A GENERALIZATION OF ROSENFELD'S LEMMA

Sally Morrison

October 22, 2005

0. Terminology and Notation. Throughout this talk, k is a differential field of characteristic zero under a set $\Delta = \{\delta_1, \ldots, \delta_m\}$ of commuting derivations, and $k\{y_1, \ldots, y_n\}$ is the differential polynomial ring in n differential indeterminates over k. We denote by Θ the set of derivative operators generated by Δ: that is, Θ is the free commutative monoid generated by $\delta_1, \ldots, \delta_m$, so that an element of Θ has form $\delta_1^{k_1}\delta_2^{k_2}\ldots\delta_m^{k_m}$. Put

$$\Theta Y = \{\theta y_i | \theta \in \Theta, 1 \leq i \leq n\}.$$

Then ΘY is algebraically independent over k, $k\{y_1, \ldots, y_n\}$ and $k[\Theta Y]$ are equal as algebras, and for each i $(1 \leq i \leq n)$ and each $\delta \in \Delta$, $\delta(\theta y_i) = (\delta\theta)y_i$.

We fix a differential ranking of ΘY; this means roughly that the set

$$\{u^k : u \in \Theta Y, k \in \mathbb{N}\}$$

has been well-ordered in a manner compatible with the derivation.

For each $f \in k\{y_1, \ldots, y_n\} \setminus k$, the *leader* of f, denoted u_f, is the highest ranked element of ΘY that appears in f, and d_f is the highest degree to which u_f appears in f. Thus we may write

$$f = I_f u_f^{d_f} + T_f,$$

where $deg_{u_f}(T_f) < d_f$ and where u_f does not appear in I_f. The polynomial I_f is called the *initial* of f, and the polynomial $S_f := \partial f / \partial u_f$ is called the *separant* of f. If θ is in $\Theta \setminus \{1\}$, then θf is linear in its leader $u_{\theta f}$, which is equal to θu_f ; and $I_{\theta f} = S_{\theta f} = S_f$, whence

$$\theta f = S_f \theta u_f + T_{\theta f},$$

where θu does not appear in S_f or in $T_{\theta f}$.

Given a subset P and a multiplicative subset M of $k\{y_1, \ldots, y_n\}$, we denote by $[P]$ and $\{P\}$ the differential ideal and the radical differential ideal, respectively, generated by P. The ideal $[P] : M^\infty$ is the contraction of the differential ideal generated by P in the localized ring $M^{-1}k\{y_1, \ldots, y_n\}$. That is,

$$[P] : M^\infty = \{g \in k\{y_1, \ldots, y_n\} \, : \, mg \in [P] \text{ for some } m \in M\}$$

1. Rosenfeld's Lemma.

Given a finite subset P of $k\{y_1, \ldots, y_n\}$, we are interested in ways of "computing" $\{P\}$ it in various senses. A crucial step in any such computation is to reduce the problem to a similar problem for a finitely generated ideal in a polynomial ring in finitely many variables. The vehicle for doing so in the partial differential case is a result known as Rosenfeld's Lemma.

<u>Rosenfeld's Lemma</u>. Let A be a coherent autoreduced subset of the differential polynomial ring $k\{y_1, \ldots, y_n\}$, and let $g \in [A] : H_A^\infty$. If g is partially reduced with respect to A, then $g \in (A) : H_A^\infty$.

The practical contribution of Rosenfeld's lemma to computational mathematics is suggested by the following equivalent statement: Let A be a coherent autoreduced subset. Let U be any subset of ΘY that contains the variables appearing A but no proper derivatives of the leaders of the elements of A. Then

$$[A] : H_A^\infty \cap k[U] = (A) : H_A^\infty.$$

<u>Comment</u>. The fact that A is *autoreduced* means that it is "differentially triangular and reduced" in the following sense: the leaders of the elements of A are all distinct, no proper derivative of a leader of an element of A appears in any other element of A, and, should the leader of an element of A appear somewhere in another element of A, it does so to a lower degree.

