Computational Differential Algebra
A Mini Introductory Course

William Sit[1]

The City College of The City University of New York

Theory of Singularities and Its Relation to
Arc Schema and Differential Algebra
L'université de Versailles Saint-Quentin-en-Yvelines
More Invariants from Arc Spaces Days
September 25–29, 2017

[1]Special thanks to Julien Sebag for the invitation.

Partially Reduced, Reduced, and Autoreduced

- A D.P. G is **partially reduced w.r.t. a (finite) set $\mathbf{A}$ of DPs** if no proper derivative of any leader u_A for any $A \in \mathbf{A}$ appears in G.
- A D.P. G is **reduced w.r.t. $\mathbf{A}$** if either $G = 0$ or G is partially reduced w.r.t. $\mathbf{A}$ and $0 \leqslant \deg_{u_A} G < \deg_{u_A} A$ for all $A \in \mathbf{A}$.
- **Warning!** F can be $\succ A$ and yet be reduced w.r.t. A.
- When $\Delta = \emptyset$, every G is partially reduced with respect to every $A \notin \mathfrak{F}$, and is reduced with respect to $\mathbf{A}$ if for every $A \in \mathbf{A}$, either u_A does not appear in G or appears to a lower degree.
- Let $\mathbf{A} \subset \mathfrak{R} \backslash \mathfrak{F}$. We say $\mathbf{A}$ is **autoreduced w.r.t. a fixed given ranking $\preceq$** if every $A \in \mathbf{A}$ is reduced with respect to every other $A' \in \mathbf{A}$.
- In particular, the empty set and the set consisting of a single differential polynomial A, $A \notin \mathfrak{F}$, are autoreduced.

Autoreduced Sets Are Finite

Proposition 4.20

Any autoreduced set $\mathbf{A}$ *is finite and triangular with respect to its leaders when its elements are arranged in order of increasing rank.*

Proof. Distinct members of $\mathbf{A}$ have distinct leaders. So $\mathbf{A}$ is finite by Dickson's Lemma.

- When $\Delta = \emptyset$, an autoreduced set $\mathbf{A} \subset \mathcal{F}[y_1, \ldots, y_n]$ is in triangular form. So $\mathbf{A}$ can have no more than n elements.

Example of an Autoreduced Set

- Let $m = 1$, $n = 2$, with the unique orderly ranking such that $w \prec z$. Let

$$\begin{aligned} A &= (z')^3(\underline{z'''})^2 - w'' \\ B &= (z')^3(\underline{z''})^2 - w'' \\ F &= \underline{w^{(4)}} - (w')^2 z''' \end{aligned}$$

- F is reduced with respect to A.
- F is not partially reduced with respect to B.
- F is of higher rank than A because the ranking is orderly.
- Since A is reduced with respect to F, $\{ A, F \}$ is autoreduced, but $\{ B, F \}$ is not.

Algebraically Reduced vs Reduced

- Any $\mathbf{A} \subset \mathfrak{R}$ may be considered as a subset of a polynomial subring $\mathfrak{F}[V]$, where $V \subset \Theta Y$ is any set containing all the derivatives that appear in one or more $A \in \mathbf{A}$. This gives rise to two notions of "autoreduction". They are **not equivalent**.
- An autoreduced subset of $\mathfrak{R}$ is an autoreduced subset of $\mathfrak{F}[V]$ (viewed as the "$\Delta = \emptyset$" case) but not conversely.
- In the previous example,

$$\begin{aligned} B &= (z')^3(\underline{z''})^2 - w'' \\ F &= \underline{w^{(4)}} - (w')^2 z''' \end{aligned}$$

F is "reduced" with respect to B in the polynomial ring $\mathfrak{F}[z', z'', z''', w'', w^{(4)}]$ and hence $\{ F, B \}$ is "algebraically autoreduced" but not (Ritt-Kolchin) autoreduced.

Comparative Rank for Autoreduced Sets

- Let $\mathbf{A}: A_1 \prec A_2 \prec \cdots \prec A_r$ and $\mathbf{B}: B_1 \prec \cdots \prec B_s$ be two autoreduced sets in $\mathfrak{F}\{y_1, \cdots, y_n\}$. We extend the concept of (comparative) rank to autoreduced sets.
- We say **A is of lower rank than B** if either

  (a). for some t, $1 \leqslant t \leqslant \min(r, s)$, $\mathrm{rank}\,(A_i) = \mathrm{rank}\,(B_i)$ for $1 \leqslant i < t$ and $\mathrm{rank}\,(A_t) \prec \mathrm{rank}\,(B_t)$, or

  (b). $r > s$ and $\mathrm{rank}\,(A_i) = \mathrm{rank}\,(B_i)$ for $1 \leqslant i \leqslant s$.

  Otherwise, **A and B have the same rank** if $r = s$ and $\mathrm{rank}\,(A_i) = \mathrm{rank}\,(B_i)$ for $1 \leqslant i \leqslant s$.
- The relation $\preceq$ is a preorder on autoreduced sets.

Proposition 4.24

Let $\mathcal{A}$ be any non-empty set of autoreduced subsets of $\mathfrak{F}\{y_1, \cdots, y_n\}$. Then there exists an autoreduced subset $\mathbf{A} \in \mathcal{A}$ which has the lowest rank.

Characteristic Sets

Example

Characteristic Set of a Differential Polynomial Ideal

- Let $\mathfrak{a}$ be a differential ideal of $\mathcal{R} = \mathcal{F}\{ y_1, \cdots , y_n \}$.
- A **characteristic set of $\mathfrak{a}$** is an autoreduced subset $\mathbf{A}$ with the property that $S_A \notin \mathfrak{a}$ for all $A \in \mathbf{A}$ and is one of lowest rank with such properties.
- By Proposition 4.24, every differential ideal has a characteristic set.
- The characteristic set of $\mathcal{R}$ or (0) is the empty set!
- For a fixed ranking, a differential ideal may have more than one characteristic set. However, the lengths of any two and the corresponding ranks of their elements are always the same.
- A characteristic set of $\mathfrak{a}$ usually does not generate $\mathfrak{a}$ as a differential ideal, or as a radical differential ideal.

Characterization of Characteristic Sets

Lemma 5.3

Let $\operatorname{char} \mathfrak{F} = 0$ *and let* **A** *be an autoreduced subset of a proper differential ideal* $\mathfrak{a}$ *in* $\mathfrak{R} = \mathfrak{F}\{\, y_1, \cdots, y_n \,\}$*. Then the following are equivalent:*

(a). **A** *has the lowest rank among all autoreduced sets* **B** *of* $\mathfrak{a}$*.*

(b). **A** *is a characteristic set of* $\mathfrak{a}$*.*

(c). $\mathfrak{a}$ *is zero-reduced with respect to* **A***.*

- A subset Σ of $\mathfrak{R} = \mathfrak{F}\{\, y_1, \cdots, y_n \,\}$ is said to be **zero-reduced** w.r.t. an autoreduced set **A** if no non-zero element $F \in \Sigma$ is reduced w.r.t. **A**.

