Singular and Applications

Gert-Martin Greuel and Gerhard Pfister

11th May 2006

A Computer Algebra System for Polynomial Computations
with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory
G.-M. Greuel, G. Pfister, H. Schönemann
Technische Universität Kaiserslautern
Fachbereich Mathematik; Zentrum für Computer Algebra
D-67663 Kaiserslautern

The computer is not the philosopher's stone but the philosopher's whetstone
Hugo Battus, Rekenen op taal 1983

1 Introduction

Being asked to present the computer algebra system SINGULAR we face the problem to make a choice which should explain at least part of the functionality of the system but, at the same time, present some non–trivial mathematics. We decided to concentrate on applications where SINGULAR has been used successfully to either solve a mathematical problem or to find the correct statement of a theorem which then could be proved without computer, or to construct interesting examples. These applications belong to algebraic geometry and singularity theory, the main area of applications, but also to group theory, general relativity, and one application outside mathematics.

In the first four sections we explain some of the basic notions and features of SINGULAR while the last six sections are devoted to applications. The content of this article is as follows:

1. Introduction
2. General Overview
3. Gröbner Bases
4. Computing in Local Rings
5. Non–Commutative GR–Algebras
6. Some Historical Remarks
7. A Theorem in Group Theory
8. Resolution of Singularities
9. SINGULAR and General Relativity
10. Curves and Surfaces with many Singularities
11. Applications outside Mathematics

2 General Overview

SINGULAR[1] is a Computer Algebra System for polynomial computations with special emphasis on the needs of algebraic geometry, commutative algebra and singularity theory.

SINGULAR's main computational objects are polynomials, ideals and modules over a large variety of rings. SINGULAR features one of the fastest and most general implementations of various algorithms for computing standard resp. Gröbner bases. Furthermore, it provides multivariate polynomial factorization, resultant, characteristic set and gcd computations, syzygy and free resolution computations, numerical root–finding, visualisation, and many more related functionalities. SINGULAR version 3 and higher contains a kernel extension for a large class of non–commutative algebras.

Based on an easy-to-use interactive shell and C-like programming language, SINGULAR's internal functionality is augmented and user-extendable by libraries written in the SINGULAR programming language or in C++. A general and efficient implementation of links as endpoints of communications allows SINGULAR to make its functionality available to and be easily incorporated into other programmes.

The main goal of the SINGULAR–group is to further develop and implement *advanced* algorithms to be used for mathematical research, in particular in commutative algebra, algebraic geometry and singularity theory. There exist already several libraries providing such algorithms, including absolute primary decomposition for several ground fields, ring normalization (integral closure), versal deformations of arbitrary isolated singularities, monodromy and spectral numbers for hypersurface singularities, resolution of singularities, Hamburger–Noether (Puiseux)–expansions of plane curve singularities and many more. Many of these algorithms are not available in other systems.

Due to non–mathematical applications SINGULAR contains also a library for symbolic–numerical polynomial solving. Although designed for supporting research in algebraic geometry and singularity theory SINGULAR has been used widely in many other mathematical and non–mathematical fields. As a specialized system, SINGULAR's aim is not to provide all the functionality of a general purpose system. The main strength of the system, besides the above mentioned functionality, is the speed of the important basic algorithms such as Gröbner basis, syzygy, and free resolution computations for modules. It is impossible to detail any of the algorithms, we rather refer to the literature, given in the references.

SINGULAR's online help system is available in various formats where the HTML format is especially user-friendly. Some reasons for the increasing popularity of SINGULAR are its speed, its functionality, its user–friendliness and last but not least, because it is free of charge.

Availability. SINGULAR is publicly available as a binary program for all common Unix platforms including LINUX, for Windows, MacOs X and several other platforms. SINGULAR is free software under the GNU General Public Licence. The current version number is 3.0.1; it can be downloaded by following the instructions given at SINGULAR's homepage `http://www.singular.uni-kl.de` where more and always up–to–date information can be found.

In 2004 the SINGULAR team was awarded the first Richard D. Jenks Memorial Prize for Excellence in Software Engineering for Computer Algebra at the ISSAC meeting in Santander.

[1] `http://www.singular.uni-kl.de`

Acknowledgements. The development of SINGULAR has been supported by the Deutsche Forschungsgemeinschaft, the Stiftung Rheinland–Pfalz für Innovation, and the VW–Stiftung which we greatfully acknowledge. We should like to mention and to thank the many mathematicians who contributed to the system, either to the kernel or by writing a library of just by giving hints for improvements.

3 Gröbner bases

Most of the important algorithms implemented in SINGULAR are based on Gröbner basis computations and on multivariate polynomial factorization . For convenience of the reader we will briefly explain the concept of Gröbner bases[2]. Let $M = \{x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \mid \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}\} \subseteq K[x_1, \ldots, x_n]$ be the set of monomials in the polynomial ring in the variables $x_1, \ldots, x_n$ over the field[3] K. On M we consider a well–ordering $<$ which is compatible with the semi–group structure, i.e. $x^\alpha < x^\beta$ implies $x^{\alpha+\gamma} < x^{\beta+\gamma}$. We assume now all polynomials sorted with respect to $<$. For $p \in K[x_1, , \ldots, x_n]$, $p \neq 0$, we write $p = C(p)L(p) + \sum\limits_{\beta < L(p)} C_\beta x^\beta$ with $C(p), C_\beta \in K$ and $L(p) \in M$. $C(p)$ is called the leading coefficient, $L(p)$ the leading monomial of p. We define $C(0) = 0$ and $L(0) = 1$. We give the following two examples for monomial orderings (which are the most important orderings in applications): the lexicographical ordering (abbreviated lp in SINGULAR)

$$x^\alpha >_{\text{lp}} x^\beta \text{ if } \alpha_j = \beta_j \text{ for } j \leq k-1 \text{ and } \alpha_k > \beta_k,$$

and the degree–reverse–lexicographical ordering (denoted dp in SINGULAR)

$$x^\alpha >_{\text{dp}} x^\beta \text{ if } \sum \alpha_i > \sum \beta_i \text{ or } \sum \alpha_i = \sum \beta_i \text{ and } \alpha_j = \beta_j \text{ for } j \geq k+1 \text{ and } \alpha_k < \beta_k$$

The following polynomial $p = 77x_2^3 + 2x_1x_2 + x_2^2 + 5x_1 + 3x_2 + 1$ is sorted with respect to dp. With respect to lp it has to be written as $2x_1x_2 + 5x_1 + 77x_2^3 + x_2^2 + 3x_2 + 1$.

A basic notion in connection with Gröbner bases is the normal form of a polynomial f with respect to a set of polynomials $G = \{f_1, \ldots, f_k\}$.

We give it in terms of an algorithm NF($f|G$):

NF($f|G$)
Input: f, G
Output: the normal form of f w.r.t. G
$h := f$
while ($\exists$ monomial $m, s.t.$ $L(h) = mL(f_i)$ for some i)
  $h := h - \frac{C(h)}{C(f_i)} m f_i$
return $(C(h)L(h) +$ NF $(h - C(h)L(h)|G)$.

Note that $N(f|G)$ is the remainder of a "division of f by G", i.e. $f = \sum\limits_{i=1}^{k} g_i f_i + NF(f|G)$ for some $g_i \in K[x_1 \ldots, x_n]$.

[2]For more details cf. [10].

[3]The fields implemented in SINGULAR are the rational numbers, finite fields and finite transcendental respectively algebraic extensions of them. For numerical calculations SINGULAR offers floating point real and complex numbers.

As an example we see (with respect to dp)

$$NF(x_1^3x_2 + x_1x_2 + x_3^2 \mid \{x_1^3 + x_3, x_3^2 - x_3\}) = x_1x_2 - x_2x_3 + x_3.$$

The normal form can be used to define Gröbner bases:

Let $I := \langle f_1, \dots, f_k \rangle = \{\sum_{i=1}^{k} h_if_i \mid h_i \in K[x_1, \dots, x_n]\}$ be the ideal generated by $f_1, \dots, f_k$. A set $G = \{g_1, \dots, g_s\} \subset I$ is called a Gröbner basis of I if it has the following property:

$$f \in I \text{ if and only if } NF(f|G) = 0.$$

It follows that G generates I.

As an example consider the linear polynomials

$$\begin{aligned} f_1 &= x_1 + x_2 + x_3 - 1 \\ f_2 &= x_1 + 2x_2 - x_3 + 2\ . \end{aligned}$$

In this case the Gauß algorithm gives the Gröbner basis

$$\begin{aligned} g_1 &= x_1 \quad + 3x_3 - 4 \\ g_2 &= \quad x_2 - 2x_3 + 3. \end{aligned}$$

Indeed, Buchberger's algorithm [3] is a common generalisation of Gauß's algorithm and Euklid's algorithm to multivariate systems of polynomial equations. Unfortunately Buchberger's algorithm to compute Gröbner bases has worst-case double exponential complexity with respect to the number of variables. Fortunately, in many cases of interest, this complexity is not reached. Nevertheless Gröbner bases can be rather complicated and it can take a lot of time to compute them.

One important property of Gröbner bases (which could be used as definition) is the following:

Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal and $L(I) = \langle \{L(f) \mid f \in I\} \rangle$ the so–called leading ideal. Then the leading monomials of a Gröbner basis generate the leading ideal.

Since the leading ideal is generated by monomials many invariants of the leading ideal can be computed efficiently by combinatorial algorithms. Since the ideal and the leading ideal have several invariants in common, such as the dimension or the Hilbert function for homogeneous ideals, these invariants can be computed if we know a Gröbner basis.

With the help of Gröbner bases we can eliminate : If G is a Gröbner basis of I with respect to lp then the set $G \cap K[x_k, \dots, x_n]$ is a Gröbner basis and hence generates $I \cap K[x_k, \dots, x_n]$. The computation of the ideal $I \cap K[x_k, \dots, x_n]$ is called elimination of $x_1, \dots, x_{k-1}$ from I. Geometrically this means that we can compute the ideal of the closure of the image under the projection $\pi : V(I) \subset K^n \to K^{n-k+1}$. Elimination is one of the most fundamental applications of Gröbner bases.

