Article Submitted to Journal of Symbolic Computation

Implicitization for Differential Rational Parametric Equations*

Xiao-Shan Gao

Institute of Systems Science, AMSS
Academia Sinica, Beijing, 100080, P.R. China
Email: xgao@mmrc.iss.ac.cn

Abstract

In this paper, we propose algorithms for the following problems in the implicitization of a set of differential rational parametric equations P. (1) To find a characteristic set for the implicit prime ideal of P. (2) To find a canonical representation for the image of P. (3) To decide whether the parameters of P are independent, and if not, to re-parameterize P so that the new parametric equations have independent parameters. (4) To compute the inversion maps of P, and as a consequence, to decide whether P is proper. If the implicit variety is of dimension one and P is not proper, to find a proper re-parameterization for P.

1. Introduction

The 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 effective algorithms that can transform between the implicit representation and parametric representation of rational varieties (1; 9; 11; 13; 18; 20; 21; 23), due to the fact that these algorithms have applications in *solid modeling*.

On the other hand, much of the *differential algebra*(5; 17; 15; 22) or the *differential algebraic geometry* (4; 24) can be regarded as a generalization of the algebraic geometry theory to the analogous theory for algebraic differential equations. However, considerable parts of the results in algebraic geometry have yet to be extended to differential case. In this paper, we will consider some computational issues related to the implicitization of differential rational parametric

* This work is supported by CNSF under an outstanding youth grant No. 69725002 and by NKBRSF No. G19980400.

equations (DRPEs). Two examples of DRPEs are

$$x = u^2, \quad y = u';$$
$$x = u, \quad y = au + b$$

where x and y are indeterminates, u is a 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 two differential equations

$$x'^2 - 4xy^2 = 0;$$
$$x'y'' - x''y' = 0$$

respectively. Differential varieties with parametric representations are defined to be *rational*. It is clear that rational differential varieties are one of the simplest type of varieties, and the parametric representations are the general solution of the corresponding differential equuations. In other words, the solutions for the corresponding differential equations may be generated if the we know its parametric representation.

In this paper, we propose algorithms for the following problems related to a set of DRPEs. (1) To find a characteristic set for the implicit prime ideal (definition in Section 3) of a set of DRPEs. (2) To find a canonical representation for the image (definition in Section 4) 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.

The rest of this paper is organized as follows. In Section 2, we introduce some basic notations. In Section 3, we show how to compute the characteristic set for the implicit ideal of a set of DRPEs. In Section 4, we show how to compute the image of a set of DRPEs. In Section 5, we treat the independency of the parameters. In Section 6, we show how to compute the inversion maps of a set of DRPEs. In Section 7, we propose several problems for further study.

2. Preliminary notations from differential algebra

In this section, we will introduce the notations needed in this paper. More details about these notations could be found in (15; 17; 24).

Let $\mathbf{K}$ be an ordinary differential field of characteristic zero, e.g., $\mathbf{Q(t)}$, $\mathbf{E}$ a universal extension field of $\mathbf{K}$, and $x_1, x_2, \ldots, y_1, y_2, \ldots, u_1, u_2, \ldots$ indeterminates over E. We denote by $x_{i,j}$ the j-th derivative of x_i. We use $\mathbf{K}\{x_1, \ldots, x_n\}$ or $\mathbf{K}\{X\}$ to denote the ring of differential polynomials (abbr. d-pols) in the indeterminates $x_1, \ldots, x_n$.

Let P be a d-pol P in $\mathbf{K}\{X\}/\mathbf{K}$. If p is the smallest p such that $P \in \mathbf{K}\{x_1, \ldots, x_p\}$, then p is called the *class* of P. If $x_{p,o}$ is the highest derivative of x_p appearing in P, then o is called the *order* of P. We may write P as the following form

$$P = a_d x_{p,o}^d + a_{d-1} x_{p,o}^{d-1} + \ldots + a_0$$

where the a_i are d-pols with orders less than o in x_p. Then $x_{p,o}$ is called the *lead* of P, $a_d \neq 0$ is called the *initial* of P and $S = \frac{\partial P}{\partial x_{p,o}}$ is called the *separant* of P. Let P be a d-pol of class p and order o. A d-pol Q is said to be reduced with P if the order of Q in x_p is less than or equal to o and the degree of $x_{p,o}$ in it is less than that in P. For two d-pols P and Q, let $R = \mathrm{prem}(P, Q)$ be the pseudo-remainder of P with respect to Q (17). We have the following *remainder formula* for R

$$JP = \sum_i B_i Q^{(i)} + R \tag{2.1}$$

where J is the product of certain powers of the initial and separant (abbr. SI-product) of Q, $Q^{(i)}$ is the i-th derivative of Q, and B_i are d-pols.

