Output Feedback Stabilization—Solution by Algebraic Geometry Methods

BRIAN D. O. ANDERSON, FELLOW, IEEE, AND RAYMOND W. SCOTT

Abstract—Given an unstable finite-dimensional linear system, one can relate the existence of a memoryless feedback law stabilizing the system to the existence of a real solution of a set of multivariable polynomial inequalities. From these inequalities, a set of equalities may be constructed with two properties: the equality set has a real solution precisely when the inequality set does; generically the equality set has a finite number of solutions. Multivariable polynomial resultants provide a method of solving the equalities subject to the condition that the equalities have a finite number of solutions. The property that there is a finite number of solutions is established using some results of algebraic geometry.

I. Introduction

THIS PAPER is concerned with a group of linear-system theory problems of which the output-feedback stabilization problem is conceptually the simplest example. The class of problems is characterized by the need to establish the existence of a real solution, and possibly to construct such a solution, to a set of polynomial inequalities. To understand the ideas further, this paper shall concentrate for the most part on the output-feedback stabilization problem.

Consider the linear system

$$\dot{x} = Fx + Gu \qquad y = H'x \tag{1.1}$$

where the symbols have the usual meanings and the system is not open loop stable, i.e., one or more eigenvalues of F has a nonnegative real part. One may ask if there exists a control law

$$u = Ky \tag{1.2}$$

which stabilizes the system (1.1); i.e., such that

$$Re[\lambda_i(F + GKH')] < 0, \qquad \text{for all } i \tag{1.3}$$

where $\{\lambda_i(A)\}$ is the set of eigenvalues of A. If such a control law exists one might then ask how it may be found.

This problem has a long history. For the case where the plant in question is scalar (i.e., has a scalar input and output), the problem is immediately recognizable as one which is amenable to such classical methods as the use of the Nyquist criterion, root locus plot, etc. But these methods fail if the input or output is not scalar. Another approach to the problem is to consider the case where the output of a completely controllable plant is the entire state vector (or something equivalent to it); a standard result is that it is always possible by output feedback (in this case state feedback) to arbitrarily position the closed-loop modes of the plant. Then one can suppose that the entire state vector is not available and ask to what extent the poles can then be positioned. Strictly one then does not have an output stabilization problem but an output-feedback pole-positioning problem, however the connection with the stabilization problem is close.

Among efforts in the direction of pole positioning, the authors note a series of works, commencing around 1970, [1]–[5]. The main idea in all these works is that, in rough terms, if the feedback matrix contains n entries in all then n closed-loop poles are assignable. The difficulty in using these results in practice is that if the total number of closed-loop poles, m say, exceeds n, then control is lost over $(m - n)$ of them in assigning n. In particular one or more of the $(m - n)$ poles may in the assigning process enter the right half plane, probably thereby rendering the assignment of n poles a pointless exercise. Moreover, the ability to predict the phenomenon is essentially lacking.

In algebraic terms, the coefficients of the closed-loop characteristic polynomial are multinomial (multivariable polynomial) functions of the entries of the gain matrix, and the stability of the closed-loop system is only expressible in terms of multinomial inequalities involving the coefficients of the characteristic polynomial. Ensuring that these inequalities hold while choosing the gain to produce certain zeros of the closed-loop polynomial is a formidable task and certainly points up the necessity of separate study, perhaps in isolation from the pole-positioning problem, of the stabilization problem.

Much of the work on the stabilization problem falls into one of two classes. The first class comprises the derivation of necessary or sufficient conditions (but not necessary and sufficient conditions) for solvability of the problem. The second class comprises the devising of heuristically based algorithms for obtaining a solution. Within the former class the authors note [6]–[8], with [6] containing a sufficient condition; [7], a further proof of that condition; and [8], a necessary condition. Reference [9] gives a necessary and sufficient condition subject to fairly retrictive conditions on the matrix H. References [10]–[13] fall into the second category, suggesting iterative algorithms for solving stabilization (and pole-positioning) problems. The general idea is to adjust the feedback law at each iteration, in a direction which makes the system "more stable" according to some criteria (such as increase in the values of the Hurwitz determinants). None of the procedures will necessarily converge, even when a solution to the stabilization problem or the pole-positioning problem is known to exist. A survey of results up to 1972 is available [14].

An advance is provided in [15], in which several procedures are proposed for tackling the stabilization problem, the pole-positioning problem, and a collection of related problems. The first of these procedures is tied to notions of decision algebra, introduced in [16] and [17] and summarized in [18]. More precisely it is shown that the existence part of the stabilization problem can in principle be settled by a finite number of

Manuscript received December 22, 1975; revised November 11, 1976. This work was supported by the Australian Research Grants Committee.

B. D. O. Anderson is with the Department of Electrical Engineering, University of Newcastle, New South Wales 2308, Australia.

R. W. Scott is with the Department of Electrical Engineering, Capricornia Institute of Advanced Education, Rockhampton, Queensland, Australia.

rational calculations. (It can only be settled "in principle" because the number of separate rational calculations—addition, subtraction, multiplication, division, and sign checking—may be prohibitively large.) The construction problem can be solved by a finite number of one-variable polynomial factorizations; the polynomials in question arise out of the calculations involved in considering the existence question, so there is no real saving obtained in considering only the construction problem alone. A second procedure suggests an iterative algorithm which will, in theory, always converge to a solution of the construction problem, if one exists. The third procedure again seeks simply to solve the construction question via the use of multivariable polynomial resultants; in [15] a potential difficulty was noted and a technique for eliminating the difficulty was conjectured. The purpose of this paper is to develop the procedure in full, in the process of which a variation of the conjecture in [15] is established.

More precisely, the procedure is as follows. First, the construction problem is formulated as one requiring determination of a real solution of a system of polynomial inequalities. (A number of other system theory problems can also be formulated this way, see [15]; the method will apply to them as well.) The inequalities are then shown to be equivalent to a set of equalities in the sense that real solutions of the inequality set and equality set correspond. The equality set in general will have an infinite number of solutions, both real and complex, and there seems to be no straightforward way of extracting a real solution should one exist. The equality set is accordingly replaced by a further equality set with three properties. First, if the first equality set has a real solution so does the second set. Second, every solution of the second set is a solution of the first set. Third, the second set in general has a finite number of solutions, both real and complex. The third property just mentioned makes it possible to determine all solutions of the second set; accordingly, a real solution of the first set can be found should one exist. Evidently, the existence question is indirectly addressed; i.e., if no solution to the equation set is obtained, one can conclude that there is no solution to the stabilization problem.

An outline of the paper is as follows. In Section II the reformulation of the construction problem is reviewed and a technique is proposed for eliminating the difficulty of an infinite number of solutions by constructing a second equality set. Section III demonstrates that the technique leads in general to a finite number of solutions. Some remarks on computing these solutions are made in Section IV. An example of the procedure is presented in Section V, while Section VI contains concluding remarks.

The major contribution is to be found in Section III. The techniques used are those of algebraic geometry. The actual algebraic-geometry results are spread over many chapters of some of the references, interspersed with much material not used here; it therefore seemed appropriate to provide a summary of these results, and this we have done in Appendices I and II.

II. The Construction Problem Reformulated

In this section, a reformulation of the construction problem originally presented in [15] is reviewed. The reformulated problem introduces a system of multivariable polynomial equations.

Suppose the feedback matrix K in (1.2) has n entries (where n is the product of the dimensions of the input and output vectors). Denote these entries by $x_1, x_2, \cdots, x_n$ and observe that the characteristic polynomial of the system (1.1)

$$\det [sI - (F + GKH')] = \sum_{j=0}^{m} \beta_j s^j \tag{2.1}$$

has coefficients β_j which are polynomials in x_j. (Here m is the dimension of the system.) Precisely what these polynomials are does not concern us here; we simply need to note that for any particular set of matrices F, G, and H the polynomials in question could be computed.

The Hurwitz determinants associated with any polynomial $\Sigma_{j=0}^{m} \beta_j s^j$ are given [19] by the leading principal minors of the $m \times m$ matrix

$$\begin{bmatrix} \beta_{m-1} & \beta_{m-3} & \beta_{m-5} & \cdots & 0 \\ \beta_m & \beta_{m-2} & \beta_{m-4} & \cdots & 0 \\ 0 & \beta_{m-1} & \beta_{m-3} & \cdots & 0 \\ 0 & \beta_m & \beta_{m-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \beta_0 \end{bmatrix}$$

Each Hurwitz determinant is a multivariable polynomial in β_j, and therefore a multivariable polynomial in x_j. Now if the Hurwitz determinants are all positive, then all the roots of the characteristic polynomial have negative real parts [19]. That is, if we denote the kth Hurwitz determinant by $p_k(x)$, where $x = (x_1, x_2, \cdots, x_n)'$, then

$$p_k(x) > 0, \qquad k = 1, 2, \cdots, m \tag{2.2}$$

holds for some real value $\bar{x}$, of the variable set x, if and only if the output-feedback problem has a solution. The values $\bar{x}_i$ satisfying (2.2) are values of the entries of a gain matrix K which stabilizes (1.1). Should there be no real n-tuple $\bar{x}$ satisfying (2.2) the stabilization problem has no solution.

It is worth noting that stability of the polynomial in (2.1) is also guaranteed if and only if all the odd- or even-order Hurwitz determinants are positive together with the first, last, and even or odd subscripted coefficients β_j. (This is the Liénard–Chipert criterion [19].) Accordingly, some of the inequalities in (2.2) may be replaced by others which may be of lower degree, thus simplifying the problem.

Another procedure for obtaining inequalities in x_i, reflecting the stability constraint, would be to use the Hermite matrix [20]. This matrix has entries which are quadratic forms in β_j, and the positive definiteness of the matrix (as checked, for example, by the positivity of leading principal minors) is a necessary and sufficient condition for (2.1) to be a stable polynomial. Each leading principal minor of the Hermite matrix will be a polynomial in β_j and therefore in x_j.

Assume therefore that an inequality set of the form (2.2) is available, with the particular derivation of that set being unimportant.

In Section III, it will be required that the $p_k(x)$ satisfy certain conditions. It is shown here that there is no loss of generality in imposing this requirement.