Proof of Lemma 5.3: (a) $\Rightarrow$ (b)

- Suppose that $\mathbf{A}$ is of lowest rank. Let $\mathbf{B}$ be a characteristic set of $\mathfrak{a}$. Clearly, $\mathbf{A}$ has lower rank than, or same rank as, $\mathbf{B}$. So it needs to be shown that $S_A \notin \mathfrak{a}$ for all $A \in \mathbf{A}$.
- This is trivially true if $\mathbf{A} = \emptyset$. Otherwise, S_A is non-zero ($\mathfrak{F}$ has characteristic zero) and is reduced with respect to $\mathbf{A}$.
- If $S_A \notin \mathfrak{a}$ for all $A \in \mathbf{A}$, then we are done.
- Suppose for some $C \in \mathbf{A}$, $F = S_C \in \mathfrak{a}$.
- Then F and the elements A of $\mathbf{A}$ for which u_A is lower than the leader u_F of F would form an autoreduced set of lower rank than $\mathbf{A}$, which would be a contradiction.

Proof of Lemma 5.3:(b) $\Rightarrow$ (c)

- Suppose there were a non-zero differential polynomial in $\mathfrak{a}$, reduced with respect to **A** and let F be one with minimal rank.
- Then $F \notin \mathfrak{F}$ because $\mathfrak{a}$ is proper.
- F together with the elements of **A** for which u_A is lower than the leader u_F of F would be an autoreduced set **B** of lower rank than **A**.
- So **B** does not have the property that all its separants are not in $\mathfrak{a}$. The only one that could fail is F because **A** is a characteristic set.
- Thus $S_F \in \mathfrak{a}$, and is non-zero and reduced with respect to **A**, but $S_F \prec F$ contradicting the minimality of F.

Proof of Lemma 5.3:(c) $\Rightarrow$ (a)

Suppose that the $\mathbf{A}\colon A_1 < \cdots < A_r$ given in (c) were not the lowest autoreduced subset of $\mathfrak{a}$.

- Let $\mathbf{B}\colon B_1 < \cdots < B_s$ be an autoreduced subset of $\mathfrak{a}$ of lowest rank.
- Then $\mathbf{B}$ has lower rank than $\mathbf{A}$.
- Either for some $t \leqslant \min(r, s)$, $\operatorname{rank}(B_i) = \operatorname{rank}(A_i)$ for $1 \leqslant i < t$ and $\operatorname{rank}(B_t) < \operatorname{rank}(A_t)$, or $s > r$, $\operatorname{rank}(B_i) = \operatorname{rank}(A_i)$ for $1 \leqslant i \leqslant r$.
- Thus, either B_t (in the first case) or B_{r+1} ($r + 1 \leqslant s$ in the second case) would be non-zero and reduced with respect to $\mathbf{A}$. This would be a contradiction to (c).

General Notation and Corollary to Lemma 5.3

- The elements of an autoreduced set will always be listed in order of increasing rank.
- For any **autoreduced set A**: $A_1 \prec \cdots \prec A_p$, we shall denote the corresponding **leaders by** $v_1, \ldots, v_p$, **initials by** $I_1, \ldots, I_p$, **separants by** $S_1, \ldots, S_p$ in addition to u_A, I_A, S_A for $A \in \mathbf{A}$.
- The **product** of initials (resp. separants, resp. initials and separants) is denoted by $I_{\mathbf{A}}$ **(resp.** $S_{\mathbf{A}}$**, resp.** $H_{\mathbf{A}}$**)** or simply I **(resp.** S**, resp.** H**)** if **A** is clear from the context.

Corollary 5.4

Let **A** *be a characteristic set of a proper differential ideal* $\mathfrak{a}$ *in* $\mathfrak{R}$*. Then* I_k *and* S_k *are not in* $\mathfrak{a}$ *for every* $A \in \mathbf{A}$*. If* $\mathfrak{a}$ *is prime, then* I, S, H *are not in* $\mathfrak{a}$*.*

Remarks on Lemma 5.3

- The lemma is trivially true for $\mathfrak{a} = (0)$ since the empty set is the only autoreduced subset (which must be a subset of $\mathfrak{R} \backslash \mathfrak{F}$).
- Let $\mathfrak{a} = \mathfrak{R}$. Then Lemma 5.3 does not hold for $\mathfrak{a}$.
- The set $\mathbf{A}_0$ consisting of $y_1, \ldots, y_n$ (rearranged perhaps) is clearly a lowest autoreduced subset of $\mathfrak{a}$ for any given ranking.
- Any other lowest autoreduced subset $\mathbf{B}$ of $\mathfrak{a}$ must have exactly n elements of the form $b_1 y_1 + c_1, \ldots, b_n y_n + c_n$ where $b_i, c_i \in \mathfrak{F}$ and $b_i \neq 0$ for all i.
- Any element of $\mathfrak{a}$ that has a separant will have it in $\mathfrak{a}$.
- By definition, the only characteristic set of $\mathfrak{a}$ is the empty set.
- Thus (a) and (b) of Lemma 5.3 are not equivalent ($\mathfrak{a} = \mathfrak{R}$).
- In this case, (c) is false (whether one uses the autoreduced set $\mathbf{A}_0$ or the empty autoreduced set).

An Example: Algebra vs Differential Algebra

- Let $\mathcal{R} = K\{\, y, z \,\}$ be an ordinary differential polynomial ring and the **ranking is orderly,** $z \prec y$.
- Let $\quad A_1 = \mathbf{y}^2 + z, \qquad A_2 = \mathbf{y}' + y.$
- Then $\mathbf{\Gamma}\colon A_1 \prec A_2$ is **algebraic autoreduced** as a subset of polynomials in $\mathcal{S} = K[z, y, y']$ and is of lowest algebraic rank for the ideal $J = (A_1, A_2)$ of $\mathcal{S}$, which is prime.
- However, $\mathbf{\Gamma}$ is **not partial autoreduced**, because A_2 is not partially reduced with respect to A_1.
- Let $\quad A_3 = A_1' + 2A_1 - 2yA_2 = \mathbf{z}' + 2z.$
- Then $A_3 \in \mathfrak{a} := [A_1, A_2]$, and $\mathfrak{a}$ is prime, with a **Ritt-Kolchin characteristic set** $\mathbf{A}\colon A_1 \prec A_3$.

Example, continued

- **A has lower Ritt-Kolchin rank than Γ**.
- We have $\mathfrak{a} = [\mathbf{A}] : 2y$ where $2y$ is the product of initials and separants of $\mathbf{A}$.
- **Thus an algebraic characteristic set of a prime ideal need not be a Ritt-Kolchin characteristic set of the differential ideal it generates**.
- The ideal J, being a subset of $\mathfrak{a}$, does not contain any non-zero element Ritt-Kolchin reduced with respect to $\mathbf{A}$, but contains A_2 which is algebraic-reduced with respect to $\mathbf{A}$ as a polynomial in $K[z, y, z', y']$.
- Also, A_3 is a non-zero differential polynomial which is Ritt-Kolchin reduced with respect to $\mathbf{\Gamma}$.

