Computer Algebra
Systems, Algorithms, Applications[1]

A.H.M. Levelt

University of Nijmegen
Mathematisch Instituut
Toernooiveld 1, 6525 ED Nijmegen
The Netherlands
E-mail: ahml@sci.kun.nl

Abstract

An introduction to computer algebra systems, their capabilities and limitations. Solution of systems of polynomial equations is a theme throughout. A discussion of some basic algorithms is followed by three applications. Showing the power of computer algebra systems for a quick analysis of problems is the main goal of the present paper.

1 Introduction

General computer algebra systems are large software packages intended for 'Mathematical computation', in particular symbolic and algebraic computation, in an interactive way. In the next section some remarks are made on the origin, development, capabilities, use and limitations of computer algebra systems. The differences with numerical computation are indicated. Algorithms are discussed in section 3. Gcd's of polynomials are important in computer algebra. It is shown why the usual Euclidean algorithm is not fit for gcd computations. The remainder of that section is devoted to the solution of polynomial equations; resultants and Gröbner bases are introduced. Section 4 on applications is the main part of the paper. Three problems are discussed which I received in mathematical form without knowing their origins. It starts with a rather easy problem on a recurrence relation. It shows nevertheless the usefulness of computer algebra systems for a quick analysis and solution of problems met in practice. The second application brings out the same point. The last application is more complicated. Several methods are used and the results compared. Apart from the first application the connecting principle in this paper is the solution of systems of polynomial equations.

[1] Lecture at the seminar SCAFI, Brussels 10-11 December 1992. Corrected 18 January 1993

2 Computer algebra systems

Electronic computers have been used from the earliest days for numerical computations. It is not generally known that the history of symbolic computation on computers is almost as old. In 1953 there appeared two Ph.D. theses at M.I.T. on differentiation of functions using a computer. Now almost 40 years later a whole series of computer algebra systems is available which can take over quite a number of tasks that were reserved to mathematicians, physicists and engineers in the old days. General computer algebra can handle floating point numbers, arbitrary large integers, rational numbers, complex numbers, polynomials, rational functions, elementary functions (*sin, cos, exp, log*), matrices (with entries each of the foregoing entities), Taylor series, etc. Arithmetic operations on these entities are performed with absolute precision. Computer algebra systems can handle very large expressions efficiently and error-free. Lots of useful procedures are built in: gcd and factorisation of integers and polynomials, differentiation of expressions, symbolic integration (integration in closed form), Taylor series expansions, solution of linear, polynomial and (certain) differential equations, etc. One can specify one's problems in a language near to 'human' mathematics. The user can add his own algorithms to the built-in ones, customizing in this way the computer algebra system to his needs or specialism.

The history of the development of computer algebra systems is complicated. We shall not go into details. The interested reader may consult [1], [2] and [5] of the References at the end of this paper. Many individuals and groups have played a role, among them (high-energy) physicists who created systems like REDUCE, SCHOONSCHIP and FORM. Another well-known computer algebra system is MACSYMA. The development of MACSYMA started in the early seventies at M.I.T. It has been used in many applications. Of the more recent systems I mention MAPLE, MATHEMATICA and AXIOM. MAPLE was born in 1980 and grew up at the University of Waterloo. This efficient and powerful system is widespread now. It is used in the examples in the present paper. MATHEMATICA is even newer (1985). It was designed by Stephen Wolfram and has become the best-known computer algebra system, partly by its efficient commercialization, but also by the quality of its user interface and the useful packages of applications to many areas of research and engineering. More than his competitors Wolfram realized the importance of a good user interface, splendid graphics and polished documentation. AXIOM became available in 1991. In fact it has a long history as an ambitious internal research project of IBM under the name SCRATCHPAD. Now it is maintained and distributed by NAG, well-known by its numerical software library. Its design is quite different from the other computer algebra systems.

A few words on special computer algebra systems which are designed for more restricted areas of mathematics. Some examples: CAYLEY for group theory, MACAULAY for algebraic geometry (Gröbner bases), FORM for high energy physics (successor to SCHOONSCHIP), CAS for algebraic number theory, LIE for

Lie algebra calculations, etc.

The maturation of computer algebra systems has taken a long time. First the basic algorithms had to be invented or improved and implemented. For this a lot of research was needed (cf. [9]). The use of computer algebra systems was not encouraged by system operators because of the enormous demands of memory and processor time. Moreover, the systems were not friendly to the user. The last decade the picture has changed. Efficient algorithms were available, but above all hardware has become very quick and cheap. A system like MAPLE performs well on a $ 3000 PC (replacing the expensive mainframe of earlier times). Nice user interfaces have removed an obstacle to wide-spread use.

Why are computer algebra systems interactive? Well, there is a profound difference from the use of numerical software. In the latter case the solution strategy does not depend on numerical values computed 'en route'. The actual numerical computations take place once the mathematical analysis has been finished. The running of the program is controlled in that the use of memory (and cpu time) can be estimated in advance. Computer algebra systems, however, are often used for analyzing problems. To a certain extent they replace pencil and paper, and even some human thinking and computing. The user's decision on the next step in the computer will often depend on the result of the previous step.

Though modern computer algebra systems are powerful tools for pure and applied mathematical research, a word of caution must be said. Computer algebra systems are not going to replace numerical computations in the next few years. What can be expected is a growing use of symbolic computation in the problem solving phase and for automatic generation of code for numerical computations. Computer algebra systems can do some amazing things, e.g. symbolic integration. However, they have their limitations. For instance, to the often asked question 'Can they solve differential equations?' the answer is 'Yes, a few'. In fact it is an enormous challenge to mathematicians, pure and applied, to invent algorithms for many domains of mathematics. Only the first small steps have been taken, the great things are for the future.

