A Direct Method for Polynomial Parametrization of Curves

Josef Schicho *
RISC Linz
Johannes Kepler University, A-4040 Linz
e-mail: `Schicho@risc.uni-linz.ac.at`
www: `http://www.risc.uni-linz.ac.at/people/jschicho`

January 8, 1999

Abstract

The problem of finding polynomial parametrization of curves - if exist - can be solved by rational parametrization methods and subsequent improvement of the result. In this paper we try to give a direct approach.

1 Introduction

It is well-known that an algebraic curve has a rational parametrization if and only if it has genus zero (see [17]). There are algorithms that compute the genus and compute a rational parametrization in case the genus is zero (see [2, 13, 15, 10, 9, 14, 16]).

It is also well-known that a curve has a polynomial parametrization if and only if it has genus zero and exactly one place at infinity (see [1]). Given a rational parametrization, one can easily reparameterize so that the infinite place corresponds to the parameter $t = \infty$, and the result is a polynomial parametrization (see [11] for details).

On the other hand, polynomial parametrizations have nicer properties than just rational parametrizations. One can use these in order to obtain simpler and more efficient algorithms for implizitization (see [5, 7]). Thus, it is not satisfactory to compute polynomial parametrizations via the more complicated rational parametrizations.

In this paper, we describe an approach for a direct method for the computation of polynomial parametrization. The paper is not complete, i.e. there is an open subproblem for which we do not yet have a fast algorithm.

*supported by the Austrian Science Fund (FWF) in the frame of "Adjoints" project (P12662-TEC)

2 A Direct Approach for Polynomial Parametrization

Let k be an arbitrary field. A plane curve C is given by an irreducible polynomial equation $F(x, y) = 0, F \in k[x, y]$. The curve C is called a polynomial curve if and only if there exists a parametrization with polynomials

$$x = X(t), y = Y(t), X, Y \in k[t].$$

Example 1 The curve with equation

$$y^2 - x^2 - x^3 = 0$$

has the parametrization

$$x = t^2 - 1, y = t^3 - t^2.$$

This can be verified by plugging in:

$$(t^3 - t^2)^2 - (t^2 - 1)^2 - (t^2 - 1)^3 = 0.$$

Assuming that C is a polynomial curve, we know the existence of a regular map $\pi : \mathbf{A}^1 \to C$. Its pullback π^* is a ring homomorphism from the function ring $k[C] = k[x, y]/(F)$ to $k[\mathbf{A}^1] = k[t]$. W.l.o.g., we may assume that that π is birational, i.e. we have a proper parametrization (see [8]). Then the pullback π^* induces an isomorphism of the function fields $k(C)$ and $k(\mathbf{A}^1) = k(t)$.

Lemma 1 *The ring $k[t]$ is isomorphic to the integral closure of $k[C]$ (in its quotient field $k(C)$).*

Proof: More precisely, we will see that the field isomorphism induced by π^* maps the integral closure of $k[C]$ isomorphically to the ring $k[t]$.

First, $t \in k[t]$ is integral over $k[C]$ because it fulfils the equation $X(t) - \pi^*(x) = 0$, which has leading coefficient in k. Thus, $k[t]$ is integral over $k[C]$.

Second, $k[t]$ is integrally closed (in its quotient field). The lemma follows immediately from these two observations.

There are efficient algorithms for computing the integral closure of the function ring of a curve. The result is a k-algebra given by generators in the function field $K(C)$. We know this k-algebra R is isomorphic to $k[t]$, but we do not know an isomorphism yet. In other words, we know the ring $k[t]$ up to an isomorphism, but we do not know a generator of $k[t]$ (for instance t).

Example 2 The integral closure of the curve with equation

$$y^2 - x^2 - x^3 = 0$$

is generated by

$$1, y, x, \frac{x + x^2}{y}.$$

(This can be found by using the MAPLE function `maxorder`.)

However, if we know an element $T \in R \subset k(C)$ such that $R = k[T]$, then we have a birational map from C to the line (namely just the rational function t). The parametrization can be found by inverting this birational map (see [12]).

For any k-algebra R, the differential module $\Omega(R/k)$ is defined as the module generated by all da, $a \in R$, factoring out the rules

$$d(a + b) = da + db, d(ab) = adb + bda.$$

If R is given by generators and relations, i.e. as the quotient of a polynomial ring $k[x_1, \ldots, x_n]$ modulo an ideal generated by $F_1, \ldots, F_m \in k[x_1, \ldots, x_n]$, then $\Omega(R/k)$ is the quotient of the module generated by $dx_1, \ldots, dx_n$, modulo the relations

$$dF_1 := \frac{\partial F_1}{\partial x_1} dx_1 + \ldots + \frac{\partial F_1}{\partial x_n} dx_n = dF_2 = \ldots = dF_m = 0$$

(see [6]). In our case, when R is given by generators in the function field $k(C)$, $\Omega(R/k)$ is generated by dQ, Q a generator. The differentials dQ can be computed using the quotient rule for differentiation.