Lemma 2.1: Without significant loss of generality, it may be assumed in (2.2) that for each k:

a) $p_k(x)$ contains no multiple factors;

b) $p_k(x) \neq [r(x)]^2 \prod_{j \in S, j \neq k} p_j(x)$;

where $r(x) \in R(x)$, the field of real rational functions of x, and $S \subseteq \{1, 2, \cdots, m\}$.

Proof: Suppose $p_k(x)$ has a multiple factor $[f(x)]^\rho$. Divide $p_k(x)$ by the appropriate power of $[f(x)]^2$, either eliminating the multiple factor or reducing it to a simple factor, depending on the parity of ρ. Call the polynomial so obtained $\bar{p}_k(x)$. Then, if $\bar{x}$ is a specialization of x, $\bar{p}_k(\bar{x}) > 0$ implies $p_k(\bar{x}) > 0$ or $f(\bar{x}) = 0$. In the latter case, we may observe that the solution set of (2.2), or indeed $\bar{p}_k(x) > 0$ for $k = 1, 2, \cdots, m$, is open if nonempty, and accordingly there exists $\tilde{x}$ near $\bar{x}$ for which $f(\tilde{x}) \neq 0$ and for which $\bar{p}_k(\tilde{x}) > 0$. Thus the solutions of $p_k(x) > 0$ for $k = 1, 2, \cdots, m$ are dense in the solutions of $\bar{p}_k(x) > 0$ for $k = 1, 2, \cdots, m$ and there is no significant loss of generality in considering the latter set.

Next, suppose that for some k, S, and $r(x) \in R(x)$

$$p_k(x) = [r(x)]^2 \prod_{\substack{j \in S \\ j \neq k}} p_j(x).$$

Any solution $\bar{x}$ of $p_j(x) > 0, j \in \{1, 2, \cdots, k-1, k+1, \cdots, m\}$, causes $p_k(\bar{x}) > 0$ or $r(\bar{x})$ to be zero or infinite. A minor adjustment to the preceding argument shows that the solutions of (2.2) are dense in the set of solutions to (2.2) with the kth inequality dropped, and again there is no loss of generality. So, since a set of $p_k(x)$ which does not satisfy the conditions of the lemma can, for the purposes of the problem under consideration, be replaced by a set which does satisfy the conditions, there is no loss of generality in assuming that the conditions hold. ∇∇∇

Remarks: 1) Strictly speaking, condition a) of the lemma (for the purposes for which it is later used) can be relaxed to the requirement that $p_k(x)$ is not a perfect square. It is then interesting to note that if the set of $p_k(x)$ is replaced by positive integers p_k, and $r(x)$, by a rational number, condition b) and the relaxed condition a) are equivalent to the requirement that the quantities $\sqrt{p_k}$ be dissimilar quadratic surds.

2) In case one has

$$p_k(x) = -[r(x)]^2 \prod_{\substack{j \in S \\ j \neq k}} p_j(x)$$

there can be no solution to (2.2).

3) The calculations required to perform the replacement of $p_k(x)$, dictated by a failure of condition a), as well as those required to check condition b) involve nothing worse than a finite number of rational operations.

4) As a simple example, consider $p_1(x) = x_1^3 x_2$, $p_2(x) = x_1^4 x_2 x_3$, and $p_3(x) = x_1 x_3$. One replaces $p_1(x)$ by $x_1 x_2$, $p_2(x)$ by $x_2 x_3$, and then observes that $p_3(x) = x_2^{-2} p_1(x) p_2(x)$. This means that one can work with only $x_1 x_2 > 0$ and $x_2 x_3 > 0$. The final pair of inequalities, however, is equivalent to the original set provided $x_1 \neq 0$.

5) A polynomial which is a perfect square will reduce to the zero polynomial.

6) As implied in the proof of the lemma, if a factor has even multiplicity (this includes all factors of polynomials which are perfect squares) and hence is eliminated entirely from a polynomial, then that factor must be evaluated at any solution obtained from the revised set to ensure that it is nonzero; should it be zero for a given solution, there always exists a neighboring solution of the revised set at which the factor is nonzero.

Return now to (2.2). Following [16], by introducing new indeterminates $t_1, t_2, \cdots, t_m$, the inequality set can be replaced by an equality set:

$$f_i(t, x) = t_i^2 p_i(x) - 1 = 0, \quad i = 1, 2, \cdots, m. \tag{2.3}$$

Here t and x denote the m-tuple $(t_1, t_2, \cdots, t_m)$ and the n-tuple $(x_1, x_2, \cdots, x_n)$, respectively, and t must be finite. Evidently, equation (2.3) has a real finite solution $(\bar{t}, \bar{x})$ if and only if (2.2) has a real solution $(\bar{x})$. (Henceforth the finiteness of all solutions is to be explicitly understood.)

As remarked earlier, the set of real solutions of (2.2), if nonempty, is open, and the same therefore is true of (2.3). Consequently, if (2.3) has any real solutions at all, it has an infinite number. Selection of a finite number, by adjoining further polynomial equalities to (2.3) so that the extended set has only a finite number of solutions, is now tried. Of course, it is crucial to ensure that if (2.3) has a real solution so does the extended set. It would be possible to choose the additional equalities more or less arbitrarily in order to obtain for the extended set a finite number of solutions, each of which would define a solution to (2.3); however, there would be no *a priori* guarantee that a real solution would result this way.

The question of how a set of multivariable polynomial equalities can be solved will be addressed later; suffice it to say here that a solution procedure can be found to recover all solutions of the equality set, assuming the number of solutions is finite.

It is now illustrated how to add equalities to (2.3). Consider the problem of minimizing

$$J = \sum_{j=1}^{n} x_j^2 + \sum_{i=1}^{m} t_i^2 \tag{2.4}$$

over t, x subject to (2.3). It is clear that, if (2.3) has any real solutions, then the minimization problem will have a real solution, and if the minimization problem has a solution this defines a solution to (2.3) and therefore to the stabilization problem.

The constrained minimization problem is approached by seeking to minimize

$$A = \sum_{j=1}^{n} x_j^2 + \sum_{i=1}^{m} t_i^2 + \sum_{k=1}^{m} L_k (t_k^2 p_k(x) - 1) \tag{2.5}$$

where the L_k are Lagrange multipliers. Setting $(\partial A/\partial t_i) = 0$ yields

$$L_i = -p_i(x)^{-1}, \quad i = 1, 2, \cdots, m.$$

Setting $(\partial A/\partial x_j) = 0$ yields, upon substituting for L_i,

$$x_j - \frac{1}{2} \sum_{k=1}^{m} t_k^4 \frac{\partial p_k}{\partial x_j} = 0, \quad j = 1, 2, \cdots, n. \tag{2.6}$$

If there is a real minimum of (2.4) it is clear from (2.3) that p_i and t_i will be nonzero, so that at such a real minimum the Jacobian

$$J\left(\frac{f_1, f_2, \cdots, f_m}{t_1, t_2, \cdots, t_m}\right) = \prod_{i=1}^{m} 2 t_i p_i \neq 0. \tag{2.7}$$

As this condition is satisfied, it is guaranteed, by a standard theorem of calculus [21, see p. 198], that (2.3) and (2.6) will hold at the constrained minimum. Note that if (2.7) were not satisfied, it might be that the minimizing values of x, t (provided they exist) would not satisfy (2.3) and (2.6)

Now (2.3) and (2.6) constitute a system of $(m + n)$ polynomial equations in $(m + n)$ unknowns. If the stabilization problem has a real solution, the constrained minimization problem has a real solution which, as noted above, must satisfy (2.3) and (2.6). Conversely, *any* solution of (2.3) and (2.6)—not just those solving a constrained minimization problem—defines a solution of the stabilization problem, since (2.3) is satisfied. Hence the stabilization problem has a solution if and only if (2.3) and (2.6) have a solution.

Solution of the system (2.3) and (2.6) is discussed in Section IV. In general, r multivariable polynomial equations in r unknowns have a finite number of (possibly complex) solutions, but this is not always the case. In the case where the number of solutions is finite, they are all determinable in principle by numerical algorithms. If among them there is a real solution the stabilization problem is solved. On the other hand, difficulty arises if the number of solutions is infinite. One may not be able to determine them all and it is not clear how one might determine even the existence of a real solution among the infinite set of solutions, let alone how one might actually compute such a solution. Evidently then, one would like to ensure that the number of solutions to (2.3) and (2.6) is always finite. In an attempt to secure this objective, it was suggested in [15] that the objective function (2.4) of the minimization problem be replaced by

$$J_w = \sum_{j=1}^{n} \mu_j x_j^2 + \sum_{i=1}^{m} \nu_i t^2 \tag{2.8}$$

for some fixed positive numbers μ_j, ν_i with the side constraint (2.3) still enforced. It was also conjectured that for almost all choices of μ_j and ν_i, (2.3) and the modified (2.6) would have only a finite number of solutions. This might be called a "weighting" perturbation of the minimization problem because the indeterminates $x_1, \cdots, t_m$ are weighted by $\mu_1, \cdots, \nu_m$. The major contribution of this paper is to propose a different perturbation of the minimization problem, and then demonstrate that the resulting polynomial equation set in general has a finite number of solutions. A perturbation chosen via a suitable random experiment will, except for isolated cases, generate an equation with a finite number of solutions.

The new perturbation might be called a "center-changing" perturbation as it entails replacing the original objective function by

$$J_c = \sum_{j=1}^{n} (x_j - \delta_j)^2 + \sum_{i=1}^{m} (t_i - \gamma_i)^2 \tag{2.9}$$

for some fixed positive numbers γ_i, δ_j. The side constraint (2.3) is still enforced. It is now conjectured that, for almost all choices of γ_i and δ_j, equation (2.3) together with the appropriate variant on (2.6) will have only a finite number of solutions. The equations resulting from the objective function (2.9) are

$$t_i^2 p_i(x) - 1 = 0, \qquad i = 1, \cdots, m$$

$$\delta_j - x_j - \frac{1}{2} \sum_{k=1}^{m} \frac{\partial p_k(x)}{\partial x_j} (\gamma_k - t_k) t_k^3 = 0, \qquad j = 1, \cdots, n. \tag{2.10}$$

It will be shown in the next section that the number of solutions of (2.10) is infinite only for isolated values of γ_i and δ_j. Of course, any real solution of (2.10) yields a solution of the stabilization problem, and if the latter has a solution so do equations (2.10).

