{23} m_1} f_1 = x_1^{m_1 m_{21}} x_3^{m_1 m_{23}} - x_1^{m_1 (m_{21} - 1)} x_2^{m_{12}} x_3^{m_{13} + m_1 m_{23}},$$

and lastly divide by $x_2^{m_{12}}$. At the end we get a polynomial

$$g = x_2^{m_{32}} k \pm x_1^{m_1 (m_{21} - 1)} x_3^{m_{13} + m_1 m_{23}}.$$

Note that if $m_{21} = 1$ then

$$g = x_2^{m_{32}} k \pm x_3^{m_{13} + m_1 m_{23}} = \pm x_3^{\alpha} + h$$

where $h \in (x_1, x_2)$ and $\alpha = m_{13} + m_1 m_{23}$. If $m_{21} \neq 1$ we will show that the process, i.e. subtracting or adding proper multiples of f_1 and dividing by $x_2^{m_{12}}$, can be carried through m_{21} times. Let $\hookrightarrow$ denote a change of a term by subtracting or adding proper multiples of f_1 .

Proposition 3.6 *If we apply $\hookrightarrow$ to the term $x_1^a x_2^b x_3^c$,n times , this term turns into the form $x_1^{a-nm_1} x_2^{b+nm_{12}} x_3^{c+nm_{13}}$.*

Proof: Let us prove it by induction. For $n = 1$ we have the following

$$x_1^a x_2^b x_3^c - x_1^{a-m_1} x_2^b x_3^c (x_1^{m_1} - x_2^{m_{12}} x_3^{m_{13}}) = x_1^{a-m_1} x_2^{b+m_{12}} x_3^{c+m_{13}}.$$

Suppose that the proposition is true for $n-1$ and applying $\hookrightarrow$ one times more we'll show that it is also true for n. Assume that we get the term

$$x_1^{a-(n-1)m_1} x_2^{b+(n-1)m_{12}} x_3^{c+(n-1)m_{13}}$$

after applying $\hookrightarrow$ to $x_1^a x_2^b x_3^c$, $(n-1)$ times. Subtracting

$$x_1^{a-nm_1} x_2^{b+(n-1)m_{12}} x_3^{c+(n-1)m_{13}} f_1$$

from the above term we get that

$$x_1^{a-nm_1} x_2^{b+nm_{12}} x_3^{c+nm_{13}}.$$

□

By binomial theorem we have the following

$$f_2^{m_1} = (x_2^{m_2} - x_1^{m_{21}} x_3^{m_{23}})^{m_1} = \sum_{j=0}^{m_1} (-1)^j \begin{pmatrix} m_1 \\ j \end{pmatrix} x_1^{(m_1-j)m_{21}} x_2^{jm_2} x_3^{(m_1-j)m_{23}}.$$

The terms of this expansion can be made divisible by $x_2^{m_{12}}$, m_{21} times, as follows:

For j=0, $x_1^{m_1 m_{21}} x_3^{m_1 m_{23}}$ turns into $x_2^{m_{21} m_{12}} x_3^{m_1 m_{23} + m_{21} m_{13}}$ after applying $\hookrightarrow$ m_{21} times by the Proposition 3.6.

For $j = m_{21}$ the term

$$x_1^{m_{21} m_{31}} x_2^{m_2 m_{21}} x_3^{m_{23} m_{31}} = x_1^{m_{21} m_{31}} x_2^{m_{12} m_{21}} x_2^{m_{32} m_{21}} x_3^{m_{23} m_{31}}$$

is already divisible by $x_2^{m_{12}}$, m_{21} times.

For $1 \leq j \leq m_{21} - 1$ the term

$$x_1^{(m_1-j)m_{21}} x_2^{jm_2} x_3^{(m_1-j)m_{23}}$$

turns into the form

$$x_1^{(m_1-j)m_{21}-(m_{21}-1)m_1} x_2^{jm_2+(m_{21}-1)m_{12}} x_3^{(m_1-j)m_{23}+(m_{21}-1)m_{13}}$$

after applying $\hookrightarrow$ $(m_{21} - 1)$ times by the Proposition 3.6.

Therefore we construct a polynomial

$$g_0 = x_2^{m_{21}m_{12}} x_3^{m_1 m_{23}+m_{21}m_{13}} + h_0$$

after applying $\hookrightarrow$ to $f_2^{m_1}$, m_{21} times, where $h_0 \in (x_1, x_2)$ is divisible by $x_2^{m_{12}}$, m_{21} times. If we divide g_0 by $x_2^{m_{12}}$, m_{21} times, then we get another polynomial

$$g = x_3^{m_1 m_{23}+m_{21}m_{13}} + h$$

where $h \in (x_1, x_2)$.