Another important application of Gröbner bases is the pre–processing for solving 0–dimensional systems of polynomial equations using triangular sets [4]. It is numerically easy and stable to compute the zero's of a triangular set. For given $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ having only finitely many common zeroes (over the algebraic closure of K) one can compute (using Gröbner bases) triangular sets $T_1, \dots, T_r$ such that the zero–set of $f_1, \dots, f_m$ is the union of the zero–sets of the triangular sets $T_i : V(f_1, \dots, f_m) = \bigcup_{i=1}^{r} V(T_i)$.

Consider the following example:

[4] Let $h_1(x_1) \in K[x_1]$, $h_2(x_1, x_2) \in K[x_1, x_2], \dots, h_n(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ then $T = \{h_1, \dots, h_n\}$ is a triangular set.

```
>ring A = 0,(x,y,z),lp;
>ideal I=x2+y+z-1, x+y2+z-1, x+y+z2-1;

>ideal J=groebner(I); J;  // the Groebner basis of I
J[1]=z6-4z4+4z3-z2
J[2]=2yz2+z4-z2
J[3]=y2-y-z2+z
J[4]=x+y+z2-1

>LIB"solve.lib";          // we load the library solve.lib
>triangL(J);              // the triangular sets
[1]:                         [2]:
   _[1]=z4-4z2+4z-1             _[1]=z2
   _[2]=2y+z2-1                 _[2]=y2-y+z
   _[3]=2x+z2-1                 _[3]=x+y-1

>list L=solve(I,6);       // we solve I directly; internally triangular sets are used
```

SINGULAR displays the 5 solutions and information on how to further use the solutions.

```
[1]:                [2]:                [3]:         [4]:         [5]:
   [1]:                [1]:                [1]:         [1]:         [1]:
      -2.414214           0.414214            0            1            0
   [2]:                [2]:                [2]:         [2]:         [2]:
      -2.414214           0.414214            0            0            1
   [3]:                [3]:                [3]:         [3]:         [3]:
      -2.414214           0.414214            1            0            0


// 'solve' created a ring, in which a list SOL of numbers (the complex
// solutions)  is stored.
// To access the list of complex solutions, type (if the name R was assigned
// to the return value):
        setring R; SOL;
```

4 Computing in local rings

The idea of Gröbner bases can be found already in papers of Gordan (1899). They have been used later by Macaulay and Gröbner to study Hilbert functions of graded ideals. The first algorithm to compute them in polynomial rings was given by Buchberger (1965) [3]. Buchberger's algorithm had an important impact on the development of symbolic methods in and outside mathemtics.

So far we considered Gröbner bases and Buchberger's algorithm for ideals in polynomial rings. An analog concept has been developed for power series rings by Hironaka (1964) in his famous proof for resolution of singularities (he called them standard bases) and, later but independently, by Grauert (1972) to prove the existence of a semi–universal deformation for isolated singularities. Mora (1982) introduced the tangent cone algorithm to compute standard bases for ideals generated by polynomials in power series rings or localizations of the polynomial ring in a maximal ideal with respect to degree orderings. This concept has been generalized to arbitrary monomial orderings (including global and local orderings as a special case) by the authors (cf. [10]). Standard bases for arbitrary monomial orderings have been implemented in SINGULAR since the beginning of 1990. We use the same concept as in section 3 but do not require that the ordering $<$ is a well–ordering[5]. Of special interest are local orderings, where $<$ is called a local ordering if $x_i < 1$ for all i. If an ordering is neither global nor local it is called a mixed ordering. Now let $>$ be a local ordering and let $S_>$ be the set of all polynomials u with $L(u) = 1$. $S_>$ is multiplicatively closed and we define $K[x_1, \ldots, x_n]_>$ to be the localization of $K[x_1, \ldots, x_n]$ by $S_>$ that is, we formally invert all polynomials $u \in S_>$. Note that $K[x_1, \ldots, x_n]_> = K[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$, the localisation of the polynomial ring at the maximal ideal $\langle x_1, \ldots, x_n \rangle$.

Let us consider the following example for a local ordering: (ds) the local degree revers lexicographical ordering

$$x^\alpha >_{\mathrm{ds}} x^\beta \text{ if } \sum \alpha_i < \sum \beta_i \text{ or } \sum \alpha_i = \sum \beta_i \text{ and } x^\alpha >_{\mathrm{dp}} x^\beta .$$

For non–well–orderings the normal form algorithm of section 3 does not terminate and has to be modified. Then the modified normal form algorithm (again called NF) can be used as before to define standard bases[6].

As before we may read informations of the ideal from the leading ideal, e.g.:

$$\begin{aligned} \dim K[x]_>/I &= \dim K[x]/L_>(I), \\ \dim_K K[x]_>/I &= \dim_K K[x]/L_>(I) \ , \end{aligned}$$

or we can compute the Hilbert–Samuel function using the leading ideal for a local degree–ordering. Many applications in singularity theory are based on standard basis computations, and computations of syzygies which can be found in the libraries of SINGULAR:

- `sing.lib` (computing invariants of singularities)
- `classify.lib` (Arnold's classification of singularities)
- `mondromy.lib` (monodromy of isolated hypersurface singularities)
- `gmssing.lib` (invariants related to the Gauß–Manin System of an isolated singularity)
- `hnoether.lib` (Hamburg–Noether resp. Puiseaux–expansion)
- `deform.lib` (miniversal deformation)

5 Non-Commutative GR-Algebras

SINGULAR allows us to compute Gröbner bases and syzygies over a large class of non-commutative algebras to which we refer as *GR-algebras* (here, GR stands for Gröbner-ready). GR-algebras are obtained from the free associative algebra on $x_1, \ldots, x_n$ by imposing specific relations. We write $K\langle \boldsymbol{x} \rangle = K\langle x_1, \ldots, x_n \rangle$ for this free algebra. That is, $K\langle \boldsymbol{x} \rangle$ is the associative graded K-algebra with K-vector space basis the words in $x_1, \ldots, x_n$,

$$B = \left\{ x_{i_1} x_{i_2} \cdots x_{i_\nu} \;\middle|\; \nu \in \mathbb{N},\ 1 \le i_\ell \le n \text{ for all } \ell \right\},$$

where multiplication and grading are defined in the obvious way. Moreover, we consider the set of special words, also called standard monomials,

$$M := \left\{ \boldsymbol{x}^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \mid \alpha \in \mathbb{N}^n \right\} \subset B .$$

[5]It is a well-ordering if and only if $x_i > 1$ or all i. Such an ordering is also called a global ordering.

[6]A set of polynomials $G = \{g_1, \ldots, g_s\}$ of the ideal $I \subseteq K[x_1, \ldots, x_n]_>$ is called a standard basis if it has the following property: $f \in I$ if and only if $\mathrm{NF}(f|G) = 0$. This is equivalent to the property that $L(I)$ is generated by $L(g_1), \ldots, L(g_s)$. A standard basis is a $K[x_1, \ldots, x_n]_>$–generating set of I.

Since M can be identified with the set of monomials in the commutative polynomial ring $K[\boldsymbol{x}]$, each monomial order $>$ on $K[\boldsymbol{x}]$ induces a total order on M which we again denote by $>$. It, thus, makes sense to speak of the *leading term* $\mathrm{L}(h) = \mathrm{L}_>(h)$ of a K-linear combination h of words in M.

Definition 5.1. A *G-algebra* R is the quotient of $K\langle \boldsymbol{x} \rangle$ by a two-sided ideal J_0 generated by elements of type

$$x_j x_i - c_{ij} x_i x_j - h_{ij}\,, \quad 1 \le i < j \le n\,, \tag{1}$$

where the c_{ij} are nonzero scalars in K, and where the h_{ij} are K-linear combinations of words in M. Further, we require that

(G1) $c_{ik}c_{jk}h_{ij}x_k - x_k h_{ij} + c_{jk}x_j h_{ik} - c_{ij}h_{ik}x_j + h_{jk}x_i - c_{ij}c_{ik}x_i h_{jk} = 0$ for all $1 \le i < j < k \le n$, and that

(G2) there is a global monomial order $>$ on $K[\boldsymbol{x}]$ such that $x_i x_j > \mathrm{L}(h_{ij})$ for all $i < j$.

Each global monomial order on $K[\boldsymbol{x}]$ satisfying (G2) is called an *admissible monomial order* for R.

Note that the "rewriting relations" (1) together with (G2) imply that each element of R can be represented by a K-linear combination of monomials. More precisely, M is a K-vector space basis for R, also called a Poincaré–Birkhoff–Witt basis of R.

The latter observations allow us to extend the theory of Gröbner bases for ideals and modules over polynomial rings to a theory of left (right) Gröbner bases for left (right) ideals and modules over G-algebras. Also, division with remainder (normal forms) and Buchberger's algorithm can be extended to G-algebras. And, we may compute two-sided (that is, left and right) Gröbner bases for two-sided ideals, which allows us to implement each quotient of a G-algebra by a two-sided ideal:

Definition 5.2. A *GR-algebra* A is the quotient $A = R/J$ of a G-algebra R by a two-sided ideal $J \subset R$.

Examples of G-algebras include quasi-commutative polynomial rings (for example, the quantum plane with $yx = q \cdot xy$), universal enveloping algebras of finite dimensional Lie algebras, positive (negative) parts of quantized enveloping algebras, some iterated Ore extensions, some non-standard quantum deformations, Weyl algebras and quantizations of Weyl algebras, Witten's deformation of $U(\mathfrak{sl}_2)$, Smith algebras, conformal $\mathfrak{sl}_2$–algebras, some diffusion algebras and several others. Many of them are predefined in SINGULAR.

Among the GR-algebras, one finds exterior algebras[7], Clifford algebras, finite dimensional associative algebras given by structure constants, and many more.

The implementation in SINGULAR can compute left (resp. right) normal forms and left (resp. right) Gröbner bases for left (resp. right) ideals or modules. Left (resp. right) syzygies and free resolutions can also be computed. This can be used to compute preimages of ideals under ring maps, intersection and quotients of ideals or modules. For more details see [13].

There are special libraries in SINGULAR for non–commutative applications:

- `center.lib` (central elements and centralizers of elements)
- `ncdecomp.lib` (central character decomposition of a module)
- `gkdim.lib` (Gelfand-Kirillov dimension).

