

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:

Nešić, D; Mareels, I M Y; Glad, T; Jirstrand, M

Title:

The Gröbner basis method in control design: An overview

Date:

2002-01-01

Citation:

Nešić, D., Mareels, I. M. Y., Glad, T. & Jirstrand, M. (2002). The Gröbner basis method in control design: An overview. IFAC Proceedings Volumes IFAC Papersonline, 35, (1), pp.13-18. Elsevier BV. <https://doi.org/10.3182/20020721-6-es-1901.00908>.

Persistent Link:

<https://hdl.handle.net/11343/299626>

THE GRÖBNER BASIS METHOD IN CONTROL THEORY: AN OVERVIEW

D.Nešić^{*,1} I.M.Y.Mareels^{*} T. Glad^{**} M. Jirstrand^{***}

^{*} *Department of Electrical and Electronic Engineering, The
University of Melbourne, Parkville, 3010, Victoria, Australia.*

^{**} *Division of Automatic Control, Linköping University, S-581 83
Linköping, Sweden.*

^{***} *MathCore AB, Wallenbergs gata 4, S-583 35 Linköping,
Sweden.*

Abstract: We present an overview of control problems where the Gröbner basis method and differential algebraic methods (in particular the Ritt's algorithm) can be used.

1. INTRODUCTION

The computer revolution has radically changed every area of engineering and control/systems engineering is not an exception. Indeed, computers have become essential tools in modeling, analysis, design and implementation of control systems. In particular, they enable the design engineer to tackle problems of ever increasing complexity (L. Blum and Shub, 1998).

The topic of this article is to highlight the effectiveness of some symbolic computation software, or the so called computer algebra, in the analysis and design of control systems. In particular two important methods are discussed: *Gröbner bases* and *Differential algebra* (in particular, Ritt's algorithm). In essence, these methods deal with *polynomials*. Computation of Gröbner bases is implemented in most commercial symbolic software packages such as Maple and Mathematica. On the other hand, Ritt's algorithm is not as yet commercially available but software implementations may be obtained from the specialists working in the field.

We consider analysis and design questions for *polynomial control system*. Polynomial systems are a natural generalization of linear systems, they possess a nice algebraic structure and their

analysis is amenable to computer algebra. Moreover, as polynomials are universal approximators, polynomial control models can be used as valid models for almost any physical system. Furthermore, the restriction to polynomial systems is not severe since any nonlinear function which satisfies a polynomial differential or algebraic equation, such as trigonometric functions, can be handled by introducing artificial states, see (Rubel and Singer, 1985) and (Lindskog, 1996) for more details.

The state space model of a polynomial control system is given by:

$$\begin{aligned}\sigma x(t) &= f(x(t), u(t)) \\ y(t) &= h(x(t), u(t)).\end{aligned}\tag{1}$$

Here $x \in \mathbb{R}^n, y \in \mathbb{R}^p, u \in \mathbb{R}^m$ represent respectively the state, the observed output and the manipulated control input of the system. The operator σ is either the derivative $\sigma x(t) = \frac{dx(t)}{dt}$ for continuous time systems (when $t \in \mathbb{R}$) or the forward difference $\sigma x(t) = x(t+1)$ for discrete-time systems (when $t \in \mathbb{N}$). $\mathbb{R}, \mathbb{Q}, \mathbb{N}$ and $\mathbb{C}$ denote respectively the sets of real, rational, natural and complex numbers. The vector functions f and h are assumed to have entries that are polynomial functions in all their variables. Moreover, for computational reasons the polynomials are assumed to have rational coefficients. Continuous-time (or discrete-time) linear systems:

¹ This work is supported by the Australian Research Council under the Large Grants Scheme.

$$\begin{aligned}\sigma x(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t),\end{aligned}\quad (2)$$

form a special subclass of polynomial control systems (1). A wide range of systems can be adequately modeled using (1). Indeed, systems as diverse as biochemical reactors, grain dryers, satellites, robots and airplanes have been successfully modeled using polynomial systems (1) (see, for instance (Nešić, 1996)).

In the context of polynomial control systems, problems like determining equilibria, estimating a domain of attraction of a stable equilibrium, locating approximately periodic solutions, as well as testing controllability and observability properties reduce naturally to the analysis of sets of algebraic polynomial equations. Such problems can be addressed using the Gröbner basis method. In any modeling exercise, the elimination of variables from sets of differential and algebraic equations plays a crucial role. This problem also arises naturally in the context of determining if two state representations are equivalent. Differential algebra and Ritt's algorithm are very useful in this context.

2. THE GRÖBNER BASIS METHOD

Central objects in the Gröbner basis theory are polynomial ideals and affine varieties (D. Cox and O'Shea, 1992). Let $p_1, \dots, p_s$ be multivariate polynomials in the variables $x_1, \dots, x_n$ whose coefficients are in the field k . The variables $x_1, \dots, x_n$ are considered as "place markers" in the polynomial. The notation $p_1, \dots, p_s \in k[x_1, \dots, x_n]$ is adopted. The affine variety (or variety) defined by the s polynomials $p_1, \dots, p_s$ is the collection of all solutions in k^n of the system of equations:

$$p_1(x_1, \dots, x_n) = 0; \dots; p_s(x_1, \dots, x_n) = 0. \quad (3)$$

Formally, the variety $\mathbf{V}(p_1, \dots, p_s)$ generated by polynomials p_i is defined as:

$$\{(a_1, \dots, a_n) \in k^n : p_i(a_1, \dots, a_n) = 0, i = 1, \dots, s\}.$$

For instance, a straight line, a parabola, an ellipse, a hyperbola and a single point are all examples of varieties in $\mathbb{R}^2$. The polynomial ideal I that is generated by $p_1, \dots, p_s$, which is denoted as $I = \langle p_1, \dots, p_s \rangle$, is a set of polynomials obtained by combining these polynomials through multiplication and addition with other polynomials, formally:

$$I := \left\{ f = \sum_{i=1}^s g_i p_i : g_i \in k[x_1, \dots, x_n] \right\}. \quad (4)$$

Polynomials $p_i, i = 1, \dots, s$ form a basis for the ideal I . A very useful interpretation of a polynomial ideal I is in terms of the equations (3).

