MM Research Preprints,23–29
No. 18, Dec. 1999. Beijing

Computations with Differential Rational Parametric Equations[1)]

Xiao-Shan Gao
Institute of Systems Science
Academia Sinica, Beijing, 100080

Abstract. This paper studies several computational problems about differential rational parametric equations. We present a method of implicitization for general differential rational parametric equations. We also present a method to decide whether the parameters of a set of parametric equations are independent, and if not, re-parameterize the parametric equations so that the new parametric equations have independent parameters. We give a method to compute the inversion maps of differential parametric equations, and as a consequence, we can decide whether the parametric equations are proper. A method to find a proper re-parameterization for a set of improper parametric differential equations of differential variety of dimension one is presented.

1. Introduction

Study of rational algebraic varieties and the corresponding rational parametric equations is a classic topic in algebraic geometry. The recent extensive study of this problem is focused on finding algorithms that can transform between the implicit representation and parametric representation of rational varieties [**?**, **?**, **?**, **?**], because these algorithms have applications in *solid modeling*.

On the other hand, much of the *differential algebra*[**?**, **?**, **?**, **?**, **?**], classic and new, or the *differential algebraic geometry* named by Wu [**?**] can be regarded as a generalization of the algebraic geometry theory to analogous theory for algebraic differential equations. However, considerable parts of the results in algebraic geometry have yet to be extended to differential case. This paper will consider some computation issues related to the implicitization of differential rational parametric equations (DRPEs). Two examples of DRPEs are

$$\begin{aligned} &x = u^2, \quad y = u' \text{ and} \\ &x = u, \quad\ \ y = au + b \end{aligned}$$

where x and y are indeterminates; u is the parameter, and a and b are arbitrary constants. It is easy to check that these two DRPEs are the parametric representation for differential varieties defined by the following differential equations.

$$\begin{aligned} &x'^2 - 4xy^2 = 0 \text{ and} \\ &x'y'' - x''y' = 0. \end{aligned}$$

[1)] This work is supported by CNSF under an outstanding youth grant (NO. 69725002) and by a “973” project.

It is clear that if a differential variety has a parametric representation then we have a method of generating all of its solutions.

In this paper, we solve the following problems related to a set of DRPEs. (1) To find a characteristic set for the implicit prime ideal (definition in Section **??**) determined by a set of DRPEs. (2) To find a canonical representation for the image (definition in Section **??**of a set of DRPEs. (3) To decide whether the parameters of a set of DRPEs are independent, and if not, to re-parameterize the DRPEs so that the new DRPEs have independent parameters. (4) To compute the inversion maps of a set of DRPEs, and as a consequence, to decide whether a set of DRPEs is proper. If the implicit variety is of dimension one and the DRPEs are not proper, to find a proper re-parameterization for the given DRPEs. This is based on a constructive proof of the differential Lüroth's theorem.

Two problems remain open: to find a basis for the implicit prime ideal of a set of DRPEs and to decide whether an implicitly given differential variety is rational, and if it is, to find a set of DRPEs for it.

The rest of this paper is organized as follows. In Section 2, we show how to compute the characteristic set for the implicit ideal of a set of DRPEs. In Section 3, we show how to compute the image of a set of DRPEs. In Section 4, we treat the independency of the parameters. In Section 5, we show how to compute the inversion maps of a set of DRPEs.

2. The implicit ideal of a set of DRPEs

Let $\mathbf{K}$ be a (ordinary) differential field of characteristic zero, e.g., $\mathbf{Q(t)}$, $\mathbf{E}$ an extension field of $\mathbf{K}$, and $x_1, x_2, \cdots, y_1, y_2, \cdots, u_1, u_2, \cdots$ indeterminates over E. We denote by $x_{i,j}$ the j-th derivation of x_i. We use $\mathbf{K}\{x_1, \cdots, x_n\}$ or $\mathbf{K}\{X\}$ to denote the ring of differential polynomials (d-pols) in the indeterminates $x_1, \cdots, x_n$. Unless explicitly mentioned otherwise, all d-pols in this paper are in $\mathbf{K}\{X\}$. For a d-pol set PS, let

$$\text{Zero}(PS) = \{x = (x_1, \cdots, x_n) \in E^n \mid \forall P \in PS, P(x) = 0\}.$$

For two d-pol sets PS and DS, we define $\text{Zero}(PS/DS) = \text{Zero}(PS) - \cup_{d \in DS}\text{Zero}(d)$.

