Computing highest-order divisors for a class of quasi-linear partial differential equations

Dima Grigoriev
CNRS, Mathématiques, Université de Lille
Villeneuve d'Ascq, 59655, France
Dmitry.Grigoryev@math.univ-lille1.fr
http://en.wikipedia.org/wiki/Dima_Grigoriev

Fritz Schwarz
Fraunhofer Gesellschaft, Institut SCAI
53754 Sankt Augustin, Germany
fritz.schwarz@scai.fraunhofer.de
www.scai.fraunhofer.de/schwarz.html

Abstract

A differential polynomial G is called a divisor of a differential polynomial F if any solution of the differential equation $G = 0$ is a solution of the equation $F = 0$. We design an algorithm which for a class of quasi-linear partial differential polynomials of order $k + 1$ finds its quasi-linear divisors of order k.

Keywords: quasi-linear differential polynomial, divisor, algorithm

Introduction

The problem of factoring linear ordinary differential operators $L = T \circ Q$ was studied in [15]. Algorithms for this problem were designed in [8], [16] (in [8] a complexity bound better than for the algorithm from [15] was established). An algorithm is exhibited in [10] for factoring a partial linear differential operator in two variables with a separable symbol. In [9], an algorithm is constructed for finding all first-order factors of a partial linear differential operator in two variables. A generalization of factoring for D-modules (in other words, for systems of linear partial differential operators) was considered in [11, 17]. A particular case of factoring for D-modules is the Laplace problem [6, 19] (one can find a short exposition of the Laplace problem in [12]).

The meaning of factoring for search of solutions is that any solution of operator Q is a solution of operator L, thus, factoring allows one to diminish the order of operators.

Much less is known for factoring non-linear (even ordinary) differential equations.

We note that our definition of divisors is in the frame of differential ideals [14], rather than the definition of factorization from [18, 4] being in terms of a composition of nonlinear ordinary differential polynomials. In [4], a decomposition algorithm is designed.

We consider partial differential polynomials viewing them as polynomials in independent variables $x_1, \dots, x_n$ and in derivatives

$$\frac{d^{i_1+\cdots+i_n}u}{dx_1^{i_1}\cdots dx_n^{i_n}}$$

[14]. We study a class of *quasi-linear* differential polynomials in which the coefficients at all its highest derivatives, i. e., with the biggest value of the order $i_1 + \cdots + i_n$, are constants.

We design an algorithm which for a given quasi-linear differential polynomial F of order $k+1$ finds the algebraic variety of all its quasi-linear divisors G of order k. Moreover, we show that in this case, $\deg G \le \deg F$ (treating F and G as algebraic polynomials). This result generalizes [13] where an algorithm was designed for finding quasi-linear divisors for quasi-linear *ordinary* differential polynomials F of order $k = 2$.

In Section 1, we bound the degree of a divisor, and in Section 2, we describe the algorithm.

It would be interesting to find divisors of F of arbitrary orders (rather than just of k) even in the case of ordinary differential equations. Also an extension to arbitrary differential polynomials (rather than quasi-linear) looks as a challenge.

Another issue to be studied is constructing a common multiple of a pair of partial differential polynomials, i. e., a differential polynomial whose solutions contain the solutions of both differential polynomials; for the case of quasi-linear ordinary differential polynomials, an algorithm was designed in [13].

1 Bound on a Degree of a Divisor

We study partial differential polynomials, i. e., polynomials of the form

$$F(\ldots, \frac{d^{i_1+\cdots+i_n}u}{dx_1^{i_1}\cdots dx_n^{i_n}}, \ldots, x_1, \ldots, x_n)$$

with coefficients over $\overline{\mathbb{Q}}$ where the maximal value of $i_1 + \cdots + i_n$ is denoted by $\operatorname{ord} F$ (the order of F) [14]. We denote the differential ring of all partial differential polynomials by D.

Definition 1.1 *A differential polynomial G is a divisor of F if any solution u from the universal extension (see, e. g., p. 133 [14]) of the field of rational functions $\overline{\mathbb{Q}}(x_1, \ldots, x_n)$ of equation $G = 0$ is a solution of $F = 0$ as well.*

Due to the differential Nullstellensatz (see, e. g., Corollary 1 p. 148 [14]) a differential polynomial G is a divisor of F iff F belongs to the radical differential ideal generated by G. We mention that a bound being in general not primitive-recursive, for the differential Nullstellensatz was established in [5].