A set of d-pols $TS = \{T_1, \ldots, T_m\}$ is an *ascending chain* if the class for T_i is less than the class of T_{i+1} and T_j is reduced with T_i for $j > i$. For a d-pol P, let $\mathrm{prem}(P, TS) = \mathrm{prem}(\mathrm{prem}(P, T_m), T_1, \ldots, T_{m-1})$. For a triangular set TS, let

$$\mathbf{SAT}(TS) = \{P \in \mathbf{K}\{X\} | \exists\, J,\, JP \in \mathrm{Ideal}(TS)\}$$

where J is an SI-product of d-pols in TS. If TS is irreducible, then $\mathbf{SAT}(TS)$ is a prime ideal and TS is called a *characteristic set* of $\mathbf{SAT}(TS)$ (17; 15). The *order* of a triangular set TS is the sum of the orders of the d-pols in TS.

For a d-pol set PS, let

$$\mathrm{Zero}(PS) = \{\eta = (\eta_1, \ldots, \eta_n) \in E^n \mid \forall P \in PS, P(\eta) = 0\}.$$

For two d-pol sets PS and DS, we define

$$\mathrm{Zero}(PS/DS) = \mathrm{Zero}(PS) - \cup_{d \in DS} \mathrm{Zero}(d).$$

We will need the following Wu-Ritt's zero decomposition theorem (17; 24).

THEOREM 2.1: *For two d-pol sets PS and DS, we have a method to find irreducible ascending chains AS_i such that*

$$\mathrm{Zero}(PS/DS) = \cup_i \mathrm{Zero}(AS_i/\mathbf{DS} \cup \{J_i\}) = \cup_i \mathrm{Zero}(\mathbf{SAT}(AS_i)/\mathbf{DS})$$

where J_i is the SI-product of AS_i.

A large amount of work has been done related to this theorem. Some of them may be found in (10; 12; 5; 14; 16).

3. The implicit ideal of a set of DRPEs

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

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ \ldots, \ x_n = \frac{P_n(U)}{Q_n(U)} \tag{3.1}$$

a set of *differential rational parametric equations* (abbr. DRPEs). We assume that not all $P_i(u)$ and $Q_i(u)$ are in $\mathbf{K}$ and $gcd(P_i(u), Q_i(u)) = 1$.

The *implicit ideal* of (3.1) is defined as

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

Zero($\mathbf{ID}(P, Q)$) is called the *implicit variety* of (3.1). It is clear that $\mathbf{ID}(P, Q)$ is a prime ideal with generic zero $(P_1/Q_1, \ldots, P_n/Q_n)$. Its differential dimension equals to the differential transcendental degree of $\mathbf{K} < P_1/Q_1, \ldots, P_n/Q_n >$ over $\mathbf{K}$.

Using the same notations introduced above, let

$$\mathbf{PS} = \{F_1 = P_1 - x_1 Q_1, \ldots, F_n = P_n - x_n Q_n\}$$

and $\mathbf{DS} = \{Q_1, \ldots, Q_n\}$. Since PS is an ascending chain under the variable order $u_1 < \ldots < u_m < x_1 < \ldots < x_n$, we may define $\mathbf{SAT}(\mathbf{PS})$.

Lemma 3.1: $\mathbf{SAT}(\mathbf{PS})$ *is a prime ideal of dimension* m *and* $\mathbf{SAT}(\mathbf{PS}) \cap \mathbf{K}\{X\}$ *is the implicit ideal of (3.1).*

Proof. Under the variable order $u_1 < \ldots < u_m < x_1 < \ldots < x_n$, $\mathbf{PS}$ is an ascending chain whose leading variables have degree one. So it is an irreducible ascending chain and $\mathbf{SAT}(\mathbf{PS})$ is a prime ideal with a generic zero $\eta = (U, P_1/Q_1, \ldots, P_n/Q_n)$ (for definition see (17; 24)). The dimension of $\mathbf{SAT}(\mathbf{PS})$ is the differential transcendental degree of η over $\mathbf{K}$, which is m. Since η is a generic zero of $\mathbf{SAT}(\mathbf{PS})$ and $(P_1/Q_1, \ldots, P_n/Q_n)$ is a generic zero of $\mathbf{ID}(P, Q)$, we have $\mathbf{ID}(P, Q) = \mathbf{SAT}(\mathbf{PS}) \cap \mathbf{K}\{X\}$. ▮

Lemma 3.2: Zero($\mathbf{PS}/\mathbf{DS}$) = Zero($\mathbf{SAT}(\mathbf{PS})/\mathbf{DS}$).