Let $u_1, \cdots, u_m$ be indeterminates over $\mathbf{E}$. For nonzero d-pols $P_1, \cdots, P_n, Q_1, \cdots, Q_n$ in $\mathbf{K}\{u_1, \cdots, u_m\}$, or $\mathbf{K}\{U\}$, we call

$$x_1 = \frac{P_1(u)}{Q_1(u)}, \ \cdots, \ x_n = \frac{P_n(u)}{Q_n(u)} \tag{2.1}$$

a set of *differential rational parametric equations* (DRPE). We assume that not all $P_i(u)$ and $Q_i(u)$ are constants and $gcd(P_i(u), Q_i(u)) = 1$.

The *implicit ideal* of (2.1) is defined as

$$\text{ID}(P, Q) = \{P \in \mathbf{K}[x_1, \cdots, x_n] \mid P(P_1/Q_1, \cdots, P_n/Q_n) \equiv 0\}.$$

$\text{Zero}(ID(P, Q))$ is called the *implicit variety* of (2.1). It is clear that $\text{ID}(P, Q)$ is a prime ideal with generic zero $(P_1/Q_1, \cdots, P_n/Q_n)$. Then its dimension equals to the transcendental degree of $\mathbf{K}(P_1/Q_1, \cdots, P_n/Q_n)$ over $\mathbf{K}$.

We may use Wu-Ritt's zero decomposition theorem [**?**] to obtain a characteristic set (CS) for the implicit ideal. Using the same notations introduced above, let

$$PS = \{F_1 = P_1 - x_1Q_1, \cdots, F_n = P_n - x_nQ_n\}$$

and $DS = \{Q_1, \cdots, Q_n\}$. Since PS is of triangular form under the variable order $u_1 < \cdots < u_m < x_1 < \cdots < x_n$, we may define

$$PD(PS) = \{P \in \mathbf{K}\{U, X\} | \text{prem}(P, PS) = 0\}.$$

Lemma 2.1 *$PD(PS)$ is a prime ideal of dimension m and $PD(PS) \cap \mathbf{K}\{X\}$ is the implicit ideal of (2.1).*

Proof. Under the variable order $u_1 < \cdots < u_m < x_1 < \cdots < x_n$, PS is an ascending chain whose leading variables have degree one. So it is an irreducible ascending chain and $PD(PS)$ is a prime ideal with a generic zero $\eta = (U, P_1/Q_1, \cdots, P_n/Q_n)$ (for definition see [**?**, **?**]). The dimension of $PD(PS)$ is the transcendental degree of η over E, which is m. Since $ID(P, Q)$ has $(P_1/Q_1, \cdots, P_n/Q_n)$ as its generic zero, we have $ID(P, Q) \subset PD(PS) \cap \mathbf{K}\{X\}$.. The other direction is obvious. ∎

Lemma 2.2

$$\text{Zero}(PS/DS) = \text{Zero}(PD(PS)/DS) = \text{Zero}(ID(P, Q)/DS)$$

Proof. The first equation is true because DS contains the initials and separants (see [**?**] for definition) of PS as an ascending chain under the variable order $u_i < x_i$. The second equation comes from Lemma **??**. ∎

By the zero decomposition method [**?**], we can find an irreducible ascending chain ASC under a new variable order $x_1 < \cdots < x_n < u_1 < \cdots < u_m$ such that

$$\text{Zero}(PS/DS) = \text{Zero}(PD(ASC)/DS). \tag{2.2}$$

ASC has the same dimension m as PS. Hence ASC contains n d-pols. By changing the order of the variables properly, we may assume ASC to be

$$\begin{array}{l} A_1(x_1, \cdots, x_{d+1}), \cdots, A_{n-d}(x_1, \cdots, x_n), \\ B_1(x_1, \cdots, x_n, t_1, \cdots, t_{s+1}), \cdots, B_{m-s}(x_1, \cdots, x_n, t_1, \cdots, t_m) \end{array} \tag{2.3}$$

where $d + s = m$. The *parameter set* of ASC is $\{x_1, \cdots, x_d,\ t_1, \cdots, t_s\}$.

