J. Symbolic Computation (1990) **10**, 7–37

Complexity of Factoring and Calculating the GCD of Linear Ordinary Differential Operators

D. YU. GRIGOR'EV

Leningrad Department of Mathematics,
V. A. Steklov Institute of the Academy of Sciences of the USSR,
Fontanka 27, Leningrad, 191011, U.S.S.R.

(*Received 17 December 1987*)

Let

$$L = \sum_{0 \le k \le n} (f_k/f) \frac{d^k}{d^k x}$$

be a linear differential operator with rational coefficients, where $f_k, f \in \bar{\mathbb{Q}}[X]$ and $\bar{\mathbb{Q}}$ is the field of algebraic numbers. Let

$$\deg_X(L) = \max_{0 \le k \le n} \{\deg_X(f_k), \deg_X(f)\}$$

and let N be an upper bound on $\deg_X(L_j)$ for all possible factorizations of the form $L = L_1 L_2 L_3$, where the operators L_j are of the same kind as L and L_2, L_3, are normalized to have leading coefficient 1. An algorithm is described that factors L within time $(N\mathscr{L})^{O(n^4)}$ where $\mathscr{L}$ is the bit size of L. Moreover, a bound $N \le \exp((\mathscr{L}2^n)^{2^n})$ is obtained. We also exhibit a polynomial time algorithm for calculating the greatest common (right) divisor of a family of operators.

1. Introduction

Let

$$L = \sum_{0 \le k \le n} (f_k/f) D^k \in F(X)[D]$$

be a linear differential operator with rational coefficients, where $D = d/dX$ is the differential operator, the field $F = \mathbb{Q}[\eta]$ is finite over the field $\mathbb{Q}$ of rational numbers, $\varphi(Z) \in \mathbb{Q}[Z]$ is the minimal polynomial over $\mathbb{Q}$ of the element η, i.e. $F = \mathbb{Q}[Z]/(\varphi)$, and the polynomials $0 \ne f, f_k \in F[X]$. For integers p, q the bit-size of the rational number p/q equals $l(p/q) = \log_2(|pq| + 1) + 1$. If we write

$$f = \sum_{j,m} f^{(j,m)} \eta^j X^m,$$

where $f^{(j,m)} \in \mathbb{Q}$, then the sizes of the coefficients of f and L are defined as

$$l(f) = \max l(f^{(j,m)}) \quad \text{and} \quad l(L) = \max_{0 \le k \le n} \{l(f_k), l(f)\}.$$

We denote the degree

$$\deg(L) = \deg_X(L) = \max_{0 \le k \le n} \{\deg(f_k), \deg(f)\}.$$

0747-7171/90/070007+31 $03.00/0

If $f_n \neq 0$, we call $n = ord(L)$ the order of L and $lc(L) = f_n/f$ its leading coefficient. In the sequel the following bounds are assumed to be satisfied:

$$\deg(\varphi) < d_1;\ \deg(L) < d;\ l(\varphi), l(L) \leq M. \tag{1}$$

The bit-size of the operator L will not exceed $M(n+2)dd_1$ (cf., for example, Chistov & Grigor'ev, 1982, 1983, 1984; Grigor'ev, 1986, 1988).

We introduce the notation $g_1 \leq g_2 \mathscr{P}(g_3, \ldots, g_k)$ for positive functions $g_1 > 0, \ldots, g_k > 0$ if, for a suitable polynomial P, an inequality $g_1 \leq g_2 P(g_3, \ldots, g_k)$ holds.

An operator L can be factored $L = L_1 \ldots L_S$ where each operator L_j is irreducible in the ring $\mathbb{C}(X)[D]$. Recall that a factorization is not unique in general, unlike the case of the usual polynomials, nevertheless, an (unordered) set $\{ord(L_1), \ldots, ord(L_S)\}$ is defined uniquely (see Cohn, 1971). In Chistov & Grigor'ev (1982) (see also Chistov & Grigor'ev, 1983, 1984; Grigor'ev & Chistov, 1984; Grigor'ev, 1986, 1987; Kaltofen, 1982*a*, *b*, 1985) a polynomial-time algorithm for factoring multivariable polynomials, in particular, over algebraic number fields is designed (see also Proposition 1.4, below) involving an algorithm for factoring univariate polynomials over rational numbers from Lenstra *et al.* (1982). The main result of the present paper consists in describing an algorithm for factoring linear operators and in its complexity analysis (see Theorems 1.1 and 1.2, below). A sketch of the proof of Theorems 1.1 and 1.2 can be found in Grigor'ev (1989).

Suppose that for any factorization $L = Q_1 Q_2 Q_3$ into a product of three operators $Q_1, Q_2, Q_3 \in \mathbb{C}(X)[D]$, with $lc(Q_2) = lc(Q_3) = 1$ for definiteness, the bound $\deg(Q_2) \leq N$ is valid for an appropriate integer N.

THEOREM 1.1. *One can design a factoring algorithm yielding for each linear ordinary differential operator L a certain factorization $L = L_1 \ldots L_S$, every L_j being irreducible in the ring $\mathbb{C}(X)[D]$, and a field $F_1 = \mathbb{Q}[\eta_1] \simeq Q[Z]/(\varphi_1) \supset F$, where $\varphi_1 \in \mathbb{Q}[Z]$ is a minimal polynomial of the element η_1, such that $L_1, \ldots, L_S \in F_1(X)[D]$. In addition, the following bounds are true:*

$$\deg(\varphi_1) \leq d_1 \mathscr{P}((N\,dn)^{n^3});\quad l(\varphi_1), l(L_j) \leq M \mathscr{P}((N\,dn)^{n^3} d_1^{\log(n)}).$$

The algorithm runs within time $\mathscr{P}(M, (N\,dn)^{n^4}, d_1^{n^2})$.

THEOREM 1.2.

$$N \leq \exp(M(dd_1 2^n)^{o(2^n)}).$$

Thus, one can estimate the running time of the factorization algorithm by a value of the same order as in Theorem 1.2.

Let us note that in spite of the common nature of their subjects, the proofs of Theorems 1.1 and 1.2 proceed independently and are based on essentially diverse observations.

