CASA – A System for Computer Aided Constructive Algebraic Geometry

Michal Mňuk* and Franz Winkler**

Research Institute for Symbolic Computation, Linz, Austria

Abstract. Increasing power of computing devices shed a new light on the role of mathematical experiments. Constructive methods yield new insights into the nature of complicated problems. This paper describes the system CASA which implements basic principles of the classical algebraic geometry. It was created around the notion of the algebraic set and is currently supporting many operations on them while adhering to simplicity and efficiency.

1 Introduction

The old masters of algebraic geometry developed this field in an inherently constructive spirit. This fact together with the increasing power of computers laid a firm basis for implementation of a large portion of this field in software. Thus it becomes possible to automatize many computations hence opening new prospects and possibilities not only to mathematical research but also to industrial applications.

The package CASA – the name standing for *Computer Algebra System for Algebraic geometry* – was designed to perform computations and utilize reasoning about geometrical objects in the classical affine and projective algebraic geometry over algebraically closed fields of characteristic 0. Usually, the underlying ground field is the field of rational numbers or finite algebraic extensions thereof. CASA has been developed at the Research Institute for Symbolic Computation, Linz, Austria, in a research group headed by F. Winkler. The project started in 1990. A first report on development of CASA appeared in [5]. Since that time many people contributed to CASA in one or in the other way. The largest part of work has been done by R. Gebauer, M. Kalkbrener, M. Mňuk, R.J. Sendra, P. Stadelmeyer, B. Wall, and F. Winkler.

CASA has been built around the notion of the algebraic set. Originally, fundamental algorithms were written for algebraic sets in implicit representation, i.e. for sets given by zeros of a set of polynomials. However, due to theoretical and practical reasons the variety of possible representations was extended to

* E-mail: `mmnuk@risc.uni-linz.ac.at`
** E-mail: `winkler@risc.uni-linz.ac.at`

comprise also the parametric, projected and the representation by power series (used for curves).

- *Implicit representation:* An algebraic set is the set of common zeros of a system of polynomial equations. To give an algebraic set in implicit form means to give finitely many polynomials.
- *Projected representation:* As a consequence of the primitive element theorem every irreducible d–dimensional algebraic set in n–dimensional space is, after a suitable linear transformation of coordinates, birationally projectable onto an irreducible d–dimensional algebraic set in $(d+1)$–dimensional space. The image of this projection can be specified by a single polynomial in $d+1$ variables. This can be generalized to unmixed-dimensional algebraic sets. An algebraic set in projected form is given by a polynomial and a tuple of rational functions (specifying the birational mapping).
- *Parametric representation:* Some irreducible algebraic sets can be parametrized by rational functions. An algebraic set in parametric form is given by a tuple of rational functions that parametrizes the algebraic set.
- *Representation by places:* All algebraic curves can be parametrized by a set of power series that are convergent around a point of the curve. An algebraic set is given by places if for each branch passing through a certain point on the algebraic set a tuple of power series that parametrizes the algebraic set around the point is specified.

CASA also works with the polynomial ideals corresponding to these geometric objects.

The operations available in CASA include

- ideal theoretic operations $+, *, \cap, /$,
- creating algebraic sets in different representations,
- generating curves of fixed multiplicities at given points,
- intersection, union, and difference of algebraic sets,
- computing tangent cones and tangent spaces,
- computation of the dimension of an algebraic set,
- decomposition into irreducible components,
- transformations of algebraic sets to hypersurfaces,
- computation of the genus of a curve,
- rational parametrization of curves,
- implicitization of parametrically given algebraic sets,
- Puiseux series expansions,
- plotting both explicitly and implicitly given curves and surfaces.

For more information on the underlying mathematics and software issues we refer to [13, 14]. Some typical sessions of CASA may be found in [8, 17, 18].

The basic philosophy of CASA is to provide a variety of operations on algebraic sets. As the efficiency of these operations is tightly bound to the way algebraic sets are represented, conversion routines have been provided to support various views on one object, to deepen the understanding of its principles, and to speed up algorithms working on algebraic sets. The major goal was to design a system which provides a comfortable, easy to use, efficient, flexible, and mathematically exact working environment for constructive algebraic geometry where all basic theoretical concepts map easily to available data structures. The fact that CASA is based solely on Maple and is fully independent of the operating system, allows it to be used on every hardware where Maple is running.