Hence we have just constructed a polynomial g which is needed in the statement of the Theorem 3.5 to show that C is the set theoretic complete intersection of the surfaces $g = 0$ and $f_1 = 0$. This construction provides the existence of such a polynomial g for all monomial space curves.

Let us give some examples to see concrete surfaces whose set theoretic complete intersections are those monomial space curves given first. These examples are given to make more clear all steps in the proof of the Theorem 3.5.

Examples

(i) The affine twisted cubic

The simplest example of a set theoretic complete intersection is the well known affine twisted cubic curve $C = C(1,2,3)$ given parametrically by

$$x_1 = t^1$$

$$x_2 = t^2$$

$$x_3 = t^3$$

where $t \in k$. By the computer program Macaulay [10] we get ideal of C as

$$I(C) = (f_1 = x_1^2 - x_2, f_2 = x_2^2 - x_1x_3, f_3 = x_3 - x_1x_2)$$

Let us first find a representation of the twisted cubic being complete intersection set theoretically, by using the idea in the proof of the Theorem 3.5 as follows:

$$f_2^2 = (x_2^2 - x_1x_3)^2 = x_2^4 - 2x_1x_2^2x^3 + x_1^2x_3^2$$

If we subtract

$$x_3^2f_1 = x_1^2x_3^2 - x_2x_3^2$$

from f_2^2 and divide by x_2, we get the polynomial

$$g = x_3^2 + x_2^3 - 2x_1x_2x_3.$$

It is easy to see that $f_3^2 = g + x_2^2f_1$ and $f_2^2 = x_2g + x_3^2f_1$, hence, the affine twisted cubic curve is the set theoretic complete intersection of the surfaces

$$f_1 = x_1^2 - x_2 = 0$$

and

$$g = x_3^2 + x_2^3 - 2x_1x_2x_3 = 0.$$

Now let us show that the affine twisted cubic curve is indeed an ideal theoretic complete intersection, that is, $I(C) = (f_1 = x_1^2 - x_2, f_3 = x_3 - x_1x_2)$. It suffices to prove that $I(C) \subset (f_1 = x_1^2 - x_2, f_3 = x_3 - x_1x_2)$, since the converse is already true. This is evident from the following relation

$$f_2 = -x_2 f_1 - x_1 f_3 \in (f_1, f_3).$$

Hence the affine twisted cubic curve is a complete intersection ideal theoretically but it is proved in the last chapter that the projective twisted cubic is not.

(ii) C=C(2,3,5)

This example illustrates all steps in the proof of the Theorem 3.5. We know from the computer program Macaulay [10] that the ideal corresponding this curve can be generated by the following polynomials :

$$f_1 = x_1^3 - x_2^2$$
$$f_2 = x_2^3 - x_1^2 x_3$$
$$f_3 = x_3 - x_1 x_2.$$

By using the same idea as in the proof of the Theorem 3.5 we consider the following

$$f_2^3 = (x_2^3 - x_1^2 x_3)^3 = x_2^9 - 3x_1^2 x_2^6 x_3 + 3x_1^4 x_2^3 x_3^2 - x_1^6 x_3^3.$$

By adding

$$x_1^3 x_3^3 f_1$$

to f_2^3 and dividing by x_2^2 we get the following

$$x_2^7 - 3x_1^2 x_2^4 x_3 + 3x_1^4 x_2 x_3^2 - x_1^3 x_3^3.$$

Similarly by adding $x_3^3 f_1$ to the above equation we get

$$x_2^7 - 3x_1^2x_2^4x_3 + 3x_1^4x_2x_3^2 - x_2^2x_3^3.$$

It can easily be seen that the third term of the above equation is not divisible by x_2^2, to make it divisible by x_2^2 we subtract