In practical terms, equations (2.10) can first be solved with all γ_i, δ_j set equal to zero. Should an infinite set of solutions arise, the values of γ_i, δ_j would be varied.

III. Demonstration of the Finiteness of the Number of Solutions

In (2.10) the fixed numbers γ_i, δ_j will now be regarded as indeterminates, and it will be shown that, in general, if γ_i and δ_j are arbitrary but fixed then the set (2.10) has a finite number of solutions.

In order to do this we will need the following lemma and theorem. The proofs of these are somewhat lengthy and the reader is advised to bypass the proofs on the initial reading.

Lemma 3.1: Let $p_k(x)$ for $x = (x_1, x_2, \cdots, x_n)$ and $k = 1, 2, \cdots, m$ be a set of polynomials in $R[x]$, none of which is identically zero, such that $p_k(x)$ contains no multiple factors and

$$p_k(x) \neq [r(x)]^2 \prod_{\substack{j \in S \\ j \neq k}} p_j(x) \tag{3.1}$$

where $r(x) \in R(x)$ and $S \subseteq \{1, 2, \cdots, m\}$. Let η_k, $k = 1, 2 \cdots, m$, be elements of an extension of $R(x)$ and algebraic over $R(x)$, defined by

$$\eta_k^2 - p_k(x) = 0, \qquad k = 1, 2, \cdots, m. \tag{3.2}$$

Then $\eta_m \notin R(x)$ $(\eta_1, \eta_2, \cdots, \eta_{m-1})$, i.e., η_m is not in the field obtained from extending by $\eta_1, \eta_2, \cdots, \eta_{m-1}$ the field of real rational functions in x.

Proof: The proof is done by induction, with the basis step corresponding to taking $m = 2$. For $m = 2$, assume $\eta_2 \in R(x)(\eta_1)$. Then η_2 can be represented as

$$\eta_2 = \frac{f_0(x) + f_1(x)\eta_1}{f_2(x) + f_3(x)\eta_1} \tag{3.3}$$

where $f_0(x)$, $f_1(x)$, $f_2(x)$, and $f_3(x)$ are rational functions ($f_2(x)$ and $f_3(x)$ are not both zero) and the numerator and denominator are polynomials in $R(x)[\eta_1]$. In (3.3) the numerator and denominator have, without loss of generality, no powers of η_1 greater than the first. This is so because $\eta_1^2 = p_1(x)$ and hence all terms may be reduced to the zeroth or first power of η_1. Now multiply the numerator and denominator of (3.3) by $(f_2(x) - f_3(x)\eta_1)$ to give

$$\eta_2 = \frac{f_0(x)f_2(x) - f_1(x)f_3(x)p_1(x) + \{f_0(x)f_3(x) - f_1(x)f_2(x)\}\eta_1}{f_2(x)^2 - f_3(x)^2 p_1(x)}.$$

Now $(f_2^2 - f_3^2 p_1)$ is nonzero, otherwise p_1 would be a perfect square in $R(x)$ and thus $R[x]$. Consequently we may write

$$\eta_2 = g_0(x) + g_1(x)\eta_1 \tag{3.4}$$

where $g_0(x) \in R(x)$ and $g_1(x) \in R(x)$.

Now $p_2(x)$ is not a perfect square so $\eta_2 \notin R(x)$. This condition requires that $g_1(x) \neq 0$ in (3.4). Also, in (3.4), $g_0(x) \neq 0$, otherwise $\eta_2 = g_1(x)\eta_1$, whence $\eta_2^2 = g_1(x)^2\eta_1^2$, i.e., $p_2(x) = g_1(x)^2 p_1(x)$ which violates condition (3.1). Rearranging (3.4) as

$$\eta_2 - g_0(x) = g_1(x)\eta_1$$

and squaring gives

$$\eta_2^2 - 2\eta_2 g_0(x) + g_0(x)^2 = g_1(x)^2 \eta_1^2$$

i.e.,

$$p_2(x) - 2\eta_2 g_0(x) + g_0(x)^2 = g_1(x)^2 p_1(x).$$

So

$$2\eta_2 g_0(x) = p_2(x) + g_0(x)^2 - g_1(x)^2 p_1(x).$$

Since $g_0(x) \neq 0$, this implies $\eta_2 \in R(x)$, which as remarked above is impossible. Hence $\eta_2 \notin R(x)(\eta_1)$ and the lemma is established for $m = 2$.

Now, in order to establish the recursion step of the induction, let $m = \mu + 1$ and consider the case where

$$\eta_i \notin R(x)(\eta_1, \eta_2, \cdots, \eta_{i-1}), \quad i = 1, 2, \cdots, \mu \quad (3.5)$$

holds. Assume (in order to ultimately obtain a contradiction) that

$$\eta_{\mu+1} \in R(x)(\eta_1, \eta_2, \cdots, \eta_\mu). \quad (3.6)$$

Then $\eta_{\mu+1}$ can be represented as

$$\eta_{\mu+1} = \frac{f_0(x, \eta_1, \cdots, \eta_{\mu-1}) + f_1(x, \eta_1, \cdots, \eta_{\mu-1})\eta_\mu}{f_2(x, \eta_1, \cdots, \eta_{\mu-1}) + f_3(x, \eta_1, \cdots, \eta_{\mu-1})\eta_\mu} \quad (3.7)$$

where $f_j(x, \eta_1, \cdots, \eta_{\mu-1})$ for $j = 0, \cdots, 3$ are members of $R(x)(\eta_1, \cdots, \eta_{\mu-1})$ with f_2 and f_3 not both zero. The numerator and denominator in (3.7) are both polynomials in $R(x)(\eta_1, \cdots, \eta_{\mu-1})[\eta_\mu]$. In (3.7) the numerator and denominator have, without loss of generality, no powers of η_μ greater than the first because $\eta_\mu^2 = p_\mu(x)$ and hence all terms may be reduced to the zeroth or first power of η_μ. Multiply the numerator and denominator of (3.7) by $f_2(x, \eta_1, \cdots, \eta_{\mu-1}) - f_3(x, \eta_1, \cdots, \eta_{\mu-1})\eta_k$ to give

$$\eta_{\mu+1} = \frac{(f_0 f_2 - f_1 f_3) + (f_0 f_3 - f_1 f_2)\eta_\mu}{f_2^2 - f_3^2 p_\mu}.$$

Now $f_2^2 - f_3^2 p_\mu$ is nonzero. Therefore, we may write

$$\eta_{\mu+1} = g_0(x, \eta_1, \cdots, \eta_{\mu-1}) + g_1(x, \eta_1, \cdots, \eta_{\mu-1})\eta_\mu \quad (3.8)$$

with $g_0(x, \eta_1, \cdots, \eta_{\mu-1})$ and $g_1(x, \eta_1, \cdots, \eta_{\mu-1}) \in R(x)(\eta_1, \cdots, \eta_{\mu-1})$. It can be seen that $g_1(x, \eta_1, \cdots, \eta_{\mu-1}) \neq 0$, otherwise $\eta_{\mu+1} \in R(x)(\eta_1, \cdots, \eta_{\mu-1})$ which contradicts the condition (3.5). To show that $g_0(x, \eta_1, \cdots, \eta_{\mu-1}) \neq 0$, suppose the contrary; then $\eta_{\mu+1} = g_1(x, \eta_1, \cdots, \eta_{\mu-1})\eta_\mu$ whence

$$p_{\mu+1}(x) = g_1(x, \eta_1, \cdots, \eta_{\mu-1})^2 p_\mu(x). \quad (3.9)$$

Ultimately, a contradiction to (3.6) is sought. However, for the moment, concentrate (in order to prove that $g_0 \neq 0$) on obtaining a contradiction arising from (3.9). This is done as follows. An argument like that leading to (3.8) shows that $g_1(x, \eta_1, \cdots, \eta_{\mu-1})$ can be written as $a_0(x, \eta_1, \cdots, \eta_{\mu-2}) + a_1(x, \eta_1, \cdots, \eta_{\mu-2})\eta_{\mu-1}$ with $a_0, a_1 \in R(x)(\eta_1, \cdots, \eta_{\mu-2})$. Then (3.9) becomes

$$\begin{aligned} p_{\mu+1}(x) = [&a_0(x, \eta_1, \cdots, \eta_{\mu-2})^2 \\ &+ 2a_0(x, \eta_1, \cdots, \eta_{\mu-2})a_1(x, \eta_1, \cdots, \eta_{\mu-2})\eta_{\mu-1} \\ &+ a_1(x, \eta_1, \cdots, \eta_{\mu-2})p_{\mu-1}(x)]\, p_\mu(x) \end{aligned}$$

and this violates condition (3.5) unless either $a_0 = 0$ or $a_1 = 0$. (One cannot have both $a_0 = 0$ and $a_1 = 0$ without making $p_{\mu+1}(x)$ zero.) Therefore, either

$$\begin{aligned} g_1(x, \eta_1, \cdots, \eta_{\mu-1}) &= a_0(x, \eta_1, \cdots, \eta_{\mu-2}) \\ &= b_0(x, \eta_1, \cdots, \eta_{\mu-3}) \\ &\quad + b_1(x, \eta_1, \cdots, \eta_{\mu-3})\eta_{\mu-2} \end{aligned}$$

or

$$\begin{aligned} g_1(x, \eta_1, \cdots, \eta_{\mu-1}) = [&b_2(x, \eta_1, \cdots, \eta_{\mu-3}) \\ &+ b_3(x, \eta_1, \cdots, \eta_{\mu-3})\eta_{\mu-2}]\, \eta_{\mu-1} \end{aligned}$$

with $b_j \in R(x)(\eta_1, \cdots, \eta_{\mu-3})$ for $j = 0, 1, 2, 3$. In the first case, it can be shown that either $b_0 = 0$ or $b_1 = 0$, and, in the second case, either $b_2 = 0$ or $b_3 = 0$. (The argument leading to these conclusions parallels that leading to the conclusion that either $a_0 = 0$ or $a_1 = 0$.) Consequently, $g_1(x, \eta_1, \cdots, \eta_{\mu-1})$ has one of the following forms:

$$b_0(x, \eta_1, \cdots, \eta_{\mu-3});$$
$$b_1(x, \eta_1, \cdots, \eta_{\mu-3})\eta_{\mu-2};$$
$$b_2(x, \eta_1, \cdots, \eta_{\mu-3})\eta_{\mu-1};$$
$$b_3(x, \eta_1, \cdots, \eta_{\mu-3})\eta_{\mu-2}\eta_{\mu-1}.$$

Continuing in this way it is shown that

$$g_1(x, \eta_1, \cdots, \eta_{\mu-1}) = r(x) \prod_{j \in S} \eta_j$$

where $S \subseteq \{1, 2, \cdots, \mu - 1\}$ and $r(x) \in R(x)$. When this expression for g_1 is used in (3.9), a contradiction to (3.1) is obtained. Since the above argument was predicated on the assumption that $g_0(x, \eta_1, \cdots, \eta_{\mu-1}) = 0$, it has been shown by contradiction that $g_0 \neq 0$. Recall also that $g_1 \neq 0$.