By multiplying p_i by arbitrary polynomials $g_i \in k[x_1, \dots, x_n]$ and adding them up, the implication of (3) is that $f = g_1 p_1 + \dots + g_s p_s = 0$, and of course $f \in I$. Hence, the ideal $I = \langle p_1, \dots, p_s \rangle$ contains all the "polynomial consequences" of the equations (3).

A notion at the core of the Gröbner basis method is that of *the monomial ordering* (a monomial is a polynomial consisting of a single term) since it introduces an appropriate extension of the notion of the leading term and the leading coefficient familiar from univariate polynomials to multivariate polynomials. One can define many different monomial orderings (e.g. lexicographic, graded lexicographic, graded reverse lexicographic, etc. (D. Cox and O'Shea, 1992)) but to be specific consider the so called lexicographic or lex ordering. Let α, β be two n -tuples of integers ($\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$). The n -tuple α is said to succeed β (in lex ordering), denoted as $\alpha \succ \beta$ if in the vector difference $\alpha - \beta = (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$, the left-most nonzero entry is positive. Obviously, it is possible to define $n!$ different lex orderings for polynomials in n variables. For the polynomial $f = 2x_1^3 x_2 x_3^3 + 4x_1^3 x_3^5$, using the lex ordering $x_1 \succ x_2 \succ x_3$ the monomial $x_1^3 x_2 x_3^3$ succeeds the monomial $x_1^3 x_3^5$ as the multidegrees of the monomials satisfy $(3, 1, 3) \succ (3, 0, 5)$. With this ordering, the leading coefficient and the leading term are respectively $LC(f) = 2$ and $LT(f) = 2x_1^3 x_2 x_3^3$. Using the alternative lex ordering $x_3 \succ x_2 \succ x_1$, the leading term becomes $LT(f) = 4x_1^3 x_3^5$.

In general, an ideal I does not have a unique basis, but given any two different bases $\langle p_1, \dots, p_s \rangle$ and $\langle g_1, \dots, g_m \rangle$ of I , the varieties $\mathbf{V}(p_1, \dots, p_s)$ and $\mathbf{V}(g_1, \dots, g_m)$ are equal. In other words, a variety only depends on the ideal generated by its defining equations. Some bases of an ideal may be simpler than other bases. Intuitively, if all the polynomials in a given basis of an ideal have a degree that is lower than the degree of any other polynomial in the ideal with respect to a particular monomial ordering, then this basis is in some sense the simplest basis. In particular, a Gröbner basis of an ideal (for a given monomial ordering) has such a property and can be thought of as the simplest or canonical basis. Given an ideal I and a monomial ordering, denote the set of leading terms of elements of I as $LT(I)$. The ideal generated by elements of $LT(I)$ is denoted $\langle LT(I) \rangle$. In general, the ideal generated by the leading terms of a particular ideal I is not the same as the ideal generated by the leading terms of the polynomials in a basis for that particular ideal I . A Gröbner basis is a special basis for which this property holds and it is formally defined as the set of polynomials $g_1, \dots, g_m$ for which $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_m) \rangle$. When computing Gröbner bases, the user specifies a

monomial ordering; different monomial orderings produce different Gröbner bases. Given a monomial ordering, the two most important properties of Gröbner bases are:

- (1) Every ideal $I \subset k[x_1, \dots, x_n]$, other than the trivial ideal $\langle 0 \rangle$, has a Gröbner basis. Furthermore, any Gröbner basis of an ideal I is a basis for I .
- (2) Given an ideal $I \subset k[x_1, \dots, x_n]$, other than the trivial ideal $\langle 0 \rangle$, a Gröbner basis of I can be computed in a finite number of algebraic operations.

The first algorithm for computation of Gröbner bases, published in the 1960's, is attributed to B. Buchberger (D. Cox and O'Shea, 1992). Since then a number of improvements have been reported and the algorithm has been implemented in most commercial symbolic software packages. The Buchberger's algorithm generalizes two well known algorithms: Gauss elimination for sets of multivariate linear algebraic equations and Euclid's algorithm for computing the greatest common divisor of a set of univariate polynomials.

2.1 Solving sets of multivariate polynomial equations

Gröbner bases facilitate solving a set of multivariate polynomial equations (3) in the same way as the Gauss elimination algorithm facilitates solving a set of linear algebraic equations. Indeed, in a given lex ordering the Gröbner basis has a triangular structure reminiscent of the triangular structure in Gauss elimination. If the Gröbner basis is given by $\{1\}$, then the system of polynomial equations has no solution.

2.1.1. Equilibria for polynomial systems Consider a polynomial system without inputs $\sigma x(t) = f(x(t))$. A state $x^* \in \mathbb{R}^n$ is called an equilibrium of this system if $x(0) = x^*$ implies that $x(t) \equiv x^*, \forall t$. Equilibria for polynomial systems are therefore obtained as solutions of a set of polynomial equations of the form $f(x) = 0$ or $f(x) = x$ for continuous-time or discrete-time systems respectively. Gröbner bases facilitate finding all equilibria.

