Number of real roots of a system of polynomial equations

Harsh Kumar
Indian Institute of Technology Kanpur

Supervised By
Prof. Jugal K Verma

5th July, 2014

1 About the Project

This report is a record of the project undertaken by me as a summer student at the Indian Institute of Technology Bombay, Mumbai under the kind supervision of Prof. Jugal K Verma. The aim of the project was to study a theorem to compute the number of real roots of set of polynomial equations given by P. Pederson, M. F. Roy and A. Szpirglas [1]. In the given report we have established the proof of this result along with some of its pre-reqisites and have also applied it to some elementary cases. This project was the result of the Summer Research Fellowship of the Indian Academy of Sciences.

2 Introduction

We start with some notations used throughout this report. Here we have assumed prior knowledge of basic ring theory. Let $f_1, f_2, f_3, \ldots, f_s \in \mathbb{C}[\bar{x}]$, where $\bar{x} = (x_1, x_2, \ldots, x_n)$ be the given set of polynomial equations. Let I be the ideal generated by $f_1, f_2, f_3, \ldots, f_s$.

$$I = (f_1, f_2, \ldots, f_s) = \{\, h_1 f_1 + h_2 f_2 + \ldots + h_s f_s : h_1, h_2, \ldots, h_s \in \mathbb{C}[\bar{x}] \,\}$$

Let V(I) be the algebraic variety generated by the set of polynomials, i.e. the set of points in the complex vector space $\mathbb{C}^n$ at which all polynomials of the ideal equal zero.

$$V(I) = \{\, \bar{a} \in \mathbb{C}^n \colon f_i(\bar{a}) = 0 \quad \forall i = 1, 2, \ldots, s \,\}$$

Let

$$V_R(I) = \{\, \bar{x} \in \mathbb{R}^n \colon f_i(\bar{a}) = 0 \quad \forall i = 1, 2, \ldots, s \,\} = V(I) \cap \mathbb{R}^n$$

Also, let $A_C = \mathbb{C}[\bar{x}]/I$ and $A = \mathbb{R}[\bar{x}]/I$

2.1 Hilbert's Nullstellensatz

To prove Hilbert's Nullstellensatz we first prove the following two lemmas.

Lemma 2.1. *Let V be a vector space and W be a subspace which is the linear span of a countable set of vectors $\{v_1, v_2, ...\}$. Then any subset of W of linearly independent vectors is either finite or countable.*

Proof. Let $W_n = L(v_1, \ldots, v_n)$ i.e. the linear span of the vectors $v_1, \ldots, v_n$. Clearly, $W = \bigcup_{i=1}^{\infty} W_n$. Let S be a subset of W of linearly independent vectors.Then,

$$S = \bigcup_{i=1}^{\infty} S \cap W_n$$

$S \cap W_n$ can have atmost n elements. So, S is either finite or countably infinite. ☐

Let $\mathbb{C}(x)$ denote the field of fractions of of $\mathbb{C}[x]$.

Lemma 2.2. *The set $\left\{ \frac{1}{x-a} : a \in \mathbb{C} \right\} \subseteq \mathbb{C}(x)$ is linearly independent over $\mathbb{C}$.*

Proof. We prove this by the method of contradiction. Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{C}$ such that $a_1, a_2, \ldots, a_n$ are all distinct. Suppose

$$\frac{b_1}{x - a_1} + \frac{b_2}{x - a_2} + \ldots + \frac{b_3}{x - a_3} = 0$$

Then

$$\sum_{i=1}^{m}(x-a_1)(x-a_2)\dots(x-a_{i-1})b_i(x-a_{i+1})\dots(x-a_n)=0.$$

If we substitute x by a_i we get $b_i=0$. And this is true for all $i=1,2,\dots,n$. This implies that S is linearly independent. $\square$

Since, $\left\{ \frac{1}{x-a} : a \in \mathbb{C} \right\}$ is countably infinite, so $\mathbb{C}[x]$ has a subspace with countably infinite basis.

Theorem 2.3 (Hilbert's Nullstellensatz)**.** *All maximal ideals of in the polynomial ring $\mathbb{C}[\bar{x}]$ are of the form $M_a=(x_1-a_1,...,x_n-a_n)$, where $a=(a_1,a_2,...,a_n)\in\mathbb{C}^n$.*

Proof. Clearly $M_a=(x_1-a_1,...,x_n-a_n)$ is a maximal ideal of $\mathbb{C}[\bar{x}]$ as $\mathbb{C}[\bar{x}]/M\cong\mathbb{C}$. To prove this isomorphism we consider the map $\phi:\mathbb{C}[\bar{x}]/M_a\longmapsto\mathbb{C}$ such that $\phi([f])=f(a)$, where $[f]$ is the image of $f\in\mathbb{C}[\bar{x}]$ in $\mathbb{C}[\bar{x}]/M$. This map is clearly onto and it preserves the ring operations. To prove that this map is one-one we let $f(a)=g(a)$, this implies that $f(a)-g(a)=0$. So $[f-g]=0$ and thus $[f]=[g]$. Now to prove the converse that every maximal ideal of $\mathbb{C}[\bar{x}]$ is of the form M_α we let M be a maximal ideal of $\mathbb{C}[\bar{x}]$. We claim that $N=M\cap\mathbb{C}[x_1]$ is a maximal ideal of $\mathbb{C}[x_1]$. To prove the claim we take the map $\pi:\mathbb{C}[x_1]\longrightarrow\mathbb{C}[\bar{x}]/M$

$$\pi(f(x_1))=f(x_1)+M$$

$$\ker(\pi)=\{\, f\in\mathbb{C}[x_1]: f\in M \,\}=M\cap\mathbb{C}[x_1]=N.$$

If, $f_1,f_2\in\mathbb{C}[\bar{x}]$ and $f_1\cdot f_2\in N$ implies $f_1\cdot f_2\in M$. But M is a prime ideal so f_1 or $f_2\in M$. Therefore, f_1 or $f_2\in N$. So, N is a prime ideal.
If $N\neq(0)$, then it is generated by a linear polynomial say $x_1-a_1\in\mathbb{C}[x_1]$. If $N=(0)$, then π is an injective map. Also, since $\mathbb{C}[\bar{x}]/M$ is a field, π has a unique extension to an embedding $\mu:\mathbb{C}(x_1)\longrightarrow\mathbb{C}[\bar{x}]/M$. But $\mathbb{C}[\bar{x}]/M$ is a complex vector space of countable dimension, so $\mathbb{C}[x_1]$ must be complex vector space of countable dimension too. But by Lemma 2.2 we know that $\left\{ \frac{1}{x_1-a} : a\in\mathbb{C} \right\}$ is an uncountable linearly independent set in $\mathbb{C}[x_1]$. And so from Lemma 2.1 $\mathbb{C}(x_1)$ must be uncountable dimensional vector space. This is a contradiction. Therefore $N\neq 0$. So, $x_1-a_1\in M$. Similarly, $x_i-a_i\in M \quad \forall i=2,3,\dots,n$. This implies, $(x_1-a_1,\dots,x_n-a_n)\subseteq M$, but M_a is a maximal ideal of $\mathbb{C}[\bar{x}]$. Thus

$$M=(x_1-a_1,\dots,x_n-a_n)=M_a$$

$\square$

Definition 2.4. *If all ideals of a ring are finitely generated then it is called a* ***Noetherian Ring****.*