Returning to the task of establishing a contradiction to (3.6), square (3.8). This yields

$$\begin{aligned} p_{\mu+1} &= g_0(x, \eta_1, \cdots, \eta_{\mu-1})^2 \\ &\quad + 2g_0(x, \eta_1, \cdots, \eta_{\mu-1})g_1(x, \eta_1, \cdots, \eta_{\mu-1})\eta_\mu \\ &\quad + g_1(x, \eta_1, \cdots, \eta_{\mu-1})^2 p_\mu(x). \end{aligned}$$

Since g_0, g_1 are nonzero, η_μ can be expressed as an element of $R(x)(\eta_1, \cdots, \eta_{\mu-1})$, contradicting (3.5). Since this argument was predicated on the assumption that (3.6) holds, there exists a contradiction to (3.6). This completes the induction step of the lemma. ∇∇∇

The authors remark that an intuitive feel for the preceding lemma may be obtained by replacing the set of $p_k(x)$ by positive (nonperfect square) integers p_k with the $\sqrt{p_k}$ dissimilar surds. Then the lemma simply says that dissimilar surds cannot be connected by rational relations.

The lemma is the key to proving the following theorem, which again has an interpretation in terms of surds.

Theorem 3.1: If η_i $(i = 1, 2, \cdots, m)$ are defined as in the preceding lemma and $k \in R(x)(\eta_1, \eta_2, \cdots, \eta_m)$ is defined as

$$\begin{aligned} k = k_0(x) + \sum_{i=1}^{m} k_i(x)\eta_i + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} k_{ij}(x)\eta_i\eta_j \\ + \cdots + k_{1,2,\cdots,m}(x)\eta_1, \cdots, \eta_m \end{aligned}$$

where $k_0(x)$, $k_i(x)$, $k_{ij}(x)$, $\cdots$, $k_{1,2,\cdots,m}(x) \in R(x)$, then $k = 0$ implies that

$$k_0(x) = 0$$
$$k_i(x) = 0, \quad i = 1, 2, \cdots, m$$
$$k_{ij}(x) = 0, \quad i = 1, \cdots, m - 1; j = i + 1, \cdots, m$$
$$\vdots$$
$$k_{1,2,\cdots,m}(x) = 0.$$

Moreover, if

$$\begin{aligned} l = l_0 + \sum_{i=1}^{m} l_i(x)\eta_i + \sum_{i=1}^{m} \sum_{j=i+1}^{n} l_{ij}(x)\eta_i\eta_j \\ + \cdots + l_{1,2,\cdots,m}(x)\eta_1, \cdots, \eta_m \end{aligned}$$

with $l_0(x), l_i(x), l_{ij}(x), \cdots, l_{1,2,\cdots,m}(x) \in R(x)$, then $kl = 0$ implies that one of k or l is zero.

Proof: The first part is proved by induction. For the basis step, corresponding to $m = 1$, observe that $0 = k_0(x) + k_1(x)\eta_1$ with $k_0, k_1 \in R(x)$ implies $k_0 = k_1 = 0$ since $\eta_1 \notin R(x)$, $\eta_1 \neq 0$.

For the recursion step, assume the theorem is true for $m = 1, 2, \cdots, \mu$. It is proved true for $m = \mu + 1$. Suppose that

$$0 = k_0(x) + \sum_{r=1}^{\mu+1} k_i(x)\eta_i + \sum_{i=1}^{\mu} \sum_{j=i+1}^{\mu+1} k_{ij}(x)\eta_i\eta_j + \cdots + k_{1,2,\cdots,\mu+1}(x)\eta_1, \cdots, \eta_{\mu+1}.$$

Write the right-hand side as $g_0(x, \eta_1, \cdots, \eta_\mu) + g_1(x, \eta_1, \cdots, \eta_\mu)\eta_{\mu+1}$ with $g_0, g_1 \in R(x)(\eta_0, \eta_1, \cdots, \eta_\mu)$. By the lemma, $\eta_{\mu+1} \notin R(x)(\eta_0, \eta_1, \cdots, \eta_\mu)$ so that $g_0 = 0$ and $g_1 = 0$. By assumption, the theorem holds true for $m = \mu$, and the equation $g_0 = 0$ then yields

$$k_0(x) = 0$$
$$k_i(x) = 0, \quad \text{for } i = 1, 2, \cdots, \mu$$
$$k_{ij}(x) = 0, \quad \text{for } i = 1, 2, \cdots, \mu - 1; j = i + 1, \cdots, \mu$$
$$\vdots$$
$$k_{1,2,\cdots,\mu}(x) = 0$$

while $g_1 = 0$ implies that

$$k_{\mu+1}(x) = 0$$
$$k_{i,\mu+1}(x) = 0, \quad \text{for } i = 1, 2, \cdots, \mu$$
$$\vdots$$
$$k_{1,2,\cdots,\mu+1}(x) = 0.$$

Together, these two sets yield the truth of the first part of the theorem, for $m = \mu + 1$. The second part of the theorem is also proved by induction. For the basis step, corresponding to $m = 1$, it is assumed that

$$(k_0 + k_1\eta_1)(l_0 + l_1\eta_1) = 0 \tag{3.10}$$

whence

$$(k_0l_0 + k_1l_1p_1) + (k_0l_1 + k_1l_0)\eta_1 = 0.$$

By the first part of the theorem

$$k_0l_0 + k_1l_1p_1 = 0 \quad \text{and} \quad k_0l_1 + k_1l_0 = 0$$

or

$$k_0l_0l_1 + k_1l_1^2p_1 = 0 \quad \text{and} \quad k_0l_0l_1 + k_1l_0^2 = 0$$

or

$$k_1l_1^2p_1 = k_1l_0^2.$$

If $k_1 = 0$, equation (3.10) and the first part of the theorem yield quickly that either $k_0 = 0$ or $l_0 = l_1 = 0$ and the basis step is proved. If, on the other hand, $k_1 \neq 0$ then

$$l_1^2p_1 = l_0$$

i.e., $\eta_1 = \pm l_0/l_1$, which is a contradiction, or $l_1 = 0$ in which case $l_0 = 0$ and the basis step is proved.

For the recursion step, assume the claim is true for $m = 1, 2, \cdots, \mu$. It is the authors' aim to prove it true for $m = \mu + 1$. Consider the case where $m = \mu + 1$; then

$$k = g_0(x, \eta_1, \cdots, \eta_\mu) + g_1(x, \eta_1, \cdots, \eta_\mu)\eta_{\mu+1}$$
$$l = f_0(x, \eta_1, \cdots, \eta_\mu) + f_1(x, \eta_1, \cdots, \eta_\mu)\eta_{\mu+1}.$$

Setting $kl = 0$ yields

$$(g_0f_0 + g_1f_1p_{\mu+1}) + (g_0f_1 + g_1f_0)\eta_{\mu+1} = 0.$$

The first part of the theorem yields

$$g_0f_0 + g_1f_1p_{\mu+1} = 0 \quad \text{and} \quad (g_0f_1 + g_1f_0) = 0.$$

The proof then proceeds in the same manner as the basis step, making use of the first part of the theorem at appropriate places. ∇∇∇

The above theorem will be used to prove that the variety defined by (2.10), repeated here for convenience,

$$t_i^2p_i(x) - 1 = 0, \quad i = 1, 2, \cdots, m$$
$$\delta_j - x_j - \frac{1}{2}\sum_{k=1}^{m} \frac{\partial p_x(x)}{\partial x_j}(\gamma_k - t_k)t_k^3 = 0, \quad j = 1, 2, \cdots, n \tag{3.11}$$

is irreducible.

Lemma 3.2: If $p_k(x)$ satisfy the conditions of Lemma 3.1 with x, t, γ, δ as indeterminates, equations (3.11) define an irreducible affine variety V_A over R.

Proof: Inspection of (3.1) reveals that all points on V_A are specializations of the point in (x, t, γ, δ) = space:

$$(X_1, \cdots, X_n, T_1^\pm, \cdots, T_m^\pm, \Gamma_1, \cdots, \Gamma_m, \Delta_1, \cdots, \Delta_n)$$

where $X_1, \cdots, X_n$ and $\Gamma_1, \cdots, \Gamma_m$ are indeterminates and

$$T_i^\pm = \pm\frac{1}{\sqrt{p_i(X)}}.$$

For $i = 1, 2, \cdots, n$ and $j = 1, 2, \cdots, m$,

$$\Delta_j = X_j + \frac{1}{2}\sum_{k=1}^{m} \frac{\partial p_x(X)}{\partial X_j}(\Gamma_k - T_k^\pm)(T_k^\pm)^3.$$

This can be verified by substitution in (3.11) with x_j and γ_k serving as independent variables. Notice that for all solutions of (3.11), $p_i(x) \neq 0$ for each i, so the quantities $T_i^\pm$ are well defined. Notice also that, as noted in Appendix II, points on V_A are *not* restricted to being real; V_A is a variety over R because its defining equations are over R, not because the points on it are restricted to being in R.