Theorem 2.3 *The implicit ideal of (2.1) is $PD(A_1, \cdots, A_{n-d})$.*

Proof. This is a consequence of Lemmas **??** and **??**. ∎

How to compute a basis for the implicit prime ideal is open.

3. The image of a set of DRPEs

The *image* of (2.1) in E^n is

$$IM(P, Q) = \{(x_1, \cdots, x_n) \in E^n \mid \exists \tau \in E^m (x_i = P_i(\tau)/Q_i(\tau))\}.$$

Lemma 3.1 *We can find differential d-pol sets PS_i and differential d-pols d_i, $i = 1, \cdots, t$, such that*

$$IM(P, Q) = \cup_{i=1}^{t} \text{Zero}(PS_i/\{d_i\}). \tag{3.1}$$

Proof. It is obvious that $IM(P,Q) = \{(x_1,\cdots,x_n) \mid \exists\tau \in E^m(Q_i(\tau)x_i - P_i(\tau) = 0 \wedge Q_i(\tau) \neq 0)\}$. Thus by the quantifier elimination theories for an differential closed field [**?**, **?**, **?**], we can find PS_i and d_i such that (3.1) is correct. ∎

The following result describes the relation between the image and the implicit variety of a set of DRPEs and a canonical representation for the image.

Theorem 3.2 *Let V be the implicit variety of (2.1) and d the dimension of V. Then*

(1) $IM(P,Q) \subset V$;

(2) $V - IM(P,Q)$ is a quasi variety with dimension less than d or with dimension d but with order less than of V; and

(3) We can find irreducible ascending chains ASC, ASC_i such that

$$IM(P,Q) = \mathrm{Zero}(PD(ASC)) - \cup_{i=1}^{k}\mathrm{Zero}(ASC_i/J_iD_i),$$

where J_i are the initial-separant-products (IS-products) of ASC_i and D_i are d-pols. We also have: (a) $PD(ASC)$ is the implicit ideal of (2.1); (b) $\mathrm{Zero}(ASC_i/J_iD_i) \subset \mathrm{Zero}(PD(ASC))$.

Proof. (1) is s consequence of Lemma **??**. (2) is a consequence of (3) and the dimension theorem in [**?**]. We need only prove (3). By Lemma **??**, we can find d-pols sets PS_i and d-pols d_i in $\mathbf{K}\{X\}$ such that

$$IM(P,Q) = \cup Zero(PS_i/DS_i).$$

By Wu-Ritt's zero decomposition algorithm[**?**], we further assume

$$IM(P,Q) = \cup Zero(ASC_i/d_iJ_i) \qquad (3.2)$$

where ASC_i are irreducible ascending chains and J_i are the IS-products of ASC_i. Let ASC_1 be an ascending chain containing least number of d-pols and with the lowest order among the ASC_i. Then $Zero(ASC_1/d_1J_1)$ is a component with maximal dimension and order in decomposition (3.2). By Lemma **??**, the implicit variety of (2.1) is $\mathrm{Zero}(PD(ASC_1))$. Then by (1) $\mathrm{Zero}(ASC_i/d_iJ_i) \subset IM(P,Q) \subset \mathrm{Zero}(PD(ASC_1))$ for all i. By the remainder formula for the pseudo remainder, $Zero(ASC_1/J_1) = Zero(PD(ASC_1)/J_1)$. Then

$$\begin{aligned} IM(P,Q) &= Zero(PD(ASC_1)/d_1J_1)\bigcup \cup Zero(ASC_i/d_iJ_i)\\ &= (Zero(PD(ASC_1)) - Zero(\{d_1J_1\}))\bigcup \cup Zero(ASC_i/d_iJ_i). \end{aligned}$$

