ARTICLE IN PRESS

Journal of Symbolic Computation ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Characteristic set method for differential–difference polynomial systems

X.S. Gao[a,1], J. Van der Hoeven[b], C.M. Yuan[a], G.L. Zhang[a]

[a] KLMM, Institute of Systems Science, AMSS, Chinese Academy of Sciences, Beijing 100190, China

[b] CNRS, Département de Mathématiques, Université Paris-Sud 91405 Orsay Cedex, France

ARTICLE INFO

Article history:
Received 13 November 2007
Accepted 22 February 2008
Available online xxxx

Keywords:
Characteristic set
Differential and difference polynomial
Regular ascending chain
Irreducible ascending chain
Zero decomposition algorithm
Perfect ideal membership problem

ABSTRACT

In this paper, we present a characteristic set method for mixed differential and difference polynomial systems. We introduce the concepts of coherent, regular, proper irreducible, and strongly irreducible ascending chains and study their properties. We give an algorithm which can be used to decompose the zero set for a finitely generated differential and difference polynomial sets into the union of the zero sets of regular and consistent ascending chains. As a consequence, we solve the perfect ideal membership problem for differential and difference polynomials.

1. Introduction

The characteristic set method is a tool for studying systems of polynomial or algebraic differential equations (Kolchin, 1973; Ritt, 1950). Recent results on the characteristic set method, which are used in this paper, can be found in Aubry et al. (1999), Boulier et al. (1995), Bouziane et al. (2001), Chou and Gao (1990, 1993), Gao and Chou (1993), Hubert (2000), Wu (1994) and Yang et al. (1996). The idea of the method is to privilege systems which have been put in a special "triangular form", also called an ascending chain or simply a chain. The zero set of any finitely generated polynomial or differentially algebraic system of equations may be decomposed into the union of the zero sets of chains. One can also use the method to solve a system of equations, to determine the dimension, the degree, and the order of a finitely generated system of polynomials or differential polynomials, to solve the radical ideal membership problem, to prove the Noetherian property of differential equation systems, to prove theorems from elementary and differential geometries, and to solve problems from

E-mail address: xgao@mmrc.iss.ac.cn (X.S. Gao).

[1] Tel.: +86 10 62541831; fax: +86 10 62630706.

0747-7171/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.02.010

engineering fields such as computer vision, computer aided design, computer graphics, and robotics. For surveys, please consult Wang (2000) and Wu (2001).

The notion of characteristic set for difference polynomial systems was proposed by Ritt and Doob (1933) and Ritt and Raudenbush (1939). The general theory of difference algebra was established by Cohn (1965). Due to differences between the differential case and the difference case, algorithms and properties for difference chains were studied only very recently (Gao et al., 2009; Gao and Yuan, 2006).

A natural problem is to consider systems of mixed differential and difference polynomials, called *DD-polynomials*. In van der Hoeven (1996), it was outlined how to generalize the characteristic set method to this setting. However, the author overlooked an additional difficulty in the proof of Rosenfeld's Lemma. Although all theoretical properties of differential algebra (dimension polynomials, finite generation of ideals, etc.; see also Kondratieva et al. (1999)) do generalize to the DD-setting, the algorithmic counterparts have to be redeveloped.

In this paper, we will present a characteristic set method for ordinary mixed DD-polynomial systems. The following results are established in this paper.

(1) Based on the concept of characteristic sets, we prove that DD-polynomial systems are Noetherian in the sense that for an infinite set $\mathbb{P}$ of DD-polynomials, there exists a finite set $\mathbb{Q}$ of DD-polynomials such that $\mathbb{P}$ and $\mathbb{Q}$ have the same solutions.
(2) We introduce the concepts of coherent and regular chains and prove that a chain is coherent and regular if and only if it is the characteristic set for its saturation ideal. This result gives a simple method to determine whether a DD-polynomial belongs to the saturation ideal of a chain.
(3) We define proper irreducible chains and prove that a proper irreducible chain is regular and its saturation ideal is reflexive. This gives a constructive criterion for a chain to be regular. We further introduce the concept of strongly irreducible chains and prove that an ideal is prime and reflexive if and only if its characteristic set is strongly irreducible and coherent.
(4) Based on the above results, we propose an algorithm which can be used to decompose the zero set for a finitely generated DD-polynomial set into the union of zero sets of proper irreducible, and thus regular and reflexive, chains.
(5) We prove that a coherent and proper irreducible chain always has zeros. As a consequence, we give an algorithm to solve the perfect ideal membership problem for DD-polynomials.

As a consequence, we could say that a major portion of the existing results on characteristic set methods for algebraic and differential polynomial systems are now been extended to the differential–difference case.

Among the five results mentioned above, the Noetherian property is different from that in Kondratieva et al. (1999), because our assumption on the differential–difference structure is more general. The other results are the main contributions of this paper.

Comparing to the factorization free decomposition algorithms for differential polynomial systems (Boulier et al., 1995; Bouziane et al., 2001; Hubert, 2000), our work has two major distinctions. First, Rosenfeld's Lemma is not valid in this case and we cannot check properties of a coherent chain from its algebraic counterpart. Secondly, in the differential case, one only needs to consider the initial and separant of a differential polynomial when constructing the saturation ideal; in our case, we need to consider all possible transforms of the initial of a difference polynomial. This makes it impossible to check whether a chain is regular as directly as in the differential case. As a partial remedy, we introduce the concept of proper irreducible chains. Another missing result is that we cannot decompose the perfect ideal generated by a set of DD-polynomials into the intersection of prime ideals. In order to do that, we need to know how to check whether a chain is strongly irreducible which is an open problem.

Comparing to the decomposition algorithms for difference polynomial systems (Gao et al., 2009; Gao and Yuan, 2006), the major difference lies in the results on proper irreducible chains. The definition for a proper irreducible chain in Gao et al. (2009) cannot be extended to the differential–difference case directly. In order to give an appropriate definition, we first work out a new definition for difference polynomials (Gao et al., 2006) and then extend this definition to the mixed case. The proofs for the facts that a proper irreducible chain is regular (Theorem 5.8) and the validity of the algorithm to check whether a chain is proper irreducible (Lemma 6.3) are essentially different from those in Gao et al. (2009) and Gao et al. (2006). In our definition of proper irreducible chains in the

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

differential–difference case, we need to check the membership for the saturation ideal of a differential chain and we generally do not know how to compute a basis for this ideal. In order to avoid this difficult question, new techniques are developed. Perfect ideal membership problem is solved for the first time in the differential–difference case.

The paper is organized as follows. In Section 2, we introduce notations. In Section 3, we prove the Noetherian property for DD-polynomial systems. In Section 4, we prove the properties for regular chains. In Section 5, we prove the properties for proper and strongly irreducible chains. In Section 6, we give the zero decomposition algorithm.

2. DD-ring and DD-polynomials

2.1. DD-operators

Let $\mathbb{K}$ be a computable field containing the field $\mathbb{Q}(x)$ of rational functions in an indeterminate x. A *differential operator* ∂ defined on $\mathbb{K}$ is a map $\partial : \mathbb{K} \to \mathbb{K}$ satisfying

$$\partial(f+g) = \partial(f) + \partial(g)$$
$$\partial(fg) = \partial(f)\cdot g + \partial(g)\cdot f$$

for any $f, g \in \mathbb{K}$. A *difference operator* δ defined on $\mathbb{K}$ is a map $\delta : \mathbb{K} \to \mathbb{K}$ satisfying

$$\delta(f+g) = \delta(f) + \delta(g)$$
$$\delta(fg) = \delta(f)\delta(g)$$
$$\delta(f) = 0 \Longleftrightarrow f = 0$$

for any $f, g \in \mathbb{K}$. We also call $\delta(f)$ the *translation* of f. Iterated translations $\delta^k(f)$ are called transforms. If all elements of $\mathbb{K}$ are functions in x, then the ordinary differentiation w.r.t. x is a differential operator. The shift operator $\delta(x) = x + 1$ and the q-difference operator $\delta(x) = qx$ are examples of difference operators.

A key fact to deal with the hybrid differential–difference case is to make an assumption on how the differential and the difference operators interact. In this paper, we assume the existence of a non-zero element $h \in \mathbb{K}$, such that the operators δ and ∂ commute according to the following rule:

$$\partial\delta = h \cdot \delta\partial. \tag{1}$$

It is easy to check that for a positive integer s, we have

$$\begin{aligned} \partial\delta^s &= h_s\delta^s\partial, \\ h_s &= \prod_{i=0}^{s-1} \delta^i(h). \end{aligned} \tag{2}$$

A product of the form $\prod_{i=0}^{k} \delta^i(h)^{n_i}$ is called an *h-product*. More generally, we have

$$\partial^r\delta^s = \Lambda_{r,r}(h_s)\delta^s\partial^r + \cdots + \Lambda_{r,1}(h_s)\delta^s\partial, \tag{3}$$

where the $\Lambda_{r,i}$ are differential polynomials which are recursively determined by

$$\begin{aligned} \Lambda_{0,0}(F) &= 1 \\ \Lambda_{r,i}(F) &= F\Lambda_{r-1,i-1}(F) + \Lambda'_{r-1,i}(F). \end{aligned}$$

In particular, $\Lambda_{r,r}(F) = F^r$ for all r.

Example 2.1. If $h = 1$, then (1) implies that the two operators are commutative, which is the case assumed in Kondratieva et al. (1999). A typical example is the shift operator S with $(Sf)(x) = f(x+1)$. More generally, the commutation rule (1) is motivated by treating the difference operator as the right-composition with a non-trivial function. Indeed, if

$$\delta(f(x)) = f(\phi(x))$$

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

for any function $f(x)$ and a fixed function $\phi(x)$, then

$$\partial\delta(f(x)) = \partial(f(\phi(x))) = \frac{\partial\phi(x)}{\partial x}\,\delta\left(\frac{\partial f(x)}{\partial x}\right) = \frac{\partial\phi(x)}{\partial x}\delta\partial(f(x)),$$

whence (1) is satisfied for $h = \partial\phi(x)/\partial x$. In particular, the q-difference operator $Q : f(x) \mapsto f(qx)$ fits in our setting, even though Q does not commute with ∂.

A field $\mathbb{K}$ with two operators δ and ∂ satisfying (1) is called a *DD-field*. A DD-field $\mathbb{K}$ is called *reflexive* if for any $a \in \mathbb{K}$ there exists a $b \in \mathbb{K}$ such that $\delta b = a$. We denote $b = \delta^{-1}a$ and call b the *inversion* of a. In this paper, we assume that $\mathbb{K}$ is a reflexive DD-field.

We denote $\Omega_0 = \{1\}$, $\Omega_1 = \{\delta, \partial\}$. For each $r \in \mathbb{N}$, we define $\Omega_{r+1} = \Omega_r \cup \delta\Omega_r \cup \partial\Omega_r$ inductively. These sets are subsets of Ω, with $\Omega = \bigcup_{r\in\mathbb{N}} \Omega_r$. It is clear that

$$\Omega = \{\delta^{n_0}\partial^{m_0}\cdots\delta^{n_t}\partial^{m_t}\}$$

where n_i and m_i are non-negative integers and where we understand that $\delta^0 = \partial^0 = Id_{\mathbb{K}}$. We denote by $\mathbb{K}[\Omega]$ the *ring of DD-operators*, which is the free associative (and generally non-commutative) algebra generated by $\mathbb{K}$, δ and ∂, subject to the commutation rule (1).

Remark 2.2. Each element $\Phi \in \mathbb{K}[\Omega]$ can also be regarded as an operator $\Phi_{\mathbb{K}}$ on $\mathbb{K}$. We will denote the set of such operators by $\mathbb{K}[\Omega]_{\mathbb{K}}$. In general, the mapping $\Phi \mapsto \Phi_{\mathbb{K}}$ is not injective. For instance, if $\delta_{\mathbb{K}} = Id$ and $\partial_{\mathbb{K}} = 0$, then $\mathbb{K}[\Omega]_{\mathbb{K}} \cong \mathbb{K}$. Similarly, if $\mathbb{K} = \mathbb{C}(x)$, $\partial_{\mathbb{K}} = \mathrm{d}/\mathrm{d}x$ and $\delta_{\mathbb{K}} : f(x) \mapsto f(qx)$ with $q = \exp(2\pi\mathrm{i}/n)$, then $\mathbb{K}[\Omega]_{\mathbb{K}} \cong \mathbb{K}[\partial] \oplus \cdots \oplus \mathbb{K}[\partial]\delta^{n-1}$. We have not pursued so far the question of finding more interesting examples of this kind.

Given $\omega \in \Omega$, we define its *total order* to be the smallest $r = \mathrm{ord}(\omega)$ with $\omega \in \Omega_r$. Let

$$\begin{aligned} \Theta &= \{\delta^{\alpha}\partial^{\beta} | \alpha, \beta \in \mathbb{N}\},\\ \Theta_{<[i,j]} &= \{\delta^k\partial^l | k \le i,\, l \le j,\, k + l < i + j\}. \end{aligned}$$

Notice that Θ is a proper subset of Ω. A *shuffle* of a word with letters in $\{\delta, \partial\}$ is obtained by repeated transposition of these letters.

Lemma 2.3. *For any shuffle $\omega = \delta^{n_1}\partial^{m_1}\cdots\delta^{n_t}\partial^{m_t} \in \Omega$ of $\delta^n\partial^m$, we have*

$$\omega = h_\omega\delta^m\partial^n + R_\omega,$$

where $n = n_1 + \cdots + n_t$, $m = m_1 + \cdots + m_t$, h_ω is an h-product and $R_\omega \in \mathbb{K}[\Theta_{<[n,m]}]$.

Proof. We prove the Lemma by induction over $n + m$. If $n + m = 0$, then we may take $h_\omega = 1$ and $R_\omega = 0$, so assume $n + m > 1$. Assume first that $\omega = \delta\hat{\omega}$. By the induction hypothesis, we have

$$\hat{\omega} = h_{\hat{\omega}}\delta^{m-1}\partial^n + R_{\hat{\omega}},$$

where $h_{\hat{\omega}}$ is an h-product and $R_{\hat{\omega}} \in \mathbb{K}[\Theta_{<[n-1,m]}]$. It follows that

$$\omega = (\delta h_{\hat{\omega}})\delta^m\partial^n + \delta R_{\hat{\omega}},$$

where $h_\omega = \delta h_{\hat{\omega}}$ is an h-product and, using the induction hypothesis, $R_\omega = \delta R_{\hat{\omega}} \in \mathbb{K}[\Theta_{<[n,m]}]$. Similarly, if $\omega = \partial\hat{\omega}$, then we may write

$$\hat{\omega} = h_{\hat{\omega}}\delta^m\partial^{n-1} + R_{\hat{\omega}}$$

and application of ∂ yields

$$\omega = h_{\hat{\omega}}h_m\delta^m\partial^n + h'_{\hat{\omega}}\delta^m\partial^{n-1} + \partial R_{\hat{\omega}},$$

where $h_\omega = h_{\hat{\omega}}h_m$ is an h-product and $R_\omega = h'_{\hat{\omega}}\delta^m\partial^{n-1} + \partial R_{\hat{\omega}} \in \mathbb{K}[\Theta_{<[n,m]}]$. □

Proposition 2.4. *We have $\mathbb{K}[\Omega] = \mathbb{K}[\Theta]$ and Θ is a basis of the $\mathbb{K}$-vector space $\mathbb{K}[\Omega]$.*

Proof. In view of the above Lemma, we have $\Omega \subseteq \mathbb{K}[\Theta]$, whence $\mathbb{K}[\Omega] \subseteq \mathbb{K}[\Theta]$, by linearity. In order to show that Θ is a free family, let us incarnate Θ as $\mathbb{K}$-linearly independent operators on a DD-superfield $\hat{\mathbb{K}} \supseteq \mathbb{K}$ (see also Remark 2.2). This can be done by taking $\hat{\mathbb{K}}$ to be the fraction field of $\mathbb{K}\langle Y\rangle$ of the ring of DD-polynomials to be constructed below. By construction, the elements in ΘY are algebraically independent in this field, so $\Phi \in \Theta \mapsto \Phi_{\hat{\mathbb{K}}}$ must be injective. This is only possible if the elements in Θ are $\mathbb{K}$-linearly independent. □

Remark 2.5. Using the commutation rule (1) the other way around, one may also rewrite each $\omega \in \delta^{\mathbb{N}}\partial^{\mathbb{N}}$ as a $\mathbb{K}$-linear combination of elements in $\Xi = \{\partial^i\delta^j | i, j \in \mathbb{N}\}$. In a similar way as above, it can be shown that $\mathbb{K}[\Omega] = \mathbb{K}[\Xi]$ and that Ξ is a basis of $\mathbb{K}[\Omega]$.

2.2. DD-polynomials

Let $\mathbb{Y} = \{y_1, \ldots, y_n\}$ be a finite number of indeterminates (which may intuitively be considered as functions of x). We denote

$$\Omega\mathbb{Y} = \{\omega y_i | \omega \in \Omega, y_i \in \mathbb{Y}\}$$
$$\Theta\mathbb{Y} = \{\delta^d\partial^s y_i | d, s \in \mathbb{N}, y_i \in \mathbb{Y}\}.$$

For convenience, we also denote

$$y_{i,d,s} = \delta^d\partial^s(y_i).$$

The set

$$\mathbb{R} = \mathbb{K}\{\mathbb{Y}\} = \mathbb{K}[\Omega\mathbb{Y}]$$

is called the *DD-ring* of *DD-polynomials* over $\mathbb{K}$ in $\mathbb{Y}$. The difference operator δ on $\mathbb{R}$ is the unique ring homomorphism which extends the difference operator on $\mathbb{K}$ and sends ωy_i to $(\delta\omega)y_i$ for each $\omega \in \Theta$ and $i \in \{1, \ldots, n\}$. The derivation ∂ on $\mathbb{R}$ is the unique derivation which extends the derivation on $\mathbb{K}$ and sends $\delta^d\partial^s y_i$ to $h_d\delta^d\partial^s y_i$ for all d, s and i. By construction, we have

Proposition 2.6. $\mathbb{K}\{\mathbb{Y}\} = \mathbb{K}[\Theta\mathbb{Y}]$ *and* $\Theta\mathbb{Y}$ *is a transcendence basis of* $\mathbb{K}\{Y\}$ *over* $\mathbb{K}$.

Remark 2.7. The Proposition implies that we may view DD-polynomials in $\mathbb{K}\{\mathbb{Y}\}$ either as DD-polynomials in a finite number of variables $\mathbb{Y}$ or as *ordinary polynomials* in an infinite number of variables $\Theta\mathbb{Y}$. In addition, we may regard them as pure *differential polynomials* in an infinite number of variables $\delta^{\mathbb{N}}\mathbb{Y}$. In this case, $y_{c,s,0}$ are considered as *differential indeterminates* and $y_{c,s,t}$ as the tth derivatives of $y_{c,s,0}$.