Define a point

$$P = (X_1, \cdots, X_n, T_1^+, \cdots, T_m^+, \Gamma_1, \cdots, \Gamma_m, \Delta_1, \cdots, \Delta_m).$$

If $f(x, t, \gamma, \delta)$ is a polynomial which vanishes on V_A, then $f(P)$, regarded as an algebraic function of X and Γ, is zero on V_A. Let k and l be two polynomials in $R[x, t, \gamma, \delta]$ such that kl vanishes on V_A; then

$$k(P)l(P) = 0$$

on V_A. The functions $k(P)$ and $l(P)$ can be expressed as

$$k(P) = k_0(X, \Gamma) + \sum_{i=1}^{n} k_i(X, \Gamma)\frac{1}{\sqrt{p(X)}} + \sum_{i=1}^{m}\sum_{j=i+1}^{m} k_{ij}(X, \Gamma)\frac{1}{\sqrt{p_i(X)}}\frac{1}{\sqrt{p_j(X)}} + \cdots$$

$$+ k_{1,2,\cdots,m}(X,\Gamma)\frac{1}{\sqrt{p_1(X)}}\frac{1}{\sqrt{p_2(X)}}\cdots\frac{1}{\sqrt{p_m(X)}} \tag{3.12}$$

$$l(P) = l_0(X,\Gamma) + \sum_{i=1}^{n} l_i(X,\Gamma)\frac{1}{\sqrt{p_i(X)}} + \sum_{i=1}^{m}\sum_{j=1+1}^{m} l_{ij}(X,\Gamma)\frac{1}{\sqrt{p_i(X)}}\frac{1}{\sqrt{p_j(X)}} + \cdots + l_{1,2,\cdots,m}(X,\Gamma)\frac{1}{\sqrt{p_1(X)}}\cdots\frac{1}{\sqrt{p_m(X)}}$$

where $k_0, k_i, k_{ij}, \cdots, k_{1,2,\cdots,m}, l_0, l_i, l_{ij}, l_{1,2,\cdots,m}$ are rational functions in $R(X,\Gamma)$. Since $p_i(X)$ satisfy the required conditions of Theorem 3.1, their inverses also satisfy the conditions, and so, by Theorem 3.1, either $k(P)$ or $l(P)$ is zero. Suppose it is k. Then by the first part of Theorem 3.2

$$k_0 = 0 \quad k_i = 0 \quad k_{ij} = 0 \quad \cdots \quad k_{1,2,\cdots,m} = 0.$$

Now suppose the coordinates of any point of V_A are substituted into $k(x,t,\gamma,\delta)$. These coordinates differ from those of some specializations of P only in the possible replacement of one or more T_i^+ by T_i^- with consequent adjustment to one or more of the Δ_j. The value of $k(\cdot,\cdot,\cdot,)$ at such a point will be given by the right-hand side of (3.12) except that the coefficients of some of the radical terms will undergo a sign change. Thus they will continue to be zero and hence k will take the value zero. Therefore k is zero at all points of V_A. So by [24, p. 23, 24] the ideal I_A associated with V_A is prime and hence V_A is irreducible [25, p. 8]. ∇∇∇

The variety V_A has a function ring R_A defined as $R[x,t,\gamma,\delta]/I_A$. In other words R_A consists of equivalence classes of polynomials such that two polynomials are in the same equivalence class if and only if their difference is in I_A, i.e., vanishes on V_A.

R_A is generated by the equivalence classes of $[X_i]$, $[T_j^+]$, $[\Gamma_k]$, and $[\Delta_l]$, where

$$[X_i] = \{f : f = X_i + g(X, T^+, \Gamma, \Delta); g \in I_A\}, \qquad i = 1, 2, \cdots, n$$

etc.

Since V_A is irreducible, it follows that R_A is an integral domain [25, p. 10] and thus extends in the usual way to a field $R(x,t,\gamma,\delta)/I_A$. This field is generated by

$$x_i = [X_i] \quad t_j = [T_j^+] \quad \gamma_k = [\Gamma_k] \quad \delta_l = [\Delta_l].$$

The dimension of V_A is the degree of transendence of this field [24, p. 53].

It is obvious from (3.11) that $\{x_i\}$ and $\{\gamma_k\}$ can be chosen as algebraically independent and that $\{t_j\}$ and $\{\delta_l\}$ are then algebraically dependent. That is dim $V_A = m + n$.

It will now be shown that the $(m+n)$ indeterminates $\{\gamma_k\}$ and $\{\delta_l\}$ can be taken as algebraically independent, which will be used to demonstrate the fact that equations (3.11) generically have a finite number of solutions for arbitrary but fixed Γ, Δ.

Lemma 3.3: There exists a point Γ^0, Δ^0 in $(m+n)$-space such that for all (Γ,Δ) in an arbitrarily small neighborhood of (Γ^0,Δ^0) there exists a set of (X,T) such that (X,T,Γ,Δ) is a point on the variety V_A.

Proof: On the variety V_A

$$\Delta_j = X_j + \frac{1}{2}\sum_{k=1}^{m}\frac{\partial p_k(X)}{\partial X_j}\left(\Gamma_k - \frac{1}{\sqrt{p_k(X)}}\right)\frac{1}{p_k(X)^{3/2}}$$

(where $(1/\sqrt{p_k(X)}$ has been substituted for $T_k(X)$).

Choose $\Gamma_k^0 = 0$ $(k = 1, 2, \cdots, m)$; then

$$\Delta_j = X_j + \frac{1}{2}\sum_{k=1}^{m}\frac{\partial p_k(X)}{\partial X_j}\frac{1}{p_k(X)^2}. \tag{3.13}$$

So the Jacobian of the $\{\Delta_l\}$ with respect to the $\{X_i\}$ is

$$J\begin{pmatrix}\Delta_1,\cdots,\Delta_n\\ X_1,\cdots,X_n\end{pmatrix} = I - \frac{1}{2}\left\{\sum_{k=1}^{m}\left(\frac{\partial^2 p_k(X)}{\partial X_j \partial X_i}\frac{1}{p_k(X)^2} - \frac{2}{p_k(X)^3}\frac{\partial p_k(X)}{\partial X_i}\frac{\partial p_k(X)}{\partial X_j}\right)\right\} = I + \frac{1}{2}H\left(\sum_{k=1}^{m}\frac{1}{p_k(X)}\right)$$

where $H[\Sigma_{k=1}^m (1/p_k(X))]$ is the Hessian matrix of $\Sigma_{k=1}^m (1/p_k(X))$.

The claim of the lemma will be shown to follow if it can be shown that for some X^0, Δ^0, related by (3.13), the Jacobian is nonsingular.

Indeed this is the case. If the maximum degree of the $p_k(x)$ is r, one can check that along almost all rays $x_1 = \rho a_1, \cdots, x_n = \rho a_n$, ρa_i is fixed, ρ is real and variable, $\Sigma_{k=1}^m (1/p_k(X))$ behaves as ρ^{-r} for large r, and $H[\Sigma_{k=1}^m (1/p_k(X))]$ has entries all of which behave as ρ^{-r-2} for large r. Accordingly, the Jacobian is approximated by the identity matrix.

Choosing X^0 to ensure a nonsingular Jacobian, denote the corresponding Δ by Δ^0. Then by the implicit function theorem [21, p. 117] for all Γ, Δ in the neighborhood of (Γ^0, Δ^0) there exists X and T satisfying (3.11). ∇∇∇

Lemma 3.4: On the variety V_A defined by (3.11) $\{\Gamma_i\}$, $\{\Delta_j\}$ are algebraically independent.

Proof: For the purposes of a proof by contradiction, assume that $\{\Gamma_i\}$, $\{\Delta_j\}$ are not algebraically independent. Then there exists a polynomial f which is not identically zero such that

$$f(\Gamma, \Delta) = 0$$

on V_A. However from Lemma 3.3 it is known that there exists a point (Γ^0, Δ^0) such that all points (Γ, Δ) within some neighborhood of (Γ^0, Δ^0) together with some (X, T) yield points on the variety. So $f(\Gamma, \Delta) = 0$ for all points in this neighborhood. Then $f(\Gamma, \Delta)$ is identically zero which is a contradiction. Hence $\{\Gamma_i\}$, $\{\Delta_j\}$ are algebraically independent. ∇∇∇

Now since the $(m+n)$ indeterminates (Γ, Δ) are algebraically independent and since the degree of transcendence of the function field of V_A is $(m+n)$ then all other variables are algebraically dependent on these; i.e., there are polynomials f_i such that

$$\begin{aligned} f_i(x_i, \gamma, \delta) &= 0, \qquad i = 1, 2, \cdots, n \\ f_{j+n}(t_j, \gamma, \delta) &= 0, \qquad j = 1, 2, \cdots, m \end{aligned} \tag{3.13}$$

for all $\{x_i\}$, $\{t_j\}$ on V_A.

The polynomial f_i can be regarded as a polynomial in x_i with coefficients in the ring $R[\gamma, \delta]$. For almost all fixed choices Γ, Δ of γ and δ, these coefficients will not all take the value zero and there will then be a finite number of values of x_i satisfying the polynomial. More generally, equation (3.13) and thus equations (3.11) will have a finite number of solutions, (X, T) for almost all choices of (Γ, Δ). This is the result it was set out to establish.

IV. Solution of Multivariable Polynomial Equalities

Formal procedures for solving multivariable polynomial equalities have been known for a long time. One can find descriptions of such procedures, which depend on the calculation of resultants, in [22], [23] for example. Appendix I should also make clear the idea that such equalities may be tackled by successively eliminating one variable at a time, until one polynomial equation (or possibly more) in a single variable is obtained. This may be solved by some root-finding algorithm (interestingly, certain root-finding algorithms do use resultants, see [26]); its solutions are then used to obtain the values of the last variable eliminated prior to obtaining the single-variable equation. Again, solving a polynomial equation in a single variable is involved. The process is repeated till one finds solution values of all variables in the original equation set, assuming there are a finite number.

Evidently, the task is, in broad terms, twofold. Elimination of variables is required, and polynomial root finding is required. Regarding the second task, much has of course been written. The first task, viewed as a problem of numerical analysis, is discussed in [27]-[31]. It is worth noting that a computational explosion appears: to compute the resultant of two r-variable polynomials of degree d, one may require $0(d+1)^r$ calculations.