Theorem 2.5. *A commutative ring with identity R is Noetherian if and only if any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$, there exists an m such that $I_m = I_{m+i}$ for all $i \geq 0$.*

Proof.

($\Longrightarrow$) $\bigcup_{n=1}^{\infty} I_n$ is an ideal of the ring R. So, it is finitely generated by say $(a_1, a_2, \ldots, a_g)$. Now let $a_i \in I_{m_i}$ for some m_i. Take m equal to the maximum of $m_1, m_2, \ldots, m_g$. Clearly, $a_i \in I_m$ for all $i = 1, 2, \ldots, g$, which implies that $I_m = \bigcup_{n=1}^{\infty} I_n$. And so, $I_m = I_{m+i}$ for all $i = 1, 2, \ldots$

($\Longleftarrow$) Let every ascending chain of ideals be stationary and I be the ideal that cannot be generated finitely. This implies that there exists a sequence $a_1, a_2, \ldots$ in I such that

$$a_n \notin (a_1, a_2, \ldots, a_{n-1}) \text{ for all } n = 1, 2, \ldots$$

Now, let $I_n = (a_1, a_2, \ldots, a_n)$. Clearly the chain of ideals I_n is a strictly ascending chain of ideals. A contradiction. So, every ideal is finitely generated.

□

Theorem 2.6 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring, then the polynomial ring $R[x]$ is also Noetherian.*

Proof. Let I be a non-zero ideal of $R[x]$ which is not finitely generated. Then, let f_1 be a non-zero polynomial of least degree in I, f_2 be a polynomial of least degree in $I \backslash (f_1)$, and so on. So, f_n is a polynomial of least degree in $I \backslash (f_1, \ldots, f_{n-1})$. Now take $\deg f_i = d_i$. Then

$$d_1 \leq d_2 \leq \ldots \leq d_n \leq \ldots$$

and

$$(f_1) < (f_1, f_2) < (f_1, f_2, f_3) < \ldots < (f_1, f_2, \ldots, f_n) < \ldots$$

Now, $f_n = a_n x^{d_n} + c_{n-1} x^{d_{n-1}} + \ldots$.

Let $J_n = (a_1, \ldots, a_n)$. Then there exists some $m \in \mathbb{N}$ such that

$$(a_1, a_2, \ldots, a_m) = (a_1, a_2, \ldots, a_{m+1})$$

$$\Longrightarrow \; a_{m+1} = b_1 a_1 + b_2 a_2 + \ldots + b_m a_m$$

for some $b_1, \ldots, b_m \in R$.
Let $g(x) = f_{m+1}(x) - \sum_{i=1}^{m} b_i f_i(x) x^{d_{m+1}-d_i}$. Then

$$\deg g(x) < d_{m+1} \text{ and } g(x) \in I \backslash (f_1, \ldots, f_m)$$

which is a contradiction to the fact that f_m is a polynomial of the least degree in $I \backslash (f_1, \ldots, f_m)$. Therefore the chain of ideals J_n is strictly ascending. But R is Noetherian so no chain of ideals can be strictly ascending. Hence we reach a contradiction.
Hence $R[x]$ is Noetherian.

□

Now we define two new notations. The first is the ideal of a variety

$$I(V) = \{f \in \mathbb{C}[\bar{x}] | f(a) = 0 \text{ for all } a \in V\}.$$

And the second is the zero set of an ideal

$$Z(I) = \{\, a \in \mathbb{C}^n : g(a) = 0 \text{ for all } g \in I \,\}.$$

Theorem 2.7 (Strong Nullstellensatz)**.** *Let J be an ideal of $\mathbb{C}[x]$. Then*

1. *$Z(J) = \phi$ if and only if $J = \mathbb{C}[\bar{x}]$.*
2. *$I(Z(J)) = \sqrt{J}$, where $\sqrt{J}$ is the radical ideal of J.*

Proof.

1. Let $Z(J) = \phi$. If $J \neq \mathbb{C}[\bar{x}]$, then there is a maximal ideal M_a which contains J. So, $f(a) = 0$ for all $f \in J$, which is a contradiction.Therefore, $Z(J) = \phi$ if and only if $J = \mathbb{C}[\bar{x}]$.

2. Now $J \subseteq I(Z(J))$ is obvious. Let $J = (f_1, f_2, \ldots, f_m)$ and $g \in I(Z(J))$, where $g \neq 0$. And let t be a new variable. $I = (f_1, f_2, \ldots, f_m, tg - 1) \subseteq \mathbb{C}[\bar{y}]$ where $\bar{y} = (x_1, x_2, \ldots, x_n, t)$. Now $Z(I) = \phi$ because if $b = (b_1, b_2, \ldots, b_{m+1}) \in \mathbb{C}^{m+1}$ belongs to $Z(I)$ then $f_1(b) = 0, f_2(b) = 0, \ldots f_m(b) = 0$ and so $g(b) = 0$, which implies that $(gt-1)(b) = -1$ which is a contradiction.
   If $Z(I) = \phi$ then $I = \mathbb{C}[\bar{y}]$. So,

   $$g_1 f_1 + g_2 f_2 + \ldots g_m f_m + g_{m+1}(gt-1) = 1$$

   for some $g_1, g_2, \ldots, g_{m+1} \in \mathbb{C}[\bar{y}]$. Put $g = 1/t$, to get

   $$\begin{aligned} g_1(x_1, x_2, \ldots, x_n, 1/g) f_1 + g_2(x_1, x_2, \ldots, x_n, 1/g) f_2 + \ldots \\ + g_m(x_1, x_2, \ldots, x_n, 1/g) f_m = 1. \end{aligned}$$

   Removing g from the denominator we obtain $g^r \in J$ which implies $g \in \sqrt{J}$.

