REDUCING MULTIVARIATE POLYNOMIAL EQUATIONS

Sándor SZABÓ

Department of Mathematics,
Faculty of Civil Engineering
Technical University of Budapest
H–1521 Budapest, Hungary

Received: December 1, 1992.

Abstract

A typical applied mathematical computation is a blend of symbolic and numerical manipulations. With the advent of computers the range of the numerical methodts is dramaticaly broadened. The purpose of this paper is not to communicate new mathematical results. It is rather to draw some attention to the symbolic computations by describing an elemntary reduction procedure for systems of multivariate polynomial equations.

Keywords: Gröbner bases, polynomial equations, ideal theory.

Introduction

After formulating various problems in mathematical terms we often face a system of multivariate polynomial equations. It is not a routine computation to solve such a system of multivariate polynomial equations. So translating a problem into this form does not seem to be a real progress in solving the original problem. As a consequence, there are no instructive examples how this setting of engineering problems provides insight into the nature of the original problem.

The recent advances in computer algebra show some promising signs that systems of multivariate polynomial might be handled more successfully and this approach might be useful in connection with problems of size that are interesting from the point of view of real life applications. One purpose of this paper is to encourage engineers not to abandon a problem at once just because it involves polynomials of several variables some of which, are suppose, on fourth power. Of course no one is going to use a technique that is absolutely unknown for him or for her. So the second purpose of this paper is to get the reader be familiar with the basic ideas. The theory of symbolic computations is mathematically very involved. Beside the novelty of the approach this also might keep away the potential users.

We will describe a radically elementary method to treat systems of multivariate polynomial equations. This may serve as a gentle introduction

into the field. Although nontrivial problems can be solved using this elementary technique it cannot be compared in power and flexibility with the most sophisticated methods based on the so-called Gröbner bases technologies. The interested reader may consult with BOEGE, W., GEBAUER, H., KREDEL, H. (1986) and CZAPOR, S.R. (1989).

Mathematical Background

The most important special case of system of multivariate polynomial equations is when each equation is linear in each variable. The sound algebraic background of the system of linear equations is provided by the linear algebra. To attack problems of size of practical interest successfully the numerical and computational aspects have to be taken into consideration and they play an equally important part of the solution.

The other extreme case of system of multivariate polynomial equations is when there is only one polynomial with only one unknown. The theoretical framework of this case is the so-called Galois theory. While the basic concepts and tools of the linear algebra generally are an important part of an engineer's arsenal those of the Galois theory are not and this standpoint is absolutely justified. This highly sophisticated theory has the famous conclusion that the general fifth degree equation cannot be solved in a finite number of steps starting from the coefficients of the polynomial using only addition, subtraction, multiplication, division and extracting roots.

Beside this pessimistic statement the theory does not really have a constructive message to tackle practical problems. So the emphasis in practically significant cases is shifted to the field of the numerical techniques.

The prospects of the general case of several multivariate polynomials are now looking quite bleak. The best we can do facing such a problem is to leave it as fast as we can.

Once again we would like to convince the reader that although the situation is really not simple it is not so hopeless either.

The algebraic geometry deals with high dimensional curves and surfaces in a very general sense. As the Galois theory is not an easy subject, nor is the algebraic geometry. However, there is a lucky circumstance here. The basic idea of simplifying system of multivariate polynomials does not require too much from the algebraic geometry. A not too ambitious approach can be motivated using very elementary concepts.

As an analogy recall that the essence of the Gauss elimination can be explained without any linear algebra. Similarly the intuitive background of the theory of multivariate polynomial equations can be described with-

out the formidable machinery of the algebraic geometry and commutative algebra. Of course this approach has severe limitations on the other hand. Using our analogy it is hard to imagine that someone can properly understand the conjugate gradient method without any knowledge of the linear dependence and independence.

Some Possible Applications

Let us try to prove the following known result from the elementary geometry. This result states that the foot points of the altitudes of a triangle and the half points of the sides of the triangle are on one circle.