A factoring algorithm is described in Schlesinger (1897) (see also Singer, 1981), which reduced (provided that a certain bound on N is obtained) factoring an operator directly to solving a system of polynomial equations whose indeterminates are the coefficients of operators L_j, and so even involving the algorithm for the latter problem with the best known complexity bound (see Chistov & Grigor'ev, 1983, 1984; Grigor'ev & Chistov, 1984; Grigor'ev, 1986, 1988; and Proposition 1.5, below) gives a considerably worse (exponential in N) bound than in Theorem 1.1). If one would follow the methods of Schlesinger (1987, p. 169), Singer (1981) (also Wasow, 1976) for estimating N, then an essentially worse bound (in particular, double exponential in d) than in Theorem 1.2 would

be achieved. Let us formulate a conjecture that it is possible to replace a term $(dd_1 2^n)^{o(2^n)}$ in Theorem 1.2 by $dd_1 2^n$, after that the bound on N would be close to a sharp one.

We describe briefly the contents of the paper. In section 2 an algorithm is designed and its complexity bound is obtained for producing an exponential part $\int P$ of a fundamental formal solution (see, e.g. Olver, 1974; Wasow, 1976; Della Dora *et al.*, 1982)

$$v(X) = \exp(\int P)(X-b)^{\rho}(\Xi_0 + \Xi_1 \ln(X-b) + \ldots + \Xi_m \ln^m(X-b)) \tag{2}$$

of the equation $Lv = 0$ in a neighbourhood of a singular point $X = b$ of the operator L, i.e. $f_n(b) = 0$, where

$$\int P = \sum_{i \le -1} p_i (X-b)^{i/\nu}$$

is a polynomial in $(X-b)^{-1/\nu}$ for a suitable natural number $\nu \ge 1$, the coefficients $p_i \in \mathbb{C}$, the exponent $\rho \in \mathbb{C}$, the series

$$\Xi_k = \sum_{j \ge 0} \xi_{k,j} (X-b)^{j/\nu}, \quad 0 \le k \le m$$

and $\xi_{0,0} \neq 0$. Applying the method from Wasow (1976) yields a worse bound on the size of coefficients p_i than the bound obtained in section 2 (see Lemma 2.5). For producing P in section 2 a differential analogy of the Newton polygon (see, e.g. Della Dora *et al.*, 1982) is involved (see Lemmas 2.2, 2.3). An equation $\mathscr{R}(Y) = 0$ is considered where $\mathscr{R}$ is the Riccatti operator of L (see, e.g. Singer, 1981), satisfying the property that $\mathscr{R}(Dv/v) = 0$ for any solution v of the equation $Lv = 0$. If one would estimate the size of the coefficients p_i following their process based on Newton polygons (see, e.g. Della Dora *et al.*, 1982), then in general the bounds would be worse than the required ones in Lemma 2.5. In this way one can get the required bounds only in the case of a non-peculiar solution Y (see Lemma 2.4). After that the case of an arbitrary solution is reduced (see Lemma 2.3) to the non-peculiar case by introducing derivative Riccatti operators (see Lemma 2.1).

In section 3, we start by assuming that $L = L_0(D-g)$ has a first order divisor with $g \in \mathbb{C}(X)$. Using the bounds established in section 2 and constructions from Schlesinger (1987, p. 167) and Singer (1981), we estimate (see Lemma 3.1) $\deg(g)$ and the sum of the absolute values of the residues of g at all complex points. After that, we are able to modify some constructions of Schlesinger (1897, p. 125) and analyse their complexity to complete the proof of Theorem 1.2.

In section 4, Theorem 1.1 is proved using the algorithm for solving a system of polynomial equations (see Proposition 1.5, below) and the algorithm for solving a system of linear (algebraic) equations with parametric coefficients (see Heintz, 1983 and also Chistov & Grigor'ev, 1984; Grigor'ev, 1986). The reduction of factoring to solving a parametric system of linear equations is contained in Lemma 4.2. We remark that just as in section 2 the algorithmic part is known and is based on the Newton–Puiseux expansion method, only the bounds on the size of the coefficients and on the complexity being new, whereas in section 4 also the factorization algorithm is new.

In section 5 an algorithm for calculating the greatest common (right) divisor $G = GCRD(Q_1, \ldots, Q_s)$ of a family of linear ordinary differential operators $Q_1, \ldots, Q_s \in F(X)[D]$ is exhibited, i.e. for any v the equality $Gv = 0$ is equivalent to the system $Q_1 v = \ldots = Q_s v = 0$. An explicit representation of the *GCRD* and an *a priori* estimate for the size of the coefficients (see Lemma 5.1) plays an important role in this algorithm. The bounds supplied by Theorem 1.2 on the size of the coefficients of a divisor give us a considerably worse complexity bound for the algorithm calculating the *GCRD* than the one calculated

in Theorem 1.3 below (this is one more difference between the case of the differential operators and the case of the usual polynomials). Let each operator Q_i, $1 \le i \le s$ satisfy the bounds (1).

THEOREM 1.3. *One can calculate* $G = GCRD(Q_1, \ldots, Q_s)$ *within time* $\mathscr{P}(M, d, d_1, n, s)$. *Moreover, the following bounds hold:*

$$\deg(G) < dns; \quad l(G) \le (M + \log(d))\mathscr{P}(d_1, n, s).$$

Similarly, one can calculate the greatest common left divisor. Later on we need the algorithms from Chistov & Grigorev (1982, 1983) for polynomial factorization and for solving systems of polynomial equations. We now give exact formulations of these results in a simplified form sufficient for our purposes. Any polynomial $f \in F[X_1, \ldots, X_n]$ can be uniquely represented in a form

$$f = \sum_{0 \le i \le \deg_Z(\varphi); i_1, \ldots, i_n} (a_{i, i_1, \ldots, i_n}/b)\eta^i X_1^{i_1} \ldots X_n^{i_n},$$

where $a_{i, i_1, \ldots, i_n}, b \in \mathbb{Z}$ and $b > 0$ is the least possible. Let

$$\deg_{X_m}(f) < r; \quad \deg_Z(\varphi) < d_1; \quad l(f), l(\varphi) \le M$$

for all $1 \le m \le n$. As a measure of the size $\mathscr{L}_1(f)$ of the polynomial f we consider in Proposition 1.4 a value $r^n d_1 M$ and analogously $\mathscr{L}_1(\varphi) = d_1 M$.

