Technical Report

Inversion of Birational Maps with Gröbner Bases

Josef Schicho

Research Institute for Symbolic Computation

Johannes Kepler University

A-4040 Linz, Austria

e-mail: Josef.Schicho@risc.uni-linz.ac.at

www: http://www.risc.uni-linz.ac.at/people/jschicho

(Received 16 July 1997)

We present an efficient algorithm for the inversion of a given birational map. The problem is reduced to find the unique solution of a maximal ideal defined over an algebraic function field.

1. Introduction

The problem of inverting a birational maps arises in several contexts in algorithmic algebraic geometry, and an efficient solution is useful in many situations.

For instance, consider the parameterization problem, which is useful for numerous applications in CAD/CAM (see section 3). A closer look to the existing parameterization algorithms reveals that a parameterization is often obtained via inversion of some birational map.

In this paper, we present a new efficient algorithm for the inversion of birational maps, based on the method of Gröbner bases (Buchberger, 1965; Buchberger, 1979; Buchberger, 1983; Becker and Weispfenning, 1993).

For a special case, the inversion problem has also been investigated in (van den Essen, 1990; S. Audoly and G. Bellu and A. Buttu and L. d'Angio, 1991) (see also (Ollivier, 1989) for related work), in the context of the Jacobian conjecture (Keller, 1939). The general problem was solved in (Sweedler, 1993) (see also (Shannon and Sweedler, 1988)). However, Sweedler's method depends on computing the components of the inverse map one by one, i.e. it requires the computation of a Gröbner basis with lexicographical termorder. It is known (see (Faugere *et al.*, 1993)) that such a Gröbner basis is much harder to compute than Gröbner bases with respect to other term orders (e.g. the reverse lexicographical termorder).

In this paper, we reduce the problem to the computation of the unique solution of a maximal ideal defined over some function field. Since this ideal is zero-dimensional, Gröbner bases with respect to any termorders can be computed fast (Lakshman and Lazard, 1991; Faugere *et al.*, 1993). This overweighs by far the disadvantage that the field arithmetic has become is more difficult. This holds especially when the image variety is relatively simple.

2. The Problem

Let k be a field. An affine variety is the zero set of an absolutely prime ideal (i.e. a prime ideal which remains prime over the algebraic closure) of $k[x_1,\ldots,x_m]$. Whenever we consider zero sets, we mean zeroes over the algebraic closure. By Hilbert's Nullstellensatz, the correspondence between varieties and absolutely prime ideals is one-to-one.

Problem 1:

Input: An affine variety $V\subset\mathbf{A}^m$.
A birational map $f: V\to f(V)\subset\mathbf{A}^n$.
Output: The image $W := f(V)\subset\mathbf{A}^n$.
The inverse $f^{-1}: W\to V$.

The variety V is represented by a set of polynomials in $k[x_1,\ldots,x_n]$ that generates Ideal(V).

The image of a rational map is the Zariski-closure of the set-theoretic image of the partial function f. It is again a variety (see (Shafarevich, 1974)).

3. Some Applications

There are several situations in algorithmic algebraic geometry, in which one has a variety and a rational map, and one knows that the map is birational but does not know the inverse. Here is a simple example.

EXAMPLE 3.1. Let $V=\mathbf{A}^1$, and let $f=(x^3-x,x^5-x)$. We show that the map f is birational to its image (a plane curve).

Let $K := k(F_1,F_2)\subset k(x)$. By Lüroth's theorem (see (Winter, 1974)), we know that $K=k(R)$ for some $R\in k(x)$. Degree considerations reveal that R has degree 1. (The degree of a rational function is the maximum of the degrees of numerator and generator. The degree of any rational function in $k(R)$ is a multiple of the degree of R.) All rational functions of degree 1 generate the same field, so we have $k(F_1,F_2)=k(x)$. Thus, x can be expressed as a rational function in F_1 and F_2. This rational function is the inverse of f.