After introducing a coordinate system the problem can be formulated in algebraic terms. The triangle can be given by its vertices and we label these vertices by 1,2,3. The foot points of the altitudes and the half point of the sides are labelled by 4,5,6 and 7,8,9, respectively.
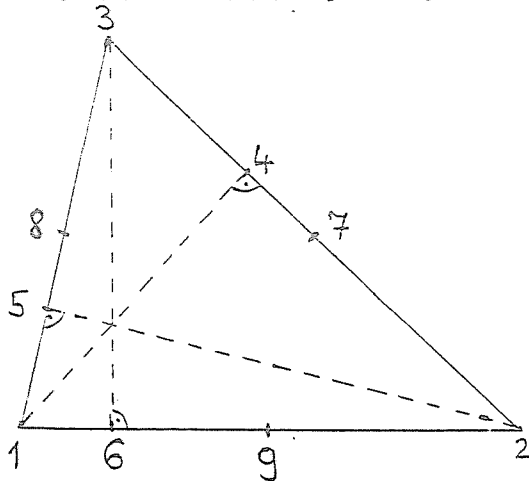

Fig. 1. We have the following information: 7 is the half point of the section 23;
8 is the half point of the section 13; 9 is the half point of the section 12;
4 is on the line 23; 5 is on the line 13; 6 is on the line 12;
the line 14 is perpendicular to the line 23;
the line 25 is perpendicular to the line 13;
the line 36 is perpendicular to the line 12.

From this we would like to draw the conclusion that 7,8,9 are on the circle which passes through 456.

If (x_i, y_i) are the coordinates of the point i, $1 - i - 9$, then the above conditions can be written in the form

$$2x_7 = x_2 + x_3, \quad 2y_7 = y_2 + y_3,$$

$$2x_8 = x_1 + x_3, \quad 2y_8 = y_1 + y_3,$$

$$2x_9 = x_1 + x_2, \quad 2y_9 = y_1 + y_2,$$

$$\begin{vmatrix} x_4 & y_4 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} x_5 & y_5 & 1 \\ x_1 & y_1 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} x_6 & y_6 & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix} = 0,$$

$$(x_4 - x_1)(x_3 - x_2) + (y_4 - y_1)(y_3 - y_2) = 0,$$

$$(x_5 - x_2)(x_3 - x_1) + (y_5 - y_2)(y_3 - y_1) = 0,$$

$$(x_6 - x_3)(x_2 - x_1) + (y_6 - y_3)(y_2 - y_1) = 0.$$

The conclusion can be written in the form

$$\begin{vmatrix} x_7^2 + y_7^2 & x_7 & y_7 & 1 \\ x_4^2 + y_4^2 & x_4 & y_4 & 1 \\ x_5^2 + y_5^2 & x_5 & y_5 & 1 \\ x_6^2 + y_6^2 & x_6 & y_6 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} x_8^2 + y_8^2 & x_8 & y_8 & 1 \\ x_4^2 + y_4^2 & x_4 & y_4 & 1 \\ x_5^2 + y_5^2 & x_5 & y_5 & 1 \\ x_6^2 + y_6^2 & x_6 & y_6 & 1 \end{vmatrix} = 0,$$

$$\begin{vmatrix} x_9^2 + y_9^2 & x_9 & y_9 & 1 \\ x_4^2 + y_4^2 & x_4 & y_4 & 1 \\ x_5^2 + y_5^2 & x_5 & y_5 & 1 \\ x_6^2 + y_6^2 & x_6 & y_6 & 1 \end{vmatrix} = 0.$$

Multiplying out and expanding the determinants we have 12 polynomial equations as conditions and 3 equations as conclusions. We can simplify the problem a bit. First $x_7, y_7, x_8, y_8, x_9, y_9$ can be substituted into the conclusion directly eliminating these variables. Then we can identify the x-axis of the coordinate system with the line 12 and the y-axis with the line 36. The result is twofold since this results $y_1 = y_2 = x_6 = y_6 = x_3 = 0$ and we get rid of the condition which expresses the fact that the line 12 is perpendicular to the line 36. This sort of algebraic reformulation of elementary geometry problems is applicable in a variety of problems. The main question is whether there is a systematic way to verify if a polynomial equation is a consequence of other given equations or not. Further if there is such a systematic method and if this verification can be carried out by a computer efficiently, then we are in position to verify certain elementary geometry results with the assistance of a computer.

Not everyone gets excited by the possibility of mechanical theorem proving. Therefore we list further possible applications having the same flavour.