PROPOSITION 1.4 (Chistov & Grigor'ev, 1982, 1983, 1984; Grigor'ev & Chistov, 1984; Grigor'ev, 1986, 1987; Kaltofen, 1985). *One can factor a polynomial* f *over* F *within time polynomial in the sizes* $\mathscr{L}_1(f), \mathscr{L}_1(\varphi)$. *Furthermore, for any divisor* $f_1 | f$ *where a polynomial* $f_1 \in F[X_1, \ldots, X_n]$ *has a certain coefficient equal to* 1, *the following bound is true:* $l(f_1) \le (M + n)\mathscr{P}(r, d_1)$.

COROLLARY. *Let the univariate polynomials* $h_1, \ldots, h_K \in F[X]$ *and* $\xi_1, \ldots, \xi_K$ *be some of their respective roots, i.e.* $h_i(\xi_i) = 0$, $1 \le i \le K$. *Consider the field* $F_1 = F(\xi_1, \ldots, \xi_K)$. *Then* $F_1 = \mathbb{Q}[\eta_0]$ *for a primitive element*

$$\eta_0 = \eta + \sum_{1 \le i \le K} \lambda_i \xi_i,$$

where $0 \le \lambda_i \le [F_1 : \mathbb{Q}]$ *are appropriate integers* ($[F_1 : \mathbb{Q}]$ *denotes the degree of the field extension*), *and let* $g \in \mathbb{Q}[Z]$ *be a monic minimal polynomial of* η_0. *One can produce all possible* g (*for different roots of* $h_1, \ldots, h_k$) *and the expressions*

$$\eta(\eta_0) = \sum_{0 \le j < \deg(g)} \eta^{(j)} \eta_0^j, \qquad \xi_i(\eta_0) = \sum_{0 \le j < \deg(g)} \xi_i^{(j)} \eta_0^j \in \mathbb{Q}[\eta_0],$$

where $\eta^{(j)}, \xi_i^{(j)} \in \mathbb{Q}$, *within time*

$$\mathscr{P}\left(M, \prod_{1 \le i \le K} \deg(h_i), d_1\right).$$

Moreover,

$$l(g), l(\eta^{(j)}), l(\xi_i^{(j)}) \le M\mathscr{P}\left(\prod_{1 \le i \le K} \deg(h_i), d_1\right).$$

Now we proceed to the problem of solving systems of algebraic equations. Let an input system $f_1 = \ldots = f_k = 0$ be given, where the polynomials $f_1, \ldots, f_k \in F[X_1, \ldots, X_n]$. Let

$$\deg_{X_1,\ldots,X_n}(f_i) < d, \quad \deg_z(\varphi) < d_1, \quad l(f_i) \leq M$$

for all $1 \leq i \leq k$. As a size $\mathscr{L}_2$ of the system in Proposition 1.5, we consider a value $(kd^n + 1)d_1 M$.

A variety $\mathscr{W} \subset \bar{F}^n$ of all roots (defined over the algebraic closure $\bar{F} = \bar{\mathbb{Q}}$ of the field F) of the system $f_1 = \ldots = f_k = 0$ is uniquely decomposable into a union of its components $\mathscr{W} = \cup_\alpha W_\alpha$, each defined and irreducible over the field F (see, e.g. Shafarevich, 1974). The algorithm from Proposition 1.5 finds the components W_α and outputs every W_α in two following manners: by its general point (see below) and by certain system of algebraic equations such that W_α coincides with a variety of all roots of this system.

Let $W \subset \bar{F}^n$ be a closed variety of dimension $\dim(W) = n - m$ defined and irreducible over F. Denote by $T_1, \ldots, T_{n-m}$ some algebraically independent elements over F. A general point of the variety W can be given by the following field isomorphism for the field $F(W)$ of rational functions on W:

$$F(T_1, \ldots, T_{n-m})[\theta] \simeq F(X_1, \ldots, X_n) = F(W) \qquad (*)$$

where the element θ is algebraic over the field $F(T_1, \ldots, T_{n-m})$. Let $\Phi(Z) \in F(T_1, \ldots, T_{n-m})[Z]$ be its minimal polynomial over $F(T_1, \ldots, T_{n-m})$ with the leading coefficient $lc_Z(\Phi) = 1$. The elements $X_1, \ldots, X_n$ are considered here as rational (co-ordinate) functions on the variety W. Under the isomorphism (*), we have $T_i \to X_{j_i}$ for suitable $1 \leq j_1 < \ldots < j_{n-m} \leq n$, where $1 \leq i \leq n-m$. Furthermore, θ is an image under isomorphism (*) of an appropriate linear function $\sum_{1 \leq i \leq n} c_i X_i$, where c_i are integers. The algorithm from Proposition 1.5 represents the isomorphism (*) by the integers $c_1, \ldots, c_n$ and also the images of co-ordinate functions $X_1, \ldots, X_n$ in the field $F(T_1, \ldots, T_{n-m})[\theta]$. Sometimes in the formulation of Proposition 1.5, we identify a rational function with its image under the isomorphism when this does not lead to misunderstanding.

