# Effective Identity Testing in Extensions of Differential Fields

*Ariane Péladan-Germa*
GAGE, École polytechnique (France)

November 21, 1994

[summary by Frédéric Chyzak]

**Abstract**

A. Péladan-Germa deals with extensions of differential rings by solutions of systems of PDE's. In the case of ODE's, the problem of equality testing in the extension ring has been solved [2, 3]. The author gives an algorithm for the more general case of PDE's [6]. It is based on the theory of differential algebra, and in particular on the concept of auto-reduced coherent sets [5, 8].

## 1. Outline of the algorithm

Let $R$ be the polynomial ring $k[x_1, \ldots, x_n]$ endowed with the usual partial derivatives $\partial_{x_i}$. The work described here gives an algorithm for effective equality testing in differential extensions of $R$ by series defined by algebraic partial differential equations. More precisely, let $f_i \in k[[x_1, \ldots, x_n]]$ be formal power series defined by equations of the form

$$Q_h\left(x_1, \ldots, x_n, \{\partial_\alpha f_i\}\right) = 0, \tag{1}$$

for polynomials $Q_h$ in finitely many derivatives $\partial_\alpha f_i$. Given these polynomials $Q_h$ and similar polynomials $P_h$, the problem is to decide whether the $f_i$'s satisfy the equations represented by the $P_h$'s, and in case they do not, to return one of the $P_h$'s that is not satisfied.

The viewpoint adopted here is to consider the formal power series $P_h\left(x_1, \ldots, x_n, \{\partial_\alpha f_i\}\right)$ as elements of the differential extension of $R$ by the $f_i$'s. However, she requires an assumption on these power series, namely that they are defined by a *complete system*. Informally, a complete system provides with sufficiently many equations and initial conditions so as to be able to compute *any* coefficient of *any* of the power series $f_i$ (see Theorem 2 below). The same also applies to all series $P_h\left(x_1, \ldots, x_n, \{\partial_\alpha f_i\}\right)$. The algorithm decides whether *all* coefficients are zero. Moreover, a complete system makes sure that the algorithm will work for any set of $P_h$'s, even for badly conditioned ones. Given the set $\mathcal{A}$ of all $P_h$'s and all $Q_h$'s, the algorithm is:

(1) Compute an *autoreduced coherent set* $\mathcal{B}$ associated to $\mathcal{A}$ and an additional polynomial $H$, the product of all *initials* and *separants* of the elements of $\mathcal{B}$. (These notions are defined below.) Informally, the set $\mathcal{B}$ defines the same series as $\mathcal{A}$, up to possible singularities described by $H$: the algorithm has to decide whether $H(f) = 0$.

(2) To this end:
- if $H(f)(0) \neq 0$ (*regular case*), then the $P_h(f)$ are all zero if and only if $\partial_\alpha B(f)(0) = 0$ for a computable finite set of derivatives and all $B \in \mathcal{B}$;
- otherwise, the algorithm is applied recursively to decide whether all $P_h(f)$'s and $H(f)$ are zero; then:

- if $H(f) \neq 0$ (*semi-regular case*), the problem reduces again to testing $\mathcal{B}(f) = 0$; $\mathcal{B}(f)$ continuously depends on the initial conditions defining $f$, and decision is done by computing a Groebner basis in an usual non-differential algebra to find the closure of an appropriate algebraic variety;
- if one of the $P_h$'s, say $P_k$, is not cancelled, return the answer $P_k(f) \neq 0$;
- otherwise (*singular case*), return the answer that all $P_h(f)$'s are zero.

Termination of this recursive algorithm is ensured by Theorem 1 below.

## 2. Differential algebra

A suitable theory to work with equations like (1) is the theory of *differential algebra* [5, 8]. Polynomials like the $P_h$'s and the $Q_h$'s are called *partial differential polynomials*, in short *pdp*'s, and form the *ring of partial differential polynomials* $\mathcal{R} = R[\{\partial_\alpha y_i\}]$. Note that this ring is a commutative ring in infinitely many indeterminates.

