ON PROPERTIES OF THE SOLUTIONS OF SYSTEMS OF POLYNOMIAL EQUATIONS

Jonathan H. Manton[1]*, J. R. J. Groves*[2] *and Yingbo Hua*[1]

[1] Department of Electrical and Electronic Engineering
[2] Department of Mathematics and Statistics
The University of Melbourne, Parkville, Victoria 3010, Australia.
j.manton@ee.unimelb.edu.au

ABSTRACT

This paper investigates the number of solutions of a simultaneous set of polynomial equations. The set of constant terms of these equations is allowed to vary and the behaviour of the solutions for "almost all" sets of constant terms is described. Precise conditions for the existence of each of an infinite number of solutions, a finite number of solutions and a unique solution are derived. The results extend to systems of rational functions and cope with nuisance variables. Other contributions include exhibiting the equivalence of solutions of polynomial equations to extensions of ring homomorphisms in commutative algebra.

1. INTRODUCTION

Determining when a polynomial map is invertible is an important yet difficult problem encountered in control theory [7]. The traditional approach to studying polynomial maps is by using algebraic geometry. The main contribution of this paper is to present an alternative, and simpler, approach based on commutative algebra.

This paper studies the archetypal system consisting of m complex polynomial equations $f_1, \cdots, f_m$ in the n complex variables $x_1, \cdots, x_n$.

$$\begin{array}{ccc} f_1(x_1, x_2, \cdots, x_n) & = & c_1 \\ \vdots & \vdots & \vdots \\ f_m(x_1, x_2, \cdots, x_n) & = & c_m \end{array} \qquad (1)$$

The constants $c_1, \cdots, c_m \in \mathbb{C}$ are referred to as the RHS (right-hand side) of (1). A physical interpretation of (1) is that the underlying state $x_1, \cdots, x_n$ cannot be observed directly but the results $c_1, \cdots, c_m$ of m measurements $f_1, \cdots, f_m$ can be. By choosing $f_1, \cdots, f_m$ so that (1) has a unique inverse, the state $x_1, \cdots, x_n$ can be determined from the observations $c_1, \cdots, c_m$.

This paper studies the global properties of (1) as the RHS varies over the space $\mathbb{C}^m$. Although symbolic algorithms exist for solving (1) for fixed values of the RHS [2], the ability of these algorithms to deduce global properties is limited. The standard approach to studying global properties is to use algebraic geometry, and indeed, Theorem 1 in Section 2.2 can be derived using algebraic geometry (although a statement of it is not readily found in the literature). Although Theorem 1 itself is not new, the novel contributions are the simple method of proof based on studying the number of extensions of a certain ring homomorphism, and furthermore, the fact that the approach trivially extends to systems of rational functions as well as to systems with nuisance variables.

This work was supported by the Australian Research Council.

2. NUMBER OF SOLUTIONS

This section converts the problem of determining the number of solutions of a system of polynomial equations to the problem of determining the number of extensions of a ring homomorphism. This transformed problem is solved by commutative algebra in Section 2.2. The results are extended to cope with nuisance variables in Section 2.3 and rational functions in Section 2.4. For an introduction to commutative algebra see [1, 6, 9]. All rings are commutative with an identity element.

2.1. Transformation of Problem

Let $S = \mathbb{C}[x_1, \cdots, x_n]$ denote the polynomial ring in the indeterminates $x_1, \cdots, x_n$. Let $\widehat{\psi} : S \to \mathbb{C}$ be a $\mathbb{C}$ - homomorphism, that is, $\widehat{\psi}$ is a function satisfying $\widehat{\psi}(f_1 + f_2) = \widehat{\psi}(f_1) + \widehat{\psi}(f_2)$, $\widehat{\psi}(f_1 f_2) = \widehat{\psi}(f_1)\widehat{\psi}(f_2)$ and $\widehat{\psi}(c) = c$ for $c \in \mathbb{C}$. Then $\widehat{\psi}$ corresponds to a solution of (1) if it satisfies the constraints $\widehat{\psi}(f_i) = c_i$, $i = 1, \cdots, m$, the solution being x_j takes the value $\widehat{\psi}(x_j)$, $j = 1, \cdots, n$. The constraints $\widehat{\psi}(f_i) = c_i$ partially specify $\widehat{\psi}$ in that if $\psi : R \to \mathbb{C}$, where $R = \mathbb{C}[f_1, \cdots, f_m] \subset S$, is the unique $\mathbb{C}$ - homomorphism satisfying $\psi(f_i) = c_i$, $i = 1, \cdots, m$ then $\widehat{\psi}$ satisfies $\widehat{\psi}(f_i) = c_i$ if and only if $\widehat{\psi}$ is a homomorphic extension of ψ (meaning the restriction of $\widehat{\psi}$ to R is ψ). These ideas conduce to the observation:

There is a one-to-one correspondence between extensions of the $\mathbb{C}$ - homomorphism $\psi : R \to \mathbb{C}$ to the ring S and solutions of (1).

Remark: If ψ does not exist for certain c_i then (1) has no solutions for these c_i. The converse is not true. An extension $\widehat{\psi}$ of ψ might not exist.