Proof. The equation is true because of the remainder formula (2.1) and the fact that $\mathbf{DS}$ contains the initials and separants of $\mathbf{PS}$ as an ascending chain under the variable order $u_i < x_j$. ▮

From Lemma 3.1, to compute a characteristic set for the implicit ideal, we need to find a characteristic set for the prime ideal $\mathbf{SAT}(\mathbf{PS})$ under the variable order $x_1 < \ldots < x_n < u_1 < \ldots < u_m$. Apply Wu-Ritt's zero decomposition theorem (24) under the variable order $x_1 < \ldots < x_n < u_1 < \ldots < u_m$, we have

$$\text{Zero}(\mathbf{PS}/\mathbf{DS}) = \cup_i \text{Zero}(AS_i/\mathbf{DS} \cup \{J_i\}) = \cup_i \text{Zero}(\mathbf{SAT}(AS_i)/\mathbf{DS})$$

where AS_i are irreducible ascending chains and J_i are the SI-products of the d-pols in AS_i. Let AS_k be an ascending chain in the above decomposition such that when substituting x_i by P_i/Q_i, every d-pol in AS_k becomes zero. Since $\eta = (U, P_1/Q_1, \ldots, P_n/Q_n) \in \mathrm{Zero}(\mathbf{PS}/\mathbf{DS})$, such a k must exist. We will show that

$$\mathbf{SAT}(AS_k) = \mathbf{SAT}(\mathbf{PS}).$$

From the above decomposition and Lemma 3.2, $\mathbf{SAT}(\mathbf{PS}) \subset \mathbf{SAT}(AS_k)$. Since η is a generic zero of $\mathbf{SAT}(\mathbf{PS})$ and is a zero of AS_k, we have $AS_k \subset \mathbf{SAT}(\mathbf{PS})$. We say that $J_k \notin \mathbf{SAT}(\mathbf{PS})$. Otherwise, $J_k \in \mathbf{SAT}(\mathbf{PS}) \subset \mathbf{SAT}(AS_k)$, which is in contradiction with the fact that AS_k is a characteristic set of $\mathbf{SAT}(AS_k)$. Combining the above two facts, we have $\mathbf{SAT}(AS_k) \subset \mathbf{SAT}(\mathbf{PS})$, which completes the proof. After changing the names of the variables, we may write AS_k as follows.

$$\begin{array}{l} A_1(x_1, \ldots, x_{d+1}), \ldots, A_{n-d}(x_1, \ldots, x_n), \\ B_1(x_1, \ldots, x_n, u_1, \ldots, u_{s+1}), \ldots, B_{m-s}(x_1, \ldots, x_n, u_1, \ldots, u_m) \end{array} \tag{3.2}$$

where $d + s = m$. The *parameter set* of AS_k is $\{x_1, \ldots, x_d,\ u_1, \ldots, u_s\}$.

THEOREM 3.1: *The implicit ideal of (3.1) is* $\mathbf{ID}(P, Q) = \mathbf{SAT}(A_1, \ldots, A_{n-d})$.

Proof. From the above computation process, (3.2) is a characteristic set of $\mathbf{SAT}(\mathbf{PS})$. Now, the result is a consequence of Lemmas 3.1 and 3.2. ∎

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

EXAMPLE 3.1: *Let us consider the following DRPEs*

$$x = u^2, y = u'. \tag{3.3}$$

Let $PS = \{x - u^2, y - u'\}$. *Under the variable order* $x < y < u$, *by Wu-Ritt's zero decomposition theorem, we have*

$$\begin{array}{rcl} \mathrm{Zero}(PS) & = & \mathrm{Zero}(\{4xy^2 - x'^2, 2yu - x'\}/xy) \\ & \cup & \mathrm{Zero}(\{x', y, u^2 - x\}/u) \\ & \cup & \mathrm{Zero}(\{x, y, u\}) \end{array}$$

Only $4xy^2 - x'^2$ *vanishes for* $x = u^2, y = u'$. *From the process of obtaining (3.2), the implicit ideal is* $\mathbf{SAT}(4xy^2 - x'^2)$. *For this example, we may obtain the basis for the implicit ideal. By the lower power theorem (17),* $\mathbf{SAT}(4xy^2 - x'^2) = [4xy^2 - x'^2]$.