Differential algebra theory introduces *differential ideals*, i.e. ideals closed under all differentiations. Usual ideals are called *algebraic* ideals. For given polynomials $P_i$, the algebraic ideal of $\mathcal{R}$ is denoted $(P_1, \ldots, P_t)$, while the differential ideal is denoted $[P_1, \ldots, P_t]$. In fact, the differential ideal $[P_1, \ldots, P_t]$ is the algebraic ideal generated by all $\partial_\alpha P_i$'s.

The problem of working with (algebraic) ideals in usual non-differential algebras of polynomials is solved by Groebner bases computations. Similar tools have been developed in the differential case: first, a process of reduction has been introduced by Ritt [8]; second, the non-differential notion of reduced base has its counterpart as *auto-reduced sets*, i.e. sets, where each element is reduced by all others; third, syzygies (i.e. critical pairs) and corresponding S-polynomials are also defined in the differential case; last, the analogue of Groebner bases are *coherent sets*, i.e. sets that reduce all their S-polynomials to 0.

An *auto-reduced coherent set associated to* a set $\mathcal{L}$ of pdp's is an auto-reduced coherent set $\mathcal{M}$ such that $[\mathcal{M}] \subset [\mathcal{L}]$, and $\mathcal{M}$ reduces all pdp's in $\mathcal{L}$ to 0. Computationally, such an associated set is obtained by introducing the critical pairs one after the other, while keeping the set under construction auto-reduced. An algorithm by F. Boulier is given in [1, 2]. Classical noetherianity arguments used in the commutative case to prove termination of algorithms do not extend to the differential case. Instead, an order is defined on auto-reduced coherent sets, and the following theorem ensures the termination of Boulier's algorithm.

THEOREM 1. *There is no infinite decreasing sequence of auto-reduced sets.*

As already mentioned, the author's algorithm is crucially based on the potential cancellation of a certain polynomial $H$. The following definitions are needed to explain how this polynomial is introduced. They also play an important rôle in the definition of a complete system. Recall that Ritt's reduction relies on an order on the indeterminates $\partial_\alpha y_i$. The *leader* $v_P$ of a pdp $P$ is the highest indeterminate that occurs in it. This notion is the analogue of head terms in usual, non-differential Groebner bases theory. Now, the *initial* $I_P$ of $P$ is the coefficient in $v_P^{\deg P}$ and the *separant* $S_P$ of $P$ is the common initial of all derivatives of $P$. Finally, given a set $\mathcal{A}$ of pdp's, write $S_\mathcal{A}$ and $H_\mathcal{A}$ for the product of the separants of these pdp's and the product of the initials and separants of these pdp's respectively.

## 3. Differential extensions by formal power series

The author's crucial assumption is that the $f_i$'s are uniquely defined by systems of PDE's and finite sets of initial conditions at the origin.

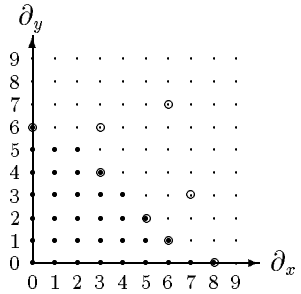


FIGURE 1. To be *under a stairs*

An indeterminate $\partial_\alpha y_i$ is *under the stairs* of a set $\mathcal{A}$ of pdp's if it is the derivative of the leader of no element of this set. An example in the case when $R = \mathbb{C}[x, y]$ and with a single function $f$ is graphically treated on Figure 1: assume the leaders of the elements of a set $\mathcal{A}$ to be $\partial_x^8 f$, $\partial_x^7\partial_y^3 f$, $\partial_x^6\partial_y f$, $\partial_x^6\partial_y^7 f$, $\partial_x^5\partial_y^2 f$, $\partial_x^3\partial_y^4 f$, $\partial_x^3\partial_y^6 f$, and $\partial_y^6 f$ (large framed circles on the figure). The indeterminates under the stairs of $\mathcal{A}$ are then $f, \ldots, \partial_x^8 f$, $\partial_y f, \ldots, \partial_x^6\partial_y f$, $\partial_y^2 f, \ldots, \partial_x^5\partial_y^2 f$, $\partial_y^3 f, \ldots, \partial_x^4\partial_y^3 f$, $\partial_y^4 f, \ldots, \partial_x^3\partial_y^4 f$, $\partial_y^5 f, \ldots, \partial_x^2\partial_y^5 f$, $\partial_y^6 f$ (smaller plain circles on the figure).