2.1.1. Connection To Elimination Theory

This section is an aside. It illustrates the difference between the algebraic approach adopted herein and the traditional approach via elimination theory. Let $I = \langle f_1 - c_1, \cdots, f_m - c_m \rangle$ be the **elimination ideal** of elimination theory [2, Sec. 3] and let $R = \mathbb{C}[f_1, \cdots, f_m]$. Both I and R are collections of polynomial consequences of (1). However, I is larger in that every polynomial consequence in R is also in I (if $f \in R$ then $f - \psi(f) \in I$) whereas the converse is not true. Unlike R, the ideal I contains consequences specific to a particular value of the c_i (for example,

the value of $f = pf_1$ where p is an arbitrary polynomial is in general unknown unless $c_1 = 0$). The ring R is fixed whereas the ideal I changes as the c_i do. This suggests R is more suited to the study of global properties of (1) than I is.

2.2. Main Results

The results presented here are for complex polynomials. Proofs and generalisations appear in Section 4.

The following definitions are used throughout. Define $R = \mathbb{C}[f_1, \cdots, f_m]$ and $S = \mathbb{C}[x_1, \cdots, x_n]$ where $f_1, \cdots, f_m \in S$. A prime denotes the field of fractions of an integral domain, thus $R' = \mathbb{C}(f_1, \cdots, f_m)$ and $S' = \mathbb{C}(x_1, \cdots, x_n)$.

For a given $c_i \in \mathbb{C}$, $\psi_c : R \to \mathbb{C}$ denotes the unique (provided it exists) $\mathbb{C}$ - homomorphism satisfying $\psi_c(f_i) = c_i$ for $i = 1, \cdots, m$ (see Section 2.1). Note that ψ_c exists if $(c_1, \cdots, c_m)$ lies in the image of the polynomial map (1).

Theorem 1 *Let $N = [S' : R']$ be the dimension of S' as a vector space over R'. If $N = \infty$ then for any point $(c_1, \cdots, c_m)$ in the image of (1), there are an infinite number of solutions of (1).*

If N is finite then there exists an $f \in R$, $f \neq 0$, such that if $(c_1, \cdots, c_m)$ is in the image of (1) and is such that $\psi_c(f) \neq 0$ then (1) has exactly N solutions.

If $R = S$ (which implies, but is not implied by $N = 1$) then for any point $(c_1, \cdots, c_m)$ in the image of (1), there is exactly one solution of (1).

Remark 1: For fixed f, $\psi_c(f)$ is a polynomial in $c_1, \cdots, c_m$.
Remark 2: It is clear that if $R = S$ then (1) has a polynomial inverse, and if $R' = S'$ then (1) has a rational inverse (a rational function is a ratio of two polynomial functions).

The truth of Theorem 1 when N is finite follows from Theorem 7 of Section 4 because S is finitely generated over R and if $[S' : R']$ is finite then S is algebraic over R (Lemma 24). The $N = \infty$ case follows from Theorem 9.

2.3. Extension of Results — Nuisance Variables

The above results extend to when only certain functions of the x_i in (1) are relevant. The ease with which this is done exemplifies the advantage over an algebraic geometric approach. Let $z_1, \cdots, z_k$ be complex polynomial functions of $x_1, \cdots, x_n$.

$$\begin{array}{ccc} z_1 & = & g_1(x_1, x_2, \cdots, x_n) \\ \vdots & \vdots & \vdots \\ z_k & = & g_k(x_1, x_2, \cdots, x_n) \end{array} \tag{2}$$

Define $T = \mathbb{C}[f_1, \cdots, f_m, g_1, \cdots, g_k]$. Given $c_1, \cdots, c_m$ in (1), the number of values $z_1, \cdots, z_k$ can take in (2) is the number of extensions of ψ from R to T (Section 2.1). All results in Section 2.2 apply with T replacing S.
Example: The system (1) can be used to model semi-blind identification [5]; let x_1 to x_k represent the unknown input, let x_{k+1} to x_n represent the unknown channel parameters, and let c_1 to c_m represent the output. If (1) has a unique solution then both the channel and the input are identifiable. The input remains identifiable even though the channel does not (that is, equalisation is always possible) if every solution of (1) assigns the same value to $x_1, \cdots, x_k$. This situation occurs (almost always) when $R' = T'$ where $R = \mathbb{C}[f_1, \cdots, f_m]$ and $T = \mathbb{C}[f_1, \cdots, f_m, x_1, \cdots, x_k]$.

2.4. Extension of Results — Systems of Rational Functions

The above results extend to the f_i in (1) being rational functions. Define $R = \mathbb{C}[f_1, \cdots, f_m]$ and $T = R[x_1, \cdots, x_n]$ where both are subrings of the field $\mathbb{C}(x_1, \cdots, x_n)$. Given $c_1, \cdots, c_m$, the number of solutions of the rational system (1) is the number of extensions of ψ from R to T (Section 2.1). All results in Section 2.2 apply with T replacing S.
Remark: The inverse of a system of rational functions with a unique solution almost everywhere is again a system of rational functions (see Remark 2 after Theorem 1).

3. APPLICATION ORIENTATED RESULTS

This section gives a necessary and sufficient condition for $[S' : R']$ to be finite and several sufficient conditions for $[S' : R'] = 1$. The notation of Section 2.2 is used; in particular $R = \mathbb{C}[f_1, \cdots, f_m]$ and $S = \mathbb{C}[x_1, \cdots, x_n]$. Several proofs require concepts from field theory which can be found in [6, Ch. 12].