Example 1. The equilibria of the system:

$$\begin{aligned}\dot{x}_1 &= x_1 + x_2 - x_3^3, \\ \dot{x}_2 &= x_1^2 + x_2 - x_3, \\ \dot{x}_3 &= -x_1 + x_2^2 + x_3,\end{aligned}$$

are obtained as solutions of the set of polynomial equations:

$$\begin{aligned}p_1 &:= x_1 + x_2 - x_3^3 = 0; \quad p_2 := x_1^2 + x_2 - x_3 = 0; \\ p_3 &:= -x_1 + x_2^2 + x_3 = 0,\end{aligned}\tag{5}$$

which is relatively hard to solve. The Gröbner basis for the ideal $\langle p_1, p_2, p_3 \rangle$ using the lexicographic ordering $x_1 \succ x_2 \succ x_3$ is computed using Maple:

$$\begin{aligned}g_1 &= x_1 + x_2 - x_3^3, \\ g_2 &= x_2 - x_3^3 + x_2^2 + x_3, \\ g_3 &= 6x_3 - 3x_3^3 - 2x_3^4 - x_3^9 + 4x_3x_2, \\ g_4 &= 4x_3 - 8x_3^3 + 3x_3^5 + x_3^{11}.\end{aligned}\tag{6}$$

By construction the equations $g_i = 0, i = 1, 2, 3, 4$ have the same solutions as (5). But obviously the polynomials g_i have a much simpler structure than the polynomials p_i . Indeed, polynomial g_4 depends only on x_3 , this allows $g_4 = 0$ to be solved numerically for x_3 . The solutions can be substituted into $g_2 = 0$ and $g_3 = 0$ to obtain polynomials in x_2 only that can then be solved numerically. This process of back-substitution can be continued until all solutions are found.

Observe that a basis for an ideal does not have a fixed number of basis polynomials, and indeed the "simpler" Gröbner basis contains more polynomials than the original basis. As may be observed it even contains more polynomials than there are variables.

2.1.2. Periodic solutions for polynomial systems

Consider the system $f\left(\frac{d^n y}{dt^n}, \dots, \frac{dy}{dt}, y, t\right) = 0$, where y can be thought of as the output of a closed-loop control system. Let f be a polynomial in all its variables. To approximately compute a periodic solution $y(t)$ of this system, the method of harmonic balancing can be used. It can be shown that under mild conditions an approximate periodic solution implies the existence of an exact periodic solution "close" to the approximate one (Mees, 1981). A truncated Fourier series can be considered as a candidate approximate periodic solution $y(t) = \sum_{k=-N}^{+N} c_k e^{-jk\omega t}$, $c_k \in \mathbb{C}$, where c_k and c_{-k} are complex conjugates. Postulating that $y(t)$ is a solution, leads to a set of polynomial equations because f is polynomial. Using the Gröbner basis method with lex ordering, this set of equations can be solved for the unknowns $c_0, c_1, \dots, c_N$ and ω to obtain $y(t)$. In practice the actual solution may not be so important and it often suffices to know that a periodic solution exists and to know its oscillation frequency ω . This can be obtained by finding the Gröbner basis of the polynomial equations with any lex ordering where ω is the lowest ranking variable.

Example 2. Consider the van der Pol equation (Forsman, 1997) $\ddot{y} - a(1 - by^2)\dot{y} + y = 0$, and postulate a periodic solution $y(t) = \sum_{k=-3}^{+3} c_k e^{-jk\omega t}$,

where $c_k = c_{kr} + c_{ki}j$, $k = 0, 1, 2, 3$ and $j = \sqrt{-1}$. Substituting $y(t)$ into the van der Pol differential equation and equating the coefficients on the left hand and right hand sides of the equation leads to:

$$\begin{aligned} p_1 &:= -c_{1r}\omega^2 - abc_{1r}^2c_{3i}\omega + c_{1r} = 0, \\ p_2 &:= 2abc_{1r}c_{3r}^2\omega + abc_{1r}^2c_{3r}\omega + 2abc_{1r}c_{3i}^2\omega \\ &\quad + abc_{1r}^3\omega - ac_{1r}\omega = 0, \\ p_3 &:= -9c_{3r}\omega^2 - 3abc_{3i}c_{3r}^2\omega - 3abc_{3i}^3\omega \\ &\quad - 6abc_{1r}^2c_{3i}\omega + 3ac_{3i}\omega + c_{3r} = 0, \\ p_4 &:= 3abc_{3r}^3\omega - 9c_{3i}\omega^2 + 3abc_{3i}^2c_{3r}\omega + 6abc_{1r}^2c_{3r}\omega \\ &\quad - 3ac_{3r}\omega + abc_{1r}^3\omega + c_{3i} = 0, \end{aligned}$$

and $c_0 = 0$, $c_2 = 0$ and $c_{1i} = 0$. The coefficients a and b are regarded as variables. To simplify the computations p_1 is divided by c_{1r} and p_2 by $ac_{1r}\omega$. A Gröbner basis of the ideal $\langle p_1, p_2, p_3, p_4 \rangle$ with the lex ordering $c_{3r} \succ c_{3i} \succ c_{1r} \succ b \succ a \succ \omega$ contains 7 polynomials of non trivial complexity (42 pages of Maple output). It contains one polynomial in ω and a only:

$$g_7 := 3249\omega^{10} + (549a^2 - 6213)\omega^8 + (3745 - 567a^2)\omega^6 \\ + (159a^2 - 842)\omega^4 + (53 - 13a^2)\omega^2 - 1.$$

Obviously for $a = 0$, the van der Pol oscillator is a simple harmonic oscillator with frequency $\omega = 1$. In the presence of nonlinear damping $a \neq 0$, the solution of $g_7 = 0$, which continues $\omega = 1$, can be expanded as:

$$\omega^2 = 1 + \alpha_1 a^2 + \alpha_2 a^4 + \alpha_3 a^6 + \dots,$$

and using Maple, the coefficients α_i are obtained $\alpha_1 = -\frac{1}{8}$, $\alpha_2 = \frac{25}{256}$, $\alpha_3 = -\frac{625}{4096}$, etc.