A *DD-ideal*, or simply an ideal, is a subset I of $\mathbb{R}$, which is an algebraic ideal in $\mathbb{R}$ and is closed under ∂ and δ. An ideal I is called *reflexive* if $\delta P \in I$ implies $P \in I$, for all $P \in \mathbb{R}$. Let $\mathbb{P}$ be a set of elements of $\mathbb{R}$. The ideal generated by $\mathbb{P}$ is denoted by $[\mathbb{P}]$. Obviously, $[\mathbb{P}]$ is the set of all linear combinations of transforms of successive derivatives of the DD-polynomials in $\mathbb{P}$. Given $P \in \mathbb{R}$, let

$$\mathbf{\Delta}_P = \{P^{i_0} \cdots (\delta^r P)^{i_r} | i_0, \ldots, i_r \in \mathbb{N}\}.$$

An ideal I is called *perfect* if $\mathbf{\Delta}_P \cap I \neq \emptyset$ implies $P \in I$ for all $P \in \mathbb{R}$. The perfect ideal generated by $\mathbb{P}$ is denoted as $\{\mathbb{P}\}$. A perfect ideal is always reflexive. An ideal I is called a *prime ideal* if for DD-polynomials P and Q, $PQ \in I$ implies $P \in I$ or $Q \in I$.

For a set of DD-polynomials $\mathbb{P}$, we write $(\mathbb{P})$ for the ordinary or *algebraic ideal* generated by $\mathbb{P}$, and $[\mathbb{P}]_\partial$ for the *differential ideal* generated by $\mathbb{P}$.

2.3. Admissible orderings

Consider a total ordering $\leq$ on $\Theta\mathbb{Y}$. For a DD-polynomial $P \in \mathbb{K}[\Theta Y]$, we define V_P to be the set of all elements of ΘY occurring in P. If $\mathbb{P}$ is a subset of $\mathbb{K}[\Theta Y]$, then we set $V_{\mathbb{P}} = \bigcup_{P\in\mathbb{P}} V_P$. If $V_P \neq \emptyset$, then V_P has a maximal element for $\leq$, which is denoted by v_P or $v(P)$. We call it the *leader* of P.

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

The ordering $\leq$ is said to be *admissible* if

$$\begin{array}{lll} A_1: & v(\theta y) < v(\delta\theta y), & \text{for any } \theta y \in \Theta Y;\\ & v(\theta y) < v(\partial\theta y), & \text{for any } \theta y \in \Theta Y;\\ A_2: & v(\delta\theta y) \leq v(\delta\theta' y'), & \text{for any } \theta y \leq \theta' y' \text{ in } \Theta Y;\\ & v(\partial\theta y) \leq v(\partial\theta' y'), & \text{for any } \theta y \leq \theta' y' \text{ in } \Theta Y. \end{array}$$

Admissible orderings exist: one example is the ordering $\leq_l$ defined by:

$$\delta^{d_1}\partial^{s_1} y_{c_1} \leq_l \delta^{d_2}\partial^{s_2} y_{c_2} \Longleftrightarrow (c_1, d_1, s_1) \leq_{lex} (c_2, d_2, s_2),$$

where $\leq_{lex}$ stands for the pure lexicographical ordering. Another popular ordering is the *total order based* ordering:

$$\delta^{d_1}\partial^{s_1} y_i <_o \delta^{d_2}\partial^{s_2} y_j \Longleftrightarrow (d_1 + s_1, d_1, s_1, i) <_{lex} (d_2 + s_2, d_2, s_2, j).$$

In this paper, we will always assume that $\leq$ is admissible. We will also assume that $y_1 < \cdots < y_n$, which can always be made to hold after a permutation of indexes.

An *extended variable* is an element of $\Theta\mathbb{Y}$ raised to some strictly positive power. The set of such variables will be denoted by $(\Theta\mathbb{Y})^*$, and we use letters with star exponents v^* to denote extended variables. We extend the admissible ordering $\leq$ on variables to extended variables by $v^d \leq (v')^e$, if and only if either $v < v'$, or $v = v'$ and $d \leq e$. The *extended leader* of a non-ground DD-polynomial P is denoted by $v_P^* = v_P^{\deg(P, v_P)}$. The admissible ordering $\leq$ can be extended to DD-polynomials. For DD-polynomials P and Q, we will write $P \leq Q$ if $v_P^* \leq v_Q^*$. If $v_P^* = v_Q^*$, then we will write $P \sim Q$.

Lemma 2.8. *Let $P_i \in \mathbb{K}[\Theta\mathbb{Y}]$. Then any descending sequence $P_1 > P_2 > P_3 > \cdots$ is finite.*

Proof. The sequence $(P_i)_{i\in\mathbb{N}}$ induces a sequence $(a_i, b_i, c_i, d_i)_{i\in\mathbb{N}}$ with $v^*(P_i) = (\delta^{b_i}\partial^{c_i} y_{a_i})^{d_i}$. Similarly, the ordering $\leq$ on $(\Theta\mathbb{Y})^*$ induces a total ordering $\leq'$ on $\{1, \ldots, n\} \times \mathbb{N}^3$, which extends the canonical partial product ordering. Now for any a_i, the sequence $(b_i, c_i, d_i)_{i\in\mathbb{N}}$ is strictly decreasing for $\leq'$, whence its finiteness, by Dickson's Lemma. □

2.4. Pseudo-remainders

We consider the DD-ring $\mathbb{K}[\Theta\mathbb{Y}]$, where $\mathbb{Y} = \{y_1, \ldots, y_n\}$. Let $\mathbb{Y}_c = \{y_1, \ldots, y_c\}$. For a DD-polynomial $P \in \mathbb{K}[\Theta\mathbb{Y}]$, we define the *class* of P to be the smallest $c = \mathrm{cls}(P)$ such that $P \in \mathbb{K}[\Theta\mathbb{Y}_c]$. If $P \in \mathbb{K}$, then we set $\mathrm{cls}(P) = 0$. If the leader of P is $\theta y_c = y_{c,i,j}$, then we define $\mathrm{ord}(P) = i + j$, $\mathrm{ord}_\delta(P, y_c) = i$, $\mathrm{ord}_\partial(P, y_c) = j$.

If the leader of $P \in \mathbb{R} \setminus \mathbb{K}$ is $y_{c,d,s}$, then P has the following canonical representation:

$$P = P_t y_{c,d,s}^t + P_{t-1} y_{c,d,s}^{t-1} + \cdots + P_0, \tag{4}$$

where $v_{P_i} < v_P$ $(i = 0, \ldots, t)$. $I_P = P_t$ is called the *initial* of P. $\mathrm{ldeg}(P) = t$ is called the *leading degree* of P. Applying ∂ and δ to P, we have

Lemma 2.9. *Let P be of form (4). Then*

$$\begin{aligned} \delta P &= (\delta P_t) y_{c,d+1,s}^t + (\delta P_{t-1}) y_{c,d+1,s}^{t-1} + \cdots + \delta P_0\\ \partial P &= S_P y_{c,d,s+1} + R, \end{aligned}$$

where

$$S_P = \prod_{i=0}^{d-1} \delta^i(h) \frac{\partial P}{\partial y_{c,d,s}}$$

is called the separant *of P and R is a DD-polynomial with lower leading variable than $y_{c,d,s+1}$.*

Proof. The first equation is obvious. The second one is a consequence of (2). □

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

Algorithm 1 — rprem(Q, P)

Input: DD-polynomials $P, Q \in \mathbb{R}$ with $P \neq 0$.
Output: The pseudo-remainder of Q w.r.t. P.

If $P \in \mathbb{K}$ then return 0.
Set $R := Q$.
While $\exists \omega^* \in V_R^*, v_P^* \preceq \omega^*$ do
  Choose the highest ω^* under $\preceq$.
  Set $R := \text{aprem}(R, (\omega/v_P)P)$. /*/
Return R

/*/ aprem(P, Q) stands for the algebraic pseudo-remainder of P w.r.t. Q in variable v_Q.

If the leader of $P \in \mathbb{R} \setminus \mathbb{K}$ is $y_{c,d,s}$, then we say that Q is *reduced* w.r.t. P if and only if (1) $y_{c,d+k,s+l}$ does not occur in Q for $k \geq 0$, $l > 0$ and (2) $\deg(Q, y_{c,d+k,s}) < \deg(P, y_{c,d,s})$ for $k \geq 0$. If $P \in \mathbb{K} \setminus \{0\}$, then 0 is the only DD-polynomial which is reduced w.r.t. P.

We define a partial ordering $\preceq$ on Θ by

$$\theta = \delta^{\alpha}\partial^{\beta} \preceq \delta^{\alpha'}\partial^{\beta'} = \theta' \Longleftrightarrow \alpha \leq \alpha' \wedge \beta \leq \beta'.$$

If $\theta \preceq \theta'$, then we define

$$\theta'/\theta = \delta^{\alpha'-\alpha}\partial^{\beta'-\beta}$$

and notice that $(\theta'/\theta)\theta$ is a shuffle of θ'.

We define a *partial ordering* $\preceq$ on extended variables by $v^* = (\theta y_i)^d \preceq (\theta' y_i)^e = (v')^*$, if and only if $\theta \preceq \theta'$ and either $d \leq e$, or θ'/θ is not a pure difference operator. We remark that $\preceq$ is still a well-quasi-ordering.

Consider DD-polynomials $P, Q \in \mathbb{R}$ with $P \neq 0$. Then the algorithm **rprem** computes the *pseudo-remainder of* Q *w.r.t.* P. It is easily checked that rprem(Q, P) is reduced w.r.t. P.

Lemma 2.10. *Define*

$$H_P = I_P S_P$$
$$\mathbf{H}_P = \mathbf{\Delta}_{I_P}\mathbf{\Delta}_{S_P} = \{IS | I \in \mathbf{\Delta}_{I_P}, S \in \mathbf{\Delta}_{H_P}\}.$$

and let $R = \text{rprem}(Q, P)$. *Then there exists an* $H \in \mathbf{H}_P$ *such that* $v_H < v_Q$ *and*

$$HQ = R \mod [P],$$

where we recall that $[P]$ *stands for the DD-ideal generated by* P.

Proof. For every step of the loop of the above procedure, the order of $I_{(\omega/v_P)P}$ is less than the order of $v(Q)$, so this is a direct consequence of the above procedure and Lemma 2.9. □

2.5. Zero sets

Let $\mathbb{P} \subset \mathbb{K}\{\mathbb{Y}\}$ be a finite system of DD-polynomials and let $\hat{\mathbb{K}}$ be a DD-superfield of $\mathbb{K}$. A *zero* of $\mathbb{P}$ in $\hat{\mathbb{K}}$ is a tuple $(\hat{y}_1, \ldots, \hat{y}_n) \in \hat{\mathbb{K}}^n$ with $P(\hat{y}_1, \ldots, \hat{y}_n) = 0$ for all $P \in \mathbb{P}$. We use Zero$(\mathbb{P})$ to denote the set of all zeros of $\mathbb{P}$. Let D be a polynomial. We use Zero$(\mathbb{P}/D)$ to denote the set of zeros of $\mathbb{P}$ which do not annul D.

If $(\hat{y}_1, \ldots, \hat{y}_n)$ is a zero of $\mathbb{P}$, the DD-morphism $\rho : \mathbb{K}\{\mathbb{Y}\} \to \hat{\mathbb{K}}$ over $\mathbb{K}$ with $\rho(y_i) = \hat{y}_i$ for each i is called a model of $\mathbb{P}$. There is a close relationship between the existence of models and the non-triviality of the perfect DD-ideal $\{\mathbb{P}\}$:

Proposition 2.11. *The system* $\mathbb{P}$ *admits a model if and only if* $1 \notin \{\mathbb{P}\}$.

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

Proof. Assume that $\mathbb{P}$ admits a model $\rho : \mathbb{K}\{\mathbb{Y}\} \to \hat{\mathbb{K}}$. Then $\mathbb{P} \subseteq \ker\rho$ and $\{\mathbb{P}\} \subseteq \{\ker\rho\}$. Moreover, the DD-ideal $\ker\rho$ is perfect: given $P \in \mathbb{K}\{\mathbb{Y}\}$ with $P^{i_0}\cdots(\delta^k P)^{i_k} \in \ker\rho$, we have $\rho(P)^{i_0}\cdots(\delta^k\rho(\mathbb{P}))^{i_k} = 0$. Since $\hat{\mathbb{K}}$ is a DD-field, it follows that $\delta^j\rho(\mathbb{P}) = 0$, whence $\rho(\mathbb{P}) = 0$ and $\mathbb{P} \in \ker\rho$. Having proved that $\ker\rho$ is perfect, it follows that $\{\mathbb{P}\} \subseteq \ker\rho$. We conclude that $1 \notin \{\mathbb{P}\}$, since $1 \notin \ker\rho$.

Conversely, if $1 \notin \{\mathbb{P}\}$, then a similar argument as in the proof of Lemma 3.14 yields the existence of a perfect prime DD-ideal $\mathfrak{p} \supseteq \{\mathbb{P}\}$. Consider the natural DD-morphism ρ of $\mathbb{K}$ into the fraction field $\hat{\mathbb{K}}$ of the DD-ring $\hat{\mathbb{R}} = \mathbb{R}/\mathfrak{p}$. By construction, $\rho(\mathbb{P}) = 0$, so ρ is a model for $\mathbb{P}$. □

Remark 2.12. More generally, one may consider a system of DD-equations $\mathbb{P} \subseteq \mathbb{K}\{\mathbb{Y}\}$ together with one DD-inequation $Q \in \mathbb{K}\{\mathbb{Y}\}$. In that case, a model of $\mathbb{P} = 0$, $Q \neq 0$ is a DD-morphism $\rho : \mathbb{K}\{\mathbb{Y}\} \to \hat{\mathbb{K}}$ over $\mathbb{K}$ with $\rho(\mathbb{P}) = 0$ and $\rho(Q) \neq 0$. In a similar way as above, one proves that $\mathbb{P} = 0$, $Q \neq 0$ admits a model if and only if $Q \notin \{\mathbb{P}\}$. Furthermore, $Q \notin \{\mathbb{P}\}$ if and only if $1 \notin \{P\} : \mathbf{H}_Q$.

Remark 2.13. Assuming that $\mathbb{K}$ is a field of meromorphic functions and that δ is the right composition with an analytic function ϕ, an interesting question is to find models $\rho : \mathbb{K}\{\mathbb{Y}\} \to \hat{\mathbb{K}}$ of $\mathbb{P}$ in DD-fields $\hat{\mathbb{K}}$ with a more analytic flavour. A typical candidate for $\hat{\mathbb{K}}$ would be the DD-field of ultimate sequences $(f_n)_{n\geq n_0}$ of analytic germs at points z_n with $z_{n+1} = \phi(z_n)$, by taking $(\delta f)_{n-1} = f_n \circ \phi$.

3. Characteristic sets of DD-polynomial ideals

3.1. Auto-reduced sets

A subset $\mathcal{A} \subseteq \mathbb{K}\{\mathbb{Y}\} \setminus \mathbb{K}$ is said to be *auto-reduced*, if each $P \in \mathcal{A}$ is reduced w.r.t. each DD-polynomial in $\mathcal{A} \setminus \{P\}$. An auto-reduced set $\mathcal{A} = \{A_1, \ldots, A_r\}$ with $v_{A_1} < \cdots < v_{A_r}$ is called an *ascending chain* or simply a *chain*.

Given $y_{i,d,s}$ to be the leading variable of a polynomial in $\mathcal{A}$, we define its *DD-index* to be (d, s). The structure of a chain could be easily understood from the DD-indices of its elements.

Proposition 3.1. *Let $\mathcal{A}$ be a chain. The set of indices for the polynomials in $\mathcal{A}$ with a fixed class i will be denoted by* IND_i. *If we arrange* $\mathrm{IND}_i = \{(a_1, b_1), \ldots, (a_s, b_s)\}$ *such that $a_1 \leq a_2 \leq \cdots \leq a_s$. Then we have*

- $a_1 < a_2 < \cdots < a_s$ *and* $b_1 \geq b_2 \geq \cdots \geq b_s$.
- *If $b_j = b_{j+1}$, then $d_{(a_j,b_j)} < d_{(a_{j+1},b_{j+1})}$, where $d_{(a_j,b_j)}$ is the leading degree of the polynomial with index* (a_j, b_j).

Proof. Let A_1 and A_2 be the corresponding DD-polynomials of (a_1, b_1) and (a_2, b_2). We show that $a_1 = a_2$ cannot happen. Otherwise, consider b_1 and b_2. If $b_1 = b_2$, then A_1 and A_2 have the same leader, which is impossible. If $b_1 < b_2$, then A_2 is not reduced w.r.t. A_1, which is also impossible. Similarly, $b_1 > b_2$ cannot happen. This proves that $a_1 < a_2$. Similarly, we can prove that $a_i < a_{i+1}$. If $b_j = b_{j+1}$, since the corresponding DD-polynomials of (a_j, b_j), (a_{j+1}, b_{j+1}) are auto-reduced, we have $d_{(a_j,b_j)} < d_{(a_{j+1},b_{j+1})}$. □

We use the following example to illustrate the above result.

Example 3.2. Consider the following chain for the ordering $\leq_l$ from Section 2.2.

$$\begin{aligned} \mathcal{A} &= \{A_1, A_2, A_3, A_4\} \\ A_1 &= y_{1,2,3}^2 \\ A_2 &= y_{1,3,2}^2 + y_{1,1,1} \\ A_3 &= y_{1,5,0}^2 + y_{1,4,1} \\ A_4 &= y_{1,7,0} + y_{1,4,0}. \end{aligned} \tag{5}$$

The DD-indices for the DD-polynomials in $\mathcal{A}$ are given in Fig. 1.

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

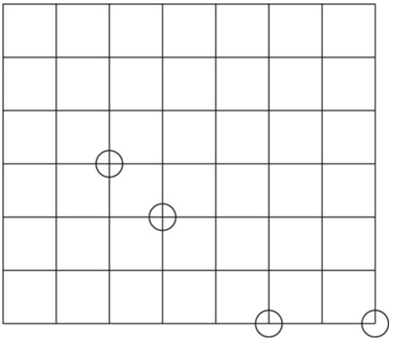

Fig. 1. The indices of chain $\mathcal{A}$ from (5).