3 Algorithms

For a mathematician algorithms are the most interesting part of computer algebra systems. At first sight he will be impressed by the enormous speed of the computations with big numbers and complicated polynomial expressions. After some time he will find out that even the quickest computer can be crippled by ill-designed algorithms. This is true a fortiori for those algorithms that are applied thousands of times, sometimes unnoticed because called indirectly. This holds e.g. for automatic simplification procedures. For this reason lots of ingenuity and energy have been spent on the development of efficient basic algorithms. A good account of this research can be found in D. Knuth's famous expression swell', is well-known in computer algebra. Note that inside the above algorithm another algorithm is hidden: the simplification of the rational number coefficients. The mathematicians have gone out of their way to construct better gcd algorithms for polynomials: e.g. several other 'polynomial remainder sequences' such as subresultant sequences. However, the most efficient method is based on another non-intuitive idea: modular calculations and the Chinese remainder theorem. Modular computations play a role in many places. One of the powerful tools of computer algebra is the factorization of polynomials (in one or several variables) in irreducible factors. Here modular factorization (Berlekamp's algorithm) is the starting point.

3.2 Solving systems of polynomial equations

Let $f_1, \ldots, f_r$ be polynomials in the variables $x_1, \ldots, x_n$ and coefficients in a field (e.g. the field **Q** of rational numbers, the real numbers **R** or the complex numbers **C**). Problem: find the common zeros of $f_1, \ldots, f_r$ (in **Q**, **R**, resp. **C**). A common zero is an n-tuple of numbers $\xi_1, \ldots, \xi_n$ such that $f_j(\xi_1, \ldots, \xi_n) = 0$ for all j.

Many problems in pure and applied mathematics come down to the solution of (systems of) polynomial equations. A classical tool is the *resultant*. It is particularly useful when solving a system $f(x, y) = 0, g(x, y) = 0$ of two equations in two unknowns. Write the polynomials in the form

$$f = f_m(x)y^m + \cdots + f_1(x)y + f_0(x),$$

$$g = g_n(x)y^n + \cdots + g_1(x)y + g_0(x),$$

where f_m and g_n are non-vanishing polynoials in x. Then the resultant of f, g with respect to y is the polynomial in x alone, defined by

$$resultant_y(f, g) = \begin{vmatrix} f_m(x) & \cdots & f_0(x) & & \\ & \ddots & & \ddots & \\ & & f_m(x) & \cdots & f_0(x) \\ g_n(x) & \cdots & g_0(x) & & \\ & \ddots & & \ddots & \\ & & g_n(x) & \cdots & g_0(x) \end{vmatrix}.$$

To be more precise: there are n rows with coefficients from f followed by m rows with coefficients from g. Let us temporarily write $R(x)$ for this resultant. The main property of resultants: For any number ξ the following statements are equivalent

(i) There exists a (complex) number η such that $f(\xi, \eta) = 0, g(\xi, \eta) = 0$.

(ii) $R(\xi) = 0$.

Now it is obvious how a system of equations $f(x, y) = 0, g(x, y) = 0$ can be solved. First compute the resultant $R(x)$. Then solve $R(x) = 0$, a polynomial equation in one variable. Let ξ be a solution. Then the main property garantuees the existence of a common solution of the equations $f(\xi, y) = 0, g(\xi, y) = 0$. The latter ones are again equations in one unknown.

Example.

$$f = 8\,x^3 + 24\,x^2y + 24\,xy^2 + 8\,y^3 - 21\,x^2 - 54\,xy - 21\,y^2 + 16\,x + 16\,y,$$

$$g = 5\,x^2 + 6\,xy + 5\,y^2 - 12\,x - 12\,y + 8.$$

We want to solve the system $f(x, y) = 0, g(x, y) = 0$. For this we compute the resultant $R(x)$ of f, g with respect to y and factorize it:

$$R(x) = 64\,(4\,x - 1)(4\,x - 5)(2\,x - 1)^2\,(x - 1)^2\,.$$

The zeros are $x = 1/4, 5/4, 1/2, 1$. First look at $x = 1/4$. We know that $f(1/4, y) = 0, g(1/4, y) = 0$ have a common solution, which turns out to be $y = 5/4$ (e.g. by computing $\gcd(f, g)$). In a similar way one finds the other solutions: $x = 5/4, y = 1/4$, $x = 1/2, y = 1/2$ and $x = 1, y = 1$.

The determinant defining the resultant looks bad for computations. However, there is a link with the Euclidean algorithm which leads to a quick calculation of the resultant. The basic formula is

$$resultant_y(f, g) = (-1)^{mn} g_n^{m-d}\, resultant_y(g, r),$$

where r is the remainder of f divided by g and d is the degree of r as a polynomial in y. Resultants play a role in many parts of computer algebra and in applications. They can also be used for the solution of more general systems of polynomial equations as we shall see in section 4.

A rather recent and very important development in connection with polynomial equations is the theory of Gröbner bases and the algorithm of B. Buchberger (Ph.D. thesis of 1965). Consider the following problem: Let $f, f_1, \ldots, f_r$ be polynomials in $x_1, \ldots, x_n$ with coefficients in a field. Decide whether f belongs to the ideal generated by $f_1, \ldots, f_r$. Buchberger solved this problem by defining special sets of generators for the ideal, so-called Gröbner bases, for which the problem is immediately (algorithmically) solvable. He also devised an algorithm for computing a Gröbner basis from the given generators $f_1, \ldots, f_r$. For non-algebraists this problem does not look exciting. But look at this application. One wants to solve the system of polynomial equations

$$yz^3 + xy^2 - xz^2 - 3\,yz^2 + x^2 - xy + 2\,yz = 0,$$

$$xyz^3 + x^2y^2 - x^2z^2 - 3\,xyz^2 + z^4 + x^3 - x^2y + 2\,xyz - 3\,z^3 + y^2 + z^2 = 0,$$

$$y^2z^3 + z^5 + xy^3 - xyz^2 - 3\,y^2z^2 - 3\,z^4 + x^2y - xy^2 + 3\,y^2z + 2\,z^3 - 3\,z^2 + 2\,z = 0.$$

Applying Buchberger's theory one can proceed as follows. Let f_1, f_2, f_3 be the left hand sides of the above polynomial equations. Consider the ideal I generated by f_1, f_2, f_3. Now compute a Gröbner basis in I (using the lexicographic order on the monomials). This yields a system of polynomial equations in 'triangular form'

$$x^2 - xy = 0,\ y^2 - z^2 = 0,\ z^3 - 3\,z^2 + 2\,z = 0$$

which can easily be solved. The method of Buchberger is almost ideal. The only drawback is that the algorithm is sometimes inefficient as we shall see in the next section.