□

2.2 Gröbner Basis

This section provides a brief introduction to the theory of Gröbner basis. Some of the proofs from this section have been skipped to ensure brevity of the report. Proof and other details such as an algorithm to find Gröbner basis can be found in [2].

Before moving on to Gröbner basis we first define what is a monomial ordering.

A **monomial order** on the set of monomials $M = \{x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} : \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{N}\}$ where $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in (\mathbb{Z}^+)^n$ is a total order $<$ with the following additional conditions :

1. $1 < x^\alpha$ for all monomials $x^\alpha \neq 1$.
2. if $x^\beta > x^\gamma$ then for any x^α, $x^\beta x^\alpha > x^\gamma x^\alpha$.

Some examples of monomial ordering include lexicographic (lex) ordering, graded lexicographic (grlex) ordering and graded reverse lexicographic (grevlex) ordering. More details can be seen in [2].

Support of a polynomial $f(x) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$ is the set $\mathrm{supp}(f) = \{\, x^\alpha \mid a_\alpha \neq 0 \,\}$.

The **initial monomial** of f, $in(f)$ is defined to be x^α such that $x^\alpha > x^\beta$ for all $x^\beta \in \mathrm{supp}(f)$.

Let I be a nonzero ideal of $\mathbb{C}[\bar{x}]$. The **initial ideal** of I, $in(I) = \{\, in(f) \mid f \in I \backslash \{0\} \,\}$.

Now, we are in a position to define Gröbner basis.

Definition 2.8. *A finite subset $G = \{\, g_1, g_2, \dots, g_t \,\}$ of an ideal I is said to be a* ***Gröbner basis*** *if*

$$(in(g_1), in(g_2), \dots, in(g_t)) = in(I).$$

Theorem 2.9. *Given a non-zero ideal I there exists a Gröbner basis G of I, fixing a monomial order. Also, G is a basis of I.*

Proof. Since $in(I)$ is a ideal of $\mathbb{C}[\bar{x}]$, it is finitely generated. So,

$$in(I) = (h_1, h_2, \dots, h_t).$$

Now, $h_i \in in(I)$ so there exists a polynomial g_i such that $h_i = in(g_i)$. Therefore

$$in(I) = (in(g_1), in(g_2), \dots, in(g_t)).$$

Hence $G = \{g_1, g_2, \ldots, g_t\}$ is a Gröbner basis of I. This proves our first claim. Next we prove the second claim. Since $g_i \in I$ so $(g_1, g_2, \ldots, g_t) \subset I$. Conversely, let $f \in I$. Dividing f by the ideal $(g_1, g_2, \ldots, g_t)$ we get

$$f = a_1 g_1 + a_2 g_2 + \ldots + a_t g_t + r$$

where $a_i \in \mathbb{C}[\bar{x}]$ for all $i = 1, 2, \ldots, t$. And $r \in \mathbb{C}[\bar{x}]$ and r is not divisible by any of $in(g_1), in(g_2), \ldots, in(g_t)$.
Now we claim that $r = 0$. Clearly,

$$r = f - a_1 g_1 - a_2 g_2 - \ldots - a_t g_t \in I$$

If $r \neq 0$, then $in(r) \in (in(g_1), in(g_2), \ldots, in(g_t))$. So, r must be divisible by some $in(g_i)$. A contradiction to the definition of remainder. Thus $r = 0$. So, $f \in (g_1, g_2, \ldots, g_t)$ and $I = (g_1, g_2, \ldots, g_t)$.

□

2.3 Finiteness Theorem

In this section we introduce the terminology regarding finite solutions of a system of polynomials and prove the finiteness theorem for determining whether a given system of polynomials has finite solutions or not.

A system is zero-dimensional if it has a finite number of solutions. This terminology comes from the fact that the algebraic variety of the solutions has dimension zero. A system with infinitely many solutions is said to be positive-dimensional.

From now on in this report we will be assuming that the ideals are zero-dimensional unless stated otherwise.

Theorem 2.10 (Finiteness Theorem)**.** *The following statements are equivalent:*

1. *number of common roots of $f_1, f_2, \ldots, f_s \in \mathbb{C}^n$ is finite, i.e., $V(I)$ is finite.*

2. *A_C is finite dimensional complex vector space.*

3. *I has a gröbner basis $G = (g_1, g_2, \ldots, g_h)$ such that after reordering we get $in(g_i) = x_i^{d_i}$, $\forall i = 1, 2, \ldots, h$.*

Proof.

$1 \implies 2:$ Let $V(I)$ be finite. Let $a_{i1}, a_{i2}, \ldots, a_{ik}$ be the ith coordinate points in $V(I)$. Then the function $f(x_i) = (x_i - a_{i1})(x_i - a_{i2}) \ldots (x_i - a_{ik})$ equals 0 at every point of $V(I)$. So, by Strong Nullstellensatz $f(x_i)^{d_i} \in I$. Then $[x_i^{d_i}] \in \mathbb{C}[\bar{x}]/I$ can be expressed in terms of residue classes of lower powers of x_i. Now let $d = \max_{i=1}^{k} kd_i$, then $\mathbb{C}[\bar{x}]/I$ has a basis of residue classes of monomials in which powers of all variables are bounded. Therefore $\mathbb{C}[\bar{x}]/I$ is finite dimensional.

$2 \implies 3:$ Let A_C be finite dimensional. Consider the residue classes

$$[1], [x_i], [x_i^2], \ldots$$

Now A_C is finite dimensional, so these must be linearly dependent. That is there exist $\alpha_0, \alpha_1, \ldots, \alpha_{t_i}$ such that

$$\alpha_0[1] + \alpha_1[x_i] + \alpha_2[x_i^2] + \ldots + \alpha_t[x_i^{t_i}] = 0.$$

$$\implies f(\bar{x}) = \alpha_0 1 + \alpha_1 x_i + \alpha_2 x_i^2 + \ldots + \alpha_{t_i} x_i^{t_i} \in I.$$

$$\implies x_i^{t_i} \in \text{in}(I).$$

$3 \implies 1:$ Let G be a Gröbner basis of I conataining g_i so that $in(g_i) = x^{d_i}$ for $i = 1, 2, \ldots, n$. Now without loss of generality we may assume that $x_i > x_{i-1} > \ldots > x_1$. Then $g_i \in \mathbb{C}[x_i, x_{i-1}, \ldots, x_1]$. So, $g_1 \in \mathbb{C}[x_1]$ is a polynomial in a single variable, whose number of solutions is bounded by d_1.Now substituting these values in $g_2 \in \mathbb{C}[x_1, x_2]$ we get equations in $\mathbb{C}[x_2]$ which again have number of solutions bounded by d_2 and the number of solutions x_2, x_1 is $d_1 d_2$. Similarly number of solutions for $x_1, x_2, \ldots, x_n = d_1 d_2 \ldots d_n$.So, $V(I)$ is finite.