Given m polynomial or rational functions $f_1, \cdots, f_m \in S'$, the **Jacobian matrix** is the $m \times n$ matrix of partial derivatives:

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix} \tag{3}$$

Proposition 2 *If $f_1, \cdots, f_m \in S'$ then $\operatorname{rank}\{J\} = \operatorname{tr.deg.}_{\mathbb{C}} R'$ (the transcendence degree of R' over $\mathbb{C}$).*

The proof of Prop. 2 requires Lemma 3 as well as standard facts on "derivations" [3, 4, 9].

Lemma 3 *Let V be a finite dimensional vector space and V^* its dual. If $V = \operatorname{span}\{x_1, \cdots, x_n\}$ and $V^* = \operatorname{span}\{f_1, \cdots, f_m\}$ then $\dim V = \operatorname{rank}\{M\}$ where M is the $m \times n$ matrix with elements $M_{ij} = f_i(x_j)$.*

Proof of Prop. 2. Let $\mathfrak{D}_{S'/\mathbb{C}}$ denote the vector space of derivations on S' over $\mathbb{C}$. The partial derivatives $\frac{\partial}{\partial x_1}, \cdots, \frac{\partial}{\partial x_n}$ form a basis for $\mathfrak{D}_{S'/\mathbb{C}}$. Any derivation on R' can be extended to a derivation on S', hence $\mathfrak{D}_{R'/\mathbb{C}} = \operatorname{span}\left\{\frac{\partial}{\partial x_1}, \cdots, \frac{\partial}{\partial x_n}\right\}$. Define the linear functionals $df_i : \mathfrak{D}_{R'/\mathbb{C}} \to \mathbb{C}$ by $df_i(D) = D(f_i)$ for any $D \in \mathfrak{D}_{R'/\mathbb{C}}$. These functionals generate the dual space $\mathfrak{D}^*_{R'/\mathbb{C}}$ of $\mathfrak{D}_{R'/\mathbb{C}}$, that is, $\mathfrak{D}^*_{R'/\mathbb{C}} = \operatorname{span}\{df_1, \cdots, df_m\}$. From Lemma 3, $\dim \mathfrak{D}_{R'/\mathbb{C}} = \operatorname{rank}\{M\}$ where $M = J$. It is a standard result that $\dim \mathfrak{D}_{R'/\mathbb{C}} = \operatorname{tr.deg.}_{\mathbb{C}} R'$. □

Proposition 4 *In Theorem 1, $[S' : R']$ is finite if and only if J has full column rank.*

PROOF. Because $\mathbb{C} \subset R' \subset S'$, $\operatorname{tr.deg.}_{R'} S' = \operatorname{tr.deg.}_{\mathbb{C}} S' - \operatorname{tr.deg.}_{\mathbb{C}} R' = n - \operatorname{tr.deg.}_{\mathbb{C}} R' = n - \operatorname{rank}\{J\}$ by Prop. 2. Now, $[S' : R']$ is finite if and only if $\operatorname{tr.deg.}_{R'} S' = 0$, that is, if and only if $\operatorname{rank}\{J\} = n$. □
Remark: Evaluating (3) at $p \in \mathbb{C}^n$ gives a matrix of numbers denoted by J_p, and moreover, J has full column rank if and only if there exists a p such that J_p has full column rank.

If $f_1, \cdots, f_n \in S$ are algebraically independent over $\mathbb{C}$ then adding almost any other equation f_{n+1} will usually ensure (1) has

a unique solution (Prop. 5). At the very worst, provided f_{n+1} is not a rational function of $f_1, \cdots, f_n$, the number of solutions will at least halve (Prop. 6).

Proposition 5 *Assume that $[S' : R']$ is finite and that there exist $g_1, \cdots, g_k \in S$ such that $S = R[g_1, \cdots, g_k]$. Define $f = \alpha_1 g_1 + \cdots + \alpha_k g_k$ where $\alpha_1, \cdots, \alpha_k \in R'$. Then there exists a non-zero polynomial h with coefficients in S' such that $h(\alpha_1, \cdots, \alpha_k) \neq 0$ implies $S' = R[f]'$.*

PROOF. If $S' = R'[f]$ then f is called a primitive element. Because $[S' : R']$ is finite, S' is an algebraic extension of R', thus $R' = S'[g_1, \cdots, g_k]$ (Lemma 23). Because R' has characteristic zero, the field extension $R' \subset S'$ is separable. Kronecker's "method of indeterminates" can be used to show the existence of an h such that $f = \alpha_1 g_1 + \cdots + \alpha_k g_k$ is a primitive element if $h(\alpha_1, \cdots, \alpha_k) \neq 0$. (See proof of "primitive element theorem" in [9, Ch. II, Theorem 19].) □

Remark: If the coefficients α_i are chosen to be complex then so too can the polynomial h.

Proposition 6 *If $N = [S' : R']$ is finite and $N > 1$ then for any $f \in S - R'$, $[S' : R[f]'] \leq \frac{N}{2}$.*

PROOF. $R' \subset R[f]' \subset S'$, thus $N = [R[f]' : R'][S' : R[f]']$ (Lemma 27). Because $f \notin R'$, $[R[f]' : R'] \geq 2$. □

4. HOMOMORPHIC EXTENSIONS

This section derives three general theorems on homomorphic extensions.

Notation: Uppercase X and Z denote indeterminates while lowercase letters denote elements. If A is a ring, $A[X]$ is the polynomial ring in the indeterminate X while if B is a ring containing A and $x \in B$ then $A[x]$ is the ring generated by A and x. If A is an integral domain then A' denotes its field of fractions. If $A \subset B$ are integral domains then $[B' : A']$ denotes the degree of the field extension B' over A'. All rings considered are commutative with an identity element.