$$3x_1x_2x_3^2f_1$$

hence we get

$$x_2^7 - 3x_1^2x_2^4x_3 + 3x_1x_2^3x_3^2 - x_2^2x_3^3.$$

Finally dividing the last equation by x_2^2 we get the polynomial

$$g = x_2^5 - 3x_1^2x_2^2x_3 + 3x_1x_2x_3^2 - x_3^3.$$

Therefore C is the set theoretic complete intersection of the surfaces

$$f_1 = x_1^3 - x_2^2 = 0$$

and

$$g = x_2^5 - 3x_1^2x_2^2x_3 + 3x_1x_2x_3^2 - x_3^3.$$

3.3 Set theoretical complete intersections in $\mathbb{A}^4$

A *semigroup* S is a set with an associative law of composition and with an identity element. But elements of S are not required to have inverses. The semigroup generated by $n_1, n_2, n_3, n_4 \in \mathbb{N} = \{0, 1, 2, \ldots\}$ is denoted by $< n_1, n_2, n_3, n_4 >$

and defined as follows

$$< n_1, n_2, n_3, n_4 >= \{\sum_{i=1}^{4} a_i n_i \mid a_i \in \mathbb{N}\}$$

where $\mathbb{N}$ denote the nonnegative integers. Let c be the greatest integer not in S. S is called a *symmetric* semigroup if $c - z \in S$ whenever z is not in S. By using the same idea as in the proof of the Theorem 3.5, Bresinsky [4] shows that if the semigroup

$$< n_1, n_2, n_3, n_4 >$$

is symmetric, then the monomial curve

$$C = C(n_1, n_2, n_3, n_4)$$

is a complete intersection set theoretically. He uses the fact that $I(C)$ is generated by 3 or 5 polynomials [5] to prove that C is a set theoretic complete intersection. Since in the first case $\mu(I(C)) \leq 3$ the curve C is indeed an ideal theoretical complete intersection, he is interested in the second case $\mu(I(C)) \leq 5$ and he showed that $\mu(C) \leq 3$ in any case. We will not give the proof of this theorem, $C(n_1, n_2, n_3, n_4)$ is a set theoretic complete intersection, in the general case but we will cover all steps in the proof by proving it on an example:

Let us consider an irreducible monomial curve $C = C(5, 6, 7, 8)$. It can be found that the generators of the prime ideal $I(C)$, using the computer program Macaulay as follows

$$I(C) = (f_1 = x_1^3 - x_3x_4, f_2 = x_2^2 - x_1x_3, f_3 = x_3^2 - x_2x_4, f_4 = x_4^2 - x_1^2x_2, f_5 = x_2x_3 - x_1x_4)$$

Lemma 3.7 (Bresinsky, [4]) $f_5 \in Rad(f_1, f_2, f_3, f_4)$.

Proof: It is easy to see that

$$f_5^2 = x_3^2 f_2 + x_1^2 f_4 + x_1x_2 f_1 \in (f_1, f_2, f_4),$$

that is, $f_5 \in Rad(f_1, f_2, f_3, f_4)$. □

Infact $f_5 \in (f_1, f_2, f_4)$ for this example but we need f_3 for other examples.

Corollary 3.8 (Bresinsky, [4]) $I(C) = Rad(f_1, f_2, f_3, f_4)$.

Proof: It is clear that $Rad(f_1, f_2, f_3, f_4) \subseteq (f_1, f_2, f_3, f_4, f_5) = I(C)$. The converse is a direct consequence of Lemma 3.7. □

Let us show that the following fact

$$Rad(f_1, f_2, f_3) = Rad(f_1, f_2, f_3, f_4) \bigcap (x_1, x_2, x_3).$$

This is equivalent to show that

Lemma 3.9 (Bresinsky, [4]) *We have the following*

$$Z(f_1, f_2, f_3) = Z(f_1, f_2, f_3, f_4) \bigcup Z(x_1, x_2, x_3).$$

Proof: $\supseteq$ is obvious. To prove the converse take an element $p = (a, b, c, d) \in Z(f_1, f_2, f_3)$. Either $a = 0$ or not. If $a = 0$ then $b = 0$ by $f_2(p) = 0$ which implies that $c = 0$ by $f_3(p) = 0$ so $p \in Z(x_1, x_2, x_3)$. If $a \neq 0$ then $b \neq 0$ otherwise $c = 0$ by $f_3(p) = 0$ which gives a contradiction $a = 0$ by $f_1(p) = 0$. Since $a \neq 0$, c and d are nonzero by $f_1(p) = 0$. Thus a, b, c and d are all nonzero. The following facts accomplish the proof

$$f_1(p) = 0 \Rightarrow a^3 = cd$$

$$f_2(p) = 0 \Rightarrow b^2 = ac$$

$$f_3(p) = 0 \Rightarrow c^2 = bd.$$

It follows from the first and last equalities that $bcd^2 = a^3c^2$, that is, $bd^2 = a^2(ac)$. From the second equality we get $bd^2 = a^2b^2$ which implies that $d^2 = a^2b$, that is $f_4(p) = 0$ which provide that $p = (a, b, c, d) \in Z(f_1, f_2, f_3, f_4)$. □

Therefore $Z(f_1, f_2, f_3) = C \bigcup L$ where the line L is the x_4 axis. We want to lose L in the union, to do this we should find a new polynomial $g \in I(C)$ such that $g = \mp x_4^{\mu} + h$, where $h \in (x_1, x_2, x_3)$ is a polynomial and μ is a positive integer.