We say that F of order $k+1$ is *quasi-linear* if

$$F = \sum_{i_1+\cdots+i_n=k+1} a_{i_1,\ldots,i_n} \cdot \frac{d^{k+1}u}{dx_1^{i_1}\cdots dx_n^{i_n}} + f$$

where coefficients $a_{i_1,\dots,i_n} \in \overline{\mathbb{Q}}$ and $\operatorname{ord} f \le k$.

In the present section we provide an algebraic criterion for a quasi-linear G of order k to be a divisor of F and bound the degree of G.

For the sake of simplifying notations we will assume that there are just two independent variables x, y, i. e., $n = 2$. Denote a quasi-linear differential polynomial

$$F = \sum_{0 \le i \le k+1} a_i \cdot \frac{d^{k+1}u}{dx^i dy^{k+1-i}} + f. \tag{1}$$

Let a quasi-linear differential polynomial

$$G = \sum_{0 \le i \le k} b_i \cdot \frac{d^k u}{dx^i dy^{k-i}} + g \tag{2}$$

be a divisor of F where $\operatorname{ord} g \le k-1$ and $b_0, \dots, b_k \in \overline{\mathbb{Q}}$. Making a $\overline{\mathbb{Q}}$-linear transformation of the independent variables x, y one can assume w.l.o.g. that $b_0 = 1$.

Theorem 1.2 *i) A quasi-linear differential polynomial G of order k is a divisor of a quasi-linear differential polynomial F of order $k+1$ (with $\deg F = d$) iff G divides (as polynomials)*

$$\left(F - c_1 \cdot \frac{dG}{dx} - c_2 \cdot \frac{dG}{dy}\right)^d$$

where

$$\operatorname{ord}\left(F - c_1 \cdot \frac{dG}{dx} - c_2 \cdot \frac{dG}{dy}\right) \le k$$

for suitable (unique) $c_1, c_2 \in \overline{\mathbb{Q}}$.

ii) In this case, $\deg G \le \deg F$.

Introduce the *highest order derivatives forms* being homogeneous polynomials

$$A := \sum_{0 \le i \le k+1} a_i \cdot v^i \cdot w^{k+1-i},\ B := \sum_{0 \le i \le k} b_i \cdot v^i \cdot w^{k-i} \in \overline{\mathbb{Q}}[v, w]$$

of the differential polynomials F and G, respectively.

Lemma 1.3 *If a quasi-linear differential polynomial G with $\operatorname{ord} G = k$ is a divisor of a quasi-linear differential polynomial F with $\operatorname{ord} F = k+1$ then there exist unique $c_1, c_2 \in \overline{\mathbb{Q}}$ such that $(c_1 \cdot v + c_2 \cdot w) \cdot B = A$, in other words $B|A$. Moreover, in this case $\operatorname{ord}(F - c_1 \cdot \frac{dG}{dx} - c_2 \cdot \frac{dG}{dy}) \le k$.*

Proof of Lemma. Due to the differential Nullstellensatz we have for suitable integer m

$$F^m = \sum_q H_q \cdot G_q \tag{3}$$

where G_q are certain partial derivatives of G and $H_q \in D$. Introduce variables $u_{i,j}$ for $\frac{d^{i+j}u}{dx^i dy^j}$ and making use repeatedly of relations $\frac{du_{i,j}}{dx} = u_{i+1,j}$, $\frac{du_{i,j}}{dy} = u_{i,j+1}$ we can consider (3) as an equality of polynomials in the variables $\{u_{i,j}\}_{i,j}$, x, y. Let a derivative of G of an order higher than 1 occur in (3) and denote by $s \geq 2$ the highest order of derivatives of G occurring in (3).

Taking appropriate $\overline{\mathbb{Q}}$-linear combinations of the equations

$$\frac{d^s G}{dx^i dy^{s-i}} = 0,\ 0 \leq i \leq s,$$

and considering their highest order derivatives one can express the variables

$$u_{j,s+k-j} = \sum_{s<l\leq s+k} c_l \cdot u_{l,s+k-l} + g_j,\ 0 \leq j \leq s \tag{4}$$

for suitable coefficients $c_l \in \overline{\mathbb{Q}}$ and differential polynomials g_j with $\operatorname{ord} g_j < s+k$. Substituting expressions (4) into (3) we get rid of all the derivatives G_q of G of order s. Observe that these substitutions do not change the left-hand side of (3). After that substitute 0 in all H_q for variables $u_{l.s+k-l}$, $s < l \leq s+k$ and for all variables $u_{i,j}$ with $i+j > s+k$, we obtain a formula similar to (3) with orders of derivatives G_q of G less than s and with variables $u_{i,j}$ occurring in G_q and H_q satisfying $i+j < s+k$.