[7]The library `sheafcoh.lib` contains procedures to compute the cohomology of coherent sheaves (in commutative algebraic geometry) via free resolutions over the exterior algebra, i.e. using non–commutative methods (algorithm of Eisenbud, Floystad and Schreyer).

6 Some historical remarks

The birth of SINGULAR can be dated back to about 1982, when we tried to generalize the following theorem of K. Saito:

Let $(X,0)$ be the germ of an isolated hypersurface singularity. The following conditions are equivalent.

(1) $(X,0)$ is quasi–homogeneous.[8]

(2) $\mu(X,0) = \tau(X,0)$[9]

(3) The Poincaré complex[10] of $(X,0)$ is exact.

It was conjectured that a similar theorem should hold for complete intersections. If $(X,0)$ is the germ of a curve singularity we succeeded in proving the equivalence of (1) and (2). To understand the relationship with (3) we first translated the question about exactness of the Poincaré complex into a purely algebraic question (note that the differential is only $\mathbb{C}$–linear but not $\mathcal{O}_{X,0}$–linear). Then we tried to compute examples which turned out to be rather difficult by hand. In those days there was no computer algebra system available which could compute Milnor numbers and Tjurina numbers for non–trivial examples. Such a system would have required the implementation of algorithms for computing standard bases for ideals and modules over local rings. Let us consider the following example.[11]

Let $f = xy + z^4, g = xz + y^5 + yz^2$ and $(X,0) \subset (\mathbb{C}^3, 0)$ be defined by $f = g = 0$. In this case we have the following formulas for the Milnor number and Tjurina number,

$$\begin{aligned} \mu(X,0) &= \dim_{\mathbb{C}} \mathbb{C}\,[[x,y,z]]/\langle f, M_1, M_2, M_3\rangle - \dim_{\mathbb{C}} \mathbb{C}[[x,y,z]]/\langle \tfrac{\partial f}{\partial x}, \tfrac{\partial f}{\partial y}, \tfrac{\partial f}{\partial z}\rangle, \\ \tau(X,0) &= \dim_{\mathbb{C}} \mathbb{C}[[x,y,z]]/\langle f, g, M_1, M_2, M_3\rangle, \end{aligned}$$

where M_1, M_2, M_3 are the 2–minors of the Jacobian matrix of (f,g).

In SINGULAR we can compute these numbers as follows:

```
> ring R = 0, (x,y,z), ds;    // compute in the localisation Q[x,y,z]_<x,y,z>
> poly f, g = xy+z4, xz+y5+yz2;
> ideal I = f, g;
> matrix J = jacob(I);        // Jacobian matrix
> ideal Tjur = I, minor(J,2);
> vdim(std(Tjur));            // compute K-dimension of R/Tjur
12                            // the Tjurina number is 12
```

Alternatively, we can use the built-in command `tjurina` from `sing.lib`.

```
> LIB "sing.lib";     // load the library sing.lib
> tjurina(I);
12
```

[8] $(X,0)$ is called quasi–homogeneous, if it is (analytically) isomorphic to the germ of the zero–set of a weighted homogeneous polynomial.

[9] If $(X,0)$ is defined by $f = 0, f \in \mathbb{C}\,[x_1,\ldots,x_n]$, then $\mu(X,0) = \dim_{\mathbb{C}} \mathbb{C}[[x_1,\ldots,x_n]]/\langle \frac{\partial f}{\partial x_1},\ldots,\frac{\partial f}{\partial x_n}\rangle$ is the Milnor number (a topological invariant) and $\tau(X,0) = \dim_{\mathbb{C}} \mathbb{C}[[x_1,\ldots,x_n]]/\langle f, \frac{\partial f}{\partial x_1},\ldots,\frac{\partial f}{\partial x_n}\rangle$ is the Tjurina number (the dimension of the base space of the semi–universal deformation).

[10] The Poincaré complex is defined as $0 \to \mathbb{C} \to \mathcal{O}_{X,0} \to \Omega^1_{X,0} \to \ldots \to \Omega^n_{X,0} \to 0$, with $\Omega^i_{X,0}$ the holomorphic i–differential forms on X. The maps are given by the differentials.

[11] This is one example of a non–quasihomogeneous singularity with exact Poincaré complex showing that (3) $\Rightarrow$ (1) fails for complete intersections. We discovered this with a forerunner of SINGULAR.

It is known that for quasihomogeneous complete intersections Tjurina and Milnor number coincide.
Computing the Milnor number we see that $(X,0)$ is not quasihomogeneous:

```
> milnor(I);                  // from sing.lib
13                            // the Milnor number is 13
```

However, the Poincaré complex is exact. To see this, we showed that it suffices to check that $\mu(X,0) = \dim_{\mathbb{C}} \Omega^2_{X,0} - \dim_{\mathbb{C}} \Omega^3_{X,0}$. Note that $\dim_{\mathbb{C}} \Omega^3_{X,0} = 1$. Moreover,

$$\Omega^2_{X,0} = \Omega^2_{\mathbb{C}^3,0} / \left(\langle f,g \rangle \Omega^2_{\mathbb{C}^3,0} + df \wedge \Omega^1_{\mathbb{C}^3,0} + dg \wedge \Omega^1_{\mathbb{C}^3,0} \right)$$

is isomorphic to $\mathcal{O}^3_{X,0}/M$, where $M \subset \mathcal{O}^3_{X,0}$ is generated by the six vectors

$$\left(\tfrac{\partial f}{\partial y}, \tfrac{\partial f}{\partial z}, 0\right),\ \left(\tfrac{\partial f}{\partial x}, 0, -\tfrac{\partial f}{\partial z}\right),\ \left(0, \tfrac{\partial f}{\partial x}, \tfrac{\partial f}{\partial y}\right),\ \left(\tfrac{\partial g}{\partial y}, \tfrac{\partial g}{\partial z}, 0\right),\ \left(\tfrac{\partial g}{\partial x}, 0, -\tfrac{\partial g}{\partial z}\right),\ \left(0, \tfrac{\partial g}{\partial x}, \tfrac{\partial g}{\partial y}\right):$$

```
> qring Q = std(I);       // quotient ring Q=R/I
> poly f = imap(R,f);     // map f from R to Q
> poly g = imap(R,g);
> module M = [diff(f,y),diff(f,z),0], [diff(f,x),0,-diff(f,z)],
.            [0,diff(f,x),diff(f,y)], [diff(g,y),diff(g,z),0],
.            [diff(g,x),0,-diff(g,z)],[0,diff(g,x),diff(g,y)];
> vdim(std(M));
14
```

Thus we computed $\dim_{\mathbb{C}} \Omega^2_{X,0} = 14 = \mu(X,0) + \dim_{\mathbb{C}} \Omega^3_{X,0}$ showing that the Poincaré complex is exact.

The first version of a standard basis algorithm (called `BuchMora`) was implemented in `BASIC` on a ZX–Spectrum by K.P. Neudendorf (born Schemmel) and the second author in 1983. This implementation allowed us to compute first examples. A serious development started in 1984 with an implementation of Mora's tangent cone algorithm in `Modula-2` on an Atari computer at the Humboldt-University in Berlin (by the second author and a group of students, including Hans Schönemann). After a while, a list of counter-examples to the above mentioned conjecture was produced (see [15]). At that time, the system could only compute with coefficients in a small prime field $\mathbb{F}_p$. However, the experiments showed which examples are candidates for a counter-example and how the computations in characteristic 0 should look like. The proof was then given manually.

7 A theorem in group theory

While the previous application of SINGULAR was an early example of a nowadays standard application of computer algebra, the following example is rather amazing. The problem is formulated in purely group–theoretic terms. We first translated it into a problem in algebraic respectively arithmetic geometry, where we had to show the existence of rational points on explicitly given varieties defined over finite fields. To solve the problem we had to apply the well–known Hasse–Weil formula but also sophisticated versions of the Lefschetz trace formula applied to the (square root of the) Frobenius morphism, as conjectured by Deligne and proved by Fujiwara. To apply the Hasse–Weil, respectively the Lefschetz trace formula we had to study the geometric structure of certain algebraic varieties given by explicit equations, find their irreducible components, their singular loci, etc. All this was done by using SINGULAR as an indispensable tool. The hardest part was finally to show that the varieties we ended up with were irreducible over the algebraic closure of given finite fields. But SINGULAR was not only used for these computations it was also essential in finding the correct formulation of the theorem.

As we shall see, parts of the theorem can now be proved without a computer while other parts (in particular the Suzuki groups) still require SINGULAR computations. However, since we give explicit solutions, the correctness of the statements can be verfied by simple (but lengthy) computations either by hand or (better) by any other computer algebra system.

The diversity of the methods required the collaboration of six authors from different fields (cf. [1]). The final proof may be considered as an example of the unity of mathematics in our more and more specializing discipline.

The problem in group theory was to characterize the finite solvable groups by two–variable identities (like $xy = yx$ for abelian groups) as we explain now.

If G is a group and $x,\ y \in G$, we inductively define

$$e_1(x,y) := x^{-2}y^{-1}x,\ e_{n+1}(x,y) := [xe_n(x,y)x^{-1}, ye_n(x,y)y^{-1}]$$

where the commutator of $g,\ h \in G$ is defined by $[g,h] := ghg^{-1}h^{-1}$.

The following theorem was proved by T. Bandman, F. Grunewald, B. Kunyavski, E. Plotkin and the authors [1]:

Theorem 7.1. *A finite Group G is solvable if and only if there is an $n \in \mathbb{N}$ such that $e_n(x,y) = 1$ for all $x,\ y \in G$.*

We start with the classification of the minimal finite non–solvable groups G (that is, all subgroups of G are solvable) by J. Thompson in 1968:

1. $\mathrm{PSL}(2,p)$, p a prime number, $p = 5$ or $p > 5$ and $p = \pm 2 \mod 5$.
2. $\mathrm{PSL}(2,2^n)$, $n \geq 2$, a prime number.
3. $\mathrm{PSL}(2,3^n)$, n odd, a prime number.
4. $\mathrm{PSL}(3,3)$.
5. $Sz(2^n)$, n odd.

Since it is easy to see that the finite solvable groups satisfy the proposed identity it is enough to show that for each group G in Thompson's list we have $x, y \in G$ with $e_1(x,y) = e_2(x,y)$ and $y \neq x^{-1}$. By the structure of the sequence e_n, this implies $1 \neq e_1(x,y) = e_n(x,y)$ for all n.