Lemma 3.3. *Any auto-reduced set is finite.*

Proof. Assume the contrary and consider an infinite auto-reduced set $\{P_1, P_2, \ldots\}$. The sequence $P_1, P_2, \ldots$ induces a sequence $(a_i, b_i, c_i, d_i)_{i\in\mathbb{N}}$ with $v^*(P_i) = (\delta^{b_i}\partial^{c_i}y_{a_i})^{d_i}$ and modulo the extraction of a subsequence, we may assume without loss of generality that $a_i = a_j$ for all i, j. If P_i is reduced w.r.t. P_j, then we cannot have $(b_i, c_i, d_i) \succeq (b_j, c_j, d_j)$ for the partial product ordering on $\mathbb{N}^3$. It follows that $(b_1, c_1, d_1), (b_2, c_2, d_2), \ldots$ are pairwise distinct and incomparable for $\preceq$. This contradicts Dickson's Lemma. □

Let $\mathcal{A} = \{A_1, \ldots, A_p\}$ and $\mathcal{B} = \{B_1, \ldots, B_q\}$ be chains. We define a partial ordering $\leq$ on chains by setting $\mathcal{A} \leq \mathcal{B}$ if there exists a j with $A_i \sim B_i$ for $1 \leq i < j$ and either $A_j < B_j$ or $j = q + 1 \leq p$. The ordering $\leq$ is also called a *ranking*.

Lemma 3.4. *Any descending chain $\mathcal{A}_1 > \mathcal{A}_2 > \mathcal{A}_3 > \cdots$ is finite.*

Proof. Assume the contrary. The first elements of the chains $\mathcal{A}_1, \mathcal{A}_2, \ldots$ satisfy $\mathcal{A}_{1,1} \geq \mathcal{A}_{2,1} \geq \cdots$. By Lemma 2.8, there exists an index j_1 with $A_{i,1} \sim A_{j_1,1}$ for all $i \geq j_1$. Similarly, there exists an index $j_2 > j_1$ with $A_{i,2} \sim A_{j_2,2}$ for all $i \geq j_2$. By induction, we get a sequence $j_1 < j_2 < \cdots$ with $A_{i,k} \sim A_{j_k,j}$ for all k and $i \geq j_k$. But then $\{A_{j_1,1}, A_{j_2,2}, \ldots\}$ is an infinite auto-reduced set, which contradicts Lemma 3.3. □

Let $\mathbb{P}$ be a set of DD-polynomials and consider the set of chains of DD-polynomials in $\mathbb{P}$. Among all those chains, the above Lemma implies that there exists at least one chain with lowest rank. Such a chain is called a *characteristic set* of $\mathbb{P}$.

A DD-polynomial is said to be *reduced w.r.t. a chain* if it is reduced to every DD-polynomial in the chain.

Lemma 3.5. *If $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ and $\mathcal{A}'$ a characteristic set of $\mathbb{P} \cup \{P\}$ for a DD-polynomial P, then we have $\mathcal{A} \geq \mathcal{A}'$. Moreover, if P is reduced w.r.t. $\mathcal{A}$, then $\mathcal{A} > \mathcal{A}'$.*

Proof. The first statement is obviously true, since the characteristic set of $\mathbb{P}$ is in $\mathbb{P} \cup \{P\}$. As to the second statement, assume $\mathcal{A} = A_1, \ldots, A_p$ and $P \in \mathbb{P}$, with $\mathrm{cls}(P) = m$, is reduced w.r.t. $\mathcal{A}$. If $m > \mathrm{cls}(A_p)$, then the chain $A_1, \ldots, A_p, P$ is of rank lower than $\mathcal{A}$. If $\mathrm{cls}(A_{k-1}) < m \leq \mathrm{cls}(A_k) \leq \mathrm{cls}(A_p)$, then the chain $A_1, \ldots, A_{k-1}, P$ is of rank lower than $\mathcal{A}$. Hence $\mathcal{A} > \mathcal{A}'$. □

Lemma 3.6. *A chain $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ if and only if $\mathbb{P}$ does not contain a non-zero DD-polynomial which is reduced w.r.t. $\mathcal{A}$.*

Proof. By Lemma 3.5, we just need to prove the sufficiency. Assume $\mathcal{B} = B_1, \ldots, B_s$ is the characteristic set of $\mathbb{P}$, while $\mathcal{A}$ is not. We have $\mathcal{B} < \mathcal{A}$. If there exists a $k \leq \min\{s, p\}$ with $B_k < A_k$, then B_k is reduced w.r.t. $\mathcal{A}$. Otherwise $s > p$ and B_{p+1} is reduced w.r.t. $\mathcal{A}$. Both of the cases contradict the hypothesis and show that $\mathcal{A}$ is the characteristic set of $\mathbb{P}$. □

3.2. Extension of chains and pseudo-remainders

To compute the pseudo-remainder of Q w.r.t. P, we need to lift the difference and differential orders of P by considering θP for certain $\theta \in \Theta$. In order to compute the pseudo-remainder of a DD-polynomial w.r.t. a chain, we also need to select a DD-polynomial in the chain and to lift its orders. But, the selection of the DD-polynomial is not unique. More seriously, for some DD-polynomial A selected from the chain and the corresponding DD-operator θ, θA might be linear in its leader, and for other DD-polynomials, the lifted DD-polynomial might not be linear in its leader. In order to give a proper definition for pseudo-remainders, we introduce the concept of extension for chains.

Let $\mathcal{A}$ be a chain. A variable $y_{c,d,s}$ is called a *principal variable* of $\mathcal{A}$ if there exists an $A \in \mathcal{A}$ such that $v_A \preceq y_{c,d,s}$. Otherwise, it is called a *parametric variable* of $\mathcal{A}$. Denote the set of principal variables and the parametric variables of $\mathcal{A}$ by $\mathbb{M}_{\mathcal{A}}$ and $\mathbb{P}_{\mathcal{A}}$ respectively. It is clear that

$$\mathbb{M}_{\mathcal{A}} \cup \mathbb{P}_{\mathcal{A}} = \Theta\mathbb{Y}. \tag{6}$$

For a DD-polynomial set $\mathbb{P}$ and $1 \le c \le n$, let $d_{\mathbb{P}}^{(c)}$ be the largest d such that $y_{c,d,s}$ occurs in $\mathbb{P}$, $s_{\mathbb{P}}^{(c)}$ the largest s such that $y_{c,d,s}$ occurs in $\mathbb{P}$, and

$$\begin{aligned}\mathbb{V}_{\mathbb{P}} &= \{y_{c,s,t} \in \mathbb{M}_{\mathcal{A}} | \exists P \in \mathbb{P}, a, b : \deg(P, y_{c,a,b}) > 0, 1 \le c \le n, s \le a, t \le b\}.\\ \mathbb{L}_{\mathbb{P}} &= \{y_{c,s,t} | \exists P \in \mathbb{P} : v_P = y_{c,s,t}\}.\end{aligned}$$

So $\mathbb{L}_{\mathbb{P}}$ is the set of leading variables of $\mathbb{P}$ and $\mathbb{V}_{\mathbb{P}}$ is the set of principal variables such that for any $v = y_{c,s,t}$ occurring in $\mathbb{P}$, all principal variables u of $\mathcal{A}$ satisfying $u \preceq v$ are in $\mathbb{V}_{\mathbb{P}}$. Note that $\mathbb{V}_{\mathbb{P}}$ implicitly depends on $\mathcal{A}$.

For a chain $\mathcal{A}$ and a set of DD-polynomials $\mathbb{P}$, we say that $\mathcal{A}_{\mathbb{P}}$ is an *extension of* $\mathcal{A}$ w.r.t. $\mathbb{P}$ if it satisfies the following properties:

- For any $P \in \mathcal{A}_{\mathbb{P}}$, there exist a $\theta \in \Theta$ and an $A \in \mathcal{A}$ such that $P = \theta A$.
- $\mathcal{A}_{\mathbb{P}}$ is an algebraic triangular set under the ordering $\le$ when all $y_{c,n,m}$ are considered as independent variables.
- $\mathbb{L}_{\mathcal{A}_{\mathbb{P}}} = \mathbb{V}_{\mathbb{P} \cup \mathcal{A}_{\mathbb{P}}}$. Intuitively, this means that if a principal variable v' of $\mathcal{A}$ occurs in $\mathbb{P} \cup \mathcal{A}_{\mathbb{P}}$, then any principal variable v satisfying $v \preceq v'$ should be the leading variable of some polynomial in $\mathcal{A}_{\mathbb{P}}$. This property guarantees that all the principle variables needed in computing a pseudo-remainder of any polynomial in $\mathbb{P}$ w.r.t. $\mathcal{A}$ will appear as leading variables of $\mathcal{A}_{\mathbb{P}}$.
- A DD-polynomial P is reduced w.r.t. $\mathcal{A}$ if and only if P is reduced w.r.t. $\mathcal{A}_P = \mathcal{A}_{\{P\}}$ when all $y_{c,n,m}$ are considered as independent variables. This property guarantees that for any $\theta A \in \mathcal{A}_{\mathbb{P}}$, θA has the lowest degree for all $\eta \in \Theta$ and $B \in \mathcal{A}$ such that $v_{\theta A} = v_{\eta B}$.

Given a DD-polynomial set $\mathbb{P}$, the algorithm **Extension** shows how to compute an extension of $\mathcal{A}$ w.r.t. $\mathbb{P}$, which is clearly satisfying the above properties. In what follows, we will use this algorithm to compute $\mathcal{A}_{\mathbb{P}}$.

Example 3.7. Continue from Example 3.2. For $P = y_{1,7,4}^2 + y_{1,3,2}$, we have $d_{\mathbb{Q}}^{(1)} = 7$, $s_{\mathbb{Q}}^{(1)} = 4$, and

$$\begin{aligned}\mathcal{A}_P = \{&A_1, \partial A_1, \partial^2 A_1, \partial^3 A_1,\\ &A_2, \partial A_2, \partial^2 A_2, \partial^3 A_2, \partial^4 A_2, \delta A_2, \delta\partial A_2, \delta\partial^2 A_2, \delta\partial^3 A_2, \delta\partial^4 A_2,\\ &A_3, \partial A_3, \partial^2 A_3, \partial^3 A_3, \partial^4 A_3, \partial^5 A_3, \delta A_3, \delta\partial A_3, \delta\partial^2 A_3, \delta\partial^3 A_3, \delta\partial^4 A_3,\\ &A_4, \partial A_4, \partial^2 A_4, \partial^3 A_4, \partial^4 A_4\}.\end{aligned}$$

Let $\omega y_1 = y_{1,5,4}$. Then for each of A_1, A_2, and A_3, its leader satisfies the condition in **S1**. The condition in **S2** is not satisfied. In **S3**, we choose the one with largest ord_δ, which is A_3. As a consequence, we will add $\partial^4 A_3$ to $\mathcal{A}_{\mathbb{P}}$. Notice that the DD-polynomial with the largest ord_δ will have the smallest ord_∂ for its leading variable.

The DD-indices for the DD-polynomials in $\mathcal{A}_{\mathbb{P}}$ are given in Fig. 2, where a solid dot represents the index of a newly added DD-polynomial.

Algorithm 2 — Extension($\mathcal{A}$,$\mathbb{P}$)

Input: A chain $\mathcal{A}$ and a set $\mathbb{P}$ of DD-polynomials.
Output: The extension $\mathcal{A}_{\mathbb{P}}$ of $\mathcal{A}$ w.r.t. $\mathbb{P}$.

S0. Let $L = \mathbb{L}_{\mathcal{A}}$, $\mathbb{Q} = \mathcal{A} \cup \mathbb{P}$, $\mathbb{H} = \{y_{c,d_{\mathbb{Q}}^{(c)},s_{\mathbb{Q}}^{(c)}}, c = 1, \ldots, n\}$, $V = \mathbb{V}_{\mathbb{H}} \setminus L$, and $\mathcal{A}_{\mathbb{P}} = \mathcal{A}$.

S1. If there exist ω, η and c with $\omega y_c \in V$, $\eta y_c \in L$ and $\eta \preceq \omega$, then choose ω and c such that ωy_c is largest for $\preceq$. If there are no such ω, η and c, then return $\mathcal{A}_{\mathbb{P}}$.

S2. If for all the $\theta y_c \in L$ satisfying $\theta \preceq \omega$, ω/θ is a difference operator, let η be the largest of those θ under $\preceq$, go to **S4**.

S3. If there exists a $\theta y_c \in L$ such that ω/θ is not a difference operator, let η be the one with largest in ord_δ. Go to **S4**.

S4. Let $A_i \in \mathcal{A}$ such that $v_{A_i} = \eta y_c$. Let $Q = (\omega/\eta)A_i$, $\mathcal{A}_{\mathbb{P}} = \mathcal{A}_{\mathbb{P}} \cup \{Q\}$, $V = V \cup (\mathbb{V}_Q \setminus \mathbb{L}_{\mathcal{A}_{\mathbb{P}}})$. Delete ωy_c from V and goto **S1**. Since all the variables in $\mathbb{V}_Q \setminus \mathbb{L}_{\mathcal{A}_{\mathbb{P}}}$ are less than ωy_c, this process will terminate.

For a DD-polynomial P, let $\mathcal{A}_P = \mathcal{A}_{\{P\}}$. The *pseudo-remainder* of a DD-polynomial P w.r.t. to a chain $\mathcal{A}$ is defined to be the algebraic pseudo-remainder of P w.r.t. to the algebraic triangular set $\mathcal{A}_P$:

$$\mathrm{rprem}(P, \mathcal{A}) = \mathrm{aprem}(P, \mathcal{A}_P).$$

Let $\mathcal{A} = A_1, \ldots, A_p$ be a chain. We define

$$\begin{aligned} \mathbf{\Delta}_{\mathcal{A}} &= \mathbf{\Delta}_{\mathcal{A}_1} \cdots \mathbf{\Delta}_{\mathcal{A}_p}, \\ H_{\mathcal{A}} &= H_{\mathcal{A}_1} \cdots H_{\mathcal{A}_p}, \\ \mathbf{H}_{\mathcal{A}} &= \mathbf{H}_{\mathcal{A}_1} \cdots \mathbf{H}_{\mathcal{A}_p}. \end{aligned}$$

Lemma 3.8. *Let $R = \mathrm{rprem}(Q, \mathcal{A})$. Then R is reduced w.r.t. $\mathcal{A}$ and there exists an $H \in \mathbf{H}_{\mathcal{A}}$ such that $v_H < v_Q$ and*

$$\begin{aligned} HQ &\equiv R \mod [\mathcal{A}] \\ HQ &\equiv R \mod (\mathcal{A}_Q). \end{aligned}$$

Proof. This is a direct consequence of the procedure to compute $\mathcal{A}_Q$ and rprem. □

The *saturation ideal* of $\mathcal{A}$ is defined to be

$$\mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbf{H}_{\mathcal{A}} = \{P \in \mathbb{K}[\Theta\mathbb{Y}] \mid \exists H \in \mathbf{H}_{\mathcal{A}} : HP \in [\mathcal{A}]\}.$$

Notice that $\mathbf{H}_{\mathcal{A}}$ is closed under translation and multiplication. Hence $\mathrm{sat}(\mathcal{A})$ is a DD-ideal. It is also clear that if $\mathrm{rprem}(P, \mathcal{A}) = 0$ then $P \in \mathrm{sat}(\mathcal{A})$. Conversely, $P \in \mathrm{sat}(\mathcal{A})$ generally does not imply $\mathrm{rprem}(P, \mathcal{A}) = 0$ and the condition for this to be valid will be given in Section 4.

3.3. Noetherian property of perfect ideals

As an application, we may prove that all perfect ideals in $\mathbb{K}[\Theta\mathbb{Y}]$ are finitely generated, or equivalently, the solutions for any set of DD-polynomials are the same as a finite set of DD-polynomials.

Given a DD-polynomial set $\mathbb{P}$, we inductively define

$$\begin{aligned} \mathbb{P}_0 &= \mathbb{P} \\ \mathbb{P}_n &= \{P | \mathbf{\Delta}_P \cap [\mathbb{P}_{n-1}] \neq \emptyset\}, \end{aligned}$$

so that

$$\{\mathbb{P}\} = \bigcup_{k \in \mathbb{N}} \mathbb{P}_k.$$

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

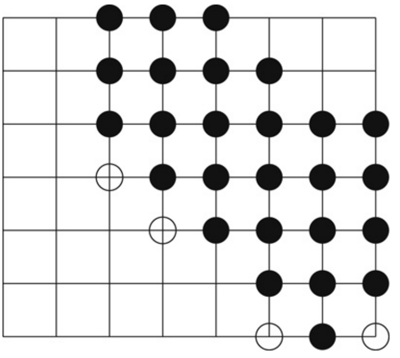

Fig. 2. The indices of chain $\mathcal{A}_P$.

Lemma 3.9. *Let* $P, Q \in \mathbb{K}[\Theta\mathbb{Y}]$. *Then* $(\delta^{r_1}\partial^{s_1}P)(\delta^{r_2}\partial^{s_2}Q) \in (PQ)_2$.

Proof. It is classical (see Ritt (1950), Page 9) that $(\partial^{s_1}P)(\partial^{s_2}Q) \in (PQ)_1$. Indeed, for any $A, B \in \mathbb{K}[\Theta\mathbb{Y}]$ with $AB \in [PQ]$, we have $A^2B' = A(AB)' - A'(AB) \in [PQ]$. By induction over n it follows that $AB^n \in [PQ] \Rightarrow (AB')^{2^n} \in [PQ]$. Hence $AB \in (PQ)_1 \Rightarrow AB' \in (PQ)_1$ and the result follows by induction over s_1 and s_2. We also have $(\delta^{r_1}P)(\delta^{r_2}Q) \in (PQ)_1$: assuming by symmetry that $d = r_2 - r_1 \geq 0$, we have $(\delta^{r_1}P)(\delta^{r_2}Q)\cdots(\delta^{r_1+d}P)(\delta^{r_2+d}Q) \in \delta^{r_2}(PQ)\mathbb{R} \subseteq [PQ]$. Applying the pure differential and the pure difference cases in turn, we obtain the Lemma. □

Lemma 3.10. *Let* $\mathbb{P}$ *be any set of elements of* $\mathbb{K}[\Theta\mathbb{Y}]$ *and* P *and* Q *any two elements of* $\mathbb{K}[\Theta\mathbb{Y}]$. *If* S *is contained in* $(\mathbb{P} \cup P)_n$ *and* T *in* $(\mathbb{P} \cup Q)_n$, $n \geq 1$, *then* ST *is contained in* $(\mathbb{P} \cup PQ)_{n+2}$.

