Parametrized Solutions of Algebraic Equations *

IMACS SC–93, Lille France

Franz Winkler
Institut für Mathematik and
Research Institute for Symbolic Computation
Johannes Kepler Universität
A-4040 Linz, Austria
e-mail: winkler@risc.uni-linz.ac.at

Abstract: In solving systems of algebraic equations we encounter basically two different situations. If the solution space is zero-dimensional we can list the finitely many solutions. This approach, however, fails if the dimension of the solution space is non-zero. We propose to use a parametrized representation for this situation, i.e. the solutions are represented by a birational map with ground coefficients onto an affine or projective linear hypersurface.

Keywords: algebraic equations, parametrization

1 Parametric versus implicit representation of solutions

Systems of algebraic equations appear in many application areas of computer algebra, eg. geometric theorem proving, robotics, chemistry, etc. There are several approaches available for carrying out the elimination theory of algebraic equations, i.e. transforming a system of algebraic equations into a triangular system, in which the variables are introduced one at a time. The most widely know approaches are resultants, Gröbner bases, and characteristic sets. Once such a triangular system has been achieved, we may encounter two basically different situations. If the solution space is zero-dimensional we can list the finitely many solutions. This approach, however, fails if the dimension of the solution space is non-zero. We propose to use a parametrized representation for this situation, i.e. the solutions are represented by a birational map with ground coefficients onto an affine or projective linear hypersurface.
For illustration let us look at two examples.

Example 1: We consider the intersection of the tacnode curve and the circle, i.e. the system of equations is

$$\begin{aligned} 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 &= 0, \\ x^2 + y^2 - 1 &= 0. \end{aligned}$$

An equivalent triangular system is

$$\begin{aligned} 3y^4 + y^3 - 3y^2 - 3y + 2 &= 0, \\ x^2 + y^2 - 1 &= 0. \end{aligned}$$

So there are exactly 4 solutions of the first equation in y, every one of which gives rise to 2 solutions in x, i.e. the number of solutions of the system is 8, counting multiplicities. In fact, as the real solutions we get

$$\begin{gathered} (0,1), \qquad (2-\text{fold}) \\ (\gamma/9, \alpha+\beta-4/9), \quad (-\gamma/9, \alpha+\beta-4/9), \end{gathered}$$

where

$$\begin{aligned} \alpha &= \sqrt[3]{233/729 + \sqrt{74}/27}, \\ \beta &= \sqrt[3]{233/729 - \sqrt{74}/27}, \\ \gamma &= \sqrt{-81\alpha^2 - 162\alpha\beta - 81\beta^2 + 72\alpha + 72\beta + 65}. \end{aligned}$$

The solution variety is 0–dimensional and the finitely many solutions can be listed explicitly. □

Example2: We consider the irreducible space curve b from the CASA sample session in [Geb91]. The defining equations for b are

$$\begin{aligned} 10y^3 - 8xy^2 - 5y^2 + 10x^2y - 8xy - 6y & \\ +6x^3 - 32x^2 + 42x - 9 &= 0, \\ 3xz - 3z + 10y^2 - 10xy + 7y + 15x^2 & \\ -28x + 6 &= 0, \\ 3yz - 3z - 2y^2 + 5xy - 5y - 6x^2 + 11x - 3 &= 0, \\ 3z^2 - 12z - 68y^2 + 80xy - 68y - 99x^2 & \\ +188x - 45 &= 0. \end{aligned}$$

*This research was supported by the *Austrian Fonds zur Förderung der wissenschaftlichen Forschung (FWF)*, Project SGC Nr. P8573-PHY, and by *FWF*, Project POSSO Nr. P9181-TEC, in cooperation with the European project (ESPRIT II) POSSO.

There are infinitely many points on b, so obviously we cannot list all the solutions. Taking z as an indetermined parameter we could, e.g. by a Gröbner basis computation, reduce the equations for b to

$$\begin{aligned}(z+2)x - 10y^2 + (3-14z)y + z^2 + 9z + 1 &= 0,\\ 50y^3 + (140z-5)y^2 + (94z^2 - 58z - 24)y & \\ -6z^3 - 74z^2 - 42z - 5 &= 0.\end{aligned}$$