Ritt-Kolchin's Reduction Algorithms

vs

Gröbner Reduction

Differentiating a Differential Polynomial (DP)

- Fix any ranking. Let $A \in \mathfrak{R}\backslash\mathfrak{F}$ have leader u_A, initial I_A and separant S_A.

$$A = \underline{I_d u_A^d} + I_{d-1} u_A^{d-1} + \cdots + I_0, \qquad (4.9)$$

where $I_A := I_d$, and $I_d, I_{d-1}, \ldots, I_0 \in \mathfrak{R}_{(u_A)}$.

- Applying the product and chain rules, we have

$$\begin{aligned}\delta A &= (\underline{\mathbf{d} I_d \mathbf{u_A^{d-1}}} + (\mathbf{d-1}) I_{d-1} \mathbf{u_A^{d-2}} + \cdots + I_1)\underline{\delta \mathbf{u_A}} + \\ &\quad \underline{\delta(I_d) u_A^d} + \delta(I_{d-1}) u_A^{d-1} + \cdots + \delta(I_1) u_A + \delta(I_0).\end{aligned}$$

- **The leader of δA is δu_A** since $v \prec u_A \Longrightarrow \delta v \prec \delta u_A$ for any derivative v that appears in any I_j, $(0 \leqslant j \leqslant d)$.
- **The initial (resp. the separant) δA is the separant of A.**
- $\delta A = S_A \delta u_A - T$, **where** $T \prec \delta u_A$.

Pseudo-division by One Derivative of a DP

- For any $1 \neq \theta \in \Theta$, we have $\theta A = S_A \theta u_A - T$ **with** $T \prec \theta u_A$.
- When we perform pseudo-division of $F \in \mathfrak{R}$ by G, we get for some $q \in \mathbb{N}$, $I_G^q \cdot F = Q \cdot G + \widetilde{F}$ with $\widetilde{F} \in \mathfrak{R}_{[u_G]}$, and either $\widetilde{F} = 0$ or $\deg_{u_G} \widetilde{F} < \deg_{u_G} G$.
- In the special case when $G = \theta A$, G is linear in $u_G = \theta u_G$, $I_G = S_G = S_A$ (independent of θ), $q = \deg_{\theta u_A} F$, and $\widetilde{F} \in \mathfrak{R}_{[u_F]}$. If θu_A appears in F, we can simply **substitute algebraically** using $\theta u_A = \frac{\theta A + T}{S_A}$ into F. The LCD is S_A^q. The remainder $\widetilde{F}$ would not involve θu_A. **However ...**
- **If θu_A is the highest derivative $v(F, A)$ of that form appearing in F to degree e**, then we have

$$S_A^e F \equiv \widetilde{F}_\theta \mod (\theta A)$$

where $\widetilde{F}_\theta$ does not involve θu_A and $v(\widetilde{F}_\theta, A) \prec v(F, A)$.

Partial Remainder Modulo a DP

- Iterating this **choice**, $v(F, A)$, using $\widetilde{F}_\theta$ in place of F, will result in a congruence of the form

$$S_A^q F \equiv \widetilde{F} \mod (\{\, \theta A \mid \theta \in \Theta, \theta \neq 1 \,\}),$$

where $q \in \mathbb{N}$ and $\widetilde{F}$ involves no proper derivatives of u_A, that is, $\widetilde{F}$ **is partially reduced w.r.t.** A.

- The iterated pseudo-divisions produce a sequence $\widetilde{F}_\theta$ with $v(\widetilde{F}_\theta, A)$ strictly decreasing and hence will terminate.

- The output of this process (partial reduction), $\widetilde{F}$, is an example of a **partial remainder of F w,r,t. A, or modulo $[A]$**.

Remainder Modulo a Single DP

- Further pseudo-reduction by A may not remove u_A from $\widetilde{F}$ but will result in lowering the degree of $\widetilde{F}$ in u_A.
- The entire process produces a pseudo-remainder $F_0 \in \mathfrak{R}$ which is partially reduced w.r.t. A, possibly 0, or $0 \leqslant \deg_{u_A} F_0 < \deg_{u_A} A$. For some $p, q \in \mathbb{N}$, F_0 satisfies:

$$I_A^p S_A^q F \equiv F_0 \mod [A].$$

- The output F_0 is reduced w.r.t. A and an example of a **remainder of F w,r,t. A, or modulo $[A]$**.
- The process has two phases: the differential elimination phase, and the algebraic elimination phase. Both can take place inside a polynomial ring with finitely many (algebraic) indeterminates, namely, $\mathfrak{R}_{[u_F]}$.

Choices in the Reduction Process w.r.t a Set

- Convention: when discussing reduction, θu_A always means $\theta \in \Theta$, $A \in \mathbf{A} : A_1 \prec \cdots \prec A_p$, with $\theta \neq 1$ in the differential phase and $\theta = 1$ otherwise. We define $D(F, \mathbf{A})$ to be **the finite set of θu_A appearing in F**, depending on the phase.
- We can choose which among the θu_A appearing in F is eliminated first. One choice is $v(F, \mathbf{A})$, defined as **the (unique) highest ranked derivative in $D(F, \mathbf{A})$ if $\neq \emptyset$**.
- Then we need to choose C and θ such that $v(F, \mathbf{A}) = \theta u_C$. One choice is $C(F.\mathbf{A})$, **the (unique) highest ranked one**, which uniquely determines θ (to be denoted $\theta(F, \mathbf{A})$.)
- Lastly, one choice of the pseudo-exponent in the pseudo-division of F by θC is **the default pseudo-exponent.**
- By requiring $\mathbf{A}$ be be autoreduced, we avoid the situation when $\theta u_C = u_A$. This clearly demarcates the differential phase from the algebraic phase.

Partial Remainders and Remainders

- Fix a ranking $\preceq$, a differential polynomial F, and a **non-empty** autoreduced set $\mathbf{A}$: $A_1 \prec A_2 \prec \cdots \prec A_p$.
- By **a partial remainder** of F w.r.t. $\mathbf{A}$, we mean any $\widetilde{F}$, partially reduced w.r.t. $\mathbf{A}$ such that there exist $s_A \in \mathbb{N}$ and $A \in \mathbf{A}$ satisfying the property that

$$\prod_{A \in \mathbf{A}} S_A^{s_A} \cdot F - \widetilde{F} \in [\mathbf{A}]. \tag{6.2}$$

- By **a remainder** of F w.r.t. $\mathbf{A}$, we mean any F_0, reduced w.r.t. $\mathbf{A}$ such that there exist $i_A, s_A \in \mathbb{N}$ and $A \in \mathbf{A}$ satisfying the property that

$$\prod_{A \in \mathbf{A}} I_A^{i_A} S_A^{s_A} \cdot F - F_0 \in [\mathbf{A}]. \tag{6.8}$$

Ritt-Kolchin's (Partial) Remainder

- Ritt and Kolchin defined **the partial remainder** $\widetilde{F}$ and **the remainder** F_0 of F w.r.t. $\mathbf{A}$ as the results of a **specific** reduction procedure.
- The choices given earlier were theirs.
- Procedure 6.3 should be run first in the differential elimination phase to obtain $\widetilde{F}$ and again in the algebraic phase with input $\widetilde{F}$ to get F_0 (with some obvious change in notation). Optionally, the pseudo-exponents and pseudo-quotients can be tracked and output if desired by uncommenting the lines preceded by a % sign.