2.2 Gröbner bases and elimination

Gröbner bases can be used to eliminate some variables of interest from a set of polynomial equations, as illustrated by Example 1, where x_1 and x_2 are eliminated from g_4 in (6). The variables that are ranked higher in the lex ordering are eliminated first. This feature of Gröbner bases can be used to obtain an estimate of the domain of attraction of equilibria for polynomial systems.

2.2.1. Estimation of the domain of attraction If the closed-loop control system is stable, it is of interest to determine those initial conditions from which the solutions converge to a specified equilibrium. The collection of all the initial conditions that converge to the same equilibrium is called the domain of attraction of that particular equilibrium. Estimating domains of attractions is a hard problem and one way of obtaining a (conservative)

estimate for the domain of attraction is to use Lyapunov functions. It is a standard result in Lyapunov theory that if $x = 0$ is an equilibrium point for the continuous-time system $\dot{x} = f(x)$, $D \subset \mathbb{R}^n$ is a domain containing $x = 0$ and $W : D \rightarrow \mathbb{R}$ is a continuously differentiable function, such that $W(0) = 0$, and for all $x \in D - \{0\}$ there holds $W(x) > 0$ and $\frac{\partial W}{\partial x} f(x) < 0$ then $x = 0$ is asymptotically stable. Given such a Lyapunov function, consider the sets $\Omega = \{x \in \mathbb{R}^n : \frac{\partial W}{\partial x} f(x) < 0\}$ and $B_d = \{x \in \mathbb{R}^n : W(x) \leq d\}$. If $B_d \subset \Omega$ for some $d > 0$, then the set B_d is an estimate for the domain of attraction. For polynomial systems with a polynomial Lyapunov function W , Gröbner bases can be used to systematically compute B_d . Indeed, it is feasible to construct the largest such set by finding d such that B_d is as large as possible and still inside Ω . For polynomial systems with polynomial Lyapunov functions, $W(x) - d$ and $\frac{\partial W}{\partial x} f(x)$ are polynomials, and hence the boundaries of the sets B_d and Ω are varieties. At the points where the varieties $\mathbf{V}(W - d)$ and $\mathbf{V}(\frac{\partial W}{\partial x} f(x))$ touch each other, the gradients of W and W are parallel. Using this information, a system of $n + 2$ polynomial equations in $n + 2$ variables is obtained:

$$\begin{aligned} W - d &= 0; \quad \frac{\partial W}{\partial x} f(x) = 0; \\ \frac{\partial}{\partial x} \left(\frac{\partial W}{\partial x} f(x) \right) - \lambda \frac{\partial W}{\partial x} &= 0. \end{aligned} \quad (7)$$

Computing a Gröbner basis for the above system of equations, where the variable d has the least rank in the lex ordering, a polynomial equation in d only is obtained. The least positive solution to this equation is the “best” value of d for which $B_d \subset \Omega$ and this yields in turn the best estimate for the domain of attraction that could be obtained with the particular Lyapunov function W .

Example 3. Consider the system (Forsman, 1997):

$$\begin{aligned} \dot{x}_1 &= -x_1 + 2x_1^2x_2, \\ \dot{x}_2 &= -x_2, \end{aligned} \quad (8)$$

with the Lyapunov function $W(x) = 3x_1^2 + 4x_1x_2 + 4x_2^2$. The polynomials (7) are in this case:

$$\begin{aligned} p_1 &:= 3x_1^2 + 4x_1x_2 + 4x_2^2 - d, \\ p_2 &:= -6x_1^2 + 12x_1^3x_2 - 8x_1x_2 + 8x_1^2x_2^2 - 8x_2^2, \\ p_3 &:= 6x_1 + 4x_2 - \lambda(36x_2x_1^2 - 12x_1 - 8x_2 \\ &\quad + 16x_2^2x_1), \\ p_4 &:= 4x_1 + 8x_2 - \lambda(12x_1^3 - 8x_1 + 16x_2x_1^2 \\ &\quad - 16x_2), \end{aligned} \quad (9)$$

and using the lexicographic ordering $x_2 \succ \lambda \succ x_1 \succ d$, the Gröbner basis of the ideal $\langle p_1, p_2, p_3, p_4 \rangle$ is computed. It contains the polynomial $g(d) =$

$4d^4 - 147d^3 + 786d^2 + 2048d$. The approximate solutions of $g(d) = 0$ are $-1.9223, 0, 8.9657, 29.707$. The smallest positive value of d for which there is a solution to the system of equations $p_i = 0$ is 8.9657 . The corresponding estimate for the domain of attraction is therefore $\{x \in \mathbb{R}^2 : W(x) \leq 8.9657\}$.

2.3 Equality of ideals

A special type of a Gröbner basis can be used to decide if two ideals are the same or not. This is the so called *reduced* Gröbner basis. A reduced Gröbner basis for an ideal I is a Gröbner basis G for I such that: $LC(p) = 1$ for all $p \in G$; and for all $p \in G$, no monomial of p lies in $\langle LT(G - \{p\}) \rangle$. The main property of reduced Gröbner bases is that given an arbitrary ideal $I \neq \langle 0 \rangle$ and a particular monomial ordering, I has a *unique* reduced Gröbner basis. Hence, two ideals J_1 and J_2 are the same if and only if their reduced Gröbner bases G_1 and G_2 are the same (G_1 and G_2 must be computed with the same monomial ordering). Most commercial computer algebra systems, such as Maple and Mathematica, provide finite algorithms for computing reduced Gröbner bases.