Since $Zero(ASC_i/d_iJ_i) \subset Zero(PD(ASC_1))$, we also have $IM(P,Q) = Zero(PD(ASC_1)) - W$ where

$$\begin{aligned} W &= Zero(PD(ASC_1) \cup \{d_1J_1\}) - \cup_{i\geq 2}\mathrm{Zero}(ASC_i/d_iJ_i))\\ &= \cap_i(\mathrm{Zero}(PD(ASC_1) \cup \{d_1J_1\}) - \mathrm{Zero}(ASC_i/d_iJ_i))\\ &= \cap_i[(\mathrm{Zero}(PD(ASC_1) \cup \{d_1J_1\}) - \mathrm{Zero}(ASC_i)) \cup \mathrm{Zero}(\{d_iJ_i\} \cup \{d_1J_1\} \cup ASC_i)]. \end{aligned}$$

Using the following formula

$$Zero(PS_1/DS_1) \cap Zero(PS_2/DS_2) = Zero(PS_1 \cup PS_2/DS_1 \cup DS_2)$$

W can be written as $\cup_j Zero(RS_j/TS_j)$ for finite d-pol sets RS_j and TS_j. Using Ritt-Wu's decomposition again, we obtain the desired formula. ∎

4. Independent parameters

The parameters $u_1, \cdots, u_m$ of DRPEs (2.1) are called *independent* if the implicit ideal of (2.1) is of dimension m, or equivalently the transcendental degree of the field $\mathbf{K}(P_1/Q_1, \cdots, P_n/Q_n)$ over $\mathbf{K}$ is m.

Lemma 4.1 *Suppose that we have constructed (2.3). Then the transcendental degree of* $K' = \mathbf{K}(P_1/Q_1, \cdots, P_n/Q_n)$ *over* $\mathbf{K}$ *is* $d = m - s > 0$. *Therefore, the parameters are independent iff* $s = 0$.

Proof. The dimension of a prime ideal equals to the number of parameters of its characteristic set. Then the result comes from Theorem **??**. ∎

Theorem 4.2 *If the parameters of (2.1) are not independent then we can find a set of new DRPEs*

$$x_1 = P_1'/Q_1', \cdots, x_n = P_n'/Q_n' \tag{4.1}$$

which has the same implicit variety as (2.1) but with independent parameters.

Proof. Since (2.3) is irreducible, we may assume that the IS-products J_j of (2.3) are d-pols reduced with (2.3) free of the leads of the d-pols in (2.3). Since Q_i is not in $ID(P, Q)$, we can find a nonzero d-pol q_i reduced with (2.3) free of the leading variables of the d-pols in (2.3). such that

$$q_i \in Ideal(A_1, \cdots, A_{n-d}, B_1, \cdots, B_{m-s}, Q_i).$$

Let $M = \prod_{i=1}^{m-s} I_i \cdot \prod_{j=1}^{n} q_j$. Then M is a d-pol reduced with (2.3) free of the leads of the d-pols in (2.3). M is of lower order than that of A_j for each leading variable of A_i. Then there exist $h_1, \cdots, h_s$ in $\mathbf{E}$ such that when replacing t_i by h_i, $i = 1, \cdots, s$, M becomes a nonzero d-pol of X. Let P_i' and Q_i' be the d-pols obtained from P_i and Q_i by replacing t_i by h_i, $i = 1, \cdots, s$. Now we have obtained (4.1). M becomes a nonzero d-pol of X. The new DRPEs define the same implicit ideal, because by the selection of the h_i, after the substitution, (2.3) is still a CS of Zero$(\{F_1', \cdots, F_n'\}/\{Q_1', \cdots, Q_n'\})$. ∎

5. Inversion maps and proper parametric equations

The *inversion problem* is that given a point $(a_1, \cdots, a_n)$ on the image of (2.1), find a set of values $(\tau_1, \cdots, \tau_m)$ for the u such that

$$a_i = P_i(\tau_1, \cdots, \tau_m)/Q_i(\tau_1, \cdots, \tau_m), i = 1, \cdots, n.$$

This problem can be reduced to a differential equation solving problem. In the following, we show that in certain cases, we can find a closed form solution to the inversion problem.