There are software systems which partially cover some of the fields of CASA, however, to authors' knowledge, there is currently no system with comparable capabilities available.

2 Structure of CASA

CASA evolved over several years from an independent set of Maple programs. From version 2.1 to 2.2 there was a significant change in the internal structure of the system. The code was reorganized into a number of separate modules. Each module contains a set of operations performing related tasks. After this, the code became cleaner and several modules may be now used as stand-alone Maple packages having distinguished name space which avoids conflicts with other software already loaded in the Maple session. The whole system is distributed as a single Maple archive of compiled routines. Unlike previous versions of CASA, the modules and their major parts are loaded into memory using Maple's `readlib`-facility when they get used for the first time. This significantly cuts the amount of memory occupied by the code keeping it free for data.

The documentation of CASA is written using a restricted set of LaTeX commands. The description of every procedure may then be converted to both online Maple help file and to high quality printouts including mathematical formulae. This approach was chosen in order to keep the on-line help consistent with printed manual.

3 Modules

3.1 Basic Operations

The central notion of CASA – the algebraic set – is implemented as a structure (Maple's unevaluated function call) holding the defining entities, a description of the underlying space in which the set is embedded, and some attributes and properties. During a computation, when a new knowledge about an algebraic set is obtained, it is added to its property list to avoid laborious recomputations when this knowledge is needed later. The information already contained in the property list is retrieved whenever some function requires it.

The module for basic operations provides functions to manipulate the structure of the algebraic set, to add new knowledge, and to query about it.

To create an algebraic set given by a polynomial ideal the function `mkImplAlgSet` is called with the generating ideal, the space in form of a list of variables, and some additional information which may be known in advance. The set is implicitly assumed to be affine if it is not explicitly declared projective (by adding the attribute `basespace=projective` to the property list.

```
> A := mkImplAlgSet([x*(x^2+y^2-1),x*z,x^2+y^2+z^2-1],
>                       [x,y,z]);
```

$$A := \text{algebraic\_set}(\,[\,x z, x(x^2+y^2-1\,), x^2+y^2+z^2-1\,], [\,x, y, z\,]\,)$$

Parametric sets are given by a list of rational functions in some parameters.

```
> P:=mkParaAlgSet([(t^4-12*t^2-3*t+13)/(t^3-2*t+1),
>                      (5*t^3-6*t^2-4)/(t^3+2*t+1)],[t]);
```

$$P := \text{algebraic\_set}\left(\left[\frac{t^4-12t^2-3t+13}{t^3-2t+1}, \frac{5t^3-6t^2-4}{t^3+2t+1}\right], [\,t\,]\right)$$

The representation may be obtained by calling the function `represent`.

```
> represent(P);
```

$$\left[\frac{t^4-12t^2-3t+13}{t^3-2t+1}, \frac{5t^3-6t^2-4}{t^3+2t+1}\right]$$

3.2 Gröbner Bases and Syzygies

The concept of Gröbner bases was originally introduced for polynomial ideals ([1]). But as shown in [9] it can be naturally generalized to submodules of a free module over polynomial rings.

Besides the improved classical Gröbner bases algorithm CASA contains an implementation of Gröbner bases for modules over polynomial rings. It allows to compute Gröbner bases for multivariate polynomial modules and solve systems of linear equations with polynomial coefficients.