4.1. Statement of Theorems

Theorem 7 is proved in Section 4.3.

Theorem 7 *Let $A \subset B$ be two integral domains such that B is finitely generated and algebraic over A and A is infinite. There exists an $a \in A$, $a \neq 0$, such that, if $\xi : A \to \Omega$ is a ring homomorphism into the algebraically closed field Ω and if $\xi(a) \neq 0$, then there are exactly $[B' : A']$ extensions of ξ to B.*

Theorem 8 and Theorem 9 are proved in Section 4.4. The two theorems complement each other.

Theorem 8 *Let $A \subset B$ be integral domains with B finitely generated over A and $[B' : A'] = \infty$. There exists an $a \in A$, $a \neq 0$, such that if $\xi : A \to \Omega$ is a homomorphism into the algebraically closed field Ω and if $\xi(a) \neq 0$, then there are an infinite number of extensions of ξ to B.*

Theorem 9 *Let $A \subset B$ be integral domains with B finitely generated over A and $[B' : A'] = \infty$. Let $\xi : A \to \Omega$ be a homomorphism into the algebraically closed field Ω. If there exists at least one extension of ξ to B then there exist an infinite number.*

4.2. Preliminaries

Define $\phi : A[X] \to A[x]$ to be the A - homomorphism satisfying $\phi(X) = x$. It is well-defined, unique and onto. Its kernel $\ker \phi = \{f \in A[X] : \phi(f) = 0\}$ is the collection of polynomials $f \in A[X]$ satisfying $f(x) = 0$. The element x is **transcendental** over A if ϕ is one-to-one. Otherwise x is **algebraic** over A.

Lemma 10 extends the homomorphism $\xi : A \to C$ to a homomorphism $\widehat{\xi} : A[x] \to C$. It requires the homomorphism $\bar{\xi}$, the extension of ξ to the polynomial ring, defined by:

$$\bar{\xi} : A[X] \to C[Z], \qquad \bar{\xi}(X) = Z,\ \bar{\xi}(a) = \xi(a),\ a \in A \quad (4)$$

For example, $\bar{\xi}(a_2X^2 + a_1X + a_0) = \xi(a_2)Z^2 + \xi(a_1)Z + \xi(a_0)$.

Lemma 10 *Let A, C be rings and $\xi : A \to C$ a homomorphism. An extension $\widehat{\xi}$ of ξ to $A[x]$ satisfying $\widehat{\xi}(x) = z$ exists if and only if $z \in C$ is a root of every polynomial in the set $\bar{\xi}(\ker \phi)$. If it exists, it is unique.*

PROOF. Let $f \in \ker \phi$ and $\bar{f} = \bar{\xi}(f)$. Write f as $f = \sum_{i=0}^{\infty} a_i X^i$ ($a_i \in A$). Because $f \in \ker \phi$, $f(x) = \sum_{i=0}^{\infty} a_i x^i = 0$. Applying $\widehat{\xi}$ to both sides shows $\sum_{i=0}^{\infty} \xi(a_i) z^i = 0$ thus z is a root of $\bar{f}$. To prove sufficiency, let $b \in A[x]$ and $g \in A[X]$ such that $b = g(x)$. Define $\widehat{\xi}(b)$ to be $\left(\bar{\xi}(g)\right)(z)$. This is unambiguous: If $g_2 \in A[X]$ is such that $b = g_2(x)$ then $g - g_2 \in \ker \phi$ and by hypothesis on z, $\left(\bar{\xi}(g - g_2)\right)(z) = 0$ showing $\left(\bar{\xi}(g)\right)(z) = \left(\bar{\xi}(g_2)\right)(z)$. To prove uniqueness, let $\widehat{\xi}$ and $\widehat{\xi}_2$ be two homomorphisms such that $\widehat{\xi}(x) = \widehat{\xi}_2(x)$. Write any element $b \in A[x]$ as $b = \sum_{i=0}^{\infty} a_i x^i$, $a_i \in A$. Then $\widehat{\xi}(b) = \sum_{i=0}^{\infty} \xi(a_i) \widehat{\xi}(x)^i = \widehat{\xi}_2(b)$. □

4.3. Finite Number of Extensions

$\bar{\xi}(\ker \phi)$ must have a simple structure for Lemma 10 to be practical. It is well-known that $\ker \phi$ is a principal ideal if A is a field. Lemma 12 generalises this to when $A[x]$ is an integral domain. First some definitions.

Definition 11 *If $A \subset B$ are integral domains and $x \in B$ is algebraic over A then the **minimal polynomial** [6] of x over A' is the monic polynomial $m' \in A'[X]$ of smallest degree such that $m'(x) = 0$. It is unique and irreducible.*

Define $\phi' : A'[X] \to A'[x]$ to be the A' - homomorphism satisfying $\phi'(X) = x$. Then $\ker \phi' = \langle m' \rangle$. If A is an integral domain and $f \in A - \{0\}$ ($f \in A$ but $f \neq 0$) then A_f is the integral domain

$$A_f = \left\{ \frac{a}{b} : a \in A,\ b \in \left\{1, f, f^2, \cdots\right\} \right\} \quad (5)$$

Define $\phi_f : A_f[X] \to A_f[x]$ to be the A_f - homomorphism satisfying $\phi_f(X) = x$.