Proof. We prove the Lemma by weak induction over n, i.e., if $n > 1$, then we assume the Lemma proved up to order $n-1$. Let $S \in (\mathbb{P} \cup P)_n$ and $T \in (\mathbb{P} \cup Q)_n$. Then there exist $\hat{S} = S^{i_0}\cdots(\delta^s S)^{i_s} \in \mathbf{\Delta}_S \cap [(\mathbb{P} \cup P)_{n-1}]$ and $\hat{T} = T^{j_0}\cdots(\delta^t T)^{j_t} \in \mathbf{\Delta}_T \cap [(\mathbb{P} \cup Q)_{n-1}]$. Increasing the i_k and j_k if necessary, we may assume without loss of generality that $(i_0, \ldots i_s) = (j_0, \ldots, j_t)$. Now $\hat{S}\hat{T}$ is a linear combination of terms of the form $U = (\delta^{r_1}\partial^{s_1}A)(\delta^{r_2}\partial^{s_2}B)$, with $A \in (\mathbb{P} \cup P)_{n-1}$ and $B \in (\mathbb{P} \cup Q)_{n-1}$. If $n = 1$, then Lemma 3.9 implies $U \in [\mathbb{P}] + (PQ)_2 \subseteq (\mathbb{P} \cup PQ)_2$. If $n > 1$, then again $U \in (\mathbb{P} \cup PQ)_{n+1}$, by the induction hypothesis. We conclude that $\hat{S}\hat{T} = (ST)^{i_0}\cdots(\delta^s(ST))^{i_s} \in [(\mathbb{P} \cup PQ)_{n+1}]$ and $ST \in (\mathbb{P} \cup PQ)_{n+2}$. □

Lemma 3.11. *Let* $\mathbb{P}$ *be any set of elements of* $\mathbb{K}[\Theta\mathbb{Y}]$ *and* P *and* Q *any two elements of* $\mathbb{K}[\mathbb{Y}]$. *Then* $\{\mathbb{P} \cup PQ\} = \{\mathbb{P} \cup P\} \cap \{\mathbb{P} \cup Q\}$.

Proof. We only need to show that, S being any element in the intersection, S is contained in $\{\mathbb{P} \cup PQ\}$. Let n be such that S is contained in $(\mathbb{P} \cup P)_n$ and in $(\mathbb{P} \cup Q)_n$. Then by Lemma 3.10, S^2 is in $(\mathbb{P} \cup PQ)_{n+2}$. Thus S is also in $(\mathbb{P} \cup PQ)_{n+2}$. □

Lemma 3.12. *Let* $\mathbb{P}, \mathbb{Q}$ *be two sets of elements of* $\mathbb{K}[\Theta\mathbb{Y}]$. *Then* $\{\mathbb{P}\} \cap \{\mathbb{Q}\} = \{\mathbb{P}\mathbb{Q}\}$.

Proof. In a similar way as for Lemma 3.10, one proves by induction over n that $\mathbb{P}_n \cap \mathbb{Q}_n \subseteq (\mathbb{P}\mathbb{Q})_{n+2}$. The result follows by passing to the limit. □

Lemma 3.13. *Let* $\mathbb{P}$ *be a subset of* $\mathbb{K}[\Theta\mathbb{Y}]$ *and* $P \in \{\mathbb{P}\}$. *Then there exists a finite subset* Σ *of* $\mathbb{P}$, *such that* $P \in \{\Sigma\}$.

Proof. Since $\{\mathbb{P}\} = \bigcup_{n\in\mathbb{N}} \mathbb{P}_n$, we have $P \in \mathbb{P}_n$ for some n. Let us prove the Lemma by induction on n. The case $n = 0$ is trivial. Assume that we have proved the Lemma up to $n - 1$. We have $\hat{P} \in [\mathbb{P}_{n-1}]$, for some $\hat{P} \in \mathbf{\Delta}_P$. Hence $\hat{P} \in [Q_1, \ldots, Q_q]$ for some $Q_1, \ldots, Q_q \in \mathbb{P}_{n-1}$. For each $1 \leq j \leq q$, there exists a finite subset Σ_j of $\mathbb{P}$, such that $Q_j \in \{\Sigma_j\}$, by the induction hypothesis. For $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_q$, we then have $P \in \{\Sigma\}$. □

Lemma 3.14. *If there exists a non-finitely generated perfect DD-ideal, then the set of non-finitely generated perfect DD-ideals admits a maximal element, and every such a maximal element is prime.*

Proof. The union of a totally ordered set of non-finitely generated perfect DD-ideals is again a non-finitely generated perfect DD-ideal. The existence of a maximal element follows therefore by Zorn's Lemma. Now let $\mathfrak{m}$ be any such maximal element. Clearly $\mathfrak{m} \neq \mathbb{K}$. Let $P, Q \in \mathbb{K}[\Theta\mathbb{Y}] \setminus \mathfrak{m}$. Then $\{\mathfrak{m}, P\}$ and $\{\mathfrak{m}, Q\}$ are finitely generated, say by Σ, resp. T. By Lemmas 3.11 and 3.12, we have $\{\mathfrak{m}, PQ\} = \{\Sigma\} \cap \{\mathrm{T}\} = \{\Sigma\mathrm{T}\}$, whence $PQ \notin \mathfrak{m}$. This proves that $\mathfrak{m}$ is prime. □

Theorem 3.15. *The DD-ring $\mathbb{K}[\Theta\mathbb{Y}]$ is Noetherian in the sense that all perfect ideals in $\mathbb{K}[\Theta\mathbb{Y}]$ are finitely generated.*

Proof. First we fix some admissible ordering on $\Theta\mathbb{Y}$. Suppose that the conclusion of the Theorem is false. By Lemma 3.14, there exists a maximal non-finitely generated perfect DD-ideal $\mathfrak{m}$, which is prime. Let $\mathcal{C}$ be a characteristic set for $\mathfrak{m}$.

Let P be in $\mathfrak{m}$. We can write $HP = R \mod [\mathcal{C}]$, where $H \in \mathbf{H}_{\mathcal{C}}$ and R is reduced w.r.t. $\mathcal{C}$. Now Lemma 3.6 implies $R = 0$, so $HP \in [\mathcal{C}]$ and $H_{\mathcal{C}}P \in \{\mathcal{C}\}$. This proves that $H_{\mathcal{C}}\mathfrak{m} \subseteq \{\mathcal{C}\}$.

Since the initials and separants of $\mathcal{C}$ are reduced w.r.t. $\mathcal{C}$, they are not in $\mathfrak{m}$. Since $\mathfrak{m}$ is prime, we have $H_{\mathcal{C}} \notin \mathfrak{m}$. So the perfect DD-ideal $\{H_{\mathcal{C}}, \mathfrak{m}\}$ strictly contains $\mathfrak{m}$. Therefore, $\{H_{\mathcal{C}}, \mathfrak{m}\}$ is finitely generated by the maximality hypothesis. Applying Lemma 3.13, each generator is in a perfect DD-ideal generated by a finite subset of $\mathfrak{m} \cup \{H_{\mathcal{C}}\}$. Hence, we can write $\{H_{\mathcal{C}}, \mathfrak{m}\} = \{H_{\mathcal{C}}, \mathbb{P}\}$, for some $\mathbb{P} \subseteq \mathfrak{m}$ and $\mathbb{P}$ is a finite set. We conclude that $\mathfrak{m}$ is finitely generated, since $\mathfrak{m} = \mathfrak{m} \cap \{H_{\mathcal{C}}, \mathfrak{m}\} = \mathfrak{m} \cap \{H_{\mathcal{C}}, \mathbb{P}\} = \{H_{\mathcal{C}}\mathfrak{m}, \mathbb{P}\} \subseteq \{\mathcal{C}, \mathbb{P}\}$. □

4. Coherent and regular chains

A key property for a chain $\mathcal{A}$ is whether it is the characteristic set of its saturation ideal $\mathrm{sat}(\mathcal{A})$. In this Section, we will give a necessary and sufficient condition for this property to hold.

4.1. Coherent chains

Consider two DD-polynomials $A_1, A_2 \in \mathbb{R} \setminus \mathbb{K}$. If $\mathrm{cls}(A_1) \neq \mathrm{cls}(A_2)$, then we define $\Delta(A_1, A_2) = 0$. If $\mathrm{cls}(A_1) = \mathrm{cls}(A_2) = c$, let $v_{A_1} = \theta_1 y_c$, $v_{A_2} = \theta_2 y_c$, and $\theta \in \Theta$ the smallest under $\preceq$ such that $\theta_1 \preceq \theta, \theta_2 \preceq \theta$. Ordering A_1 and A_2 such that $\deg((\theta/\theta_1)A_1) \geq \deg((\theta/\theta_2)A_2)$, we define the *$\Delta$-polynomial* of A_1 and A_2 to be

$$\Delta(A_1, A_2) = \mathrm{aprem}_{\theta y_c}((\theta/\theta_1)A_1, (\theta/\theta_2)A_2).$$

Given a chain $\mathcal{A} = A_1, \ldots, A_s$, we denote by $\Delta(\mathcal{A})$ the set of non-zero Δ-polynomials $\Delta(A_1, A_2)$ for all $A_1, A_2 \in \mathcal{A}$. A chain $\mathcal{A}$ is said to be *coherent*, if $\mathrm{rprem}(P, \mathcal{A}) = 0$ for all $P \in \Delta(\mathcal{A})$. A linear combination $C = \sum_{\theta \in \Theta} Q_\theta \theta A_i$ will be said to be *canonical* if θA_i in the expression are distinct elements in $\mathcal{A}_P$ for a DD-polynomial P. In other words, $C \in (\mathcal{A}_P)$.

Lemma 4.1. *Let $\mathcal{A}$ be a coherent chain, $A \in \mathcal{A}$, and $\theta \in \Theta$. Then there exist a DD-polynomial P and an $H \in \mathbf{H}_{\mathcal{A}}$ such that $v_H < v_{\theta A}$ and $H\theta A$ has a canonical representation:*

$$H\theta A = \sum_{v_B \leq v_A, B \in \mathcal{A}_P} Q_B B. \tag{7}$$

Proof. Let $c = \mathrm{cls}(A)$. The DD-polynomials in $\mathcal{A}$ with class c are $A_{c,1}, \ldots, A_{c,k_c}$ and $A = A_{c,i}$.

If $\theta A \in \mathcal{A}_{\theta A}$, the Lemma is true. Otherwise, we will prove this by induction on the ordering of $v_{\theta A}$. Let $A_{c,k}$ be largest w.r.t. $\leq$, such that $\mathrm{ord}_\delta(A_{c,k}) \leq \mathrm{ord}_\delta(\theta A)$. Then the B with $v_B = v_{\theta A}$ in (7) must be $\bar{\theta}_k A_{c,k}$ for a $\bar{\theta}_k \in \Theta$. Consider the Δ-polynomial $R = \Delta(A_{c,i}, A_{c,k})$ of $A_{c,k}$ and $A_{c,i}$. Then there exists $t \in \mathbb{N}, \theta_i \in \Theta$, and $\theta_k \in \Theta$, such that $v_{\theta_i A_{c,i}} = v_{\theta_k A_{c,k}}$ and

$$H_1^t \theta_i A = Q\theta_k A_{c,k} + R$$

where H_1 is either the initial or the separant of $A_{c,k}$ and $v_R < v_{\theta_i A}$. We have $v_{H_1} < v_{\theta_i A}$. Since $\mathcal{A}$ is a coherent chain, $\mathrm{rprem}(R, \mathcal{A}) = \mathrm{aprem}(R, A_R) = 0$. We have

$$H_2 R = \sum_{A \in A_R, v_A \leq v_R} B_A A,$$

where $H_2 \in \mathbf{H}_{\mathcal{A}}$ such that $v_{H_2} < v_R < v_{\theta_i A}$. So we have

$$H_2 H_1^t \theta_i A = H_2 Q \theta_k A_{c,k} + \sum_{A \in \mathcal{A}_R, v_A < v_{\theta_i A}} B_A A.$$

From the index diagram (Fig. 2), we have $\theta_i \preceq \theta$. Let $\bar{\theta} = \theta/\theta_i = \delta^d \partial^s$ and $\bar{\theta}_k \in \Theta$ be a shuffle of $\bar{\theta}\theta_k$. Perform $\bar{\theta}$ on the above equation, by Lemma 2.3, we have

$$g\delta^d (H_2 H_1^t)\theta A = F\bar{\theta}_k A_{c,k} + \sum_{B \in \mathcal{A}, \eta \in \Theta, v_{\eta B} < v_{\theta A}} C_B \eta B,$$

where $g \in \mathbb{K}$. Use the induction hypothesis, we have that each ηB has a canonical representation. So there exist a DD-polynomial P' and an $H_3 \in \mathbf{H}_{\mathcal{A}}$ with $v_{H_3} < v_{\theta A}$ such that

$$H_3 \left(\sum_{B \in \mathcal{A}, \eta \in \Theta, v_{\eta B} < v_{\theta A}} C_B \eta B \right) = \sum_{v_C < v_{\theta A}, C \in \mathcal{A}'_P} Q_C C.$$

Let $H = H_3 g \delta^d (H_2 H_1^t)$. Then $v_H < v_{\theta A}$, $H \in \mathbf{H}_{\mathcal{A}}$ and $H\theta A$ has a canonical representation of form (7). □

Lemma 4.2. *Let $\mathcal{A} = A_1, \ldots, A_l$ be a coherent chain. For any $f = \sum g_{i,j}\eta_j A_i$, there is an $H \in \mathbf{H}_{\mathcal{A}}$ such that $H \cdot f$ has a canonical representation, and $v_H < \max\{v_{\eta_j A_i}\}$.*

Proof. This is a direct consequence of Lemma 4.1. □

4.2. Regular algebraic triangular sets

We will recall some results about regularity of algebraic polynomials with respect to an algebraic triangular set.

Let $\mathcal{A} = A_1, \ldots, A_p$ be a non-trivial triangular set in $\mathbb{K}[x_1, \ldots, x_n]$ over a field $\mathbb{K}$ of characteristic zero. Let y_i be the leading variable of A_i, $y = \{y_1, \ldots, y_p\}$ and $u = \{x_1, \ldots, x_n\} \setminus y$. u is called the *parameter set* of $\mathcal{A}$. We can denote $\mathbb{K}[x_1, \ldots, x_n]$ as $\mathbb{K}[u, y]$. For a triangular set $\mathcal{A} = A_1, \ldots, A_p$, let

$$\begin{aligned} I_{\mathcal{A}} &= \{I_{A_1}^{i_1} \cdots I_{A_p}^{i_p} | i_1, \ldots, i_p, \in \mathbb{N}\} \qquad (8) \\ H_{\mathcal{A}} &= \{I_{A_1}^{i_1} S_{A_1}^{j_1} \cdots I_{A_p}^{i_p} S_{A_p}^{j_p} | i_1, j_1, \ldots, i_p, j_p \in \mathbb{N}\}. \end{aligned}$$

The quotient ideal

$$\mathrm{asat}(\mathcal{A}) = (\mathcal{A}) : I_{\mathcal{A}}$$

is called the *algebraic saturation ideal*.

For a polynomial P and a triangular set $\mathcal{A} = A_1, A_2, \ldots, A_p$ in $\mathbb{K}[u, y]$ with u as the parameter set, let

$$P_p = P, P_{i-1} = \mathrm{Resl}(P_i, A_i, y_i), i = p, \ldots, 1$$

and define $\mathrm{Resl}(P, \mathcal{A}) = P_0$, where $\mathrm{Resl}(P, Q, y)$ is the resultant of P and Q w.r.t. y. We assume that if y does not appear in P, $\mathrm{Resl}(P, Q, y) = P$. It is clear that $\mathrm{Resl}(P, \mathcal{A}) \in \mathbb{K}[u]$.

A polynomial P is said to be *regular* w.r.t. a triangular set $\mathcal{A}$ if $\mathrm{Resl}(P, \mathcal{A}) \neq 0$. $\mathcal{A} = A_1, \ldots, A_p$ is called *regular* if the initials of A_i are regular w.r.t. $\mathcal{A}$. $\mathcal{A}$ is called *saturated* if the initials and separants of A_i are regular w.r.t. $\mathcal{A}$.

Lemma 4.3 (Aubry et al., 1999). *Let $\mathcal{A}$ be a triangular set. Then $\mathcal{A}$ is a characteristic set of* $\mathrm{asat}(\mathcal{A}) = (\mathcal{A}) : I_{\mathcal{A}}$ *if and only if $\mathcal{A}$ is regular.*

Lemma 4.4 (Bouziane et al., 2001). *A polynomial g is not regular w.r.t. a regular triangular set $\mathcal{A}$ if and only if there is a non-zero f in $\mathbb{K}[u, y]$ such that $fg \in (\mathcal{A})$ and g is reduced w.r.t. $\mathcal{A}$.*

Lemma 4.5 (Aubry et al., 1999, Bouziane et al., 2001). *Let $\mathcal{A}$ be a regular triangular set. Then a polynomial P is regular w.r.t. $\mathcal{A}$ if and only if $(P, \mathcal{A}) \cap \mathbb{K}[u] \neq \{0\}$.*

Lemma 4.6 (Bouziane et al., 2001, Hubert, 2000). *Let $\mathcal{A}$ be a saturated triangular set. Then $(\mathcal{A}) : I_{\mathcal{A}} = (\mathcal{A}) : H_{\mathcal{A}}$ is a radical ideal.*

4.3. Regular chains

Let $\mathcal{A}$ be a chain and P a DD-polynomial. P is said to be *regular* w.r.t. $\mathcal{A}$ if it is regular w.r.t. $\mathcal{A}_P$ when P and $\mathcal{A}_P$ are treated as algebraic polynomials. We say that $\mathcal{A}$ is *regular* if any DD-polynomial in $\mathbf{H}_{\mathcal{A}}$ is regular w.r.t. $\mathcal{A}$.

Lemma 4.7. *If a chain $\mathcal{A}$ is a characteristic set of* $\mathrm{sat}(\mathcal{A})$*, then for any DD-polynomial P, $\mathcal{A}_P$ is a regular algebraic triangular set.*

Proof. By Lemma 4.3, we only need to prove that $\mathcal{B} = \mathcal{A}_P$ is the characteristic set of $(\mathcal{B}) : I_{\mathcal{B}}$. Let W be the set of all the θy_j such that θy_j is of lower or equal ordering than a $\bar{\theta} y_j$ occurring in $\mathcal{B}$. Then $\mathcal{B} \subseteq \mathbb{K}[W]$. If $\mathcal{B}$ is not a characteristic set of $(\mathcal{B}) : I_{\mathcal{B}}$, then there exists a non-zero $Q \in (\mathcal{B}) : I_{\mathcal{B}} \cap \mathbb{K}[W]$ which is reduced w.r.t. $\mathcal{B}$. Q does not contain any θy_i of higher ordering than those in W. As a consequence, Q is also reduced w.r.t. $\mathcal{A}$. Since $Q \in (\mathcal{B}) : I_{\mathcal{B}} \subseteq \mathrm{sat}(\mathcal{A})$ and $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$ (by Lemma 3.6), we get the contradiction $Q = 0$. □

Lemma 4.8. *Let $\mathcal{A}$ be a coherent and regular chain, and R a DD-polynomial reduced w.r.t. $\mathcal{A}$. If $R \in \mathrm{sat}(\mathcal{A})$, then $R = 0$, or equivalently, $\mathcal{A}$ is the characteristic set of* $\mathrm{sat}(\mathcal{A})$.