Continuing in this way, we get rid of all the variables $u_{i,j}$ in the right-hand side of (3) with $i+j > k+1$.

After that we employ formulae (4) with $s=1$ to achieve that the differential polynomial $F_0 := F - c_1 \cdot \frac{dG}{dx} - c_2 \cdot \frac{dG}{dy}$ does not contain derivatives $u_{0,k+1}$, $u_{1,k}$ for suitable $c_1, c_2 \in \overline{\mathbb{Q}}$. Then (3) implies that

$$F_0^m = H^{(1)} \cdot \frac{dG}{dx} + H^{(2)} \cdot \frac{dG}{dy} + H^{(0)} \cdot G \tag{5}$$

for some differential polynomials $H^{(1)}$, $H^{(2)}$, $H^{(0)}$ of orders at most $k+1$. Now substitute formulae (4) with $s=1$ in formula (5), this results in

$$F_0^m = H \cdot G \tag{6}$$

for appropriate $H \in D$. Therefore, since F_0 contains derivatives of order $k+1$ with constant coefficients, all these coefficients vanish, thus, $\operatorname{ord} F_0 \leq k$, hence $\operatorname{ord} H \leq k$. Consequently,

$$F_0 = f - c_1 \cdot \frac{dg}{dx} - c_2 \cdot \frac{dg}{dy} \tag{7}$$

(see (1), (2)) and $(c_1 \cdot v + c_2 \cdot w) \cdot B = A$. The Lemma is proved. $\square$

Proof of Theorem. Substitute formulae

$$\frac{dg}{dx} = \sum_{i+j\leq k-1} \frac{\partial g}{\partial u_{i,j}} \cdot u_{i+1,j} + \frac{\partial g}{\partial x}; \quad \frac{dg}{dy} = \sum_{i+j\leq k-1} \frac{\partial g}{\partial u_{i,j}} \cdot u_{i,j+1} + \frac{\partial g}{\partial y} \tag{8}$$

in (7), and we substitute the obtained expression for F_0 in the left-hand side of (6), then we substitute in the resulting formula the expression for $u_{0,k} = -\sum_{1\leq i\leq k} b_i \cdot u_{i,k-i} - g$ from (2). After the latter substitution, the right-hand side of (6) vanishes, and we deduce (taking into account (2)) the equality

$$0 = f|_{(u_{0,k}=-\sum_{1\leq i\leq k} b_i\cdot u_{i,k-i}-g)} - c_1 \cdot (\sum_{i+j\leq k-1} \frac{\partial g}{\partial u_{i,j}} \cdot u_{i+1,j} + \frac{\partial g}{\partial x})+ \tag{9}$$

$$c_2 \cdot (\frac{\partial g}{\partial u_{0,k-1}}(\sum_{1\leq i\leq k} b_i u_{i,k-i} + g) - \sum_{i+j\leq k-1,\,(i,j)\neq(0,k-1)} \frac{\partial g}{\partial u_{i,j}} u_{i,j+1} - \frac{\partial g}{\partial y}) \tag{10}$$

One can rewrite

$$f|_{(u_{0,k}=-\sum_{1\leq i\leq k} b_i\cdot u_{i,k-i}-g)} = f|_{(u_{0,k}=-\sum_{1\leq i\leq k} b_i\cdot u_{i,k-i})} + h\cdot g$$

for suitable $h \in D$. Therefore, (9) and (10) imply the following divisibility relation

$$g|(f|_{(u_{0,k}=-\sum_{1\leq i\leq k} b_i\cdot u_{i,k-i})} - c_1 \cdot (\sum_{i+j\leq k-1} \frac{\partial g}{\partial u_{i,j}} \cdot u_{i+1,j} + \frac{\partial g}{\partial x})+ \tag{11}$$

$$c_2 \cdot (\frac{\partial g}{\partial u_{0,k-1}} \cdot \sum_{1\leq i\leq k} b_i \cdot u_{i,k-i} - \sum_{i+j\leq k-1,\,(i,j)\neq(0,k-1)} \frac{\partial g}{\partial u_{i,j}} \cdot u_{i,j+1} - \frac{\partial g}{\partial y})) \tag{12}$$

Denote the polynomial in the variables $\{u_{i,j}\}_{i,j}$, x, y in the right-hand side of (11), (12) by P.

