COHERENCE AND PRIME DECOMPOSITION

Throughout, $k$ 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 $\Theta$ the set of derivative operators generated by $\Delta$: that is, $\Theta$ is the free commutative monoid generated by $\delta_1, \ldots, \delta_m$, so that an element of $\Theta$ 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 $\Theta Y$ 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 $\Theta Y$. This means that the set $\Theta Y$ has been well-ordered in a manner compatible with the derivation: that is, for $v, v_1, v_2 \in \Theta Y$ and $\delta \in \Delta$,

$$v < \delta v$$

and

$$v_1 < v_2 \Rightarrow \delta v_1 \ < \delta v_2$$

We extend to powers of the elements of $\Theta Y$ via

$$u^d < v^e \iff u < v \text{ or } u = v \text{ and } d < e.$$

For each $f \in k\{y_1, \ldots, y_n\} \setminus k$, the $\boxed{\textit{leader}}$ of $f$, denoted $u_f$, is the highest ranked element of $\Theta Y$ 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 $\boxed{\textit{initial}}$ of $f$, and the polynomial $S_f := \partial f/\partial u_f$ is called the $\boxed{\textit{separant}}$ of $f$. We extend our differential ranking to a pre-order on $k\{y_1, \ldots, y_n\}$ by decreeing the $\boxed{rank}$ of $f$ to be $u_f^{d_f}$. (An element of $k$ is understood to have lower rank than any element of $k\{y_1, \ldots, y_n\} \setminus k$). If $\theta$ is in $\Theta \setminus \{1\}$, then $\theta f$ is linear in its leader $u_{\theta f}$, which is equal to $\theta u_f$ ; and $I_{\theta f} = S_{\theta f} = S_f$, whence

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

where $\theta u$ does not appear in $S_f$ or in $T_{\theta f}$. (This is basically a restatement of the chain rule for differentiation. ...)

Given a subset $A$ of $k\{y_1, \ldots, y_n\}$, we denote by $(A)$, $[A]$ and $\{A\}$ the ideal, the $\boxed{\text{differential ideal}}$ and the $\boxed{\text{radical differential ideal}}$, respectively, generated by $A$.

We have

$$\{A\} = \sqrt{[A]}.$$

If $\mathfrak{a}$ is any radical differential ideal of $k\{y_1, \ldots, y_n\}$, then there is a *finite* set $A$ such that

$$\mathfrak{a} = \{A\},$$

and there are finitely many differential prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_k$, minimal over $\mathfrak{a}$ such that

$$\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \mathfrak{p}_k$$

These prime ideals are called the prime components of $\mathfrak{a}$.

Our aim is to shed some light on a solution to the following

**PROBLEM**

GIVEN: A finite subset $P$ of $k\{y_1, \ldots, y_n\}$.

FIND: A finite set of prime differential ideals whose intersection is $\{P\}$. ... $\square$

Put

$$\Theta(A) = \{\theta f | \theta \in \Theta,\ f \in A\},$$

and

$$A_{[v]} = \{f \in A : rank(f) \leq v\}$$
$$A_{(v)} = \{f \in A : rank(f) < v\}$$

If $A$ is finite, we denote by $H_A$ the product of the initials and separants of the elements of $A$. By $[A] : H_A^\infty$ we mean the ideal

$$[A] : H_A^\infty = \{g \in k\{y_1, \ldots, y_n\} : H_A^k g \in [A] \text{ for some } k \in \mathbb{N}\}.$$

Working with this ideal essentially allows division of elements of $A$ by initials and separants. ...

Now let $A \subset k\{y_1, \ldots, y_n\} \setminus k$ and $g \in k\{y_1, \ldots, y_n\} \setminus k$. We say that $g$ is partially reduced with respect to $A$ if no proper derivative of any leader of an element of $A$ appears in $g$. We say that $g$ is reduced with respect to $A$ if $g$ is partially reduced with respect to $A$ and if the leader of an element $a$ of $A$ either does not appear in $g$ at all, or does so only with degree less than $d_f$.

We say that $A$ is auto-reduced if every element of $A$ is reduced with respect to every other element of $A$.

Example 1. In the ordinary differential polynomial ring $k\{y, z\}$, ranked so that $y << z$ (meaning every derivative of $y$ is lower than any derivative of $z$), put $f = (y^{'''})^2 + y$. There are many ways to find a second differential polynomial $g$ such that $A = \{f, g\}$ is auto-reduced. ...

One choice would be $g = y^{'''} z' + z^5$. □

We see, therefore, that if $k\{y_1, \ldots, y_n\}$is an *ordinary* differential polynomial ring and $A$ is auto-reduced, then the leaders of the elements of $A$ are all derivatives of different $y_i$'s ; in particular, $A$ has at most $n$ elements and $\Theta A$ (not merely $A$) is "triangular" in the sense that its elements have distinct leaders.

The situation is more complicated in the partial case.