4 Applications

4.1 A recurrence relation

The following problem was posed by a researcher of physical chemistry department of the Ruhr University at Bochum, Germany. It arose in statistical mechanics. A sequence of numbers $g_1, g_2, \ldots$ is given. Another sequence $f_0, f_1, \ldots$ is defined recursively by

$$f_0 = 1, f_n = g_n s^2 - \sum_{i=1}^{n} \binom{n}{k} f_{n-k} \text{ for } n \geq 1.$$

Here s is a parameter. The question is to compute the f_n efficiently, preferably by finding some explicit expression.

What can we do with such a problem? Well, a mathematical solution avoiding computers is certainly possible. We shall come back to this. However, one can save one's mental energy using a computer algebra system and a general strategy. One simply writes down the commands which compute the successive f_n. Using MAPLE this goes as follows:

```
g:=[23,11,-17,5,23,-2,7,34]: # example input list

f[0]:=1;
for n from 1 to nops(g) do
f[n]:=expand(g[n]*s^2-sum('binomial(n,i)*f[n-i]','i'=1..n))
od;
```

The result is

```
                              f[0] := 1
```

```
                     2
       f[1] := 23 s   - 1

                       2
     f[2] := - 35 s   + 1

                     2
       f[3] := 19 s   - 1

                     2
       f[4] := 47 s   + 1

                       2
    f[5] := - 167 s   - 1

                      2
      f[6] := 302 s   + 1

                       2
    f[7] := - 336 s   - 1

                     2
       f[8] := 60 s   + 1
```

This yields a result but no insight. Let us do now the same computation with a 'general' g.

```
g:=[g1,g2,g3,g4,g5,g6,g7,g8]:
```

The result is

```
              f[0] := 1

                     2
       f[1] := s   g1 - 1

                  2           2
 f[2] := g2 s   - 2 s   g1 + 1
```

```
                             2         2      2
                 f[3] := g3 s  - 3 g2 s  + 3 s  g1 - 1

                        2         2         2      2
            f[4] := g4 s  - 4 g3 s  + 6 g2 s  - 4 s  g1 + 1

            2         2          2          2      2
f[5] := g5 s  - 5 g4 s  + 10 g3 s  - 10 g2 s  + 5 s  g1 - 1

            2         2          2          2          2
f[6] := g6 s  - 6 g5 s  + 15 g4 s  - 20 g3 s  + 15 g2 s

          2
     - 6 s  g1 + 1


            2              2          2          2         2
f[7] := g7 s  - 1 - 21 g2 s  - 35 g4 s  + 35 g3 s  - 7 g6 s

              2      2
     + 21 g5 s  + 7 s  g1


            2              2          2          2          2
f[8] := g8 s  + 1 + 28 g2 s  + 70 g4 s  - 56 g3 s  + 28 g6 s

              2     2            2
     - 56 g5 s - 8 s  g1 - 8 g7 s
```

Here one recognizes immediately Pascal's triangle and the conjectured general formula is

$$f_n := (-1)^n - s^2 \sum_{i=1}^{n} (-1)^{n+i+1} \binom{n}{i} g_i$$

which can easily be proved by induction.
Final remark. The same result can be found by the well-known generating functions technique. This costs some thought and there is more risk of errors.

4.2 Common solutions of two differential equations

A few months ago I got the following problem from an American friend who had got it in his turn from friends of friends. Consider the differential equations

$$\frac{d^2y}{dx^2} = \frac{1}{3}\left(\frac{1}{y} - \frac{1}{x}\frac{dy}{dx}\right)\left[1 + \left(\frac{dy}{dx}\right)^2\right] \tag{1}$$

and

$$A_3(x,y)\left(\frac{dy}{dx}\right)^3 + A_2(x,y)\left(\frac{dy}{dx}\right)^2 + A_1(x,y)\left(\frac{dy}{dx}\right) + A_0(x,y) = 0, \tag{2}$$

where

$$\left\{\begin{array}{lcl} A_3(x,y) & = & -4x^2y + 14y^3 - 9tx^2y^3 \\ A_2(x,y) & = & -8xy^2 + 16x^3 + 9tx^3y^2 \\ A_1(x,y) & = & 8x^2y - 16y^3 - 9tx^2y^3 \\ A_0(x,y) & = & 4xy^2 - 14x^3 + 9tx^3y^2 \end{array}\right. \tag{3}$$

Both (1) and (2) are ordinary, non-linear differential equations for the unknown function y of the (real or complex) variable x. t plays the role of a parameter.

Problem. *Determine the common solutions (if any) of (1) and (2).*

It was conjectured that $y = x$ and $y = -x$ were the only common solutions. That was all that I knew. I had no idea about the origin of the problem. I was able to solve the problem quickly thanks to MAPLE and I sent the solution to my friend. A couple of days later I got an electronic message from the mathematicians Th. Hasanis and Th. Vlachos of the University of Ioannina in Greece thanking me for my help and promising some preprints ([6], [7]). From the title [6] one sees that the problem comes from differential geometry. Explaining the context would take more time and space than solving the problem. Moreover it does not contribute anything to the solution. So we shall not dive into differential geometry. Before discussing the solution I must state my big surprise when I received the report [6] soon afterwards and started reading the appendix. There was an analysis and partial solution of the problem absolutely similar to what I'm going to explain, including the computer calculations!

Let us now try to solve the problem. Each of these equations on its own is unpleasant. So what hope remains for finding common solutions? After looking a bit more at the equations one might get the following idea. Differentiate the second equation with respect to x. Then some new equation (6) in $x, y, dy/dx, d^2y/dx^2$ appears. Elimination of d^2y/dx^2 from (1) and (6) yields an equation (7) in $x, y, dy/dx$. Now we have the two equations (2) and (7) in $x, y, dy/dx$. Eliminating dy/dx from these equations yields an equation (8) in x, y. This is necessarily a polynomial equation: it defines y as a function of x. Any common solution of the given differential equations (1) and (2) must be a solution of (8). So try to find the solutions of (8).