The equation of the image and the inverse map can be found by computing the resultant and the first subresultant of x^3-x-y_1 and x^5-x-y_2 with respect to x (see (Hong and Schicho, 1997)). The equation of the image curve is

$$y_1^5-8y_1^2y_2+5y_1y_2^2-y_2^3+4y_2^3=0,$$

and the inverse map is

$$(y_1,y_2)\mapsto x=\frac{y_1^2y_2}{y_2^2-2y_1y_2}.$$

An important application is related to the problem of rational parameterization of surfaces, which has many applications in CAD/CAM, like reliable surface plotting and display (see (Farin, 1988)), motion display and computing transformations (see (Hoffmann, 1989), computing cutter offset curves (see (Qiulin and Davies, 1987; Arrondo *et al.*, 1997)), and many others. The reason why parameterization is important to these algorithms is that they use the NURBSs (see (Piegl and Tiller, 1997)), i.e. certain parametric representations.

The parameterization problem asks for a parameterization of an implicitly given surface, in terms of rational functions in two parameters. Not every algebraic surface has a parameterization, but those who have form an interesting and important subclass (the class of rational surfaces).

In the parameterization algorithm (Schicho, 1995; Schicho, 1997) (which is the only one working for arbitrary rational surfaces), a birational map f is constructed from the given surface to the plane. Then, a parameterization is obtained by inverting f.

Example 3.2. Let V be the surface in $\mathbf{A}^3$ with equation

$$x_1(x_2^2 - x_1x_3)(x_3^2 - x_2) + (x_1 - x_2x_3)^2 = 0.$$

Let $f : V \rightarrow \mathbf{A}^2$ be the map

$$(x_1, x_2, x_3) \mapsto (y_1, y_2) = (\frac{x_2^2 - x_1x_3}{x_1 - x_2x_3}, \frac{x_3^2 - x_2}{x_1 - x_2x_3}).$$

This map is birational, and an inverse will be constructed below. The inverse map is a parameterization of V in terms of rational functions in y_1, y_2.

In principle, one could also use the general inversion algorithm in this paper for curve parameterization. Almost any known parameterization algorithm, e.g. those in (Walker, 1978; Abhyankar and Bajaj, 1987; Sendra and Winkler, 1991; Schicho, 1992; van Hoeij, 1994; Mñuk *et al.*, 1996; Mñuk, 1996; Sendra and Winkler, 1997), first construct a certain birational function f from the given curve (even if it is not always given a name). Then, the parameterization is found by inverting f. This could be done by our general algorithm. However, experiments showed that the ad hoc methods used in most of the mentioned algorithms (based on resultant techniques) outbeat the general inversion algorithm.

4. The Algorithm

First, we observe that the problem can be reduced to the following easier problem.

Problem 2:

Input: An affine variety $V \subset \mathbf{A}^m$.
A birational polynomial map $f : V \rightarrow f(V) \subset \mathbf{A}^n$.

Output: The image $W := f(V) \in \mathbf{A}^n$.
The inverse $f^{-1} : W \rightarrow V$.

To reduce problem 1 to problem 2, we use a sort of 'Rabinovich trick' to invert the denominator by introducing a new variable.

Reduction of problem 1 to problem 2:

Reduce the rational functions defining f to the greatest common denominator D;
[Now, $f = (F_1/D, \ldots, F_n/D)$.]

$S' :=$ add $x_{m+1}D - 1$ to S;
$f' := (F_1 x_{m+1}, \ldots, F_n x_{m+1})$;
Y, $(G_1, \ldots, G_{m+1}) :=$ solve problem 2 for S', f';
return Y, $(G_1, \ldots, G_m)$;

EXAMPLE 4.1. Let V and f be as in example 3.2. Then V' is defined as the surface in $\mathbf{A}^4$ defined by the equations

$$x_1(x_2^2 - x_1x_3)(x_3^2 - x_2) + (x_1 - x_2x_3)^2 = x_4(x_1 - x_2x_3) - 1 = 0,$$

and $f' : V' \to \mathbf{A}^2$ is the polynomial map

$$(x_1, x_2, x_3, x_4) \mapsto (y_1, y_2) = ((x_2^2 - x_1x_3)x_4, (x_3^2 - x_2)x_4).$$

LEMMA 4.1. *Let $V \subset \mathrm{A}^m$ be a variety. Let $S \subset k[x_1, \ldots, x_m]$ be a set of generators for Ideal(V). Let $D \in k[x_1, \ldots, x_m]$, such that $D \notin$ Ideal(V). Then the ideal generated by S and $x_{m+1}D - 1$ in $k[x_1, \ldots, x_{m+1}]$ is absolutely prime.*

PROOF. We may assume that k is algebraically closed, and replace 'absolutely prime' by 'prime'.