2.3.1. Analysis of discrete-time polynomial systems Fundamental control theoretic concepts such as controllability or observability can be reduced to the problem of computing maximal control invariant varieties. This is well known for linear systems (computation of control invariant subspaces), but it holds equally well for discrete-time polynomial systems of the form $x(t+1) = f(x(t), u(t))$. For such systems, a variety V is control invariant if $f(V, u) \subset V$ for all possible control inputs u . The computation of the maximal control invariant subset of a given variety V can be completed in finitely many operations. Consider the defining ideal of the variety V ; say $J_1 = \langle g_{1,1}, \dots, g_{1,m_1} \rangle$, where $g_{j,k} \in \mathbb{Q}[x]$. If the variety corresponding to J_1 were control invariant then $g_{1,k} \circ f(x, u) \equiv 0$ for all u and all $k = 1, \dots, m_1$. The polynomials $g_{1,k} \circ f(x, u)$ can be viewed as polynomials in u with coefficients in $\mathbb{Q}[x]$. Denote the collection of all these coefficients as $g_{2,k}, k = 1, 2, \dots, m_2$ and the corresponding ideal as $J_2 = \langle g_{2,1}, \dots, g_{2,m_2} \rangle$. Invariance would imply that $J_1 = J_2$ and if this is not the case, then obviously $J_1 \subset J_2$ and the corresponding varieties satisfy $V_1 \supset V_2$. This process can be continued to construct an ascending chain of ideals (or descending chain of varieties) $J_1 \subset J_2 \subset J_3 \subset \dots$. This chain must terminate in finitely many steps (D. Cox and O'Shea, 1992). That is, there exists an integer N such that $\dots \subset J_{N-1} \subset J_N =$

$J_{N+1} = \dots$. The variety $V(J_N)$ is the maximal control invariant subset of $V(J_1)$. Checking if $J_k = J_{k+1}$ can be completed via the computation of reduced Gröbner bases for J_k and J_{k+1} .

Observability: The discrete-time polynomial system

$$\begin{aligned} x(t+1) &= f(x(t), u(t)) , \\ y(t) &= h(x(t)) , \end{aligned} \quad (10)$$

is said to be observable if for each pair of initial states $\xi \neq \eta$, there exists an integer N and an input sequence $U_N = \{u(0), \dots, u(N-1)\}$ such that the solutions starting at ξ and η produce different outputs after N steps, that is $h(x(N, \xi, U_N)) \neq h(x(N, \eta, U_N))$. The polynomial $h(x(N, \xi, U_N)) - h(x(N, \eta, U_N))$ can be regarded as a polynomial in elements of U_N with coefficients in $\mathbb{Q}[\xi, \eta]$. A chain of ideals J_k is constructed using these coefficients and at each step the condition $J_k = J_{k+1}$ is tested. It can be shown that if J_N for some N has a reduced Gröbner basis $\{\xi_1 - \eta_1, \dots, \xi_n - \eta_n\}$ then $J_{N+1} = J_N$ and the system is observable. The above discussed algorithm for computing invariant sets streamlines these computations and allows a systematic determination of the integer N . An example of how this algorithm is applied to a class of the so called simple Wiener systems can be found in (Nešić, 1998).

Example 4. Consider the simple Wiener system (Nešić, 1998):

$$\begin{aligned} x_1(k+1) &= x_2(k) , \\ x_2(k+1) &= -x_1(k) - 2x_2(k) + u(k) , \\ y(k) &= x_1^2(k) . \end{aligned} \quad (11)$$

The system consists of a linear dynamical system and a quadratic static output nonlinearity. The ideal $J_1 = \langle \eta_1^2 - \xi_1^2 \rangle$ and the output equation (11) are used to construct the following ideals:

$$\begin{aligned} J_2 &= \langle \eta_1^2 - \xi_1^2, \eta_2^2 - \xi_2^2 \rangle, \\ J_3 &= \langle \eta_1^2 - \xi_1^2, \eta_2^2 - \xi_2^2, (\eta_1 + 2\eta_2)^2 - (\xi_1 + 2\xi_2)^2, \\ &\quad (\eta_1 + 2\eta_2) - (\xi_1 + 2\xi_2) \rangle, \\ J_4 &= \langle \eta_1^2 - \xi_1^2, \eta_2^2 - \xi_2^2, (\eta_1 + 2\eta_2)^2 - (\xi_1 + 2\xi_2)^2, \\ &\quad (\eta_1 + 2\eta_2) - (\xi_1 + 2\xi_2), (2\eta_1 + \eta_2)^2 \\ &\quad 2 - (2\xi_1 + \xi_2)^2, \eta_1 + \eta_2 - 2\xi_1 - \xi_2, -2\eta_1 - 3\eta_2 \\ &\quad + 2\xi_1 + 3\xi_2 \rangle . \end{aligned} \quad (12)$$

Using the lex ordering $\xi_1 \succ \xi_2 \succ \eta_1 \succ \eta_2$, the reduced Gröbner basis for J_4 is $G_4 = \{\eta_1 - \xi_1, \eta_2 - \xi_2\}$ and therefore the system (11) is observable with $N = 4$.