So far so good. But what does (8) look like? Can we really perform all those derivations and eliminations? Let us try. To simplify our notations write $z = dy/dx, w = d^2y/dx^2$ and

$$P = A_3(x,y)z^3 + A_2(x,y)z^2 + A_1(x,y)z + A_0(x,y).$$

Then equation (1) becomes

$$w = \frac{1}{3}\left(\frac{1}{y} - \frac{z}{x}\right)(1+z^2) \tag{4}$$

and (2) becomes

$$P = 0. \tag{5}$$

Now dP/dx can be computed by hand (unpleasant) or by MAPLE (or any other computer algebra system). The result is

$$\begin{aligned} \frac{dP}{dx} &= 27\,tx^2y^2z^2 - 18\,txy^3z^3 - 18\,txy^3z + 27\,tx^2y^2 \\ &\quad -8\,xyz^3 + 48\,x^2z^2 - 8\,y^2z^2 + 16\,xyz - 42\,x^2 + 4\,y^2 \\ &\quad +(18\,tx^3y^2z - 27\,tx^2y^3z^2 - 9\,tx^2y^3 - 12\,x^2yz^2 \\ &\quad +42\,y^3z^2 + 32\,x^3z - 16\,xy^2z + 8\,x^2y - 16\,y^3)w = 0. \end{aligned} \tag{6}$$

Now substitute w from (4) in (6) and obtain

$$\begin{aligned} Q &\equiv (27\,tx^2y^4 + 12\,x^2y^2 - 42\,y^4)z^5 \\ &\quad +(-126\,tx^3y^3 - 56\,x^3y + 184\,xy^3)z^4 \\ &\quad +(72\,tx^4y^2 - 18\,tx^2y^4 + 32\,x^4 - 84\,x^2y^2 - 26\,y^4)z^3 \\ &\quad +(-54\,tx^3y^3 + 132\,x^3y - 126\,xy^3)z^2 \\ &\quad +(72\,tx^4y^2 - 45\,tx^2y^4 + 32\,x^4 + 48\,x^2y^2 + 16\,y^4)z \\ &\quad +72\,tx^3y^3 - 118\,x^3y - 4\,xy^3. \end{aligned} \tag{7}$$

Now we must eliminate z from the equations (5) and (7). The mathematical tool for this is the resultant as we have seen in section 3. The resultant $R = resultant_z(P, Q)$ of P and Q with respect to z is a polynomial in t, x, y with the following property: if $t = t_0, x = x_0, y = y_0, z = z_0$ is a common solution of $P = 0, Q = 0$, then $t = t_0, x = x_0, y = y_0$ is a solution of $R = 0$. The computation of $R = resultant_z(P, Q)$ is a matter of seconds (awkward by paper and pencil) and returns a polynomial in t, x, y with 67 terms which we do not reproduce here. Instead we try to factorize R as a product of irreducible polynomials. The result is

$$R = 972\,x^3y^4\,(x+y)\,(x-y)\,f\,g, \tag{8}$$

where

$$f = 4x^2 - 14y^2 + 9tx^2y^2$$

and

$$\begin{aligned} g \;=\; & 10497600\,t^5x^{18}y^8 + 23783625\,t^5x^{16}y^{10} + 18862875\,t^5x^{14}y^{12} \\ & +18862875\,t^5x^{12}y^{14} + 23783625\,t^5x^{10}y^{16} + 10497600\,t^5x^8y^{18} \\ & +39657600\,t^4x^{18}y^6 - 96782040\,t^4x^{16}y^8 + 18669690\,t^4x^{14}y^{10} \\ & -71893980\,t^4x^{12}y^{12} + 18669690\,t^4x^{10}y^{14} - 96782040\,t^4x^8y^{16} \\ & +39657600\,t^4x^6y^{18} - 43545600\,t^3x^{18}y^4 - 33988896\,t^3x^{16}y^6 \\ & +99268416\,t^3x^{14}y^8 - 65010276\,t^3x^{12}y^{10} - 65010276\,t^3x^{10}y^{12} \\ & +99268416\,t^3x^8y^{14} - 33988896\,t^3x^6y^{16} - 43545600\,t^3x^4y^{18} \\ & -58521600\,t^2x^{18}y^2 + 163236096\,t^2x^{16}y^4 - 250900056\,t^2x^{14}y^6 \\ & +180082080\,t^2x^{12}y^8 - 158754744\,t^2x^{10}y^{10} + 180082080\,t^2x^8y^{12} \\ & -250900056\,t^2x^6y^{14} + 163236096\,t^2x^4y^{16} - 58521600\,t^2x^2y^{18} \\ & -14336000\,tx^{18} + 142511360\,tx^{16}y^2 - 203510080\,tx^{14}y^4 \\ & +299759904\,tx^{12}y^6 - 63472352\,tx^{10}y^8 - 63472352\,tx^8y^{10} \\ & +299759904\,tx^6y^{12} - 203510080\,tx^4y^{14} + 142511360\,tx^2y^{16} \\ & -14336000\,ty^{18} + 26880000\,x^{16} - 70294400\,x^{14}y^2 \\ & +43869056\,x^{12}y^4 + 34700192\,x^{10}y^6 - 104814400\,x^8y^8 \\ & +34700192\,x^6y^{10} + 43869056\,x^4y^{12} - 70294400\,x^2y^{14} \\ & +26880000\,y^{16}. \end{aligned}$$

Remark. Computer algebra systems are strong in factorization of polynomials. From the human point of view there is a big difference between the above computation of the resultant and the factorization. With a lot of energy, precision and scratch paper one may succeed in calculating the resultant avoiding computers (though the risk of making errors is considerable). The factorization is much harder. Yes, there is an algorithm, otherwise computers would be unable to perform this task. However, this algorithm is much more complicated than the one for computing the resultant. Few mathematicians do know that algorithm. Instead when meeting polynomials in their research, they try to factorize by ad hoc methods. However, if unsuccessful, they cannot be sure that the polynomial is irreducible. As opposed to this if a computer algebra system cannot factor a polynomial, that polynomial is guarantueed irreducible. (That is to say... Some months ago somebody discovered that the reducible polynomial

$$\begin{aligned} & x^{15} - x^{14} + 10x^{12} + 20x^{11} + 20x^{10} - 200x^9 - 400x^8 - 300x^7 \\ & -2100x^6 - 6000x^5 - 1000x^4 + 10000x^3 + 10000x^2 + 100000 \end{aligned}$$

cannot be factored by MAPLE V)

Back to our problem. The common solutions of (1) and (2) must be solutions of $R = 0$, whence of one of the factors of R. So we must check each of $x = 0$,

$y = 0$, $x + y = 0$, $x - y = 0$, $f = 0$, $g = 0$ and see whether it yields a common solution of (1) and (2). This is easy for the first four: $y = x$ and $y = -x$ are common solutions, $x = 0$ and $y = 0$ are not. Next, $f = 0$ leads to

$$y = \frac{2x}{\sqrt{14 - 9tx^2}},\ y = \frac{-2x}{\sqrt{14 - 9tx^2}}$$

and an elementary calculation shows that neither satisfies (2) (neither for general t nor for special values of t).