The fact that g is *partially reduced* with respect to A means that no proper derivative of an element of A appears in g.

Of course ΘA, which is the set we're really concerned with, need *not* be triangular– not, at least, in the partial case. We'll define *coherence* later. It will turn out to substitute for the lack of triangularity of $\Theta(A)$ □

Our generalization of Rosenfeld's Lemma will involve modifying each of the three hypotheses *autoreduced*, *partially reduced*, and *coherent*.

<u>Example</u>. Put a differential ranking on $k\{u, v, w\}$ in any way such that $u < \delta_1 w$ and $v < \delta_2 w$. Put

$$A = \{f_1 \, , \, f_2\} = \{ \, \delta_1 w - u \, , \, \delta_2 w - v \, \}.$$

Clearly A is autoreduced. Of course ΘA is not triangular. For example, the two differential polynomials

$$\delta_2 f_1 = \delta_1\delta_2 w - \delta_2 u$$
$$\delta_1 f_2 = \delta_1\delta_2 w - \delta_1 v$$

have the same leader. Furthermore, letting U be the set consisting of the derivatives of the variables of order less than 2, we see that the "integrability condition" $\delta_2 f_1 - \delta_1 f_2 = \delta_1 v - \delta_2 u$ is in $[A] : H_A^\infty \cap k[U]$ but it is *not* in $(A) : H_A^\infty$. This is NOT GOOD.

Interlude. What is an "integrability" or "compatibility" condition anyway ?

2. Generalization of partially reduced and autoreduced. Let P be a finite subset of $k\{y_1, \ldots, y_n\} \setminus k$.

Definition. g is semi-reduced with respect to P if no leader of an element of $\Theta P \setminus P$ appears in g.

Remark. In the case that P is (partially) autoreduced, "semi-reduced" is equivalent to "partially reduced", although in general it is a weaker condition.

Example. In $k\{y\}$, let $P = \{y, \delta y\}$, $g = \delta y$. Then g is semi-reduced but not partially reduced with respect to P.

Definition. A subset P of $k\{y_1, \ldots, y_n\}$ is Δ-complete if each element of P is semi-reduced with respect to P.

That is: if $f, g \in P$ and if θu_f appears in g, then θf is itself already in P.

Proposition. If P is Δ-complete, then every element of H_P is semi-reduced with respect to P.

Proof. Let $p \in P$. No leader of an element of $\Theta P \setminus P$ appears in p, so certainly such a leader cannot appear in I_p or S_p. □

3. Computing the Δ-completion.

Let $P \subset k\{y_1, \ldots, y_n\} \setminus k$, and let $F \subset \Theta P$. There is a smallest Δ-complete set $Comp^\Delta(F)$ such that

$$F \subset Comp^\Delta(F) \subset \Theta(F),$$

whence

$$[F] = [Comp^\Delta(F)] \text{ and } H_F = H_{Comp^\Delta(F)}.$$

$Comp^\Delta(F)$ and be computed by the following algorithm.

Input: A finite subset F of ΘP
Output: $C = Comp^{\Delta}(F)$
$A := F$
REPEAT
    $S := \Theta F \setminus A$
    $B := \emptyset$
    FOR each $a \in A$ and $s \in S$
        IF u_s appears in a THEN $B = B \cup \{s\}$
    $A := A \cup B$
UNTIL $B = \emptyset$. □

In short, if A is not Δ-complete, take any offending θa and replace A by $A \cup \{\theta a\}$.

It is easy to see $Comp^{\Delta}(F)$ exists and that the algorithm does the right thing, but we must show that it terminates.

