HySaX Project — FWF P11160-TEC
Progress Report for the Year 1996

Franz Winkler and Tran Quoc Nam
Institut für Mathematik and
Research Institute for Symbolic Computation (RISC)
Johannes Kepler Universität Linz, Austria

March 4, 1997

In 1996, we made rapid progress in both theoretical and practical aspects. In the following we describe shortly the main results obtained in this first year of the project. Further information on the project HySaX can be obtained from the web page

`http://www.risc.uni-linz.ac.at:81/projects/basic/hysax`

<u>On the Dimension of the Irreducible Components of an Algebraic Set</u>

Irreducible decomposition is widely used in algebraic geometry, computer aided geometric design, etc. In fact, it has been used as the first and requisite step in many constructive computations such as parameterization, genus computation, projection of an algebraic set onto a hypersurface. It is a well-known result that we can algorithmically decompose an algebraic set (in K^n, where K is a field) into a union of finitely many irreducible and noncontractive components. The decomposition of an algebraic set is unique up to the order in which the components are written. The classical approach involves the computation of characteristic sets and Gröbner bases, which can be prohibitively expensive.

Meanwhile in practice, for example in computer aided geometric design (cagd) or visualization, we need only an approximation of the algebraic set, in particular for one-dimensional algebraic sets. In fact, approximation and representation of one-dimensional algebraic sets in higher dimensional space is a fundamental and difficult problem in computer aided geometric design (cagd), visualization and solid modeling. For example, the intersection of two parametric surfaces can be seen as a space curve in a 4-dimensional space and the intersection of an implicit surface with an r-offset surface of another implicit surface can be seen as a space curve in a 6-dimensional space.

In [Tran3,4] we present some new results concerning the dimension of the irreducible components of an algebraic set. We also show how to use our results to develop hybrid symbolic-numerical algorithms, which aim at the goals of efficiency and reliability, for solving the problem of approximation and representation of one-dimensional algebraic sets in computer aided geometric design and visualization.

Extending Dixon's Resultant by Using Pseudoinverse Matrices

In applied mathematics such as cagd and solid modeling, we often have to eliminate several variables from a system of equations (e.g. the problem of implicitization). Theoretically, the Gröbner bases method, Ritt's characteristic set method or successive Sylvester resultant computations can be used to achieve this. But they are inefficient and require a lot of memory space.

Meanwhile, Dixon's resultant is an efficient method to simultaneously eliminate several variables from a system of nonhomogeneous polynomial equations at a time. In contrast with the successive resultant computation techniques which eliminate variables one by one and compute numerous intermediate resultants before finally computing the resultant of the whole set, Dixon's resultant creates a much smaller matrix and avoids such intermediate results, and hence is much faster and also saves memory space.

But unfortunately, Dixon's resultant does not work for most algebraic and geometric problems. Dixon's resultant is a method for obtaining the resultant of $n+1$ generic n-degree polynomials in n variables — a condition which cannot be satisfied by most problems arising in practice. For most practical problems, the matrix set up in Dixon's method, the Dixon matrix, becomes singular or even nonsquare.

In [Tran5], by using techniques from the theory of pseudoinverse matrices, we overcome some of the above obstacles and extend Dixon's resultant to an arbitrary system of $n+1$ nonzero polynomials where the Dixon matrix can be singular or even nonsquare. This same approach can also be used to extend other multivariate resultant methods such as Macaulay resultants or sparse resultants. Roughly speaking, our extended Dixon's resultant method leads to the computation of an exactly general solution of a system of linear equations with multivariate polynomial coefficients.

We plan to continue this research on Dixon resultants. In particular, we want to investigate interpolation techniques for fast computation of these resultants.

Intersection of Surfaces

In [Tran1, 2] we present a hybrid symbolic-numerical method for approximation and representation of intersections of surfaces – a fundamental and difficult problem in computer aided geometric design (cagd) and solid modeling. The main contributions of these paper are that: firstly, we solve the problem of finding a starting point for each branch of the algebraic set by using a new iterative method of the author's for finding the roots of an arbitrary system of equations; secondly, we compromise between the two main goals of the method, namely reliability and efficiency, by using symbolic computations when needed, utilizing floating-point and parallel arithmetic whenever possible; and finally, we prevent duplicate tracing, additional singularities and reduce the degree of the defining polynomials by using a new result of the author's on constructible irreducible decomposition.

Our method is a hybrid method that uses exact computation or numerical computation when needed. In the method, we separately treat the 3-dimensional cases and the higher dimensional cases. For tracing intersections of two implicit surfaces in 3-dimensional space, the method overcomes the main difficulties of numerical tracing, namely finding a sample point for every real branch and marching through singularities by using techniques for real root isolation of polynomials with real algebraic number coefficients and the extended Dixon's resultant method for solving polynomial systems.

The method can also be used for tracing along incomplete intersection space curves; i.e. space curves which can only be generated by at least 3 surfaces in 3-dimensional space, or algebraic curves in higher dimensional space. In these cases, the key step of the algorithm is based upon a combination of dimension theory, characteristic sets method and an iterative method of the author's for finding the roots of an arbitrary system of equations, namely the "Extended Newton's Method".

Our algorithm for one-dimensional algebraic sets overcomes the main difficulties of numerical tracing, namely finding a sample point for every real branch. The method does not require the expensive computation of irreducible decomposition. Moreover, it will prevent duplicate tracing and additional singularities as we may have when we trace a reducible space curve. The method also overcomes the difficulties of roundoff errors near the singularities and component jumping. Further it utilizes floating-point and parallel arithmetic whenever possible. Experiments from examples found in the literature shows the considerable speed up of the method.

Points on Algebraic Curves and Parametrization

A plane algebraic curve is classically given as the zeros of a bivariate polynomial. However, this implicit representation is badly suited for many applications, for instance in computer aided geometric design. What we want in many of these applications is a rational parametrization of an algebraic curve. In our previous work and also in previous projects funded by FWF we have investigated symbolic algorithms for the parametrization of algebraic curves, and in fact we have developed a "optimal" algorithm, in the sense that we get a parametrization over the smallest algebraic extension field possible. This optimal algorithm depends crucially on our ability to find simple points on the curve over small extension fields, or, in the best case, over the original coefficient field. In fact, it is enough to be able to do this for conics.

We have applied Legendre's theory of solving quadratic Diophantine equations to our problem, and we have also been able to generalize Legendre's theory to other practically interesting fields, such as rational functions over the rationals, i.e. $\mathbb{Q}(t)$. This work is described in [Hill], [Win1,3,5].

Given an algebraic curve defined over the rational number field, we can decide whether the curve has infinitely many points over $\mathbb{Q}$ (and consequently can be parametrized over $\mathbb{Q}$), over $\mathbb{R}$, or needs a complex algebraic extension. We are able to extend these decision methods from $\mathbb{Q}$ to $\mathbb{Q}(t)$. We conjecture that this extension should lead to parametrization algorithms for certain surfaces of interest in computer aided geometric design.

Development of the program system CASA

The program system CASA was presented at the seminar "Computeralgebra--Software" at Schloß Dagstuhl [Win2], at the workshop "Computeralgebra" in Klagenfurt [Win4], and at the DISCO'96 conference in Karlsruhe [MnWi]. Several of the theoretical achievements mentioned above were incorporated in CASA. A new version of the system is planned for April 1997.

The CASA system is used by many colleagues around the world. More than 100 people have downloaded CASA and probably installed it at their sites. In particular, we know that the system is used at ETH Zürich, universities in Madrid and Santander, TU München, and several other universities in Europe, USA and Australia.