A distinguishing property of the generators of $k[t]$ is the following.

Lemma 2 *The differential module $\Omega(k[t]/k)$ is cyclic (i.e. generated by one element), and any generator is of the form $c \cdot dt$, $c \in k - \{0\}$.*

Proof: This is obvious from the formula

$$\Omega(k[t]/k) = k[t]dt.$$

Once we have a generator for $\Omega(R/k)$, it is easy to formally "integrate" it and get a generator for R. Thus, we are left with the problem of finding a generator for a given cyclic module over a given k-algebra R.

Example 3 Consider again the curve with equation

$$y^2 - x^2 - x^3 = 0.$$

We already saw that the integral closure is generated by

$$1, y, x, \frac{x + x^2}{y}.$$

The curve equation implies

$$2ydy - 2xdx - 3x^2dx = 0, \text{ hence } dy = \frac{2x + 3x^2}{2y}dx.$$

The differential module $\Omega(R/k)$ is generated by

$$dx, dy = \frac{2x + 3x^2}{2y}dx, d(\frac{x + x^2}{y}) = \frac{x}{2y}dx.$$

Now, the first two generators are actually multiples of the other two:

$$dx = \frac{2x + 2x^2}{y}(\frac{x}{2y}dx), dy = (2 + 3x)(\frac{x}{2y}dx).$$

Hence the module is indeed generated by $d(\frac{x+x^2}{y}) = \frac{x}{2y}dx$. We conclude that $\frac{x+x^2}{y}$ generates R, and the rational map

$$C \to k, (x, y) \mapsto \frac{x + x^2}{y}$$

is birational. Its inverse is the parametrization above.

It should be noted that the problem of finding a generator for a cyclic module is solved algorithmically in the homogenuous case. More general, there is an algorithm that computes a minimal generating set for a module given by generators and relations (the Macaulay script "prune" in [3], see also [4]).

References

[1] Abhyankar, S. S. *Algebraic Geometry for Scientists and Engineers.* No. 35 in Mathematical Surveys and Monographs. American Mathematical Society, Providence, Rhode Island, 1990.

[2] Abhyankar, S. S., and Bajaj, B. Automatic parametrization of curves and surfaces III. *Computer Aided Geometric Design 5-4* (1987), 309–323.

[3] Bayer, D., Stillman, M., and Stillman, M. *Macaulay User Manual.* Harvard University, 1993.

[4] Eisenbud, D. *Commutative Algebra with a View towards Algebraic Geometry.* Springer, 1994.

[5] Gao, X.-S., and Chou, S.-C. Implicitization of Rational Parametric Equations. *J. Symb. Comput. 14* (1992), pages 459–470.

[6] Hartshorne, R. *Algebraic geometry.* Springer–Verlag, 1977.

[7] Kalkbrener, M. Implicitization of Rational Curves and Surfaces. In *Lect. Notes in Comp. Sci. 508, AAECC-8* (Tokyo, Japan, Aug. 1990), Sakata, Ed.

[8] Lausch, H., and Nöbauer, W. *Algebra of polynomials*. North-Holland, 1973.

[9] Mňuk, M. *Algebraic parametrization of rational curves*. PhD thesis, RISC Linz, 1996.

[10] Mňuk, M., Sendra, J. R., and Winkler, F. On the complexity of parametrizing curves. *Beitr. Algebra und Geometrie 37/2* (1996), 309–328.

[11] Manocha, D., and Canny, J. Rational curves with polynomial parametrization. *Computer Aided Design* (1991), 12–19.

[12] Schicho, J. Inversion of rational maps with gröbner bases. In *Gröbner bases and applications* (1998), B. Buchberger and F. Winkler, Eds., Cambridge Univ. Press.

[13] Sendra, J., and Winkler, F. Symbolic parametrization of curves. *Journal of Symbolic Computation 12*, 6 (1991), 607–632.

[14] Sendra, J., and Winkler, F. Parametrization of algebraic curves over optimal field extensions. *Journal of Symbolic Computation 23*, 2/3 (1997), 191–208.

[15] van Hoeij, M. Computing parametrizations of rational algebraic curves. In *ISSAC-94* (1994), ACM Press, pp. 187–190.

[16] van Hoeij, M. Rational parametrizations of algebraic curves using canonical divisors. *Journal of Symbolic Computation 23* (1997), 209–227.

[17] Walker, R. J. *Algebraic Curves*. Springer, 1978.