Minimal Decomposition and Computation of Differential Bases for an Algebraic Differential Equation

Évelyne Hubert
LMC, Grenoble

September 21, 1996

[summary by Bruno Salvy]

Abstract

Singular and general solutions of algebraic differential equations can be expressed in a differential algebra setting regardless of the existence of closed-form. Theoretical and algorithmic tools in this area are presented.

1. Types of solutions

Consider the following differential equation:

\[ y'' - 4xy + 8y^2 = 0. \]  \hspace{1cm} (1)

This equation admits three solutions of different types:

\[ y(x) = a(x - a)^2, \quad y(x) = 0, \quad y(x) = \frac{4}{27}x^3. \]  \hspace{1cm} (2)

The first one is the general solution and the two other ones are singular solutions. The solution \( y(x) = 0 \) is actually a special case of the general solution and is called a particular singular solution; the third one is an essential singular solution. As showed by Figure 1, both singular solutions appear as envelopes of the general solution. In general, this is true of essential singular solutions of first order equations.

\[ \text{Figure 1. Solutions of (1)} \]
In the general case of an equation
\[ P(x, y, y', \ldots, y^{(n)}) = 0, \]
where \( P \) is a polynomial, the singular solutions are the simultaneous solutions of \( P \) and its sepa-
rant \( \partial P/\partial y^{(n)} \). Through differential algebra, a meaning can also be given to the “general” solution
even when no closed-form exists. It is also possible to distinguish algebraically between a particular
singular solution and an essential one. The aim of É. Hubert’s work is to provide algorithms dealing
with general and singular solutions in this framework.

To an ordinary differential equation like (1) is associated a differential polynomial
\[ p = y_1^3 - 4x y_0 y_1 + 8y_0^2 \in \mathbb{Q}(x)\{y\}. \]
More generally, the differential ring \( A = A\{y\} \) is a ring of polynomials in the variables \( y_0, y_1, y_2, \ldots \)
edowed with an operator \( \delta \) which is a derivation on the commutative integral domain \( A \) and
which is such that \( \delta y_i = y_{i+1} \). A differential ideal is an ideal stable under \( \delta \). For instance the
differential ideal generated by a differential polynomial \( p \) is the polynomial ideal generated by \( p \)
and its derivatives:
\[ [p] = (p, \delta p, \delta^2 p, \ldots). \]
Of particular interest is the radical of this ideal:
\[ \{p\} = \sqrt{[p]} = \{a \in A \mid \exists k \in \mathbb{N}, a^k \in [p]\}. \]
This is the set of differential polynomials vanishing on all the solutions of \( p \). A differential ideal \( I \)
is prime when \( ab \in I \Rightarrow a \in I \) or \( b \in I \).

We now restrict to \( A = \mathbb{Q}(x) \) for simplicity, but the results can be stated in much more generality,
see [4, 5]. An important property is that a radical differential ideal \( R \) can be decomposed into a
finite intersection of prime differential ideals:
\[ R = \bigcap_{k=1}^{r} P_k. \]
When none of the \( P_k \) is included in another one, this decomposition is called minimal and is unique.
These \( P_k \)'s are then called essential components of \( R \). In the same way as \( \{p\} \) corresponds to the
solutions of \( p \), each of the essential components of \( \{p\} \) corresponds to one type of solutions of \( p \). In
the same example as before, a decomposition is
\[ \{p\} = \{p, y_2^2 - 2x y_2 + 2y_1, y_3\} \cap \{y_0\} \cap \{27y_0 - 4x^3\}, \]
each term corresponding to one of (2). This decomposition is not minimal since the second ideal
obviously contains the first one and therefore corresponds to a particular singular solution. The
minimal decomposition is obtained by removing this second term. Testing the inclusion of the
general component (the first one here) into one of the other ones is related to Ritt’s problem; its
algorithmic resolution via the computation of a differential basis of each component is one of the
aims of [3].

While the singular solutions obviously correspond to components of the ideal \( \{p, s\} \), where \( s \) is
the separant of \( p \), the general solution corresponds to the quotient of \( \{p\} \) by \( s \), where the quotient of a radical differential ideal \( R \) by an element \( s \in A \) is defined as
\[ R : s = \{a \in A \mid sa \in R\}, \]
which is itself a radical differential ideal. Two properties are of interest: for any non-empty subset \( \sigma \)
of \( A \), one has \( \{\sigma\} : s \cap \{\sigma, s\} \); when \( p \) is irreducible as a polynomial in \( y_0, y_1, \ldots \) and \( s \) is its
separant, the ideal \( \{ p \} : s \) is prime. Thus \( G_p = \{ p \} : s \) is an essential component of \( \{ p \} \) which is called the general component of \( p \).

2. Algorithms for minimal decompositions

We now turn to the actual computation of the minimal decomposition

\[
\{ p \} = G_p \cap R_1 \cap \cdots \cap R_k.
\]

Ritt showed that each essential component \( R_i \) is the general component of some differential polynomial \( a_i \). The computation of a minimal decomposition then requires finding these \( a_i \)'s and insuring that the decomposition is minimal.