We shall give an idea on how to prove the theorem for the group PSL(2,q).[12] The case PSL(3,3) is easy but the case of the Suzuki groups $Sz(2^n)$ is much more difficult and we refer to the paper [1].

Proposition 7.2. *If $q = p^k$ for a prime p and $q \neq 2, 3$, then there are x, y in $PSL(2, \mathbb{F}_q)$ with $y \neq x^{-1}$ and $e_1(x,y) = e_2(x,y)$.*

The proof will use some explicit computations with the following matrices. Let $R = \mathbb{Z}$ or $\mathbb{F}_q$ and define

$$x(t) := \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix}, \quad y(b,c) := \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} \in \mathrm{SL}(2,R)$$

[12] $\mathrm{PSL}(2,\mathbb{F}_q) = \mathrm{SL}(2,\mathbb{F}_q)/\left(\{\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\} \mid a^2 = 1\right\}$, $\mathrm{PSL}(2,\mathbb{F}_5) = \mathrm{PSL}(2,\mathbb{F}_4) = A_5$.

for $t, b, c \in R$.

Let $I \subseteq \mathbb{Z}[b,c,t]$ be the ideal generated by the four entries of the matrix $e_1(x,y) - e_2(x,y)$. Using SINGULAR we can obtain I as follows:

```
>LIB"linalg.lib";
>ring R = 0,(b,c,t),dp;
>matrix X[2][2] =      t, -1,
                       1, 0;
>matrix Y[2][2] =      1, b,
                       c, 1+bc;
>matrix iX = inverse(X);
>matrix iY = inverse(Y);
>matrix M=iX*Y*iX*iY*X*X-Y*iX*iX*iY*X*iY;
>ideal I=flatten(M); I;
I[1]=b3c2t2+b2c2t3-b2c2t2-bc2t3-b3ct+b2c2t+b2ct2+2bc2t2+bct3
     +b2c2+b2ct+bc2t-bct2-c2t2-ct3-b2t+bct+c2t+ct2+2bc+c2+bt
     +2ct+c+1;
I[2]=-b3ct2-b2ct3+b2c2t+bc2t2+b3t-b2ct-2bct2-b2c+bct+c2t+ct2
      -bt-ct-b-c-1;
I[3]=b3c3t2+b2c3t3-b2c2t3-bc2t4-b3c2t+b2c3t+2b2c2t2+2bc3t2
     +2bc2t3+b2c2t+2b2ct2+bc2t2-c2t3-ct4-2b2ct+bc2t+c3t+bct2
     +2c2t2+ct3-b2c-b2t+bct+c2t +bt2+3ct2+bc-bt-b-c+1;
I[4]=-b3c2t2-b2c2t3+b2c2t2+bc2t3+b3ct-b2c2t-b2ct2-2bc2t2-bct3
     -2b2ct+c2t2+ct3+b2t-bct-c2t-ct2+b2-bt-2ct-b-t+1;
```

To prove the Proposition above, it is enough to prove the following

Lemma 7.3. *Let q be as in the Proposition, then the variety $V^{(q)} = V(I\mathbb{F}_q[b,c,t]) \subset {\mathbb{F}_q}^3$ defined by setting the four generators of I to zero is not empty.*

We apply the theorem of Hasse–Weil as generalised by Aubry and Perret to singular curves and use the fact that the affine curve C has, at most, $\deg(\overline{C})$ rational points less than the projective closure $\overline{C}$:

Theorem 7.4. *Let $C \subseteq \mathbb{A}^n$ be an absolutely irreducible affine curve defined over the finite field $\mathbb{F}_q$ and $\overline{C} \subset \mathbb{P}^n$ the projective closure, then the number of $\mathbb{F}_q$–rational points of C is at least $q + 1 - 2p_a\sqrt{q} - d$ with d the degree and p_a the arithmetic genus of $\overline{C}$.*

Note that the Hilbert function of $\overline{C}$, $H(t) = dt - p_a + 1$, can be computed from the homogeneous ideal I_h of $\overline{C}$, hence we can compute d and p_a without any knowledge about the singularities of $\overline{C}$.

Let L be the algebraic closure of $\mathbb{F}_q$. To apply the proposition, we have to prove that C is absolutely irreducible, that is, that $IL[b,c,t]$ is a prime ideal. This is already hard to compute. It turned out that the computation over the function field $L(t)$ was easier.

Lemma 7.5. *$IL(t)[b,c] = \langle f_1, f_2 \rangle$ with*

$$\begin{aligned} f_1 &= t^2b^4 - t^3(t-2)b^3 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)b^2 \\ &\quad + t^2(t^2 - 2t - 1)(t-2)b + (t^2 - 2t - 1)^2 \\ f_2 &= t(t^2 - 2t - 1)c + t^2b^3 + (-t^4 + 2t^3)b^2 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)b \\ &\quad + (t^5 - 4t^4 + 3t^3 + 2t^2)\,. \end{aligned}$$

Moreover, we have $IL[b,c,t] = \langle f_1, f_2 \rangle : h^2$, $h = t(t^2 - 2t - 1)$.

This can be tested in SINGULAR as follows

```
>ring S=(0,t),(c,b),lp;
>ideal I=imap(R,I);
>ideal J=std(I); J;
J[1]=(t2)*b4+(-t4+2t3)*b3+(-t5+3t4-2t3+2t+1)*b2+(t5-4t4+3t3+2t2)
      *b+(t4-4t3+2t2+4t+1)
J[2]=(t3-2t2-t)*c+(t2)*b3+(-t4+2t3)*b2+(-t5+3t4-2t3+2t+1)
      *b+(t5-4t4+3t3+2t2)
```

Now $IL(t)[b,c] \cap L[b,c,t] = \langle f_1, f_2 \rangle : h^2 = IL[b,c,t]$. Therefore, it is enough to prove that $IL(t)[b,c]$ is a prime ideal which is equivalent to prove that f_1 is irreducible in $L(t)[b]$. By the lemma of Gauß we have to prove that f_1 is irreducible in $L[t,b]$.

Let $P(x) := t^2 f_1(x/t)$, then

$$\begin{aligned} P(x) &= x^4 - t^2(t-2)x^3 + (-t^5+3t^4-2t^3+2t+1)x^2 + t^3(t-2)(t^2-2t-1)x \\ &\quad + t^2(t^2-2t-1)^2 \,. \end{aligned}$$

Clearly it suffices to prove that $P \in L[x,t]$ is irreducible.

To show that P is not divisible by any factor of degree 2 in x we make the following "Ansatz":

$$p = (x^2 + ax + b)\,(x^2 + gx + d), \qquad (*)$$

a, b, g, d polynomials in t with indeterminates `a(i)`, `b(i)`, `g(i)`, `d(i)` as coefficient. It is easy to see that we can assume

$$\deg(b) \le 5, \deg(a) \le 3, \deg(d) \le 3, \deg(g) \le 2\,.$$

Then a decomposition (*) with `a(i)`, `b(i)`, `g(i)`, `d(i)` $\in \overline{\mathbb{F}}_p$ does not exist if and only if the ideal `C` of the coefficients in x, t of $P - (x^2+ax+b)(x^2+gx+d)$ has no solution in $\overline{\mathbb{F}}_p$. By our characterization of Gröbner bases this is equivalent to the fact that a Gröbner basis of `C` contains $1 \in \mathbb{F}_p$.

The ideal `C` of coefficients from our Ansatz:

```
C[1]=-b(5)*d(3)
C[2]=-b(5)*g(2)
C[3]=-b(4)*d(3)-b(5)*d(2)
C[4]=-b(4)*g(2)-b(5)*g(1)-d(3)-1
C[5]=-b(3)*d(3)-b(4)*d(2)-b(5)*d(1)+1
C[6]=-b(5)-g(2)-1
C[7]=a(0)*b(5)-a(2)*d(3)-b(3)*g(2)-b(4)*g(1)-d(2)+4

⋮

C[24]=-a(0)^2*b(0)+b(0)^2-b(0)
```

For a given prime p it is easy to compute the Gröbner basis of C and to verify that $1 \in C$. However, we cannot check infinitely many primes. What we do is to use that the polynomials generating C have integer coefficients. Hence, if we can express some integer m as a polynomial combination of the generators of C where all polynomials have integer coefficients, then for any prime p, $p \nmid m$, $1 \in \mathbb{F}_p$ is contained in C (mod p).

We use the `lift` command of SINGULAR to show that (over $\mathbb{Z}$) $m = 4 \in$ `C`:

```
>matrix M=lift(C,4); M;
M[1,1]=-a(0)+8*b(0)*b(3)-8*b(0)*b(4)-16*b(0)*g(1)*g(2)-...
M[2,1]=-a(0)^2+6*a(0)*b(3)-30*a(0)*b(5)*d(1)+200*a(0)*b(5)*d(2)-...
M[3,1]=-8*b(0)*g(1)-8*b(0)*g(2)+8*b(1)*g(2)+8*b(1)-...
M[4,1]=-16*b(0)*g(2)*d(3)-18*b(0)*g(2)+8*b(0)*d(2)-8*b(0)*d(3)-...
M[5,1]=8*a(2)*b(0)+142*a(2)*d(1)*d(3)+41*a(2)*d(1)-...
M[6,1]=a(0)^2*g(2)+8*a(0)*b(0)*d(3)-6*a(0)*b(3)*g(2)+5*a(0)*b(3)+...
M[7,1]=8*b(0)*d(3)+5*b(3)-15*b(5)*d(1)+100*b(5)*d(2)-...

⋮

M[24,1]=0
```

The computation shows that

$$\binom{*}{*} \qquad 4 = \sum_{i=1}^{24} M[i,1] \cdot \texttt{C}\,[i].$$

Note that it is difficult to find the polynomials $M[i,j]$ but once they are found it is easy to check that the relation $\binom{*}{*}$ holds.

The relation $\binom{*}{*}$ implies that over $\overline{\mathbb{F}_p}$, $p \neq 2$, the polynomial P has no quadratic factor. Similarly, one can show that it has no linear factor. This implies that P is absolutely irreducible in $\mathbb{F}_p[t,x]$ for all $p \neq 2$. The case $p = 2$ can be treated by a direct computation over $\mathbb{F}_p$.