Example 2. If $\Delta = \{\delta_1, \delta_2\}$, the set

$$A = \{f_1, f_2\} = \{\,\delta_1 y - y\,,\, \delta_2 y\,\}$$

is an auto-reduced subset of $k\{y\}$ with respect to any ranking. ... But $\Theta(A)$ is not triangular. ... **S** □

Example 3. If $\delta_1\delta_2^6 y$ is the leader of one element of an autoreduced set $A$ of $k\{y\}$, what other leaders could elements of $A$ have?

It turns out that every auto-reduced set is finite even in the partial case.

It may be helpful to think of "auto-reduced" as the closest we can come to "reduced row-echelon form". ...

Given an auto-reduced set $A$ and an element $f \in k\{y_1, \ldots, y_n\}$ the ... remainder of $f$ is a ... differential polynomial $r$, reduced with respect to $A$, such that for some $h \in H_A$ we have

$$hf - r \in (\Theta(A)_{[u_f]}).$$

We find $r$ by pseudo-reduction (i.e by successive division by elements of $\Theta(A)$, each regarded as a polynomial of one variable). ... Note that if $f \in [A]$, so is $r$, and that if $r \in [A] : H_A^\infty$, so is $f$.

We can order the set of all auto-reduced sets. Under this ordering we have:

Proposition. Every non-empty set of auto-reduced sets has a smallest element.

Definition. Let $I$ be a differential ideal. A minimal auto-reduced subset of $I$ is called a characteristic set of $I$.

Theorem. Let $A$ be an auto-reduced subset of $I$. Then $A$ is a characteristic set of $I \iff$ every element of $I$ has remainder zero with respect to $A$. ...

Note that this supplies us with a *membership criterion* for $I$.

Proof. ... □

Definition. Let $A$ be an auto-reduced subset of $k\{y_1, \ldots, y_n\}$, and let $H_A$ be the product of the initials and separants of the elements of $A$. 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 $\theta f$ 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

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

□

In Example 2, namely,

$$A = \{f_1, f_2\} = \{\,\delta_1 y - y\,,\, \delta_2 y\,\},$$

we have $S^\Delta(f_1, f_2) = -\delta_2 y$

...

Remark. Observe that in our notation we have

$$\begin{aligned} S^\Delta(f, f') &= S_{f'}\theta f - S_f \theta' f' \\ &= S_{f'}(S_f u_{\theta f} + T_{\theta f}) - S_f(S_{f'} u_{\theta f'} + T_{\theta' f'}) \\ &= S_{f'}(S_f u_{f,f'} + T_{\theta f}) - S_f(S_{f'} u_{f,f'} + T_{\theta' f'}) \\ &= S_{f'} T_{\theta f} - S_f T_{\theta' f'} \\ &\in [A]_{(u_{f,f'})} = (\Theta A)_{(u_{f,f'})}. \end{aligned}$$

But in general,

$$S^\Delta(f, f') \notin (\,\Theta(A)_{(u_{f,f'})}\,).$$

Example 3. Assume $u << v << w$. Put

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

(Observe that finding a solution of $A = 0$ is a standard sophomore calculus problem. ...)

Clearly $A$ is auto-reduced. ... We get

$$\begin{aligned} S^\Delta(f_1, f_2) &= \delta_2 f_1 - \delta_1 f_2 \\ &= \delta_1 v - \delta_2 u \\ &\in (\Theta A)_{(u_{f_1,f_2})} \setminus (\Theta(A)_{(u_{f_1,f_2})}) \ldots \end{aligned}$$

Roughly speaking, this says that the $S^\Delta$-polynomial gives an "integrability condition". ... Note also in passing that $S^\Delta(f_1, f_2)$ is reduced with respect to $A$. So $A$ is not a characteristic set of $\{A\}$.

Example 4. Let $y >> z$, and let $A = \{f, g\}$ where

$$f = (\delta_1 y)^2 + \delta_1 y \qquad\qquad g = (\delta_2 y) z^2 + z$$

Then

$$\begin{aligned}\delta_2 f &= (2\delta_1 y + 1)\delta_1\delta_2 y = S_f u_{f,g} \\ \delta_1 g &= z^2 \delta_1\delta_2 y + (2(\delta_2 y)z + 1)\delta_2 z = S_g u_{f,g} + T_{\delta_1 g}.\end{aligned}$$

Thus

$$\begin{aligned}S^\Delta(f,g) &= S_g \delta_2 f - S_f \delta_1 g \\ &= -S_f T_{\delta_1 g} \\ &= -(2\delta_1 y + 1)(2(\delta_2 y)z + 1)\delta_2 z\end{aligned}$$

Once again, $S^\Delta(f,g)$ appears to be an element of $(\Theta A)_{(u_{f,g})} \setminus (\Theta(A)_{(u_{f,g})})$. This time, $S^\Delta(f,g)$ is not partially reduced with respect to $A$. □

Definition. The set $A$ is $\boxed{\Delta\text{-coherent}}$ if

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

whenever $f,\ f' \in \Theta A$.