Theorem 3.10 (Bresinsky, [4]) *If $g \in I(C)$ is a polynomial such that $f_2 \in Rad(g, f_1, f_3)$ and $g = \mp x_4^{\mu} + h$, where $h \in (x_1, x_2, x_3)$ is a polynomial and μ is a positive integer, then we have $C = Z(g, f_1, f_3)$.*

Proof: It is clear that $C \subseteq Z(g, f_1, f_3)$. To prove converse, we take any point $p = (a, b, c, d) \in Z(g, f_1, f_3)$. Then $f_2(p) = 0$, since $f_2 \in Rad(g, f_1, f_3)$. Either $a = 0$ or not. If $a = 0$ then $b = 0$ by $f_2(p) = 0$ which implies that $c = 0$ by $f_3(p) = 0$. It follows that $d = 0$, from $g(0, 0, 0, d) = \mp d^{\mu} + h(0, 0, 0) = 0$, where $h \in (x_1, x_2, x_3)$ is a polynomial and μ is a positive integer. So $p = (0, 0, 0, 0) \in C$.

If $a \neq 0$ then $b \neq 0$ otherwise $c = 0$ by $f_3(p) = 0$ which gives a contradiction $a = 0$ by $f_1(p) = 0$. Since $a \neq 0$, c and d are nonzero by $f_1(p) = 0$. Thus a, b, c and d are all nonzero. The following facts accomplish the proof

$$f_1(p) = 0 \Rightarrow a^3 = cd$$

$$f_2(p) = 0 \Rightarrow b^2 = ac$$

$$f_3(p) = 0 \Rightarrow c^2 = bd.$$

It follows from the first and last equalities that $bcd^2 = a^3c^2$, that is, $bd^2 = a^2(ac)$. From the second equality we get $bd^2 = a^2b^2$ which implies that $d^2 = a^2b$, that is $f_4(p) = 0$ which provide that $p = (a, b, c, d) \in Z(f_1, f_2, f_3, f_4) = C$. □

According to above Theorem 3.10 to show that $C(5, 6, 7, 8)$ is a set theoretic complete intersection it suffices to construct such a polynomial g. To construct it consider

$$f_2^3 = x_2^6 - 3x_2^4x_1x_3 + 3x_2^2x_1^2x_3^2 - x_1^3x_3^3$$

by adding $x_3^3 f_1$ to f_2^3 we get

$$x_2^6 - 3x_2^4 x_1 x_3 + 3x_2^2 x_1^2 x_3^2 - x_3^4 x_4$$

again by adding $x_4 f_3^2$ to the above equation we get

$$x_2^6 - 3x_2^4 x_1 x_3 + 3x_2^2 x_1^2 x_3^2 + x_2^2 x_4^3 - 2x_2 x_3^2 x_4^2.$$

We want to get a term consist only of a power of x_4. If we can divide every term by x_2^2 we are done. It can easily be seen in the above expression that the last term is not divisible by x_2^2. To make it divisible let us add $2x_2 x_4^2 f_3$ to the last equation. Hence we have

$$x_2^6 - 3x_2^4 x_1 x_3 + 3x_2^2 x_1^2 x_3^2 - x_2^2 x_4^3.$$

Now we can divide every term by x_2^2 to get

$$g = x_2^4 - 3x_2^2 x_1 x_3 + 3x_1^2 x_3^2 - x_4^3.$$

By the construction of g we have

$$f_2^3 = x_2^2 g - x_3^3 f_1 - x_4 f_3^2 - 2x_2 x_4^2 f_3 \in (g, f_1, f_3)$$

that is, $f_2 \in Rad(g, f_1, f_3)$. Therefore $C = Z(g, f_1, f_3)$, that is, C is the set theoretical complete intersection of the hypersurfaces

$$g = x_2^4 - 3x_2^2 x_1 x_3 + 3x_1^2 x_3^2 - x_4^3 = 0,$$

$$f_1 = x_1^3 - x_3 x_4 = 0$$

and

$$f_3 = x_3^2 - x_2 x_4 = 0.$$

4

Examples for the ideal theoretical case

In this chapter we suggest examples to point out that the minimal number of polynomials generating an algebraic set in an n space is n set theoretically, it may be much larger than n ideal theoretically. We present a theorem of Bresinsky which says that there are some monomial curves in $\mathbb{A}^n$ with $n > 3$, having arbitrary large minimal number of elements to generate their ideal [6]. These examples also show the strength of Eisenbud and Evans' Theorem 2.10 and Theorem 2.13.