Lemma 12 *Let $B = A[x]$ where A and B are integral domains and x is algebraic over A. Let m' be the minimal polynomial of x over A'. The degree of m' is $[B' : A']$. There exists an $f \in A$, $f \neq 0$, such that $\ker \phi_f = \langle m' \rangle$.*

PROOF. Let n be the degree of m'. Then $n = [A'[x] : A']$ ([8, Prop. 4.3]). Because $B' = A'[x]$ (Lemma 23), $n = [B' : A']$ too. Write m' as $m' = X^n + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \cdots + \frac{a_0}{b_0}$, $a_i \in A$, $b_i \in A - \{0\}$. Define $f = b_0 b_1 \cdots b_{n-1} \in A - \{0\}$. Then $m' \in \ker \phi_f$. Let $p \in \ker \phi_f$. There exist unique polynomials $q, r \in A_f[X]$ such that $p = qm' + r$ and either $r = 0$ or the degree of r is less than n (Lemma 26). Because $p(x) = 0$, $r(x) = p(x) - q(x)m'(x) = 0$. Therefore $r \in \ker \phi'$ but unless $r = 0$ this contradicts the minimality of m' (Def. 11). Thus $p = qm'$ which proves $\ker \phi_f = \langle m' \rangle$. □

It is sufficient to consider A_f rather than A.

Lemma 13 *Let $A \subset B$ be integral domains and $\xi : A \to K$ a homomorphism into the field K. If $f \in A$ is such that $\xi(f) \neq 0$ then there is a unique extension ξ_f of ξ to A_f (5). There is a one-to-one and onto mapping between extensions of ξ to B and ξ_f to B_f.*

PROOF. Assume $\xi(f) \neq 0$. For $g \in R$ and p a nonnegative integer, define $\xi_f\left(\frac{g}{f^p}\right) = \frac{\xi(g)}{\xi(f)^p}$. It is the unique extension of ξ to A_f. If $\widehat{\xi}_f : B_f \to K$ is an extension of ξ_f then the restriction $\widehat{\xi}$ of $\widehat{\xi}_f$ to B is an extension of ξ (if $a \in A$ then $\widehat{\xi}(a) = \widehat{\xi}_f(a) = \xi_f(a) = \xi(a)$). Similarly, any extension $\widehat{\xi} : B \to \Omega$ uniquely extends to $\widehat{\xi}_f$ on B_f. The homomorphism $\widehat{\xi}_f$ is an extension of ξ_f (if $\frac{a}{b} \in A_f$ then $a \in A$ and $b \in \{1, f, f^2, \cdots\} \subset A$ thus $\widehat{\xi}_f\left(\frac{a}{b}\right) = \frac{\widehat{\xi}(a)}{\widehat{\xi}(b)} = \frac{\xi(a)}{\xi(b)} = \xi_f\left(\frac{a}{b}\right)$). Both mappings are thus one-to-one and onto. □

The definition of $\bar{\xi}$ (4) uniquely extends to $A_f[X]$ if $\xi(f) \neq 0$:

$$\bar{\xi}_f : A_f[X] \to K[Z], \qquad \bar{\xi}_f(X) = Z,\ \bar{\xi}_f(a) = \xi_f(a),\ a \in A_f \tag{6}$$

where ξ_f is the unique extension of ξ to A_f (Lemma 13).

Lemma 12 and Lemma 10 together suggest that the roots of $\bar{\xi}_f(m')$ determine distinct extensions. Multiple roots lead to the same extension. Lemma 29 takes care of this.

Lemma 14 *Let $B = A[x]$ where A and B are integral domains, x is algebraic over A and A is infinite. There exists an $a \in A$, $a \neq 0$, such that if $\xi : A \to \Omega$ is a ring homomorphism into the algebraically closed field Ω and if $\xi(a) \neq 0$, then there are exactly $[B' : A']$ extensions of ξ to B.*

PROOF. Let m' be the minimal polynomial of x over A'. Its degree is $n = [B' : A']$ (Lemma 12). Choose $f \in A - \{0\}$ so that $\ker \phi_f = \langle m' \rangle$ (Lemma 12). Later $a \in A$ will be chosen so that $\xi(a) \neq 0$ implies $\xi(f) \neq 0$. Thus there exists a unique extension $\xi_f : A_f \to \Omega$ of ξ (Lemma 13). Because $B_f = A_f[x]$ (Lemma 21), it suffices to show there are n extensions of ξ_f to B_f (Lemma 13). Let $g \in A_f$ be the resultant of m' and its formal derivative (Lemma 29). Because A' has characteristic zero, m' is separable over A' ([8, Prop. 8.6]), thus $g \neq 0$ (Lemma 29). Write $g = \frac{g_1}{g_2}$ where $g_1 \in A$ and $g_2 \in \{1, f, f^2, \cdots\}$. Choose $a = fg_1 \neq 0$. Then $\xi(a) \neq 0$ ensures $\bar{\xi}_f(m')$ has exactly n distinct roots in Ω (Lemma 29). The number of extensions of ξ_f to B_f is the number of simultaneous roots of every polynomial in the set $\bar{\xi}_f(\ker \phi_f) = \bar{\xi}_f(\langle m' \rangle)$ (Lemma 10). This equals n (see below), completing the proof. Let $\bar{p} \in \bar{\xi}_f(\langle m' \rangle)$. Then $\bar{p} = \bar{\xi}_f(p)$ for some $p \in \langle m' \rangle$, so $p = qm'$ for some $q \in A_f[X]$. Because $\bar{p} = \bar{\xi}_f(qm') = \bar{\xi}_f(q)\bar{\xi}_f(m')$, if z is a root of $\bar{\xi}_f(m')$ it is also a root of $\bar{p}$. This shows the number of simultaneous roots of $\bar{\xi}_f(\langle m' \rangle)$ equals n, the number of roots of $\bar{\xi}_f(m')$. □

Theorem 7 extends Lemma 14 by induction.