4. The image of a set of DRPEs

The *image* of (3.1) in E^n is

$$\mathbf{IM}(P,Q) = \{(\eta_1,\ldots,\eta_n) \in E^n \mid \exists \tau \in E^m(\eta_i = P_i(\tau)/Q_i(\tau))\}.$$

LEMMA 4.1: *We can find d-pol sets PS_i and d-pols d_i, $i=1,\ldots,t$, such that*

$$\mathbf{IM}(P,Q) = \cup_{i=1}^{t}\mathrm{Zero}(PS_i/\{d_i\}). \tag{4.1}$$

Proof. It is obvious that $\mathbf{IM}(P,Q) = \{(x_1,\ldots,x_n) \mid \exists \tau \in E^m(Q_i(\tau)x_i - P_i(\tau) = 0 \wedge Q_i(\tau) \neq 0)\}$. Thus by the quantifier elimination theories for a differential closed field (7; 10), we can find PS_i and d_i such that (4.1) is valid. ▮

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

THEOREM 4.1: *Let V be the implicit variety of (3.1) and d the dimension of V. Then*

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

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

(3) We can find irreducible ascending chains AS, AS_i such that

$$\mathbf{IM}(P,Q) = \mathrm{Zero}(\mathbf{SAT}(AS)) - \cup_{i=1}^{k}\mathrm{Zero}(AS_i/J_iD_i),$$

where $\mathbf{SAT}(AS)$ is the implicit ideal of (3.1), J_i are the SI-products of AS_i and D_i are d-pols.

Proof. (1) is a consequence of Lemma 3.1. (2) is a consequence of (3) and the differential dimension theorem in (17). We need only to prove (3). By Lemma 4.1, we can find d-pols sets PS_k and d-pols d_k in $\mathbf{K}\{X\}$ such that

$$\mathbf{IM}(P,Q) = \cup\mathrm{Zero}(PS_k/d_k).$$

By Wu-Ritt's zero decomposition algorithm (24), we further assume

$$\mathbf{IM}(P,Q) = \cup\mathrm{Zero}(AS_i/d_iJ_i) \tag{4.2}$$

where AS_i are irreducible ascending chains and J_i are the SI-products of AS_i. Let AS_1 be an ascending chain containing least number of d-pols and with the largest order among these AS_i. We will show that the implicit variety V of (3.1) is $\mathrm{Zero}(\mathbf{SAT}(AS_1))$. Because of (1), we have $\mathrm{Zero}(\mathbf{SAT}(AS_1)/d_1J_1) \subset V$. Since both V and $\mathrm{Zero}(\mathbf{SAT}(AS_1))$ are irreducible, we have $\mathrm{Zero}(\mathbf{SAT}(AS_1)) \subset V$. To prove the other direction, first notice that a *generic zero* of V is in $\mathbf{IM}(P,Q)$. Since $\mathrm{Zero}(AS_1/d_1J_1)$ is a component with maximal dimension and order in decomposition (4.2), it must contain a generic zero of V and hence

$V \subset \mathrm{Zero}(\mathbf{SAT}(AS_1))$. Thus, $V = \mathrm{Zero}(\mathbf{SAT}(AS_1))$. By the remainder formula (2.1), $\mathrm{Zero}(AS_1/J_1) = \mathrm{Zero}(\mathbf{SAT}(AS_1)/J_1)$. Then

$$\begin{aligned}\mathbf{IM}(P,Q) &= \mathrm{Zero}(\mathbf{SAT}(AS_1)/d_1J_1)\bigcup\cup\mathrm{Zero}(AS_i/d_iJ_i)\\ &= (\mathrm{Zero}(\mathbf{SAT}(AS_1)) - \mathrm{Zero}(\{d_1J_1\}))\bigcup\cup\mathrm{Zero}(AS_i/d_iJ_i).\\ &= \mathrm{Zero}(\mathbf{SAT}(AS_1)) - (\mathrm{Zero}(\{d_1J_1\}) - \cup\mathrm{Zero}(AS_i/d_iJ_i)).\end{aligned}$$