The analysis in [6] stopped here. But there is still some serious work left which I shall briefly explain. MAPLE was used for most computations that follow. Let y be a function of x (and the parameter t) defined by $g = 0$. Claim: y is not a common solution of (1) and (2). This is somewhat harder to prove. Assume $t \neq 0$ (the easier case $t = 0$ is left to the reader). A function y of x satisfying $g(x, y) = 0$ is called algebraic. It is defined everywhere in the complex plane as a multivalued analytic function of x (for any value $\neq 0$ of t. Because of the highest term $-143360000ty^{18}$ of g there are no poles or 'branched' poles at $x = 0$). Let us study the branches at $x = 0$. The equation $g(0, y) = 0$ has three solutions $y = 0, y = \sqrt{15/8t}, y = -\sqrt{15/8t}$. We shall treat theses cases separately.

(i) Branches at (0,0). The plain curve defined by $g(x, y) = 0$ has a singularity at the origin. The nature of that singularity can be seen from the lowest order part. Up to a constant factor that part equals

$$\begin{aligned}&840000y^{16} - 2196700x^2y^{14} + 1370908x^4y^{12} + 1084381x^6y^{10} \\ &-3275450x^8y^8 + 1084381x^{10}y^6 + 1370908x^{12}y^4 \\ &-2196700x^{14}y^2 + 840000x^{16}.\end{aligned} \qquad (9)$$

This form is irreducible over $\mathbf{Q}$ (Check by computer algebra!). So $(0, 0)$ is an ordinary multiple point of multiplicity 16. Hence the branches are regular functions having power series expansions $y = a_1x + a_2x^2 + a_3x^3 + \cdots$. Substituting this series in (2) and comparing coefficients of the various powers of x leads to the following equation

$$(a_1 - 1)(a_1 + 1)(a_1^4 - a_1^2 + 1) = 0.$$

However, none of the solutions a_1 leads to a tangent line $y = a_1x$ to g at (0,0), because (9) does not vanish when such $y = a_1x$ is substituted.

(ii) Branches at $(0, \sqrt{15/8t})$. Write $y = y_0 + v$ where $y_0 = \sqrt{15/8t}$. Expand $g(x, y_0+v)$ as a polynomial in x, v. The lowest order term is v (times a constant). This means that the tangent to the curve $g(x, y) = 0$ at $(0, y_0)$ is horizontal and that $(0, y_0)$ is an ordinary point of the curve. So the branch admits a power series expansion $y = y_0 + b_2v^2 + b_3v^3 + \cdots$. Substituting this power series in $g = 0$ and equating powers of v one finds $b_2 = -197/2250ty_0$. In a similar way substitution of $y = y_0 + b_2v^2 + b_3v^3 + \cdots$ in (1) leads to $b_2 = 1/15ty_0$. This is a contradiction.

(iii) Branches at $(0, -\sqrt{15/8t})$. Similar to (ii).

Conclusion. It is doubtful whether the basic idea of the solution could have led to success without the use of a computer algebra system. It would have certainly taken much more time than the one morning that I needed. It is a brute force solution I admit. But once this solution is obtained one has gained sufficient insight and feeling in order to try and find a solution avoiding the computer. This may be considered more satisfying, but it is also an unrealistic luxury in a situation where 'time is money'. A great advantage of computer algebra systems lies in the possibility of quick analysis of a wide variety of pure and applied mathematics problems.

4.3 A problem from kinematic geometry of mechanisms

Last summer there was a discussion in the MAPLE User Group on dual curves and surfaces. It was started by Mr. Ross McAree of the Robotics Laboratory, Department of Mechanical Engineering at the University of Melbourne. He asked for help in computing the 'dual' of a surface in 3-space. He rightly stated that the computation comes down to the solution of a system of polynomial equations (with parameters). He used MAPLE's 'solve' for the (easy) case of quadratic surfaces and concluded that the procedure becomes hopeless for surfaces of higher degree. He got several reactions. It was explained to him that all this was good old algebraic geometry and that the natural tool to compute the dual surface is Gröbner bases. This was demonstrated for a quadratic surface. Though I agreed in principle, I had my doubts. So I showed the MAPLE User Group the example of a plane curve of degree 3 (an elliptic curve in homogeneous form) for which the dual curve should be computed using MAPLE's Gröbner basis package. The computation went on for one hour on a Sun4/490 and then I stopped it. This was for me the starting point of some more experimentation which finally led to a complete solution of McAree's problem (to be formulated below). Further on I shall come back to kinematic geometry, but I shall first explain the simple mathematics of dual curves and surfaces and show various computations.

Let us start with plane curves and dual curves. A plane algebraic curve C is given by a polynomial equation $f(x, y) = 0$ (with some obvious restrictions). In order to keep things simple inhomogeneous coordinates and equations are used instead of the more customary homogeneous ones. Let (x_0, y_0) be a (general) point of the curve (i.e. $f(x_0, y_0) = 0$). Then the tangent line at (x_0, y_0) to the curve has the equation

$$f_x(x_0, y_0)x + f_y(x_0, y_0)y - (f_x(x_0, y_0)x_0 + f_y(x_0, y_0)y_0) = 0.$$

For the equation $ax + by + c = 0$ of a straight line the pair $(a/c, b/c)$ is called the line coordinates of that line. So the tangent line at (x_0, y_0) to C has line coordinates

$$\xi_0 = \frac{-f_x(x_0, y_0)}{f_x(x_0, y_0)x_0 + f_y(x_0, y_0)y_0}, \ \eta_0 = \frac{-f_y(x_0, y_0)}{f_x(x_0, y_0)x_0 + f_y(x_0, y_0)y_0}.$$