Proof of Theorem 7. Write $B = A[x_1, \cdots, x_m]$. Define the integral domains $C_0 = A$ and $C_i = A[x_1, \cdots, x_i]$ for $i = 1, \cdots, m$. Then $C_i = C_{i-1}[x_i]$ with x_i algebraic over C_{i-1} and $C_i' = C_{i-1}'[x_i]$ (Lemma 23). Assume by induction on k that there exists an $a_k \in A$ such that $\xi(a_k) \neq 0$ implies there are exactly $n_k = [C_k' : C_0']$ extensions of ξ to C_k. This is true for $k = 1$ (Lemma 14). Let these extensions be $\xi_k^{(i)}$ for $i = 1, \cdots, n_k$. For each i, there exists a $c_i \in C_k$ such that $\xi_k^{(i)}$ can be extended to C_{k+1} in $[C_{k+1}' : C_k']$ ways if $\xi_k^{(i)}(c_i) \neq 0$ (Lemma 14). If $\xi_k^{(i)}(c_i) = 0$ then $\xi_k^{(i)}(b_i c_i) = 0$ for any $b_i \in C_k$. There exists a b_i such that $b_i c_i \in A$ (Lemma 25); let $d_i = b_i c_i$. Thus $\xi(d_i) \neq 0$ implies $\xi_k^{(i)}(c_i) \neq 0$. Choose $a_{k+1} = a_k d_1 d_2 \cdots d_{n_k}$. Then $\xi(a_{k+1}) \neq 0$ implies each of the n_k extensions to C_k can be extended in $[C_{k+1}' : C_k']$ ways to C_{k+1}. This is a total of $n_{k+1} = n_k[C_{k+1}' : C_k']$ ways. By the degrees theorem (Lemma 27), $n_{k+1} = [C_{k+1}' : C_0']$. This completes the induction step. □

4.4. Infinite Number of Extensions

The following lemma is [1, Prop. 5.23].

Lemma 15 *Let $A \subset B$ be integral domains with B finitely generated over A. There exists an $a \in A$, $a \neq 0$, such that if $\xi : A \to \Omega$ is a homomorphism into the algebraically closed field Ω and if $\xi(a) \neq 0$, then there exists an extension $\widehat{\xi} : B \to \Omega$ of ξ.*

Proof of Theorem 8. Choose an $x \in B$ transcendental over A (Lemma 24). There exists a non-zero $a_x \in A[x]$ such that any homomorphism $\xi_x : A[x] \to \Omega$ satisfying $\xi_x(a_x) \neq 0$ extends to $\widehat{\xi} : B \to \Omega$ (Lemma 15). Thus the proof is complete once it is shown there are an infinite number of extensions ξ_x of ξ satisfying $\xi_x(a_x) \neq 0$. Write $a_x = a_n x^n + \cdots + a_0$ where $a_i \in A$. Then $\xi_x(a_x) = \xi(a_n)\xi_x(x)^n + \cdots + \xi(a_0)$. This is a non-zero polynomial if $\xi(a_n) \neq 0$; choose $a = a_n$. Because Ω is an infinite field, there are an infinite number of values $\xi_x(x)$ can be assigned such that $\xi_x(a_x) \neq 0$. Each such assignment determines an extension ξ_x of ξ (Lemma 10). □

The rest of this section builds up to a proof of Theorem 9. The following lemma is fundamental [1, 6].

Lemma 16 (Noether's Normalisation Lemma) *Let k be a field and $A \neq 0$ a finitely generated k-algebra. Then there exist elements $x_1, \cdots, x_r \in A$ which are algebraically independent over k and such that A is integral over $k[x_1, \cdots, x_r]$.*

Lemma 17 *Let $A \subset B$ be two rings such that B is integral over A. Let $\xi : A \to \Omega$ be a homomorphism into the algebraically closed field Ω. Then ξ extends to a homomorphism $\widehat{\xi} : B \to \Omega$.*

SKETCH OF PROOF. This is [1, Exercise 5.2]. Let p be the kernel of ξ; then p is a prime ideal of A. There exists a prime ideal q of B such that $q \cap A = p$ ([1, Th. 5.10]). It follows that B/q is integral over A/p ([1, Prop. 5.6]). Let K denote the field of fractions of B/q. It follows from [1, Th. 5.21] and the

preceding discussion that ξ can be extended to a valuation ring of K containing A/p. Such a valuation ring is integrally closed and so must contain any subring of K which is integral over A. Thus, in particular, it contains B/q and so ξ can be extended to B/q. □

Lemma 18 *Let k be a field and $A \neq 0$ a finitely generated k-algebra. Let $\xi : k \to \Omega$ be a homomorphism into the algebraic closure Ω of k. Then there exists an extension $\widehat{\xi} : A \to \Omega$ of ξ. If there exists an $x \in A$ transcendental over k then there are an infinite number of such extensions.*