Let us first quote the work of Bresinsky [6]. Let $C = C(n_1, n_2, n_3, n_4)$ be the monomial curve defined by

$$n_1 = rs$$
$$n_2 = rd$$
$$n_3 = rs + d$$
$$n_4 = sd$$

where $s \geq 4$ is even integer, $r = s + 1$, $d = s - 1$. Bresinsky shows that we must have s polynomials to generate C ideal theoretically, i.e. $\mu(I(C)) \geq s$. Thus for any integer $s \geq 4$, we can construct a monomial curve whose defining ideal requires at least s generators.

4.1 A monomial curve C in $\mathbb{A}^3$ with $\mu(C) = 2$, $\mu(I(C)) = 3$

In the first chapter we mentioned a result of Murthy which tells us that any prime ideal of height 2 in $k[x_1, x_2, x_3]$, which is a complete intersection locally, that is, in a neighbourhood of any point of the corresponding curve the prime ideal can be generated by 2 polynomials, can be generated by 3 polynomials. The following remark shows that this result is best possible:

Remark 4.1 *A prime ideal of height* 2 *in* $k[x_1, x_2, x_3]$*, which is a complete intersection locally, need not be generated by* 2 *polynomials.*

Proof: In chapter 3, we gave a general proof of the theorem that all monomial space curves are complete intersection set theoretically but now we will show that although the curve C defined below is a complete intersection of 2 surfaces its ideal cannot be generated by 2 polynomials. Let us consider a monomial space curve $C = C(3, 4, 5)$ defined parametrically by

$$x_1 = t^3$$

$$x_2 = t^4$$

$$x_3 = t^5$$

If we define a homomorphism

$$\varphi : k[x_1, x_2, x_3] \longmapsto k[t]$$

$$x_1 = t^3$$

$$x_2 = t^4$$

$$x_3 = t^5$$

then we can easily show that $Ker(\varphi) = I(C)$ is a prime ideal and generated by the following polynomials:

$$f_1 = x_1^3 - x_2x_3$$

$$f_2 = x_2^2 - x_1x_3$$

$$f_3 = x_3^2 - x_1^2x_2$$

by the computer program Macaulay [10].

Let $g = x_1^4 - 2x_1x_2x_3 + x_2^3$ be another polynomial, by following equalities

$$f_1^2 = x_2^2f_3 + x_1^2g$$

$$f_2^2 = x_1^2f_3 + x_2g$$

we get $I(C) \subset Rad(f_3, g)$ so $Z(f_3, g) \subset C$.

Conversely $f_3(t^3, t^4, t^5) = g(t^3, t^4, t^5) = 0$, i.e., $C \subset Z(f_3, g)$. Hence C is the complete intersection of the surfaces $g = 0$ and $f_3 = 0$.

Affine coordinate ring $A(C)$ of the curve C is isomorphic to $k[t]$, since φ is indeed an isomorphism. Hence $dim(C) = dimA(C) = 1$. Since $I(C)$ is prime ideal, C is irreducible and its coordinate ring $A(C)$ is integral domain. For any integral domain D which is a finitely generated k-algebra we have

$$dim(D) = dim(D/P) + height(P)$$

Hence $height(I(C)) = 2$ by $dim(k[x_1, x_2, x_3]) = 3$. Let us show that $I(C)$ cannot be generated by two polynomials. Let

$$deg(x_1) = 3$$

$$deg(x_2) = 4$$

$$deg(x_3) = 5$$

thus we get the following

$$deg(f_1) = 9$$
$$deg(f_2) = 8$$
$$deg(f_3) = 10$$

Suppose that $I(C) = (g,h)$. If g,h have degree greater than 8 then f_2 is not in the ideal generated by g and h which is a contradiction hence one of them must have degree 8, say $deg(g) = 8$. A monomial $x_1^{m_1}x_2^{m_2}x_3^{m_3}$ has at least degree 3 so a polynomial contained in the ideal generated by g must has at least degree 11. So f_1 and f_3 is not in the ideal generated by g. If degree of h is greater than 9 then f_1 is not in the ideal generated by g and h, so degree of h must be 9. But in this case f_3 is not in the ideal generated by g and h which is a contradiction. Hence $I(C)$ cannot be generated by 2 polynomials.