Consider the following linear system of equations in $z_1, z_2, z_3 \in K[x,y]$:

$$\begin{pmatrix} x^3-y & xy-1 & -x+y^2 \\ -x+y & x^3-1 & y-1 \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} xy^2-y^2 \\ -x^5+x^2-x+y^2 \end{pmatrix}$$

The function `msolveGB` yields the basis of the solution space.

```
> msolveGB([[x^3-y,-x+y],[x*y-1,x^3-1],[-x+y^2,y-1]],
>           [x*y^2-y^2,-x^5+x^2-x+y^2],[x,y],term,tdeg);
```

$$
\begin{aligned}
&[[y,-x^2,x],[[-1+x+y-y^2+xy-xy^2+x^3y^2-x^4,\\
&\qquad y-y^2-x^3-x^2+xy+xy^2-y^3+x^3y,\\
&\qquad x-2y+x^3+xy^2+x^3y-x^2y-x^6]]]
\end{aligned}
$$

3.3 Set Operations

The canonical correspondence of algebraic sets and radical polynomial ideals allows to perform set theoretic operations on algebraic sets (union, difference, intersection, Zariski closure, etc). The basic algorithm used here is the computation of Gröbner bases in polynomial rings.

Let us consider the algebraic set A from Section 3.1 and represent it as an intersection of radical ideals by calling the function `computeRadical`.

```
> radA := computeRadical(A);
```

$$
\begin{aligned}
radA :=&\text{algebraic\_set}([z,x^2+y^2-1],[x,y,z]),\\
&\text{algebraic\_set}([x,y^2+z^2-1],[x,y,z])
\end{aligned}
$$

The union of the two algebraic sets from above is obtained using `implUnion`.

```
> G:=implUnion(radA);
```

$$
\begin{aligned}
G := \text{algebraic\_set}([&xz, zy^2+z^3-z, x^3+y^2x-x,\\
&x^2y^2+x^2z^2-x^2+y^4+y^2z^2-2y^2-z^2+1],[z,x,y])
\end{aligned}
$$

Using the corresponding operations on ideals, the closure of the set theoretic difference of A and the second component $radA_2$ of $radA$ is computed.

$$
\begin{aligned}
A &= \text{algebraic\_set}([x(x^2+y^2-1),xz,x^2+y^2+z^2-1],[x,y,z])\\
radA_2 &= \text{algebraic\_set}([x,y^2+z^2-1],[x,y,z])
\end{aligned}
$$

```
> implDifference(A,radA[2]);
```

$$
\text{algebraic\_set}([z,x^2+y^2-1],[x,y,z])
$$

3.4 Conversions

To utilize efficient computations over algebraic sets and to support different views, many conversion operations between representations mentioned above are implemented in CASA. The conversion of a one-dimensional set in implicit form to a parametric representation is done by the algorithm described in [12]. To implicitize parametric sets, Gröbner basis computation is used. Algorithms for converting algebraic sets to projected representation are described in [15]. Puiseux series are used to obtain curves represented by places (series).

To convert the set A to the projected representation, `convertRep(A,proj)` is called.

```
> B:=convertRep(A,proj);
```

$$B := \text{algebraic\_set}([[x^2+y^2-1],[x,y,0]],[y,x]),$$
$$\text{algebraic\_set}([[z^2-1+x^2],[0,-x,z]],[x,z])$$

The representation of the first set

```
> represent(B[1]);
```

$$[[x^2+y^2-1],[x,y,0]]$$

consists of a list defining a hypersurface x^2+y^2-1 in the 2-dimensional affine space and a mapping

$$\begin{array}{ccc} \mathbb{A}^2 & \longrightarrow & \mathbb{A}^3 \\ (x,y) & \longrightarrow & (x,y,0) \end{array}$$

In this computation, the Gröbner basis of A has been determined and automatically added to the property list by some function called by `convertRep`.

```
> attributes(A);
```

$$[groebnerbasis = [plex, [x^2+y^2+z^2-1, xz, zy^2+z^3-z]]]$$

The basis will be retrieved whenever it is needed in subsequent tasks.

Among others, routines to convert parametric representation to the implicit one are implemented in CASA. The following parametric space curve C may be represented as a zero set of an ideal in $K[x,y,z]$ with 4 generators given below.

```
> C:=mkParaAlgSet([(t^4+3*t^2-7*t+4)/(t^2-3*t+1),
>                  (4*t^2-1)/(2*t^2-3),t],[t]);
```

$$C := \text{algebraic\_set}\left(\left[\frac{t^4+3t^2-7t+4}{t^2-3t+1}, \frac{4t^2-1}{2t^2-3}, t\right], [t]\right)$$

```
> convertRep(C,impl);
```