Rosenfeld's Lemma. Let $A$ be a coherent auto-reduced 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 $g \in (A) : H_A^\infty$.

EQUIVALENTLY: Let $U$ be any subset of $\Theta Y$ that contains the variables appearing $A$ but no proper derivatives of the leaders of the elements of $A$. Then

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

Although it's not immediately obvious from either the lemma or Rosenfeld's proof of it, Rosenfeld's Lemma actually tells us that coherence permits us to express elements of $[A]$ in terms of a *triangular* subset of $\Theta(A)$.

Theorem. If $A$ is a characteristic set of a prime differential ideal $\mathfrak{p}$ of $k\{y_1, \ldots, y_n\}$, then $\mathfrak{p} = [A] : H_A^\infty$, $A$ is coherent, and $(A) : H_A^\infty$ is a prime ideal not containing a nonzero element reduced with respect to $A$.

Conversely, if $A$ is a coherent auto-reduced subset of $k\{y_1, \ldots, y_n\}$ such that $(A) : H_A^\infty$ is prime and does not contain a nonzero element reduced with respect to $A$, then $A$ is a characteristic set of a prime differential ideal of $k\{y_1, \ldots, y_n\}$. □

**PROBLEM**

GIVEN: A finite subset $P$ of $k\{y_1, \ldots, y_n\}$.
FIND: A finite set of prime differential ideals whose intersection is $\mathfrak{p}$.

Remarks.

1. Here "find" means "find a characteristic set of".
2. The set obtained must include every prime component of $\{P\}$, but in general also includes other differential prime ideals.
3. In order to eliminate the superfluous prime differential ideals, we would have to solve the famous *Ritt Problem* : Given characteristic sets of two differential prime ideals, determine whether one of the ideals is contained in the other. This problem is totally unsolved except for special cases.

SOLUTION "IN PRINCIPLE"

Given a finite set $P$ of differential polynomials, put

$$\mathbb{A}(P) = \text{ a minimal auto-reduced subset of } P \ldots$$

$\mathbb{A}(P)$ is not unique, but its rank is.

Lemma. Let $A$ be an auto-reduced set and let $f$ and $g$ be reduced with respect to $A$.

1. $\mathbb{A}(P \cup \{f\})$ is lower than $\mathbb{A}(P)$.
2. If $fg \in \{P\}$, then $\{P\} = \{P, f\} \cap \{P, g\}$.

□

The proof that the following procedure works is an induction on the rank of $\mathbb{A}(P)$.

A PROCEDURE (SORT OF)

Algorithms for computing the required characteristic sets require some combination of the following.

We begin with the finite set $P$.

Step 1. Find $\mathbb{A}(P)$. If you are extremely lucky, $A := \mathbb{A}\ (P)$ will be a coherent auto-reduced subset of $k\{y_1, \ldots, y_n\}$ such that $(A) : H_A^\infty$ is prime and does not contain a nonzero element reduced with respect to $A$. In this case, $[A] : H_A^\infty$ is a prime differential ideal containing $\{P\}$ and having characteristic set $\mathbb{A}(P)$, whence

$$\{P\} = [A] : H_A^\infty \cap (\cap_{a \in \mathbb{A}(P)} \{P, I_a\}) \cap (\cap_{a \in \mathbb{A}(P)} \{P, S_a\}).$$

Step 2. If not that lucky, maybe there is at least one $p \in P$ whose remainder $r$ with respect to $\mathbb{A}$ is not zero. In this case, replace $P$ by $P \cup \{r\}$, and, $\mathbb{A}\ (P)$ by $\mathbb{A}\ (P \cup \{r\})$. (We'll still call the resulting sets $P$ and $\mathbb{A}\ (P)$.) By the Lemma, the new $\mathbb{A}\ (P)$ has lower rank than the original. Do this for every such $f$, until every $p \in P$ has remainder 0 with respect to $\mathbb{A}\ (P)$. Again putting $A := \mathbb{A}\ (P)$, we now have $A \subset P \subset [A] : H_A^\infty$.

Step 3. If you're still unlucky, maybe there exist $f, g \in \mathbb{A}\ (P)$, whose $S^\Delta$-polynomial has non-zero remainder $d$ with respect to $\mathbb{A}\ (P)$. Proceed as in Step 2. The new $\mathbb{A}\ (P)$ is coherent.

Step 4. Finally, what if $(A) : H_A^\infty$ is not prime? Suppose $fg \in (A) : H_A^\infty$ but $f, g \notin (A) : H_A^\infty$. The same is true of the remainders of $f$ and $g$, so we may as well suppose that $f$ and $g$ are reduced with respect to $A$. Then by the Lemma we have $\{P\} = \{P, f\} \cap \{P, g\}$, once again lowering the characteristic sets.

The procedure terminates in the required decomposition.