2.3.2. A brief overview of literature and related problems Gröbner bases are useful for a range of

other control problems, such as the inverse kinematic problem and motion planning in robotics (D. Cox and O'Shea, 1992), the computation of the switching surfaces in the solution of time optimal control problems (Glad, 1995; U. Walther and Tannenbaum, 1999), identifiability, input-output equivalence of different state space realizations, normal forms and zero dynamics (Fortell, 1995), analysis of hybrid control systems, computation of limit cycles for discrete-time polynomial systems, observability of continuous-time polynomial systems, forward accessibility of discrete-time polynomial systems, etc.

In control design for linear systems, the linear functional observer problem, the model matching problem, the deterministic identification problem and the disturbance decoupling problem play a central role. All these problems can be seen as the characterization of a maximally control invariant subspace of a given subspace of the state space ((Ed.), 1999). In control theory this problem is known as the cover problem. The cover problem can be solved via a computation of elementary divisors of matrix pencils, which in turn leads to multi-linear equations where the unknowns are the basis vectors of the invariant subspace. The Gröbner basis method facilitates the analytic solution to this problem. The elegance of this approach stems from the fact that in one single algorithm all possible (typically infinitely many) control invariant subspaces can be explicitly characterized. The degrees of freedom established in this process can then be further exploited to optimize other desirable system properties, such as sensitivity.

We have focused on the use of Gröbner bases for commutative rings over infinite fields; i.e. finding Gröbner bases in the context of polynomials with rational coefficients. Two important related areas are Gröbner bases for commutative rings over finite fields and Gröbner bases in the context of non-commutative rings. The former is of interest in the context of discrete event dynamic systems (Germundsson, 1995; Gunnarsson, 1997) and coding theory in communications. The latter is useful for control theoretic problems involving polynomial matrices in (KronewitterIII, 2000). In particular, in (KronewitterIII, 2000) a new extra term in the expansion of the classical state feedback optimal control problem in the singular perturbation form was obtained using non-commutative Gröbner bases.

An important drawback of Buchberger's algorithm is that even with the best known versions of the algorithm, it is easy to generate examples for which the computation of a Gröbner basis requires inordinate amounts of computer resources, time and/or memory wise. The main bottlenecks are

that the total degrees of the intermediate polynomials that the algorithm generates may be quite large and that the coefficients of the Gröbner basis may be complicated rational numbers. This may be the case even if the original ideal generators are polynomials of small degrees with small integer coefficients. In general, the intermediate polynomials observed in the computation of a Gröbner basis can have total degrees of the order of 2^{2^d} , where d is the total degree of the ideal generators. Although this appears to be a rather negative result, this result typifies the worst case scenario. It appears that the running time and the storage requirements seem to be much more manageable on average. It is important to emphasize that different monomial orderings may produce very different computational times and some experimentation with the ordering may yield significant reductions in computation time.

3. DIFFERENTIAL ALGEBRA IN CONTROL

In the 1980s differential algebra was introduced into control problems, see (Fliess and Glad, 1993). Differential algebra can be used to transform a polynomial system from one representation to another. In general differential algebra plays an important role in realization theory of nonlinear control systems. In the context of control, the problems that lend themselves to differential algebra are varied such as, the determination of observability, identifiability, the calculation of zero dynamics, regulator computations, and tracking control.

3.1 Differential algebraic tools

Differential algebra provides tools for dealing with systems of polynomial differential equations. In this algebra the derivative operation has a center stage. A multivariate polynomial in variables $y_1, \dots, y_N$ and their derivatives is called a *differential polynomial* in $y_1, \dots, y_N$. For instance, $f\left(\frac{d^n y}{dt^n}, \dots, \frac{dy}{dt}, y\right)$ is a differential polynomial in y if f is a polynomial in all its variables.

The concept of *ranking* is introduced for differential polynomials. It is very similar to the concept of monomial ordering for polynomials. Ranking is a total ordering of all variables and their derivatives. Examples involving two variables are

$$u \prec y \prec \dot{u} \prec \dot{y} \prec \ddot{u} \prec \ddot{y} \prec \dots$$

and

$$u \prec \dot{u} \prec \ddot{u} \prec \dots \prec y \prec \dot{y} \prec \ddot{y} \prec \dots$$

where $\prec$ denotes “is ranked lower than”. Any ranking is possible provided it satisfies two conditions:

$$u^{(\mu)} \prec u^{(\mu+\sigma)} \\ u^{(\mu)} \prec y^{(\nu)} \Rightarrow u^{(\mu+\sigma)} \prec y^{(\nu+\sigma)}$$

for all variables u and y , all nonnegative integers μ and ν , and all positive integers σ . The highest ranking variable or derivative of a variable in a differential polynomial is called the *leader*. The ranking of variables gives a ranking of differential polynomials. They are simply ranked as their leaders. If they have the same leader, they are considered as polynomials in their leader and the one of lowest degree is ranked lower.

Let A, B be two differential polynomials and let A have the leader v . Then B is said to be *reduced* with respect to A if there is no derivative of v in B and if B has lower degree than A when both are regarded as polynomials in v . A set

$$A_1, \dots, A_p$$

of differential polynomials is called *auto-reduced* if all the A_i are pairwise reduced with respect to each other. Normally auto-reduced sets are ordered so that $A_1, \dots, A_p$ are in increasing rank. Auto-reduced sets are ranked as follows. Let $\mathbf{A} = A_1, \dots, A_r$ and $\mathbf{B} = B_1, \dots, B_s$ be two ordered auto-reduced sets. $\mathbf{A}$ is ranked lower if either there is an integer k , $0 \leq k \leq \min(s, r)$ such that

$$\text{rank} A_j = \text{rank} B_j, \quad j = 0, \dots, k-1$$

$$\text{rank} A_k \prec \text{rank} B_k$$

or else if $r > s$ and

$$\text{rank} A_j = \text{rank} B_j, \quad j = 0, \dots, s$$

A *characteristic set* for a given set of differential polynomials is an auto-reduced subset such that no other auto-reduced subset is ranked lower.