Proof. Let $\mathcal{A} = A_1, A_2, \ldots, A_l$. Since $R \in \mathrm{sat}(\mathcal{A})$, there is an $H_1 \in \mathbf{H}_{\mathcal{A}}$ such that $H_1 \cdot R \equiv 0 \mod [\mathcal{A}]$. Since $\mathcal{A}$ is regular, H_1 is difference regular w.r.t. $\mathcal{A}$, that is, there exists a DD-polynomial $\bar{H_1}$ and a non-zero $N \in \mathbb{K}[V]$ such that

$$\bar{H_1} \cdot H_1 = N + \sum_{v_B \le v_{H_1}, B \in \mathcal{A}_{H_1}} Q_B B$$

where V is the set of parameters of A_{H_1} as an algebraic triangular set. Hence,

$$NR \equiv \bar{H_1} \cdot H_1 \cdot R \equiv 0 \mod [\mathcal{A}].$$

Or equivalently,

$$N \cdot R = \sum g_{i,j} \theta_{i,j} A_j. \tag{9}$$

Since $\mathcal{A}$ is a coherent chain, by Lemma 4.2, there is an $H_2 \in \mathbf{H}_{\mathcal{A}}$ such that $H_2 \cdot N \cdot R$ has a canonical representation, where $v_{H_2} < \max\{v_{\theta_{i,j} A_j}\}$ in Eq. (9). That is

$$H_2 \cdot N \cdot R = \sum_{ij} \bar{g}_{i,j} \rho_{i,j} A_j, \tag{10}$$

where $v_{\rho_{i,j} A_j}$ are pairwise different. If $\max\{v_{\rho_{i,j} A_j}\}$ in (10) is lower than $\max\{v_{\theta_{i,j} A_j}\}$ in (9), we have already reduced the highest ordering of $v_{\theta_{i,j} A_j}$ in (9). Otherwise, assume $v_{\rho_a A_b} = \max\{v_{\rho_{i,j} A_j}\}$ and $\rho_a A_b = I_b \cdot v_{\rho_a A_b}^{d_b} + R_b$. Substituting $v_{\rho_a A_b}^{d_b}$ by $-\frac{R_b}{I_b}$ in (10) leaves the left-hand side unchanged since $v_{H_2} < v_{\rho_a A_b}$, N is free of $v_{\rho_a A_b}$ and $\deg(R, v_{\rho_a A_b}) < \deg(\rho_a A_b, v_{\rho_a A_b})$. In the right-hand side, $\rho_a A_b$ becomes zero, i.e. $\max\{v_{\rho_{i,j} A_j}\}$ decreases. Clearing denominators of the substituted formula of (10), we obtain a new equation:

$$I_b^t \cdot H_2 \cdot N \cdot R = \sum f_{ij} \tau_{i,j} A_j. \tag{11}$$

Notice that in the right-hand side of (11), the highest ordering of $\tau_{i,j} A_j$ and $I_b^t \cdot H_2$ are less than $v_{\rho_a A_b}$ and $I_b^t \cdot H_2$ is regular w.r.t. $\mathcal{A}$. Then after multiplying a DD-polynomial, the right-hand side of (11) can be represented as a linear combination of $\tau_{i,j} A_j$ all of which is strictly lower than $v_{\rho_a A_b}$. Repeating the above process, we can obtain a non-zero $\bar{N} \in \mathbb{K}[V]$, such that

$$\bar{N} \cdot R = 0.$$

Then $R = 0$. By Lemma 3.6, $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. □

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

The above Lemma is a modified differential–difference version of Rosenfeld's Lemma (Rosenfeld, 1959). Notice that both the condition and the conclusion are stronger in our version. The following example shows that Rosenfeld's Lemma (Rosenfeld, 1959) cannot directly be extended to differential–difference case. Consequently, the approach proposed in Boulier et al. (1995) does not directly generalize to the differential–difference setting.

Example 4.9. Let us consider the chain $\mathcal{A} = \{y_{1,1,0}^2 - 1, (y_{1,0,0} - 1)y_{2,0,0}^2 + 1\}$ in $\mathbb{K}\{y_1, y_2\}$. $\mathcal{A}$ is coherent and $y_{1,1,0} + 1$ is reduced w.r.t. $\mathcal{A}$. $y_{1,1,0} + 1 \in \text{sat}(\mathcal{A})$, because $H = \mathrm{I}_{(y_{1,0,0}-1)y_{2,0,0}^2+1} = y_{1,0,0} - 1$ and $\delta(H)(y_{1,1,0} + 1) = y_{1,1,0}^2 - 1 \in [\mathcal{A}]$. On the other hand, $y_{1,1,0} + 1 \notin \text{asat}(\mathcal{A})$.

The following Theorem is one of the main results in this paper.

Theorem 4.10. *A chain $\mathcal{A}$ is the characteristic set of* sat($\mathcal{A}$) *if and only if $\mathcal{A}$ is coherent and regular.*

Proof. If $\mathcal{A}$ is coherent and regular, then by Lemma 4.8, $\mathcal{A}$ is a characteristic set of sat($\mathcal{A}$). Conversely, let $\mathcal{A} = A_1, A_2, \ldots, A_l$ be a characteristic set of the saturation ideal sat($\mathcal{A}$) and $I_i = I_{A_i}$, $S_i = S_{A_i}$. For any $1 \le i < j \le l$, let $R = \text{rprem}(\Delta_{i,j}, \mathcal{A})$, so that $R \in \text{sat}(\mathcal{A})$ and R is reduced w.r.t. $\mathcal{A}$. It follows that $R = 0$, since $\mathcal{A}$ is the characteristic set of sat($\mathcal{A}$), whence $\mathcal{A}$ is coherent. In order to prove that $\mathcal{A}$ is regular, we need to show that any $P \in \mathbf{H}_{\mathcal{A}}$ is regular w.r.t. $\mathcal{A}$. Assume this is not true. By definition, P is not regular w.r.t. the algebraic triangular set $\mathcal{A}_P$. By Lemma 4.7, $\mathcal{A}_P$ is regular. By Lemma 4.4, there is an $F \neq 0$ which is reduced w.r.t. $\mathcal{A}_P$ (and hence $\mathcal{A}$), such that $P \cdot F \in (\mathcal{A}_P) \subseteq [\mathcal{A}]$. Since $P \in \mathbf{H}_{\mathcal{A}}$, $F \in \text{sat}(\mathcal{A})$, F is reduced w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is the characteristic set of sat($\mathcal{A}$), we have $F = 0$, a contradiction. Hence, P is regular w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is regular. □

As a Corollary, we have

Corollary 4.11. *Let $\mathcal{A}$ be a coherent and regular chain. Then* $\text{sat}(\mathcal{A}) = \{P | \text{rprem}(P, \mathcal{A}) = 0\}$.

Theorem 4.10 is significant because it provides a theoretically easy way to check whether a DD-polynomial is in sat($\mathcal{A}$). Unfortunately, and unlike the algebraic and differential cases, it is difficult to ensure that $\mathcal{A}$ is regular. Indeed, even if the initials and separants of $\mathcal{A}$ are regular w.r.t. $\mathcal{A}$, it may still happen that $\text{sat}(\mathcal{A}) = [1]$:

Example 4.12. Let $\mathcal{A} = \{\delta y_1, y_1y_2 + 1\}$. The initial of $y_1y_2 + 1$, $I = y_1$, is regular w.r.t. $\mathcal{A}$, but $\delta I \cdot 1 \in [\mathcal{A}]$ which implies $1 \in \text{sat}(\mathcal{A})$.

Theorem 4.13. *If $\mathcal{A}$ is a coherent and regular chain, then*

$$\text{sat}(\mathcal{A}) = \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : H_{\mathcal{A}_P} = \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : I_{\mathcal{A}_P}.$$

Proof. It is easy to see that $\text{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbf{H}_{\mathcal{A}} \supset \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : H_{\mathcal{A}_P}$. Let $f \in \text{sat}(\mathcal{A})$. Since $\mathcal{A}$ is coherent and regular, $\mathcal{A}$ is the characteristic set of sat($\mathcal{A}$). Then $\text{rprem}(P, \mathcal{A}) = 0$, or $\text{prem}(f, \mathcal{A}_P) = 0$. We have $P \in (\mathcal{A}_P) : H_{\mathcal{A}_P}$. Hence $\text{sat}(\mathcal{A}) \subseteq \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : H_{\mathcal{A}_P}$. Since $\mathcal{A}$ is regular, $\mathcal{A}_P$ is saturated, by Lemma 4.6, $(\mathcal{A}_P) : I_{\mathcal{A}_P} = (\mathcal{A}_P) : H_{\mathcal{A}_P}$, so we proved the Theorem. □

5. Irreducible chains

We do not know of any direct method to check whether a given chain is regular, since this requires an infinite number of regularity tests for all possible transforms of the initials and separants. In this Section, we will give a constructive criterion for a chain to be regular by introducing the concept of proper irreducible chains.

5.1. Irreducible algebraic and differential chains

To define the concept of proper irreducible chains, we need several properties of algebraic irreducible triangular sets. An algebraic triangular set $\mathcal{B}$ is called *irreducible* if $\mathcal{B}$ is regular and there exist no polynomials P and Q which are reduced w.r.t. $\mathcal{B}$ and such that $PQ \in \text{asat}(\mathcal{B})$ (Ritt, 1950; Wu, 1989).

Lemma 5.1 (*Wu, 1994*). *Let $\mathcal{A}$ be an irreducible algebraic triangular set. Then* asat($\mathcal{A}$) *is a prime ideal and for any polynomial P, P is regular w.r.t. $\mathcal{A}$ if and only if $P \notin$* asat($\mathcal{A}$).

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

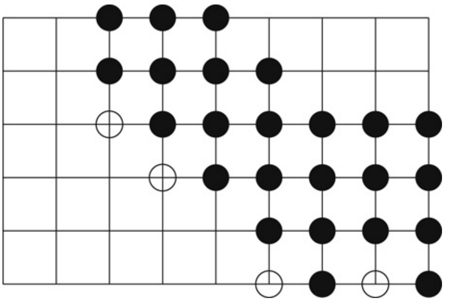

Fig. 3. The indices of triangular set $\mathcal{A}^*$.

The above Lemma was extended to the case of ordinary differential polynomials. Let $\mathcal{A}$ be a differential triangular set (Ritt and Doob, 1933; Wu, 1994). The *differential saturation ideal* of $\mathcal{A}$ is defined to be

$$\mathrm{dsat}(\mathcal{A}) = [\mathcal{A}]_\partial : H_{\mathcal{A}}^{\infty} \tag{12}$$

where $[\mathcal{A}]_\partial$ is the differential ideal generated by $\mathcal{A}$ and $H_{\mathcal{A}}$ is defined in (8) when $\mathcal{A}$ is treated as a differential triangular set.

Lemma 5.2 (*Ritt and Doob, 1933, Wu, 1989*). *Let $\mathcal{A}$ be a triangular set consisting of ordinary differential polynomials. If $\mathcal{A}$ is irreducible when considered as an algebraic triangular set, then* $\mathrm{dsat}(\mathcal{A})$ *is a prime differential ideal with $\mathcal{A}$ as its characteristic set.*

Let $\mathcal{A}$ be a chain and $\mathbb{P} \subset \mathbb{K}\{\mathbb{Y}\}$. A DD-polynomial corresponding to the bottom index in each column of the index figure (like Fig. 3) of $\mathcal{A}_{\mathbb{P}}$ is of form $\delta^d A$ for an $A \in \mathcal{A}$. The set of these DD-polynomials is called the *difference part* of $\mathcal{A}_{\mathbb{P}}$ and is denoted by $\bar{\mathcal{A}}_{\mathbb{P}}$. The following result is clear.

Lemma 5.3. *$\bar{\mathcal{A}}_{\mathbb{P}}$ is a differential triangular set when the DD-polynomials are treated as differential polynomials (see Remark 2.7).*

5.2. Proper irreducible chains

Let $\mathcal{A}$ be a chain. We assume the ranking to be an elimination ranking, and after a proper renaming of the variables, we can put it under the following form:

$$\mathcal{A} = \begin{cases} A_{1,1}(\mathbb{U}, y_1), \ldots, A_{1,k_1}(\mathbb{U}, y_1) \\ \ldots \\ A_{p,1}(\mathbb{U}, y_1, \ldots, y_p), \ldots, A_{p,k_p}(\mathbb{U}, y_1, \ldots, y_p) \end{cases} \tag{13}$$

where $\mathbb{U} = \{u_1, \ldots, u_q\}$ and $p + q = n$. For any i, we assume that $\mathrm{cls}(A_{i,j}) = \mathrm{cls}(A_{i,k})$.

Let $\mathcal{A}^* = \mathcal{A}_{\delta\mathcal{A}_{\mathcal{A}}}$ and $\bar{\mathcal{A}} = \bar{\mathcal{A}}^*$ the difference part of $\mathcal{A}^*$ (definition in Section 5.1). $\bar{\mathcal{A}}$ and $\mathcal{A}^*$ will play a central role in the rest of this paper. Let $\mathcal{A}$ be the chain in (5), then the index set of $\mathcal{A}^*$ is given in Fig. 3. The index set of $\bar{\mathcal{A}}$ is $\{(2, 3), (3, 2), (4, 2), (5, 0), (6, 0), (7, 0), (8, 0)\}$.

A chain $\mathcal{A}$ is said to be *proper irreducible* if

- $\mathcal{A}^*$ is an algebraic irreducible triangular set; and
- $\delta P \in \mathrm{dsat}(\bar{\mathcal{A}})$ implies $P \in \mathrm{dsat}(\bar{\mathcal{A}})$. Note that $\bar{\mathcal{A}}$ is a differential triangular set.

Remark 5.4. The first condition in the above definition is equivalent to the fact that $\bar{\mathcal{A}}$ is a differential irreducible triangular set. Since $\bar{\mathcal{A}} \subset \mathcal{A}^*$, and the leading variables are distinct differential variables, $\bar{\mathcal{A}}$ is a differential irreducible triangular set. On the other hand, each DD-polynomial in $\mathcal{A}^* \setminus \bar{\mathcal{A}}$ is obtained by differentiations of a DD-polynomial in $\bar{\mathcal{A}}$. Thus, a DD-polynomial in $\mathcal{A}^* \setminus \bar{\mathcal{A}}$ is linear in its leader and with the separant of a DD-polynomial in $\bar{\mathcal{A}}$ as its initial. Since $\bar{\mathcal{A}}$ is differential irreducible, these initials are regular w.r.t. $\bar{\mathcal{A}}$ and hence $\mathcal{A}^*$. As a consequence $\mathcal{A}^*$ is an irreducible algebraic triangular set.

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

Lemma 5.5. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (13). If P is a non-zero DD-polynomial in $\mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, then δP is regular w.r.t. $\mathcal{A}$, where $\mathbb{P}_{\mathcal{A}}$ is defined in (6).*

Proof. Notice that the indices of δP can be obtained by adding one to the δ-order of the indices of P, or equivalently by moving the indices of P to the right-hand side by one in the index Figure of $\mathcal{A}$. For an illustration, please consult Fig. 3. As a consequence, the DD-polynomials $A \in \mathcal{A}_{\delta P}$ such that v_A appears in δP correspond to the leftmost indices on each row in the index Figure of $\mathcal{A}_{\delta P}$. Let us denote these DD-polynomials by $\mathbb{H}$.

To test whether δP is regular w.r.t. $\mathcal{A}_{\delta P}$, we only need to consider those DD-polynomials in $\mathcal{A}_{\delta P}$ which will be needed when eliminating the leading variables of $\mathbb{H}$ with resultant computations. More precisely, these DD-polynomials $\mathcal{C}$ can be found recursively as follows:

- $\mathcal{C} = \mathbb{H}$, and
- if there exists an $A \in \mathcal{A}_{\delta P}$ such that $v_A \in \mathbb{V}_{\mathcal{C}} \setminus \mathbb{L}_{\mathcal{C}}$, then add A to $\mathcal{C}$.

From the definition of regularity, it is clear that δP is regular w.r.t. $\mathcal{A}_{\delta P}$ iff δP is regular w.r.t. $\mathcal{C}$. If $A \in \mathbb{H}$, then either $A \in \bar{\mathcal{A}}$ or $A = \partial^s A_0, A_0 \in \bar{\mathcal{A}}$. Let $A = \partial^s A_0, A_0 \in \bar{\mathcal{A}}$. Due our choice of the ordering $\leq_l$, we have $d^{(c)}_{\{\partial^s A_0\}} \leq d^{(c)}_{\bar{\mathcal{A}}}$ for any class c. Therefore, starting from A, all the DD-polynomials constructed in the above procedure are also of the form $\partial^s B_0$ for $B_0 \in \bar{\mathcal{A}}$. Since all DD-polynomials in $\mathcal{C} \setminus \bar{\mathcal{A}}$ are linear in their leaders with their initials in $H_{\bar{\mathcal{A}}}$ and $\bar{\mathcal{A}}$ is irreducible, we know that $\mathcal{C}$ is an irreducible triangular set and $\mathrm{asat}(\mathcal{C}) \subseteq \mathrm{dsat}(\bar{\mathcal{A}})$.

Suppose that δP is not regular w.r.t. $\mathcal{A}_{\delta P}$. Then δP is not regular w.r.t. $\mathcal{C}$. Since $\mathcal{C}$ is irreducible, Lemma 5.1 implies $\delta P \in \mathrm{asat}(\mathcal{C}) \subseteq \mathrm{dsat}(\bar{\mathcal{A}})$. By the definition of proper irreducible chains, $P \in \mathrm{dsat}(\bar{\mathcal{A}})$. By Lemma 5.2, $\mathrm{dprem}(P, \bar{\mathcal{A}}) = 0$. On the other hand, since $P \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, we have $\mathrm{dprem}(P, \bar{\mathcal{A}}) = P = 0$; a contradiction. □

The following example shows that, if we replace dsat by asat in the definition of proper irreducible chains, then the above Lemma becomes false.