However, Gröbner bases do not specialize [Wei92], so for particular values of z this triangular system might be incorrect. This problem can be overcome by further investigations, as described in [Wei92]. A more serious drawback is the fact that for determining the values of y and x corresponding to a fixed z we again have to solve a polynomial equation.
Alternatively we could determine the rational parametrization

$$\begin{aligned}x &= \frac{125t^3 + 400t^2 + 445t + 204}{2d(t)},\\ y &= \frac{5(25t^3 + 65t^2 + 23t - 27)}{2d(t)},\\ z &= -\frac{5(25t^3 + 80t^2 + 71t + 12)}{2d(t)}\end{aligned}$$

where

$$d(t) = 125t^3 + 550t^2 + 835t + 441.$$

(see [Geb91]). Such a rational parametrization gives us all but a finite number of points of the curve b, and moreover we do not have to solve polynomial equations in order to determine the values of x, y, and z corresponding to a fixed value of the parameter t. □

2 Parametrization of algebraic curves

A plane algebraic curve C over the field $\mathbf{K}$ of characteristic 0 can be represented in different ways, for instance as the set of zeros of a polynomial equation

$$C = \{(x,y) \mid 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 = 0,\ x, y \in \mathbf{C}\},$$

or as the set of values of rational functions

$$\begin{aligned}C = \{ & (\phi(t), \chi(t)) \mid \\ & \phi(t) = -\tfrac{18t^4+21t^3-7t-2}{18t^4+48t^3+64t^2+40t+9},\\ & \chi(t) = \tfrac{36t^4+84t^3+73t^2+28t+4}{18t^4+48t^3+64t^2+40t+9}, \quad t \in \mathbf{C}\}.\end{aligned}$$

We call the first representation *implicit* and the second *explicit* or *parametric*.

Definition: *The irreducible affine curve C defined by the irreducible polynomial $f(x,y) \in \mathbf{K}[x,y]$ is rational or parametrizable iff there exist rational functions $\phi(t), \chi(t) \in \mathbf{K}(t)$ such that*
(1) for almost all (i.e. for all but a finite number of exceptions) $t_0 \in \mathbf{K}$, $(\phi(t_0), \chi(t_0))$ is a point on C, and
(2) for almost every point (x_0, y_0) on C there is a $t_0 \in \mathbf{K}$ 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. □

So the curve C is parametrizable if and only if C is birationally equivalent to a line. Not every plane curve is parametrizable. The problem is to determine if a curve C can be parametrized and if so find a parametrization.

Parametrization problem:
given: an irreducible polynomial $f(x,y) \in \mathbf{K}[x,y]$ defining an irreducible affine algebraic plane curve C
decide: the rationality of C
find: (if C is rational) rational functions $\phi(t), \chi(t) \in \mathbf{K}(t)$ such that (ϕ, χ) is a rational parametrization of C. □

In [SeW91] an algebraic algorithm is described for solving the parametrization problem for any plane algebraic curve. This algorithm has been implemented in the program system CASA. An alternative approach is decribed in [Sch92]. Recently an improvement of Hilbert and Hurwitz' method [HiH90] for birationally transforming curves has been developed [SeW93], which should allow a considerable speed-up of the parametrization algorithm.
Space curves can be treated by finding a suitable birational projection to a plane curve, parametrizing the plane curve, and applying the inverse of the projection to the parametrization of the plane curve. For surfaces the problem becomes more involved. An algorithmic approach is currently under development [Sch93].

2.1 The Hilbert-Hurwitz method

We describe briefly the approach in [HiH90] to finding rational points on rational curves and also to finding parametrizations of such curves. We consider plane algebraic curves in projective space, i.e. a curve is defined by a homogeneous polynomial $F(x_1, x_2, x_3)$ in the polynomial ring $K[x_1, x_2, x_3]$. This is necessary because only when we take into account all the singularities of such a curve in projective space will we be able to parametrize the curve. However, we can always think of a projective curve as an affine curve with finitely many additional points on the line at infinity.
Let $F(x_1, x_2, x_3)$ be a homogeneous polynomial of degree d defining the rational curve C. Let H be a generic representative of a linear system of curves of degree $d-2$. If we force H to pass through every r–fold singularity on C with multiplicity $r-1$, then H is expressed in terms of $d-1$ indeterminate coefficients as

$$H = t_1\phi_1 + \ldots + t_{d-1}\phi_{d-1}, \qquad (1)$$

where the ϕ_i's are homogeneous polynomials of degree $d-2$ over the field K. I.e. H is a projective linear system of curves of degree $d-2$ and of dimension $d-2$. For arbitrary parameters $\lambda_1, \ldots, \lambda_{d-1}$ the curve