Our goal is to prove that $\deg g \leq \deg f$. Suppose the contrary. Then (11), (12) entail that $\deg P \leq \deg g$ (taking into account that $\deg f \leq \deg g$ by the supposition) and whence $P = c\cdot g$ for appropriate $c \in \overline{\mathbb{Q}}$. Consider a linear deglex ordering $\prec$ of monomials in $\{u_{i,j}\}_{i+j\leq k-1}$, x, y in which $u_{i,j} \prec u_{l,s}$ when $i+j > l+s$ (the remaining requirements on the ordering do not matter). We observe that the highest (w.r.t. $\prec$) monomial in g cannot occur in P since $\deg f < \deg g$ by the supposition. This leads to a contradiction with the equality $P = c\cdot g$ which proves inequality $\deg g \leq \deg f$. Summarizing, we conclude Theorem 1.2 ii).

To prove Theorem 1.2 i) in the direction when G is a divisor of F we apply Lemma 1.3 and note that one can take $m = d$ in (6) owing to Theorem 1.2 ii) because if $G|F_0^m$ for some m then $G|F_0^{\deg G}$. To prove the converse we observe that $G|(F_0 - c_1 \cdot \frac{dg}{dx} - c_2 \cdot \frac{dg}{dy})^d$ implies (3) (with $m = d$). $\square$

We present the following simple example just to illustrate the notations.

Example 1 *Here we use the notations* $u_x = \frac{\partial u}{\partial x}$ *and so on.*

$$G = u_x + u_y + g(x,y);$$

$$F = u_{xx} + 5u_{xy} + 6u_{yy} + \frac{\partial g}{\partial x} + 3\frac{\partial g}{\partial y} + H(x,y,u,u_x,u_y)\cdot(u_x+2u_y+g);$$

$c_1 = 1,\ c_2 = 3,\ A = v^2 + 5vw + 6w^2,\ B = v + 2w;$

$$F_0 = F - u_{xx} - 2u_{xy} - \frac{\partial g}{\partial x} - 3(u_{xy} + 2u_{yy} + \frac{\partial g}{\partial y}) = H \cdot G.$$

2 Algorithm to Find the Algebraic Variety of All the Divisors

Now we proceed to an algorithm which for a quasi-linear $F \in D$ with $\operatorname{ord} F = k+1$, $\deg F = d$ yields the algebraic variety of all its divisors of order k (let $k \geq 1$). Making a $\overline{\mathbb{Q}}$-linear transformation of independent variables x, y one can assume w.l.o.g. that the coefficient $a_0 = 1$ (see (1)), this is compatible with the assumption $b_0 = 1$ due to Lemma 1.3.

First the algorithm factorizes the highest order derivatives form $A = \sum_{0\leq i\leq k+1} a_i \cdot v^i \cdot w^{k+1-i} \in \overline{\mathbb{Q}}[v,w]$ (see Lemma 1.3), say with the help of [2], [7]. Pick one of its at most of $k+1$ factors with degree k as a candidate for the highest order derivatives form $B = \sum_{0\leq i\leq k} b_i \cdot v^i \cdot w^{k-i} \in \overline{\mathbb{Q}}[v,w]$ of a divisor G of F. One can assume w.l.o.g. that $b_0 = 1$ (if $b_0 = 0$ we discard this candidate). Hence $(c_1 \cdot v + c_2 \cdot w) \cdot B = A$ for some $c_1, c_2 \in \overline{\mathbb{Q}}$ (actually, $c_2 = 1$ since $a_0 = b_0 = 1$).

Due to Theorem 1.2 ii) $\deg G \leq \deg F$, and we write a candidate for G as a polynomial with indeterminate coefficients over $\overline{\mathbb{Q}}$. In view of Theorem 1.2 i) one has to verify whether G divides $(F - c_1 \cdot \frac{dG}{dx} - c_2 \cdot \frac{dG}{dy})^d$ employing (8) (cf. also (9), (10), (11), and (12)). For this goal we introduce H (see (6)) with indeterminate coefficients over $\overline{\mathbb{Q}}$ and verify the condition

$$\left(F - c_1 \cdot \frac{dG}{dx} - c_2 \cdot \frac{dG}{dy}\right)^d = H \cdot G \qquad (13)$$

as a system of polynomial equations invoking the quantifier elimination algorithm from [3] (eliminating the indeterminate coefficients of H). The latter algorithm finds the irreducible components of the algebraic variety of all divisors G.

To estimate the complexity of the designed algorithm one has to specify how does the algorithm represent the coefficients of F from $\overline{\mathbb{Q}}$. A customary way to this end is to represent them as elements from an appropriate finite extension of $\mathbb{Q}$ (see e. g. [1, 2, 7, 3]). Denote by L a bound on the bit-size of such a representation (say, in a particular case of rational numbers p/q its bit-size is defined as $\lceil \log_2(p+1)(q+1) \rceil$).