4.2 A monomial curve C in $\mathbb{A}^4$ with $\mu(C) \leq 4$, $\mu(I(C)) \leq 9$

In this example we see that although the minimal number of polynomials generating C is 4 set theoretically, it is 9 ideal theoretically. This shows the strength of Eisenbud and Evans' Theorem 2.10. Let us consider the monomial curve C defined parametrically by

$$x_1 = t^{12}$$
$$x_2 = t^{13}$$
$$x_3 = t^{16}$$
$$x_4 = t^{17}.$$

It follows from the computer program Macaulay [10] that the generators of

$I(C)$ are the following polynomials

$$\begin{aligned} f_1 &= x_3^4 - x_2x_4^3 \\ f_2 &= x_2x_3 - x_1x_4 \\ f_3 &= x_2^4 - x_1^3x_3 \\ f_4 &= x_1x_3^3 - x_2^2x_4^2 \\ f_5 &= x_1x_2^3 - x_4^3 \\ f_6 &= x_1^2x_3^2 - x_2^3x_4 \\ f_7 &= x_1^2x_2^2 - x_3x_4^2 \\ f_8 &= x_1^3x_2 - x_3^2x_4 \\ f_9 &= x_1^4 - x_3^3 \end{aligned}$$

It can be easily checked that the following equalities hold

$$\begin{aligned} f_1 &= x_2f_5 - x_1f_3 - x_3f_9 \\ f_4^2 &= x_1^2x_2x_3^2f_5 + (x_4^4 - x_1^3x_3^2)f_3 - x_1^2x_3^3f_9 - (x_1^2x_3x_4^3 + 2x_1x_2x_3^2x_4^2)f_2 \\ f_6^2 &= x_2^2x_4^2f_3 + x_1^3x_3f_4 - 2x_1^2x_2^2x_3x_4f_2 \\ f_7^2 &= x_2^4f_9 - x_3^2x_4f_5 + (x_2^3x_3^2 + 2x_1x_2^2x_3x_4)f_2 \\ f_8^2 &= x_3^5x_4f_5 + (x_1^2x_2^2 - x_2^4x_3^3)f_9 + (2x_1^2x_2x_3^2 - x_2^3x_3^5 - 2x_1x_2^2x_3^4x_4)f_2 \end{aligned}$$

thus we get $f_1, f_4, f_6, f_7, f_8 \in Rad(f_2, f_3, f_5, f_9)$ which implies that

$$I(C) = Rad(f_2, f_3, f_5, f_9).$$

Hence $C = Z(f_2, f_3, f_5, f_9)$.

4.3 Projective twisted cubic curve

Projective twisted cubic curve C is a monomial curve in $\mathbb{P}^3$ having parametric representation as follows

$$\begin{aligned} x &= u^3 \\ y &= u^2t \\ z &= ut^2 \\ w &= t^3 \end{aligned}$$

where $(0,0) \neq (u,t) \in k^2$. We know from the computer program Macaulay [10] that the homogeneous prime ideal $I(C)$ of the projective twisted cubic curve is generated by the following polynomials

$$\begin{aligned} f_1 &= xw - yz \\ f_2 &= y^2 - xz \\ f_3 &= z^2 - yw. \end{aligned}$$

Now let us show that although the projective twisted cubic curve is a complete intersection set theoretically, it is not a complete intersection ideal theoretically, i.e. $\mu(I(C)) > 2$ and $\mu(C) = 2$.

Let $f = zf_3 + wf_1 = z^3 - 2yzw + xw^2$. It is easy to see that

$$C = Z(f_1, f_2, f_3) \subseteq Z(f, f_2).$$

On the other hand, we have

$$\begin{aligned} f_1^2 &= xf + z^2 f_2, \\ f_3^2 &= zf + w^2 f_2, \end{aligned}$$

which implies that $Z(f, f_2) \subseteq C = Z(f_1, f_2, f_3)$.

Therefore $C = Z(f, f_2)$ and $\mu(C) = 2$.