A mechanical structure made up of segments of given length joined at given points is defined by certain number of variables and polynomial equations. Every movement of this object must take these equations into account. As a consequence manipulating polynomials we may check whether a robot arm can reach a given point or not.

Probably a more realistic area of application is the field of differential equations. We shortly mention two straightforward ideas. Consider for example the next explicit system of ordinary differential equations

$$\frac{dx}{dt} = f, \ \frac{dy}{dt} = g, \ \frac{dz}{dt} = h,$$

where f, g, h are polynomials of the variables x, y, z, t and certain parameters, say α, β. We may be interested in the steady state solution of this system. In this case the left hand sides are equal to zero and so the steady state solution is the one of the resulting polynomial equation system.

Working with functions (one or several variables) we often replace the functions by a truncated power series. This is a common idea in the catastrophe theory or in finite element computation or solving differential equations. The vanishing of the coefficients of the corresponding powers is a necessary condition for the power series to constitute a solution of the problem. In the case these cofficients are polynomials, the original problem leads to a system of polynomial equations.

Euclidean Algorithm

We have already mentioned Gauss' elimination procedure as an illustration. In fact the origin of the method we would like to sketch goes back to Euclid.

In order to find the greatest common divisor of two integers, say 525 and 231 following Euclid we may proceed in the following way. Suppose that d is a common divisor of these numbers. As d divides 525 and 231, it must divide $525 - 2 - 231$. Thus the common divisors of the pair $(525, 231)$ coincide with the common divisors of the pair $(63, 231)$. Of course we can swap here to get the pair $(231, 63)$. Continuing in this fashion we get

$$(42, 63), \ (63, 42), \ (21, 42), \ (42, 21), \ (0, 21), \ (21, 0).$$

from which we can read off the information that the greatest common divisor of 525 and 231 is 21.

We can apply this idea to find the greatest common divisor of two polynomials. Although Euclid did not work with polynomials we also call this method Euclidean algorithm.

Consider the polynomials

$$x^4 + 3x^3 - x^2 - 4x - 3, \ 3x^3 + 10x^2 + 2x - 3$$

and suppose that d is a common divisor of these polynomials. Here d is a polynomial of x. We are looking for a polynomial that divides both of the given polynomials and whose degree is as large as possible. Clearly d divides

$$3(x^4 + 3x^2 - x^2 - 4x - 3) - x(3x^3 + 10x^2 + 2x - 3).$$

Thus from the pair

$$(x^4 + 3x^3 - x^2 - 4x - 3, \ 3x^3 + 10x^2 + 2x - 3)$$

we have the new pair

$$(-x^3 - 5x^2 - 9x - 9, \ 3x^3 + 10x^2 + 2x - 3).$$

Now d has to divide

$$-3(-x^3 - 5x^2 - 9x - 9) + (3x^3 + 10x^2 + 2x - 3)$$

which produces the pair

$$(3x^3 + 10x^2 + 2x - 3, \ 5x^2 + 25x + 30).$$

Of course in this kind of computation we may replace $5x^2 + 25x + 30$ by $x^2 + 5x + 6$. Next d must divide

$$(3x^3 + 10x^2 + 2x - 3) - 3x(x^2 + 5x + 6).$$

This gives the pair $(x^2 + 5x + 6, \ 9x + 27)$ or the pair $(x^2 + 5x + 6, \ x + 3)$. Finally, we have the pairs $(0, \ x + 3)$ and $(x + 3, \ 0)$. Thus $x + 3$ is a greatest common divisor of the original two polynomials. We can see that the greatest common divisor is not uniquely determined since for instance $2x + 6$ and $-x - 3$ are also common divisors with maximal degree.

This technique also works in connection with multivariate polynomials. Consider the polynomials.

$$x^2 - 2xy + y^2 - 1, \ x^2 + 3xy - 4x - 5y^2 + 3.$$

These can be viewed as polynomials in the variables x and y or they can be viewed as polynomials in the variable x, where the coefficients themselves are polynomials in y. From this point of view the polynomials are

$$x^2 + (-2y)x + (y^2 - 1), \quad x^2 + (3y - 4)x + (-5y^2 + 3).$$

Suppose that d is a common divisor of the polynomials. Here d is a polynomial of x, where the coefficients are polynomials of y. The common divisor we are looking for is the greatest in the sense that its degree (in x) is the greatest possible.