In the remainder of this section, two possible simplications to this elimination task are indicated, one arising from the special form of this problem.

Suppose that in (2.10) γ_k and δ_j are all zero; i.e., the system in question is

$$t_i^2 p_i(x) - 1 = 0, \qquad i = 1, 2, \cdots, m$$

$$x_j - \frac{1}{2}\sum_{k=1}^{m} \frac{\partial p_k(x)}{\partial x_j} t_k^4 = 0, \qquad j = 1, 2, \cdots, n. \qquad (4.1)$$

The first simplification involves the elimination of the variables t_i without the intervention of resultants. Multiply the jth equation in the last n equations of (4.1) by

$$\prod_{i \in S_j} [p_i(x)]^2 \qquad \text{when} \qquad S_j = \left\{ i \,\middle|\, \frac{\partial p_i(x)}{\partial x_j} \equiv 0 \text{ fails} \right\}.$$

When this is done and one uses the first m equations of (4.1), there results

$$x_j \prod_{i \in S_j} [p_i(x)]^2 - \frac{1}{2}\sum_{k=1}^{m} \frac{\partial p_k(x)}{\partial x_j} \prod_{i \in S_j - \{k\}} [p_i(x)]^2 = 0,$$

$$j = 1, 2, \cdots, n. \qquad (4.2)$$

This is a set of n polynomial equations in n unknowns. Certainly any solution of (4.1) satisfies this set of equations, and any solution $\bar{x}$ of (4.2) for which $p_i(x) \neq 0$ for all i defines a solution of (4.1). Provided then that (4.2) has a finite number of solutions (which is not guaranteed), one can solve the original problem using (4.2).

The above argument needs a major modification in case one or more of γ_k is nonzero; the details are omitted here.

The second possible simplification comes about as follows. Consider a multivariable polynomial equality set

$$f_i(x_1, x_2, \cdots, x_r) = 0, \qquad i = 1, 2, \cdots, r. \qquad (4.3)$$

Let $g_j(x_1, \cdots, x_{r-1})$, for j in some indexing set, be a set of resultants with respect to x_r of various distinct pairs of f_i in (4.3). For example, g_1 may be Res (f_1, f_2), g_2 may be Res (f_2, f_3), etc. The number of such g_j is left unspecified.

Similarly, one can consider a set of pairwise resultants $h_k(x_1, \cdots, x_{r-2})$ defined from g_j, and, in fact, one can continue the process down to a one-variable polynomial. The following observations are then made.

1) If $f_i(\bar{x}_1, \cdots, \bar{x}_r) = 0$ for all i, then $g_j(\bar{x}_1, \cdots, \bar{x}_{r-1}) = 0$ for all j, and $h_k(\bar{x}_1, \cdots, \bar{x}_{r-2}) = 0$, and so on for all pairwise resultants with fewer variables.

2) (This is a consequence of above.) If $g_j(x_1, \cdots, x_{r-1}) = 0$, for all j, has at most a finite number of solutions so does $f_i(x_1, \cdots, x_r) = 0$ for all i. If $h_k(x_1, \cdots, x_{r-2}) = 0$, for all k, has at most a finite number of solutions so does $g_j(x_1, \cdots, x_{r-1}) = 0$ for all j. Ultimately, if all one-variable pairwise resultants have at most a finite number of (common) solutions so does $f_i(x_1, \cdots, x_r) = 0$ for all i.

3) If $g_j(\tilde{x}_1, \cdots, \tilde{x}_{r-1}) = 0$ for all j, by polynomial factorization one can check if there exist values of x_r such that $f_i(\tilde{x}_1, \cdots, \tilde{x}_{r-1}, x_r) = 0$. Combining this observation with 1, it follows that if all solutions of $g_j(x_1, \cdots, x_{r-1}) = 0$ are known and are finite in number, all solutions (if any) of $f_i(x_1, \cdots, x_r) = 0$ can be found by polynomial factorization. Extending this idea to pairwise resultants involving fewer variables, one sees that, ultimately, from the set of one-variable pairwise resultants, *provided* the set is nonempty, one can construct all the solutions of $f_i(x_1, \cdots, x_r) = 0$ by polynomial factorization.

From the third observation, it is concluded that the key to the simplification is to ensure that at least one pairwise resultant with only one variable is obtained. This may or may not be possible in a given situation. It is probably sensible to initially compute $(r-1)$ of the set of g_j, $(r-2)$ of the set of h_k, etc., on the grounds that, generally, p polynomial equations in p unknowns have a finite number of solutions. If this fails to lead to a one-variable resultant which is not identically zero, one could introduce further pairwise resultants.

V. An Example of the Procedure

As an example of the procedure for computing a stabilizing output feedback, consider the example in [15, p. 59]. The plant to be stabilized is

$$\dot{x} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 13 & 0 \end{bmatrix} x + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u$$

$$y = \begin{bmatrix} 0 & 5 & -1 \\ -1 & -1 & 0 \end{bmatrix} x. \qquad (5.1)$$

For the indeterminate gain matrix $K = [v, w]$ the closed-loop system matrix is

$$F + GKH' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -w & 5v - w + 13 & -v \end{bmatrix}$$

which has the characteristic polynomial $s^3 + v^2 s + (w - 5v - 13) + w$. The Lienard–Chipart test implies that for a stabilizing feedback law one needs real v and w satisfying

$$p_1(v, w) = w(v - 1) - v(5v + 13) > 0$$

$$p_2(v, w) = v > 0$$

$$p_3(v, w) = w > 0. \qquad (5.2)$$

This inequality set corresponds to (2.2), and, since it clearly satisfies the conditions set out in Lemma 2.1, can be used to

The final point which should be made is that the ideas in this paper apply to numerous problems other than the output-feedback stabilization problem, such as, for example, the problems mentioned in [15, p. 65]. The output-feedback stabilization problem has simply been used as a peg on which to hang the ideas.

Appendix I
Resultants and Resultant Systems

Resultant of Two Polynomials in a Single Indeterminate

Consider the two polynomials

$$f_1(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$
$$f_2(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0. \quad \text{(A1.1)}$$

One may simply be concerned with equations whose coefficients lie in some given ground field K (e.g., the field of real or rational numbers), or one may consider equations with coefficients which belong to an extension of K, see [22, p. 146]. A case of particular interest arises when the coefficients lie in $K[\alpha, \beta, \cdots, \delta]$, the ring of polynomials in certain independent indeterminates $\alpha, \beta, \cdots, \delta$ over the ground field K. In this way one can arrange for (A1.1) to have indeterminate coefficients.

The resultant of the polynomials $f_1(x)$ and $f_2(x)$ with respect to x (or relative to x) is defined as follows:

$$\operatorname{Res}(f_1, f_2) = \det \begin{bmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \cdots & & & & & & & \cdots \\ 0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_2 & b_1 & b_0 & \cdots & 0 \\ \cdots & & & & & & & \cdots \\ 0 & 0 & \cdots & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix} \quad \text{(A1.2)}$$

Since $\operatorname{Res}(f_1, f_2)$ is a determinant of the coefficients, it is a polynomial in the coefficients of $f_1(x)$ and $f_2(x)$, which is independent of x.

The representation of $\operatorname{Res}(f_1, f_2)$ shown in (A1.2) is the Sylvester form. This is the simplest representation, but there are better methods of computing $\operatorname{Res}(f_1, f_2)$ than by evaluating the determinant in (A1.2). (See, for example, [27], [28].)

Theorem A1.1: $\operatorname{Res}(f_1, f_2) = 0$ if and only if either $a_n = b_m = 0$ or $f_1(x)$ and $f_2(x)$ have a common factor of positive degree in x.

Proof: See [18, p. 298].

Corollary: $\operatorname{Res}(f_1, f_2) = 0$ if and only if either $a_n = b_m = 0$ or the two polynomial equations

$$f_1(x) = 0$$
$$f_2(x) = 0 \quad \text{(A1.3)}$$

have a common solution in a suitable extension field of K.

Example 1: For $f_1(x) = x^2 + 3x + 2$ and $f_2(x) = x + 2$,

$$\operatorname{Res}(f_1, f_2) = \det \begin{vmatrix} 1 & 3 & 2 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{vmatrix} = 0.$$

So $x^2 + 3x + 2 = 0$ and $x + 2 = 0$ have a common solution.

Example 2: This is an example of a case with coefficients in the ring of polynomials $R[y]$. The polynomials are $f_1(x) = x^2 + 3yx + 2y$ and $f(x) = yx + 2$. Since the polynomials have indeterminate coefficients, the resultant will involve the indeterminate y.

$$\operatorname{Res}(f_1, f_2) = \det \begin{vmatrix} 1 & 3y & 2y \\ y & 2 & 0 \\ 0 & y & 2 \end{vmatrix} = 4 - 6y^2 + 2y^3.$$

So $x^2 + 3yx + 2y = 0$ and $yx + 2 = 0$ have a common solution if and only if $2y^3 - 6y^2 + 4 = 0$. (Note that the leading coefficients are not zero.) This result holds for any particular value of y, i.e., for a "specialization" of the indeterminate y. In particular the specialization $y = 1$ gives the same result as example 1 above.

The resultant of two inhomogeneous polynomials has been studied. Now, on the other hand, consider two homogeneous polynomial equations in the two unknowns x_0, x_1:

$$f_1(x_0, x_1) = a_n x_1^n + a_{n-1}x_0 x_1^{n-1} + \cdots + a_0 x_0^n = 0$$
$$f_2(x_0, x_1) = b_m x_1^m + b_{m-1}x_0 x_1^{m-1} + \cdots + b_0 x_0^m = 0 \quad \text{(A1.4)}$$

where the coefficients lie in some field or ring K, similar to the coefficients of (A1.1). Define the resultant $\operatorname{Res}(f_1, f_2)$ as in (A1.2). Theorem A1.1 can be restated for homogeneous equations without the alternative condition $a_n = b_m = 0$, provided that the usual convention of disregarding the trivial solution $(x_0 = 0, x_1 = 0)$, which always exists for homogeneous polynomial equations, is adopted.