$$(\lambda_1\phi_1 + \ldots + \lambda_{d-1}\phi_{d-1})$$

intersects the curve C in the fixed singular points of C and in $d-2$ additional points depending on $\lambda_1, \ldots, \lambda_{d-1}$.
Now take three independent elements Φ_1, Φ_2, Φ_3 of the linear system H and transform F by means of

$$y_1 : y_2 : y_3 = \Phi_1 : \Phi_2 : \Phi_3 \tag{2}$$

to obtain an irreducible form $G(y_1, y_2, y_3)$ of degree $d-2$ over K. Since this transformation is rational, almost every rational point on C corresponds to a rational point on the curve C' defined by G and vice versa. Hence, the original problem is reduced to dealing with the curve C' which is also rational but of degree $d-2$. Continuing this process we finally arrive at a rational cubic or conic. From a parametrization of C' we can get a parametrization of C by applying the inverse of the rational transformation (2).
The main difficulty of this approach is that, in general $\mathcal{O}(d)$ rational transformations have to be applied in order to reduce the original curve to a cubic or conic. This renders the method all but impossible in practical applications.

2.2 A faster method

The procedure described in [SeW93] allows to construct a family of exactly $d-4$ regular points on a curve C of degree d by applying a single birational transformation. Forcing the linear system H to pass through these additional $d-4$ points results in a reduction of the dimension of the system H to 2, i.e.

$$H = t_1\phi_1 + t_2\phi_2 + t_3\phi_3. \tag{3}$$

So if we now transform the curve C by the transformation (2), we will obtain a conic C_2 which is birationally equivalent to C. A parametrization of C_2 is then subject to the inverse of the transformation (2) to get a parametrization of C.
In this process we need to compute only 2 birational transformations in contrast to $\mathcal{O}(d)$ such transformations in the original approach by Hilbert and Hurwitz.

Example 3: Let C be the curve of degree 10 defined by the the polynomial F.

$$\begin{aligned}&F(x_1,x_2,x_3) = \\ &x_1x_2^4x_3^5 + x_1x_2^5x_3^4 + x_1^2x_2^3x_3^5 + x_1^5x_2^2x_3^3 - 19x_1^2x_2^5x_3^3 \\ &-53x_2^3x_2^4x_3^3 + x_1^5x_2x_3^4 + x_1^5x_2^5 + x_1^5x_3^5 + 43x_1^3x_2^3x_3^4 \\ &+x_1^4x_2^3x_3^3 + 12x_1^4x_2^4x_3^2 + 57x_1^3x_2^5x_3^2 - 19x_1^5x_2^3x_3^2 \\ &-36x_1^4x_2^5x_3 + x_2^5x_3^5 + 21x_1^5x_2^4x_3 - 15x_1^3x_2^2x_3^5.\end{aligned}$$

The singularities of C are $P_1 = (1:1:1)$, $P_2 = (0:0:1)$, $P_3 = (1:0:0)$, $P_4 = (0:1:0)$, where P_1 is a 4–fold point and P_2, P_3, P_4 are 5–fold points.

$$\mathcal{F} = \{(1-2t : 1+2t : 1+4t)\}_{a(t)=0},$$

where $a(t) = 5984t^6 + 13936t^5 + 7808t^4 - 7240t^3 - 8762t^2 - 2965t - 327$, is a family of 6 different regular points on C. Now if we force a linear system of curves of degree 8 to pass through P_1, P_2, P_3, P_4 with mulitplicity $3, 4, 4, 4$, respectively, and through the points in $\mathcal{F}$, the resulting system is of dimension 2, i.e.

$$H(x_1, x_2, x_3) = t_1\phi_1 + t_2\phi_2 + t_3\phi_3.$$

Taking 3 curves Φ_1, Φ_2, Φ_3 in the system H and applying the birational transformation

$$\begin{aligned}y_1 &= \Phi_1(x_1, x_2, x_3),\\ y_2 &= \Phi_2(x_1, x_2, x_3),\\ y_3 &= \Phi_3(x_1, x_2, x_3),\end{aligned}$$

we arrive at the conic C_2 defined by

$$\begin{aligned}&G(y_1, y_2, y_3) = \\ &-3y_2^2 - 4y_1y_2 + y_1^2 + 8y_2y_3 + 4y_1y_3 - 5y_3^2 = 0.\end{aligned}$$

C_2 has the parametrization

$$y_1 = \frac{8t^2 - 2t}{3t^2 + 4t - 1},\ y_2 = \frac{-23t^2 + 28t - 5}{9t^2 + 12t - 3},\ y_3 = 1.$$

