CASA: A Computer Algebra Package for Constructive Algebraic Geometry *

R. Gebauer, M. Kalkbrener, B. Wall, F. Winkler
RISC-Linz, Johannes Kepler Universität
A-4040 Linz, Austria

Abstract

The program package CASA is designed to enhance the power of a traditional computer algebra system by adding programs for constructive algebraic geometry. The objects that CASA works with are algebraic sets in affine or projective spaces over a field. The geometric objects may be given in various different representations. CASA is able to analyse properties of algebraic sets, such as to compute their dimensions, compute their irreducible components, determine singular points, determine intersection properties and the like. The user can also create 2- and 3-dimensional pictures of curves and surfaces.

1 Introduction

CASA (Computer Algebra Software for Algebraic geometry) is designed to enhance the power of a traditional computer algebra system by adding a package of programs for constructive algebraic geometry. As the underlying computer algebra system we have chosen Maple 4.3, because it is widely available and relatively comfortable to program in. Actually, CASA is not a finished product. We have started working on CASA about a year ago and many of the features we envision for CASA have not been implemented yet. So this paper reports on work in progress.

Computer algebra systems are very powerful tools for calculating with polynomials, rational functions, and the like (among other domains). Algebraic geometry is the theory of geometric objects that can be described as the solutions of sets of polynomial equations. In the last few decades the research interest in algebraic geometry has shifted from constructive aspects to non-constructive investigations. Now, however, that computer algebra systems have been around for quite some time, it seems natural to apply them for actually constructing objects and deciding statements in algebraic geometry. This is the goal of the CASA project. For related work we refer to [BR90], [Ben90], [SSB89].

Some of the applications of CASA are computing the singularities of curves and surfaces, determining topological pictures of algebraic sets, expanding algebraic curves in power series, computing the intersection of algebraic curves and surfaces, applying various transformations to algebraic sets, determining the dimension, decomposing into irreducible components, calculating in the coordinate ring of an algebraic set, computing with functions defined on an algebraic set. The CASA system works with algebraic sets in various different representations. So an important feature of the system is the ability to change from one representation into another.

Applications include geometric modeling with algebraic curves and surfaces, and any problem domain which needs solutions of algebraic equations. For instance, problems in quantum physics have been solved successfully by using CASA (see [KHSH90]).

2 Definitions and Notations

Let K be a finitely generated field extension of the rational numbers.

For a given subset F of $K[x_1, \ldots, x_n]$, $Ideal(F)$ denotes the ideal in $K[x_1, \ldots, x_n]$ generated by F and $V(F)$ denotes the algebraic set of F, i.e. the set

$$\{a \in \mathbb{C}^n \mid f(a) = 0 \text{ for every } f \in F\}.$$

*The work reported herein has been supported by the *Austrian Fonds zur Förderung der wissenschaftlichen Forschung* under Project Nr. P6763

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.
© 1991 ACM 0-89791-437-6/91/0006/0403...$1.50

An algebraic set V is irreducible if it cannot be written as the union of two non-empty proper algebraic subsets of V.

Theoretically all computations could be carried out in $\bar{K}$. However, some of the algorithms in Maple 4.3 (e.g. Gröbner bases) do not work for polynomials with coefficients in an algebraic extension field. This puts a restriction on the input class of some of our algorithms. We expect that these problems will be solved in a new version of Maple.

3 Data Structures

In CASA an algebraic set is specified by three items: the representation of the algebraic set, a variable list and a table of attributes. There are four different kinds of representations. The algebraic set can be given in implicit, parametric or projected form or as a set of places (a more detailed description is provided at the end of this section). The variable list is used to distinguish between variables and parameters. The table of attributes contains properties of the algebraic set, like the dimension or a list of independent variables. These attributes are queried by some of the algorithms to avoid duplicate computations. In the sequel the different types of representations are described.