Example. Let $k\{u, y, z\}$ be the ordinary differential polynomial with derivation δ, and put an elimination ranking on $k\{u, y, z\}$ so that for all i, j, k we have

$$\delta^i u < \delta^j y < \delta^k z.$$

Denoting derivatives by subscripts (e.g. $\delta^2 u = u_2$), let

$$F = P = \{u \, , \, y + u_3 \, , \, z + y + y_2 \, , \, z_1\}$$

Denote by A_i and B_i the values of A and B after the ith iteration. From the algorithm we obtain

$$\begin{aligned} B_1 &= \{u_3 \, , \, y_2 + u_5 \, , \, \boxed{z_1} + y_1 + y_3\} \\ B_2 &= \{u_5 \, , \, y_1 + u_4 \, , \, \boxed{y_3} + u_6\} \\ B_3 &= \{u_4 \, , \boxed{u_6}\} \\ B_4 &= \emptyset. \end{aligned}$$

Thus

$$Comp^{\Delta}(P) = P \cup B_1 \cup B_2 \cup B_3.$$

PROOF OF TERMINATION. Denote by A_i and B_i the values of A and B after the ith iteration. Then $A_0 = F$ and $B_0 = \emptyset$. For $i \geq 1$, we have

$$\begin{aligned} B_i &= \{s \in \Theta(F) \setminus A_{i-1} \; : \; u_s \text{ appears in } A_{i-1}\} \\ A_i &= A_{i-1} \cup B_i. \end{aligned}$$

Lemma. Let $i \geq 2$ and let $s \in B_i$. Then

(a) u_s does not appear in any element of A_{i-2}.

(b) u_s appears in some element of B_{i-1}.

(c) u_s is not the leader of any element of B_{i-1}.

Proof. Let $s \in \Theta(F) \setminus F$ and suppose that u_s appears in an element of A_{i-2}. Using in succession the definitions of B_{i-1}, A_{i-1} and B_i, we have:

$$\begin{aligned} u_s \text{ appears in an element of } A_{i-2} &\Rightarrow s \in A_{i-2} \cup B_{i-1} \\ &\Rightarrow s \in A_{i-1} \\ &\Rightarrow s \notin B_i. \end{aligned}$$

Thus (a) holds. (b) follows immediately, since, by definition of B_i, u_s appears in an element of $A_{i-1} = A_{i-2} \cup B_{i-1}$. Finally, (c) follows from (a) and the definition of B_{i-1}. □

Now let m_i be an element of B_i $(i \geq 2)$ of maximum rank. By parts (b) and (c) of the Lemma, u_{m_i} appears in an element b_{i-1} of B_{i-1}, and $u_{m_i} \neq u_{b_{i-1}}$, whence $u_{m_i} < u_{b_{i-1}} \leq u_{m_{i-1}}$.

Thus $(u_{m_i})_{i \geq 1}$ is a strictly decreasing sequence.. So $B_i = \emptyset$ for sufficiently large $i \in \mathbb{N}$, and the algorithm terminates. □

4. Coherence.

Let A be an autoreduced subset of $k\{y_1, \ldots, y_n\}$, and let H_A be the multiplicative subset generated by the initials and separants of the elements of A.

Rosenfeld defines coherence as follows:

Definition.

1. Let f, $f' \in A$. If u_f and $u_{f'}$ are derivatives of the same differential indeterminate, there is a smallest common derivative, $\boxed{u_{f,f'}}$ of u_f and $u_{f'}$. Let θf and $\theta' f'$ be the unique derivatives of f and f' such that $u_{f,f'} = u_{\theta f} = u_{\theta' f'}$. The $\boxed{S^\Delta\text{-polynomial}}$ of f and f' is

$$S^\Delta(f, f') = S_{f'} \theta f - S_f \theta' f'$$

2. The set A is $\boxed{\text{coherent}}$ if

$$S^\Delta(f, f') \in \Theta(A)_{(u_{f,f'})} : H_A^\infty$$

whenever f, $f' \in \Theta A$. □

Note that $u_{f,f'}$ always gets eliminated—that is, it doesn't appear in $S^{\Delta}(f,f')$, since

$$\begin{aligned} S^{\Delta}(f,f') &= S_{f'}(S_f u_{f,f'} + T_{\theta f}) - S_f(S'_f u_{f,f'} + T_{\theta' f'}) \\ &= S_{f'} T_{\Theta f} - S_f T_{\theta' f'} \end{aligned}$$

Thus, putting $U = \Theta(Y)_{(u_{f,f'})}$, we have

$$S^{\Delta}(f,f') \in [A] : H_A^{\infty} \cap k[U].$$

To say that A is coherent means that also $S^{\Delta}(f,f')$ is in the (in general smaller) ideal $(\Theta(A)_{(u_{f,f'})}) : H^{\infty}$ of $k[U]$.