PROPOSITION 1.5 (Chistov & Grigor'ev, 1983, 1984; Grigor'ev & Chistov, 1984; Grigor'ev, 1986). *An algorithm can be designed which produces a general point of every component W_α and constructs a certain family of polynomials $\Psi_\alpha^{(1)}, \ldots, \Psi_\alpha^{(\bar{N})} \in F[X_1, \ldots, X_n]$ such that W_α coincides with the variety of all roots of a system $\Psi_\alpha^{(1)} = \ldots = \Psi_\alpha^{(\bar{N})} = 0$. Denote $n - m = \dim(W_\alpha)$, $\theta_\alpha = \theta$, $\Phi_\alpha = \Phi$ (see (*)). Then $\deg_Z(\Phi_\alpha) \leq \deg(W_\alpha) \leq d$, for all j, s the degrees*

$$\deg_{T_1,\ldots,T_{n-m}}(\Phi_\alpha), \deg_{T_1,\ldots,T_{n-m}}(X_j) \leq \mathscr{P}(d^m, d_1) \quad \text{and} \quad \deg_{X_1,\ldots,X_n}(\Psi_\alpha^{(s)}) \leq d^{2m}$$

The number of equations $\bar{N} \leq m^2 d^{4m}$. Furthermore,

$$l(\Phi_\alpha), l(X_j) \leq (M+n)\mathscr{P}(d^m, d_1) \quad \text{and} \quad l(\Psi_\alpha^{(s)}) \leq M\mathscr{P}(d^n, d_1).$$

Finally, the total running time of the algorithm can be bounded by $\mathscr{P}(M, (d^n d_1)^n, k)$. Obviously, the latter value does not exceed $\mathscr{P}(\mathscr{L}_2^{\log(\mathscr{L}_2)})$, in other words, is subexponential in the size.

2. Calculating and Estimating Coefficients of the Exponential Part of a Fundamental Solution of a Linear Ordinary Differential Operator

Recall (see, e.g. Wasow, 1976) that there exist exactly n fundamental solutions of the form (2) of the equation $Lv=0$. Moreover, for each $0 \le m_0 \le m$, the expression

$$v_{m_0} = \exp(\int P)(X-b)^{\rho}\left(\sum_{1 \le i \le m_0} \binom{m-m_0+i}{m-m_0} \Xi_{m-m_0+i} \ln^i(X-b)\right)$$

is also a fundamental solution of the equation $Lv_{m_0}=0$. In particular, for $m_0=0$ the logarithmic derivative $Dv_0/v_0 = P+\rho(X-b)^{-1}+\bar{\Xi}$, where the series

$$\bar{\Xi} = \sum_{j \ge -s+1} \xi_j (X-b)^{j/s}$$

does not contain logarithmic terms. Let $P=P_1+P_2$, where every power of $(X-b)$ occurring in P_1 is less than every power of $(X-b)$ occurring in P_2, then we call P_1 a prefix of the solution (2). If there are exactly m_1 fundamental solutions with a prefix P_1, then we say that P_1 has a multiplicity m_1. Observe that $1 \le \nu \le n$ since the expression obtained from (2) by replacing $(X-b)^{1/\nu}$ by $\omega(X-b)^{1/\nu}$ in the series $P, \Xi_0, \ldots, \Xi_m$, where $\omega^\nu = 1$, is also a fundamental solution of the equation $Lv=0$. Recall (see, e.g. Olver, 1974) that the series (2) does not converge in general, but yet it converges asymptotically in the sense of Poincare. In what follows, we assume, for simplicity of notation, that the singular point $b=\infty$. In this case, X^{-1} plays the role of $(X-b)$ in formula (2).

Introduce a variable Y and the (non-linear) differential polynomials $\tau_0=1$, $\tau_1=Y$, $\ldots, \tau_{i+1}=Y\tau_i+D\tau_i, \ldots$, i.e. the usual polynomials in the derivatives $Y, DY, D^2Y, \ldots$. Define the Riccatti operator

$$\mathscr{R}(Y) = \mathscr{R}_L(Y) = \sum_{0 \le k \le n} f_k \tau_k$$

of the operator L. It is well known (see, e.g. Schlesinger, 1897; Singer, 1981) that $\mathscr{R}(Dv/v)=0$ iff $Lv=0$. For a fundamental solution v (see (2)) we also call Dv/v fundamental solution of the equation $\mathscr{R}(Y)=0$. For $0 \le k \le n$ the image

$$\mathscr{R}^{(k)}(\mathscr{R}(Y)) = k! \sum_{0 \le i \le n-k} \binom{i+k}{k} f_{i+k}\tau_i$$

of the Riccatti operator under the action of a linear mapping $\mathscr{R}^{(k)}$ on the linear space generated by the differential polynomials $\tau_0, \tau_1, \ldots$ over the field $F(X)$, will be called the kth derivative of the operator $\mathscr{R}$ (or kth derivative Riccatti operator of L). Taking into account that L is fixed we adopt an abbreviation $\mathscr{R}^{(k)}(Y) = \mathscr{R}^{(k)}(\mathscr{R}(Y))$. Evidently, $\mathscr{R}^{(0)}(Y) = \mathscr{R}(Y)$. The following analogy of the Taylor formula is valid:

LEMMA 2.1.

(a) $\mathscr{R}(Y+y) = \sum_{0 \le i \le n} \frac{1}{i!} \tau_i \mathscr{R}^{(i)}(y)$; *and* (b) $\mathscr{R}^{(m)}\mathscr{R}^{(k)} = \mathscr{R}^{(m+k)}$.

PROOF. We proceed by induction on j for the operators $L=D^j$. Assume that

$$\mathscr{R}_{D^j}(Y+y) = \tau_j(Y+y) = \sum_{0 \le i \le j} \binom{j}{i} \tau_i(Y)\tau_{j-i}(y).$$

Then

$$\begin{aligned}\mathscr{R}_{D^{j+1}}(Y+y) &= \tau_{j+1}(Y+y) = (Y+y)\tau_j(Y+y) + D\tau_j(Y+y)\\ &= (Y+y)\sum_{0\le i\le j}\binom{j}{i}(D\tau_i(Y))\tau_{j-i}(y) + \sum_{0\le i\le j}\binom{j}{i}\tau_i(Y)(D\tau_{j-i}(y))\\ &= \sum_{0\le i\le j}\binom{j}{i}\tau_{i+1}(Y)\tau_{j-i}(y) + \sum_{0\le i\le j}\binom{j}{i}\tau_i(Y)\tau_{j-i+1}(y)\\ &= \sum_{0\le i\le j}\binom{j+1}{i}\tau_i(Y)\tau_{j-i+1}(y).\end{aligned}$$

That proves the statement of (a) for $L = D^{j+1}$. One can complete the proof of (a) by linearity.