Implicit Form: A representation in implicit form consists of a list of polynomials $f_1, \ldots, f_k$ over K in the variables $x_1, \ldots, x_n$ specified in the variable list. The algebraic set defined by these polynomials is

$$V(\{f_1, \ldots, f_k\}).$$

Parametric Form: A representation in parametric form consists of a list of rational functions $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ over K in the variables $t_1, \ldots, t_k$ specified in the variable list. The algebraic set defined by this parametrization is

$$V(\{g \in K[x_1, \ldots, x_n] \mid \\ g(\tfrac{p_1(t_1,\ldots,t_k)}{q_1(t_1,\ldots,t_k)}, \ldots, \tfrac{p_n(t_1,\ldots,t_k)}{q_n(t_1,\ldots,t_k)}) = 0\}).$$

Projected Form: Some algorithms in constructive algebraic geometry are described to operate on hypersurfaces. It is possible to reduce the general case to hypersurfaces. As a consequence of the Theorem of the Primitive Element, every irreducible k-dimensional variety in n-dimensional space is - after a suitable linear transformation of coordinates - birationally projectable onto an irreducible k-dimensional variety in $k+1$-dimensional space. This "projection" is one–to–one for all but finitely many points on the algebraic set. For instance algebraic space curves can be mapped birationally onto planar curves. It can be attempted to parameterize the planar curve and then map the parametrization back to a parametrization of the space curve. We call an irreducible hypersurface given in implicit form by a polynomial f and a list of rational functions $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ a representation in projected form. f, the p's and the q's are polynomials in the variables $t_1, \ldots, t_{k+1}$ specified in the variable list. Let $(a_1, \ldots, a_{k+1}) \in \mathbb{C}^{k+1}$ be a generic point of f, i.e. $f(a_1, \ldots, a_{k+1}) = 0$ and $a_1, \ldots, a_{k+1}$ have transcendence degree k over K. The algebraic set defined by this projected representation is

$$V(\{g \in K[x_1, \ldots, x_n] \mid \\ g(\tfrac{p_1(a_1,\ldots,a_{k+1})}{q_1(a_1,\ldots,a_{k+1})}, \ldots, \tfrac{p_n(a_1,\ldots,a_{k+1})}{q_n(a_1,\ldots,a_{k+1})}) = 0\}).$$

Places: Algebraic sets can also be locally parametrized by power series. Let $p_1, \ldots, p_n$ be univariate power series with coefficients in K. These power series are a description of the algebraic set given in implicit form by a polynomial f and center $(a_1, \ldots, a_n) \in K^n$, if $f(p_1, \ldots, p_n) = 0$ and $p_1(0) = a_1, \ldots, p_n(0) = a_n$. A parametrization in power series with a singular point as center may require more than one tuple of power series to describe all branches of the algebraic set. The representation by places consists of r, $(r \geq 1)$, lists of power series $[p_{11}, \ldots, p_{n1}], \ldots, [p_{1r}, \ldots, p_{nr}]$. The power series are in the variables specified in the variable list. The algebraic set defined by this representation is

$$V(\{g \in K[x_1, \ldots, x_n] \mid \\ g(p_{11}, \ldots, p_{n1}) = 0, \ldots, g(p_{1r}, \ldots, p_{nr}) = 0\}).$$

4 Algorithms

4.1 Conversion Algorithms between Different Representations

One of the design goals of CASA is to provide algorithms for converting a given algebraic set from any representation to any other. However, there are certain limitations, because not all conversions are theoretically possible. For instance, not all curves given in implicit form can be parameterized by rational functions. A short description of the conversion algorithms is given in the sequel.

Rational Parametrization of Curves: The irreducible plane curve C defined by the irreducible polynomial $f(x,y) \in K[x,y]$ is *rational* iff there exist rational functions $\phi(t), \chi(t) \in K(t)$ such that (1) for almost all (i.e. for all but a finite number of exceptions) $t_0 \in \mathbb{C}$, $(\phi(t_0), \chi(t_0))$ is a point on C, and (2) for almost every point (x_0, y_0) on C there is a $t_0 \in \mathbb{C}$ such that $(x_0, y_0) = (\phi(t_0), \chi(t_0))$. If ϕ, χ satisfy the conditions (1) and (2), (ϕ, χ) is a *rational parametrization* of C.