As d is a common divisor it must divide

$$\left[x^2 + (-2y)x + (y^2 - 1)\right] - \left[x^2 + (3y - 4y)x + (-5y^2 + 3)\right]$$

which focuses our attention on the pair

$$\left(x^2 + (-2y)x + (y^2 - 1), \quad (-5y + 4)x + (6y^2 - 4)\right).$$

Hence d has to divide

$$(5y - 4)\left[x^2 + (-2y)x + (y^2 - 1)\right] + x\left[-(5y - 4)x + (6y^2 - 4)\right]$$

which gives the pair

$$\left((-4y^2 + 8y - 4)x + (y^2 - 1)(5y - 4), \quad (-5y + 4)x + (6y^2 - 4)\right).$$

Therefore d divides

$$(-5y + 4)\left[(-4y^2 + 8y - 4)x + (y^2 - 1)(5y - 4)\right]$$

$$-(-y^2 + 8y - 4)\left[(-5y + 4)x + (6y^2 - 4)\right].$$

From the resulting pair

$$\left((-5y+4)(y^2 - 1)(5y - 4) - (-4y^2 + 8y - 4)(6y^2 - 4), \quad (-5y+4)x + (6y^2 - 4)\right)$$

or from the pair

$$\left((-5y + 4)x + (6y^2 - 4), \quad -(y^2 - 1)(5y - 4)^2 + 8(y - 1)^2(3y^2 - 2)\right)$$

we have the new pair

$$\Big(-(y^2-1)(5y-4)^2+8(y-1)^2(3y^2-2),\ 4(y-1)^2(6y^2-4)-(5y-4)^2(y^2-1)\Big).$$

Even if we do not finish the computation we can see that the degree (in x) of the greatest common divisor of the original two polynomial is at most zero. In other words the greatest common divisor cannot contain x.

   The essence of the procedure we worked with so far consists of constructing pairs of polynomials, where the first pair is formed from the given two polynomials. Another key observation we will use in connection with these pairs beside the previous ones is that each polynomial occurring in any of these pairs is a linear combination (with polynomial coefficients) of the original polynomials. To make this statement clearer suppose that g and h are the original polynomials and p is a polynomial occurring as a member of one of the pairs. Then there are polynomials u and v such that $p = ug + vh$.

   This claim clearly holds for g and h the members of the initial pair since $g = 1 \cdot g + 0 \cdot h$ and $h = 0 \cdot g + 1 \cdot h$. Following the way we construct the next pair we can verify the claim for the members of this pair as well and we can continue our argument as long as we need.

A Naive Reduction Procedure

The tools now are together to sketch an elimination procedure. Let f, g, h, k be polynomials of the variables x, y, z and consider the system of equations

$$f = 0,\ g = 0,\ h = 0,\ k = 0. \tag{1}$$

First view f, g, h, k as polynomials of x, where the coefficients are polynomials of y and z. Starting with the pair (f, g) using the Euclidean algorithm we construct newer and newer pairs of polynomials. Suppose that p is one of the elements of such a pair. We know that there exist polynomials u and v so that $p = uf + vg$. Thus if (α, β, γ) is a solution of the system (1), then (α, β, γ) satisfies both $f = 0$ and $g = 0$. Therefore (α, β, γ) satisfies $p = 0$ as well. Conversely if (α, β, γ) satisfies $f = 0$ and $p = 0$, then it must satisfy $g = 0$ as well. This means that the original (1) system is equivalent to the new system

$$f = 0,\ p = 0,\ h = 0,\ k = 0. \tag{2}$$

If by chance we detect a p that does not contain x, then the second equation of the corresponding (2) system does not contain x. In other words we eliminated successfully x from the second equation.

In case the polynomial f admits a nontrivial factoring, say $f = rs$, where r and s are not constant polynomials, then the original system of equation (1) forks into two simpler systems of equations

$$r = 0, \ g = 0, \ h = 0, \ k = 0$$

and

$$s = 0, \ g = 0, \ h = 0, \ k = 0.$$

The Euclidean algorithm can reveal such a nontrivial factoring. For instance this is the case when the degree of the greatest common divisor of f and g is at least one. Of course we can detect nontrivial factoring by inspection.