Example 5.6. Let $A_1 = y_{1,2,0} - y_{0,0,0}$, $A_2 = y_{2,2,0} - y_{0,0,2}$, and $\mathcal{A} = A_1, A_2$. It is easy to see that $\bar{\mathcal{A}}$ is an algebraic irreducible triangular set. Let $Q = y_{2,0,0} - y_{1,0,2} \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$. We have $\delta^2 Q = A_2 - \partial^2 A_1 \in \mathrm{sat}(\mathcal{A})$, but $Q \notin \mathrm{sat}(\mathcal{A})$.

The following is a key Lemma for proper irreducible chains.

Lemma 5.7. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of form (13). If P is regular w.r.t. $\mathcal{A}$, then δP is regular w.r.t. $\mathcal{A}$.*

Proof. We prove the Lemma by induction on the order of P. If $P \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, then we are done by Lemma 5.5. Assuming that the conclusion holds for any DD-polynomial Q with $v_Q <_l v_P$, we will prove the Lemma for P.

We first prove the following result.

$$\text{If } H \in \mathbf{H}_{\mathcal{A}} \text{ and } v_H <_l v_{\delta P}, \text{ then } H \text{ is regular w.r.t. } \mathcal{A}. \tag{14}$$

Let I be the set of the initials and separants of the DD-polynomials in $\bar{\mathcal{A}}$. By Lemma 5.1, any element in I is regular w.r.t. $\mathcal{A}^*$ and hence regular w.r.t. $\mathcal{A}$. Let $I_i = \delta^i I$ for $i \geq 0$. If $H \in I_1$ and $v_H <_l v_{\delta P}$, then $H = \delta L, L \in I$, and $v_L <_l v_P$. By the induction hypothesis, H is regular w.r.t. $\mathcal{A}$. Repeating the above procedure, we can prove that if $H \in I_i$ and $v_H <_l v_{\delta P}$, then H is regular w.r.t. $\mathcal{A}$. Since $\mathbf{H}_{\mathcal{A}}$ is the set of products of elements in all I_i, each $H \in \mathbf{H}_{\mathcal{A}}$ satisfying $v_H <_l v_{\delta P}$ is regular w.r.t. $\mathcal{A}$.

Let $\mathcal{B} = \{A \in \mathcal{A}_{\delta P} \mid v_A \leq v_{\delta P}\}$. By (14), $\mathcal{B}$ is a regular algebraic triangular set.

Since P is regular w.r.t. $\mathcal{A}$, there exist a DD-polynomial Q and a non-zero DD-polynomial $G \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ such that $Q \cdot P \equiv G \bmod (\mathcal{A}_P)$. This can be expressed by the following equation:

$$Q \cdot P = G + \sum_{A \in \mathcal{A}_P, v_A \leq v_P} B_A A. \tag{15}$$

Since G is obtained from P by eliminating some variables using DD-polynomials in $\mathcal{A}_P$, we have $v_G \leq v_P$ and $s^{(c)}_{\{G\}} \leq s^{(c)}_{\mathcal{A}_P}, d^{(c)}_{\{G\}} \leq d^{(c)}_{\mathcal{A}_P}$, for each class c. Hence $\mathbb{V}_{\delta G} \subseteq \mathbb{L}_{\mathcal{A}_P} \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$. By Lemma 5.5, δG is regular w.r.t. $\mathcal{A}_{\delta G}$. From $v_G \leq v_P$ and $\mathbb{V}_{\delta G} \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$, it follows that δG is regular w.r.t. $\mathcal{B}$.

Applying δ on (15), we have

$$\delta Q \cdot \delta P = \delta G + \sum_{\delta A \in \delta \mathcal{A}_P, v_{\delta A} \leq v_{\delta P}} \delta B_A \delta A. \tag{16}$$

For any δA in the above equation, there are two cases. (1) $\delta A \in \mathcal{A}_{\delta P}$. (2) $\delta A \notin \mathcal{A}_{\delta P}$. Since $\mathcal{A}$ is coherent, Lemma 4.1 yields an $H \in \mathbf{H}_{\mathcal{A}}$, $v_H <_l v_{\delta A} \leq v_{\delta P}$ such that $H\delta A$ has a canonical representation. Hence, there exists an $H \in \mathbf{H}_{\mathcal{A}}$, $v_H <_l v_{\delta P}$ and a DD-polynomial R such that

$$H\delta Q \cdot \delta P = H\delta G + \sum_{A \in \mathcal{A}_R, v_A \leq v_{\delta P}} C_A A.$$

Since $v_H <_l v_{\delta P}$, H is regular w.r.t. $\mathcal{A}$, by (14). Since δG is regular w.r.t. $\mathcal{B}$ and $v_{\delta G} \leq v_{\delta P}$, there exist DD-polynomials $P_1 \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, Q_1, T such that $P_1 \neq 0$ and

$$Q_1 H\delta G = P_1 + \sum_{A \in \mathcal{A}_T, v_A \leq v_{\delta P}} D_A A.$$

So there exists a DD-polynomial R_1 with

$$Q_1 H\delta Q \cdot \delta P = P_1 + \sum_{A \in \mathcal{A}_{R_1}, v_A \leq v_{\delta P}} E_A A. \tag{17}$$

We decompose the sum in Eq. (17) into two parts:

$$Q_1 H\delta Q \cdot \delta P = P_1 + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_{\delta P}} E_A A + \sum_{B \notin \mathcal{A}_{\delta P}, B \in \mathcal{A}_{R_1}, v_B \leq v_{\delta P}} E_B B. \tag{18}$$

In the rightmost sum in this equation, let $B_1 = I_{B_1} v_{B_1}^{k_1} - U_1$ be largest for the ordering $\leq_l$, where $I_{B_1} \in \mathbf{H}_{\mathcal{A}}$ is the initial of B_1. Since all the B in this sum are in $\mathcal{A}_{R_1}$, B_1 is determined uniquely. Replacing $v_{B_1}^{k_1}$ by U_1/I_{B_1}, we have

$$Q_1' \delta P = I_{B_1}^{t_1} P_1 + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_{\delta P}} E_A' A + \sum_{A \notin \mathcal{A}_{\delta P}, A \in \mathcal{A}_{R_1}, v_B <_l v_{B_1}} E_B' B, \tag{19}$$

where $v_{I_{B_1}} <_l v_{B_1} \leq_l v_{\delta P}$, $t_1 \in \mathbb{N}$, and I_{B_1} is regular w.r.t. $\mathcal{A}$. Since $\mathbb{V}_{\delta P} \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$, $P_1 \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ and for $A \in \mathcal{A}_{\delta P}$, $\mathbb{V}_A \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$, for any $B \neq B_1$ in the third part of Eq. (17), $v_B <_l v_{B_1}$, they do not change under the above substitution.

Since I_{B_1} is regular w.r.t. $\mathcal{A}$, similar to the above procedure, there exist DD-polynomials $Q_2, P_2 \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, R_2, such that $P_2 \neq 0$ and

$$Q_2 \delta P = P_2 + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_{\delta P}} F_A A + \sum_{B \notin \mathcal{A}_{\delta P}, B \in \mathcal{A}_{R_2}, v_B <_l v_{B_1} \leq v_{\delta P}} F_B B. \tag{20}$$

The leader of each B in the above equation is less than v_{B_1}. Repeating the procedure for (20), by Lemma 3.4, after a finite number of steps, the rightmost sum in Eq. (20) will be eliminated. As a consequence, there is an H and a non-zero $R \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ such that

$$H\delta P = R + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_{\delta P}} Q_A A = R + \sum_{A \in \mathcal{A}_{\mathcal{B}}} Q_A A.$$

Since $\mathcal{B}$ is a regular algebraic triangular set, by Lemma 4.5, δP is regular w.r.t. $\mathcal{B} \subseteq \mathcal{A}_{\delta P}$. That is δP is regular w.r.t. $\mathcal{A}$. □

The following result gives a constructive criterion to check whether a chain is regular.

Theorem 5.8. *A coherent and proper irreducible chain is regular.*

Proof. Let $\bar{\mathcal{A}} = A_1, \ldots, A_m$, $I_j = I_{A_j}$, and $S_j = S_{A_j}$. Since $\bar{\mathcal{A}}$ is an irreducible differential triangular set, Lemma 5.1 implies that I_j and S_j are regular w.r.t. $\bar{\mathcal{A}}$ and hence regular w.r.t. $\mathcal{A}$. By Lemma 5.7, all $\delta^i I_j$, $\delta^i S_j$ are regular w.r.t. $\mathcal{A}$. As a consequence, the products of $\delta^i I_j$, $\delta^i S_j$ are regular w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is regular. □

The condition in the above Theorem can be lessened. This gives the following result which will be used below in the procedure to check whether a given chain is regular. For details, please refer to Lemma 6.3.

Corollary 5.9. *Let $\mathcal{A}$ be a chain satisfying the following conditions*

- *$\mathcal{A}^*$ is an algebraic irreducible triangular set, and*
- *$\delta P \in \mathrm{asat}(\mathcal{A}^*)$ implies $P \in \mathrm{asat}(\mathcal{A}^*)$.*

Then $\mathcal{A}$ is regular.

Proof. Let $\mathcal{A}^* = A_1, \ldots, A_m$, $I_j = I_(A_j)$, and $S_j = S_{A_j}$. Then the ∂-orders for $\delta^i I_j$, $\delta^i S_j$ are less than or equal to $d = \max_{A \in \mathcal{A}^*} \mathrm{ord}_\partial(A)$. Hence we only need to prove that Lemma 5.7 is still valid for a chain $\mathcal{A}$ satisfying the conditions in this corollary and under the extra hypothesis $\mathrm{ord}_\partial(P) \le d$. For this, it suffices to show that Lemma 5.5 is still valid under these conditions. This is indeed the case, because $\mathrm{ord}_\partial(P) \le d$ implies $\mathcal{C} \subset \mathcal{A}^*$, and the rest of the proofs can be carried out similarly. □

Theorem 5.10. *Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then $\mathrm{sat}(\mathcal{A})$ is reflexive.*

Proof. For any $\delta P \in \mathrm{sat}(\mathcal{A})$, if $P \notin \mathrm{sat}(\mathcal{A})$, then $\mathrm{rprem}(P, \mathcal{A}) \neq 0$ and $\delta \mathrm{rprem}(P, \mathcal{A}) \in \mathrm{sat}(\mathcal{A})$. So we can assume that $\delta P \in \mathrm{sat}(\mathcal{A})$ and P is reduced w.r.t. $\mathcal{A}$. By Theorems 5.8 and 4.10, $\mathcal{A}$ is both regular and the characteristic set of $\mathrm{sat}(\mathcal{A})$. Since $\delta P \in \mathrm{sat}(\mathcal{A})$ we have $\mathrm{rprem}(\delta P, \mathcal{A}) = 0$. So there exists an $H \in I_{\mathcal{A}_{\delta P}}$ such that $H\delta P \in (\mathcal{A}_{\delta P})$ and H is regular w.r.t. $\mathcal{A}_{\delta P}$. Consequently, there exists a non-zero $G \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ with

$$G\delta P = \sum_{A \in \mathcal{A}_{\delta P}} B_A A. \tag{21}$$

Let $\mathcal{C} = \mathcal{A}_{\delta P} \cap \{\delta^d \partial^s A \mid \delta^d A \in \mathcal{A}^*\}$. We have $[\mathcal{C}] \subseteq \mathrm{dsat}(\bar{\mathcal{A}})$. Since each DD-polynomial $A \in \mathcal{A}_{\delta P} \setminus \mathcal{C}$ must be the transform of a DD-polynomial B which corresponds to the last index of a row in the index diagram for $\mathcal{C}$, the leading degree of A is the same as that of B. As a consequence, δP is reduced w.r.t. $\mathcal{A}_{\delta P} \setminus \mathcal{C}$. We decompose the right-hand side of Eq. (21) into two parts:

$$G\delta P = \sum_{A \in \mathcal{C}} D_A A + \sum_{B \in \mathcal{A}_{\delta P} \setminus \mathcal{C}} D_B B.$$

Let $B = I_B v_B^k - U$, where $I_B \in \mathbf{H}_{\mathcal{A}}$ is the initial of B. Replacing v_B^k by U/I_B, we have

$$HG\delta P = \sum_{A \in \mathcal{C}} C_A A \in [\mathcal{C}] \subseteq \mathrm{dsat}(\bar{\mathcal{A}}),$$

where $H \in \mathbf{H}_{\mathcal{A}}$ and is regular w.r.t. $\mathcal{A}$. Since $G \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ and δP is reduced w.r.t. $\mathcal{A}_{\delta P} \setminus \mathcal{C}$, $G\delta P$ does not change under the above substitution. Let $B \in \mathcal{A}_{\delta P} \setminus \mathcal{C}$ with class c. For any $A \in \mathcal{C}$, by the construction of $\mathcal{A}^*$, $d_{\{A\}}^{(c)} <_l d_{\{B\}}^{(c)}$ and hence A will not change under the above substitution. Since $\mathcal{A}^*$ is irreducible, $G \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, H is regular w.r.t. $\mathcal{A}$, and $HG\delta P \in \mathrm{dsat}(\bar{\mathcal{A}})$, by Lemma 5.2, we have $HG \notin \mathrm{dsat}(\bar{\mathcal{A}})$ and $\delta P \in \mathrm{dsat}(\bar{\mathcal{A}})$. Since $\mathcal{A}$ is proper irreducible, we have $P \in \mathrm{dsat}(\bar{\mathcal{A}}) \subseteq \mathrm{sat}(\mathcal{A})$; a contradiction. □

5.3. Consistency of proper irreducible chains

In order to solve the perfect ideal membership problem, we need to show that a coherent and proper irreducible chain $\mathcal{A}$ is *consistent*, or equivalently, that $\mathrm{sat}(\mathcal{A})$ admits a zero in a suitable DD-extension field. This is achieved by extending Cohn's theory of kernels to the DD-case.

Let $\mathbb{K}$ be a DD-field. We will denote by $\mathbb{K}(f_1, \ldots, f_r)_\partial$ the differential field extension of $\mathbb{K}$ with elements $f_1, \ldots, f_r$ in some differential overfield of $\mathbb{K}$. We will denote by $\mathbb{K}\{g_1, \ldots, g_r\}$ the DD-field extension of $\mathbb{K}$ with elements $g_1, \ldots, g_r$ in some DD-overfield of $\mathbb{K}$.

Let $a_i = (a_{i,1}, \ldots, a_{i,n})$, $i = 0, \ldots, r$ be n-tuples, where $a_{i,j}$ are elements from a differential extension field of $\mathbb{K}$. Consider the differential field

$$R = \mathbb{K}(a_0, a_1, \ldots, a_r)_\partial$$

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

together with a differential ring isomorphism

$$T : \mathbb{K}(a_0, \ldots, a_{r-1})_\partial \to \mathbb{K}(a_1, \ldots, a_r)_\partial$$

which extends δ and such that $Ta_i = a_{i+1}$, $i = 0, \ldots, r-1$. The differential ring R endowed with such an operator T is called a *DD-kernel* of length r.

Definition 5.11. Let $U = \{u_1, \ldots, u_q\}$ be such that $u_j = a_{r,i_j}$ for $i_1 < \cdots < i_q$. If U is a differential transcendence basis for a_r over $\mathbb{K}(a_0, a_1, \ldots, a_{r-1})$, then U is called a *DD-parametric set*. We denote by $\dim(R)$ the differential dimension of $\mathbb{K}(a_0, a_1, \ldots, a_r)$ over $\mathbb{K}(a_0, a_1, \ldots, a_{r-1})$. Then a DD-parametric set contains precisely $\dim(R)$ elements. Furthermore, we can define $\partial\mathrm{ord}_U R$ to be the differential order of $\mathbb{K}(a_0, \ldots, a_r)_\partial$ over $\mathbb{K}(a_0, \ldots, a_{r-1}, U)_\partial$ (Ritt, 1950).

We need the following results, which can be found in Ritt (1950), on pages 49 and 51.

Lemma 5.12 (*Ritt, 1950*). *Let Σ and Σ' be non-trivial differential prime ideals of respective dimensions q and q', such that Σ' is a proper divisor of Σ. Then $q \leq q'$. If $q = q'$, then every parametric set U for Σ' is a parametric set for Σ and the order of Σ' relative to U is less than the order of Σ relative to U.*

Lemma 5.13 (*Ritt, 1950*). *Let Σ be a non-trivial differential prime ideal of dimension q. Let Σ' be the differential ideal generated by Σ in an extension $\mathbb{K}'$ of $\mathbb{K}$. Then Σ' is perfect and each of its essential prime divisors Σ_j, $j = 1, \ldots, s$, is of dimension q. If $q > 0$, then every parametric set U for Σ is a parametric set for every Σ_j and the orders of the Σ_j relative to U are all equal to the order of Σ relative to U. If $q = 0$, then every Σ_j has the same order as Σ.*

The following lemma is a key ingredient for proving the consistency of a proper irreducible chain. Its proof is analogous to Cohn's proof (Cohn, 1965, page 150) in the pure difference case.

Lemma 5.14. *There is a* prolongation *R' of R consisting of a differential overfield $\mathbb{K}(a, \ldots, a_r, a_{r+1})_\partial$ of $\mathbb{K}(a, \ldots, a_r)_\partial$ and an extension T' of T to a differential isomorphism of $\mathbb{K}(a, \ldots, a_r)_\partial$ onto $\mathbb{K}(a_1, \ldots, a_{r+1})_\partial$ with $T'a_r = a_{r+1}$.*

Proof. Let Π be the differential prime ideal with generic zero a_r in the differential polynomial ring $\mathbb{K}(a, \ldots, a_{r-1})_\partial\{X\}$, where X denotes $(x_1, \ldots, x_n)$. Let Π' be obtained from Π by replacing the coefficients of the polynomials of Π by their images under T. Then Π' is a prime differential ideal in $\mathbb{K}(a_1, \ldots, a_r)_\partial\{X\}$ and generates an ideal Σ in $\mathbb{K}(a, \ldots, a_r)_\partial\{X\}$. Let Φ be an essential prime divisor of Σ. By Lemma 5.13, the differential dimension of Φ is equal to that of Π'. If U is the parametric set of Π', then it must be the parametric set of Φ, and the order of Φ w.r.t. U is equal to the order of Π' w.r.t. U. We choose a_{r+1} to be a generic zero of Φ. Let $\Pi'' = \{P \in \mathbb{K}(a_1, \ldots, a_r)_\partial\{X\} \mid P(a_{r+1}) = 0\}$, and denote by U the parametric set of Π''. Then $\dim(\Pi'') = |U|$ and the differential order of Π'' w.r.t. U is equal to the differential order of Φ w.r.t. U. So Π', Π'' admit the same parametric set and the same order w.r.t. this parametric set. Since a_{r+1} is also a zero of Π', we have $\Pi' \subset \Pi''$. By Lemma 5.12, we know that $\Pi' = \Pi''$, and a_{r+1} is also a generic zero of Π'. Consequently, there is an isomorphism T' of $\mathbb{K}(a, \ldots, a_r)_\partial$ onto $\mathbb{K}(a_1, \ldots, a_{r+1})_\partial$ which is an extension of T. This proves the lemma. □

Theorem 5.15. *Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then* $\mathrm{Zero}(\mathrm{sat}(\mathcal{A})) \neq \emptyset$.