Inversion maps for (2.1) are functions

$$t_1 = f_1(x_1, \cdots, x_n), \cdots, t_m = f_m(x_1, \cdots, x_n)$$

such that $x_i \equiv P_i(f_1, \cdots, f_m)/Q_i(f_1, \cdots, f_m)$ are true on the implicit variety V of (2.1) except for a proper subset of V.

The inversion problem is closely related to whether a set of parametric equations is proper. DRPEs (2.1) are called *proper* if for each $(a_1, \cdots, a_n) \in IM(P,Q)$ there exists only one $(\tau_1, \cdots, \tau_m) \in E^m$ such that $a_i = P_i(\tau_1, \cdots, \tau_m)/Q_i(\tau_1, \cdots, \tau_m)$, $i = 1, \cdots, n$. Let us assume that the parameters $u_1, \cdots, u_m$ of (2.1) are independent, i.e., $s = 0$. Then (2.3) becomes

$$
\begin{array}{l}
A_1(x_1, \cdots, x_{m+1}) \\
\cdots \\
A_{n-m}(x_1, \cdots, x_n) \\
B_1(x_1, \cdots, x_n, t_1) \\
\cdots \\
B_m(x_1, \cdots, x_n, t_1, \cdots, t_m)
\end{array} \tag{5.1}
$$

Theorem 5.1 *Using the above notations, we have*

(a) $B_i(x, t_1, \cdots, t_i) = 0$ determine t_i $(i = 1, \cdots, m)$ as functions of $x_1, \cdots, x_n$ which are a set of inversion maps for (2.1).

(b) (2.1) is proper if and only if $B_i = I_i t_i - U_i$ are linear in t_i for $i = 1, \cdots, m$, and if this is case, the inversion maps are

$$t_1 = U_1/I_1, \cdots, t_m = U_m/I_m$$

where the I_i and U_i are d-pols in $\mathbf{K}\{X\}$.

Proof. Let M be the IS-product of (5.1). Let $x' = (x'_1, ..., x'_n)$ be a zero on the implicit variety V of (2.1) such that $M(x') \not\equiv 0$. Then we can show that $B_i(x', t_1, ..., t_i) = 0$, $i = 1, ..., m$, determine a set of values $t' = (t'_1, ..., t'_m)$ for the t_i s.t. $Q_i(t') \neq 0$. Thus $F_h(t', x') = P_h(t')x'_h - Q_h(t') = 0$, i.e., $x'_h = P_h(t')/Q_h(t')$. Note that $Zero(M) \cap V$ is a proper subset of V, we have proved (a).

To prove (b), first note that the $B_i = 0$ $(i = 1, ..., m)$ are the relations between the x and $t_1, ..., t_i$ in ID' which have the lowest degree in t_i. Also different solutions of $B_i = 0$ for the same x give same value for the x_i. Since (5.1) is an irreducible ascending chain, for a generic zero x' on the implicit variety V, $B_i(x', t_1, ..., t_i) = 0$, $i = 1, ..., m$, have no multiple roots for the t_i. Therefore a point $x \in IM(P,Q)$ corresponds to one set of values for t_i iff B_i are linear in t_i, $i = 1, ..., m$. Let $B_i = I_i t_i - U_i$ where I_i and U_i are in $\mathbf{K}\{X\}$ then the inversion maps are $t_i = U_i/I_i$, $i = 1, ..., m$. ∎

Theorem 5.2 *If $m = 1$ and DRPEs (2.1) are not proper, we can find a new parameter $s = f(t_1)/g(t_1)$ where f and g are in $\mathbf{K}\{t_1\}$ such that the re-parameterization of (2.1) in terms of s,*

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ \cdots, \ x_n = \frac{F_n(s)}{G_n(s)} \tag{5.2}$$

are proper.

Proof. Let $K' = \mathbf{K} < P_1/Q_1, \cdots, P_n/Q_n >$ be the differential extension field of $\mathbf{K}$ by adding $P_1/Q_1, \cdots, P_n/Q_n$. Since $P_1(t_1) - Q_1(t_1)l = 0$ where $l = P_1(t_1)/Q_1(t_1) \in K'$, t_1 is algebraic over K'. Let $f(y) = a_r y^r + \cdots + a_0$ be an irreducible d-pol in $K'\{y\}$ for which $f(t_1) = 0$.