To show that C is not a complete intersection ideal theoretically, let us choose the following degrees, in fact the degrees can be chosen in different ways, in order to make proof in short we choose

$$deg(w) = 3$$
$$deg(z) = 4$$
$$deg(y) = 5$$
$$deg(x) = 6$$

thus we get

$$deg(f_1) = 9$$
$$deg(f_2) = 10$$
$$deg(f_3) = 8$$

Suppose that $I(C) = (g, h)$, for some homogeneous polynomials g and h. If g and h have degree greater than 8 then f_3 is not in the ideal generated by g and h which is a contradiction hence one of them must have degree 8, say $deg(g) = 8$. A monomial $x^{m_1}y^{m_2}z^{m_3}w^{m_4}$ has at least degree 3 (when $m_i = 0$, for $i = 1, 2, 3$ and $m_4 = 1$), so a polynomial contained in the ideal generated by g must has at least degree 11. So f_1 and f_3 is not in the ideal generated by g. If degree of h is greater than 9 then f_1 is not in the ideal generated by g and h, which is a contradiction, so degree of h must be 9. But in this case f_3 is not in the ideal generated by g and h which gives a contradiction. Hence $I(C)$ cannot be generated by g and h polynomials, i.e., $\mu(I(C)) > 2$.

5

Future Researches

As a last word, I would like to mention some prospective problems on which research may proceed based upon the results presented in this thesis.

Historically, the problem of finding the minimal number of elements generating an algebraic set in n space was treated by Kronecker in 1882 [15]. Kronecker succeeded to prove that $n+1$ elements suffice to generate an algebraic set in n space. In 1973, Eisenbud and Evans improved the result for sufficiency to n elements, by using the methods of Commutative Algebra [7]. Hence the next natural aim would be to reduce this minimal number of sufficient elements to $n-1$. This is not always possible, which is the case for zero dimensional algebraic sets in n space by Theorem 4 in [[9], page 204]. So the next aim would be to characterize under which condition it is possible to reduce this minimal number to $n-1$. As a general problem it is very hard to determine the reduction to $n-1$. So a natural path for research may be to investigate the characterization of reducibility of this minimal number to $n-1$ in some certain special cases such as monomial curves in n space or irreducible smooth curves in 3 space.

A result of Bresinsky tells us that this minimal number reduces to $n-1$ for monomial curves of type $C(m_1,\ldots,m_n)$ for which $\langle m_1,\ldots,m_n\rangle$ is a symmetric semigroup in the case of affine $n=4$ space [4]. My current insight through the mentioned result is that this minimal number reduces to $n-1(=3)$ for the monomial curves $C(m_1,\ldots,m_n)$ for which $\langle m_1,\ldots,m_n\rangle$ may not be a symmetric semigroup in the case of $n=4$. It may be interesting to show that if $\langle m_1,m_2,m_3\rangle$ is a symmetric semigroup and m_4 is the greatest integer which is not in $\langle m_1,m_2,m_3\rangle$, then the monomial curve $C(m_1,m_2,m_3,m_4)$ is a complete intersection set theoretically.

Another result of Robbiano and Valla tells us that if the projective coordinate ring of a monomial curve in $\mathbb{P}^3$ is Cohen Macaulay then this curve is a set theoretic complete intersection of 2 surfaces [23]. So a further insight of research may start with the rational quartic curve $C_4=(t^4,t^3u,tu^3,u^4)$ whose projective coordinate ring is not Cohen Macaulay.

From a different direction, ideal theoretically, Bresinsky has constructed some monomial curves in $\mathbb{A}^n$ whose defining ideals need arbitrary large minimal number of generators [6]. Arslan S.F. has recently constructed a family of monomial curves in $\mathbb{A}^n$ whose ideals need arbitrary large minimal number of generators. He has also shown that the ideal of the Cohen Maculay tangent cone of the curve that he constructed, need arbitrary large minimal number of generators [2]. So my current insight for prospective research is to construct such counter examples to exclude the characterization of the minimal number of generators under some certain condition in projective case.