(b) $$\mathscr{R}^{(m)}\mathscr{R}^{(k)}(Y) = k!\,m!\sum_{0\le i\le n-k-m}\binom{i+k+m}{k}\binom{i+m}{m}f_{i+k+m}\tau_i$$

$$= (k+m)!\binom{i+k+m}{k+m}f_{i+k+m}\tau_i = \mathscr{R}^{(k+m)}(Y).$$

Lemma 2.1 is proved.

Further, we shall produce a prefix P of a fundamental solution $Y = P + \rho X^{-1} + \Xi$ of the equation $\mathscr{R}(Y) = 0$, where

$$P = \sum_{0\le i<(\delta_0+1)\nu}\gamma_i X^{\delta_0 - i/\nu}$$

with $\delta_0\nu$ an integer and $\gamma_0 \neq 0$, by means of a process similar to Newton–Puiseux expansions (for its algebraic version and the complexity bounds, see Chistov, 1986), starting with the largest powers of the variable X. This process is explained in a form suitable for our purposes in Della Dora *et al.* (1982); however, for estimating the complexity of producing P and the size of γ_i, we need some additional properties, see Lemmas 2.2, 2.3, below (these are also of independent interest). Since we only deal with fundamental solutions of $\mathscr{R}(Y)$ in what follows, we shall omit the term "fundamental". Thus, assume that $P = y + \gamma X^{\delta} + \ldots$ and a prefix y of P has already been produced, γX^{δ} is the next term, in particular $\delta > -1$. Then γ, δ satisfy the requirement (see, e.g. Della Dora *et al.*, 1982) that in the expression $\mathscr{R}(y+\gamma X^{\delta})$ the leading coefficient relative to the variable X (being a polynomial in the indeterminates γ, δ) has to vanish for γ, δ under consideration. By virtue of Lemma 2.1(a)

$$\mathscr{R}(y+\gamma X^{\delta}) = \sum_{0\le k\le n}\frac{1}{k!}\tau_k(\gamma X^{\delta})\mathscr{R}^{(k)}(y) \tag{3}$$

For a series $z = \alpha_0 X^{\beta_0} + \alpha_1 X^{\beta_1} + \ldots$, where $\beta_0 > \beta_1 > \ldots$ and $\alpha_i \neq 0$ for $i \ge 0$, denote by $lt(z) = \alpha_0 X^{\beta_0}$ the leading term of the series, as above $\alpha_0 = lc(z)$. Then $lt(\tau_k(\gamma X^{\delta})) = \gamma^k X^{k\delta}$ since $\delta > -1$.

Write

$$\mathscr{R}^{(k)}(y) = \sum_{j\nu\in Z}\alpha_{j,k}X^j \in C[X^{1/\nu}, X^{-1/\nu}]$$

and for every $0 \le k \le n$ mark on the (X, Y)-plane all the points (j, k) for which $\alpha_{j,k} \neq 0$. We shall say that a coefficient $\alpha_{j,k}$ corresponds to the point (j, k). Denote by $\mathbf{P}(y)$ the convex hull of the union of all these points (for $0 \le k \le n$) with the point $(-\infty, 0)$. Thus, $\mathbf{P}(y)$ contains two rays, lying on the line $\{Y = n\}$ and on a line $\{Y = k_0\}$, where k_0 is the least k such that $\mathscr{R}^{(k)}(y) \neq 0$ (in the degenerate case $n = k_0$ $\mathbf{P}(y)$ consists of a single ray). $\mathbf{P}(y)$ also contains several other edges. $\mathbf{P}(y)$ is the Newton polygon of the equation $\mathscr{R}(Y+y) = 0$.

If an edge contains points $(j_1, k_1), (j_2, k_2)$ then its slope is defined as a number $-(j_1 - j_2)/(k_1 - k_2)$. When ordering the edges from top to bottom their slopes decrease. If X^{β} is the least power of X occurring in y, then at the current step for producing the next term γX^{δ} the algorithm looks through the edges in $\mathbf{P}(y)$ with the slopes δ satisfying inequalities $-1 < \delta < \beta$. If there is an edge in $\mathbf{P}(y)$ with a slope less or equal to (-1), then one of the possible prefixes $P = y$ is already produced. Fix a certain edge e with a slope $-1 < \delta < \beta$ and yield a polynomial

$$h_e(Z) = \sum_{(\deg(\mathscr{R}^{(k)}(y)), k) \in e} \frac{1}{k!} lc(\mathscr{R}^{(k)}(y)) Z^k,$$

where the summation ranges over all the points $(j, k) = (\deg(\mathscr{R}^{(k)}(y)), k)$ of the edge e. Then $lt(\mathscr{R}(y + \gamma X^{\delta})) = h_e(\gamma) X^{j+\delta k}$ according to (3), where (j, k) is an arbitrary point of the edge e; observe that $j + \delta k$ does not depend on the choice of the point of e. Thus, at the current step of producing a prefix P of a solution of the equation $\mathscr{R}(Y) = 0$, the next term $\gamma X^{\delta} \neq 0$ is chosen so that δ is the slope of some edge e, where $-1 < \delta < \beta$, and, furthermore, $h_e(\gamma) = 0$. The algorithm looks through all possible γ, δ satisfying the formulated requirements and this leads to different prefixes P.

In the following Lemma 2.2 the properties of the Newton polygon $\mathbf{P}(y + \gamma X^{\delta})$ at the next step of producing the prefix P of the solution of the equation $\mathscr{R}(Y) = 0$ are exhibited. Remark that $\mathbf{P}(y + \gamma X^{\delta})$ is the Newton polygon of the equation $\mathscr{R}(Y + y + \gamma X^{\delta}) = 0$.

LEMMA 2.2. *In the polygon* $\mathbf{P}(y + \gamma X^{\delta})$ *the edges, situated above the edge e, are the same as in* $\mathbf{P}(y)$, *and, moreover, in both polygons the coefficients corresponding to the points on these edges coincide. Furthermore, in* $\mathbf{P}(y + \gamma X^{\delta})$ *there is either an edge* $\bar{e}$ *parallel to e originating from the same upper vertex as the edge e, where the ordinate of the lower vertex of e equals the multiplicity of the root* γ *of the polynomial* h_e, *when* h_e *has more than one root, or* h_e *has the single root* γ, *and in this case the edge of the polygon* $\mathbf{P}(y + \gamma X^{\delta})$ *originating from the upper vertex of the edge e has a slope less than* δ.