When the set of derivatives that are under the stairs of a set $\mathcal{A}$ of pdp's is finite, this set is called a *closed set*. The idea is that a closed set makes it possible, under some assumptions, to recursively compute the values at the origin of all derivatives, provided that the values at the origin of all derivatives under the stairs are given. A *complete system* consists of a closed auto-reduced coherent set $\mathcal{A}$ together with a finite set $IC$ of initial conditions (the values at the origin of the derivatives that are under the stairs), with the additional property that for all $A \in \mathcal{A}$, $A(f)(0) = 0$ but $S_A(f)(0) \neq 0$. These conditions make it possible to compute all values at the origin of all derivatives. This yields the following very old theorem [4, 7].

THEOREM 2. *For any given complete system $(\mathcal{A}, IC)$, there exists a single $m$-tuple of formal power series which are solutions of $\mathcal{A}$ and which satisfy the initial conditions $IC$. This tuple is computable, i.e. each coefficient of each $f_i$ is computable.*

More precisely, the coefficients of an $f_i$ are given by a recursive algorithm. Moreover, it is easily proved that each coefficient continuously depends on the initial condition $IC$, viewed as element of a finite dimensional vector space.

## 4. Justification for the algorithm

Henceforth, the formal power series $f_i$ are assumed to be defined by a fixed complete system $(\mathcal{A}, IC)$, and the ring $\mathcal{R}$ is assumed to be effective. The problem is to test whether $P_i(f) = 0$ for all $P_i$ in a given set $\{P_1, \ldots, P_t\}$ of pdp's in $\mathcal{R}\setminus R$. This is equivalent to testing whether $f$ is a solution of the system $\{\mathcal{A}, P_1, \ldots, P_r\}$. Boulier's algorithm, which was alluded to before, first reduces the problem to computing with auto-reduced coherent sets, as will be detailed below. Let $\mathcal{B}$ be an auto-reduced coherent set associated with $\{\mathcal{A}, P_1, \ldots, P_t\}$, i.e. a set that satisfies $[\mathcal{B}] \subset [\mathcal{A}, P_1, \ldots, P_t]$, and $Q \xrightarrow{\mathcal{B}} 0$ for all $Q \in \{\mathcal{A}, P_1, \ldots, P_t\}$.

Return into pseudo-reduction: given a set $\mathcal{Q}$ of pdp's, let $H_\mathcal{Q}$ be the product of the initials and separants of the elements of $\mathcal{Q}$ and $S_\mathcal{Q}$ the product of all separants only. Given an ideal $\mathfrak{I}$ which is not necessarily a differential ideal and a pdp $H$, let $\mathfrak{I} : H^\infty$ denote the set of all pdp's $P$ for which there exists a $\nu \in \mathbb{N}$ such that $H^\nu P \in \mathfrak{I}$. This set is actually an ideal and $P \xrightarrow{\mathcal{Q}} 0$ is equivalent to $P \in \mathcal{Q} : H_\mathcal{Q}^\infty$ [2, 5]. With this notation, it is clear that

$$[\mathcal{B}] \subset [\mathcal{A}, P_1, \ldots, P_t] \subset [\mathcal{B}] : H_\mathcal{B}^\infty . \tag{2}$$

Therefore if $H_{\mathcal{B}}(f) \neq 0$, then when $f$ vanishes at all the elements of $\mathcal{B}$ it vanishes at all the $P_i$'s, so that the problem reduces to testing whether $\mathcal{B}(f) = 0$. Otherwise $H_{\mathcal{B}}(f) = 0$ and the problem reduces to testing whether $f$ is a solution of the system $\{\mathcal{A}, P_1, \ldots, P_r, H_{\mathcal{B}}\}$. Provided that the test for $\mathcal{B}(f) = 0$ is effective, this yields a recursive algorithm that terminates because of Theorem 1. Two cases have to be considered, according to the value of $H_{\mathcal{B}}(f)(0)$.