Denote

$$N_0 := \binom{k+n}{n} + n,\ N := \binom{N_0 + d^2}{d^2}.$$

The complexity of the designed algorithm is majorated by the complexity of solving (13) which leads to the quantifier elimination for a system of polynomials in at most of N indeterminates being the coefficients at the monomials of degrees d for polynomial G and of degrees d^2-d for polynomial H in N_0 variables $\{u_{i_1,\dots,i_n} : i_1+\cdots+i_n \leq k\} \cup \{x_1, \dots, x_n\}$. The degrees of these polynomials do not exceed d, and their number is bounded by N. The bit-sizes of the coefficients of these polynomials are less than $L + O(\log N)$. The complexity of the quantifier elimination algorithm [3] applied to this system does not exceed a polynomial in L, d^{N^2}. Summarizing and utilizing the notations introduced above, we conclude with

Theorem 2.1 *There is an algorithm which for a given quasi-linear differential polynomial of an order $k+1$ produces the irreducible components of the algebraic variety of all its quasi-linear divisors of order k. The complexity of the algorithm can be bounded by a polynomial in L, d^{N^2}.*

Acknowledgements. The first author is grateful to the Max-Planck Institut für Mathematik, Bonn for its hospitality during writing this paper and to Labex CEMPI (ANR-11-LABX-0007-01). The authors appreciate the valuable remarks of the anonymous referees which encouraged an improvement of the exposition.

References

[1] Basu, S., Pollack, R., Roy, M.-F., Algorithms in real algebraic geometry, Springer, Berlin (2006).

[2] Chistov, A., An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time, J.Soviet Math. 34, 1838–1882 (1986).

[3] Chistov, A., Grigoriev, D., Complexity of quantifier elimination in the theory of algebraically closed fields, LNCS **176**, pp. 17–31 (1984).

[4] Gao, X. S., Zhang, M., Decomposition of ordinary differential polynomials, Appl. Alg. Eng. Commun. Comput. 19, 1–25 (2008).

[5] Golubitsky, O., Kondratieva, M., Ovchinnikov, A., Szanto, A., A bound for orders in differential Nullstellensatz, J. Algebra 322, 3852–3877 (2009).

[6] Goursat, E., Leçons sur L'intégration des Équations aux Dérivées Partielles. Vol. II, A. Hermann, Paris (1898).

[7] Grigoriev, D., Polynomial factoring over a finite field and solving systems of algebraic equations, J. Soviet Math. 34, 1762–1803 (1986).

[8] Grigoriev, D., Complexity of factoring and GCD calculating of ordinary linear differential operators, J. Symp. Comput. 10, 7–37 (1990).

[9] Grigoriev, D., Analogue of Newton-Puiseux series for non-holonomic D-modules and factoring, Moscow Math. J. 9, 775–800 (2009).

[10] Grigoriev, D., Schwarz, F., Factoring and solving linear partial differential equations, Computing **73** (2004), 179–197.

[11] Grigoriev, D., Schwarz, F., Loewy and primary decompositions of D-modules, Adv. Appl. Math. 38, 526–541 (2007).

[12] Grigoriev, D., Schwarz, F., Non-holonomic ideal in the plane and absolute factoring. In: Proc. Intern. Symp. Symbol. Algebr. Comput., ACM, Munich, pp. 93–97 (2010).

[13] Grigoriev, D., Schwarz, F., Computing divisors and common multiples of quasi-linear ordinary differential equations, LNCS 8136, pp. 140–147 (2013).

[14] Kolchin, E., Differential Algebra and Algebraic Groups, Academic Press, New York, London (1973).

[15] Schlesinger, L., Handbuch der Theorie der linearen Differentialgleichungen II, Teubner, Leipzig (1897).

[16] Schwarz, F., A factorization algorithm for linear ordinary differential equations. In: Proc. ACM Intern. Symp. Symbol. Algebr. Comput., Portland, pp. 17–25 (1989).

[17] Schwarz, F., Loewy Decomposition of Linear Differential Equations, Springer, Vienna (2012).

[18] Tsarev, S., On factorization of nonlinear ordinary differential equations. In: Proc. ACM Symp. Symbol. Algebr. Comput., Vancouver, pp. 159–164 (1999).

[19] Tsarev, S., Generalized Laplace transformations and integration of hyperbolic systems of linear partial differential equations. In: Proc. Intern. Symp. Symbol. Algebr. Comput., ACM, Peking, pp. 325–331 (2005).