Using the following formulas

$$\mathrm{Zero}(PS_1/D_1)\cap\mathrm{Zero}(PS_2/D_2) = \mathrm{Zero}(PS_1\cup PS_2/D_1D_2)$$

$$\mathrm{Zero}(PS_1/D_1) - \mathrm{Zero}(PS_2/D_2) = \cup_{P\in PS_2}\mathrm{Zero}(PS_1/D_1P)\cup\mathrm{Zero}(PS_1\cup\{D_2\}/D_1)$$

we may transform $\mathbf{IM}(P,Q)$ to the desired form. ∎

Example 4.1: *Continue from Example 3.1. We will compute the image of DRPE (3.3). Using the projection method in (10) we have*

$$\begin{aligned}\mathbf{IM}(P,Q) &= \mathrm{Zero}(\{4xy^2 - x'^2\}/xy)\cup\mathrm{Zero}(\{x',y\}/x)\cup\mathrm{Zero}(\{x,y\})\\ &= \mathrm{Zero}(\{4xy^2 - x'^2\}/xy)\cup\mathrm{Zero}(\{x',y\})\end{aligned}$$

By Theorem 4.1, we may find the following canonical representation

$$\mathbf{IM}(P,Q) = \mathrm{Zero}(4xy^2 - x') - \mathrm{Zero}(x/y).$$

From the above example, we see that the image is generally not equal to the implicit variety.

5. Independent parameters

The parameters $u_1,\dots,u_m$ of DRPEs (3.1) are called *independent* if the implicit ideal of (3.1) is of dimension m, or equivalently the differential transcendental degree of the field $\mathbf{K} < P_1/Q_1,\dots,\ P_n/Q_n >$ over $\mathbf{K}$ is m.

Lemma 5.1: *Suppose that we have constructed (3.2). Then the dimension of* $\mathbf{ID}(P,Q)$ *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 (17). Then the result comes from Theorem 3.1. ∎

Theorem 5.1: *If the parameters of (3.1) are not independent and* $\mathbf{K} = \mathbf{Q}(t)$ *is the field of the rational functions, then we can find a set of new DRPEs*

$$x_1 = P_1'/Q_1',\dots,x_n = P_n'/Q_n' \tag{5.1}$$

which has the same implicit variety as (3.1) but with independent parameters.

Proof. Since (3.2) is irreducible, we may assume that the SI-products J_j of (3.2) are d-pols free of the leads of the d-pols in (3.2). Since $\text{prem}(Q_i, (3.2))$ is not zero, we can find a nonzero d-pol q_i reduced with (3.2) and free of the leads of the d-pols in (3.2) such that

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

Let $M = \prod_{i=1}^{m-s} J_i \cdot \prod_{j=1}^{n} q_j$. M is a d-pol free of the leads of the d-pols in (3.2). Then M is not in $\mathbf{SAT}((3.2))$. Since $\mathbf{K} = \mathbf{Q}(t)$, there exist $h_1, \ldots, h_s$ in $\mathbf{K}$ such that when replacing u_i by h_i, $i = 1, \ldots, s$, M becomes a nonzero d-pol M' (17). Let P_i', Q_i', A_i', and B_i' be the d-pols obtained from P_i, Q_i, A_i and B_i by replacing u_i by h_i, $i = 1, \ldots, s$. Now we have obtained (5.1). Also note that after the substitution (3.2) is still an ascending chain, which is denoted by (3.2)'. Let the implicit varieties defined by (5.1) and (3.1) be W and V respectively. We want to prove $W = V$. By the selection of h_i, it is clear that $W \subset V$. Let $x' = (x_1', \ldots, x_n')$ be a generic point of V. By the selection of h_i, M' is reduced with (3.2)'. Then by the project theorem (10; 7), we may solve u_i, $i = s+1, \ldots, m$, from $B_i' = 0$, which do not vanish M, and hence neither Q_i and the initial and separant of B_i. Let the solution of $B_i' = 0$ be h_{s_i}, and $\eta = (x_1', \ldots, x_n', h_1, \ldots, h_m)$. Since $F_i = P_i - x_i Q_i \in$
$SAT(3.2)$, there exists an SI-product J of (3.2) such that

$$JF_i = 0 \text{mod}(3.2)$$

Since $J(\eta) \neq 0$, we have $F_i'(\eta) = P_i'(\eta) - x_i' Q_i'(\eta) = 0$. In other words, $x_i' = P_i'(\eta)/Q_i'(\eta)$ and $x' \in W$. We have proved $W = V$. ∎