Theorem A1.2: With $f_1(x_0, x_1)$ and $f_2(x_0, x_1)$ as in (A1.4), then $\operatorname{Res}(f_1, f_2) = 0$ if and only if $f_1(x_0, x_1) = 0$ and $f_2(x_0, x_1) = 0$ have a common solution in a suitable extension field of K.

Proof: This result follows trivially from the corollary of Theorem A1.1. If $\operatorname{Res}(f_1, f_2) = 0$, either equations (A1.1) have a common solution, α say, in which case $(1, \alpha)$ is a common solution of (A1.4), or $a_n = b_m = 0$, in which case $(0, x_1)$ is a solution of equations (A1.4) for arbitrary x_1. Conversely, if equations (A1.4) have a common solution of the form $(1, \alpha)$, equations (A1.1) have a common solution α and $\operatorname{Res}(f_1, f_2) = 0$, while if there is a common solution of the form $(0, \alpha)$, $\alpha \neq 0$, equations (A1.4) imply $a_n = b_m = 0$ whence $\operatorname{Res}(f_1, f_2) = 0$ again.

A. Resultant Systems

Now consider systems of r polynomial equations.

Theorem A1.3: Given r polynomials $f_1(x), \cdots, f_r(x)$ in one indeterminate x and with indeterminate coefficients, there exists a set of polynomials $d_1, \cdots, d_N$ in the coefficients of $f_i(x)$, with the property that for specializations of the coefficients the conditions $d_1 = 0, \cdots, d_N = 0$ are necessary and sufficient to ensure that either the equations

$$f_i(x) = 0, \qquad i = 1, \cdots, r \quad \text{(A1.5)}$$

are soluble in some extension field of the field of coefficients (if the coefficients lie in a ring then the quotient field of that ring is the field of coefficients) or the leading coefficients in $f_1(x), \cdots, f_r(x)$ all vanish.

Proof: See [22, pp. 156-158]. The procedure for constructing the d_i is also outlined in this reference.

The polynomials $d_1, \cdots, d_N$ are called a resultant system of the set of equations (A1.5).

Theorem A1.3 can be extended to multivariable polynomials as follows.

Theorem A1.4: Given r polynomial equations in n unknowns,

$$f_i(x_1, \cdots, x_n) = 0, \quad i = 1, \cdots, r \tag{A1.6}$$

with indeterminate coefficients, there exists a set of polynomials (which are polynomials in the indeterminate coefficients of f_i and in $x_1, \cdots, x_{n-1}$), call them $h_i(x_1, \cdots, x_{n-1})$, $i = 1, \cdots, N$, such that, for specialization of the coefficients of f_i, the condition that

$$h_i(x_1, \cdots, x_{n-1}) = 0, \quad i = 1, \cdots, N \tag{A1.7}$$

has a solution is necessary and sufficient to ensure that i) (A1.6) has a solution, or ii) the coefficients of the highest degree term in x_n in $f_1, \cdots, f_r$ all vanish at the solution of (A1.7).

An alternative statement of the theorem which indicates the relationship between the solutions of (A1.6) and (A1.7) states that the polynomials $h_i(x_1, \cdots, x_{n-1})$, $i = 1, \cdots, N$, described above have the following properties (where $\bar{x}_i$ is a specialization of x_i).

i) The necessary conditions for the equations, in the single indeterminate x_n

$$f_i(\bar{x}_1, \cdots, \bar{x}_{n-1}, x_n) = 0 \tag{A1.8}$$

to have a solution are $h_i(\bar{x}_1, \cdots, \bar{x}_{n-1}) = 0, i = 1, \cdots, N$.

ii) If $h_i(\bar{x}_1, \cdots, \bar{x}_{n-1}) = 0, i = 1, \cdots, N$, then either (A1.8) has a solution or all the highest degree coefficients of the polynomials $f_i(\bar{x}_1, \cdots, \bar{x}_{n-1}, x_n)$, in the single indeterminate x_n, are zero.

Proof: Reference [22, p. 162] discusses the theorem for coefficients in a ground field K but the discussion is also valid for the theorem as stated above with indeterminate coefficients.

If the system (A1.6) consists of equations involving polynomials which are homogeneous in $x_0, x_1, \cdots, x_n$, then the statement of Theorem A1.4 can be modified to leave out the condition that all the coefficients of highest degree in x_n must not be zero, and the polynomials h_i become homogeneous.

The set of polynomials h_i is called a resultant system of (A1.6) with respect to x_n.

It is shown in [22, p. 163] how, by a suitable preliminary (invertible) change of variables, the possibility of the leading coefficients being zero in the inhomogeneous case can be avoided. By means of this change of variables one can obtain a resultant system of polynomial equations in $(n - 1)$ unknowns, for which the existence of a solution is a necessary and sufficient condition for the existence of a solution to (A1.6) in n unknowns.

This process, of changing variables and then eliminating one variable by computing a resultant system with respect to it, can be repeated n times to eliminate n variables subject to a proviso below. The result is a set of polynomials $d_1, \cdots, d_s$ in the original coefficients of the polynomial f_i (i.e., $x_1, \cdots, x_n$ have been eliminated), for which the properties $d_1 = 0, \cdots, d_s = 0$ are necessary and sufficient conditions for the existence of a solution to the set (A1.6). The final set of polynomials is called the resultant system of (A1.6) with respect to $x_1, \cdots, x_n$.

It is possible for the elimination process to yield at some stage a system consisting of either a single equation in more than one unknown or no equation at all. In the first case, the original system may be solved for all specializations of all but one of the unknowns, and, in the second case, for all specializations of all the variables appearing in the equation set whose resultant system vanishes on elimination of one variable, i.e., the equation set encountered in the next to last stage. In either case, there is an infinite number of solutions to the original set. One can still conceive of the elimination process being repeated n times, but the resultant system obtained consists of identically zero polynomials.

When it is not required that all variables be eliminated, one has the following result.

Theorem A1.5: Given r homogeneous polynomial equations in m unknowns

$$f_i(x_1, \cdots, x_m) = 0, \quad i = 1, \cdots, r \tag{A1.9}$$

with coefficients in the ground field K, there exists a set of homogeneous polynomials, in the coefficients of f_i, $h_i(x_1, \cdots, x_t)$, $i = 1, \cdots, s$, with the property that, if $\bar{x}_i$ is a specialization of x_i,

$$f_i(\bar{x}_1, \cdots, \bar{x}_t, x_{t+1}, \cdots, x_m) = 0 \quad i = 1, \cdots, r$$

has a solution if and only if

$$h_i(\bar{x}_1, \cdots, \bar{x}_t) = 0, \quad i = 1, \cdots, s.$$

The set of polynomials h_i is called the resultant system of (A1.9) with respect to $x_{t+1}, \cdots, x_m$. The "only if" part of the theorem remains true for nonhomogeneous polynomials $f_i(x_1, \cdots, x_m)$.

Appendix II
Varieties

The material in this appendix is intended as a summary of some of the major principles and theorems involved with the geometrical concept of a variety. The ground field over which spaces will be constructed need only be commutative with characteristic zero, but the authors are concerned, in particular, with the real field R, and their discussion will be couched in terms of the ground field being R.

A. Varieties

Consider the set of points whose coordinates satisfy the equations

$$f_i(x_0, x_1, \cdots, x_m) = 0, \quad i = 1, \cdots, s \tag{A2.1}$$

where $f_i(x_0, \cdots, x_m) \in R[x_0, \cdots, x_m]$ are polynomials in $x_0, \cdots, x_m$ with real coefficients. The aggregate of points defined by the solution set of (A2.1) is called an algebraic variety or simply a variety. For example consider the following pair of equations:

$$\begin{aligned} t_1^2 x_1 - x_2^3 &= 0 \\ x_1 - x_2 &= 0. \end{aligned} \tag{A2.2}$$

The variety V defined by these equations is the set of points $(\bar{x}_1, \bar{x}_2, \bar{t}_1)$ for which equations (A2.2) are simultaneously satisfied.

The authors remark that the integer s in (A2.1) is finite, and that $(\bar{x}_1, \bar{x}_2, \bar{t}_1)$ are not restricted to the ground field, here R, but may be in an extension field, e.g., the complex field.

The notion of a variety is essentially the same as the notion of a polynomial ideal. (A polynomial ideal over R is a set of polynomials in $R[x_0, \cdots, x_m]$ closed under addition, subtraction, and multiplication by any polynomial in $R[x_0, \cdots, x_m]$.) For it can be shown, see [24, p. 17], that the set of polynomials which are zero at all solutions of (A2.1) constitute a polynomial ideal. (Polynomial ideals will subsequently be referred to simply as ideals.) Conversely the set of points *which are zeros of all polynomials in an ideal* is a variety [24, p. 17]. (The technical point at issue in proving the converse is to show that the set of points which are zeros of all polynomials of the ideal is identical to the set of points which are zeros of a *finite* set of polynomials of the ideal; the tool for doing this is Hilbert's Basis Theorem.)

B. Irreducible Varieties

A variety V is reducible if it can be expressed as the "sum" of two varieties, each of which is distinct from V. (The sum of two varieties is the totality of points lying on the two varieties.)

If a variety is not reducible it is said to be irreducible.

Theorem A2.1: A necessary and sufficient condition for the reducibility of a variety V is the existence of a product fg of two polynomials, $f(x_0, \cdots, x_m)$ and $g(x_0, \cdots, x_m) \in R[x_0, \cdots, x_m]$, which vanishes at all points of V without either polynomial having this property.

Proof: The theorem is proved in [24, p. 23].