Now we drop the subscript 0 and define a map ϕ from C into the plane by

$$\phi(x, y) = (\xi, \eta), \text{ where } \xi = -f_x/h, \ \eta = -f_y/h, \ h = xf_x + yf_y.$$

The interesting point is now that $\phi(x, y)$ runs through an algebraic curve C' when (x, y) runs through C. C' is called the 'dual curve of C'. How do we find an equation for C'? A minute's thought shows that we must eliminate x, y from the 3 relations $f = 0$, $\xi = -f_x/h$, $\eta = -f_y/h$ or, written differently,

$$f = 0, \ f_x + \xi h = 0, \ f_y + \eta h = 0.$$

Example. $f = x(x-1)(x-2) - y^2$. Here are the MAPLE commands:

```
with(grobner):
f:=x*(x-1)*(x-2)-y^2:
fx:=diff(f,x):
fy:=diff(f,y):
h:=x*fx+y*fy:
G:=gbasis({f,sh+fx,th+fy},[x,y,s,t],plex);
```

Note that s is used instead of ξ and t instead of η. You need not know precisely what the last line means. A Gröbner basis is computed and the theory says that it will contain one polynomial depending on s and t alone. That polynomial f' defines the dual curve C'. The MAPLE computation takes about 1000 seconds on a 15 MIPS computer and yields

$$\begin{aligned} f' \ &= \ -4\xi^4\eta^2 - 24\xi^2\eta^4 - 4\eta^6 + 8\xi^5 + 48\xi^3\eta^2 - 24\xi\eta^4 \\ &\quad +12\xi^4 + 132\xi^2\eta^2 + 4\xi^3 + 108\xi\eta^2 + 27\eta^2. \end{aligned}$$

The word 'dual' suggests a reciprocity. Indeed, if C' is the dual curve of C, then C is the dual curve of C'.

The extension to surfaces in three-dimensional space is obvious. Let S be the defined by the polynomial equation $f(x, y, z) = 0$. The tangent lines to the curve are replaced by tangent planes to the surface. If $\xi\, x + \eta\, y + \zeta\, z + 1 = 0$ is the equation of a tangent plane, we call (ξ, η, ζ) the coordinates of the plane, etc. The dual S' of the surface S is defined by a polynomial equation $f'(\xi, \eta, \zeta) = 0$ where f' is obtained by eliminating x, y, z from the polynomial equations

$$f = 0, \xi\, h + f_x = 0, \eta\, h + f_y = 0, \zeta\, h + f_z = 0 \tag{10}$$

and $h = x\, f_x + y\, f_y + z\, f_z$. Now one might try to find f' the way we did before in the curve situation using Gröbner bases or otherwise. Finally, as expected, the dual surface of S' is the surface S.

Let us look now at McAree's problem. Here the surface S' is given and S must be found. S' is defined by

$$f' = a^2\xi^4 + b^2\eta^4 + c^2\zeta^4 - 2(bc\eta^2\zeta^2 + ca\zeta^2\xi^2 + ab\xi^2\eta^2) - 4(\xi^2 + \eta^2 + \zeta^2). \quad (11)$$

a, b, c are parameters satisfying $a+b+c = 0$. 'Dualizing' (10) we get the system of polynomial equations

$$f' = 0, xh' + f'_\xi = 0, yh' + f'_\eta = 0, zh' + f'_\zeta = 0, \quad (12)$$

where $h' = \xi f'_\xi + \eta f'_\eta + \zeta f'_\zeta$. The equation $f = 0$ of S will result by eliminating ξ, η, ζ from (12). Since there is not much chance that a Gröbner bases computation using Maple will end in a reasonable amount of time, we shall use a computer algebra system which is famous for its efficient Gröbner basis computations. First we try to solve the problem for special values of a, b, c: $a = 2, b = -3, c = 1$. MACAULAY computes with homogeneous polynomials. So we must homogenize f'. Then the MACAULAY session looks as follows.

```
Macaulay version 3.0, created 8/14/89

% ring R
! characteristic (if not 31991)       ?
! number of variables                 ? 4
!   4 variables, please               ? xyzw
! variable weights (if not all 1)     ?
! monomial order (if not rev. lex.)   ?
;   largest degree of a monomial        : 512

% ideal I
! number of generators ? 1
! (1,1) ? (4x^4+9y^4+z^4)-2(-3y^2z^2+2z^2x^2-6x^2y^2) \
; -4(x^2+y^2+z^2)w^2)

% <dual_variety I 1 J

% type J
;x6+3x4y2+3x2y4+y6+3x4z2+6x2y2z2+3y4z2+3x2z4+3y2z4+z6+5x4w2 \
;-8x2y2w2-25/4y4w2-44x2z2w2-43/2y2z2w2+47/4z4w2+3x2w4+13y2w4 \
;+33z2w4-9w6
```

The computation takes a few minutes. The last expression is the polynomial defining the dual surface in homogeneous form. The inhomogeneous form is obtained by substituting $w = 1$. In a more attractive form it reads like this

$$f = x^6 + 3x^4y^2 + 3x^2y^4 + y^6 + 3x^4z^2 + 6x^2y^2z^2 + 3y^4z^2 \quad (13)$$

$$+3x^2z^4+3y^2z^4+z^6+5x^4-8x^2y^2-\frac{25}{4}y^4-44x^2z^2$$
$$-\frac{43}{2}y^2z^2+\frac{47}{4}z^4+3x^2+13y^2+33z^2-9.$$

After this success one hopes that the MACAULAY computation for general parameter values is feasible. McAree and I have tried in vain. So the computation seems impossible. In fact it is not. Good old resultants perform the miracle! I shall sketch the method leaving out details.