Procedure 6.3

Ritt-Kolchin's (Partial) Remainder Algorithm

Input: *A ranking* $\preceq$, *a non-empty autoreduced set* $\mathbf{A}$, $F \in \mathfrak{R}$

Output: $\widetilde{F}$, *partial remainder* (*resp.* F_0, *remainder*) *of* F

Procedure:

$\widetilde{F} := F$

% $e_A := 0$ for all $A \in \mathbf{A}$

% $Q_w := 0$ for all $w \in \Theta Y, w \preceq u_F$

While $D(\widetilde{F}, \mathbf{A}) \neq \emptyset$ **repeat**

$v := v(\widetilde{F}, \mathbf{A})$

$C := C(\widetilde{F}, \mathbf{A})$

$\theta := \theta(\widetilde{F}, \mathbf{A})$

$\mathcal{S}$:= largest polynomial subring of $\mathcal{R}_{[u_{\widetilde{F}}]}$ not containing v

% $Q_v := Q_v + Q(\widetilde{F}, \theta C, \mathcal{S}, v)$

% $e_C := e_C + E(\widetilde{F}, \theta C, \mathcal{S}, v)$

$\widetilde{F} := R(\widetilde{F}, \theta C, \mathcal{S}, v)$

return $\widetilde{F}$

Constructive Aspects of Procedure 6.3

- The initialization of Q_w apparently could involve infinitely many w if the ranking is not sequential. However, a new program variable Q_v can be created each time a new v is used during implementation. The set of Q_w needed is finite.
- The commented lines (with % sign) keep track of, and collect, the pseudo-quotients Q_v and exponents e_A (e_A is s_A for the partial reduction phase, and i_A for the algebraic phase), and may return two representations:

$$\prod_{A \in \mathbf{A}} S_A^{s_A} \cdot F - \widetilde{F} = \sum_{A \in \mathbf{A}, 1 \neq \theta \in \Theta, \theta A \preceq F} Q_{\theta u_A} \theta A \qquad (6.2a)$$

$$\prod_{A \in \mathbf{A}} I_A^{i_A} S_A^{s_A} \cdot F - F_0 = \sum_{A \in \mathbf{A}, \theta \in \Theta, \theta A \preceq F} Q'_{\theta u_A} \theta A \qquad (6.8a)$$

where $Q_{\theta u_A}, Q'_{\theta u_A} \in \mathfrak{R}_{[u_F]}$.

Differential Ideal Membership Test

Corollary 6.13

Let $\mathfrak{a}$ be a **proper** *differential ideal in $\mathfrak{R} = \mathfrak{F}\{y_1, \cdots, y_n\}$. Let $\preceq$ be a ranking and let $\mathbf{A}\colon A_1, \ldots, A_p$ be a* **characteristic set** *of $\mathfrak{a}$ relative to the ranking $\preceq$. Let $H = \prod_{k=1}^{p} I_k S_k$ be the product of initials and separants of $\mathbf{A}$, and let $\mathfrak{a}_H := [\mathbf{A}] : H^\infty$. Let $F \in \mathfrak{a}$ and F_0 be any remainder of F w.r.t. $\mathbf{A}$. Then*

(a). $F_0 = 0$;

(b). $\mathfrak{a} \subseteq \mathfrak{a}_H$, *and if $\mathfrak{a}$ prime, equality holds;*

(c). *if $\mathfrak{a}$ is radical, $\mathfrak{a}_H$ is radical and $a_H = \mathfrak{a} : H$.*

- If $\mathfrak{a}$ is prime, then $F \in \mathfrak{a}$ if and only if $F_0 = 0$. So we have a prime differential ideal membership test.
- Later, with the decomposition algorithm of radical differential ideals into primes, we can solve the membership problem for radical differential ideals.

Proof of Corollary 6.13

- (a). Since $F_0 \in \mathfrak{a}$ and is reduced, and **A** is a characteristic set, $F_0 = 0$ by Lemma 5.3: $\mathfrak{a}$ is zero-reduced w.r.t any characteristic set of $\mathfrak{a}$.
- By definition, $\mathfrak{a} \subseteq \mathfrak{a} \colon H := \{\, F \in \mathfrak{R} \mid HF \in \mathfrak{a} \,\} \subseteq \mathfrak{a}_H$.
- (b) By definition, F and F_0 satisfy an equation of the form (6.8a) holds and hence $F \in \mathfrak{a}_H$ by Part (a).
  Suppose $\mathfrak{a}$ is prime. Let $P \in \mathfrak{a}_H$, say $H^t P \in [\mathbf{A}] \subseteq \mathfrak{a}$ for some $t \in \mathbb{N}$. If $t = 0$, $P \in \mathfrak{a}$, otherwise since $H \notin \mathfrak{a}$ (by Corollary 5.4), $P \in \mathfrak{a}$.
- (c) Suppose $\mathfrak{a}$ is radical. Then $a\colon H$ is radical.
  If $Q \in \mathfrak{a}_H$, then $H^s Q \in \mathfrak{a}$ for some $s \geqslant 0$. Since $\mathfrak{a}$ is radical, $HQ \in \mathfrak{a}$ and $Q \in \mathfrak{a}\colon H$, proving $\mathfrak{a} : H = \mathfrak{a}\colon H$.

Rosenfeld Properties

Ideal Properties

Decidability Questions

Rosenfeld Properties of an Autoreduced Set

- The link between algebra and differential algebra is made possible by a property of certain autoreduced sets first introduced in a lemma of Rosenfeld [35].

- Broadly speaking, this property is what permits reducing certain computational problems in differential polynomial algebra to those of polynomial algebra.

- We call this property as the **Rosenfeld property**, and introduce a stronger variation and investigate the relations between certain differential ideals and their polynomial counterparts.

General Setup for Rosenfeld Properties

- $\mathbf{A} : A_1, \ldots, A_p$ is an autoreduced subset of $\mathcal{R} := \mathcal{F}\{\, y_1, \cdots, y_n \,\}$ and $v_i = u_{A_i}$.
- V is a subset of ΘY such that $\mathbf{A} \subset \mathcal{F}[V]$.
- $\mathcal{S}_0 := \mathcal{F}[V \backslash \{\, v_1, \ldots, v_p \,\}]$.
- We view $\mathbf{A}$ as a set of polynomials in $\mathcal{S}_0[v_1, \ldots, v_p]$, triangular over $\mathcal{S}_0$ with respect to $v_1, \ldots, v_p$.
- If $G = I$ (resp. $G = S$, resp. $G = H$), then
  J_G^V is the **ideal** $(\mathbf{A}) : G^\infty$ of $\mathcal{S}_0[v_1, \ldots, v_p] = \mathcal{F}[V]$;
  J_G is the **ideal** $(\mathbf{A}) : G^\infty$ of $\mathcal{R}$;
  $\mathfrak{a}_G$ is the **differential ideal** $[\mathbf{A}] : G^\infty$ of $\mathcal{R}$.
- J_G^V (resp. $\mathfrak{a}_G$) are called the **saturation (resp. differential) ideal of A w.r.t. initials (separants, initials and separants) in their (resp. differential) rings.**