Proof. Let $\mathcal{A}$ be a proper irreducible chain of the form (13). Denote the difference part of $\mathcal{A}^*$ by

$$\bar{\mathcal{A}} = \{B_{1,1}, \ldots, B_{1,c_1}, \ldots, B_{p,1}, \ldots, B_{p,c_p}\},$$

where $\mathrm{lvar}(B_{i,j}) = y_i$. Let $o_i = \mathrm{ord}_\delta(B_{i,c_i}, y_i)$, $i = 1, \ldots, p$, $e = \max_{A \in \mathcal{A}^*, 1 \leq i \leq q} \{\mathrm{ord}_\delta(A, u_i)\}$,

$$U_0 = \{\delta^j u_i \mid 1 \leq i \leq q, 0 \leq j \leq e\}, \quad U_1 = \delta U_0 = \{\delta^j u_i \mid 1 \leq i \leq q, 1 \leq j \leq e+1\},$$
$$Y_0 = \{\delta^j y_i \mid 1 \leq i \leq p,\ 0 \leq j \leq o_i - 1\}, Y_1 = \delta Y_0 = \{\delta^j y_i \mid 1 \leq i \leq p,\ 1 \leq j \leq o_i\}.$$

Then $V_0 = U_0 \cup Y_0$ and $V_1 = \delta V_0 = U_1 \cup Y_1$ have the same number of elements.

Since $\mathcal{A}$ is proper irreducible, $\bar{\mathcal{A}}$ is an irreducible differential triangular set when $\delta^i u_j$ and $\delta^i y_j$ are treated as independent differential variables. Hence, $\mathrm{dsat}(\bar{\mathcal{A}})$ is a differential prime ideal in $\mathbb{K}\{\hat{V}\}$, where $\hat{V} = U_0 \cup Y_0 \cup \{\delta^{o_1} y_1, \ldots, \delta^{o_p} y_p\}$. Let $\eta = (\alpha_{i,j}, \beta_{i,j})$ be a generic zero of this differential prime ideal. Then every polynomial in $\bar{\mathcal{A}}$ vanishes at $\delta^j u_i = \alpha_{i,j}$, $\delta^j y_i = \beta_{i,j}$, but not their initials and separants.

We will construct a DD-kernel of length one. Let a_0 and a_1 be obtained from V_0 and V_1 by replacing $\delta^j u_i$ and $\delta^j y_i$ with the corresponding $\alpha_{i,j}$ and $\beta_{i,j}$. We take $\mathbb{K}(a_0, a_1)_\partial$ for our kernel. The difference operator δ introduces a map from $\mathbb{K}(a_0)_\partial$ to $\mathbb{K}(a_1)_\partial$ by $\delta(\alpha_{i,j}) = \alpha_{i,j+1}$ and $\delta(\beta_{i,j}) = \beta_{i,j+1}$. We will prove that δ gives rise to an isomorphism between $\mathbb{K}(a_0)_\partial$ and $\mathbb{K}(a_1)_\partial$. Let

$$\mathcal{B}_0 = \bar{\mathcal{A}} - \{B_{1,c_1}, \ldots, B_{p,c_p}\},\ \mathcal{B}_1 = \{\delta A \mid A \in \mathcal{B}_0\}.$$

From the definition of $\bar{\mathcal{A}}$, $\mathcal{B}_0 \neq \emptyset$ and the δ-order of y_k in $B_{i,j} \in \mathcal{B}_0$ does not exceed $o_k - 1$. As a consequence, a_0 is a generic zero of the differential prime ideal $I_0 = \mathrm{dsat}(\mathcal{B}_0)$. Let $I = \mathrm{dsat}(\bar{\mathcal{A}})$.

Since $\delta\mathcal{B}_0 = \mathcal{B}_1$ and $\delta a_0 = a_1$, by the nature of the difference operator, $\mathcal{B}_1$ is an irreducible differential triangular set in $\mathbb{K}\{V_1\}$, and a_1 is a zero of the prime ideal I_1 with $\mathcal{B}_1$ as a characteristic set. We will prove that $I_1 = \mathrm{dsat}(\mathcal{B}_1) = I \cap \mathbb{K}\{V_1\}$, which means that a_1 is generic.

In order to show that $I_1 = I \cap \mathbb{K}\{V_1\}$, let $t_i = \mathrm{ord}_\delta(B_{i,1})$, $U^* = U_0 \cup U_1$, $Y^* = Y_0 \cup Y_1$. Since $\mathrm{dsat}(\mathcal{A})$ is reflexive, we can choose U_1 and $\{y_{i,j} | 1 \le i \le p,\ 1 \le j \le t_i\}$ as the parametric set of the differential ideal $I \cap \mathbb{K}\{U_1, Y_1\}$. Moreover, the differential order of $I \cap \mathbb{K}\{U_1, Y_1\}$ w.r.t. this parametric set equals the differential order of $I \cap \mathbb{K}\{U_0, Y_0\}$ w.r.t. its parametric set U_0 and $\{y_{i,j} | 1 \le i \le p,\ 0 \le j \le t_i - 1\}$. Hence, the number of parameters and the order w.r.t. these parameters are the same for I_0 and $I \cap \mathbb{K}\{U_1, V_1\}$. Now the number of parameters and the order w.r.t. these parameters also coincide for I_0 and I_1. Since the prime ideals I_1 and $I \cap \mathbb{K}\{U_1, V_1\}$ satisfy $I_1 \subset I \cap \mathbb{K}\{V_1\}$, Lemma 5.12 implies that they have the same dimension and order, whence $I_1 = I \cap \mathbb{K}\{V_1\}$. Since $\delta : I_0 \to I_1$ is an isomorphism between two prime ideals, $\delta : \mathbb{K}(a_0)_\partial \to \mathbb{K}(a_1)_\partial$ is a differential field isomorphism.

At this point, we have proved that $\mathbb{K}(a_0, a_1)_\partial$ is a DD-kernel over $\mathbb{K}$. By successive applications of Lemma 5.14, we obtain a sequence of kernels $R_h = \mathbb{K}(a, \ldots, a_{r+h})_\partial$, $h = 0, 1, \ldots$, and isomorphisms T_h of $\mathbb{K}(a, \ldots, a_{r+h-1})_\partial$ onto $\mathbb{K}(a_1, \ldots, a_{r+h})_\partial$ such that R_{h+1} is a prolongation of R_h, and $R_0 = R$. The union of all R_h, $h = 0, 1, \ldots$ defines a DD-field $\mathbb{K}\langle a \rangle = \mathbb{K}(a, a_1, \ldots)_\partial$, where the difference operator is defined by $\delta a_i = a_{i+1}$. We denote ψ to be the value induced by η in $\mathbb{K}\langle a \rangle$. We will show that ψ is a zero of $\mathrm{sat}(\mathcal{A})$.

Let $A \in \mathcal{A}$. From the construction of the kernel, A vanishes at ψ, contrary to its initial and separant. Furthermore, $\delta P(\psi) = 0$ implies $P(\psi) = 0$ for any DD-polynomial P: using the isomorphism $\delta : \mathbb{K}(a, a_1, \ldots, a_r) \to \mathbb{K}(a_1, \ldots, a_{r+1})$, we have $(\delta P)(a_1, \ldots, a_{r+1}) = 0 \Rightarrow P(a, a_1, \ldots, a_r) = 0$. Consequently, $\delta^d \partial^s A$ vanishes at ψ for all d and s, but not its initial. We conclude that $\psi \in \mathrm{Zero}(\mathrm{sat}(\mathcal{A}))$. □

5.4. Strongly irreducible chains

We first show that a proper irreducible chain does not necessarily define a prime ideal.

Example 5.16. Consider $\mathcal{A} = \{A_1 = y_{1,0,0}^2 + t,\ A_2 = y_{2,0,0}^2 + t + k\}$ from Cohn (1948) in $\mathbb{K}\{y_1, y_2\}$ where $\mathbb{K}$ is $Q(t)$ with the difference operator $\delta t = t + 1$ and k is a positive integer. $\mathcal{A}^* = \{A_1, \delta A_1, A_2, \delta A_2\}$. If $k > 1$, then $\mathcal{A}$ is proper irreducible. But $\mathrm{sat}(\mathcal{A})$ is not prime, because $A_2 - \delta^k(A_1) = (y_{2,0,0} - y_{1,k,0})(y_{2,0,0} + y_{1,k,0})$.

A proper irreducible chain $\mathcal{A}$ is said to be *strongly irreducible* if $\mathcal{A}_P$ is an algebraic irreducible triangular set for any DD-polynomial P. In this Section, we will prove that any reflexive prime ideal can be described with strongly irreducible chains. The following Theorem gives a description of prime ideals in terms of strongly irreducible chains.

Theorem 5.17. *Let $\mathcal{A}$ be a coherent and strongly irreducible chain. Then $\mathrm{sat}(\mathcal{A})$ is a reflexive prime ideal. On the other side, if I is a reflexive prime ideal and $\mathcal{A}$ the characteristic set for I, then $I = \mathrm{sat}(\mathcal{A})$ and $\mathcal{A}$ is a coherent and strongly irreducible chain.*

Proof. "$\Longrightarrow$" Since $\mathcal{A}$ is coherent and proper irreducible, Theorem 4.10 implies that $\mathcal{A}$ is regular and $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. For two DD-polynomials P and Q such that $PQ \in \mathrm{sat}(\mathcal{A})$, Theorem 4.13 yields a DD-polynomial R with $PQ \in \mathrm{asat}(\mathcal{A}_R)$. Since $\mathcal{A}_R$ is an irreducible triangular set, Lemma 5.1 implies $P \in \text{asat}(\mathcal{A}_R)$ or $Q \in \text{asat}(\mathcal{A}_R)$. Therefore, sat$(A)$ is a prime ideal. By Theorem 5.10, sat$(\mathcal{A})$ is reflexive. This shows that sat$(\mathcal{A})$ is a reflexive prime ideal.

"$\Longleftarrow$" Since $\mathcal{A}$ is the characteristic set of I, it is coherent, regular, and $I \subseteq \text{sat}(\mathcal{A})$, by Theorem 4.10. On the other hand, for $P \in \text{sat}(\mathcal{A})$, there exists an $H \in \mathbf{H}_{\mathcal{A}}$ with $HP \in [\mathcal{A}]$. Since I is a reflexive prime ideal, the initials and separants of $\mathcal{A}$, as well as their transforms, are not in I. Hence $P \in I$ and $I = \text{sat}(\mathcal{A})$. For any DD-polynomial P, $\mathcal{A}_P$ is an irreducible triangular set. Otherwise there exist DD-polynomials G and H, which are reduced w.r.t. $\mathcal{A}_P$, and such that $GH \in \text{asat}(\mathcal{A}_P) \subseteq \text{sat}(\mathcal{A})$. Hence G and H are reduced w.r.t. $\mathcal{A}$. As a consequence, $G, H \notin I = \text{sat}(\mathcal{A})$ but $GH \in I$, which contradicts to the fact that I is a prime ideal. If $\delta P \in \text{dsat}(\bar{\mathcal{A}})$, we have $\delta P \in \text{sat}(\mathcal{A}) = I$, whence $P \in \text{sat}(\mathcal{A})$. Since $\mathcal{A}$ is coherent and regular, we have $P \in \text{asat}(\mathcal{A}_P)$. Since $\mathcal{A}$ is irreducible, dsat$(\bar{\mathcal{A}})$ is a prime differential ideal. Without loss of generality, we may assume that $d^{(c)}_{\{\delta P\}} \le d^{(c)}_{\bar{\mathcal{A}}}$ for all c, where $d^{(c)}_{\mathbb{P}}$ is the largest d such that $y_{c,d,s}$ occurs in $\mathbb{P}$. As a consequence $\mathcal{A}_P \subseteq \text{dsat}(\bar{\mathcal{A}})$ and $P \in \text{asat}(\mathcal{A}_P) \subseteq \text{dsat}(\bar{\mathcal{A}})$. $\square$

6. Zero decomposition algorithms

In this Section, we will present an algorithm which can be used to decompose the zero set of a finite DD-polynomial system into the union of the zero sets of proper irreducible chains. Such algorithms are called *zero decomposition algorithms*. We will also show how to solve the perfect ideal membership problem.

6.1. Test of proper irreducibility

In this section, we will give an algorithm to check whether a chain is proper irreducible. The following algorithm checks if a chain is regular.

Algorithm 3 Regular($\mathcal{A}$)

Input: A coherent chain $\mathcal{A}$ of the form (13) such that $\mathcal{A}^*$ is irreducible.
Output: (true,$\emptyset$) if $\mathcal{A}$ is regular.
(false,$\bar{\mathbb{P}}$) otherwise. $\bar{\mathbb{P}}$ consists of DD-polynomials reduced w.r.t. $\mathcal{A}$ such that

$$\text{Zero}(\mathcal{A}) = \text{Zero}(\mathcal{A} \cup \bar{\mathbb{P}}) \cup \bigcup_i \text{Zero}(\mathcal{A} \cup \{I_i\}) \cup \bigcup_j \text{Zero}(\mathcal{A} \cup \{S_j\}) \tag{22}$$

where I_i and S_i are the initials and separants of the DD-polynomials in $\mathcal{A}$.

$G :=$**GBasis**(asat$(\mathcal{A}^*)$) /*/
$G_1 := \mathbb{E}^{-1}(G \cap \mathbb{K}[U_1, Y_1])$ where
U_1, Y_1 are the variables in G minus those $u_{j,0,s}, y_{k,0,t}$ with ord$_\delta$ zero.
If $G_1 \subset (G)$ then return (true,$\emptyset$).
Else return (false,{aprem$(g, \mathcal{A}^*) \mid g \in G_1 \setminus (G)$}).

/*/ G := **GBasis**(asat$(\mathcal{A}^*)$) computes the Groebner basis w.r.t. the eliminating ordering $y_{c,0,i} > y_{c,0,i-1} > \cdots y_{c-1,0,t} > \cdots > y_{1,0,s} > u_{d,0,l} > \cdots > u_{1,0,k} > \cdots$. In Gao and Chou (1993), it is proved that for any chain $\mathcal{A} \subset \mathbb{K}[x_1, \ldots, x_n]$, we have asat$(\mathcal{A}) = (\mathcal{A}, zI_{\mathcal{A}} - 1) \cap \mathbb{K}[x_1, \ldots, x_n]$, where z is a new variable. Based on this result, we can compute the Groebner basis of asat$(\mathcal{A}^*)$.

Proposition 6.1. *Algorithm* **Regular** *is correct.*

Proof. If the algorithm returns true, we will show that $\mathcal{A}$ is regular. Since $\mathcal{A}^*$ is irreducible, by Corollary 5.9, we need only to show that $\delta P \in \text{asat}(\mathcal{A}^*)$ implies $P \in \text{asat}(\mathcal{A}^*)$. If $\delta P \in \text{asat}(\mathcal{A}^*)$, from the variable order used by us, we have $\delta P \in (G \cap \mathbb{K}[U_1, Y_1])$ and whence $P \in (G_1) \subset (G)$. Thus, $\mathcal{A}$ is regular. If the algorithm returns false, for $g \in G_1 \setminus (G)$, we have aprem$(g, \mathcal{A}^*) \neq 0$ and it is reduced w.r.t. $\mathcal{A}$. It is clear that the right-hand side of (22) is included in Zero$(\mathcal{A})$. For $\eta \in \text{Zero}(\mathcal{A})$, if $I_i(\eta)S_j(\eta) = 0$ we have $\eta \in \text{Zero}(\mathcal{A} \cup \{I_i\}) \cup \text{Zero}(\mathcal{A} \cup \{S_j\})$. Otherwise, from the definition of asat, for any $P \in \bar{\mathbb{P}}$, $\delta P(\eta) = 0$ and hence $P(\eta) = 0$. We thus proved (22). $\square$

Algorithm **DCS** converts an irreducible differential triangular set under one variable order to an irreducible differential triangular set under another variable order.

Algorithm 4 — DCS($\mathcal{A}$)

Input: $\mathcal{A}$ is an irreducible differential triangular set in $\mathbb{K}\{\mathbb{Y}\}$ with any variable order.
Output: A differential characteristic set $\mathcal{B}$ of $\mathrm{dsat}(\mathcal{A})$ under the variable ordering: $y_{c_1,0,i} > y_{c_2,k,j}$ for any $k \neq 0$.

Let H be the product of the initials and separants of $\mathcal{A}$.
Compute a zero decomposition

$$\mathrm{Zero}(\mathcal{A}/H) = \bigcup_{i=1}^{m} \mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_i)/H)$$

with the Variety Decomposition Theorem on page 308 of Wu (1989), where $\mathcal{A}_i$ are irreducible differential chains.
For k from 1 to m do
if $\mathrm{dprem}(P, \mathcal{A}) = 0$ for all $P \in \mathcal{A}_k$ return A_k.

Proposition 6.2. *The algorithm* **DCS** *is correct.*

Proof. By the definition of dsat, we have

$$\mathrm{Zero}(\mathrm{dsat}(\mathcal{A})/H) = \mathrm{Zero}(\mathcal{A}/H) = \bigcup_{i} \mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_i)/H). \tag{23}$$

Since $\mathcal{A}$ is irreducible, by Lemma 5.2, $\mathrm{dsat}(\mathcal{A})$ is a differential prime ideal. Then $\mathrm{dsat}(\mathcal{A}) \subseteq \mathrm{dsat}(\mathcal{A}_i)$ for any i. Due to (23), a generic zero of $\mathrm{dsat}(\mathcal{A})$ must be in some $\mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_k))$. For this k, we have $\mathrm{dprem}(P, \mathcal{A}) = 0$ for all $P \in \mathcal{A}_k$. So such a k exists. We will show that $\mathrm{dsat}(\mathcal{A}) = \mathrm{dsat}(\mathcal{A}_k)$. For any $P \in \mathrm{dsat}(\mathcal{A}_k)$, there exists an $H_1 \in H_{\mathcal{A}_k}$ such that $H_1 P \in [\mathcal{A}_k]$. We have $H_1 \notin \mathrm{dsat}(\mathcal{A})$, since otherwise $H_1 \in \mathrm{dsat}(\mathcal{A}) \subseteq \mathrm{dsat}(A_k)$. Since $\mathrm{dprem}(P, \mathcal{A}) = 0$ for all $P \in \mathcal{A}_k$, there exists an $H_2 \in H_{\mathcal{A}}$ with $H_1 H_2 P \in [\mathcal{A}]$. Since $H_1 H_2 \notin \mathrm{dsat}(\mathcal{A})$, we have $P \in \mathrm{dsat}(\mathcal{A})$. So $\mathrm{dsat}(\mathcal{A}) = \mathrm{dsat}(\mathcal{A}_k)$. □

Now, we can give the algorithm to check whether a chain is proper irreducible.