EXAMPLE 5.1: *Let us consider the following DRPEs*

$$x = u^2 + 2uv^2 + v^4, y = u' + 2vv'. \tag{5.2}$$

Let $PS = \{x - u^2 - 2uv^2 - v^4, y - u' - 2vv'\}$. *Under the variable order* $x < y < v < u$, *by Wu-Ritt's zero decomposition theorem, we have*

$$\begin{aligned}
\text{Zero}(PS) &= \text{Zero}(\{4xy^2 - x'^2, 2y(u - v^2) - x'\}/xy) \\
&\cup \text{Zero}(\{x', y, (u - v^2)^2 - x\}/u - v^2) \\
&\cup \text{Zero}(\{x, y, u - v^2\})
\end{aligned}$$

It is easy to check that the parameters u *and* v *are not independent. To find a set of independent parameters, we need only to select a value for* v *such that* $M = xy = (u^2 + 2uv^2 + v^4)(u' + 2vv')$ *is not zero. Let* $v = 0$, *(5.2) becomes (3.3), which has an independent parameter.*

6. Inversion maps and proper parametric equations

The *inversion problem* is that given a point $(a_1, \ldots, a_n)$ on the image of (3.1), find a set of values $(\tau_1, \ldots, \tau_m)$ for the u such that

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

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 (3.1) are functions in $x_{i,j}$

$$u_1 = f_1(x_1, \ldots, x_n), \ldots, u_m = f_m(x_1, \ldots, x_n)$$

such that $x_i \equiv P_i(f_1, \ldots, f_m)/Q_i(f_1, \ldots, f_m)$ become identities when replacing x_i by P_i/Q_i.

The inversion problem is closely related to whether a set of parametric equations is proper. DRPEs (3.1) are called *proper* if for each $(a_1, \ldots, a_n) \in \mathbf{IM}(P, Q) - V$, there exists only one $(\tau_1, \ldots, \tau_m) \in E^m$ such that $a_i = P_i(\tau_1, \ldots, \tau_m)/Q_i(\tau_1, \ldots, \tau_m)$, $i = 1, \ldots, n$, where V is a subset of $\mathbf{IM}(P, Q)$ with less dimension than that of $\mathbf{IM}(P, Q)$, or with the same dimension as $\mathbf{IM}(P, Q)$ but with less order than that of $\mathbf{IM}(P, Q)$ with respect to the same set of parameters. For the definitions of dimension and order, please consult (17; 15).

By Theorem 5.1, we may assume that the parameters $u_1, \ldots, u_m$ of (3.1) are independent, i.e., $s = 0$. Then (3.2) becomes

$$\begin{array}{l} A_1(x_1, \ldots, x_{m+1}) \\ \ldots \\ A_{n-m}(x_1, \ldots, x_n) \\ B_1(x_1, \ldots, x_n, u_1) \\ \ldots \\ B_m(x_1, \ldots, x_n, u_1, \ldots, u_m) \end{array} \tag{6.1}$$

THEOREM 6.1: *Using the above notations, we have*

(a) $B_i(x, u_1, \ldots, u_i) = 0$ determine u_i $(i = 1, \ldots, m)$ as functions of $x_{i,j}$ which are a set of inversion maps for (3.1).

(b) (3.1) is proper if and only if $B_i = I_i u_i - U_i$ are linear in u_i for $i = 1, \ldots, m$, and if this is the case, the inversion maps are

$$u_1 = U_1/I_1, \ldots, u_m = U_m/I_m$$

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

Proof. By Lemma 3.2, (6.1) is a characteristic set of $\mathbf{SAT}(\mathbf{PS})$, which leads to (a). We need only to subtract $V = \mathrm{Zero}(J)$ from $\mathbf{IM}(P, Q)$, where J is the product of the initials and separants of B_i. The fact that V satisfies the conditions in the definition is due to the dimension theorems proved in (17). To prove (b), first note that the $B_i = 0$ $(i = 1, ..., m)$ are the relations between the x and $u_1, ..., u_i$ which have the lowest order and degree in u_i. Also different solutions of $B_i = 0$ for the same x give the same value for the x_i. Since (6.1) is an irreducible ascending chain, for a generic zero x' on the implicit variety V, $B_i(x', u_1, ..., u_i) = 0$, $i = 1, ..., m$, always have multiple roots for the u_i if B_i is not linear in u_i. Therefore a point $x \in \mathbf{IM}(P, Q)$ corresponds to one set of values for u_i iff B_i are linear in u_i, $i = 1, ..., m$. Let $B_i = I_i u_i - U_i$ where I_i and U_i are in $\mathbf{K}\{X\}$ then the inversion maps are $u_i = U_i/I_i$, $i = 1, ..., m$. ∎

THEOREM 6.2: *If $m = 1$ and DRPEs (3.1) are not proper, we can find a new parameter $s = f(u_1)/g(u_1)$ where f and g are in $\mathbf{K}\{u_1\}$ such that the re-parameterization of (3.1) in terms of s,*

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ \ldots, \ x_n = \frac{F_n(s)}{G_n(s)} \tag{6.2}$$

are proper.