Now we can apply the theorem of Hasse–Weil to prove Lemma 7.3.

We compute the Hilbert polynomial $H(t)$ of the projective curve corresponding to I. We obtain $H(t) = 10t - 11$. The corresponding SINGULAR session is:

```
>ring S=0,(b,c,t,w),dp;
>option(contentSB);
>ideal I=imap(R,I);
>ideal J=std(I); J;
J[1]=bct-t2+2t+1
J[2]=bt3-ct3+t4-b2t+bct-c2t-2bt2+2ct2-3t3+bc+t2+t+1
J[3]=b2c2-b2ct+bc2t-bct2+b2+2bc+c2-b+c-t+2
J[4]=c2t3-ct4+c3t-2c2t2+3ct3-t4-bc2+bt2-2ct2+4t3-2bt+ct-3t2-b-2t
```

It can easily be seen that J induces a Gröbner basis in $\mathbb{F}_p[b,c,t,w]$ for all p, because `option(contentSB)` forces SINGULAR to avoid division by integers.

We homogenise J with respect to w and obtain again a Gröbner basis, cf. [10], with respect to the degree reverse lexicographical ordering. Since the leading coefficients of J have all coefficient 1 and since J and the leading ideal of J have the same Hilbert polynomial, the Hilbert polynomial is the same in any characteristic.

```
J=homog(J,w);
hilbPoly(J);
-11,10
```

From the the result we see that the degree $d = 10$ and the arithmetic genus $p_a = 12$. Using theorem 7.4, we obtain:

$$\#V^{(q)} \geq q + 1 - 24\sqrt{q} - 10.$$

This implies that $V^{(q)}$ is not empty if $q > 593$.

For the remaining prime powers q, we check directly by computer that $V^{(q)}$ is not empty.

8 Resolution of singularities

Resolution of singularities of algebraic varieties is considered to be one of the deepest theorems in algebraic geometry. It is classical for curves, has been proved by Abhyankar for surfaces (in any characteristic) and by Hironaka in general (in characteristic 0). The case of positive characteristic is, in general, still open.

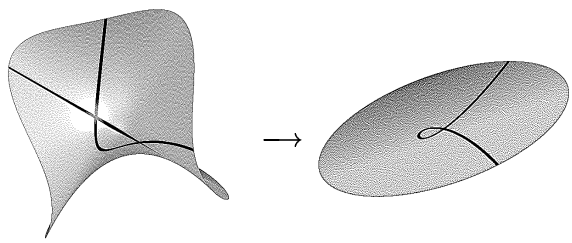
Let $V = V(f_1, \dots, f_m) \subseteq K^n$ be an affine algebraic variety and assume the ideal $\langle f_1, \dots, f_m \rangle$ is radical. The Zariski–tangent space $T_{V,p}$ of V at p is the affine subspace at p defined by the vector space

$$\{y = (y_1, \dots, y_n) \in \mathbb{C}^n \mid \sum \frac{\partial f_i}{\partial x_j}(p) y_j = 0 \text{ for all } i\}.$$

Regular points of V are points with maximal rank of the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$, i.e. points where the tangent space has the dimension of the variety V. Let us denote by $\text{Sing}(V)$ the set of singular points. In case of a hypersurface $V = V(f)$ with squarefree f, we have $\text{Sing}(V) = V\left(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f_i}{\partial x_n}\right)$.

The problem of resolution of singularities can be formulated as follows. Given a reduced algebraic variety X construct a non–singular variety X' and a proper[13] birational[14] map $\pi : X' \to X$ such that π induces an isomorphism $X' \smallsetminus \pi^{-1}(\text{Sing}(X)) \cong X \smallsetminus \text{Sing}(X)$. The first proof that the resolution of singularities in characteristic zero is always possible was given by Hironaka in 1964. Some years ago Villamayor and Encinas and independently Bierstone and Milman gave constructive proofs for this theorem leading to algorithms which we implemented in SINGULAR. With these algorithms one can compute the so–called embedded resolution. We start with a variety X embedded in a smooth n–dimensional variety W. The idea of the resolution process is to use a sequence of blowing ups.[15]

The choice of the centers in this sequence of blowing ups is the crucial point in the resolution process. The center has to be chosen in such a way that after the blowing up the singularity of the strict transform together with the configuration of exceptional divisors[16] improves. The intersection of the exceptional divisors in the process of blowing ups should be as simple as possible.[17]



The picture shows the blowing up of K^2 at 0. The result is the variety $X = \{x, y; u : v) \in K^2 \times \mathbb{P}^1 \mid xv = yu\}$ with the canonical projection $\pi : X \to K^2, \pi(x, y; u : v) = (x, y)$. On the surface X we can see the strict transform of the curve defined by $y^2 - x^2(x+1)$ and the exceptional divisor intersecting it in two points.

[13]In the classical topology *proper* means that the preimages of compact sets are compact again.

[14]The map is locally defined by rational functions and has an inverse of this type.

[15]Blowing ups are special birational maps replacing the points of a smooth subvariety (the center of the blowing up) by projective spaces. If the dimension of the variety is n and the dimension of the center is d then its points will be replaced by $\mathbb{P}^{n-d-1}$.

[16]If $\pi : W' \to W$ is the blowing up with center $C \subseteq X \subseteq W$ then $\pi^{-1}(C)$ is the exceptional divisor. The closure of $\pi^{-1}(X \smallsetminus C)$ in W' is called the strict transform of X.

[17]The exceptional divisors should have normal crossings and should also have normal crossings with the resolved variety.

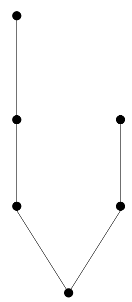
The center should be contained in the singular locus of X. The choice of the center for the next blowing up in the resolution process is guided by an invariant which is a vector of integers and locally defined at each point. The invariants at the points can be compared lexicographically and the center has to be choosen as the set of points with maximal value of the invariant. There are several possibilities to define such an invariant and every choice leads to different algorithms. The definition of such an invariant is rather complicated and includes the knowledge about the "history"of the resolution process. The invariant has values in a well-ordered set and its maximals value decreases under blowing up in the correct center which guarantees termination of the resolution process. For details and improvements see [6], [7].

As an example we compute the resolution of an isolated surface singularity:

```
>LIB"resolve.lib";              // load the resolution algorithm
>LIB"reszeta.lib";              // load its application algorithms
>LIB"resgraph.lib";             // load the graphical output routines

>ring R=0,(x,y,z),dp;           // define the ring Q[x,y,z]
>ideal I=x7+y2-z2;              // an A6 surface singularity

>list L=resolve(I);             // compute the resolution
>size(L[1]); size(L[2]);
7
13
```

The list `L` consists of two list of `L[1]` and `L[2]` which both contain a list of 7 resp. 13 rings. The first list of rings collects all information on the resolution in the 7 final charts (where the singularity is resolved). The second list collects all information on intermediate results of the resolution process. To display the tree of all the 13 charts considered in the resolution process, we may use the `Restree` command (from `resgraph.lib`). Instead, we compute the intersection form and the genera of the exceptional divisors. We do not print the intersection matrix. Instead, we use `InterDiv` from `resgraph.lib` to get a graphic visualization:

```
>list iD=intersectionDiv(L);   // compute intersection properties
>iD[2];                        // genera of exceptional divisors
0,0,0,0,0,0

>InterDiv(iD[1]);              // draw dual graph of resolution
```



In the diagram, each filled circle corresponds to an exceptional divisor with self intersection -2. Otherwise, the self intersection is displayed. The circles are joined by a line iff the corresponding exceptional divisors meet.

Next, we compute the Denef-Loeser zeta function, which codes a lot of information of the resolution:

```
>zetaDL(L,1);
[1]:
   (s+8)/(7s2+15s+8)
```

9 SINGULAR and general relativity

Let us now describe an application of SINGULAR to a problem in general realtivity.

We are interested in constructing stationary axisymmetric solutions to the Einstein equations for a vacuum gravitational field.

A standard method proceeds by reducing them to a two dimensional nonlinear equation, the *Ernst equation* (cf. [4])

$$(\mathrm{Re}\mathcal{E})(\mathcal{E}_{,\rho\rho}+\mathcal{E}_{,\zeta\zeta}+\frac{1}{\rho}\mathcal{E}_{,\rho})=\mathcal{E}_{,\rho}^{2}+\mathcal{E}_{,\zeta}^{2} \tag{1}$$

for the complex valued function $\mathcal{E}(\rho,\zeta)=f(\rho,\zeta)+ib(\rho,\zeta)$, with $f=\mathrm{Re}\mathcal{E}$ the real part and $b=\mathrm{Im}\mathcal{E}$ the imaginary part of $\mathcal{E}$, and commas denoting partial derivation.

Equation (1) can be rewritten as

$$\begin{aligned} f\Delta f &= |Df|^2-|Db|^2 \\ f\Delta b &= 2(Df,Db) \end{aligned} \tag{2}$$

Here Δ is the Laplace operator of the flat metric $g=d\rho^2+\rho^2 d\varphi^2+d\zeta^2$ where ρ,ζ and φ are cylindrical coordinates on $\mathbb{R}^3$ and the above functions are independent of φ. Similarly $(,)$ denotes the g–sealer product and $|\ |$ the g–norm.

Equations (2) are singular at

$$E_f=\{(\rho,\zeta)\mid f(\rho,\zeta)=0,\rho>0\}$$

which is called the $\mathcal{E}$*–ergosurface*[18].

Assuming smoothness of f and b in a neighbourhood of E_f, the problem arises whether the solution of (2) produces a smooth space–time metric. Since examples are known where the metric is singular there and others where it is smooth, one would like to derive necessary and sufficent conditions of smoothness of the space–time metric near E_f.

In [4] the following is proved:

Theorem 9.1. *Consider a smooth solution $f+ib$ of (1) such that f has no zeroes of infinite order at E_f. Then there is a neighbourhood of E_f on which the space–time metric obtained by solving (2) is smooth and has Lorentzian signature.*

Let us explain how SINGULAR came into play in proving this result.