PROOF. By Lemma 16, A is integral over $k[x_1, \cdots, x_r]$. If there exists an $x \in A$ transcendental over k then $r \geq 1$. Any homomorphism on $k[x_1, \cdots, x_r]$ extends to A (Lemma 17). All that remains is to show there are an infinite number of extensions ξ_1 of ξ to $k[x_1, \cdots, x_r]$ if $r \geq 1$. Any element $x \in k[x_1, \cdots, x_r]$ is *uniquely* expressible as a polynomial in the x_i. Thus for any $z_1, \cdots, z_r \in \Omega$, an extension ξ_1 of ξ to $k[x_1, \cdots, x_r]$ is well-defined by the conditions $\xi_1(x_i) = z_i$ for $i = 1, \cdots, r$. Since Ω is an infinite field, there are an infinite number of distinct extensions. □

Let p be a prime ideal. Define the **local ring** (a ring having a unique maximal ideal) A_p by

$$A_p = \left\{ \frac{a}{b} : \ a \in A, \ b \in A - p \right\} \tag{7}$$

Lemma 19 *Let $\xi : A \to K$ be a homomorphism on the ring A to the field K. Let $p = \ker \xi$ and A_p the localisation of A at p (7). Then there is a unique extension $\xi_p : A_p \to K$ of ξ. Furthermore $M = \ker \xi_p$ is the unique maximal ideal of the local ring A_p.*

PROOF. Because any subring of K is an integral domain, p is a prime ideal, thus A_p is well-defined. It can be shown that $\xi_p\left(\frac{a}{b}\right) = \frac{\xi(a)}{\xi(b)}$ for any $a \in A$, $b \in A - p$ defines a homomorphism on A_p. Clearly it is unique. It is also clear that $\ker \xi_p = \left\{ \frac{a}{b} : \ a \in p, b \in A - p \right\}$. This is the form of the unique maximal ideal of A_p. □

In conflicting yet concise notation, define B_p by

$$B_p = \left\{ \frac{a}{b} : \ a \in B, \ b \in A - p \right\} \tag{8}$$

Theorem 9 extends ξ to B by first extending it to A_p, then to B_p, then restricting it to B.

Lemma 20 *Let $A \subset B$ be rings and K a field. Let $\widehat{\xi} : B \to K$ be a homomorphism and $\xi : A \to K$ its restriction. Define $p = \ker \xi$ and B_p by (8). Then there is a unique extension $\widehat{\xi}_p : B_p \to K$ of $\widehat{\xi}$. Furthermore, $\widehat{\xi}_p$ is an extension of ξ_p in Lemma 19.*

PROOF. Because p is prime, $A - p$ is a multiplicatively closed set and B_p is well-defined. It can be shown that $\widehat{\xi}_p\left(\frac{a}{b}\right) = \frac{\widehat{\xi}(a)}{\widehat{\xi}(b)}$ for any $a \in B$, $b \in A - p$ defines a homomorphism on B_p. Clearly it is unique. Let $\frac{a}{b} \in A_p$, that is, $a \in A$, $b \in A - p$. Then $\widehat{\xi}_p\left(\frac{a}{b}\right) = \frac{\xi(a)}{\xi(b)} = \xi_p\left(\frac{a}{b}\right)$ showing $\widehat{\xi}_p$ is an extension of ξ_p. □

Proof of Theorem 9. Define $p = \ker \xi$ and let ξ_p be the unique extension of ξ to A_p and M its kernel (Lemma 19). Define B_p by (8) so that $A_p \subset B_p$. The ideal $B_pM \cap A_p$ equals either M or A_p. Assume $B_pM \cap A_p = A_p$. Then no ideal I of B_p exists such that $I \cap A_p = M$. This contradicts the existence of $\widehat{\xi}_p$ (Lemma 20) since $\ker \widehat{\xi}_p \cap A_p = M$. Therefore $B_pM \cap A_p = M$, allowing A_p/M to be naturally imbedded in B_p/B_pM. This makes B_p/B_pM a k-algebra where $k = A_p/M$. Let $x \in B$ be transcendental over A (Lemma 24) and thus over A_p too. Because $A_p[x]M \cap A_p = M$, the following diagram is commutative.

$$\begin{array}{ccccc} A_p & \longrightarrow & A_p[x] & \longrightarrow & B_p \\ \downarrow & & \downarrow & & \downarrow \\ A_p/M & \longrightarrow & A_p[x]/A_p[x]M & \longrightarrow & B_p/B_pM \end{array} \tag{9}$$

Let $x + B_pM$ denote the image of x in B_p/B_pM. It is transcendental over k for otherwise $x + A_p[x]M$ satisfies a monic polynomial $(x + A_p[x]M)^n + (a_{n-1} + A_p[x]M)(x + A_p[x]M)^{n-1} + \cdots + (a_0 + A_p[x]M)$ where $a_i \in A_p$. This means that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A_p[x]M$. However $A_p[x]M$ contains no monic polynomials (Lemma 28). Let $\xi' : A_p/M \to \Omega$ be the homomorphism induced by ξ_p. From Lemma 18 there exist an infinite number of extensions $\widehat{\xi'} : B_p/B_pM \to \Omega$ of ξ'. Each of these extensions defines a distinct homomorphism $\widehat{\xi}_p : B_p \to \Omega$ given by $\widehat{\xi}_p(b) = \widehat{\xi'}(b + B_pM)$. Each $\widehat{\xi}_p$ contracts to a distinct $\widehat{\xi} : B \to \Omega$ (Lemma 20). □

4.5. Miscellaneous Lemmas

This section is a collection of lemmas required above. Straightforward proofs are omitted.