Algorithm 5 — ProIrr($\mathcal{A}$)

Input: A coherent chain $\mathcal{A}$ of the form (13) such that $\mathcal{A}^*$ is irreducible.
Output: (true,∅), if $\mathcal{A}$ is proper irreducible.
(false,$\bar{\mathbb{P}}$), otherwise. $\bar{\mathbb{P}}$ consists of DD-polynomials reduced w.r.t. $\mathcal{A}$ such that

$$\mathrm{Zero}(\mathcal{A}) = \mathrm{Zero}(\mathcal{A} \cup \bar{\mathbb{P}}) \cup \bigcup_i \mathrm{Zero}(\mathcal{A} \cup \{I_i\}) \cup \bigcup_i \mathrm{Zero}(\mathcal{A} \cup \{S_i\}) \tag{24}$$

where I_i and S_i are the initials and separants of the polynomials in $\mathcal{A}$.

Let $(test, \bar{\mathbb{P}}) = \textbf{Regular}(\mathcal{A}^*)$.
If $test = false$, then return(false,$\bar{\mathbb{P}}$)
Else, let $G := \textbf{DCS}(\bar{\mathcal{A}})$
$G_1 := G \cap \mathbb{K}[U_1, Y_1]$ where
U_1, Y_1 are the variables in G, except for those $u_{i,0,j}, y_{i,0,k}$ with zero ord_δ.
$G_1 := \delta^{-r} G_1$, where r is the largest s, such that $\delta^{-s} G_1$ is a DD-polynomial.
If $\mathrm{dprem}(g, \bar{\mathcal{A}}) = 0$ for all $g \in G_1$, then return (true,∅).
Else return (false,$\{\mathrm{dprem}(g, \bar{\mathcal{A}}) \neq 0 \mid g \in G_1\}$).

Proposition 6.3. *The algorithm* **ProIrr** *is valid.*

Proof. If **ProIrr($\mathcal{A}$)** returns (true,$\emptyset$), then we will show that $P \in \text{dsat}(\bar{\mathcal{A}})$ for any $\delta P \in \text{dsat}(\bar{\mathcal{A}})$. Since $\text{dsat}(\bar{\mathcal{A}}) = \text{dsat}(\mathcal{A}_k)$, where $\mathcal{A}_k$ is obtained from **DCS**($\bar{\mathcal{A}}$), we have $\delta P \in \text{dsat}(\mathcal{A}_k)$. Since $\mathcal{A}_k$ is an irreducible differential chain, $\text{dprem}(\delta P, \mathcal{A}_k) = 0$. We denote $G_1 = \mathcal{A}_k \cap \mathbb{K}[U_1, Y_1]$, $G_0 = \delta^{-1}G_1$, where $\mathbb{K}[U_1, Y_1]$ is described in algorithm **ProIrr**. Then $\text{dprem}(\delta P, \mathcal{A}_k) = \text{dprem}(\delta P, G_1) = 0$. So there exists an $H \in H_{G_1}$ with

$$H\delta P = \sum_{i\in\mathbb{N}, B\in G_1} Q_{i,B}\partial^i B,$$

where $H, B, Q_{i,B} \in \mathbb{K}[U_1, Y_1]$. Applying δ^{-1} to this equation, we obtain $(\delta^{-1}H)P \in [G_0]_\partial$. Since $d^{(c)}_{\{G\}} \leq d^{(c)}_{\{\bar{\mathcal{A}}\}}$ for all $G \in G_0$ and c, we have $\mathcal{A}_G \subseteq [\bar{\mathcal{A}}]_\partial$ and $\text{rprem}(G, \mathcal{A}) = \text{aprem}(G, \mathcal{A}_G) = \text{dprem}(G, \bar{\mathcal{A}}) = 0$. Consequently, $(\delta^{-1}H)P \in \text{dsat}(\bar{\mathcal{A}})$. Since $\mathcal{A}_k$ is an irreducible differential chain and H is regular w.r.t. $\mathcal{A}_k$, it is regular w.r.t. $\mathcal{A}_H \subset [\bar{\mathcal{A}}]_\partial$. It follows that $\delta^{-1}H$ must be regular w.r.t. $\mathcal{A}_{\delta^{-1}H} \subset [\bar{\mathcal{A}}]_\partial$; otherwise $\delta^{-1}H \in \text{asat}(\mathcal{A}_{\delta^{-1}H})$. Since **Regular** returns true, $\mathcal{A}$ is regular. By Theorem 4.10, we infer that $\mathcal{A}$ is the characteristic set of $\text{sat}(\mathcal{A})$, so that $H \in \text{sat}(\mathcal{A})$. Since $\mathcal{A}$ is regular, $\text{rprem}(H, \mathcal{A}) = \text{aprem}(H, \mathcal{A}_H) = \text{dprem}(H, \bar{\mathcal{A}}) = 0$; a contradiction. We conclude that $P \in \text{dsat}(\bar{\mathcal{A}})$. Eq. (24) can be proved similarly to that of (22). $\square$

6.2. The zero decomposition algorithm

We first give two lemmas. A chain $\mathcal{A}$ is called a *Wu characteristic set* of a set $\mathbb{P}$ of DD-polynomials if $\mathcal{A} \subseteq [\mathbb{P}]$ and $\text{rprem}(P, \mathcal{A}) = 0$ for all $P \in \mathbb{P}$. As a direct consequence of Lemma 3.8, we have

Lemma 6.4. *Let $\mathbb{P}$ be a finite set of DD-polynomials, $\mathcal{A} = A_1, \ldots, A_m$ a Wu characteristic set of $\mathbb{P}$, $I_i = I_{A_i}$, $S_i = S_{A_i}$, and $H = \prod_{i=1}^m I_i S_i$. Then*

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\mathcal{A}/H) \cup \bigcup_{i=1}^m \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) \cup \bigcup_{i=1}^m \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$$

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\text{sat}(\mathcal{A})) \cup \bigcup_{i=1}^m \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) \cup \bigcup_{i=1}^m \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\}).$$

Lemma 6.5. *(Lemma 3 on page 181 in Wu (1994)) If $\mathcal{B}$ is a reducible algebraic triangular set, then we can find a set of polynomials $\mathbb{P} = \{P_1, P_2, \ldots, P_h\}$ such that each P_i is reduced w.r.t. $\mathcal{B}$ and*

$$\text{Zero}(\mathcal{B}) = \bigcup_{i=1}^h \text{Zero}(\mathcal{B} \cup \{P_i\}) \cup \bigcup_i \text{Zero}(\mathcal{B} \cup \{I_i\}).$$

Here I_i stand for the initials of the polynomials in $\mathcal{B}$.

We are now in a position to state the main algorithm **ZDT** of this paper which achieves the zero decomposition of a perfect DD-ideal.

Theorem 6.6. *Let $\mathbb{P}$ be a finite set of DD-polynomials in $\mathbb{K}\{y_1, \ldots, y_n\}$. Then the algorithm* **ZDT** *computes a sequence of coherent and proper irreducible chains $\mathcal{A}_1, \ldots, \mathcal{A}_k$, such that*

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^k \text{Zero}(\mathcal{A}_i/H_i)$$

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^k \text{Zero}(\text{sat}(\mathcal{A}_i)),$$

where H_i is a product of the initials and separants of $\mathcal{A}_i$.

Algorithm 6 — ZDT($\mathbb{P}$)

Input: A finite set $\mathbb{P}$ of DD-polynomials.
Output: $W = \{\mathcal{A}_1, \ldots, \mathcal{A}_k\}$ such that $\mathcal{A}_i$ is a coherent and proper irreducible chain and $\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_i))$.

Let $\mathcal{B} := \mathrm{CS}(\mathbb{P})$, $\mathcal{B} := B_1, \ldots, B_p$. /*/
If $\mathcal{B} = 1$ then return {}.
Else
  Let $\mathbb{R} := \{\mathrm{rprem}(f, \mathcal{B}) \neq 0 \mid f \in (\mathbb{P} \setminus \mathcal{B}) \cup \Delta(\mathcal{B})\}$.
  If $\mathbb{R} = \emptyset$ then
    If $\mathcal{B}^*$ is not algebraic irreducible then
      return W:= $\cup_{i=1}^{k}$**ZDT**$(\mathbb{P} \cup \mathcal{B} \cup \{P_i\})\cup$ **ZDT** $(\mathbb{P} \cup \mathcal{B} \cup \{I_i\})$,
      where P_i, I_j correspond to the polynomials in Lemma 6.5 for $\mathcal{B}^*$
    Else, let $(test, \bar{\mathbb{P}})$:=**ProIrr**$(\mathcal{B})$.
      If $test$ then W = $\{\mathcal{B}\}\cup$**ZDT**$(\mathbb{P} \cup \mathcal{B} \cup \{I_i\})\cup$**ZDT**$(\mathbb{P} \cup \mathcal{B} \cup \{S_i\})$.
      Else W:= **ZDT**$(\mathbb{P}, \mathcal{B}, \bar{\mathbb{P}})\cup$ **ZDT** $(\mathbb{P} \cup \mathcal{B} \cup \{I_i\})\cup$ **ZDT** $(\mathbb{P} \cup \mathcal{B} \cup \{S_i\})$,
        where I_i, S_i are the initials and separants of the DD-polynomials in $\mathcal{B}$
  Else W :=**ZDT**$(\mathbb{P} \cup \mathbb{R})$.

/*/ CS($\mathbb{P}$) gives the characteristic set of $\mathbb{P}$. Since $\mathbb{P}$ is finite, it is easy to find CS($\mathbb{P}$).

Proof. The algorithm **ZDT** is similar to the algebraic and differential zero decomposition algorithms in Ritt and Doob (1933) and Wu (1994), except for using algorithm **ProIrr**. If $\mathbb{R} = \emptyset$, then $\mathcal{B}$ is a coherent Wu characteristic set of $\mathbb{P}$. If $\mathcal{B}^*$ is not algebraic irreducible, by Lemma 6.5, we have

$$\mathrm{Zero}(\mathcal{B}^*) = \mathrm{Zero}(\mathcal{B}) = \bigcup_{i=1}^{h} \mathrm{Zero}(\mathcal{B} \cup \{P_i\}) \ \cup \ \bigcup_{j} \mathrm{Zero}(\mathcal{B} \cup \{I_j\}).$$

Since $\mathcal{B}$ is a Wu characteristic set of $\mathbb{P}$, we have $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{P} \cup \mathcal{B}) = \bigcup_{i=1}^{h} \mathrm{Zero}(\mathbb{P} \cup \mathcal{B} \cup \{P_i\}) \cup \cup_j \mathrm{Zero}(\mathbb{P} \cup \mathcal{B} \cup \{I_j\})$.

Since $\mathcal{B}$ is coherent and $\mathcal{B}^*$ is irreducible, we can call Algorithm **ProIrr**($\mathcal{B}$). If $test = true$, the result comes from Lemma 6.4. If $test = false$, from Algorithm **ProIrr**, we have

$$\mathrm{Zero}(\mathcal{B}) = \mathrm{Zero}(\mathcal{B} \cup \bar{\mathbb{P}}) \cup \mathrm{Zero}(\mathcal{B} \cup \{I_i\}) \cup \mathrm{Zero}(\mathcal{B} \cup \{S_i\}).$$

Since $\mathcal{B}$ is a Wu characteristic set of $\mathbb{P}$, we have $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{P}\cup\mathcal{B}) = \mathrm{Zero}(\mathbb{P}\cup\mathcal{B}\cup\bar{\mathbb{P}})\cup\cup_i\mathrm{Zero}(\mathbb{P}\cup \mathcal{B} \cup \{I_i\}) \cup \mathrm{Zero}(\mathbb{P} \cup \mathcal{B} \cup \{S_i\})$. This proves the correctness of the algorithm. The termination of the algorithm is guaranteed by Lemmas 3.4 and 3.5. □

We now show how to solve the perfect ideal membership problem.

Corollary 6.7. *There exists an algorithm which takes a finite set $\mathbb{P} \subseteq \mathbb{K}$ and $Q \in \mathbb{P}$ on input and which checks whether $Q \in \{\mathbb{P}\}$.*

Proof. By Proposition 2.11, we have $Q \in \{\mathbb{P}\}$ if and only if $\mathrm{Zero}(\mathbb{P} \cup \{zQ - 1\}) = \emptyset$ for a new variable z. Now the theorem yields a decomposition

$$\mathrm{Zero}(\mathbb{P} \cup \{zQ - 1\}) = \bigcup_{i=1}^{m} \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_i)), \tag{25}$$

where $\mathcal{A}_i$ are coherent and proper irreducible chains. We have $\mathrm{Zero}(\mathrm{sat}(\mathcal{A}_i)) \neq \emptyset$ for each i, by Theorem 5.15. Hence $Q \in \{\mathbb{P}\}$ if and only if $m = 0$ in (25). □

Example 6.8. Let $A_1 = y_{1,2,0} - y_{0,0,0}, A_2 = y_{2,2,0} - y_{0,0,2}$ and $\mathcal{A} = A_1, A_2$. Then $\mathcal{A}$ is already a coherent chain and the algorithm **ZDT** directly calls **ProIrr**($\mathcal{A}$). The algorithm **ProIrr** calls **DCS**($\bar{\mathcal{A}}$), since $\mathcal{A}^* = A_1, \delta A_1, A_2, \delta A_2$ is an algebraic irreducible triangular set. In the algorithm **DCS**, we have $H = 1$ and, under the new variable order $y_{0,0,2} > y_{0,0,0} > y_{0,1,2} > y_{0,1,0} > y_{1,2,0} > y_{1,3,0} > y_{2,2,0} > y_{2,3,0}$,

$$\mathrm{Zero}(\mathcal{A}^*) = \mathrm{Zero}(\mathrm{dsat}(A_1, \delta A_1, A_3, \delta A_3)) = \mathrm{Zero}(A_1, \delta A_1, A_3, \delta A_3),$$

Please cite this article in press as: Gao, X.S., et al., Characteristic set method for differential–difference polynomial systems. Journal of Symbolic Computation (2009), doi:10.1016/j.jsc.2008.02.010

where $A_3 = y_{2,2,0} - y_{1,2,2}$. The algorithm **DCS** returns A_1, δA_1, A_3, δA_3. Back in the algorithm **ProIrr** we have $G_1 = \delta^{-2}\{A_3\} = \{A_4 = y_{2,0,0} - y_{1,0,2}\}$. The algorithm **ProIrr** returns (false,$\{A_4\}$). We now return to the algorithm **ZDT** with input $\{A_1, A_2, A_4\}$. Since $\mathcal{B} = A_1, A_4$ is a coherent and proper irreducible chain, the algorithm returns $\mathcal{B}$ and we have $\text{Zero}(\mathcal{A}) = \text{Zero}(\text{sat}(\mathcal{B})) = \text{Zero}(\mathcal{B})$.

Acknowledgements

The first, third and fourth authors' work is partially supported by the National Key Basic Research Project of China. The second author's work has partially been supported by the Gecko ANR project.

References

Aubry, P., Lazard, D., Maza, M.M., 1999. On the theory of triangular sets. Journal of Symbolic Computation 28, 105–124.

Boulier, F., Lazard, D., Ollivier, F., Petitiot, M., 1995. Representation for the radical of a finitely generated differential ideal. In: Proc. of ISSAC'95. ACM Press, New York, pp. 158–166.

Bouziane, D., Kandri Rody, A., Maârouf, H., 2001. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. Journal of Symbolic Computation 31, 631–649.

Chou, S.C., Gao, X.S., 1990. Ritt–Wu's decomposition algorithm and geometry theorem proving. In: Stickel, M.E. (Ed.), CADE'10. In: LNCS, vol. 449. Springer-Verlag, pp. 207–220.

Chou, S.C., Gao, X.S., 1993. Automated reasoning in differential geometry and mechanics: Part I. An improved version of Ritt–Wu's decomposition algorithm. Journal of Automated Reasoning 10, 161–172.

Cohn, R.M., 1965. Difference Algebra. Interscience Publishers.

Cohn, R.M., 1948. Manifolds of difference polynomials. Transactions of AMS 64, 133–172.

Gao, X.S., Chou, S.C., 1993. The dimension of ascending chains. Chinese Science Bulletin 38 (5), 396–399.

Gao, X.S., Luo, Y., Yuan, C.M., 2009. A characteristic set method for ordinary difference polynomial systems. Journal of Symbolic Computation 44, 242–260.

Gao, X.S., Luo, Y., Zhang, G., 2006. A characteristic set method for ordinary difference polynomial systems. In: MM-Preprints, vol. 25. pp. 84–102.

Gao, X.S., Yuan, C., 2006. Resolvent systems of difference polynomial ideals. In: Proc. ISSAC 2006. ACM Press, New York, pp. 101–108.

Hubert, É., 2000. Factorization-free decomposition algorithms in differential algebra. Journal of Symbolic Computation 29, 641–662.

Kolchin, E., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.

Kondratieva, M.V., Levin, A.B., Mikhalev, A.V., Pankratiev, E.V., 1999. Differential and Difference Dimension Polynomials. Kluwer Academic Publishers.

Ritt, J.F., 1950. Differential Algebra. American Mathematical Society.

Ritt, J.F., Doob, J.L., 1933. Systems of algebraic difference equations. American Journal of Mathematics 55, 505–514.

Ritt, J.F., Raudenbush, H.W., 1939. Ideal theory and algebraic difference equations. Transactions of AMS 46, 445–452.

Rosenfeld, A., 1959. Specialization in differential algebra. Transactions of American Mathematical Society 90, 394–407.

Wang, D., 2000. Elimination Methods. Springer, Berlin.

van der Hoeven, J., 1996. Differential and mixed differential-difference equations from the effective viewpoint. Preprints.

Wu, W.T., 1989. On the foundation of algebraic differential polynomial geometry. Systems Science & Mathematical Sciences 2 (4), 289–312.

Wu, W.T., 1984. Basic Principle of Mechanical Theorem Proving in Geometries. Science Press, Beijing, English translation, Springer, Wien, 1994.

Wu, W.T., 2001. Mathematics Machenization. Science Press/Kluwer, Beijing.

Yang, L., Zhang, J.Z., Hou, X.R., 1996. Non-linear Algebraic Equations and Automated Theorem Proving. ShangHai Science and Education Pub., Shanghai (in Chinese).