It was shown before by Chrusciel, Meinel and Szybka that first or second order zeroes of f at $(\rho_0,\zeta_0)\in E_f$ always lead to a smooth space–time metric. This would prove the theorem, provided that higher order zeroes of f do not exist.

[18] Because (1) degenerates at E_f there is no reason to expect smoothness of f there itself. However, large classes of explicit solutions are known, where f can be extended analytically across E_f and the discussions here is concerned with these solutions.

The reason why this might be true is the following. Consider the Taylor expansion of $\mathcal{E}$ at (ρ_0, ζ_0) and assume without loss of generality that $\mathcal{E}(\rho_0, \zeta_0) = 0$. Let $\mathcal{E}_k$ be the tangent cone of $\mathcal{E}$ at (ρ_0, ζ_0), that is, the homogeneous polynomial in $(\rho - \rho_0, \zeta - \zeta_0)$ of degree k consisting of the non–vanishing terms of lowest order of the Taylor expansion of $\mathcal{E}$ at (ρ_0, ζ_0). Since $\mathcal{E}_k$ is homogeneous of degree k in 2 variables its real resp. imaginary part f resp. b depend both on $k+1$ free parameters. If one inserts $\mathcal{E}_k$ in (1) and truncates the resulting equation at the lowest non–vanishing order one obtains a homogeneous polynomial W_k of degree $2k-2$ whose vanishing is a necessary condition for $\mathcal{E}$ to solve (1). The real and imaginary part of W_k are a linear combination of $2k-1$ monomials[19] and their vanishing imposes hence $2(2k-1)$ quadratic condition on the $2(2k+1)$ free parameters of $\mathcal{E}_k$.

For $k \geq 3$ we have more equations than variables and the optimistic guess was that this system has no (non–trivial) solutions. This would imply the non–existence of higher order zeroes of f and hence the theorem.

The first insight, provided by SINGULAR was to show that the equations $W_k = 0$ are *not independent* for $k = 3, 4, 5$.

During the Oberwolfach meeting "Mathematical Aspects of General Relativity", January 8-14, 2006, Piotr Chrusciel mentioned the problem to the first author of this article. He also mentioned that they had been able to find solutions of $W_k = 0$ for $k = 2$ using Maple. But they were unable to settle the case $k = 3$ or higher using the widely available commercial computer algebra programmes; the problem was too complicated to be handled by those systems via direct implementations.

Of course, this was a challenge for SINGULAR. Taylorizing f and b at $\rho_0 + i\zeta_0$ up to order k, we get with $x = \rho - \rho_0, y = \zeta - \zeta_0$

$$f = \sum_{i=0}^{k} a_i x^{k-i} y^i \ , \ b = \sum_{i=0}^{k} b_i x^{k-i} y^i,$$

where a_i, b_i are indeterminates.

It is now easy to set up the truncated equations for (2) and to create, for a given k, the system of $4k-2$ equations $W_k = 0$, depending on the variables $a_0, \ldots, a_k, b_0, \ldots, b_k$, coded in the ideal W:

```
>int k=3;
>ring R = 0,(a(0..k),b(0..k),y,x),dp;

>poly f,b;
>int i;
>for (i=0; i<=k; i++)
>{
>  f = f + a(i)*x^(k-i)*y^(i);
>  b = b + b(i)*x^(k-i)*y^(i);
>}

>poly Lf = diff(diff(f,x),x)+diff(diff(f,y),y); //Laplacian of f
>poly Lb = diff(diff(b,x),x)+diff(diff(b,y),y);
>poly Df = diff(f,x)^2 + diff(f,y)^2;
>poly Db = diff(b,x)^2 + diff(b,y)^2;
>poly fb = diff(f,x)*diff(b,x)+ diff(f,y)*diff(b,y);
```

[19]Note, that the complex valued function $\mathcal{E}(\rho, \zeta)$ depends on the two real variables ρ, ζ, i.e. W_k is a homogeneous polynomial in two variables of degree $2k-2$.

```
>poly Eq1 = f*Lf - Df + Db;          //truncated equations (2) to solve
>poly Eq2 = f*Lb - 2*fb;

>matrix co = coef(Eq1,xy);
>ideal W = co[2,1..2*k-1];
>co = coef(Eq2,xy);
>W = W, ideal(co[2,1..2*k-1]);       //conditions on the coefficients of (2)

>ring S = 0,(a(0..k),b(0..k)),dp;
>ideal W = imap(R,W);
>dim (groebner(W));
```

For $k = 3$, the command `dim(groebner (W));` returns 2, hence there is a 1–dimensional projective variety of nontrivial *complex* solutions of $W_k = 0$. As a_i resp. b_i are the coefficient of the real resp. the imaginary part of ζ, we are looking for *real* solutions of $W_k = 0$ which are not all zero. The Gröbner basis itself consists of 46 generators for $k = 3$ and does not give any insight in the structure on the solution set. Since the solution set has positive dimension numerical solving is not appropriate - we need "symbolic solving". The breakthrough came by decomposing $W_k = 0$ into irreducible components. The SINGULAR command `primdecGTZ(W)`, returned (in a few seconds) for $k = 3, 4$ ideals of the different components of $W_k = 0$ which could be interpreted easily.

```
>LIB "primdec.lib";
>list mpr = minAssGTZ(W);
>mpr;
[1]:                              [2]:
   _[1]=a(2)^2+a(3)^2                _[1]=b(2)^2+9*b(3)^2
   _[2]=b(3)                         _[2]=b(1)+3*b(3)
   _[3]=b(2)                         _[3]=3*b(0)+b(2)
   _[4]=b(1)                         _[4]=-a(3)*b(2)+a(2)*b(3)
   _[5]=b(0)                         _[5]=a(2)*b(2)+9*a(3)*b(3)
   _[6]=a(1)-a(3)                    _[6]=a(2)^2+9*a(3)^2
   _[7]=a(0)-a(2)                    _[7]=a(1)+3*a(3)
                                     _[8]=3*a(0)+a(2)

[3]:                              [4]:
   _[1]=3*a(3)+b(2)                  _[1]=3*a(3)-b(2)
   _[2]=a(2)-3*b(3)                  _[2]=a(2)+3*b(3)
   _[3]=b(1)+3*b(3)                  _[3]=b(1)+3*b(3)
   _[4]=3*b(0)+b(2)                  _[4]=3*b(0)+b(2)
   _[5]=a(1)+3*a(3)                  _[5]=a(1)+3*a(3)
   _[6]=3*a(0)+a(2)                  _[6]=3*a(0)+a(2)
```

We see that the equations [1] and [2] have only trivial real solutions. However, [4] resp. [3] provide non–trivial real solutions. These are of the form

$$f + ib = \alpha w^3 \quad \text{resp. } f + ib = \alpha \overline{w}^3$$

with $\alpha = a_0 + ib_0, w = x + iy$, as can be easily checked.

The solutions $\mathcal{E}_k$ of the equations W_k found by SINGULAR belong to the general family

$$\mathcal{E}_k = \alpha(z - z_0)^k, \tag{5}$$

where $\alpha \in \mathbb{C}$, with $z = \rho + i\zeta$ (or to the complex conjugate family). It is straightforward, using the Cauchy–Riemann equations, to check that functions of this form satisfy (2) and hence (1), for all $k \in \mathbb{N}$. Thus, this second insight provided by SINGULAR led us to discover a solution of the leading order equations for all k. Moreover SINGULAR showed that (5) and its complex conjugate are all solutions with $b \neq 0$ for small k which could then be proved analytically for all k.

One can show that higher order zeros of $\mathcal{E}$ with a leading order Taylor polynomial (3) *do lead* to a space–time metric which is *indeed smooth* across E_f, thus proving the theorem.

10 Curves and Surfaces with many Singularities

We describe now a typical example how SINGULAR was used to support research in algebraic geometry by creating interesting examples.

Let $X \subset \mathbb{P}^n_{\mathbb{C}}$ be a projective hypersurface being the zero set of $f(z_0, \ldots, z_n) \in \mathbb{C}[z_0, \ldots, z_n]$, a homogeneous polynomial of degree $d > 0$. It follows from Bezout's theorem that X cannot have too complicated or too many singularities with respect to d, thus combining local and global properties. Bezout's theorem says that if the intersection of n hypersurfaces in $\mathbb{P}^n$ consist of finitely many points then the number of intersection points (counted with appropriate multiplicities) is equal to the product of the degrees of the hypersurfaces.

In particular, if p is a singular point of X and if L is a line in general position then the intersection number of X and L at p is equal to the multiplicity mult (X, p), the order of the Taylor expansion of f at p. In particular X cannot have any singularity of multiplicity bigger than its degree, which shows that each individual singularity on X cannot be too complicated. To get an estimate for the number of singularities we can use another local invariant, the Milnor number $\mu(X,p) = \dim_{\mathbb{C}} \mathbb{C}\,[[x_1, \ldots, x_n]]\,/\langle \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \rangle$ if $x_1, \ldots, x_n$ are local coordiantes with center p and $f = 0$ a local analytic equation of X at p. If we assume that X has only isolated singularities, then $\mu(X,p) < \infty$ for all $p \in X$ and, by choosing general projective coordinates, we may assume that no singularity of X lies on $\{z_0 = 0\}$. Considering the intersection of the hypersurfaces $\frac{\partial f}{\partial z_i} = 0, i = 1, \ldots, n$, we obtain from Bezout's theorem

$$(d-1)^n \geq \sum_{p \in \mathrm{Sing}(X)} \mu(X,p). \qquad (*)$$

Since $\mu(X,p) = 0$ if p is nonsingular and $\mu(X,p) = 1$ iff p is a node[20] we get that the number of singularities of X is bounded by $d^n + O(d^{n-1})$ and that the number of non–nodes is bounded by $\frac{1}{2}d^n + O(d^{n-1})$. Of course, this bound is very coarse and better bounds have been given, e.g. by using the semi–continuity of the singularity spectrum by Varchenko. These bounds concern the coefficient of d^n but not the asymptotic $O(d^n)$ if d goes to infinity.

[20]An A_k–singularity has the local analytic equation $x_1^2 + \cdots + x_n^{k+1} = 0$. A_1–singularities are calles *nodes*, A_2-singularities *cusps*.