The function ring $k[V] := k[x_1, \ldots, x_m]/(S)$ is an integral domain, and the canonical image $\overline{D}$ of D in A is not zero. Obviously, we have

$$k[x_1, \ldots, x_{m+1}]/(S, x_{m+1}D - 1) \cong k[V][x_{m+1}]/(x_{m+1}\overline{D} - 1).$$

This is isomorphic to the localization $D^{-1}k[V]$, which is again an integral domain. □

THEOREM 4.1. *The above reduction of problem 1 to problem 2 is correct.*

PROOF. Let V' be the variety defined by S', and let $p : V' \to V$ be the projection on the first m coordinates. Then p is birational and $f \circ p = f'$. Hence $f(V) = f'(V')$. If g is the inverse of f', then $p \circ g$ is the inverse of f. □

Suppose that $f : V \to f(V) \in \mathbf{A}^n$ is given by the polynomials $F_1, \ldots, F_n \in k[x_1, \ldots, x_n]$. It is known how to compute the equations of $f(V)$: we have to eliminate the variables $x_1, \ldots, x_m$ in the system

$$S \cup \{y_1 - F_1, \ldots, y_n - F_n\}.$$

(Here $y_1, \ldots, y_n$ are new variables, forming a system of coordinates for $\mathbf{A}^n$.)

Algorithm *ComputeImage*:
Input: A finite set $S \subset k[x_1, \ldots, x_m]$, representing a variety V in A^m.
An n-tuple $(F_1, \ldots, F_n) \in k[x_1, \ldots, x_m]^n$,
representing a polynomial map f into A^n.
Output: A Gröbner bases for Ideal($f(V)$).
$T := S \cup \{y_1 - F_1, \ldots, y_n - F_n\}$;
$\prec :=$ a termorder such that each x_i is greater than any monomial in $y_1, \ldots, y_n$;
$G :=$ a Gröbner basis of T w.r.t. $\prec$;
$G' := G \cap k[y_1, \ldots, y_n]$;
return G';

THEOREM 4.2. *The algorithm ComputeImage is correct.*

PROOF. See (Cox *et al.*, 1992). The essential point of the proof is the elimination property of Gröbner bases (see (Buchberger, 1985)). □

Note that we can sometimes skip this step, namely if we already know that the image variety is the whole $\mathbf{A}^n$ (e.g. for computing parameterizations).

To compute the inverse map, we do arithmetic in the function field $k(W)$. Its elements are represented by fractions (F/G) of polynomials in $k[y_1, \ldots, y_n]$, such that $G \notin \mathrm{Ideal}(V)$. Since we are equipped with a Gröbner basis of Ideal(V), we can test for zero, by deciding whether $F \in \mathrm{Ideal}(V)$. (It will never be necessary to decide ideal membership of denominators, because all fractions in our computation arise by addition, multiplication, and division by nonzero elements, starting with a set of integral elements.)

We have a canonical homomorphism

$$\phi : k[x_1, \ldots, x_m] \to k(W)$$

with kernel Ideal(W). In the following, we will denote the canonical images by overlining.

LEMMA 4.2. *If f is birational, then the ideal I generated by S and $\overline{y_1} - F_1, \ldots, \overline{y_n} - F_n$ is an absolutely maximal ideal in $k(W)[x_1, \ldots, x_m]$ (i.e. a maximal ideal which remains maximal over the algebraic closure of $k(W)$). The inverse of f is represented by the unique zero in $(G_1, \ldots, G_m) \in k(W)^m$.*

PROOF. Note that $P_g := (\overline{y_1}, \ldots, \overline{y_n})$ is a generic point of W, i.e. a point defined over some field extension with the property that $F(P_g) = 0$ implies $F \in \mathrm{Ideal}(W)$ for all $F \in k[y_1, \ldots, y_m]$. The zeroes of the ideal I form the inverse image of the generic point. Since f is birational, the inverse image of a generic point consists of exactly one point, which lies a priori in the algebraic closure of $k(W)$.

Let $g : W \to V$ be the inverse of f, represented by $(G_1, \ldots, G_m) \in k(W)^m$. Then $f \circ g = \mathrm{id}_W$ implies $f(G_1, \ldots, G_m) = P_g$.