An irreducible curve C in n–dimensional space can be parametrized by projecting it onto a plane curve C', i.e. representing it by an irreducible polynomial $f(x,y)$ and rational functions $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, and parametrizing the plane curve C' by (ϕ, χ). Then

$$\frac{p_1}{q_1}(\phi, \chi), \ldots, \frac{p_n}{q_n}(\phi, \chi)$$

is a rational parametrization of C.

So we arrive at the following parametrization problem:

given: an irreducible polynomial $f(x,y) \in \overline{\mathbb{Q}}[x,y]$ defining an irreducible affine algebraic plane curve C (irreducible over $\mathbb{C}$)

decide: the rationality of C

find: (if C is rational) rational functions $\phi(t), \chi(t) \in \overline{\mathbb{Q}}(t)$ such that (ϕ, χ) is a rational parametrization of C.

CASA contains an algorithm that solves exactly this problem. During the execution of this algorithm the singularity structure of the curve is determined. For curves of genus zero a parametrization is computed by forcing a pencil of curves through these singularities and sufficiently many simple points of the curve. The mathematics behind this parametrization algorithm is described in [SW91].

Implicitization: At present we have implemented three algorithms for finding implicit representations of algebraic sets given in parametric form (see [Kal90b] and [Kal90a]). Each of these algorithms is based on the computation of Gröbner bases. We will only give a short description of one of these algorithms here.

Given the rational parametrization

$$x_1 := \frac{p_1}{q_1}, \ldots\ldots x_n = \frac{p_n}{q_n},$$

where p's and q's are polynomials in $t_1, \ldots, t_k$ over the field K, the algorithm computes the square–free form q of the polynomial $\prod_{i=1}^{n} q_i$. Then the implicit representation of the given algebraic set is found by computing

$$GB(\{p_1 \cdot x_1 - q_1, \ldots, p_n \cdot x_n - q_n, q \cdot z - 1\}) \\ \cap K[x_1, \ldots, x_n],$$

where z is a new variable and GB is the Gröbner basis with respect to the lexical ordering with $x_1 \prec \ldots \prec x_n \prec t_1 \prec \ldots \prec t_k \prec z$.

Conversion from Projected to Implicit Form: If an irreducible algebraic set is given in projected form, i.e. by an irreducible polynomial f in $K[t_1, \ldots, t_{k+1}]$ and rational functions

$$x_1 := \frac{p_1}{q_1}, \ldots\ldots x_n = \frac{p_n}{q_n},$$

where p's and q's are polynomials in $t_1, \ldots, t_{k+1}$ over the field K, then we compute an implicit representation of this algebraic set by a strategy similar to the strategy used in the implicitization algorithm:

The implicit representation of the given algebraic set is found by computing

$$GB(\{p_1 \cdot x_1 - q_1, \ldots, p_n \cdot x_n - q_n, q \cdot z - 1, f\}) \\ \cap K[x_1, \ldots, x_n],$$

where z is a new variable, q is the square–free form of the polynomial $\prod_{i=1}^{n} q_i$, and GB is the Gröbner basis with respect to the lexical ordering with $x_1 \prec \ldots \prec x_n \prec t_1 \prec \ldots \prec t_{k+1} \prec z$.

Projection: Every irreducible k-dimensional variety V in n-dimensional space is — after a suitable linear transformation of coordinates — birationally projectable onto an irreducible d-dimensional variety V' in $d+1$-dimensional space. We have implemented an algorithm to project an implicitly given, irreducible, k-dimensional algebraic set in n-dimensional space onto a k-dimensional hypersurface. This algorithm is based on the computation of Gröbner bases. A detailed description can be found in [Kal91].

Power Series Expansions of Curves: On a planar curve one can compute the places centering around the points of the curve. For curves in implicit form we implemented the Newton polygon method (see for instance [Wal78]). Actually we use refinements of this classical method for singular points ([Duv89]) and regular points ([KT78]). For curves in parametric form numerator and denominator of the rational functions are view as power series and divides out. In both cases a suitable parameter substitution as preprocessing allows to computer the series around a given center.