By an application of the inverse of the birational transformation we get the following parametrization of C:

$$x_1 = \frac{p_1(t)}{q_1(t)},\ x_2 = \frac{p_2(t)}{q_2(t)},\ x_3 = 1,$$

where

$$\begin{aligned}p_1(t) = \ & -36417t^5 + 47205t^4 - 23118t^3 + 4926t^2 \\ & -369t - 3,\\ q_1(t) = \ & 216175t^5 - 283559t^4 + 146986t^3 \\ & -37354t^2 + 4631t - 223,\\ p_2(t) = \ & 3(12139t^5 - 15735t^4 + 7706t^3 - 1642t^2 \\ & +123t + 1),\\ q_2(t) = \ & 4843t^5 + 17821t^4 - 23234t^3 + 10034t^2 \\ & -1801t + 113.\end{aligned}$$

□

3 An Example: The Offset Curve to a Parabola

Offset curves are of central interest in geometric modeling, see for instance Hoffmann [Hof89]. An offset curve consists of those points which are at a fixed distance from a given curve.
We consider the offset curve to a parabola in the sense of Farouki and Neff [FaN90]. The parabola C_P can be parametrized as

$$x = t, \quad y = t^2.$$

Imagine that a circle of radius 1 is moved along the points (t, t^2) of the parabola and intersected with the normal line $(x - t) = -2t(y - t^2)$ to the parabola at

(t, t^2). The offset curve C_O to the parabola is then defined by

$$\begin{array}{ll} (x-t)^2+(y-t^2)^2-1=0, & \text{(circle)} \\ (x-t)+2t(y-t^2)=0, & \text{(normal line)} \end{array}$$

or, after elimination of the parameter t, by the single equation

$$\begin{array}{c} 16x^6+16x^4y^2-40x^4y-47x^4-32x^2y^3+6x^2y \\ +28x^2+16y^4-40y^3+9y^2+40y-25 \\ =0. \end{array}$$

C_O turns out to be a rational curve, so we can solve this equation by expressing the x and y coordinates of a point on C_O in terms of a parameter t, e.g.

$$x(t)=\frac{p_1(t)}{q_1(t)}, \quad y(t)=\frac{p_2(t)}{q_2(t)},$$

where

$$\begin{array}{lcl} p_1(t) & = & 2(26351t^4-44574t^3+22416t^2-4514t \\ & & +321), \\ q_1(t) & = & 5(91395t^4-84364t^3+29202t^2-4492t \\ & & +259), \\ p_2(t) & = & -307089223t^6+422392458t^5 \\ & & -240991145t^4+72992460t^3 \\ & & -12376745t^2+1113738t-41543, \\ q_2(t) & = & 25(12338325t^6-17055630t^5 \\ & & +9812603t^4-3007492t^3+517883t^2 \\ & & -47502t+1813). \end{array}$$

4 References

[FaN90] R.T. Farouki, C.A. Neff, "Algebraic Properties of Plane Offset Curves", *Computer Aided Geom. Design* **7**, 101–127 (1990).

[Geb91] R. Gebauer, M. Kalkbrener, B. Wall, F. Winkler, "CASA: A Computer Algebra Package for Constructive Algebraic Geometry", *Proc. ISSAC'91*, 403–410, S.M. Watt (ed.), ACM Press (1991).

[HiH90] D. Hilbert, A. Hurwitz, "Über die Diophantischen Gleichungen vom Geschlecht Null", *Acta Math.* **14**, 217–224 (1890).

[Hof89] C.M. Hoffmann, *Geometric & Solid Modeling*, Morgan Kaufmann Publ. (1989)

[Sch92] J. Schicho, "On the Choice of Pencils in the Parametrization of Curves", *J. Symb. Comp.* **14/6**, 557–576 (1992).

[Sch93] J. Schicho, Ph.D. thesis, in progress, RISC-Linz.

[SeW91] J.R. Sendra, F. Winkler, "Symbolic Parametrization of Curves", *J. Symb. Comp.* **12/6**, 607–631 (1991).

[SeW93] J.R. Sendra, F. Winkler, "Determining Simple Points of Rational Algebraic Curves", Techn. Rep. RISC-Linz (1993)

[Wei92] V. Weispfenning, "Comprehensive Gröbner Bases", *J. Symb. Comp.* **14/1**, 1–29 (1992).