□

Definition 2.11. *A reduced gröbner basis for a polynomial ideal I is a gröbner basis G for I sich that:*

1. *Coefficient of $in(g)$ is 1 for all $g \in G$.*
2. *For all $g \in G$, no monomial of g lies in $in(G - \{g\})$.*

This theorem also gives us a computational method to check whether the given set of polynomials are zero dimensional. All we need to do is calculate the reduced gröbner basis of the ideal and check the leading monomials. If they are all of the form $x_i^{d_i}$ then the ideal is zero dimensional.

2.4 Symmetric Bilinear forms

In this section we introduce notation of the bilinear form used in the Main Theorem.

Let $h \in \mathbb{R}[\bar{x}]$. Let $m_h : \mathbb{R}[\bar{x}]/I \to \mathbb{R}[\bar{x}]/I$ be a map such that $m_h([f]) = [hf]$, where $[f]$ is the image of the function $f \in \mathbb{R}[\bar{x}]$ in $\mathbb{R}[\bar{x}]/I$. We denote the matrix associated with this map by M_h.

We define a symmetric bilinear form $B_h : A \times A \to \mathbb{R}$

$$B_h([f],[g]) = tr(M_{hfg}),$$

where $f, g \in \mathbb{R}[x]$ and $[f],[g]$ are their images in A. It is easy to see that the above equation results in a symmetric bilinear form.

Now if we assume $\{v_i\}$ be a basis of A. Then matrix for B_h is

$$(B_h)_{i,j} = tr(m_{hv_iv_j})$$

Let Q_h be the assosiated quadratic form. Then,

$$Q_h = xB_hx^t \qquad \text{, where } x = \begin{bmatrix} x_1 & x_2 & \dots & x_n \end{bmatrix}.$$

Also, let $\sigma(Q_h)$ be the signature and $\rho(q_h)$ be the rank of the associated quadratic form.

3 Main Theorem

Using the notations of the previous section we can now state the main result of this report given by Pederson, Roy and Szpirglas [1].

Theorem 3.1 (Main theorem)**.**

$$\sigma(Q_h) = \#\{\bar{x} \in V_R(I) : h(\bar{x}) > 0\} - \#\{\bar{x} \in V_R(I) : h(\bar{x}) < 0\}.$$

$$\rho(Q_h) = \#\{\bar{x} \in V_C(I) : h(\bar{x}) \neq 0\}.$$

Corollary 3.1.1.

$$\sigma(Q_1) = \#\{\bar{x} \in V_R(I)\}.$$

Proof. Let $h = 1$ in the main theorem. Since $1 \not\leq 0$, $h(\bar{x}) > 0$ for all $\bar{x} \in V_R(I)$. Therefore

$$\sigma(Q_1) = \#(V_R(I)).$$

□

To calculate the number of real roots all we need to do is calculate the signature of Q_1.

4 Proof of the Main Theorem

From now on we will assume $V_C(I) = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$

Theorem 4.1. *There exists $k > 0$ such that for each $i \in \{1, 2, \ldots, r\}$*

$$M_{\alpha_i}^{k+1} + I = M_{\alpha_i}^{k} + I.$$

Proof. Clearly,

$$M_{\alpha_i} \supseteq M_{\alpha_i}^2 \supseteq M_{\alpha_i}^3 \supseteq \ldots$$
$$\implies M_{\alpha_i} + I \supseteq M_{\alpha_i}^2 + I \supseteq M_{\alpha_i}^3 + I \supseteq \ldots$$

Now, $\mathbb{C}[x]$ is a Noetherian ring.(By Hilbert's Basis Theorem) and in a commutative Noetherian ring which is a finite dimensional vector space every descending chain of ideals is finite. So, there exists a k_i such that

$$M_{\alpha_i}^{k_i} + I = M_{\alpha_i}^{k_i+j} + I \qquad \forall j = 1, 2, \ldots$$

Let $k = \max_{i=1}^{r} k_i$ Then,

$$M_{\alpha_i}^{k+j} + I = M_{\alpha_i}^{k} + I \text{ for all } i = 1, 2, \ldots, r \text{ and for all } j = 1, 2, \ldots$$

□

For any α in $\mathbb{C}^n$, let $\bar{M_\alpha}$ is the image of M_α in A_C.

Theorem 4.2.

$$A_C \cong \prod_{i=1}^{r} \frac{A_C}{\bar{M_{\alpha_i}}^k}.$$

Proof. Since $A_C = \mathbb{C}[\bar{x}]/I$ and $\bar{M_{\alpha_i}}^k = (M_\alpha^k + I)/I$. Therefore,

$$\frac{A_C}{\bar{M_{\alpha_i}}^k} \cong \frac{\mathbb{C}[\bar{x}]}{M_{\alpha_i}^k + I}.$$

So, the above theorem reduces to proving that

$$\frac{\mathbb{C}[\bar{x}]}{I} \cong \prod_{i=1}^{r} \frac{\mathbb{C}[\bar{x}]}{M_{\alpha_i}^k + I}.$$

Now to prove the above statement we consider the natural map

$$\phi : \mathbb{C}[\bar{x}] \to \prod_{i=1}^{r} \frac{\mathbb{C}[\bar{x}]}{M_{\alpha_i}^k + I} \text{ , } \phi(f(\bar{x})) = (f(\bar{x}) + (M_{\alpha_i}^k + I)).$$

This map is clearly a homomorphism. So, we consider its kernel.

$$\ker(\phi) = \left\{ f \in \mathbb{C}[\bar{x}] : f \in (M_{\alpha_i}^k + I) \ , \forall i = 1, 2, \ldots, r \right\}.$$

$$\implies \ker(\phi) = \bigcap_{i=1}^{r} (M_{\alpha_i}^k + I).$$

Now, as $M_{\alpha_i}^k$ and $M_{\alpha_j}^k$ are comaximal when $i \neq j$, so by Chinese Remainder Theorem [4] we have

$$\begin{aligned}
\bigcap_{i=1}^{r} (M_{\alpha_i}^k + I) &= \prod_{i=1}^{r} (M_{\alpha_i}^k + I) \\
&= \prod_{i=1}^{r} M_{\alpha_i}^k + I \\
&= \bigcap_{i=1}^{r} M_{\alpha_i}^k + I.
\end{aligned}$$

Let, $J = \bigcap_{i=1}^{r} M_{\alpha_i}$.