*Regular case.* This corresponds to the case when $H_{\mathcal{B}}(f)(0) \neq 0$. For each $B \in \mathcal{B}$, $B(f)$ is a formal power series, which is zero if and only if $\partial_\alpha B(f)(0) = 0$ for all derivation $\partial_\alpha$ (including the identity). A rather technical theorem [6] reduces the problem to considering only finitely many members of this infinite set. Because of the non-nullity of $H_{\mathcal{B}}(f)(0)$, the values at the origin of all the $\partial_\alpha B(f)$'s are polynomials in the $\partial_\beta B(f)(0)$ for $\beta$'s such that $v_{\partial_\beta B}$ is under the stairs of $\mathcal{A}$, that is for a finite number of initial conditions. More precisely, $\mathcal{B}(f) = 0$ if and only if all these $\partial_\beta B(f)(0)$ equal 0. Since the zero-test in $\mathcal{R}$ is assumed to be effective, this solves the problem in the regular case.

*Semi-singular case.* This corresponds to the case when $H_{\mathcal{B}}(f)(0) = 0$ while $H_{\mathcal{B}}(f) \neq 0$. Once again, the initial problem on the $P_i$'s reduces to testing $\mathcal{B}(f) = 0$, but the algorithm developed in the regular case cannot be applied as is. An explicit formula for $f$ in terms of the initial conditions $IC$ shows that $f$ depends continuously on $IC$. The initial conditions $IC$ provide values of the $\partial_\alpha f_i$ for all $\alpha$ such that $\partial_\alpha y_i$ is under the stairs of $\mathcal{A}$. So $IC$ can be viewed as a vector $c$ of a finite dimensional space. Call $R'$ the ring of polynomials $k[x_1, \ldots, x_n, \partial_\alpha y_i]$ where the $\alpha$'s are such that $v_{\partial_\alpha y_i}$ is under the stairs of $\mathcal{A}$ and the $\partial_\alpha y_i$'s are viewed as indeterminates. Let now $W$ be the variety defined by the ideal $\mathfrak{I}$ of $R'$ generated by the $\partial_\alpha B$'s such that $\partial_\alpha B$ is under the stairs of $\mathcal{B}$, and $W'$ the variety defined by $H_{\mathcal{B}} = 0$. The regular case dealt with the implication $c \in W \setminus W' \Longrightarrow \mathcal{B}(f) = 0$. In the current case, the following theorem [6] reduces the problem to computing with algebraic varieties.

THEOREM 3. *Let $c$ be initial conditions such that the system $(\mathcal{A}, IC)$ is complete and $H_{\mathcal{B}}(f) \neq 0$. Then $\mathcal{B}(f) = 0 \Longleftrightarrow c \in \overline{W \setminus W'}$.*

This condition is tested by computing a Groebner bases for the radical of the ideal $\mathfrak{I} : H_{\mathcal{B}}^{\infty}$ using an algorithm described in [2], and testing if each polynomial of the constructed base vanishes at $c$.

The previous justification yields the algorithm that was outlined before.

## Bibliography


[1] Boulier (F.), Lazard (D.), Ollivier (F.), and Petitot (M.). – Representation for the radical of a finitely generated differential ideal. In *Proceedings ISSAC'95*. pp. 158–166. – Association for Computing Machinery, 1995.

[2] Boulier (François). – *Étude et implantation de quelques algorithmes en algèbre différentielle.* – Thèse, Université de Lille, April 1994.

[3] Denef (J.) and Lipshitz (L.). – Power series solutions of algebraic differential equations. *Mathematische Annalen*, vol. 267, 1984, pp. 213–238.

[4] Janet (M.). – Systèmes d'équations aux dérivées partielles. *Journal de Mathématiques*, vol. 8, n° 3, 1920.

[5] Kolchin (E. R.). – *Differential Algebraic Groups.* – Academic Press, New York, 1973.

[6] Péladan-Germa (Ariane). – Testing identities of series defined by algebraic partial differential equations. In *Actes de AAECC'11. Lecture Notes in Computer Science*, pp. 393–407. – Springer-Verlag, 1995. Proceedings AAECC'11, Paris, 1995.

[7] Riquier. – *Les systèmes d'équations aux dérivées partielles.* – Gauthier-Villars, Paris, 1910.

[8] Ritt (Joseph Fels). – *Differential Algebra.* – A.M.S., 1950, *A.M.S. Colloquium*, vol. XXXIII.