4.2 Further Operations on Algebraic Sets

Equation Solving: CASA contains an algorithm based on the computation of primitive polynomial remainder sequences and elimination sequences that solves systems of algebraic equations in three variables (see [Kal90c]). More precisely, for a finite set $F \subseteq K[x_1, x_2, x_3]$ the algorithm computes the decomposition

$$V(F) = \bigcup_{i=1}^{m} V(E_i)$$

such that for all $i \in \{1, \dots, m\}$

- E_i is a finite subset of $K[x_1, x_2, x_3]$,
- every common zero of the polynomials in $E_i \cap K[x_1, \dots, x_j]$ is a common zero of the polynomials in $Ideal(E_i) \cap K[x_1, \dots, x_j]$ for every $j \in \{1, 2, 3\}$,
- if $V(F)$ consists of finitely many points then E_i has three elements, a univariate polynomial in x_1, a bivariate polynomial in x_1 and x_2, and a polynomial in three variables.

Dimension and Independent Variables: To compute dimensions of algebraic sets we use one of several different definitions. The dimension of an algebraic set V is the dimension of the ideal I of polynomials in $K[x_1, \dots, x_n]$ vanishing on V. If I is a proper ideal in $K[x_1, \dots, x_n]$ then the dimension of I is the maximal number of elements in any set S of variables independent modulo I. $S \subset \{x_1, \dots, x_n\}$ is independent modulo the proper ideal I if $K[S] \cap I = \{0\}$. We have implemented the computation of the dimension of an implicitly represented algebraic set by doing one Gröbner basis calculation (for details confer [KW88]). As a byproduct we obtain a set of independent variables.

Proper Parametrizations: An algebraic curve in parametric form, given by the rational functions $\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}$ in the variable t, can be reparametrized using a parameter substitution

$$t = \frac{a_n s^m + a_{m-1} s^{m-1} + \dots + a_0}{b_n s^m + b_{m-1} s^{m-1} + \dots + b_0}.$$

The appearance of the curve is not altered, only the relationship between points on the curve and parameter values. If there is a one-to-one correspondence between parameter values t and points on the curve (with exception of singular points), then there is an m-to-one correspondence between parameter values s and points on the curve. Curves which have a one-to-one relationship between parameter values and points on the curve are called properly parametrized curves. Every curve can be reparametrized such that the new parametrization is proper (Lüroth's Theorem, see [Wal78]). We have implemented an algorithm of Sederberg to compute proper parametrizations (confer [Sed86]).

Decomposition of Algebraic Sets in Irreducible Components: CASA contains an algorithm computing the irreducible components of an algebraic set given in implicit form. The output is a sequence of implicitly represented irreducible algebraic sets. The algorithm is based on the computation of Ritt's characteristic sets and Gröbner bases, for details see [Rit50], [Wan89], [Wu84].