We start with f' as in (11) and define

$$h'=\xi f'_\xi+\eta f'_\eta+\zeta f'_\zeta,\ g_1=xh'+f'_\xi,\ g_2=yh'+f'_\eta,\ g_3=zh'+f'_\zeta.$$

We must eliminate now ξ,η,ζ from the equations

$$f'=0,\ g_1=0,\ g_2=0,\ g_3=0.$$

Let us start eliminating ζ. For this we use resultants with respect to ζ:

$$k_1=resultant_\zeta(f',g_1),\ k_2=resultant_\zeta(f',g_2),\ k_3=resultant_\zeta(f,g_3)$$

and the equations

$$k_1=0,\ k_2=0,\ k_3=0 \tag{14}$$

must be fulfilled. These are polynomial equations in x,y,z,ξ,η with a,b as parameters. It turns out that k_1 and k_2 are squares of polynomials, $k_1=p_1^2$, $k_2=p_2^2$, say. Moreover, k_3 is product of a factor depending only on a,b and a polynomial p_3. So the system of equations (14) can be replaced by $p_1=0,p_2=0,p_3=0$. In the next step we eliminate η from these equations by defining

$$q=resultant_\eta(p_1,p_2),\ r=resultant_\eta(p_1,p_3).$$

q and r are polynomials in x,y,z,ξ and the parameters a,b. Writing down all these definitions is easy enough. But can the computer algebra system really perform all the computations? The answer is yes, but the sheer size of the expressions is enormous. MAPLE produces q as a product of a polynomial in a,b alone and another factor $\bar{q}$ with 4641 terms. Similarly, r is product of a polynomial in a,b alone and a factor $\bar{r}$ with 4393 terms. In spite of their excessive size $\bar{q}$ and $\bar{r}$ can be factored in a reasonable amount of time. The simplest non-trival factor of $\bar{q}$ is

$$\begin{aligned}\bar{q} \ = \ & b^2\xi^3x^4-2ab\xi^3x^2y^2+a^2\xi^3y^4\\ & -(4ab\xi^2+2b^2\xi^2+4)x^3+(4a^2\xi^2+2ab\xi^2)xy^2\\ & -(a^3b\xi^3+a^2b^2\xi^3+a^2\xi-b^2\xi)x^2+(a^3b\xi^3+a^4\xi^3)y^2.\end{aligned}$$

The simplest non-trivial factor of $\bar{r}$ is

$$\begin{aligned}\bar{r} \ = \ & (a^2\xi^3+2ab\xi^3+b^2\xi^3)x^4+(2a^2\xi^3+2ab\xi^3)x^2z^2+a^2\xi^3z^4\\ & -(2b^2\xi^2-2a^2\xi^2+4)x^3-(2ab\xi^2-2a^2\xi^2)xz^2\\ & -(a^3b\xi^3+a^2b^2\xi^3-b^2\xi-2ab\xi)x^2-a^3b\xi^3z^2.\end{aligned}$$

The final step is the elimination of ξ from $\bar{q} = 0$, $\bar{r} = 0$. Define

$$R = resultant_\xi(\bar{q}, \bar{r}).$$

Then s contains 2 non-trivial factors R_1, R_2 where

$$\begin{aligned} R_1 \;=\; & 4x^6 + 4y^6 + 4z^6 + 12x^4y^2 + 12x^4z^2 + 12x^2y^4 + 12x^2z^4 + 12y^4z^2 \\ & +12y^2z^4 + 24x^2y^2z^2 + (-a^2 + 8ab + 8b^2)x^4 + (8a^2 + 8ab - b^2)y^4 \\ & -(a^2 + 10ab + b^2)z^4 - (20a^2 + 38ab + 20b^2)x^2y^2 \\ & -(20a^2 + 2ab + 2b^2)y^2z^2 - (2a^2 + 2ab + 20b^2)x^2z^2 \\ & +(-2a^3b + 2a^2b^2 + 8ab^3 + 4b^4)x^2 + (4a^4 + 8a^3b + 2a^2b^2 - 2ab^3)y^2 \\ & +(2a^3b + 8a^2b^2 + 2ab^3)z^2 - (a^4b^2 + 2a^3b^3 + a^2b^4). \end{aligned}$$

R_2 will not be shown, because we can verify that R_1 is indeed the equation of the dual surface. (Check that $R_1/4$ specializes to (13) when $a = 2, b = -3$). Because of the reciprocity it suffices to prove that if (ξ, η, ζ) is a point of S', then its image $(-f'_\xi/h', -f'_\eta/h', -f'_\zeta/h')$ on the dual surface S of S' satisfies $R_1(-f'_\xi/h', -f'_\eta/h', -f'_\zeta/h') = 0$. In other words, $f'(\xi, \eta, \zeta) = 0$ should imply $R_1(-f'_\xi/h', -f'_\eta/h', -f'_\zeta/h')$. In order to see that this true one computes the numerator of $R_1(-f'_\xi/h', -f'_\eta/h', -f'_\zeta/h')$ (a polynomial with 3275 terms) which turns out to be divisible by f'.

I got the expression R_1 at about the time that Mr. McAree answered my question on the origin of the problem. It turned out to be a problem in kinematic geometry of mechanisms which I shall explain succinctly below, and he had candidate for S. Here I only state his conjecture: S is the 'sextic point surface' defined by $SPS = 4P^3 + 27Q^2 = 0$ where

$$\begin{aligned} P &= x^2 + y^2 + z^2 + \{h_\alpha h_\beta + h_\beta h_\gamma + h_\alpha h_\gamma\}, \\ Q &= h_\alpha x^2 + h_\beta y^2 + h_\gamma z^2 + h_\alpha h_\beta h_\gamma \end{aligned}$$

and

$$h_\beta - h_\gamma = a,\; h_\gamma - h_\alpha = b,\; h_\alpha - h_\beta = c.$$

Indeed the reader will have no difficulty in checking that $SPS + R_1 = 0$, that is to say under the implicit assumption $h_\alpha + h_\beta + h_\gamma = 0$.

A final remark on the computation. The argument used to identify $R_1 = 0$ as the equation of the dual of the surface S' can be applied directly to verify McAree's conjecture, a computation of the dual is not needed!

The 'mechanisms' in the title of this section are, loosely speaking, objects composed of rigid bodies connected by joints of several types. For obvious practical reasons this was already an important discipline in the last century. Modern robotics has renewed the interest.