Then at least one of a_i/a_r, say $\eta = a_s/a_r$, is not in $\mathbf{K}$. By a proof of Lüroth's theorem [**?**], we have $K' = \mathbf{K}(\eta)$. This means that $x_i = P_i/Q_i$ can be expressed as rational functions of η and η also can be expressed as a differential rational function of $x_i = P_i/Q_i$, i.e., there is a one-to-one correspondence between the values of the $x_i = P_i/Q_i$ and η. Therefore η is the new parameter we seek. To compute η, by Theorem **??**, we can find an inversion map $B_1(x_1, \cdots, x_n, t_1) = 0$ of the curve. Then $B_1'(y) = B_1(P_1/Q_1, \cdots, P_n/Q_n, y) = 0$ is a d-pol in $K'\{y\}$ with lowest degree in y such that $B_1'(t_1) = 0$, i.e., $B_1'(y)$ can be taken as $f(y)$. So s can be obtained as follows. If B_1 is linear in t_1, nothing needs to be done. Otherwise let

$$B_1 = b_r t_1^r + \cdots + b_0$$

where the b_i are in $\mathbf{Q}[x]$. By (2.1), b_i can also be expressed as differential rational functions $a_i(t_1)$, $i = 1, \cdots, r$. At least one of a_i/a_r, say a_0/a_r, is not an element in $\mathbf{Q}$. Let $s = a_0/a_r$. Eliminating t_1 from (2.1) and $a_r s - a_0$, we can get (5.2). Note that a_i comes from b_i by substituting x_j by P_j/Q_j, $j = 1, \cdots, n$, then $s = b_0/b_r$ is an inversion map of (5.2). ∎

References

[1] S.S. Abhyankar and C. Bajaj, Automatic parameterization of rational curves and surfaces, III: algebraic plane curves, *Comp. Aided Geo. Design*, **5**, 309-321, 1988.

[2] B. Buchberger, Applications of Gröbner bases in non-linear computational geometry, L.N.C.S. No 296, R.JanBen (Ed.), pp. 52–80, Springer-Verlag, 1987.

[3] F. Boulier, D. Lazard, F. Ollivier and M. Petitot, Representation for the Radical of a Finitely Generated Differential Ideal, in Levelt, A.H.M (ed): Proc. ISSAC'95, ACM Press, 158-166, 1995.

[4] A. L. Chistov and D. Yu Grigor'ev. (1990), Complexity of Quantifier Elimination in the Theory of Ordinary Differential Equations, Preprint, 1990.

[5] Gao, X. S. and Chou S.C. (1992a): Implicitization of rational parametric equations, *Journal of Symbolic Computation*, **14**, 459–470.

[6] X.S. Gao and S.C. Chou, A Zero Structure Theorem for Differential Parametric Systems, *Journal of Symbolic Computation*, vol. 16, p. 585-595, 1994.

[7] C.M. Hoffmann, *Geometric and solid modeling: an introduction*, Morgan Kaufmann Publishers Inc, 1989.

[8] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, 1973.

[9] J. F. Ritt, *Differential algebra*, Amer. Math. Sco. Colloquium, (1950).

[10] T. W. Sederberg, D. C. Anderson, D. C. and R. N. Goldman, Implicit representation of parametric curves and surfaces, *Computer Vision, Graph, Image Proc.*, **28**, 72–84, 1984.

[11] A. Seidenberg, An Elimination Theory for Differential Algebra, *Univ. California Publication in Math.*, 3 (1956), 31-65.

[12] J.R. Sendra and F. Winkler, Symbolic parameterization curves, *J. of Symbolic Computation*, **12**, 607–632, 1991.

[13] A. Rosenfeld, Specilization in Differential Algebra, *Trans. Amer. Math. Soc.*, 1959, **90**, 394-407.

[14] W.T. Wu, Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.*, 4(1984), 207 –235, Re-published in *J. Automated Reasoning*, 1986.

[15] W.T. Wu, W.T. Wu, On the Foundation of Algebraic Differential Geometry. Math. Mech. Res. Preprints, Inst. of Sys. Sci., no. 3, pp. 1–26, 1989.