Examples

It is beyond the scope of this paper to show that the elimination procedure we described always works and terminates in finitely many steps. Neither we have the slightest intention to classify the resulting reduced system in order to decide whether it is consistent or inconsistent or in case it is consistent how can we read off the dimension of the solution set and the solutions themselves. Rather we illustrate the procedure with some examples of small size.

First consider the system of equations

$$f = x + y + z = 0,$$
$$g = xy + xz + yz = 0,$$
$$h = xyz + 1 = 0.$$

Consider f, g, h as polynomials of x, where the coefficients are polynomials of y and z. Starting with f and g using the Euclidean algorithm we find the polynomial $y^2 + yz + z^2$, which does not contain x. Similarly starting with f and h we find $y^2z + yz^2 - 1$. Hence the system

$$f = 0, \ g = 0, \ h = 0$$

is equivalent to the system

$$f = x + y + z = 0,$$
$$g_1 = y^2 + yz + z^2 = 0,$$
$$h_1 = y^2z + yz^2 - 1 = 0.$$

Here x is eliminated from the second and third equation.

Now consider g_1 and h_1 as polynomials of y, where the coefficients are polynomials of z. From the (g_1, h_1) pair the Euclidean algorithm gives the polynomial $z^3 + 1$. Therefore the system $f = 0$, $g_1 = 0$, $h_1 = 0$ is equivalent to

$$f = x + y + z = 0,$$
$$g_1 = y^2 + yz + z^2 = 0,$$
$$h_2 = z^3 + 1 = 0.$$

The solutions of $z^3 + 1 = 0$ are

$$-1, \quad -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad \frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

The values of y and x can be determined by substituting back to the second and first equations.

As our next example consider the system of equations

$$f = x^2 - 2xy + y^2 - 1 = 0,$$
$$g = x^2 + 3xy - 4x - 5y^2 + 3 = 0.$$

View f and g as polynomials of x, where the coefficients are of polynomials of y. We have seen in the previous section that the Euclidean algorithm gives

$$g_1 = [8(3y^2 - 2)(y - 1) - (y + 1)(5y - 4)^2](y - 1).$$

The system $f = 0$, $g = 0$ is equivalent to the system $f = 0$, $g_1 = 0$. The solutions of $g_1 = 0$ are

$$0, \quad 1, \quad -\frac{9}{2} + \frac{\sqrt{113}}{2}, \quad -\frac{9}{2} - \frac{\sqrt{113}}{2}.$$

The values of x can be determined from the first equation using these values.

In the last example we illustrate how to detect a non trivial factorization effecting the solution procedure. Let us solve the system of equations

$$f = x + y + z + t = 0,$$
$$g = xy + xt + yz + zt = 0,$$
$$h = xyz + xyt + xzt + yzt = 0,$$
$$k = xyzt + 1 = 0.$$

By inspection we find the factorization

$$xy + xt + yz + zt = x(y + t) + z(y + t) = (x + z)(y + t).$$

As $g = 0$, either $x + z = 0$ or $y + t = 0$. On the other hand since $f = 0$ from $x + z = 0$ it follows that $y + t = 0$ and conversely from $y + t = 0$ it follows that $x + z = 0$.

Substituting $z = -x$ and $t = -y$ into h and k we have

$$-x^2y - xy^2 + x^2y + xy^2 \text{ and } x^2y^2 + 1.$$

Therefore the system $f = 0$, $g = 0$, $h = 0$, $k = 0$ is equivalent to the system

$$x + z = 0, \ y + t = 0, \ x^2y^2 + 1 = 0.$$

For each given (complex) value of x we can compute the corresponding value of y from the last equation and then the value of z and t from the first and second equations. Thus the solution set is one dimensional and can be parameterized by x.

References

BOEGE, W. – GEBAUER, R. – KREDEL, H. (1986): Examples for Solving Systems of Algebraic Equations by Calculating Gröbner Bases, *Journal of Symbolic Computations* Vol. 2, pp. 83–98.

CZAPOR, S. R. (1989): Solving Algebraic Equations Via Buchberger's Algorithm, *Eurocal'87*, pp. 260–269, Berlin, Heidelberg.