Proof. Let $K' = \mathbf{K} < P_1/Q_1, \ldots, P_n/Q_n >$ be the differential extension field of $\mathbf{K}$ by adding $P_1/Q_1, \ldots, P_n/Q_n$. Since $P_1(u_1) - Q_1(u_1)l = 0$ where $l = P_1(u_1)/Q_1(u_1) \in K'$, u_1 is differential over K'. Let I be the prime ideal in $\mathbf{K}'\{y\}$ with u_1 as a generic point and $\{f\}$ the characteristic set for I. Write f as the following,

$$f(y) = a_r D_1 y + \ldots + a_1 D_r y + a_0$$

where $a_i \in K'$ and $D_i y$ are products of derivatives of y. 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 (17), we have $K' = \mathbf{K}(\eta)$. This means that $x_i = P_i/Q_i$ can be expressed as differential rational functions of η and η also can be expressed as a differential rational function of $x_i = P_i/Q_i$. In other words, 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 6.1, we can find an inversion map $B_1(x_1, \ldots, x_n, u_1) = 0$ of the DPREs. Then $B_1'(y) = B_1(P_1/Q_1, \ldots, P_n/Q_n, y) = 0$ is a d-pol in $K'\{y\}$ with lowest degree in y such that $B_1'(u_1) = 0$, i.e., $B_1'(y)$ can be taken as $f(y)$. So s can be obtained as follows. If B_1 is linear in u_1, nothing needs to be done. Otherwise let

$$B_1 = b_r D_1 u_1 + \ldots + b_1 D_r u_1 + b_0$$

where the b_i are in $\mathbf{Q}[x]$ and $D_1 u_1$ are products of derivatives of u_1. Substituting x_i by P_i/Q_i, b_i can be expressed as differential rational functions $a_i(u_1)$, $i = 1, \ldots, r$. At least one of a_i/a_r, say a_0/a_r, is not an element in $\mathbf{Q}$. Let $s = a_0/a_r$. Eliminate u_1 from (3.1) and $a_r s - a_0$to obtain a d-pol R_i in x_i and s. By Lüroth's theorem (17), $R_i = Q_i' x_i - P_i'$ must be linear in x_i. We thus obtain (6.2). Note that a_i comes from b_i by substituting x_j by P_j/Q_j, $j = 1, \ldots, n$, then $s = b_0/b_r$ is an inversion map of (6.2). ∎

Example 6.1: *Let us consider the following DRPEs*

$$x = u^4, y = 2uu'. \tag{6.3}$$

Let $PS = \{x - u^4, y - 2uu'\}$. *Under the variable order* $x < y < u$, *by Wu-Ritt's zero decomposition theorem (24), we have*

$$\begin{aligned}\mathrm{Zero}(PS) &= \mathrm{Zero}(\{4xy^2 - x'^2, 2yu^2 - x'\}/xy)\\ &\cup\ \mathrm{Zero}(\{x', y, u^4 - x\}/u)\\ &\cup\ \mathrm{Zero}(\{x, y, u\})\end{aligned}$$

DRPEs (6.3) are not proper. An inversion map is $u = \sqrt{\frac{x'}{2y}}$. *To find a set of proper DRPEs, by Theorem 6.2, we select a new parameter* $s = u^2$. *Eliminating* u *from* $s = u^2$ *and (6.3), we obtain a new set of parametric equations*

$$x = s^2, y = s'$$

which has the same implicit ideal as (6.3) and is proper. This is actually DRPEs (3.3). The inversion map for this set of proper parametric equations is $s = \frac{x'}{2y}$, *which has meaning for those points in the image satisfying* $y \neq 0$.