Now, we have to show that I is absolutely maximal. Since I has exactly one zero over the algebraic closure, it is zero-dimensional. Since the unique zero is defined over the field $k(W)$, the ideal I is a primary ideal, and its associated prime ideal is absolutely maximal. It remains to show that I is prime.

Let I' be the ideal in $k[W][x_1, \ldots, x_m] = k[x_1, \ldots, x_m, \overline{y_1}, \ldots, \overline{y_n}]$ generated by S and $\overline{y_1} - F_1, \ldots, \overline{y_n} - F_n$. It is a prime ideal, because the quotient is an integral domain (isomorphic to $k[V]$). Let S' be the set of all nonzero elements in $k[W]$. Then $k(W)[x_1, \ldots, x_m]$ is the localization of $k[W][x_1, \ldots, x_n]$ at S', and I is the extension of I'. Moreover, S' is disjoint from I'. Then, primality of I follows from the lemma below. □

LEMMA 4.3. *Let A be a Noetherian integral domain, let I be a prime ideal, and let S be a multiplicative set disjoint from I. Then $S^{-1}I$ is prime in $S^{-1}A$.*

PROOF. Let a/s_1, b/s_2 be two fractions such that their product is in $S^{-1}I$. Because I is finitely generated, there is an element $s_3 \in S$ such that $s_3 ab \in I$. Now, I is prime, and s_3 is not in I, hence either a or b is in I, and the lemma follows. □

If I is a maximal ideal in $k[x_1, \ldots, x_m]$ with a solution defined over k, then a reduced Gröbner bases of I has the shape

$$\{a_1x_1 + b_1, \ldots, a_mx_m + b_m\}$$

for some $a_1, \ldots, a_m \in k - \{0\}$, $b_1, \ldots, b_m \in k$, regardless of the term order (see (Becker and Weispfenning, 1993)). Therefore, it is trivial to find the solution once we have the Gröbner basis.

Algorithm *InvertMap*:
Input: A finite set $S \subset k[x_1, \ldots, x_m]$, representing a variety V in A^m.
Input: A finite set $T \subset k[y_1, \ldots, y_n]$, representing a variety W in A^n.
An n-tuple $(F_1, \ldots, F_n) \in k[x_1, \ldots, x_m]^n$,
representing a birational polynomial map f to W.
Output: An m-tuple $(G_1, \ldots, G_m) \in k[y_1, \ldots, y_n]^m$, representing the inverse f^{-1}.
$S' := S \cup \{y_1 - F_1, \ldots, y_n - F_n\}$;
$S'' :=$ compute a Gröbner basis of S' over $k(W)$;
$(G_1, \ldots, G_n) :=$ solve S'' (trivial);
return $(G_1, \ldots, G_n)$

Example 4.2. Let V and f be as V' and f' in example 4.1. We compute a Gröbner basis of the set

$$S' := \{x_1(x_2^2 - x_1x_3)(x_3^2 - x_2) + (x_1 - x_2x_3)^2, x_4(x_1 - x_2x_3) - 1, (x_2^2 - x_1x_3)x_4 - y_1,$$
$$(x_3^2 - x_2)x_4 - y_2\}$$

with total degree order, where y_1 and y_2 are regarded as constants. The result is

$$S'' = \{(y_2y_1^2 - y_1)x_2 + y_1^3 + 1, y_1y_2x_1 + 1, (y_2y_1^2 - y_1)x_3 - y_2 - y_1^2,$$
$$(y_2y_1^5 - y_1 + 3y_2y_1^2 + y_2^2)x_4 - y_2^3y_1^4 + 2y_2^2y_1^3 - y_2y_1^2\}.$$

Therefore, the solution is

$$(G_1, G_2, G_3, G_4) = (\frac{-1}{y_1y_2}, \frac{-y_1^3 - 1}{y_2y_1^2 - y_1}, \frac{y_2 + y_1^2}{y_2y_1^2 - y_1}, \frac{y_2^3y_1^4 - 2y_2^2y_1^3 + y_2y_1^2}{y_2y_1^5 - y_1 + 3y_2y_1^2 + y_2^2}).$$

This is a representation of the inverse map $f^{-1} : \mathbf{A}^2 \to V$. The first three components form a parameterization of the surface in example 3.2 (see also example 4.1).