$$\begin{aligned}&\text{algebraic\_set}([5010x+9772y-3500z+1500zx-17843+884x^2\\&\quad+21960xy-13421y^2+8076y^3-176x^3+1304x^3y+9548y^2x^2\\&\quad-1072x^3y^2-1688y^3x^2+430y^3x-14280y^2x-12536x^2y\\&\quad+232x^3y^3, 392x+3136y+176x^2+2996xy-2793-2702y^2\\&\quad+2184y^3+1724y^2x^2-768y^3x^2+1564y^3x-4132y^2x-673y^4\\&\quad-1392x^2y+116y^4x^2-148y^4x, 590zy^2-1260zy+910z\\&\quad+116y^3x^2-86x+189y-88x^2-2356xy+653y^2-673y^3\\&\quad-536y^2x^2-148y^3x+1519+1558y^2x+652x^2y, 250z^2\\&\quad-116y^3x^2+196x+1026y+88x^2+1596xy-838y^2+673y^3\\&\quad+536y^2x^2+148y^3x-1268y^2x-1459-652x^2y], [x,y,z])\end{aligned}$$

3.5 Dimension

For the dimension computation the algorithm in [6] was implemented in CASA. Only one Gröbner basis w.r.t. a lexicographic term ordering needs to be computed for determining the dimension of an ideal.

```
> U := mkImplAlgSet([36*z*y^2*x+8*x^3*z^5+16*x^3*z^2*y^3
>            -8*x^5*z -4*x^3*z^2*y^2-2*z*y^2*x^2-z^2*y^4,
>          12*x^6*z*y^2-48*x^4*z-39*z*y^6-12*z*y^2*x,
>          -12*x^3*z-3*z*y^2],[x, y, z]);
```

$$\begin{aligned}&U := \text{algebraic\_set}([12x^6zy^2-48x^4z-39zy^6-12zy^2x,\\&\qquad 36zy^2x+8x^3z^5+16x^3z^2y^3-8x^5z-4x^3z^2y^2-2zy^2x^2-z^2y^4,\\&\qquad -12x^3z-3zy^2], [x,y,z])\end{aligned}$$

```
> dimension(U);
```

$$2$$

3.6 Decomposition

Decomposing algebraic sets into irreducible parts is achieved by constructing the characteristic set for the defining polynomial ideal (cf. [16]). For sets in 3-dimensional space, the projected representation onto unmixed dimensional hypersurfaces may be used to achieve partial splitting. The factors of generating polynomials of hypersurfaces yield then the irreducible components.

```
> N:=mkImplAlgSet([-y^2*z^2 + 10*y^2*z - y*z^2 - 25*y^2
>          + 6*y*z + x - 5*y +1,y^3*z^2 - 10*y^3*z + 25*y^3
>          - y^2*z + 5*y^2 - y*z + y]);

> U:=decompose(N);
```

$$
\begin{aligned}
U :=&\text{algebraic\_set}([y, 1+x], [x,y,z]),\\
&\text{algebraic\_set}([\\
&20yz+zx+5z-x^2y-54y-152y^2-22y^2x\\
&\quad -19yx+2y^2x^2-4,\\
&y^3x^2-76y^3-15y^2-3y-1-11y^3x-15y^2x-3yx-x,\\
&4z^2+zx-23z-2y^2x^2+152y^2+106y+36+22y^2x+41yx\\
&\quad +16x-x^2y, -16x^2y+65z-44x-438y-1064y^2+2zx\\
&\quad -306y^2x-197yx-8y^2x^2+2y^2x^3-x^3y+zx^2-108], [x,y,z])
\end{aligned}
$$

3.7 Curves

Many algorithms for dealing with algebraic curves are implemented – parametrization and implicitization, tangent cones, adjoint curves, singularities, implicit plots, etc. All algorithms use symbolic methods to achieve exact results. In the future, mixed symbolic-numerical methods will be implemented to gain more speed-up while keeping sufficient accuracy.