Now, let $\{h_1, \ldots, h_l\}$ be the generators of J .Then by Hilbert's Nullstelensatz, there exists a positive integer λ_i such that

$$h_i^{\lambda_i} \in I.$$

Let, $\lambda = \max_{i=1}^{r} \lambda_i$. Then

$$\begin{aligned}
& h_i^{\lambda} \in I \\
& \implies J^{\lambda} \subseteq I \\
& \implies (\bigcap_{i=1}^{r} M_{\alpha_i})^{\lambda} \subseteq I \\
& \implies (\prod_{i=1}^{r} M_{\alpha_i})^{\lambda} \subseteq I \qquad \text{[By Chinese remainder theorem]} \\
& \implies \prod_{i=1}^{r} M_{\alpha_i}^{\lambda} \subseteq I \\
& \implies \bigcap_{i=1}^{r} M_{\alpha_i}^{\lambda} \subseteq I.
\end{aligned}$$

Now, since $M_{\alpha_i}^k \subseteq M_{\alpha_i}^\lambda$,

$$\therefore \bigcap_{i=1}^{r} M_{\alpha_i}^k \subseteq I$$
$$\implies \bigcap_{i=1}^{r} M_{\alpha_i}^k + I = I$$
$$\implies \ker(\phi) = I.$$

Therefore,

$$\frac{\mathbb{C}[\bar{x}]}{I} \cong \prod_{i=1}^{r} \frac{\mathbb{C}[\bar{x}]}{M_{\alpha_i}^k + I}$$

And so,

$$A_C \cong \prod_{i=1}^{r} \frac{A_C}{\bar{M_{\alpha_i}}^k}$$

$\square$

Now, since A_C is a finite dimensional vector space over $\mathbb{C}$, $\frac{A_C}{\bar{M_{\alpha_i}}^k}$ are also finite dimensional for all $i \in \{1, \ldots, r\}$.

Also, let $\frac{A_C}{\bar{M_{\alpha_i}}^k} = A_\alpha$ and $dim_{\mathbb{C}} A_\alpha = e_\alpha$.

Lemma 4.3. *The subspace A_{α_i} are invariant under m_h.*

Proof. Now, $A_{\alpha_i} = \frac{\mathbb{C}[\bar{x}]}{M_{\alpha_i}^k + I}$. So, let $p/q \in A_{\alpha_i}$ where $p \in \mathbb{C}[\bar{x}]$ and $q \in M_{\alpha_i}^k + I$. $h.(p/q) = (hp)/q$ is of the same form. Hence, the subspace A_{α_i} are invariant under m_h. $\square$

Lemma 4.4. *Multiplication by $g(\bar{x}) = h(\bar{x}) - h(\alpha)$ is a nilpotent operator in A_α .*

Proof. Now,

$$A_\alpha = \frac{A}{\bar{M_\alpha}^k}$$

Also, $\bar{M_\alpha}^k$ is an M_α - primary ideal whose variety consists of a single point $\alpha \in V_C$. Clearly, $g(\alpha) = 0$. Therefore by Hilbert's Nullstellensatz , $g^\lambda \in \bar{M}_\alpha$. Hence, m_g is nilpotent. $\square$

Now, m_g is nilpotent. So, there exists a basis of A_α in which the matrix associated with the operator g is upper triangular.
Since, $h(\bar{x}) = g(\bar{x}) + h(\alpha)$ So, the matrix of multiplication by $h(\bar{x})$ is of the form

$$\begin{bmatrix} h(\alpha) & * & \cdots & * \\ 0 & h(\alpha) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h(\alpha) \end{bmatrix}.$$

Therefore $h(\alpha)$ is an eigenvalue of multiplicity e_α for the matrix m_h.

Theorem 4.5. *Consider the bilinear for $B_h : A \times A \to \mathbb{R}$. Then*

$$B_h([f],[g]) = \sum_{i=1}^{r} e_{\alpha_i} h(\alpha_i) f(\alpha_i) g(\alpha_i).$$

Proof. Matrix of $h(\bar{x})$ in A_{α_i} is of the form

$$\begin{bmatrix} h(\alpha) & * & \cdots & * \\ 0 & h(\alpha) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h(\alpha) \end{bmatrix}.$$

Now, since

$$A_C \cong \prod_{i=1}^{r} \frac{A_C}{\bar{M}_{\alpha_i}^{\ k}}.$$

Therefore, the matrix of $h(\bar{x})$ in A_C is of the form

$$\begin{bmatrix}
h(\alpha_1) & * & \cdots & * & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & h(\alpha_1) & \ddots & * & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & & \ddots & h(\alpha_1) & 0 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 \\
\vdots & \ddots & & 0 & h(\alpha_2) & * & \cdots & * & 0 & \cdots & \cdots & \vdots \\
 & & & & 0 & h(\alpha_2) & \ddots & * & \vdots & & & \vdots \\
\vdots & \ddots & & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & & & & & & & h(\alpha_2) & 0 & \cdots & \cdots & 0 \\
\vdots & \ddots & & \ddots & & \ddots & & & \ddots & & & \vdots \\
 & & & & & & & & & h(\alpha_r) & \cdots & * \\
\vdots & & \ddots & & \ddots & & \ddots & & \ddots & & \ddots & \vdots \\
0 & 0 & 0 & \cdots & & \cdots & & \cdots & & \cdots & 0 & h(\alpha_r)
\end{bmatrix}.$$

Therefore,

$$tr(m_h) = \sum_{i=1}^{r} e_{\alpha_i} h(\alpha_i).$$

$$\begin{aligned} \implies B_h([f],[g]) &= tr(m_{hfg}) \\ &= \sum_{i=1}^{r} e_{\alpha_i} h(\alpha_i) f(\alpha_i) g(\alpha_i). \end{aligned}$$

□

Since, $e_{\alpha_i} h(\alpha_i) f(\alpha_i) g(\alpha_i) \in \mathbb{R}$, therefore it is a symmetric function of coordinates of the points in V_C.

Let $\mathscr{B} = \{\omega_0, \omega_1, \ldots, \omega_{p-1}\}$ be a monomial basis for the $\mathbb{R}$-vector space A, where $\omega_0 = 1$. The symmetric matrix associated with B_h in the basis $\mathscr{B}$ is

$$(B_h)_{ij} = tr(m_{h\omega_i\omega_j}) = \sum_{k=1}^{r} e_{\alpha_k} h(\alpha_k) \omega_i(\alpha_k) \omega_j(\alpha_k).$$

Let us reorder the elements of $V_C(I)$ as $\{\beta_1, \beta_2, \ldots, \beta_p\}$, where the first e_{α_1} elements equal α_1, the next e_{α_2} elements equal α_2 and so on.