For example consider the following system of equations in six-dimensional affine space with points represented by $(x_1, x_2, x_3, t_1, t_2, t_3)$.

$$f_1 = t_1^2 x_1 x_2 - 1 = 0$$
$$f_2 = t_2^2 x_2 x_3 - 1 = 0$$
$$f_3 = t_3^2 x_1 x_3 - 1 = 0. \tag{A2.3}$$

The set of solutions of (A2.3) defines a variety V. Consider now the two polynomials $g_1 = t_1 t_2 x_1 x_2 - t_3 x_1$ and $g_2 = t_1 t_2 x_2 x_3 + t_3 x_3$. Observe that

$$g_1 g_2 = t_1^2 t_2^2 x_1 x_2^2 x_3 - t_3^2 x_1 x_3$$
$$= (t_1^2 x_1 x_2)(t_2^2 x_2 x_3) - (t_3^2 x_1 x_3).$$

Clearly $g_1 g_2 = 0$ on V. However the point $(1, 1, 1, 1, 1, 1) \in V$ is not a zero of g_2 and the point $(1, 1, 1, -1, 1, 1) \in V$ is not a zero of g_1. Neither g_1 nor g_2 vanishes on V, but $g_1 g_2$ vanishes on V, so by Theorem A2.1, the variety defined by the set of equations (A2.3) is reducible.

The ideal associated with an irreducible variety is a prime ideal [24, p. 23, 24].

Theorem A2.2: Every variety V can be expressed as the sum of a finite number of irreducible varieties (called the components of V).

Proof: This theorem is proved in [24, p. 25].

For example, consider the reducible variety V defined by the following equation:

$$t_1^2 x_1^2 - 1 = 0. \tag{A2.4}$$

Now V is reducible because the polynomial on the left-hand side of (A2.4) is reducible. Consider the two irreducible varieties V_1 and V_2 defined by the equations $t_1 x_1 - 1 = 0$ and $t_1 x_1 + 1 = 0$, respectively. Since $t_1^2 x_1^2 - 1 = (t_1 x_1 - 1)(t_1 x_1 + 1)$, it is clear that $V = V_1 + V_2$; i.e., the set of zeros of $t_1^2 x_1^2 - 1$ is the union of the sets of zeros of $t_1 x_1 - 1$ and $t_1 x_1 + 1$. On the other hand, the variety defined by $t_1^2 x_1^2 + 1 = 0$ is irreducible over R, though over a base field of complex numbers it is of course reducible. The base field is therefore important in questions of irreducibility.

C. Function Fields and the Dimension of Irreducible Varieties

If a variety, in n-space, is irreducible with associated prime ideal I_A, then the field of fractions of the residue class ring $R[x_1, \cdots, x_n]/I_A$, see [24, p. 16], is called the "function field" of V [24, p. 24], [25, p. 10]. Function fields are only defined for irreducible varieties. Without this restriction one would merely obtain rings with zero divisors [34, p. 28]. The function field of an irreducible variety is made up of rational functions F/G for which the denominator polynomials G are not members of the associated prime ideal, and for which one may consider that $F_1/G_1 = F_2/G_2$ if $F_1 G_2 - F_2 G_1 \in I_A$ [24, p. 24].

The maximum number of elements of a field ϕ, an extension field of a base field R, which are algebraically independent over the base field R is termed the degree of transcendence of ϕ over R. The function field of an irreducible variety, denoted $K(x_1, \cdots, x_n)/I_A$, is a finitely generated field extension of R [25, p. 10]. Consequently the number of elements of $K(x_1, \cdots, x_n)/I_A$ which are algebraically independent over R is finite. Thus one may define the dimension, dim V, of an irreducible variety V defined over a base field R as the degree of transcendence over R of the function field of V. The function field $R(x_1, \cdots, x_n)/I_A$ may be represented as $(\xi_1, \cdots, \xi_n)$, where the ξ_i are equivalence classes $[x_i]$ defined as $[x_i] = \{f: f = x_i + g(x_1, \cdots, x_n/g \in I_A\}$. The number of ξ_i which are algebraically independent is the degree of transcendence of $R(x_1, \cdots, x_n)/I_A$ over R and is thus the dimension of the variety from which $R(x_1, \cdots, x_n)/I_A$ was generated. The notion of dimension agrees with intuition in that a variety which is a curve has dimension 1, a linear subspace of dimension d *qua* linear subspace has dimension d *qua* variety, and so on.

Consider, for example, the irreducible variety consisting of points in (x_1, x_2)-space which are solutions of $x_2^2 x_1 - 1 = 0$. The function field is $R(\xi_1, \xi_2 = (1/\sqrt{\xi_1}))$ since x and t are related by $x_2^2 x_1 - 1 = 0$. The number of independent ξ_i is one so the dimension of the variety is one, which intuitively ties in with the fact that $x_2^2 x_1 - 1 = 0$ *is a hypersurface in 2-space.*

The following theorem is very important in the analysis of Section III.

Theorem A2.3: An irreducible variety V of dimension zero *consists of a finite number of points.*

Proof: See [24, p. 54]. Let V be an irreducible variety in n-space. Let the function field of V be $R(\xi_1, \cdots, \xi_n)$. Since dim $V = 0$, the ξ_i are algebraic over R; i.e., there exists n polynomials f_i such that $f_i(\xi_i) = 0$, $i = 1, 2, \cdots, n$. Now $f(\xi_i) = 0$ if and only if $f(x_i) \in I_A$, the ideal associated with V [33, p. 29]. Equivalently, $f(x_i) = 0$ for all points on V and hence x_i assume only a finite number of values on V. ∇∇∇

The material in this appendix is used in Section III to demonstrate that, in general, the output-feedback problem formulation of [15], reviewed in Section II, has only a finite number of solutions.

References

[1] E. J. Davison, "On pole assignment in linear systems with incomplete state feedback," *IEEE Trans. Automat. Control*, vol. AC-15, pp. 348-351, June 1970.

[2] A. Jameson, "Design of single-input systems for specified roots using output feedback," *IEEE Trans. Automat. Contr.*, vol. AC-15, pp. 345-348, June 1970.

[3] F. Fallside and H. Seraji, "Direct design procedure for multivariable feedback systems," *Proc. Inst. Elec. Eng.*, vol. 118, no. 6, pp. 797-801, June 1971.

[4] —, "Pole shifting procedure for multivariable systems using

output feedback," *Proc. Inst. Elec. Eng.*, vol. 118, no. 11, pp. 1648-1654, Nov. 1971.

[5] R. Patel, "Pole assignment by means of unrestricted rank output feedback," *Proc. Inst. Elec. Eng.*, vol. 121, no. 8, pp. 874-878, Aug. 1974.

[6] M. Li, "On output feedback stabilizability of linear systems," *IEEE Trans. Automat. Contr.*, vol. AC-17, pp. 408-410, June 1972.

[7] M. Denham, "Stabilization of linear multivariable systems by output feedback," *IEEE Trans. Automat. Contr.*, vol. AC-18, pp. 62-63, Feb. 1973.

[8] H. Seraji, "Stabilisation by means of output feedback," *Proc. Inst. Elec. Eng.*, vol. 120, no. 11, pp. 1428-1432, Nov. 1973.

[9] N. Munro, "Further results on pole-shifting using output feedback," *Int. J. Control*, vol. 20, no. 5, pp. 775-786, Nov. 1974.

[10] K. Ichikawa, "Output feedback stabilisation," *Int. J. Control*, vol. 16, no. 3, pp. 513-522, Sept. 1972.

[11] W. Koenigsberg and D. Frederick, "Output feedback control with application to unstable linear systems," in *Proc. Joint Automat. Control Conf.*, pp. 674-682, 1970.

[12] D. McBrinn and R. Roy, "Stabilization of linear multivariable systems, by output feedback," *IEEE Trans. Automat. Contr.*, vol. AC-17, pp. 243-245, Apr. 1972.

[13] T. Fortmann, "Stabilisation of multivariable systems with constant gain feedback," in *Proc. Joint Automat. Control Conf.*, pp. 294-301, 1973.

[14] C. Johnson, "Stabilisation of linear dynamical systems with output feedback," in *Proc. 5th IFAC Congr. (Paris)*, paper 29.3 (4a), 1972.

[15] B. Anderson, N. Bose, and E. Jury, "Output feedback stabilization and related problems—Solution via decision methods," *IEEE Trans. Automat. Contr.*, vol. AC-20, pp. 53-66, Feb. 1975.

[16] A. Seidenberg, "A new decision method for elementary algebra," *Ann. Math*, vol. 60, pp. 365-374, 1954.

[17] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*. Berkeley, CA: Univ. California Press, 1951.

[18] N. Jacobson, *Lectures in Abstract Algebra*, Vol. III. Princeton, NJ: Von Nostrand, 1964.

[19] F. Gantmacher, *The Theory of Matrices*, Vol. II. New York: Chelsea, 1959.

[20] S. Barnett, *Matrices in Control Theory*. London, England: Von Nostrand Reinhold, 1971.

[21] R. Courant, *Differential and Integral Calculus*, Vol. II. London, England: Blackie, 1936.

[22] W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, Vol. I. Cambridge, England: Cambridge Univ. Press, 1968.

[23] B. L. Van Der Waerden, *Algebra*. New York: Ungar, 1970.

[24] I. R. Shafarevich, *Basic Algebraic Geometry*. Berlin, Germany: Springer-Verlag, 1974.

[25] J. Humphries, *Linear Algebraic Groups*. Berlin, Germany: Springer-Verlag, 1975.

[26] E. H. Bareiss, "Resultant procedure and the mechanization of the Graeff process," *J. ACM*, vol. 7, pp. 346-386, 1960.

[27] G. E. Collins, "Subresultants and reduced polynomial remainder sequences," *J. ACM*, vol. 14, no. 1, pp. 128-142, Jan. 1967.

[28] S. Ku and R. Adler, "Computing polynomial resultants: Bezout's determinants vs Collin's reduced P.R.S. algorithm," *Comm. ACM*, vol. 12, no. 1, pp. 23-30, Jan. 1969.

[29] G. E. Collins, "The calculation of multivariate polynomial resultants," *J. ACM*, vol. 18, no. 4, pp. 515-532, Oct. 1971.

[30] ——, "Computer algebra of polynomials and rational functions," *Amer. Math. Monthly*, vol. 80, pp. 725-755, Sept. 1973.

[31] ——, "Comment on a paper by Ku and Adler," *Comm. ACM*, vol. 12, no. 6, pp. 302, June 1969.

[32] E. I. Jury, "The theory and applications of inners," *Proc. IEEE*, vol. 63, pp. 1044-1068, July 1975.

[33] S. Lefschetz, *Algebraic Geometry*. London, England: Oxford Univ. Press, 1953.