Rosenfeld Property and Strong Rosenfeld Property

- We say that **A** has the **Rosenfeld Property** (resp. **Strong Rosenfeld Property**) if every differential polynomial F partially reduced (w.r.t. **A**) belonging to the differential ideal $\mathfrak{a}_H$ (resp. $\mathfrak{a}_S$) already belongs to the ideal J_H (resp. J_S) in $\mathfrak{R}$.
- **Strong Rosenfeld Property** $\Rightarrow$ **Rosenfeld Property**.
  Proof: Let $F \in \mathfrak{a}_H = \mathfrak{a}_S : I^\infty$ be partially reduced; then $I^t F \in \mathfrak{a}_S$ and since the initials I_A are partially reduced, $I^t F \in J_S$ by the Strong Rosenfeld Property. Hence $F \in J_H = J_S : I^\infty$.
- For the differential ideals $\mathfrak{a}_H$ and $\mathfrak{a}_S$, we shall be interested in the properties of being **prime, radical, and zero-reduced**.
- **Which of these three properties may be deduced from corresponding properties of the ideals J_H, J_S?**

The Answers? **A L L !**

Proposition 7.3

Suppose **A** *has the Rosenfeld Property (resp. Strong Rosenfeld Property). Then*

(a). $\mathfrak{a}_H$ *(resp.* $\mathfrak{a}_S$*) is prime if and only if* J_H *(resp.* J_S*) is;*

(b). $\mathfrak{a}_H$ *(resp.* $\mathfrak{a}_S$*) is radical if and only if* J_H *(resp.* J_S*) is;*

(c). $\mathfrak{a}_H$ *(resp.* $\mathfrak{a}_S$*) is zero-reduced if and only if* J_H *(resp.* J_S*) is.*

- Even if **A** does not have the Rosenfeld Property, **the ideal J_S is always radical**. This fact is known as **Lazard's Lemma**. It follows that $J_H = J_S : I$ **is also always radical**.
- Thus by the above, $\mathfrak{a}_H$ (resp. $\mathfrak{a}_S$) is radical if **A** has the Rosenfeld property (resp. strong Rosenfeld property).
- However, J_I **may be prime but $\mathfrak{a}_I$ is not even radical!** Example after some more development.

Proof of Proposition 7.3(a)

- We will only prove the case when **A** has the strong Rosenfeld property. Let $F, G \in \mathfrak{R}$ and let $\widetilde{F}$ (resp. $\widetilde{G}$) be some partial remainder of F (resp. G) with respect to **A**.

J_S is prime implies $\mathfrak{a}_S$ is prime.

- Suppose $FG \in \mathfrak{a}_S$. Since $S^pF \equiv \widetilde{F} \mod [\mathbf{A}]$ and $S^qG \equiv \widetilde{G} \mod [\mathbf{A}]$, $\widetilde{F}\widetilde{G} \in \mathfrak{a}_S$ and is partially reduced and hence by the Strong Rosenfeld Property, $\widetilde{F}\widetilde{G} \in J_S$.
So say $\widetilde{F} \in J_S \subseteq \mathfrak{a}_S$. By congruence, $F \in= \mathfrak{a}_S$ and $\mathfrak{a}_S$ is prime.

$\mathfrak{a}_S$ is prime implies J_S is prime.

- Let V be the set of all derivatives θy_j that are partially reduced with respect to **A**. Let $J_S^V = (\mathbf{A}) \colon S^\infty$ in $\mathfrak{F}[V]$. Then $J_S^V = J_S \cap \mathfrak{F}[V] \subseteq \mathfrak{a}_S \cap \mathfrak{F}[V]$. By the Strong Rosenfeld Property, equality holds, and hence J_S^V is prime and so is J_S.

Decidability of the Three Properties

- The three properties of J_H and J_S are properties of $\mathbf{A}$, and are independent of the ambient (finite) polynomial ring containing $\mathbf{A}$. Moreover, these properties are computationally decidable.

Exercise 7.7

Let $\emptyset \neq V \subseteq \Theta Y$, J^V an ideal in $\mathfrak{F}[V]$, and J the ideal in $\mathfrak{R}$ generated by J^V. Then J is prime (resp. radical, resp. zero-reduced w.r.t. an autoreduced set $\mathbf{A} \subset \mathfrak{F}[V]$) $\iff$ J^V is.

Proposition 7.8

Let J be an ideal generated by a given set Φ in a polynomial ring $\mathfrak{F}[V]$ with V finite. Then the property of J being prime or radical is decidable. Moreover, if J is not radical, then one can find a polynomial $F \notin J$, and a natural number e such that $F^e \in J$; if J is not prime, then one can find a pair of polynomials $F, F' \notin J$ such that $FF' \in J$.

Proof of Proposition 7.8

Testing if ideal is radical

- Using the Gröbner basis method, we may assume that J is proper, compute the radical $\sqrt{J}$ of J, and test the inclusion $\sqrt{J} \subseteq J$, thus deciding whether J is a radical ideal or not.

When J is not prime and not radical

- The Gröbner basis of $\sqrt{J}$ will include a polynomial $F \notin J$. By Nullstellensatz and the Rabinowitsch Trick, we can find an exponent $e \geqslant 2$ such that $F^e \in J$. Let $F' = F^{e-1}$.

When J is not prime but is radical

- If J is radical, compute its irredundant prime decomposition $J = J_1 \cap \cdots \cap J_r$. If $r = 1$, J is prime. Otherwise, find an $F_i \in J_i$ but $F_i \notin J$. Let k be the least integer i such that the product $F_1 F_2 \cdots F_i$ belongs to J. Then $k > 1$ and take $F = F_1 \cdots F_{k-1}$ and $F' = F_k$.

Coherence and Subcoherence

Rosenfeld Properties

Equivalence Questions

Autoreduced Set as a Characteristic Set of Its Saturated Differential Ideal by H

Lemma 7.9

- *Let* $\mathbf{A}: A_1 < \cdots < A_p$ *be an* **autoreduced** *set in* $\mathfrak{R}$. *Let* I *be the product of initials* $I_1, \ldots, I_p$. *Let* V *be a finite subset of* ΘY *such that* $\mathbf{A} \subset \mathfrak{F}[V]$. *Suppose:*

  (a). $\mathbf{A}$ *has* **the Rosenfeld Property**;

  (b). $\mathbf{A}$, *as a* **triangular** *set of polynomials in* $\mathfrak{F}[V]$ *with respect to its leaders* $v_1, \ldots, v_p$ **has invertible initials**;

  (c). **the ideal** J_I^V **of** $\mathfrak{F}[V]$ **is radical and** $J_I^V = J_H^V$ (*resp.* J_I^V *is prime and does not contain any separants of* $\mathbf{A}$).

- **Then** $J_I = J_H$, *the differential ideal* $\mathfrak{a}_H$ **is radical** (*resp. prime*) *and* **A is its characteristic set**.