Ritt's low power theorem states that when an irreducible differential polynomial \( p \) of a differential ring \( A\{y_1, \ldots, y_n\} \) is contained in one of the ideals \( \{ y_i \} \), then \( \{ y_i \} \) is an essential component of \( \{ p \} \) if and only if the lowest degree terms of \( p \) do not contain a derivative of \( y_i \). This theorem can be used to give a criterion for \( G_a \) to be an essential component of \( \{ p \} \) after a preparation process which rewrites \( p \) as a differential polynomial in \( a \):

\[
s_a^k p = \sum_{\alpha_0, \ldots, \alpha_e} c_{\alpha} a_{\alpha_0}^{\alpha_0} \cdots a_{\alpha_e}^{\alpha_e},
\]

where \( s_a \) is the separant of \( a \), \( a_i = \delta^i a \), \( c_{\alpha_0, \ldots, \alpha_e} \notin G_a \) and \( e \) is the difference between the order \( n \) of \( p \) and the order \( m \) of \( a \). This reduction process is performed in three stages: for \( i \) from 1 to \( e \), \( a_i = \delta a_{i-1} \) can be rewritten \( a_i = s_a y_{m+i} + t_i \) for some \( t_i \). Then \( y_n \) is replaced by \( (a_e - t_e)/s_a \) in \( p \).

After normalization this yields

\[
s_a^k p = \sum c_{\alpha} a_{\alpha}^{\alpha},
\]

where the coefficients do not involve derivatives higher than \( y_{n-1} \). The process is then repeated with the \( y_{n-i} \) in succession. This rewrites all the \( y_{m+i} \) for \( i > 0 \). Then in each monomial \( c_a a_1^{a_1} \cdots a_e^{a_e} \), the coefficient \( c_a \) is rewritten \( c_{\alpha} a_0^{\alpha_0} \), where \( a_0 \) is the largest integer \( k \) such that \( a^k \) divides \( c_a \).

In our previous example, the reduction of \( p \) in terms of \( y_0 \) is tautologous; the lowest degree terms of \( p \) is \(-4x y_0 y_1 + 8 y_0^2 \) and thus \( \{ y_0 \} \) is not an essential component. The reduction of \( p \) in terms of \( a = 27 y_0 - 4x^3 \) is more interesting. The separant \( s_a = 27 \) is constant and the first step of the reduction process yields \( a_1 = 27 y_1 - 12 x^2 \). Then \( p \) is rewritten successively

\[
p = y_1^3 - 4 x y_0 y_1 + 8 y_0^2,
\]

\[
19683 p = a_1^3 + 36 x^2 a_1^2 - 108 x (27 y_0 - 4 x^3) a_1 + 216 (27 y_0 - 4 x^3)(27 y_0 - 4 x^3),
\]

\[
19683 p = a_1^3 + 36 x^2 a_1^2 - 108 x a_0 a_1 + 216 (27 y_0 - 2 x^3) a_0.
\]

The lowest degree term is \( 216 (27 y_0 - 2 x^3) a_0 \) which does not involve \( a_1 \) and thus \( \{ 27 y_0 - 4 x^3 \} \) is an essential component. (There also exists a simpler algorithm in this case since \( p \) is of order 1 [2]).

The computation of the \( a_i \)'s relies on the Rosenfeld-Gröbner algorithm [1] which has been implemented in Maple by F. Boulier. Given a system \( \Sigma \) of differential polynomials and a ranking, this algorithm computes a decomposition of the radical ideal \( \{ \Sigma \} \) as a finite intersection of radical differential ideals:

\[
\{ \Sigma \} = I_1 \cap \cdots \cap I_s,
\]

each \( I_i \) being described by a system of polynomial equations and inequations and a characteristic set. This decomposition makes it possible to test membership in the \( I_i \)'s and therefore in \( \{ \Sigma \} \) by simple reductions. Note that the \( I_i \)'s are not necessarily prime.
A lemma of Lazard's combined with Ritt's result mentioned above shows that the $I_i$'s corresponding to essential components of $\{p,s\}$ must have a characteristic set reduced to one differential polynomial. This makes it possible to filter out some of the radical ideals. Then prime differential ideals can be obtained by factorization. This leads to the following algorithm.

Output: $a_1, \ldots, a_r$ such that $G_p, G_{a_1}, \ldots, G_{a_r}$ are the essential components of $\{p\}$.

$G :=$ Rosenfeld-Gröbner($[p,s]$);
$A := []$;
for each $R$ in $G$ with cardinality 1 do
  for each factor $b$ of $R[1]$ do
    if low-powers(preparation($p,b)) = ch b_0$ then $A := A \cup [b]$;

Return $A$.

In our example, the output of Rosenfeld-Gröbner is

$$\{y_0\}, \quad \{27y_0 - 4x^3\},$$

from where the computations above have been performed.

It is possible to avoid the factorization and perform only gcd computations. In some cases, this algorithm can also be extended to compute a differential basis of $G_p$. This is helpful to compute power series solutions when the initial conditions lie on a singular solution. We refer to [3] for details.

References