The *separant* S_A of a differential polynomial A is the partial derivative of A with respect to the leader, while the *initial* I_A is the coefficient of the highest power of the leader in A . If a differential polynomial f is not reduced with respect to another differential polynomial g , then either f contains some derivative of the leader u_g of g or else f contains u_g to a higher power. In the former case one could differentiate g a suitable number (say σ) of times and perform a pseudo-division to remove that derivative, giving a relation

$$S^\nu f = Qg^{(\sigma)} + R \quad (13)$$

where S is the separant of g and R does not contain the highest derivative of u_g which is present in f . If f contains u_g to a higher power a pseudo-division of f by g can be performed to obtain

$$I^\nu f = Qg + R \quad (14)$$

where I is the initial of g and R is reduced with respect to g .

3.1.1. Observability In control theory a system is called observable if it is possible to compute the state from inputs and outputs. Using differential algebra, the observability question can be answered in a constructive manner for continuous-time polynomial systems (1).

Example 5. Consider the system

$$\dot{x}_1 = x_2^2 \quad \dot{x}_2 = u \quad y = x_1$$

which is in state-space form. Suppose an input-output description, i.e. a description directly relating u and y is called for. The original set of equations is equivalent to

$$y - x_1 = 0, \quad \dot{y} - x_2^2 = 0, \quad \dot{x}_2 - u = 0. \quad (15)$$

It is now possible to eliminate the derivative of x_2 by forming

$$p = \frac{d}{dt}(\dot{y} - x_2^2) + 2x_2(\dot{x}_2 - u) = \ddot{y} - 2x_2u. \quad (16)$$

From this construction it follows that $p = 0$ whenever the equations of (15) are satisfied. The last equation of (15) can be replaced by $p = 0$ to get the system description

$$y - x_1 = 0, \quad \dot{y} - x_2^2 = 0, \quad \ddot{y} - 2x_2u = 0. \quad (17)$$

From (16) it follows that every solution of (15) also solves (17). If, moreover, it is known that $x_2 \neq 0$, then the converse is also true and (15) and (17) are equivalent. It is now possible to form

$$x_2(\ddot{y} - 2x_2u) - 2u(\dot{y} - x_2^2) = x_2\ddot{y} - 2u\dot{y}, \quad (18)$$

and it readily follows that

$$y - x_1 = 0, \quad \ddot{y} - 2x_2u = 0, \quad x_2\ddot{y} - 2u\dot{y} = 0,$$

is equivalent to (17) if also $u \neq 0$. Finally form

$$\ddot{y}(\ddot{y} - 2x_2u) + 2u(x_2\ddot{y} - 2u\dot{y}) = \ddot{y}^2 - 4u^2\dot{y},$$

to conclude that, provided $ux_2 \neq 0$, (15) is equivalent to the following system description:

$$\ddot{y}^2 - 4u^2\dot{y} = 0, \quad y - x_1 = 0, \quad \ddot{y} - 2x_2u = 0. \quad (19)$$

The left most equation is an input-output relation, while the middle and right equations show how x_1 and x_2 can be computed from the input and output. This establishes the observability question, and more.

Using the terminology of differential algebra, the state space form is an auto-reduced set under the ranking

$$u \prec x_1 \prec x_2 \prec y \prec \dot{u} \prec \dot{x}_1 \prec \dot{x}_2 \prec \dot{y} \prec \dots,$$

while (19) is an auto-reduced set under the ranking

$$u^{(\cdot)} \prec y^{(\cdot)} \prec x_1^{(\cdot)} \prec x_2^{(\cdot)}.$$

Auto-reduced sets thus give a generalization of several of the standard forms for dynamic systems.

3.1.2. Global identifiability A system that is parameterized with a (constant) parameter θ

$$\dot{x} = f(x, u, \theta); \quad y = h(x, \theta), \quad (20)$$

is said to be globally identifiable if given input and output measurements $u(t)$ and $y(t)$ over an interval $t \in [0, T]$ there is only one constant value of θ that satisfies (20). Global identifiability of polynomial systems (1) can be checked in a constructive manner using the tools from differential algebra. Moreover, conditions on u and y under which the system is not globally identifiable can also be obtained, as is illustrated below.

Example 6. Consider the system $\ddot{y} + 2\theta\dot{y} + \theta^2 y = 0$, where θ is a constant parameter. Can θ be identified by observing the output y ? Using the notation $p = \ddot{y} + 2\theta\dot{y} + \theta^2 y$, compute the expression

$$\dot{y}p - y\dot{p} = \dot{y}\ddot{y} - y\dot{y}^{(3)} + 2\theta(\dot{y}^2 - y\dot{y}).$$

It follows readily that θ is uniquely determined by y (and its derivatives), provided that along the output trajectory $(\dot{y}^2 - y\dot{y}) \neq 0$. This is thus an excitation condition which guarantees global identifiability.