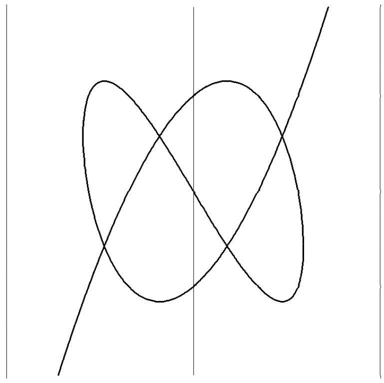


Figure 1: A 4–nodal plane curve of degree 5, with equation $x^5 - \frac{5}{3}x^3 + \frac{5}{16}x - \frac{1}{4}y^3 + \frac{3}{16}y = 0$, which is a deformation of E_8 : $x^5 - y^3 = 0$.

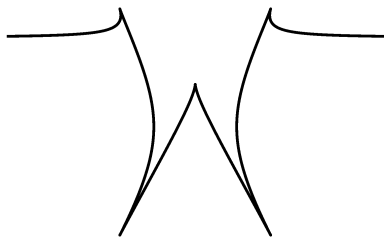


Figure 2: A plane curve of degree 5 with 5 cusps, the maximal possible number. The equation is $\frac{129}{8}x^4y - \frac{85}{8}x^2y^3\frac{57}{32}y^5 - 20x^4 - \frac{21}{4}x^2y^2\frac{33}{8}y^4 - 12x^2y + \frac{73}{8}y^3 + 32x^2 = 0$.

On the other hand, from the very beginning of algebraic geometry, the existence of hypersurfaces with many singularities has been a problem of constant importance and interest, from Descartes, Pascal, Newton over Plücker and Severi to Zariski and Harris until nowadays. Except for the simplest case, the number of nodes on a plane curve settled by Severi in 1921, no general answer is known. The problem turned out to be extremely hard and the partial results so far suggest that a generel condition for the existence of singularities of a given type which is necessary and sufficient at the same time cannot be expected for more complicated singularities than nodes.

Two directions of research have been established in this connection: (I) to find sufficient existence conditions which are proper (i.e. have the asymptotic $\alpha d^n + O(d^{n-1})$ with a constant α which is not necesarily optimal) or (II) to find necessary and sufficient conditions for small d and the simplest singularities like nodes and cusps[20](cf. Fig. 1 and Fig. 2).

Let us first consider (I). The first general asymptotic proper conditions for the existence were found only in 1989 in [8] in the case of plane curves. The coefficient α has been improved subsequently (cf. the forthcoming book [9]) in particular if we ask for the maximum μ such that a plane curve of degree d has a single singularity with Milnor number μ. The precise answer to this question is still unknown but we know (cf.[9]) that $\mu \geq d^2/2 + O(d)$.

This result is just an existence statement, the proof gives no hint how to produce any equation. Having a method for constructing curves of low degree with many singularities, Lossen was able to produce explicit equations. In order to check his construction and improve the results, he made extensive use of SINGULAR to compute standard bases for global as well as for local orderings. One of his examples is the following:

Example: The irreducible curve C with affine equation $f(x,y) = 0$,

$$\begin{aligned} f(x,y) = y^2 - 2y(x^{10} &+ \frac{1}{2}x^9y^2 - \frac{1}{8}x^8y^4 + \frac{1}{16}x^7y^6 - \frac{5}{128}x^6y^8 + \frac{7}{256}x^5y^{10} \\ &- \frac{21}{1024}x^4y^{12} + \frac{33}{2048}x^3y^{14} - \frac{429}{32768}x^2y^{16} + \frac{715}{65536}xy^{18} \\ &- \frac{2431}{262144}y^{20}) + x^{20} + x^{19}y^2 \end{aligned}$$

has degree 21 and an A_{228}–singularity ($x^2 - y^{229} = 0$) as its only singularity.

In order to verify this, one may proceed, using SINGULAR, as follows:

```
>ring s = 0,(x,y),ds;
>poly f = y2-2x10y-x9y3+1/4x8y5-1/8x7y7+5/64x6y9-7/128x5y11+21/512x4y13
        -33/1024x3y15+429/16384x2y17+x20-715/32768xy19+x19y2+2431/131072y21;
>matrix Hess = jacob(jacob(f));          //the Hessian matrix of f
>print(subst(subst(Hess,x,0),y,0));      //the Hessian matrix for x=y=0
0,0,
0,2
>vdim(std(jacob(f)));                    //the Milnor number of f
228
```

Since the rank of the Hessian at 0 is 1, f has an A_k singularity at 0; it is an A_{228} singularity since the Milnor number is 228. To show that the projective curve C defined by f has no other singularities, we have to show that C has no further singularities in the affine part and no singularity at infinity. The second assertion is easy, the first follows from

$$\dim_{\mathbb{C}}(K[x,y]_{\langle x,y\rangle}/\langle \text{jacob}(f), f\rangle = \dim_{\mathbb{C}}(K[x,y]/\langle \text{jacob}(f), f\rangle,$$

confirmed by SINGULAR:

```
>vdim(std(jacob(f)+f));
228                    //multiplicity of Sing(C) at 0  (local ordering)
>ring r = 0,(x,y),dp;
>poly f = fetch(s,f);
>vdim(std(jacob(f)+f));
228                    //total multiplicity of Sing(C) (global ordering)
```

The existence problem (II) for hypersurfaces in $\mathbb{P}^3$ of low degree with specific singularities (such as nodes) has attracted attention of many researchers. Let $m(d)$ denote the maximum number of nodes on a surface X of degree d in $\mathbb{P}^3_{\mathbb{C}}$. It is known that $m(d) = 1, 4, 16, 31, 65$ for $d = 2, 3, 4, 5, 6$ but for $d \geq 7$ we only know $\frac{5}{12}d^3 \leq m(d) \leq \frac{4}{9}d^3$ up to $O(d^2)$, but the exact value of $m(d)$ is unknown. Note that the lower bounds are obtained in each case by a specific construction, due to Schläfli, Kummer, Togliatti, Chmutov and Barth. In 2004 O. Labs constructed a surface of degree 7 with 99 nodes which is the current world record for surfaces of degree 7 (but which is still smaller than the known upper bound 104).

The construction of Labs is a very instructive example on how geometric reasoning with computer experiments over finite fields of small characteristic can be used to support research in algebraic geometry.

The arguments of Labs can be roughly summarized as follows. Inspired by previous work of Barth and Endraß, Labs considers a 6–parameter family $S_{a_1,\ldots,a_6} \in \mathbb{Z}[x,y,z]$ of homogeneous polynomials of degree 7, and the aim was to construct explicit algebraic numbers $a_1, \ldots, a_6$ such that $S_{a_1,\ldots,a_6}$ defines a nodal surface having more than the previously known 93 nodes. Computer experiments with SINGULAR over small prime fields suggested that the maximum number of nodes on $S_{a_1,\ldots,a_6}$ is 99 and that such examples should exist for $a_6 = 1$. Using the symmetry of the family $S = S_{a_1,\ldots,a_5,1}$, it is sufficient to consider the plane curve defined by $S_y := S|_{y=0}$ and find parameters $\alpha_1, \ldots, \alpha_5$ such that S_y has many nodes (from which the number of nodes on S can be computed).

Of course, to work in the plane $y = 0$ allows much faster computations. By running SINGULAR computations over all possible parameter combinations for small prime fields $\mathbb{F}_p (11 \leq p \leq 53)$ he finds some 99–nodal surfaces over these fields. To find conditions for the parameters, Labs used geometric properties of the plane curve S_y together with extensive SINGULAR computations such as elimination and factorization (for details see [12]). He ended up with $a_1, \ldots, a_5$ being polynomial expression in $\alpha \in \mathbb{C}$, $7\alpha^3 + 7\alpha + 1 = 0$, such that the resulting polynomial S_α defines a surface with exactly 99 nodes over several prime fields.

It turns out that the same conditions give a 99–nodal septic surface in characteristic 0 which can be proved by a straightforward computations with SINGULAR. The following surface in $\mathbb{P}^3(\mathbb{C})$ of degree 7 with equation $S_\alpha = P - U_\alpha$ has exactly 99 nodes and no other singularities, where

$$\begin{aligned}
P: &= x\cdot\left[x^6 - 3\cdot 7\cdot x^4y^2 + 5\cdot 7\cdot x^2y^4 - 7\cdot y^6\right] \\
&\quad +7\cdot z\cdot\left[\left(x^2+y^2\right)^3 - 2^3\cdot z^2\cdot\left(x^2+y^2\right)^2 + 2^4\cdot z^4\cdot\left(x^2+y^2\right)\right] - 2^6\cdot z^7, \\
U_\alpha: &= (z + a_5 w)\left((z+w)(x^2+y^2) + a_1 z^3 + a_2 z^2 w + a_3 z w^2 + a_4 w^3\right)^2, \\
a_1 &= -\tfrac{12}{7}\alpha^2 - \tfrac{384}{49}\alpha - \tfrac{8}{7}, \qquad a_4 = -\tfrac{8}{7}\alpha^2 + \tfrac{8}{49}\alpha - \tfrac{8}{7}, \\
a_2 &= -\tfrac{32}{7}\alpha^2 + \tfrac{24}{49}\alpha - 4, \qquad a_5 = 49\alpha^2 - 7\alpha + 50. \\
a_3 &= -4\alpha^2 + \tfrac{24}{49}\alpha - 4,
\end{aligned}$$

Note that $7\alpha^3 + 7\alpha + 1 = 0$ has one real solution $\approx -0,14010685$ and for this value all 99 nodes of S_α are real, which allows to draw a nice picture of S_α (Fig. 3).