PROOF. Let an edge e_1 with slope $\delta_1 > \delta$ be situated in the polygon $\mathbf{P}(y)$ above the edge e, and let a certain point $(j_1, k_1) \in e_1$. Because of Lemma 1.2, for each $o \le k \le n$ we have

$$\mathscr{R}^{(k)}(y + \gamma X^{\delta}) = \sum_{k \le i \le n} \frac{1}{(i-k)!} \tau_{i-k}(\gamma X^{\delta}) \mathscr{R}^{(i)}(y). \tag{4}$$

Denote by $\mathbf{L}_{e_1}$ the line containing the edge e_1. Consider an open half-plane Υ_{e_1} situated on the same side of the line $\mathbf{L}_{e_1}$ as the polygon $\mathbf{P}(y)$. Since

$$\deg(\tau_{i-k}(\gamma X^{\delta}) \mathscr{R}^{(i)}(y)) = \deg(\mathscr{R}^{(i)}(y)) + \delta(i-k),$$

for $n \ge i > k$ the inequalities

$$\deg(\tau_{i-k}(\gamma X^{\delta}) \mathscr{R}^{(i)}(y)) + \delta_1 k < \deg(\mathscr{R}^{(i)}(y)) + \delta_1 i \le j_1 + \delta_1 k_1$$

are true, taking into account that the point $(\deg(\mathscr{R}^{(i)}(y)), i)$ lies in the closed half-plane $\bar{\Upsilon}_{e_1}$. If every point $(j, k) \in \mathbf{P}(y)$ with ordinate k lies in Υ_{e_1}, then $\deg(\mathscr{R}^{(k)}(y)) + \delta_1 k < j_1 + \delta_1 k_1$, hence (4) implies that each point $(j, k) \in \mathscr{R}(y + \gamma X^\delta)$ with the same ordinate k also lies in Υ_{e_1} by virtue of the inequality $\deg(\mathscr{R}^{(k)}(y + \gamma X^\delta)) + \delta_1 k < j_1 + \delta_1 k_1$. For $n \geq i \geq k_1$ one gets an inequality

$$\deg(\tau_{i-k_1}(\gamma X^\delta)\mathscr{R}^{(i)}(y)) + \delta_1 k_1 < j_1 + \delta_1 k_1 = \deg(\mathscr{R}^{(k_1)}(y)) + \delta_1 k_1$$

and taking into account (4) one deduces the equalities

$$\deg(\mathscr{R}^{(k_1)}(y + \gamma X^\delta)) = \deg(\mathscr{R}^{(k_1)}(y)), \quad lt(\mathscr{R}^{(k_1)}(y + \gamma X^\delta)) = lt(R^{(k_1)}(y))$$

and the first statement of Lemma 2.2.

Arguing as above one concludes from (4) that the polygon $\mathbf{P}(y + \gamma X^\delta)$ is situated in $\bar{\Upsilon}_e$. We have already shown that the upper vertex of the edge e belongs to the polygon $\mathbf{P}(y + \gamma X^\delta)$. Assume a point $(j, k) \in \mathbf{P}(y + \gamma X^\delta)$ lies on $\mathbf{L}_e$. Then $\deg(\mathscr{R}^{(k)}(y + \gamma X^\delta)) = j$, and according to the inequality $\deg(\tau_{i-k}(\gamma X^\delta)\mathscr{R}^{(i)}(y)) \leq j$ for $n \geq i \geq k$ because the point $(\mathscr{R}^{(i)}(y), i) \in \Upsilon_e$, (4) implies that the leading coefficient

$$lc(\mathscr{R}^{(k)}(y + \gamma X^\delta)) = \sum_{k \leq i \leq n; (\deg R^{(i)}(y), i) \in e} \frac{1}{(i-k)!} \cdot \gamma^{i-k} lc(R^{(i)}(y)) = (D^k h_e)(\gamma)$$

equals the kth derivative of the polynomial h_e at the point γ. Therefore, if k_0 denotes the multiplicity of the root γ of the polynomial h_e, then the points of the line $\mathbf{L}_e$ with ordinates less than k_0 do not belong to $\mathbf{P}(y + \gamma X^\delta)$, whereas the point with the ordinate k_0 does. Lemma 2.2 is proved.

One can infer from Lemma 2.2 by inverse induction that the multiplicity of the prefix $y + \gamma X^\delta$ is less than or equal to the multiplicity of the root γ of the polynomial h_e, in other words, to the sum of the lengths of projections into the axis Y of all the edges in the polygon $\mathbf{P}(y + \gamma X^\delta)$ with the slopes less than δ (hence these values coincide taking into account that there exist exactly n (fundamental) solutions of the equation $\mathscr{R}(Y) = 0$, cf. Della Dora *et al.*, 1982). The inductive step in the case when γ is not the single root of the polynomial h_e follows from the fact that the length of projection of the edge e onto the axis Y equals the sum of the multiplicities of all non-zero roots of the polynomial h_e. If $h_e = c(Z - \gamma)^k$ for suitable $c \in \mathbb{C}$, $k \in \mathbb{N}$, then e is the single edge (whose projection has length k) in the polygon $\mathbf{P}(y)$ with a slope not exceeding δ.