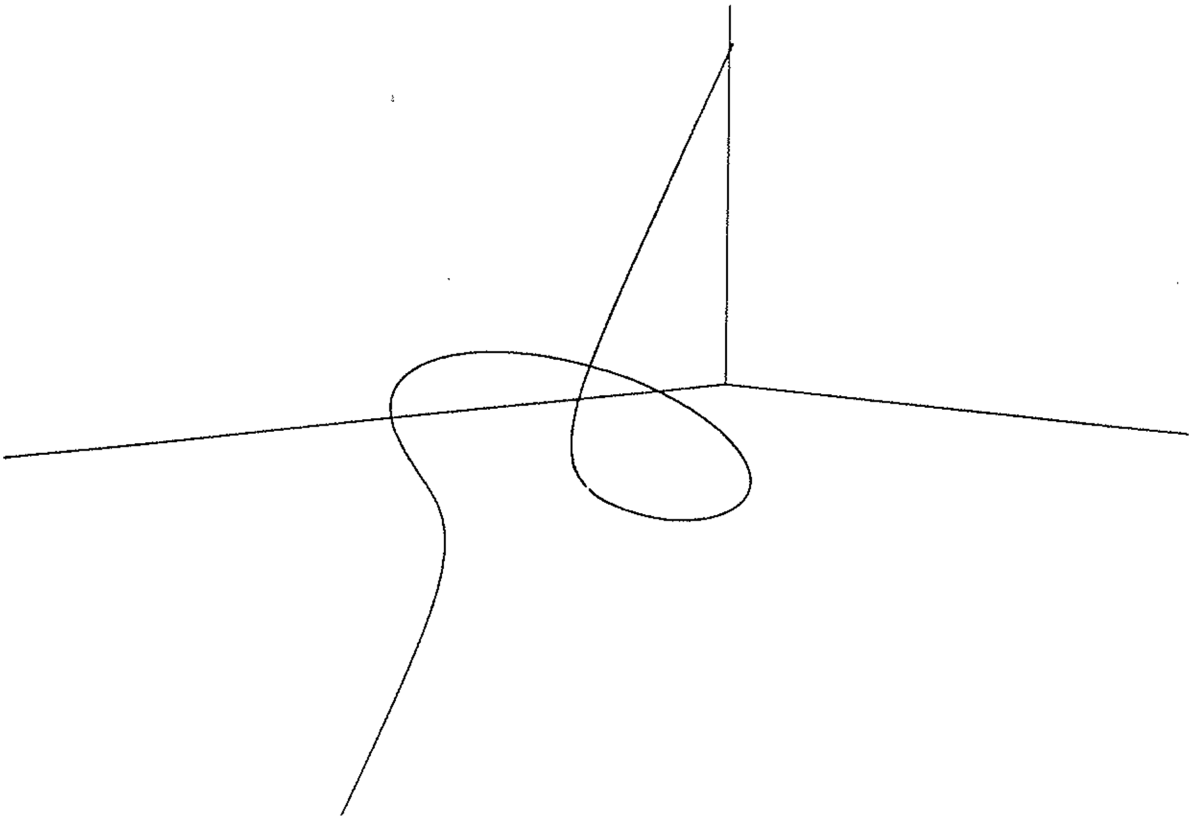
Graphics Representation of Curves and Surfaces: Maple 4.3 provides a function "plot", which results in an internal MAPLE–structure of 2D-curves given in parametric form or as a list of points which have to be connected. This internal structure can be plotted. Such an internal representation of a curve can be visualized on the screen or printer. It is also desirable to draw curves and surfaces given in any other representation, in particular, implicit 2D-curves. The function "plotAlgSet" results in a file containing the graphic representation of a curve or surface given in any type of representation except implicit 3D-curves. For drawing an implicit 3D-curve one can convert the curve from implicit to projected form and then draw the converted curve. This process may result in a loss of finitely many points on the curve. A similar phenomenon occurs in the rational parametrization of the curves. There are several optional parameters to specify, for instance, whether points have to be connected by splines or lines, a title for the drawing, the order of places (i.e. each place ends with the term of the given order), etc.

HELP facility: To use CASA one must get information on the procedures and functions in CASA, i.e. available procedures and functions, sequence of parameters, optional parameters, function results, etc. A call of the function "helpAlgSet" provides information on certain procedures and functions in CASA.