Proof of Lemma 7.9

- J_I is generated by J_I^V, and is radical (resp. prime).
- Observe that when J_I^V is prime and does not contain any separants of **A**, the assumption $J_I^V = J_H^V$ also holds. Hence $J_I = J_H$ in either situation.
- By Proposition 7.3, $\mathfrak{a}_H$ **is radical (resp. prime)**.
- Let $F \in \mathfrak{a}_H$ be reduced with respect to **A**, By the Rosenfeld Property, $F \in J_H = J_I$. Expressing F as a sum $\sum C_M M$, where M is a monomial in $\overline{V} = \Theta Y \backslash V$ and $C_M \in \mathfrak{F}[V]$ shows each $C_M \in J_I^V$, and is reduced w.r.t. **A**. By Lemma 3.6, $C_M = 0$ for all M and $F = 0$. Hence $\mathfrak{a}_H$ **is zero-reduced**.
- Since the initials and separants of **A** are reduced, they are not in $\mathfrak{a}_H$. $\mathfrak{a}_H$ is a proper ideal. By Lemma 5.3, **A is a characteristic set of** $\mathfrak{a}_H$.

Comments on Lemma 7.9

- **The condition $J_I^V = J_H^V$, or equivalently, J_I^V is radical is not really needed** (Hubert [18, Proposition 3.3]). We also know $\mathfrak{a}_H$ is radical (by Lazard's Lemma and Rosenfeld).
- We include the condition separately here for algorithmic and theoretical reasons.
- Algorithmically, it may be easier to **verify equality of two (polynomial) ideals** than to **test if an ideal is radical**.
- Theoretically, I don't know how to show $\mathfrak{a}_H$ is zero-reduced without using $J_H = J_I$. Instead of $F \in J_I$, we would have $S^e F \in J_I$, and the product $S^e F$ is no longer reduced.
- It is possible that $\mathfrak{a}_H \neq \mathfrak{a}_I$ under the full hypothesis of Lemma 7.9 (in fact, not even under the extra assumption that $\mathbf{A}$ has invertible separants). Example later.

Autoreduced Set as a Characteristic Set of Its Saturated Differential Ideal by S

Exercise 7.12

- Let $\mathbf{A}: A_1 < \cdots < A_p$ be an **autoreduced** set in $\mathcal{R}$ **with the Strong Rosenfeld Property**.
- Let V be a finite subset of ΘY such that $\mathbf{A} \subset \mathcal{F}[V]$.
- Suppose that $\mathbf{A}$, as a **triangular** set of polynomials in $\mathcal{F}[V]$ with respect to its leaders $v_1, \ldots, v_p$ **has invertible initials**, whose product is denoted by I.
- Suppose further that **the ideal** J_I^V **of** $\mathcal{F}[V]$ **is radical** (**resp. prime**) **and** $J_I^V = J_S^V$.
- **Then** $J_I = J_S = J_H$, the differential ideal $\mathfrak{a}_S$ **is radical** (resp. prime), $\mathfrak{a}_S = \mathfrak{a}_H = [\mathbf{A}]: S$, and **A is a characteristic set of** $\mathfrak{a}_S$.
- The proof is analogous to the proof for Lemma 7.9.

Coherence and Rosenfeld's Lemma

- Rosenfeld [35] introduced a **sufficient** condition he called **coherence** on autoreduced sets to ensure that the Rosenfeld property holds and verifiable in a finite number of steps. His Lemma says: **A coherent autoreduced set has the Rosenfeld property**.
- Kolchin [24, p. 135] generalized this to L-**coherence relative to an ideal** L (not necessarily differential, but generated by partially reduced differential polynomials) and over **differential domains of arbitrary characteristic**.
- Morrison [30] introduced notions of **semi-reduction**, **relative coherence**, and Δ-**completeness** with a generalization of Rosenfeld's Lemma.
- Here, we cover Rosenfeld's version of coherence, and three more, one stronger, one equivalent to the Rosenfeld Property, and the last to the Strong Rosenfeld Property.

Coherence and Subcoherence and Strong Versions

- For any $v \in \Theta Y$, and an autoreduced set $\mathbf{A}$, let

$$\mathbf{A}_{(v)} := \{\, \theta A \mid A \in \mathbf{A}, \theta \in \Theta, \theta u_A \prec v \,\}.$$

- A pair (A, A') with $A, A' \in \mathbf{A}$ whose leaders $u_A, u_{A'}$ have a common derivative is called a **Δ-pair**. If $v = \theta u_A = \theta' u_{A'}$ is a common derivative, then $\theta \neq 1$ and $\theta' \neq 1$. We define the **Δ-Syzygy-polynomial w.r.t. the Δ-pair (A, A') and common leading derivative v** to be

$$\Delta(A, A', v) := S_{A'}\theta A - S_A\theta' A' = S_{A'}(S_A v - T) - S_A(S_{A'} v - T')$$

which has lower rank than v.

- We say $\mathbf{A}$ is **coherent** (resp. **subcoherent**, resp. **strongly coherent**, resp. **strongly subcoherent**) if **every** $\Delta(A, A', v)$ belongs to the **ideal** $(\mathbf{A}_{(v)})\colon H^\infty$ (resp. $(\mathbf{A} \cup \mathbf{A}_{(v)})\colon H^\infty$, resp. $(\mathbf{A}_{(v)})\colon S^\infty$, resp. $(\mathbf{A} \cup \mathbf{A}_{(v)})\colon S^\infty$) in the polynomial ring $\mathcal{R}$.

The Four Coherences at a Glance

- strongly coherent $\Rightarrow$ coherent and strongly subcoherent.
- coherent or strongly subcoherent$\Rightarrow$ subcoherent.

$$
\begin{array}{ccc}
\textbf{coherent} & \Rightarrow & \textbf{subcoherent} \\
(\mathbf{A}_{(v)}): H^\infty & \subseteq & (\mathbf{A} \cup \mathbf{A}_{(v)}): H^\infty \\
\Uparrow \quad \cup & & \cup \quad \Uparrow \\
(\mathbf{A}_{(v)}): S^\infty & \subseteq & (\mathbf{A} \cup \mathbf{A}_{(v)}): S^\infty \\
\textbf{strongly coherent} & \Rightarrow & \textbf{strongly subcoherent}
\end{array}
$$

- If $\mathbf{A}$ has no Δ-pairs (for example, if $\mathcal{R}$ is an ordinary differential polynomial ring, or if $\mathbf{A}$ consists of a singleton), then it is strongly coherent.

Decidability and Open Problems

- **The coherence or strong coherence property of an autoreduced set is decidable** since it is enough to verify for finitely many Δ-pairs (A, A') the membership condition on $\Delta(A, A', v)$ when v is a least common derivative of $u_A, u_{A'}$ in a polynomial subring $\mathcal{F}[V]$ of $\mathcal{R}$ where $V \subset \Theta Y$ is finite.

Open Problems

- It is not known whether the properties of subcoherence and strongly subcoherence are decidable. However, they are respectively equivalent to the Rosenfeld property and strong Rosenfeld property.