3.1.3. The algorithms of Ritt and Seidenberg

The concepts of the previous section were introduced in the 1930s by the American mathematician Ritt, (Ritt, 1950). He devised an algorithm by which it is possible to start with an arbitrary number of differential polynomials, introducing a suitable ranking of the variables and performing successive operations of the type described by (13), (14) to arrive at an equivalent representation in the form of an auto-reduced set of equations. This auto-reduced set has the property that an f belonging to the original differential polynomials can be reduced to zero, using (13) and (14) for different g 's belonging to the auto-reduced set. If certain factorization conditions are met then Ritt showed that the generated auto-reduced set is a characteristic set, not only for the explicitly generated polynomials, but also for an infinite set of polynomials constituting the so called differential ideal. Ritt used his algorithmic procedure to produce an extensive theory for polynomial systems of differential equations. Later a more systematic algebraic treatment was given by Kolchin, (Kolchin, 1973). The theory was also extended to partial differential equations (Kolchin, 1973) and difference equations (Cohn, 1979).

From the viewpoint of practical calculations, a major drawback of Ritt's algorithm is the factorization which it requires, since this is a task of high computational complexity. Seidenberg, (Seidenberg, 1956), has proposed an algorithm for deciding solvability of systems of equations

and inequations. The algorithm uses (13), (14) repeatedly to eliminate variables and reduce the problem to the single variable case. As in the simple example above, equivalence of the original and final sets of equations require the separant S and initial I of (13), (14) to be nonzero. To handle this, Seidenberg's algorithm splits the problem into different subproblems, considering the cases $S = 0$, $S \neq 0$ (or $I = 0$, $I \neq 0$) together with the original equations and inequations. By repeated splitting a tree of subproblems is generated. Each subproblem is finally reduced to a single variable problem for which solvability can be decided. In recent years several variations of Ritt's and Seidenberg's algorithms have been implemented in symbolic manipulation languages like Maple or Mathematica.

3.2 Other control problems

Differential algebra calculations can be used to compute the zero dynamics of a system. This dynamics is obtained by restricting the output to be zero. By adding the equation $y = 0$ and using Ritt's algorithm with a suitable ranking, it is possible to obtain a description of the resulting dynamics. In a similar manner a regulator description can be obtained. Suppose a differential equation describing the desired response from reference signal to output is given. Using this equation together with the system dynamics as the input to Ritt's algorithm, it is possible to arrive at an equation containing the control signal together with the reference and output signals. This equation can be interpreted as a description of the regulator, although it can be difficult to implement due to its implicit nature in the general case.

4. CONCLUSION

The possibilities offered through symbolic (and numeric) software in order to address control problems are as varied and exciting as the control problems themselves. This article just presented the tip of an iceberg. Dealing with complexity in control design is the main issue. For control algorithm developers there is now more than ever a compelling need to focus on reliable software algorithms that allow non specialists to approach with confidence a control problem. Software tools that provide information to the user about the likelihood of success and the difficulties in a particular solution are called for to make this a reality.

5. REFERENCES

- Cohn, R. M. (1979). *Difference algebra*. R.E. Krieger Pub. Co.
- D. Cox, J. Little and D. O'Shea (1992). *Ideals, varieties and algorithms*. Springer-Verlag.
- (Ed.), N. Munro (1999). *Symbolic methods in control system analysis and design*. The Institution of Electrical Engineers.
- Fliess, M. and S. T. Glad (1993). An algebraic approach to linear and nonlinear control. In: *Essays on control: Perspectives in the theory and its applications* (H. L. Trentelman and J. C. Willems, Eds.). Birkhäuser.
- Forsman, K. (1997). Constructive commutative algebra in nonlinear control. PhD thesis. Department of Electrical Engineering, Linköping University. Linköping, Sweden.
- Fortell, H. (1995). Algebraic approaches to normal forms and zero dynamics. PhD thesis. Department of Electrical Engineering, Linköping University. Linköping, Sweden.
- Germundsson, R. (1995). Symbolic systems. PhD thesis. Department of Electrical Engineering, Linköping University. Linköping, Sweden.
- Glad, S. T. (1995). An algebraic approach to bang-bang control. In: *European Control Conference, ECC 95*. Vol. 4. Rome, Italy. pp. 2892–2895.
- Gunnarsson, J. (1997). Symbolic methods and tools for discrete event dynamic systems. PhD thesis. Department of Electrical Engineering, Linköping University. Linköping, Sweden.
- Kolchin, E. R. (1973). *Differential Algebra and Algebraic Groups*. Academic Press.
- KronewitterIII, F. D. (2000). Non-commutative computer algebra. PhD thesis. The University of California, San Diego.
- L. Blum, S. Smale, F. Cucker and M. Shub (1998). *Complexity and real computation*. Springer-Verlag.
- Lindskog, P. (1996). Methods, Algorithms and Tools for System Identification Based on Prior Knowledge. PhD thesis 436. Department of Electrical Engineering, Linköping University. Sweden.
- Mees, A. (1981). *Dynamics of feedback systems*. Wiley.
- Nešić, D. (1996). Dead-beat control for polynomial systems. PhD thesis. RSISE, Australian National University. Canberra, Australia.
- Nešić, D. (1998). A note on observability tests for general polynomial and simple wiener-hammerstein systems. *Syst. Contr. Lett.* **35**, 219–227.
- Ritt, J. F. (1950). *Differential Algebra*. American Mathematical Society.
- Rubel, L. A. and M. F. Singer (1985). A differentially algebraic elimination theorem with applications to analog computability in the calculus of variations. In: *Proc. of American Math. Soc.*. Vol. 94. Springer - Verlag. pp. 653–658.
- Seidenberg, A. (1956). An elimination theory for differential algebra. pp. 31–66. University of California Publications in Mathematics: New Series. Berkeley and Los Angeles, California.
- U. Walther, T. Georgiou and A. Tannenbaum (1999). Computational algebraic geometry and switching surfaces in optimal control. In: *Proc. Conf. Decis. Contr.*. Phoenix, Arizona. pp. 4724–4729.