LEMMA 2.3. *Let the equation $\mathscr{R}(Y) = 0$ have exactly m solutions with prefix y. Then for every $0 \leq k < m$, the equation $\mathscr{R}^{(k)}(Y) = 0$ has exactly $m - k$ solutions with the prefix y. Furthermore, the equation $\mathscr{R}^{(m)}(Y) = 0$ has no solutions with the prefix y.*

PROOF. Let $y = y_1 + \gamma X^\delta + \ldots$, where y_1 is a certain prefix of y (possibly empty). Suppose that it is already shown that the equation $\mathscr{R}^{(k)}(Y) = 0$ has not less than $m - k$ solutions with the prefix y_1. Consider the Newton polygon $\mathbf{P}^{(k)}(y_1)$ corresponding to the prefix y_1 of a solution of the equation $\mathscr{R}^{(k)}(Y) = 0$, i.e. $\mathbf{P}^{(k)}(y_1)$ is the Newton polygon of the equation $\mathscr{R}^{(k)}(Y + y_1) = 0$. Because of Lemma 2.1(b), the polygon $\mathbf{P}^{(k)}(y_1)$ (including the coefficients corresponding to the points of the polygon) is obtained from the points $(\deg(\mathscr{R}^{(s)}(y_1)), s)$, $0 \leq s \leq n$ (recall that their convex hull with the point $(-\infty, 0)$ coincides with the polygon $\mathbf{P}(y_1) = \mathbf{P}^{(0)}(y_1)$ transformed in the following way. One first shifts it downwards by k, then deletes all points below the X-axis and takes the convex hull of the remaining points and

the point $(-\infty, 0)$. Therefore, for each edge of the polygon $\mathbf{P}(y_1)$ the corresponding polynomial

$$h_e(Z) = \sum_{(\deg(\mathscr{R}^{(i)}(y_1)), i) \in e} \frac{1}{i!} lc(\mathscr{R}^{(i)}(y_1)) Z^i$$

is transformed into the polynomial

$$h_{e^{(k)}}(Z) = \sum_{(\deg(\mathscr{R}^{(k+l)}(y_1)), l) \in e^{(k)}} \frac{1}{l!} lc(\mathscr{R}^{(k+l)}(y_1)) Z^l$$

$$= \sum_{(\deg(\mathscr{R}^{(i)}(y_1)), i) \in e; i \geq k} \frac{1}{(i-k)!} lc(\mathscr{R}^{(i)}(y_1)) Z^{i-k} = D^k h_e$$

which corresponds to the edge $e^{(k)}$ of the polygon $\mathbf{P}^{(k)}(y_1)$, obtained from e by shifting downwards by k, deleting the part below the X-axis (observe that after taking the kth derivative D^k the corresponding terms of the polynomial h_e disappear) and possibly deleting some other vertices, provided the edge $e^{(k)}$ occurs in the polygon $\mathbf{P}^{(k)}(y_1)$. Note that the latter condition holds iff $D^k h_e$ contains at least two terms.

Consider the edge e_0 with slope δ in the polygon $\mathbf{P}(y_1)$, and the corresponding term γX^δ. The multiplicity of the root γ of the polynomial h_{e_0} is greater than or equal to m according to the assumption made in the lemma, in particular, $\deg(h_{e_0}) \geq m > k$ and the upper vertex of the edge e_0 lies above the line $\{Y = k\}$, moreover, $D^k h_{e_0}(\gamma) = 0$, so $D^k h_{e_0}$ contains at least two terms, hence in the polygon $\mathbf{P}^{(k)}(y_1)$ there is an edge $e_0^{(k)}$ with slope δ. The polynomial $h_{e_0^{(k)}} = D^k h_{e_0}$ corresponds to this edge and has the root γ with multiplicity greater than or equal to $m-k$. This shows that the equation $\mathscr{R}^{(k)}(Y) = 0$ has at least $m-k$ solutions with the prefix $y_1 + \gamma X^\delta$. Continuing this process further, one deduces that the equation $\mathscr{R}^{(k)}(Y) = 0$ has at least $m-k$ solutions with the prefix y.

Now we show that the equation $\mathscr{R}^{(m)}(Y) = 0$ has no solutions with the prefix y. Consider a uniquely defined (possibly empty) prefix y_1 such that $y = y_1 + \gamma X^\delta + \ldots$ and either y_1 is a prefix of at least $(m+1)$ solutions of the equation $\mathscr{R}(Y) = 0$ (provided that y_1 is non-empty), whereas the prefix $y_1 + \gamma X^\delta$ has a multiplicity m. Then in $\mathbf{P}(y_1)$ there is an edge e_0 with slope δ and γ being the root of the polynomial h_{e_0} with multiplicity m. If the upper vertex of the edge e_0 has ordinate $l = \deg(h_{e_0})$ greater than m, then according to what was shown above, either there is an edge $e_0^{(m)}$ in the polygon $\mathbf{P}^{(m)}(y_1)$ with slope δ without γ being a root of the polynomial $h_{e_0^{(m)}} = D^m h_{e_0}$ corresponding to this edge, or there is no edge with slope δ, hence there is no solution of the equation $\mathscr{R}^{(m)}(Y) = 0$ with the prefix $y_1 + \gamma X^\delta$. Otherwise, if $l = m$, then in the polygon $\mathbf{P}^{(m)}(y_1)$ there is no edge with slope δ, therefore $y_1 + \gamma X^\delta$ is not a prefix of any solution of the equation $\mathscr{R}^{(m)}(Y) = 0$. This proves the second statement of Lemma 2.3.

In order to complete the proof of the first statement of the lemma, assume that the equation $\mathscr{R}^{(k)}(Y) = 0$ has more than $m-k$ solutions with the prefix y. According to what was shown above, the equation $\mathscr{R}^{(m)}(Y) = \mathscr{R}^{(m-k)}\mathscr{R}^{(k)}(Y) = 0$ (see Lemma 2.1(b)) has at least one solution with the prefix y. This contradiction of the second statement of the lemma proves the first one and thereby Lemma 2.3.

Recall that we are considering a (fundamental) solution

$$Y = P + \rho X^{-1} + \Xi = \sum_{0 \leq t < (\delta_0 + 1)\nu} \gamma_t X^{\delta_0 - t/\nu} + \rho X^{-1} + \Xi \tag{5}$$

of the equation $\mathscr{R}(Y) = 0$ and P being its prefix, with $\gamma_0 \neq 0$, $\delta_0 \nu \in Z$, $1 \leq \nu \leq n$ (see the

Introduction). Observe that $\delta_0 \le d-1$ taking into account that δ_0 is the slope of a certain edge of the Newton polygon $\mathbf{P} = \mathbf{P}(0)$ of the equation $\mathscr{R}(Y) = 0$ (see the beginning of the present section), and that the edges of $\mathbf{P}$ have vertices with integer co-ordinates of the form $(\deg(f_k), k)$, hence the edges are situated in the rectangle bounded by the lines $Y = 0$, $Y = n$, $X = 0$, $X = d-1$ (see (1)). In particular, P contains at most dn terms.