A Practical Sufficiency Test

- For $\mathbf{A}$ to be coherent (resp. strongly coherent), it is **sufficient** that **the Ritt-Kolchin remainder (resp. partial remainder) of every $\Delta(A, A', v)$ be zero**.
- Reason: For any $F \in \mathfrak{R}$ with rank $\prec v$ and whose Ritt-Kolchin remainder (resp. partial remainder) is zero, the Ritt-Kolchin reduction process shows that for some $s \in \mathbb{N}$, $H^s F \in (\mathbf{A}_{(v)})$ (resp. $S^s F \in (\mathbf{A}_{(v)})$) and hence $F \in (\mathbf{A}_{(v)}) : H^\infty$ (resp. $F \in (\mathbf{A}_{(v)}) : S^\infty$).
- From this, it also follows that **any characteristic set of a differential ideal is coherent**.

Relationship Between Coherence and Rosenfeld Property

Lemma 8.8

(**Rosenfeld**) *An autoreduced set* $\mathbf{A}$ *is subcoherent* (*resp. strongly subcoherent*) *if and only if it has the Rosenfeld property* (*resp. strong Rosenfeld property*)*.*

- When the subcoherence (resp. strong subcoherence) of an autoreduced set has been constructively verified, our proof later provides an algorithm to re-express any partially reduced element $F \in \mathfrak{a}_G$ as an element of J_G (where $G = H$ or $G = S$).
- Subcoherence is probably what Rosenfeld [35, p. 397] had in mind where he claimed wrongly, that coherence is equivalent to the Rosenfeld property.

Proof of Lemma 8.8: Sufficiency

- Suppose **A** is subcoherent (resp. strongly subcoherent) and let $G = H$ (resp. $G = S$).
- Let $\mathbf{A} : A_1 < \cdots < A_p$ with corresponding leaders $v_1 < \cdots < v_p$. Let $F \in \mathfrak{a}_G$ be partially reduced with respect to **A**. For some $s \in \mathbb{N}$, $G^s F \in [\mathbf{A}]$. Let

$$G^s F = \sum_{j, \theta_j \neq 1,} C_j \theta_j A_{k_j} + \sum_i B_i A_i. \qquad (8.9)$$

- If possible, let v be the highest leader among all $\theta_j v_{k_j}$, and separate the terms in the first sum into two sums: one sum involving those summands with $\theta_j v_{k_j}$ having leaders $< v$ and the other involving those having leaders v.

Proof of Sufficiency (Continued)

$$G^s F = \sum_{\substack{j,\theta_j \neq 1,\\ \theta_j v_{k_j} < v}} C_j \theta_j A_{k_j} + \sum_{\substack{\ell,\theta_\ell \neq 1,\\ \theta_\ell v_{k_\ell} = v}} D_\ell \theta_\ell A_{k_\ell} + \sum_i B_i A_i.$$

- In the middle sum, choose an index h. Multiply the above by S_{k_h} (the separant of A_{k_h}) and rewrite the equation as

$$\begin{aligned} S_{k_h} G^s F &= \sum_{\substack{j,\theta_j \neq 1,\\ \theta_j v_{k_j} < v}} C'_j \theta_j A_{k_j} + \sum_{\substack{\ell \neq h,\theta_\ell \neq 1,\\ \theta_\ell v_{k_\ell} = v}} D_\ell (S_{k_h} \theta_\ell A_{k_\ell} - S_{k_\ell} \theta_h A_{k_h}) \\ &+ D'_h \theta_h A_{k_h} + \sum_i B'_i A_i. \end{aligned} \tag{8.10}$$

Proof of Sufficiency Continued

- Now v, being a proper derivative of a leader v_{k_h}, does not appear in $S_{k_h} G^s F$ which is partially reduced w.r.t. **A**, and v does not appear in A_i (last sum), $\theta_j A_{k_j}$ (first sum).
- By the subcoherence (resp. strong subcoherence) of **A**,

$$\Delta(A_{k_h}, A_{k_\ell}, v) := S_{k_h}\theta_\ell A_{k_\ell} - S_{k_\ell}\theta_h A_{k_h} \in (\mathbf{A} \cup \mathbf{A}_{(v)}) : G^\infty,$$

  and does not involve v.
- After multiplying (8.10) by a suitable product of initials and separants (resp. separants), we may distribute the resulting second sum among the first and last sums, obtaining an equation

$$G^{s'} F \;=\; \sum_{\substack{j,\theta_j \neq 1,\\ \theta_j v_{k_j} < v}} C''_j \theta_j A_{k_j} + D''_h \theta_h A_{k_h} + \sum_i B''_i A_i. \quad (8.11)$$

Proof of Sufficiency Continued

- Using $\theta_h A_{k_h} = S_{k_h} v - T_{k_h}$, where $T_{k_h} \prec v$, and treating v as an algebraic indeterminate, we may substitute $v = T_{k_h}/S_{k_h}$ into (8.11).
- After clearing denominators, multiplying by possibly other initials and separants (resp. separants) of **A**, and regrouping, we obtain, for some s'',

$$G^{s''} F = \sum_{j, \theta'_j \neq 1,} C'''_j \theta'_j A_{k'_j} + \sum_i B'''_i A_i.$$

- This equation has the same form as (8.9), except that the highest derivative among $\theta'_j A_{k'_j}$ is $< v$.
- Repeating the argument till we obtain an equation like (8.9) where the first sum is absent, proving that $F \in J_G$.

Proof of Lemma 8.8: Necessity

- Suppose the Rosenfeld property (resp. strong Rosenfeld property) holds.
- Let $F = \Delta(A, A', v)$, where v is some common derivative of $u_A, u_{A'}$. Let $\widetilde{F}$ be the Ritt-Kolchin partial remainder of F.
- Then by Eq. (**??**), we have $S^e F \equiv \widetilde{F} \mod (\mathbf{A}_{(v)})$ for some suitable power of S.
- Thus $\widetilde{F} \in [\mathbf{A}]$ and by the Rosenfeld property (resp. strong Rosenfeld property), $\widetilde{F} \in J_G$ where $G = H$ (resp. $G = S$).
- Multiplying by initials and separants, we may replace S^e by $G^{e'}$ so that $G^{e'} F \in (\mathbf{A} \cup \mathbf{A}_{(v)})$ and this proves that $\mathbf{A}$ is subcoherent (resp. strongly subcoherent).

The Promised Example

Example 8.14

Let the ranking in $\mathfrak{R} := \mathfrak{F}\{z, y, t\}$ be unmixed such that $z < y < t$ and orderly in each of the differential indeterminates. Let $\mathbf{A} : A_1 \prec A_2 \prec A_3 \prec A_4$ where

$$A_1 = \boldsymbol{\delta_2^4 z} + \delta_2^2 z, \qquad A_2 = \boldsymbol{\delta_1 y} + z,$$
$$A_3 = \boldsymbol{\delta_2^2 y}, \qquad A_4 = \mathbf{t^2}.$$

- Then $\mathbf{A}$ is autoreduced and $S_4 = 2t$, $S_4^2 = 4A_4$. The only Δ-pair (A_2, A_3). Let $v = \delta_1\delta_2^2 y$ and let $\theta \in \Theta$. Let G be either H or S. Then $(\mathbf{A}) : G^\infty = (\mathbf{A} \cup \mathbf{A}_{(\theta v)}) : G^\infty = (1)$.
- So $\mathbf{A}$ is (strongly) subcoherent and has the (Strong) Rosenfeld Property.
- However, $\mathbf{A}$ is not coherent (*a fortiori* not strongly coherent) since $F := \Delta(A_2, A_3, v) = \delta_2^2 z \notin (\mathbf{A}_{(v)}) : H^\infty$.