Lemma 21 *If $B = A[x]$ are integral domains and $f \in A - \{0\}$ then $B_f = A_f[x]$.*

Lemma 22 *Let $A \subset B$ be integral domains. Then $x \in B$ is algebraic over A if and only if x is algebraic over A'.*

Lemma 23 *If $B = A[x_1, \cdots, x_n]$ are integral domains and the x_i are algebraic over A then $B' = A'[x_1, \cdots, x_n]$.*

Lemma 24 *Let $A \subset B$ be integral domains and B finitely generated over A. Then B is algebraic over A if and only if $[B' : A']$ is finite.*

Lemma 25 *Let $A \subset B$ be integral domains with B algebraic over A. For any $c \in B$ there exists a $b \in B$ such that $bc \in A$.*

Lemma 26 *Let R be an integral domain. Let $m \in R[X]$ be a monic polynomial of degree n. Then for any polynomial $f \in R[X]$ there exist unique polynomials $q, r \in R[X]$ such that $f = qm + r$ and either $r = 0$ or r has degree less than n.*

Lemma 27 (Degrees Theorem) *Let $F \subset K \subset L$ be extensions of fields. Then $[L : F]$ is finite if and only if $[L : K]$ and $[K : F]$ are finite; furthermore, when this is the case, $[L : F] = [L : K][K : F]$.*

Lemma 28 *Let $A \subset B$ be rings with $B = A[x]$ and x transcendental over A. Let I be a proper ideal in A. Then $BI \subset I[x]$ where $I[x]$ denotes the set of polynomials with coefficients in I. In particular, BI contains no monic polynomial in $A[x]$.*

4.5.1. Resultants and Multiple Roots

Let K be a field and $f, g \in K[X]$ two polynomials. If $f = a_m X^m + \cdots + a_0$ and $g = b_n X^n + \cdots + b_0$ where $a_i, b_i \in K$ then the **resultant** [2, Sec. 3.5] of f and g, denoted $\mathrm{Res}(f, g)$, is a polynomial in the a_i and b_i with coefficients either 1 or -1. Its importance is that f and g have a common factor in $K[X]$ of degree ≥ 1 if and only if $\mathrm{Res}(f, g) = 0$.

Lemma 29 *Let A be an integral domain and $\xi : A \to K$ a homomorphism into the field K. Define $\bar{\xi}$ by (4). Let $m \in A[X]$ be monic and define $\bar{m} = \bar{\xi}(m) \in K[Z]$. Let $g = \mathrm{Res}(m, dm)$ where dm is the formal derivative of m. Then $g \in A$ and is such that $\xi(g) = 0$ if and only if $\bar{m}$ has a repeated root in a splitting field of K. Furthermore $g = 0$ if and only if m has a repeated root in a splitting field of A'.*

PROOF. The resultant commutes with homomorphisms and formal derivatives, thus

$$\mathrm{Res}(\bar{m}, d\bar{m}) = \mathrm{Res}\left(\bar{\xi}(m), \bar{\xi}(dm)\right) = \xi(\mathrm{Res}(m, dm)) = \xi(g).$$

By [8, Lemma 8.5], m has a multiple root in a splitting field of A' if and only if m and dm have a common factor in $A'[X]$, that is, if and only if $g = 0$. Analogously, $\bar{m}$ has a multiple root in a splitting field of K if and only if $\bar{m}$ and $d\bar{m}$ have a common factor in $K[Z]$, that is, if and only if $\xi(g) = 0$. □

5. CONCLUSION

Precise conditions for a system of polynomial equations (1) to have a unique solution are derived in a series of results (Theorem 1, Prop. 4, Prop. 5). The distinguishing feature of this work is that the number of solutions is studied by exploiting the one-to-one correspondence between solutions and extensions of ring homomorphisms described in Section 2.1.

It is expected that this "ring-homomorphic" approach to the study of polynomial equations will lead to the discovery of further properties of polynomial equations. Indeed, this approach has certain advantages over other ways in which polynomial equations have been studied; Section 2.1.1 explains the difference between this approach and that of elimination theory, while Section 2.3 and Section 2.4 show that the ring-homomorphic approach readily extends to cope with nuisance variables and rational functions.

Section 4 derived quite general theorems on the number of distinct extensions of a ring homomorphism. Although existence proofs such as Lemma 15 are available in the literature, the results on the *number* of distinct extensions seem to be confined to Galois theory. Since Galois theory considers field extensions, Theorem 7 can be interpreted as a generalisation to integral domains.

6. REFERENCES

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[2] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, 2nd edition, 1996.

[3] N. Jacobson. *Basic Algebra*, volume 2. San Francisco, W. H. Freeman, 1980.

[4] S. Lang. *Algebra*. Addison-Wesley, 1965.

[5] J. H. Manton, Y. Hua, Y. Zheng, and C. Zhang. Semi-blind identification of finite impulse response channels. In *IEEE Conference on Acoustics, Speech and Signal Processing*, volume 4, pages 2369–2372, Seattle, Washington, May 1998.

[6] R. Y. Sharp. *Steps in Commutative Algebra*. Cambridge University Press, 1990.

[7] E. D. Sontag. On the observability of polynomial systems, I: Finite-time problems. *SIAM J. Control and Optimization*, 17(1):139–151, 1979.

[8] I. Stewart. *Galois Theory*. Chapman and Hall, second edition, 1989.

[9] O. Zariski and P. Samuel. *Commutative Algebra*, volume 1. Springer-Verlag, 1975.