7. Several problems for further study

Several problems in the implicitization of DRPEs remain open. One is to find a basis for the implicit ideal, which should be very difficult because it is closely related to the computation of Gröbner basis for differential ideals. Another problem is to find a proper re-parameterization for a set of im-proper DRPEs in the general case. This is possible if we may extend the Lüroth's theorem to the multi-variable case. In the algebraic case, if the base field K is the complex number field $\mathbf{C}$, then there always exists a proper reparametrization for the original improper parametric equations for algebraic surfaces (6). However if the base field K is $\mathbf{Q}$ (the field of rational numbers) or $\mathbf{R}$ (the field of real numbers), this needs not to be the case (19). If the implicit variety determined by the parametric equations are of dimension > 2, then even for $K = \mathbf{C}$ there exist improper parametric equations that do not have a proper reparametrization (2). From Example 4.1, we see that the image is generally not equal to the implicit variety. An interesting problem is to find conditions for DRPEs under which the image is exactly the implicit variety. For some results in algebraic case, see (8).

The results in this paper are about the implicitization of DRPEs. The inverse problem, i.e., to decide whether an implicitly given differential variety is rational, and if it is, to find a set of DRPEs for it, is still open. In algebraic case, this problem is closely related to the singularities and genus of the corresponding algebraic variety. Please consult (1; 20; 21) for some results in algebraic case. It would be very interesting to develop such methods in the differential case.

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. M. Artin and D. Mumford, Some Elementary Examples of Unirational Varieties Which Are Non-rational, *Proc. London Math. Soc.*, **25**, 75-95, 1972.

3. 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, Berlin, 1987.

4. A. Buium and P.J. Cassidy, Differential algebraic geometry and differential algebraic groups: from algebraic differential equations to Diophantine geometry, in H. Bass et al eds, *Selected Works of Ellis Kolchin, with Commentary*, pp. 567-636, Providence, RI, American Mathematical Society, 1998.

5. F. Boulier, D. Lazard, F. Ollivier and M. Petitot, Representation for the radical of a finitely generated differential ideal, *Proc. ISSAC'95*, Levelt, A.H.M (ed), ACM Press, New York, pp.158-166, 1995.

6. I. Castelnuvo, Sulla Rationalita della Involuzioni Pinae, *Math. Ann.*, **44**, 125–155, 1894.

7. A. L. Chistov and D. Yu Grigor'ev, Complexity of quantifier elimination in the theory of ordinary differential equations, Preprint, 1990.

8. X.S. Gao and S.C. Chou, On the Normal Parameterization of Curves and Surfaces, *The International Journal of Computational Geometry* and *Applications*, **1**, 125-136, 1991.

9. X.S. Gao and S. C. Chou, Implicitization of rational parametric equations, *Journal of Symbolic Computation*, **14**, 459-470, 1992.

10. X.S. Gao and S.C. Chou, A zero structure theorem for differential parametric systems, *Journal of Symbolic Computation*, **16**, 585-595, 1994.

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

12. E. Hubert, Factorization-free decomposition algorithms in differential algebra. *J. Symbolic Computation*, **29**, 641-662, 2000.

13. M. Kalkbrener, *Three contributions to elimination theory*, PhD Thesis, Johannes Kepler University, 1991.

14. Z.M. Li and D. Wang, Coherent, regular and simple systems in zero decomposition of partial differential systems, *Sys. Sci. Math. Sci.*, **12**(supple), 43–60, 1999.

15. E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, London, 1973.

16. G. Reid, Algorithms for reducing a system of PDEs to standard form, determining the dimension of its solution space and calculating its Taylor series solution, *European J. of Appl. Math.*, **2**, 293-318, 1991.

17. J. F. Ritt, *Differential algebra*, Amer. Math. Sco. Colloquium, New York, 1950.

18. 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.

19. B. Segre, Sull Esistenza, Sia Nel Campo Rationale chenel Campo Reale, *Rend. Accad. Naz. Lincei* **10**, 564–570, 1951.

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

21. J. Schicho, *Rational parameterization of algebraic surfaces*, PhD Thesis, Johannes Kepler University, 1995.

22. A. Rosenfeld, Specialization in differential algebra, *Trans. Amer. Math. Soc.*, **90**, 394-407, 1959.

23. D. Wang, Reasoning about geometric problems using an elimination method. In: *Automated practical reasoning: Algebraic approaches*, Pfalzgraf, J., Wang, D., eds., pp. 147–185, Springer, Wien New York, 1995.

24. W.T. Wu, A constructive theory of differential algebraic geometry, in LNM **1255**, pp. 173–189, Springer, Berlin Heidelberg, 1987.