Characterizing Characteristic Sets: Sufficiency

Theorem 8.15

Let $\mathbf{A}\colon A_1 \prec \cdots \prec A_p$ *be an autoreduced set of* $\mathfrak{R}$. *Let* V *be a finite subset of* ΘY *such that* $\mathbf{A} \subset \mathfrak{F}[V]$. *Suppose:*

(a). *The Ritt-Kolchin remainder of* $\Delta(A, A', v)$ *with respect to* $\mathbf{A}$ *is zero for every* Δ*-pair* $A, A' \in \mathbf{A}$.

(b). $\mathbf{A}$, *as a triangular set of polynomials in* $\mathfrak{F}[V]$ *with respect to its leaders* $v_1, \ldots, v_p$, *has invertible initials over* $\mathcal{S}_0 = \mathfrak{F}[V \backslash \{ v_1, \ldots, v_p \}]$.

(c). *The saturation ideal* $J_I^V := (\mathbf{A})\colon I^\infty$ *in* $\mathfrak{F}[V]$ *w.r.t. initials of* $\mathbf{A}$ *is radical and* $J_I^V = J_H^V$ *(resp. prime and does not contain any separants of* $\mathbf{A}$*).*

Then $J_H = J_I$, *and* $\mathbf{A}$ *is a characteristic set of the radical (resp. prime) differential ideal* $\mathfrak{a}_H$.

Characterizing Characteristic Set: Necessity

Theorem 8.15 (continued)
Conversely, if **A** *is a characteristic set of a radical (resp. prime) differential ideal* $\mathfrak{p}$ *and if* $J_H = J_I$, *then* $\mathfrak{p} : H = \mathfrak{a}_H$ (*resp.* $\mathfrak{p} = \mathfrak{a}_H$) *and* (a), (b), *and* (c) *hold.*

- The sufficiency part of Theorem 8.15 is very similar to Lemma 7.9. Since it is an open problem whether the (Strong) Rosenfeld Property is decidable, it is not easy to apply Lemma 7.9 to show **A** is a characteristic set of $\mathfrak{a}_H$.
- Theorem 8.15 (a) provides a verifiable criterion compared to the (Strong) Rosenfeld Property in Lemma 7.9(a). Moreover, the converse part of Theorem 8.15 shows the three conditions are necessary.

Proof of Theorem 8.15

Sufficiency

- Condition (a) implies that **A** is coherent, which implies that **A** is subcoherent, which implies that **A** has the Rosenfeld Property (Lemma 8.8). The sufficiency of the conditions and further conclusions then follow from Lemma 7.9.

Necessity

- Suppose **A** is a characteristic set of a prime differential ideal $\mathfrak{p}$. Then it is coherent and $\mathfrak{p} = \mathfrak{a}_H$ (resp. $\mathfrak{p} : H = \mathfrak{a}_H$) (Corollary 6.13) and $\mathfrak{p}$ is zero-reduced with respect to **A** (Lemma 5.3).
- In particular, the Ritt-Kolchin remainder of every $\Delta(A, A', v)$, which belongs to $\mathfrak{p}$, is therefore zero.

Proof of Theorem 8.15: Necessity (Continued)

- By Proposition 7.3, J_I (which is also J_H by hypothesis) is radical (resp. prime), and hence by 7.7, J_I^V is radical (resp. prime). Since the initials and separants of $\mathbf{A}$ are not in $\mathfrak{p}$, they are not in J_I^V.
- In fact, we may replace V by the subset V' consisting of all $\theta y_j \in V$ that appears in some $A \in \mathbf{A}$, and $J_I^{V'}$ is radical (resp. prime).
- Let $G \in J_I^{V'}$. Then G is partially reduced with respect to $\mathbf{A}$. The Ritt-Kolchin remainder of G with respect to $\mathbf{A}$ is simply the pseudo-remainder of G with respect to $\mathbf{A}$, and since $G \in \mathfrak{p}$, this remainder is zero by Corollary 6.13.
- By Corollary 3.20, $\mathbf{A}$ has invertible initials over $\mathcal{S}_0' = \mathfrak{F}[V' \backslash \{ v_1, \ldots, v_p \}]$ and hence also over $\mathcal{S}_0$. This completes the proof.

Necessary Conditions on CS of Prime and Radical

The three conditions on **A** in Theorem 8.15 are verifiable algorithmically. These conditions differ from and generalize the classical ones given by Lemma 2 on page 167 of Kolchin [24]. For comparison, we pose them here as exercises, and we add also the cases when ideals are radical.

Exercise 8.16

Suppose **A** is a characteristic set of a prime (resp. radical) differential ideal $\mathfrak{p}$. Prove that

(a). $\mathfrak{p} = \mathfrak{a}_H$ (resp. $\mathfrak{p} \colon H = \mathfrak{a}_H$),

(b). **A** is coherent,

(c). J_H is prime (resp. radical), and

(d). J_H is zero-reduced.

Exercise 8.17

Let **A** be an autoreduced set. Suppose

(a). **A** has the Rosenfeld property (resp. the strong Rosenfeld property),

(b). J_H (resp. J_S) is prime (or radical), and

(c). J_H (resp. J_S) is zero-reduced.

Prove that $\mathfrak{a}_H$ (resp. $\mathfrak{a}_S$) is a prime (or radical) differential ideal with **A** as a characteristic set; in particular, **A** is coherent.

Revisiting an Example

- Let $\mathfrak{R} = \mathfrak{F}\{ z, y \}$ be an ordinary differential polynomial ring under an orderly ranking such that $z < y$.
- Let $A_1 = \mathbf{y}^2 + z$, $A_2 = \mathbf{y}' + y$, $A_3 = \mathbf{z}' + 2z$. The set $\mathbf{A}\colon A_1, A_3$ is autoreduced, strongly coherent, and has invertible initials and invertible separants.
- Gröbner basis can verify that $J_I = J_S = J_H = (A_1, A_3)$, which is prime and contains no separant.
- By Theorem 8.15 (and also Exercise 7.12), $\mathbf{A}$ is a characteristic set of the prime differential ideal $\mathfrak{a}_H = \mathfrak{a}_S = [A_1, A_3]\colon (2y)^\infty$, which is $[A_1, A_2]$.
- However, $\mathfrak{a}_I = [A_1, A_3] \neq \mathfrak{a}_H$ since $A_2 \notin \mathfrak{a}_I$. In fact, $\mathfrak{a}_I$ is not even a radical differential ideal since $A_2 \in \sqrt{\mathfrak{a}_I}$ but $A_2 \notin \mathfrak{a}_I$.