5 Sample Session

```
    |\^/|
._|\|   |/|_. Copyright (c) 1989-1990 the University of Waterloo
 \  MAPLE  /  Version 4.3 --- Mar 1989
 <____ ____>  For on-line help, type  help();
      |
# First we load the CASA files.
>
> read Casa:

# We generate an algebraic set in implicit form and assign it to the variable a.
>
> a := mkImplAlgSet([3*x**2-4*y**2+z**2-8*y*z+4*x*z-4*x+1, x**2+2*y**2+2*y*z+x*z
> -2*x-y-3*z],[x,y,z]);
                         2      2    2
  a := algebraic_set([3 x  - 4 y  + z  - 8 y z + 4 x z - 4 x + 1,

                         2      2
                        x  + 2 y  + 2 y z + x z - 2 x - y - 3 z], [x, y, z],

      attr)

# Now a is decomposed in its irreducible components.
>
> decompose(a);

 algebraic_set(

          3        2      2          2                        3              2
     [10 y  - 8 x y  - 5 y  + 10 y x  - 6 y - 8 y x - 9 + 6 x  + 42 x - 32 x ,

                           2        2
         3 x z - 3 z + 15 x  + 10 y  - 28 x + 7 y - 10 y x + 6,

                          2      2
         3 y z - 3 z - 6 x  - 2 y  + 11 x - 5 y + 5 y x - 3,

            2              2        2
         3 z  - 12 z - 99 x  - 68 y  + 188 x - 68 y + 80 y x - 45],

     [x, y, z], attr),

     algebraic_set([- 1 + 2 y, x + z], [x, y, z], attr)

# a decomposes into two components, one line and one space curve.
# We assign the curve to the variable b.
>
> b := "[1]:
>
# b is one-dimensional. We check this by computing the dimension.
>
> dimension(b);

                                       1

# Next b is birationally projected onto a planar curve in the x-z plane. The representation
# of b as a planar curve + birational map is assigned to c.
>
> c := impl2proj(b);
```

```
c := algebraic_set(

[
                 2      3                    2                     2       3
[17 z - 12 - 60 z  + 5 z  + (71 - 68 z + 39 z ) x + (- 80 + 35 z) x  + 25 x ],

         2                         2
      - z  + 6 z - 1 + (8 - 6 z) x  - 5 x
[x, - -----------------------------------, z]],
                    2 + 4 z

[x, z], attr)

# We plot the space curve given in projected representation. In this case PostScript output
# is produced and stored in the file c.ps

> plotAlgSet(c,x=-5..5,z=-5..5,numpoints=200,plotdevice=postscript,plotoutput='c.ps');
```



```
# A parametrization of c is obtained by parametrizing the planar curve and mapping the
# result back to 3D-space.
>
> d := proj2para(c);

  d := algebraic_set(

                       2        3                  3       2
          445 t + 400 t  + 125 t  + 204         25 t  + 65 t  + 23 t - 27
     [1/2 -----------------------------, 5/2 ------------------------------,
                     3                2                3                2
          441 + 125 t  + 835 t + 550 t       441 + 125 t  + 835 t + 550 t
```

```
                                  3       2
                  71 t + 12 + 25 t  + 80 t
          - 5/2 ------------------------------],
                           3                2
                441 + 125 t  + 835 t + 550 t

      [t], attr)

# In the following we analyze the planar curve obtained by the projection of the space
# curve. The function represent pulls out the representation polynomial. It is assigned to g.
>
> g := represent(c)[1][1];
                      2      3                      2                     2       3
g :=  17 z - 12 - 60 z  + 5 z  + (- 68 z + 71 + 39 z ) x + (- 80 + 35 z) x  + 25 x

# A curve in 2-dimensional space is formed. Here the second (optional) argument,
# a list of variables, is given to specify that the curve is planar.
>
> e := mkImplAlgSet([g],[x,z]);
e := algebraic_set(

                 2      3                      2                     2       3
[17 z - 12 - 60 z  + 5 z  + (- 68 z + 71 + 39 z ) x + (- 80 + 35 z) x  + 25 x ],

[x, z], attr)

# The algorithm tsolve computes the solution of a system of equations in at most
# three variables. It is based on the computation of polynomial remainder sequences.
# tsolve is used to determine the singularities of the planar curve given by g.
>
> tsolve([g,diff(g,x),diff(g,z)],[x,z]);
                            [[z + 1/2, 180 x - 306]]

# A power series expansion of the curve can be computed around this singularity.
>
> f := impl2plac(e,[306/180,-1/2]);
 f := algebraic_set([[proc(powparm) ... end, proc(powparm) ... end],

                        [proc(powparm) ... end, proc(powparm) ... end]], [T],

     attr)

# The function shAlgSet is used to print out a finite approximation of the series.
# The second argument gives the number of terms that are computed.
>
> shAlgSet(f,3);
The algebraic set is given by the following places:
                                      /                  1/2\
      17        1                     |       1         2   |  2      3
   [[---- + ---------- T, - 1/2 + T + |- 300 ---- - 210 ----| T  + O(T )],
      10           1/2                \       %1        %1  /
            5 - 5 2

                                         /                  1/2\
         17        1                     |       1         2   |  2      3
       [---- + ---------- T, - 1/2 + T + |- 300 ---- - 210 ----| T  + O(T )]]
         10           1/2                \       %1        %1  /
               5 + 5 2
                                           1/2
%1 :=                           - 48 - 36 2
```