Theorem 4.3. *The algorithm Invertmap is correct.*

Proof. Obvious from lemma 4.2. □

References

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

Arrondo, E., Sendra, J., Sendra, J. R. (1997). Parametric generalized offsets to hypersurfaces. *Journal of Symbolic Computation*, **23**:267–285.

Becker, T., Weispfenning, V. (1993). *Gröbner bases - a computational approach to commutative algebra.* Graduate Texts in Mathematics. Springer Verlag, New York, Berlin, Heidelberg.

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal.* PhD thesis, Universitat Innsbruck, Institut fur Mathematik. German.

Buchberger, B. (1979). A criterion for detecting unnecessary reductions in the construction of Grobner bases. In *Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation.* Springer-Verlag.

Buchberger, B. (1983). A note on the complexity of constructing Grobner-bases. In *Lecture Notes in Computer Science - Proc. EUROCAL '83.* Springer-Veralg.

Buchberger, B. (1985). Groebner bases: An algorithmic method in polynomial ideal theory. In Bose, N. K., editor, *Recent Trends in Multidimensional Systems Theory*, chapter 6. D. Riedel Publ. Comp.

Cox, D., Little, J., ÓShea, D. (1992). *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer Verlag, New York, Berlin, Heidelberg.

Farin, G. F. (1988). *Curves and Surfaces for Computer Aided Geometric Design: A practical guide.* Academic Press, New York.

Faugere, J., Gianni, P., Lazard, D., Mora, T. (1993). Efficient Computation of Zero-dimensional Groebner Bases by Change of Ordering. *Journal of Symbolic Computation*, **16**:329–344.

Hoffmann, C. M. (1989). *Geometric and Solid Modelling – an Introduction.* Morgan Kauffmann Publisher, San Mateo, California.

Hong, H., Schicho, J. (1997). Algorithms for trigonometric curves. *Journal of Symbolic Computation.* submitted as # 1629.

Keller, O. (1939). Ganze cremona transformationen. *Monatsh. Math. Phys.*, **47**:299–306.

Lakshman, Y. N., Lazard, D. (1991). On the complexity of zero-dimensional algebraic systems. In *Proceedings MEGA'90*, pages 217–225. Birkhäuser.

Mñuk, M. (1996). *Algebraic parametrization of rational curves.* PhD thesis, RISC Linz.

Mñuk, M., Sendra, J. R., Winkler, F. (1996). On the complexity of parametrizing curves. *Beitr. Algebra und Geometrie*, **37/2**.

Ollivier, F. (1989). Inversibility of rational mappings and structural identifiability in automatics. *ISSAC-89*, pages 43–54.

Piegl, L., Tiller, W. (1997). *The NURBS book.* Springer.

Qiulin, D., Davies, B. J. (1987). *Surface engineering geometry for computer-aided design and manufacture.* John Wiley.

S. Audoly and G. Bellu and A. Buttu and L. d'Angio (1991). Procedures to investigate injectivity of polynomial maps and compute the inverse. *Applicable Algebra in Engineering, Communication and Computing*, **2**:91–103.

Schicho, J. (1992). On the choice of pencils in the parametrization of curves. *Journal of Symbolic Computation*, **14**(6):557–576.

Schicho, J. (1995). *Rational parametrization of surfaces.* PhD thesis, RISC Linz.

Schicho, J. (1997). Rational parameterization of surfaces. *Journal of Symbolic Computation.* submitted as # 1586.

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

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

Shafarevich, I. R. (1974). *Algebraic geometry.* Springer.

Shannon, D., Sweedler, M. (1988). Using gröbner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence. *Journal of Symbolic Computation*, **6**(2/3):267–273.

Sweedler, M. (1993). Using Gröbner bases to determine the algebraic and transcendental nature of field extensions. *Applicable Algebra in Engineering, Communication and Computing*, **10**:66–75.

van den Essen, A. (1990). A criterion to decide if a polynomial map is invertible and to compute the inverse. *Comm. Alg.*, **18**(10):3183–3186.

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

Walker, R. J. (1978). *Algebraic Curves.* Springer-Verlag, New York, Berlin, Heidelberg.

Winter, D. J. (1974). *The structure of fields.* Springer.