Let us consider a curve C_1 in the 2-dimensional projective space.

```
> C1:=mkImplAlgSet([-15*y^2*z^3-76*y^3*z^2-z^5-3*y*z^4
>       -15*x*y^2*z^2-11*x*y^3*z-x*z^4-3*x*y*z^3+y^3*x^2],
>       [x,y,z],{basespace=projective});
```

$$
\begin{aligned}
C_1 :=&\text{algebraic\_set}([-15y^2z^3-76y^3z^2-z^5-3yz^4-15xy^2z^2-11xy^3z\\
&\quad -xz^4-3xyz^3+y^3x^2], [x,y,z])
\end{aligned}
$$

The function `singularities` yields all singular points of C_1 decomposed into classes points having the same multiplicity.

```
> singularities(C1);
```

$$\begin{aligned}
&\text{table}([\\
&3 = [[1,0,0]]\\
&2 = \left[\left[\text{RootOf}(\_Z^2+2\_Z+65), -\frac{1}{4}-\frac{1}{20}\text{RootOf}(\_Z^2+2\_Z+65), 1\right],\right.\\
&\qquad \left.[0,1,0]\right]\\
&])
\end{aligned}$$

The above curve has one triple point and three[1] double points, it has genus 0, and hence may be converted into parametric representation.

```
> convertRep(C1,para);
```

$$\text{algebraic\_set}\left(\left[-t^3-15t^2-75t-126, -\frac{t+5}{26+t^2+11t}, 1\right], [t]\right)$$

3.8 Plotting

Visualization of algebraic sets is a critical task. Their in many cases complicated nature must be faithfully translated into a picture. For the majority of tasks, only singular or other distinguished points of algebraic sets yield some interesting information. These objects have to be treated with care, requiring special analysis. CASA makes a thorough effort to obtain correct information about the local topology in neighborhoods of singularities and other critical points.

The curve C_1 from Section 3.7 is a projective curve. We may consider the affine pieces of C_1, i.e. $C_{1,x} = C_1 \cap V(x-1)$, $C_{1,y} = C_1 \cap V(y-1)$, and $C_{1,z} = C_1 \cap V(z-1)$:

```
> C1x:=convertSpace(C1,affine,x);
> C1y:=convertSpace(C1,affine,y);
> C1z:=convertSpace(C1,affine,z);
```

$$\begin{aligned}
C_{1,x} := \text{algebraic\_set}([&-15y^2z^3-76y^3z^2-z^5-3yz^4-15y^2z^2\\
&-11y^3z-z^4-3yz^3+y^3],[y,z])\\
C_{1,y} := \text{algebraic\_set}([&-15z^3-76z^2-z^5-3z^4-15xz^2-11xz\\
&-xz^4-3xz^3+x^2],[x,z])\\
C_{1,z} := \text{algebraic\_set}([&-15y^2-76y^3-1-3y-15xy^2-11xy^3\\
&-x-3xy+y^3x^2],[x,y])
\end{aligned}$$

[1] Note that the first "point" in the list of double points is a class of two points each corresponding to one root of $z^2+2z+65$.

Based on the analysis of certain distinguished points, CASA's function `plotAlgSet` makes exact and topologically correct drawings. See figure 1.

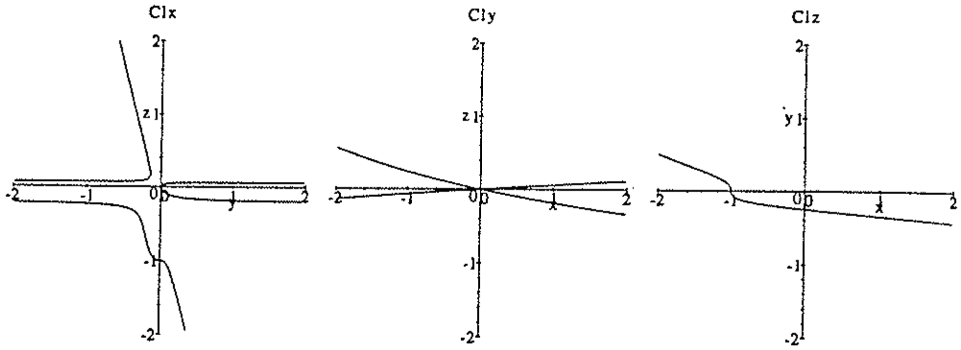

Figure 1. Affine pieces $C_{1,x}$, $C_{1,y}$, and $C_{1,z}$ of C_1

4 Future Developments

The CASA system is undergoing steady development. In next releases, parametrization of surfaces, recent results in parametrization of curves, search for rational points on curves, an improved hybrid symbolic-numerical algorithm for plotting algebraic sets, offset curves and surfaces, and Hilbert polynomial series will be implemented.