Acknowledgement

We thank Dongming Wang for providing us with the code for the decomposition algorithm and for suggesting a nice example.

Conclusion

Computer algebra can be applied to solve many interesting problems in algebraic geometry. We have described the program system CASA, which provides a variety of operations for algebraic curves and surfaces. Whatever is described in this paper is available in the CASA system. However, there are still many algebraic and geometric algorithms that we plan to implement in the future.

References

[Ben90] D. Bennett. Interactive Display and Manipulation of Curves and Surfaces of Mathematical Functions. *ACM SIGSAM Bulletin*, 24(3), 1990.

[BR90] C. Bajaj and A. Royappa. The GANITH Algebraic Geometry Toolkit. In A. Miola, editor, *Lect. Notes in Comp. Sci. 429, DISCO '90*, pages 268–269, Capri, Italy, April 1990. also in: ACM SIGSAM Bulletin 24(3).

[Duv89] D. Duval. Rational Puiseux Expansion. *Compositio Mathematica*, 70:119–154, 1989.

[Kal90a] M. Kalkbrener. Implicitization by Using Gröbner Bases. Technical Report RISC-Series 90-27, Univ. of Linz, 1990.

[Kal90b] M. Kalkbrener. Implicitization of Rational Curves and Surfaces. In *Proc. AAECC-8 (to appear)*, 1990.

[Kal90c] M. Kalkbrener. Primitive Polynomial Remainder Sequences. Technical Report RISC-LINZ Series no. 90-01, Research Institute for Symbolic Computation, Univ. of Linz, 1990.

[Kal91] M. Kalkbrener. Birational Projections of Irreducible Varieties. Technical Report RISC-LINZ Series no. 90-59, Research Institute for Symbolic Computation, Univ. of Linz, 1991.

[KHSH90] M. Kalkbrener, W. Herfort, J. Seke, and M.O. Hittmair. Application of primitive polynomial remainder sequences to a problem of quantum optics. *Sitzungsbericht der österr. Akademie der Wissenschaften (to appear)*, 1990.

[KT78] H. T. Kung and J. F. Traub. All Algebraic Functions Can Be Computed Fast. *J. of the ACM*, 25:245–260, 1978.

[KW88] H. Kredel and V. Weispfenning. Computing Dimension and Independent Sets for Polynomial Ideals. *J. Symb. Comput.*, 6(2 and 3):231–248, 1988.

[Rit50] J. F. Ritt. *Differential Algebra*. AMS, 1950.

[Sed86] T. W. Sederberg. Improperly parametrized rational curves. *Computer Aided Geom. Design*, 3(1):67–75, 1986.

[SSB89] M. Stillman, M. Stillman, and D. Bayer. *Macaulay User Manual*, 1989.

[SW91] J. R. Sendra and F. Winkler. Symbolic Parametrization of Curves. *J. of Symbolic Computation*, 1991. (To appear).

[Wal78] R. J. Walker. *algebraic curves*. Springer-Verlag, second edition, 1978.

[Wan89] D. Wang. A Method for Determining the Finite Basis of an Ideal from its Characteristic Set with Application to Irreducible Decomposition of Algebraic Varieties. Technical report, RISC-Linz series no. 89-50.0, Research Institute for Symbolic Computation, University of Linz, Austria, Dec. 1989.

[Wu84] W. Wu. Basic Priniciples of Mechanical Theorem Proving in Elementary Geometries. *Journal Sys. Sci. & Math. Scis.*, 4:207–235, 1984.