Example. Put a differential ranking on $k\{u,v,w\}$ in any way such that $u < \delta_1 w$ and $v < \delta_2 w$. Put

$$A = \{f_1\,,\, f_2\} = \{\,\delta_1 w - u\,,\, \delta_2 w - v\,\}.$$

We have $S^{\Delta}(f,f') = \delta_2 f - \delta_1 f' = \delta_1 v - \delta_1 u \notin (A)_{(\delta_1 \delta_2 w)}$, so A is not coherent.

Rosenfeld's Lemma again. Let U be any subset of ΘY that contains the variables appearing A but no proper derivatives of the leaders of the elements of A. Then

$$[A] : H_A^{\infty} \cap k[U] = (A) : H_A^{\infty}.$$

Roughly speaking, Rosenfeld's Lemma says that all "integrability" conditions are generated by the finitely many S^{Δ}-polynomials.

5. Generalization of Coherence.

Let P be a finite subset of $k\{y_1,\ldots,y_n\}$, let M be a multiplicative subset of $k\{y_1,\ldots,y_n\}$, and assume that $H_P \subset M$

Definition. Let $A \subset \Theta P \setminus P$. The set A is $\boxed{\Delta\text{-coherent relative to } P \text{ and } M}$ if

$$S^{\Delta}(f,f') \in (\Theta P)_{(u_{f,f'})} : M^{\infty}$$

whenever $f,\ f' \in \boxed{\Theta A}$.

Proposition. In the above notation, A is Δ-coherent relative to P and M if and only if

$$S^{\Delta}(f,f') \in (\Theta P)_{(u_{f,f'})} : M^{\infty}$$

whenever $f,\ f' \in \boxed{A}$.

So determining whether A is relatively Δ-coherent requires only a finite number of computations. Given A, furthermore, there is an algorithm to compute a set $Coh_M(A)$ and a multiplicative set N containing M such that $A \subset Coh_M(A) \subset \Theta P \setminus P$ and $Coh_M(A)$ is coherent relative to P and N.

'Triangulation' Lemma. Let $A \subset \Theta(P) \setminus P$, and suppose that A is Δ-coherent relative to P and M. Let $g \in A$ and suppose that

$$g = \sum_{i=1}^{r} g_i \theta_i p_i,$$

where $\theta_i p_i \in A$ and $u_{\theta_i p_i} = v$ $(1 \leq i \leq r)$. Then $g \in (\theta_r p_r\,,\, \Theta(P)_{(v)}) : M^\infty$.

Proof. For each i $(1 \leq i \leq r)$ we have

$$S^\Delta(\theta_i p_i, \theta_r p_r) = S_r \theta_i p_i - S_i \theta_r p_r,$$

whence

$$\begin{aligned} S_r \theta_i p_i &= S^\Delta(\theta_i p_i, \theta_r p_r) + S_i \theta_r p_r \\ &\in (A_{(v)}\,,\, \theta p_r). \end{aligned}$$

Since $S_r \in M$,

$$g \in (\Theta(P)_{(v)}\,,\, \theta p_r) : M^\infty.$$

$\square$

6. Generalization of Rosenfeld's Lemma.

The Problem. Let $P \subset k\{y_1, \ldots, y_n\}$ and let M be a multiplicative set containing S_P. Suppose that $\Theta P \setminus P$ is Δ-coherent relative to P and M. I want to find another finite subset C of $k\{y_1, \ldots, y_n\}$ such that (i) $[C] = [P]$, (ii) $H_P = H_C$, (iii) $\Theta C \setminus C$ is Δ-coherent relative to C and M, and (iv) letting U be the set of variables of ΘY actually occurring in C, we have

$$[P] : M^\infty \cap k[U] = [C] : M^\infty \cap k[U] = (C) : M^\infty\,.$$

I claim that $C = Comp^\Delta(P)$ fills the bill.