Availability

CASA is available for anonymous ftp at *ftp.risc.uni-linz.ac.at* in the directory */pub/CASA*. As of this writing the version 2.2 (patchlevel 1) is available. A WWW page may be accessed at *http://info.risc.uni-linz.ac.at:/labs-info/compal/software/casa/casa.html*.

References

1. Bruno Buchberger. An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional System Theory*, pages 184–232. Reidel, Dordrecht Boston Lancaster, 1985.

2. Bruce W. Char, Keith O. Geddes, Gaston H. Gonnet, Benton L. Leong, Michael B. Monagan, and Stephen M. Watt. *Maple V Library Reference Manual.* Springer-Verlag, 1991.
3. Bruce W. Char, Keith O. Geddes, Gaston H. Gonnet, Benton L. Leong, Michael B. Monagan, and Stephen M. Watt. *Maple V: Language Reference Manual.* Springer-Verlag, 1991.
4. Bruce W. Char, Keith O. Geddes, Gaston H. Gonnet, Benton L. Leong, Michael B. Monagan, and Stephen M. Watt. *First Leaves. A Tutorial Introduction to Maple V.* Springer-Verlag, 1992.
5. Richard Gebauer, Michael Kalkbrener, Bernhard Wall, and Franz Winkler. CASA: A Computer Algebra Package for Constructive Algebraic Geometry. In S. M. Watt, editor, *ISSAC 91*, pages 403–410, Bonn, Germany, July 1991. ACM Press.
6. H. Kredel and V. Weispfenning. Computing dimension and independent set for polynomial ideals. *J. Symb. Comput.*, 6:231–248, 1983.
7. Michal Mňuk. *Algebraic and Geometric Approach to Parametrization of Rational Curves.* PhD thesis, Research Institute for Symbolic Computation, Linz, Austria, December 1995.
8. Michal Mňuk, Bernhard Wall, and Franz Winkler. CASA reference manual (version 2.2). Technical Report 95-05, Research Institute for Symbolic Computation, Linz, Austria, 1995. See also *http://info.risc.uni-linz.ac.at:/labs-info/compal/software/casa/casa.html.*
9. F. Mora and H.M. Möller. New constructive methods in classical ideal theory. *J. Algebra*, pages 138–178, 1986.
10. Tran Quoc-Nam. A hybrid symbolic-numerical method for tracing surface-to-surface intersections. In A.H.M. Levelt, editor, *Proc. ISSAC'95*, pages 51–58. ACM Press, 1995.
11. Tran Quoc-Nam. On the symbolic-numerical methods for finding the roots of an arbitrary system of non-linear algebraic equations. In *Proc. ATCM'95*, Singapore, 1995. The Assoc. of Math. Eds.
12. J. Rafael Sendra and Franz Winkler. Symbolic parametrization of curves. *J. Symb. Comput.*, 12(6):607–631, 1991.
13. Igor A. Shafarevich. *Basic Algebraic Geometry*, volume 1. Springer Verlag, second edition, 1994.
14. Robert J. Walker. *Algebraic Curves.* Princeton University Press, 1950.
15. Bernhard Wall. *Symbolic Computation with Algebraic Sets.* PhD thesis, Research Institute for Symbolic Computation, Linz, Austria, 1993.
16. Dongming Wang. Irreducible decomposition fo algebraic varieties via characteristic sets and grbner bases. Technical Report 92–55, Research Institute for Symbolic Computation, August 1992.
17. Franz Winkler. Constructive algebraic geometry with CASA. Talk at workshop CoCoA, Cortona, Italy, 1993.
18. Franz Winkler. Algebraic computation in geometry. *Math. and Computers in Simulation*, (1319), 1996.