Now, if we let

$$W = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \omega_1(\beta_1) & \omega_1(\beta_2) & \ldots & \omega_1(\beta_p) \\ \omega_2(\beta_1) & \omega_2(\beta_2) & \ldots & \omega_2(\beta_p) \\ \vdots & \vdots & & \vdots \\ \omega_p(\beta_1) & \omega_p(\beta_2) & \ldots & \omega_p(\beta_p) \end{bmatrix}$$

and

$$\Delta_h = \begin{bmatrix} h(\beta_1) & 0 & \cdots & 0 \\ 0 & h(\beta_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h(\beta_p) \end{bmatrix}.$$

Then $B_h = W \Delta_h W^t$. Now let

$$x = \begin{bmatrix} x_1 & x_2 & \cdots & x_p \end{bmatrix}.$$

Therefore,

$$\begin{aligned}
Q_h &= xB_hx^t \\
&= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\sum_{k=1}^{p} x_ix_j\omega_i(\beta_k)\omega_j(\beta_k) \\
&= \sum_{k=1}^{p}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} x_ix_j\omega_i(\beta_k)\omega_j(\beta_k) \\
&= \sum_{k=1}^{p}(x_0 + x_1\omega_1(\beta_k) + x_2\omega_2(\beta_k) + \ldots + x_{p-1}\omega_{p-1}(\beta_k))^2 \\
&= \sum_{k=1}^{r} h(\alpha_k)(x_0 + x_1\omega_1(\alpha_k) + x_2\omega_2(\alpha_k) + \ldots + x_{p-1}\omega_{p-1}(\alpha_k))^2.
\end{aligned}$$

Let

$$y(a,x) = x_0 + x_1\omega_1(a) + \ldots + x_{p-1}\omega_{p-1}(a) \text{ and } b(a,x) = (y(a,x))^2$$

and $\lambda_1, \lambda_2, \ldots, \lambda_a$ be the real roots with $m_1, m_2, \ldots, m_a$ as their multiplicities. Also, let $\gamma_1, \bar{\gamma_1}, \gamma_2, \bar{\gamma_2}, \ldots, \gamma_b, \bar{\gamma_b}$ with multiplicities $w_1, w_2, \ldots, w_b$. Then

$$Q_h = \sum_{k=1}^{a} m_kh(\lambda_k)b(\lambda, x) + \sum_{i=1}^{b} w_i(h(\gamma)b(\gamma, x) + h(\bar{\gamma})b(\bar{\gamma}, x)).$$

Now, suppose $h(\gamma) = g(\gamma)^2$. Then

$$g(\gamma)y(\gamma, x) = \sum_{k=1}^{p} x_k\omega_k(\gamma)g(\gamma).$$

If we take $\omega_k(\gamma)g(\gamma) = c_k + \mathrm{i}d_k$ then

$$\begin{aligned}
g(\gamma)y(\gamma, x) &= \sum_{k=0}^{p-1} x_k(c_k + \mathrm{i}d_k) \\
&= d + \mathrm{i}d'
\end{aligned}$$

where d, d' are real linear forms.

Also,

$$\begin{aligned}
g(\bar{\gamma})y(\bar{\gamma},x) &= \sum_{k=0}^{p-1} x_k\omega_k(\bar{\gamma})g(\bar{\gamma}) \\
&= \sum_{k=0}^{p-1} x_k \; \overline{\omega_k(\gamma)g(\gamma)} \\
&= \sum_{k=0}^{p-1} x_k(c'_k - \mathrm{i}d'_k) \\
&= d - \mathrm{i}d'.
\end{aligned}$$

So,

$$\begin{aligned}
h(\gamma)b(\gamma,x) + h(\bar{\gamma})b(\bar{\gamma},x) &= (d+\mathrm{i}d')^2 + (d-\mathrm{i}d')^2 \\
&= 2d^2 - 2d'^2.
\end{aligned}$$

Rank of a quadratic form is the number of squares of linearly independent real linear forms. Therefore,

$$\begin{aligned}
\rho(Q_h) &= a + 2b \\
&= \text{No. of distinct roots of the ideal} \\
&= \#\{\bar{x} \in V_C(I) : h(\bar{x}) \neq 0\}.
\end{aligned}$$

Also, signature of quadratic form is the number of squares of linearly independent real linear forms with positive coefficient minus the number of squares of linearly independent real linear forms with negative coefficients. Therefore,

$$\begin{aligned}
\sigma(Q_h) &= a + b - b \\
&= a \\
&= \text{No. of distinct real roots of the ideal} \\
&= \#\{\bar{x} \in V_R(I) : h(\bar{x}) > 0\} - \#\{\bar{x} \in V_R(I) : h(\bar{x}) < 0\}.
\end{aligned}$$

5 Method of Application

This section outlines how the Main Theorem can be used to compute the number of real solutions of a given set of polynomial equation with zero dimensional ideal.

Let $f_1, f_2, \ldots f_k$ be the given set of polynomial equations and ideal $I = (f_1, f_2, \ldots f_k)$. First of all we calculate the Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ of I. And next we calculate the standard monomial basis $S = \{s[1], s[2], \ldots, s[m]\}$ of ideal I. The standard monomial basis is calculated by first calculating

$$B = \{\, x^\alpha : x^\alpha \text{ is not divisble by } in(g_1), in(g_2), \ldots, in(g_t) \,\}$$

Then $S = \{\, [x^\alpha] : x^\alpha \in B \,\}$ is a basis of the vector space $\mathbb{C}[\bar{x}]/I$ Next to calculate the matrix B_h we calculate $tr(M_{hs[i]s[j]})$.

5.1 Calculation of M_h

M_h is the matrix assosiated with the map $m_h : \mathbb{C}[\bar{x}]/I \longmapsto \mathbb{C}[\bar{x}]/I$
To find the matrix M_h we need to express $[gx^\alpha]$ in terms of elements of S. For this we divide gx^α by G to get the remainder $\overline{gx^\alpha}^G$. We write $\overline{gx^\alpha}^G = \sum_{\beta=1}^{m} c_{\alpha\beta} x^\beta$. Thus,

$$M_h = (c_{\alpha\beta}).$$

Clearly, B_h is a symmetric real matrix. So, all its eigenvalues are real. Also, the signature of the matrix is the number of positive real eigenvalues minus the number of negetive real eigenvalues. This can be calculated by generating the characteristic polynomial of B_h. And then by applying Descartes' Rule of Signs to the characteristic polynomial of B_h.