The instantaneous movement of a rigid body can be described by an angular velocity ω around an instantaneous rotation axis and a translational velocity τ

parallel to the rotational axis (with respect to a 'fixed' object). For more than a century such instantaneous movements have been studied by means of 'screws'. A screw is given by a straight line in three-space, the screw axis, and a 'pitch', a real number. In the case considered here the screw axis is the instantaneous rotational axis and the pitch is the number h such that $h\omega = \tau$. Note that the screw does not describe the instantaneous movement of a body completely (τ or ω must be known too). However, the description in terms of screws turns out to be very useful. Now think of a robot arm consisting of three rigid pieces α, β, γ, α being connected by a screw S_α to the (fixed) wall (i.e. S_α is the screw defined by the instantaneous movement of α with respect to the wall), β by a screw S_β to α, γ by a screw S_γ to β. We want to know the instantaneous movement of γ with respect to the wall which is again given by a screw S (and a angular velocity or translational velocity). Knowing S, we know the instantaneous movement of γ if e.g. $\tau_\alpha, \tau_\beta, \tau_\gamma$ are known. S itself is completely determined by $S_\alpha, S_\beta, S_\gamma$ and e.g. the ratio $\omega_\alpha : \omega_\beta : \omega_\gamma$. Hence for given (independent) $S_\alpha, S_\beta, S_\gamma$ the screw S depends on two parameters. The possible S form a so-called 'three-system' (consisting of the screws 'linearly dependent' on $S_\alpha, S_\beta, S_\gamma$). In the special case of $S_\alpha, S_\beta, S_\gamma$ along the cartesian coordinate axis, an easy description of the three-system is possible by means of the following equation

$$(h_\alpha - h)x^2 + (h_\beta - h)y^2 + (h_\gamma - h)z^2 + (h_\alpha - h)(h_\beta - h)(h_\gamma - h) = 0, \quad (15)$$

where $h, h_\alpha, h_\beta, h_\gamma$ are the pitches of $S, S_\alpha, S_\beta, S_\gamma$, respectively. For a proof cf. ([8]), chapter 12, in particular formula (12.12). For fixed h equation (15) represents a quadric and the two systems of straight lines on it are the axes of the screws of the three-system having pitch h. For a given point (x, y, z) three values of h satisfy (15). So there are three screws passing through (x, y, z). For the three values of h there are three possibilities: (i) all three are real and different, (ii) one is real, the two remaining being conjugate complex and different, (iii) at least two are equal. The latter one is the 'critical' case, the transition from (i) to (ii). (iii) holds when the discriminant of (15) with respect to h vanishes. This discriminant is just SPS, if $h_\alpha + h_\beta + h_\gamma = 0$ is assumed.

The intersection of the three-system with an arbitrary plane $\xi x + \eta y + \zeta z + 1 = 0$ gives (for fixed h) a conic section. An expression in coordinates x, y in that plane can be obtained by eliminating z from (15) and $\xi x + \eta y + \zeta z + 1 = 0$. This conic section degenerates in two straight lines (screw axis) when

$$(h - h_\beta)(h - h_\gamma)\xi^2 + (h - h_\gamma)(h - h_\alpha)\eta^2 + (h - h_\alpha)(h - h_\beta)\zeta^2 + 1 = 0. \quad (16)$$

Hence in a given plane one finds two screws of the three-system. More precisely, for the screw axes one has the following possibilities: (i) both real and different, (ii) both conjugate complex and different, (iii) coincidence. The latter case is again the critical one. It holds if and only if the discriminant of (16) vanishes. This discriminant is

$$QES \quad = \quad ((h_\beta + h_\gamma)\xi^2 + (h_\gamma + h_\alpha)\eta^2 + (h_\alpha + h_\beta)\zeta^2)^2$$

$$-4(\xi^2+\eta^2+\zeta^2)(h_\beta h_\gamma \xi^2 + h_\gamma h_\alpha \eta^2 + h_\alpha h_\beta \zeta^2 + 1).$$

This is exactly the f' (cf. (11)) we started with, and McAree's conjecture was that $QES = 0$ is dual to $SPS = 0$. The interested reader is referred to [8], in particular Chapter 12 and Examples 12B, 4 and 6.

References

[1] A. Boyle, B.F. Caviness (ed.), *Future Directions for Research in Symbolic Computation*, Report of a Workshop on Symbolic and Algebraic Computation, Washington DC, 1988, Society for Industrial and Applied Mathematics, Philadelphia, 3600 University City Science Center, Philadelphia, PA 19104-2688, 1990

[2] B. Buchberger, G.E. Collins, R. Loos, *Computer Algebra, Symbolic and Algebraic Computation*, Springer-Verlag, Wien/ New York, 1981, ISBN 3-211-81684-4

[3] J.H. Davenport, Y. Siret, E. Tournier, *Calcul formel*, Etudes et recherches en informatique, Masson, Paris, New York, 1987, ISBN 2-225-80990-9

[4] J.H. Davenport, Y. Siret, E. Tournier, *Computer Algebra*, Academic Press, 1988, ISBN 0-12-204230-1

[5] K.O. Geddes, S.R. Czapor, G. Labahn, *Algorithms for Computer Algebra*, Kluwer, Boston, 1992

[6] Th. Hasanis, Th. Vlachos, *Hypersurfaces with constant scalar curvature and constant mean curvature*, Technical Report, No 189, Dept. of Mathematics, University of Ioannina, 1991

[7] Th. Hasanis, Th. Vlachos, *Hypersurfaces in E^4 with harmonic mean curvature vector field*, Preprint, Department of Mathematics, University of Ioannina

[8] K.H. Hunt, *Kinematic Geometry of Mechanisms*, Oxford Engineering Science Series 7, Oxford University Press, 1990, ISBN 0-19-856233-0

[9] D.E. Knuth, *The Art of Computer Programming, Vol 2. Seminumerical Algorithms*, Addison-Wesley Publishing Company Reading, Massachusetts, 2nd edition, 1981, ISBN 0-201-03822-6

[10] M.A.H. MacCallum, F.J. Wright, *Algebraic Computing with* REDUCE, Clarendon Press, Oxford,1991, ISBN 0-19-853444-2

[11] M. Mignotte, *Mathématiques pour le calcul formel*, Presses Universitaires de France, Paris, 1989, ISBN 2-13-042259-4

[12] R. Pavelle (ed.), *Applications of Computer Algebra*, Kluwer Academic Publishers, Boston, Dordrecht, Lancaster,1985, ISBN 0-89838-173-8