Bibliography

[1] Abhyankar, S.S. "Algebraic space curves", Sem. Math. Sup. 43 Montreal(1971)

[2] Arslan, S.F. "Cohen Macaulayness of tangent cones", Proc. Amer. Math. Soc. 128 (2000) 2243-2251

[3] Bresinsky, H. "Monomial space curves in $\mathbb{A}^3$ as set theoretic complete intersections", Proc. Amer. Math. Soc. 75 (1979) 23-24

[4] Bresinsky, H. "Monomial Gorenstein curves in $\mathbb{A}^4$ as set theoretic complete intersections", Manuscripta Math. 27 (1979) 353-358

[5] Bresinsky, H. "Symmetric semigroups of integers generated by 4 elements", Manuscripta Math. 17 (1975) 205-219

[6] Bresinsky, H. "On prime ideals with generic zero $x_i = t_i^{n}$", Proc. Amer. Math. Soc. 47 (1975) 329-332

[7] Eisenbud, D. and Evans, E.G. "Every Algebraic Set in n-space is the intersection of n Hypersurfaces", Inventios Math. 19 (1973) 107-112

[8] Forster, O. "Über die anzahl der erzengenden eines idelas in einem Noetherschen ring", Math. Z. 84 (1964) 80-87

[9] Geyer, W.D. "On the number of equations which are necessary to describe an algebraic set in n-space", Lecture Notes, Sociedade Brasileira de Mathematica (SBM), Separat das Atas da 3 Escola de Algebra, volume 9, 1977, Rio de Janeiro, Brasil.

[10] Grayson, D.R. and Stillman, M.E. "Macaulay 2, a software system for research in algebraic geometry". Available at http://www.math.uiuc.edu/Macaulay2/

[11] Hartshorne, R. "Complete intersections and connectedness", Am. J. Math., 84 (1962) 175-193

[12] Herzog, J. "Generators and relations of abelian semigroups and semigroup rings", Manuscripta Math. 3 (1970) 175-193

[13] Jaffe, D. B. "On the set theoretic complete intersections in $\mathbb{P}^3$", Math. Ann. 285,(1989) 165-176

[14] Kneser, M. "Über die darstellung algebraicher raumkurven als durchschnitte von flächen", Arch. Math, 11 ,(1960) 157-158

[15] Kronecker, L. "Grundzüge einer arithmetischen theorie der algebraischen größen", J. Reine Angew. Math, (1882) 1-123

[16] Kunz, E. "Introduction to Commutative Algebra and Algebraic Geometry", Birkhäuser, Boston, Basel, Stuttgart, 1985

[17] Macaulay, F.S. "Algebraic theory of moduler systems", Cambridge Tracts 19 Cambridge (1916)

[18] Murthy, M.P. "Generators for certain ideals in Regular rings of dimension3", Forschungsinstitut fr Mathematik der ETH , (1971) 179-184

[19] Murthy, M.P. and Towber, J. "Algebraic vector bundles over $\mathbb{A}^3$ are trivial", Inventios Math. 24 (1974) 173-189

[20] Patil, D. "Certain monomial curves are set theoratical complete intersections", Manuscripta Math. 68 (1990) 399-204

[21] Perron, O. "Über das Vahlensche Beispiel zu einem Satz von Kronecker", Math.Z. 47 (1941) 318-324

[22] Robbiano, L. and Valla, G. "On set-theoretic complete intersections in the projective space", Rend. Sem. Mat. Fis. Milano LIII (1983) 333-346

[23] Robbiano, L. and Valla, G. "Some curves in $\mathbb{P}^3$ are set-theoretic complete intersections", in: Algebraic Geometry-Open problems, Proceedings Ravello 1982, Lecture Notes in Mathematics, Vol 997 (Springer, New York, 1983) 391-346

[24] Segre, B. "Intersezioni complete di due ipersuperficie algebriche in uno spazio afine, e non estendibilita di un teorema si seshadri", Rev. Roumaine Math. Pures Appl. 15 (1970) 1527-1534

[25] Serre, J.P. "Sur les modules projectifs", Sem. Dubreil-Pisot. 14 (1960/61) exp.2

[26] Storch, U. "Bemerkung zu einem Satz von Kneser", Arch. Math, 123 (1972) 403-404

[27] Thoma, A. "Monomial space curves in $\mathbb{P}^3_k$ as binomial set theoretic complete intersections", Proc. Amer. Math. Soc. 107 (1989) 55-61

[28] Thoma, A. "Ideal theoretic complete intersections in $\mathbb{P}^3_k$", Proc. Amer. Math. Soc. 107 (1989) 341-345

[29] Thoma, A. "On the set theoretic complete intersections in $\mathbb{P}^3_k$", Manuscripta Math. 70 (1991) 261-266

[30] Vahlen, K.T., "Bemerkung zur vollständigen darstellung algebraisher raumkurven", J. Reine Angew. Math, 108, (1891) 346-347