Descartes' Rule of Signs : The rule states that if the terms of a single-variable polynomial with real coefficients are ordered by descending variable exponent, then the number of positive roots of the polynomial is either equal to the number of sign differences between consecutive nonzero coefficients, or is less than it by an even number. Multiple roots of the same value are counted separately.

6 Applications

Calculations in this section have been done with the help of Singular, which is a free computer algebra system for polynomial computations.

6.1 Predicting the intersection of a circle and a line

Let

$$f_1 = x^2 + y^2 - 1,$$

$$f_2 = y \text{ , and}$$

$$I = (f_1, f_2).$$

The reduced gröbner basis G of $I = (y, x^2)$ (with lexicographic ordering).
The standard monomial basis of I , $S = \{1, x\}$.
So,

$$B_1 = \begin{bmatrix} \mathrm{tr}(m_1) & \mathrm{tr}(m_x) \\ \mathrm{tr}(m_x) & \mathrm{tr}(m_{x^2}) \end{bmatrix}$$

Now $m_1 = I_{2\times 2}$. So, $\mathrm{tr}(m_1) = 2$.

$$m_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

So, $\mathrm{tr}(m_1) = 0$.

$$m_x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Clearly, $\mathrm{tr}(m_{x^2}) = 2$.

$$B_1 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

$$\rho(B_1) = 2.$$

$$\sigma(B_1) = 2.$$

Therefore, the number of complex roots is 2 of which both are real, which is as expected.

6.2 Another example

This example has been taken from [3].

We calculate the number of real roots of

$$x^2 - 2xz + 5 = 0$$
$$xy^2 + yz + 1 = 0$$
$$3y^2 - 8xz = 0$$

in the box

$$R = \{\, (x, y, z) \in \mathbb{R}^3 : 0 < x < 1\ ,\ -3 < y < -2\ ,\ 2 < z < 3 \,\}\,.$$

Let $f_1 = x^2 - 2xz + 5$, $f_2 = xy^2 + yz + 1 = 0$ and $f_3 = 3y^2 - 8xz = 0$. Let I be the ideal generated by f_1, f_2, f_3.

Let monomial order be grevlex with $x > y > z$, then Gröbner basis of I

$$\begin{aligned}
&= \{2xz - z^2 - 5,\ 3y^2 - 4z^2 - 20, 4z^3 + 3xy + 20z + 3,\\
&\quad 20yz^2 + 40x^2 + 6xy - 3yz + 100y,\\
&\quad 240x^2y + 120x^2 + 18xy - 9yz + 800z^2 + 240x - 120z + 4000,\\
&\quad 160x^3 + 415xy - 80z^2 - 224x - 30y + 12z - 385\}.
\end{aligned}$$

Standard Monomial basis of $I = \{x^2\ ,\ xy\ ,\ x\ ,\ zy\ ,\ y\ ,\ z^2\ ,\ z\ ,\ 1\}$.

1. Let $h = 1$, then characteristic polynomial of the bilinear form B_1 is

$$\begin{aligned}
&x8 - 64224067/153600x^7\\
&\quad + 12130860888367/294912000x^6\\
&\quad + 2638731539952569/1769472000x^5\\
&\quad - 31306101585401873/147456000x^4\\
&\quad - 169194519425557201/49152000x^3\\
&\quad + 2155841825870863099/110592000x^2\\
&\quad + 33460624524617011/1105920x\\
&\quad - 14481627815488313/138240.
\end{aligned}$$

$$\begin{aligned}
\sigma(B_1) &= \#\text{ positive eigenvalues - }\#\text{ negetive eigenvalues}\\
&= \#signchanges - (8 - \#signchanges)\\
&= 5 - 3\\
&= 2\\
&= \#(V_R(I)).
\end{aligned}$$

So, the total number of real solutions of the given set of polynomial equations is two.

2. Let $h_1 = x(x-1)$, then characteristic polynomial of the bilinear form B_{h_1} is

$$\begin{aligned}
x^8 &- 1067218137463/147456000x^7 \\
&+ 435851680112989913869/90596966400000x^6 \\
&+ 4910822308449468355447279/724775731200000x^5 \\
&- 10423537458543245689895032 27/289910292480000x^4 \\
&- 3141202221489607244978379887277/289910292480000x^3 \\
&+ 1644666173815175072512183358543/322122547200000x^2 \\
&+ 223718942844947867901763375705 29/21474836480000x \\
&+ 3713500533218353115410132702317/2147483648000
\end{aligned}$$

$$\begin{aligned}
\sigma(B_{x(x-1)}) &= \#\text{ positive eigenvalues - }\#\text{ negetive eigenvalues} \\
&= \#signchanges - (8 - \#signchanges) \\
&= 4 - 4 \\
&= 0 \\
&= \#\{\bar{a} \in V(I) : h_1(\bar{a}) > 0\} - \#\{\bar{a} \in V(I) : h_1(\bar{a}) < 0\}
\end{aligned}$$

3. Let $h_2 = x^2(x-1)^2$, then characteristic polynomial is

$$\begin{aligned}
x^8 &- 12608962215827209/47185920000x^7 \\
&+ 18572984085854404742866391 0503/27831388078080000000x^6 \\
&+ 536184846482845306302192434954441 17/20038599416217600000000x^5 \\
&- 168653543368744368445249721831457676363 13/21374506043965440000000x^4 \\
&- 1964400103040120358711933899299842044709 8461/94997804639846400000000x^3 \\
&+ 1077438613669002186395044916736009594081898569/562949953421312000000000x^2 \\
&+ 2959271678264710259089575163693264012674905104 29/11258999068426240000000x \\
&- 2571066819418849669222053606915931047258913 5531/900719925474099200000
\end{aligned}$$

$$\begin{aligned}
\sigma(B_{x^2(x-1)^2}) &= 5 - 3 \\
&= 2 \\
&= \#\{\bar{a} \in V(I) : h_2(\bar{a}) > 0\} - \#\{\bar{a} \in V(I) : h_2(\bar{a}) < 0\} \\
&= \#\{\bar{a} \in V(I) : h_1(\bar{a}) > 0\} + \#\{\bar{a} \in V(I) : h_1(\bar{a}) < 0\}
\end{aligned}$$

$$\therefore \#\{\bar{a} \in V_R(I) : h_1(\bar{a}) < 0\} = 1. \tag{1}$$

i.e., there is one solution to the equation in the strip bounded by the lines $x = 0$ and $x = 1$.