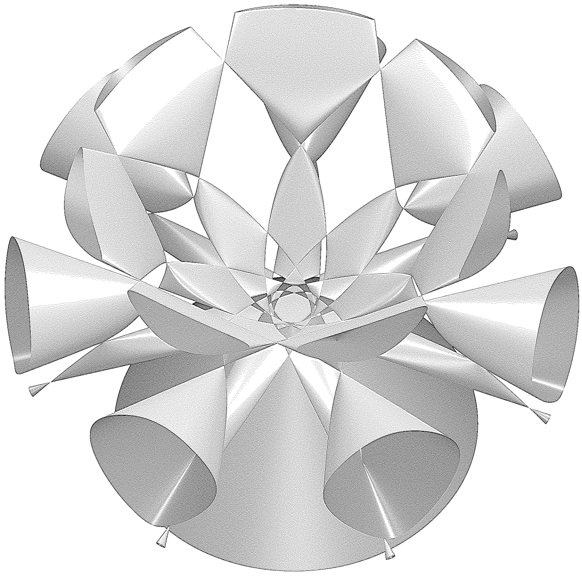


Figure 3: Lab's 99–nodal septic

The following SINGULAR code verifies that Lab's septic has indeed 99 nodes and no other singularities.

```
>LIB "all.lib";

>ring r = (0,alpha), (x,y,w,z), dp;
>minpoly = 7*alpha^3 + 7*alpha + 1;
```

```
>poly a(1) = -12/7*alpha^2 - 384/49*alpha - 8/7;
>poly a(2) = -32/7*alpha^2  + 24/49*alpha - 4;
>poly a(3) =    -4*alpha^2  + 24/49*alpha - 4;
>poly a(4) =  -8/7*alpha^2   + 8/49*alpha - 8/7;
>poly a(5) =    49*alpha^2      - 7*alpha + 50;

>poly P = x*(x^6-3*7*x^4*y^2+5*7*x^2*y^4-7*y^6)
         + 7*z*((x^2+y^2)^3-2^3*z^2*(x^2+y^2)^2+2^4*z^4*(x^2+y^2)) - 2^6*z^7;
>poly C = a(1)*z^3+a(2)*z^2*w+a(3)*z*w^2+a(4)*w^3+(z+w)*(x^2+y^2);
>poly U = (z+a(5)*w)*C^2;
>poly S = P-U;
```

The following computation verifies that the total Tjurina number of S_α is 99 and that all singularities are ordinary double points, using the Hessian criterion. We check the total Tjurina number of the projective surface:

```
>ideal sl = jacob(S);                //the singular locus of S
>ideal newsl = groebner(sl);         //a groebner basis
>dim(newsl)-1;                       //dimension of the projective variety.
2
>mult(newsl);                        //total tjurina number
99
```

Check now that all singularities are ordinary double points:

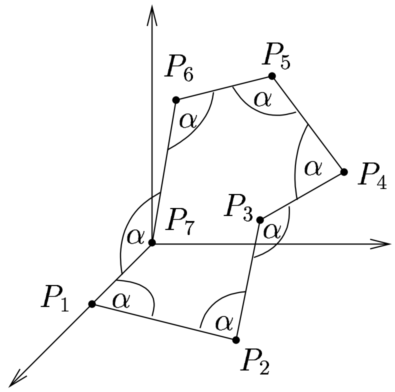
```
>matrix mHS = jacob(jacob(S));
>ideal nonnodes = minor(mHS,2), sl;  //the ideal of non-nodes
>nonnodes = groebner(nonnodes);
>dim(nonnodes);
0
```

Since the dimension is zero, the projective dimension of nonnodes is -1, that is, there are no non-nodes.

11 Applications outside Mathematics

Gröbner basis techniques and multivariate factorization methods can be applied whenever a problem can be expressed in terms of polynomial equalities and inequalities and Singular has been used to solve a variety of such problems from outside mathematics. It should be stressed, however, that quite often the hardes part is not the computation but the "modelling", that is, the proper formulation which makes the computation possible.

First we want to describe an application which came from robotics resp. chemistry and was communicated to us by Levelt in 1996.



Consider the picture above of the heptagon in 3–space. Let $a_i = \overrightarrow{P_i P_{i+1}}$ for $i \leq 6$ and $a_7 = \overrightarrow{P_7 P_1}$. Assume that all vectors have length 1 and that the angels between them are the same. This can be expressed by the following equations (where c is a parameter):

(1) $(a_1, a_2) = (a_2, a_3) = \ldots = (a_7, a_1) = c = \cos(\alpha)$

(2) $(a_1, a_1) = (a_2, a_2) = \ldots = (a_7, a_7) = 1$

(3) $a_1 + a_2 + \ldots + a_7 = 0$.

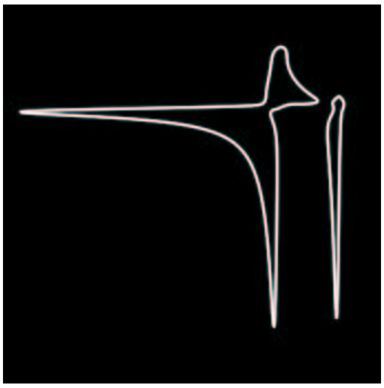
Different values of c lead to different applications. For $c = 0$ the equations describe the configuration space of a robot and for $c = \frac{1}{3}$ the configuration space of a molecule. The question was to find out the degree of freedom of the heptagon. Can it move in 3–space (a_7 fixed)? For $c = \frac{1}{3}$ one obtains after several simplifications the following system of equations:

```
>ring R=0,(v,w,x,y,z,t),dp;
>ideal I= 81y2z2-54wyz+54y2z+54yz2-72w2+198wy-207y2+198wz-225yz-207z2+114w-141y-141z+10,
81w2x2+54w2x+54wx2-54wxz-207w2-225wx-207x2+198wz+198xz-72z2-141w-141x+114z+10,
324vw2x+432vw2+540vwx+432w2x-432wxy-432vwz+324wyz+180vw+846w2-576vx+180wx-306wy+144xy
   +144vz-306wz-36yz+12v+585w+12x-318y-318z-79,
81v2w2+54v2w+54vw2-54vwy-207v2-225vw-207w2+198vy+198wy-72y2-141v-141w+114y+10;
```

Computing a Gröbner basis it is easy to see that the equations describe a curve in 5–space. One question (of Levelt) was to compute the projection to the w, x–plane. The result is the following polynomial of degree 36:

```
1334309862964227464374150 5w20x16+18458805154059402163602552w20x15
+12528539096440613433050772w19x16-30746954363668257130849879 2w20x14
-30874508927355581181051418 8w19x15-33577046978930597852363651 4w18x16
                          .
                          .
                          .
-576037223947325427883968750 00w2x-562097034857559173822718750 00wx2
-29459059311819369252628125000x3-34563868786388679774687500 00w2
-38806507749291062943750000 0wx-35009556055943665474687500 00x2
+12640978440323069725000000 00w+11265787052659087725000000 00x
+24065849284119685000000000 0
```

Several years ago it was a difficult task to compute the elimination and took several hours. If we plot (using `surf.lib`) the result, we see the curve of possible w, x–coordinates of the molecule in 5–space. In particular, the heptagon can move and the configuration space has at least two connected components:



We just want to mention some other applications:[21]

- sizing analog electronic circuits
- formal verifications of digital electronic circuits[22]
- coding theory (*AG*–Codes which use algebraic curves over finite fields and vector spaces given by divisors on these curves for coding)[23]
- glass melting
- modelling in economy (here, as quite often, the problem is to find all positive real roots of a given system of polynomial equations).
- medicine

References

[1] T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskii, G. Pfister, E. Plotkin: Engel-Like Identities Characterizing Finite Solvable Groups. Preprint, http://arXiv.org/abs/math.GR/0303165, (2003). To be published in Compos. Math. (2006).

[2] Bandman, T.; Greuel, G.-M.; Grunewald, F.; Kunyavskii, B.; Pfister, G.; Plotkin, E.: Two-variable identities for finite solvable groups. *Comptes Rendus de l'academie des sciences, Ser. I*, **337**, 581–586 (2003).

[3] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD Thesis, University of Innsbruck, Austria (1965).

[4] Chrusciel, P; Greuel, G.-M.; Meinel, R.; S. Szybka: The Ernst equation and ergosurfaces. Preprint, http://arxiv.org/abs/gr-qc/0603041, (2006), 1-23.

[21] `http://www.singular.uni-kl.de/DEMOS/GP-MEGA-03/HTML/applications.html`

[22] Boolean functions are modelling the in– and output behaviour of electronic circuits. A Boolean function is a map $F : (\mathbb{Z}/2)^n \to \mathbb{Z}/2$ and can be represented (not uniquely) as a polynomial in $\mathbb{Z}/2[x_1, \ldots, x_n]$. It is unique in the so–called Boolean ring $\mathbb{Z}/2[x_1, \ldots, x_n]/\langle x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle$. The model leads to the problem to decide whether a given system of Boolean functions $f_1 = \cdots = f_k = 0$ has a solution. This is not the case if a minimal Gröbner basis is $\{1\}$.

[23] This is implemented in the SINGULAR library `brnoeth.lib`.

[5] Decker, W.; Lossen, C.: *Computing in Algebraic Geometry. A Quick Start using* SINGULAR. Springer-Verlag, 2006.

[6] Frühbis–Krüger, A., Pfister, G.: Auflösung von Singularitäten, DMV-Mitteilungen 13-2 (2005), 89-105

[7] Frühbis–Krüger, A., Pfister, G.: Algorithmic Resolution of Singularities, In: C. Lossen, G. Pfister: Singularities and Computer Algebra. LMS Lecture Notes 324, Cambridge University Press 157-184 (2006)

[8] G.-M. Greuel, Ch. Lossen, E. Shustin: Plane curves of minimal degree with prescribed singularities. Invent. Math. 133 (1998), 539-580.

[9] G.-M. Greuel, Ch. Lossen, E. Shustin: Singular Algebraic Curves. Monograph to appear. Springer–Verlag.

[10] Greuel, G.-M.; Pfister, G.: *A* SINGULAR *introduction to commutative algebra.* Springer-Verlag, 2002.

[11] Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 3.0. A Computer Algebra System for Polynomial Computations. ZCA, TU Kaiserslautern (2005). `http://www.singular.uni-kl.de`.

[12] Labs, O.: A Septic with 99 real Nodes, arXiv:math.A6/0409348

[13] Levandovskyy, V.: Non-Commutative Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications and Implementations. Kaiserslautern, 2005.

[14] Lossen, C; Pfister, G. (Eds.): *Singularities and Computer Algebra*, LMS Lecture Notes 324, Cambridge University Press (2006).

[15] Pfister, G.; Schönemann, H.: Singularities with exact Poincaré complex but not quasihomogeneous. *Revista Mathematica Madrid*, **2**, 161–171 (1989).