Theorem. Let $P \subset k\{y_1, \ldots, y_n\}$ and let M be a multiplicative set containing S_P. Suppose that $\Theta P \setminus P$ is Δ-coherent relative to P and M and that each element of M is semi-reduced with respect to P. Let $g \in [P] : M^\infty$. Then:

(a) If g is semi-reduced with respect to $Comp^\Delta(P)$, then $g \in (Comp^\Delta(P)) : M^\infty$. Equivalently,

(b) If P is Δ-complete, and if $g \in [P] : M^\infty$ is semi-reduced with respect to P, then $g \in (P) : M^\infty$.

Remark. For our purpose, (a) suggests that Rosenfeld's "auto-reduced" hypothesis may actually be counterproductive. If you start out with a set P that is (partially) auto-reduced, you can un-partially reduce it until finally

$$[Comp^{\Delta}(P)] : M^{\infty} \cap k[U] = (Comp^{\Delta}(P)) : M^{\infty}$$

for appropriate U.

Proof.

Put $C = Comp^{\Delta}(P)$. Then $[C] = [P]$ and $S_C = S_P$. Also $\Theta C \setminus C$ is Δ-coherent with respect to C and M because

$$\Theta C \setminus C \subset \Theta P \setminus P \subset \Theta P$$

Thus we may as well assume in (a) that P is Δ-complete; that is, we need only prove (b).

There is a smallest element of ΘY, call it v, such that

$$g \in (P \cup \Theta(P)_{[v]}) : M^{\infty}.$$

Then for some $m \in M$, $p_i \in P$, and $g_i \in k\{y_1, \ldots, y_n\}$ $(1 \leq i \leq s)$, we have

$$mg = \sum_{i=1}^{r} g_i \theta_i p_i + \sum_{i=r+1}^{s} g_i \theta_i p_i,$$

where $v = u_{\theta_i p_i}$ $(1 \leq i \leq r)$ and $\theta_i p_i \in P \cup \Theta(P)_{(v)}$ $(r+1 \leq i \leq s)$. We may and do assume that $\theta_i p_i \in \Theta(P)_{(v)}$ $(r+1 \leq i \leq s)$. If v is small enough—for instance if v is the smallest leader of an element of P—then $\Theta(P)_{[v]} \subset P$, so $g \in (P) : M^{\infty}$ as desired.

Suppose for a contradiction that $\Theta(P)_{[v]} \not\subset P$. By minimality of v, some $\theta_i p_i$ $(1 \leq i \leq r)$ is not in P. It follows from the Δ-completeness of P that no $\theta_i p_i$ $(1 \leq i \leq r)$ is in P. So by the Triangulation Lemma, $g \in (\Theta(P)_{(v)}, \theta_r p_r) : M^{\infty}$. That is, we have an equation

$$m'g = g_r \theta_r p_r + \sum_{i'=1}^{s'} g'_j \theta'_j p'_j,$$

with each $\theta'_i p'_i \in P \cup \Theta(P)_{(v)}$. We may write $\theta p_r = S_r v + T$, where $T \in (\Theta(P)_{(v)})$. Under the substitution

$$v = \frac{-T}{S_r},$$

$\theta_r p_r$ vanishes and g_r and each g'_j is replaced by a quotient whose numerator is in $k\{y_1, \ldots, y_n\}$ and whose denominator is a power of S_r. Everything else is unaffected. So making this substitution and clearing denominators shows that

$$g \in (P \cup \Theta(P)_{(v)}) : M^\infty,$$

contradicting the minimality of v. We conclude that $\Theta(P)_{[v]} \subset P$, and therefore that $g \in (P) : M^\infty$. $\square$