4. Let $h_3 = (y + 2)(y + 3)$, then characteristic polynomial is

$$\begin{aligned} x^8 &- 170585159/1843200x^7 \\ &- 121392557391239417/42467328000x^6 \\ &+ 440520946345885980323/382205952000x^5 \\ &+ 21814057620771531835171/95551488000x^4 \\ &+ 379936436591661703639619/71663616000x^3 \\ &- 162148554725185477427807/2985984000x^2 \\ &- 20500118134600596233107/24883200x \\ &- 1135837514452194853529/933120 \end{aligned}$$

$$\sigma(B_{(y+2)(y+3)}) = -2$$

5. Let$h_4 = (y + 2)^2(y + 3)^2$ characteristic polynomial is

$$\begin{aligned} x^8 &+ 121225911557/22118400x^7 \\ &- 8671569891207595479713/6115295232000x^6 \\ &+ 178362247700110932014171401/41278242816000x^5 \\ &+ 2400361445330925378993955879/429981696000x^4 \\ &+ 1731947420002963285855717090927/2902376448000x^3 \\ &- 13405075995399387535548400968989/241864704000x^2 \\ &+ 250783907435563929488334783403/3023308800x \\ &- 89087143771028998946840057/6298560 \end{aligned}$$

$$\sigma(B_{(y+2)^2(y+3)^2}) = 2$$

$$\therefore \#\{\bar{a} \in V_R(I) : h_3(\bar{a}) < 0\} = 1. \tag{2}$$

i.e., there is one solution to the equation in the strip bounded by the lines $y = -2$ and $y = -3$.

6. Let $h_5 = (z-3)(z-4)$, then characteristic polynomial is

$$\begin{aligned} x^8 &+ 9367967/98304x^7 \\ &- 143904397702589/603979776x^6 \\ &+ 9840394174505791/603979776x^5 \\ &+ 892221694624446889/603979776x^4 \\ &- 9925002321421477201/150994944x^3 \\ &- 45796312301563191403/37748736x^2 \\ &+ 33635402313366019175/2097152x \\ &+ 3258366258484870425/262144 \end{aligned}$$

$$\sigma(B_{(z-3)(z-4)}) = 0$$

7. Let $h_6 = (z-3)^2(z-4)^2$,then characteristic polynomial is

$$\begin{aligned} x^8 &- 4887105475/1572864x^7 \\ &+ 6987095127439955/17179869184x^6 \\ &+ 1600246627291078937\,45/103079215104x^5 \\ &- 135420246675712843599 25/51539607552x^4 \\ &- 2213488047666648070438 25/12884901888x^3 \\ &+ 6510141027720167362599125/3221225472x^2 \\ &+ 1469530374804890051622 1875/268435456x \\ &- 98972875101477939159375/67108864 \end{aligned}$$

$$\sigma(B_{(z-3)^2(z-4)^2}) = 2$$

$$\therefore \#\{\bar{a} \in V_R(I) : h_5(\bar{a}) < 0\} = 1. \tag{3}$$

i.e., there is one solution to the equation in the strip bounded by the lines $z = 2$ and $z = 3$.

8. Let $h_7 = x(x-1)(z-2)(z-3)$,then characteristic polynomial is

$$\begin{aligned} x^8 &- 282644986303/31457280x^7 \\ &- 63841775345560073987 81/61847529062400x^6 \\ &+ 41051590864081186865197 21/247390116249600x^5 \\ &+ 5216452200104003972071658449/19791209299968x^4 \\ &- 2343722804610631638679095017178 23/19791209299968 00x^3 \\ &- 108067058708377603125434912821216 11/439804651110400x^2 \\ &+ 1668894959314836477294891220457528 67/43980465111040x \\ &- 9023806295720598070446622466630 31/4398046511104 \end{aligned}$$

$$\sigma(B_{x(x-1)(z-2)(z-3)}) = 2$$

9. Let $h_8 = x^2(x-1)^2(z-2)^2(z-3)^2$,then characteristic polynomial is

$$\begin{aligned} x^8 &- 158687645609642293/96636764160x^7 \\ &+ 47616978852084736240396912184 39/12970366926827028480x^6 \\ &+ 3615281492865531534065070964 3765792421/9338664187315460505 60x^5 \\ &- 106835954768890198168243858305 40479137016533/99612417998031578726 40x^4 \\ &- 40016827622049420707097827305528628958 6342530207/88544371553805847756 80x^3 \\ &+ 72027317701220237356877509660869987801040931945 63181/236118324143482260684 \\ &+ 15937812871573421918108838757390102121496633432530572545/47223664828696452 \\ &- 7590946230993182705894652171738940620479579319850095/18889465931478580854 7 \end{aligned}$$

$$\sigma(B_{x^2(x-1)^2(z-2)^2(z-3)^2}) = 2$$

$$\therefore \#\{\bar{a} \in V_R(I) : h_7(\bar{a}) < 0\} = 0.$$

So, there cannot be a root in the regions where $h_7(\bar{a}) < 0$ which is the set $\{\bar{a} \in \mathbb{R}^3 : h_1(\bar{a}) < 0 \text{ or } h_5(\bar{a}) < 0\} \backslash \{\bar{a} \in \mathbb{R}^3 : h_1(\bar{a}) < 0 \text{ and } h_5(\bar{a}) < 0\}$. But from (1) and (3) we already know that there is a root in each of the regions $h_1(\bar{a}) < 0$ and $h_5(\bar{a}) < 0$. Therefore there must be a unique root of the ideal in the region $\{\bar{a} \in \mathbb{R} : h_1(\bar{a}) < 0 \text{ and } h_5(\bar{a}) < 0\}$. Also both the real roots of the ideal are such that $-3 < y < -2$. So, there exists a unique root of the ideal in the required rectangular box.

References

[1] P. Pedersen, Marie-Franoise Roy, Aviva Szpirglas(1993), "Counting real zeros in the multivariate case", Progress in Mathematics Volume 109, pp 203-224.

[2] David Cox, John Little, Donal OShea(2007) *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*(3rd edition), New York: Springer.

[3] David Cox, John Little, Donal OShea(2005) *Using Algebraic Geometry*(2nd edition), New York: Springer, pp 37-76.

[4] Wikipedia (2014), "Chinese remainder theorem", http://en.wikipedia.org/wiki/Chinese_remainder_theorem [accessed 01 Jul 2014]