Consider a field $F_Y = F(\gamma_0, \gamma_1, \ldots)$ generated over F by all the coefficients of the solution Y (note, see, e.g. Olver, 1974; Wasow, 1976, that in fact F_Y is generated by the coefficients of P and by ρ). We see that the degree of the finite extension of fields $[F_Y : F] \le n$, since for every field embedding $\sigma : F_Y \to \bar{F}$ over the field F (see van der Waerden, 1971) the expression $\sigma(Y)$ is also a solution of the equation $\mathscr{R}(Y) = 0$ (cf. Singer, 1981). We shall say that a solution Y (see (5)) is non-peculiar when γ_0 is a root of the polynomial h_e with multiplicity one, where e is an edge of the polygon $\mathbf{P}$ with the slope δ_0. In the following lemma the coefficients of P (see (5)) are estimated in the case of a non-peculiar solution Y.

LEMMA 2.4. *Let Y (see (5)) be non-peculiar solution of the equation $\mathscr{R}(Y) = 0$. Then*

$$\gamma_t \in F_Y = F[\gamma_0] = \mathbb{Q}[\eta_0] \simeq \mathbb{Q}[Z]/(\phi_0),$$

where $\phi_0 \in \mathbb{Q}[Z]$ is the minimal polynomial of the primitive element η_0 over the field $\mathbb{Q}$. Furthermore,

$$\deg_Z(\phi_0) = \deg_Z(\varphi)[F_Y : F] < d_1 n$$

(see (1)) and the sizes of the coefficients $l(\phi_0), l(f_k), l(\eta) \le M\mathscr{P}(d_1, n)$, here $l(f_k)$ (respectively $l(\eta)$) is the size of coefficients of the polynomial f_k (respectively, the size of the primitive element η of the field $F = \mathbb{Q}[\eta]$), see the beginning of the Introduction, in the field F_Y. One can produce the polynomial ϕ_0 within time $\mathscr{P}(M, d_1, n)$. Moreover, if $\delta_0 \ge 0$, then for $0 \le t < (\delta_0 + 1)\nu$ the size $l(\gamma_t) \le (M + \log(d))\mathscr{P}(d_1, n, t)$ and the time required for producing γ_t can be bounded by a polynomial in M, d, d_1, n. Otherwise, if $\delta_0 < 0$, then $l(\gamma_t) \le (M + \log(d))\mathscr{P}(d_1, n^t)$ and γ_t can be produced within time polynomial in M, d, d_1, n^t.

PROOF. Consider the edge e_0 with slope δ_0 in the polygon $\mathbf{P}$ and denote a polynomial

$$\phi_1 = h_{e_0} = \sum_{(\deg(f_k), k) \in e_0} \frac{1}{k!} lc(f_k) Z^k.$$

The algorithm picks out some divisor $\tilde{\phi}_1 | \phi_1$, irreducible over F, with the aid of Proposition 1.4 (see the Introduction) satisfying the property that the polynomials $\tilde{\phi}_1$ and $\phi_1/\tilde{\phi}_1$ are relatively prime (a divisor with the latter property exists by virtue of the non-peculiarity of Y). Taking into account that $\phi_1(\gamma_0) = 0$, one can assume without loss of generality that $\tilde{\phi}_1(\gamma_0) = 0$. Based on the corollary following Proposition 1.4, the algorithm yields a primitive element η_0 over $\mathbb{Q}$ of the field $F[Z]/(\tilde{\phi}_1)$ and its minimal (over $\mathbb{Q}$) polynomial ϕ_0 (we show below that

$$F_Y = \mathbb{Q}[\eta_0] \simeq \mathbb{Q}[Z]/(\phi_0) \simeq F[Z]/(\tilde{\phi}_1)).$$

Since $\deg_Z(\phi_1) \le n$, $l(\phi_1) \le M + 0(n \log(n))$, Proposition 1.4 and its corollary imply the bounds $l(\tilde{\phi}_1), l(\phi_0), l(\eta), l(\gamma_0), l(f_k) \le \mathscr{M}\mathscr{P}(d_1, n)$ (see (1)) and also the time bound $\mathscr{P}(M, d_1, n)$ for yielding $\tilde{\phi}_1, \phi_0$ and the expressions η, γ_0, f_k in the field $\mathbb{Q}[\eta_0]$.

After the first step of producing P (see above) the Newton polygon $\mathbf{P}(\gamma_0 X^{\delta_0})$ will be constructed. Taking into account that the multiplicity of the root γ_0 of the polynomial h_{e_0} equals one, Lemma 2.2 implies that in the polygon there is the unique edge e_1 with a slope

$\delta_1 = \delta_0 - s_1/\nu$ less than δ_0, where s_1 is a natural number, and, moreover, the vertices of e_1 are $(j, 1), (j_1, 0)$ where $j = \deg(\mathscr{R}^{(1)}(\gamma_0 X^{\delta_0}))$, $j_1 = \deg(\mathscr{R}(\gamma_0 X^{\delta_0}))$. Therefore, the polynomial

$$h_{e_1} = lc(\mathscr{R}^{(1)}(\gamma_0 X^{\delta_0}))Z + lc(\mathscr{R}(\gamma_0 X^{\delta_0}))$$

is linear and in the succeeding steps of producing P (see Lemma 2.2) the polynomials corresponding to the edges of the constructed polygons are also linear, hence the field $F_Y = F(\gamma_0, \gamma_1, \ldots) = F[\gamma_0] = \mathbb{Q}[\eta_0]$. Because of Lemma 2.2, the leading coefficient $lc(\mathscr{R}^{(1)}(\gamma_0 X^{\delta_0})) \neq 0$ of these polynomials does not change. Write for brevity $h_{e_1} = \beta_0 Z + \beta_1$, then $\gamma_{s_1} = -\beta_1/\beta_0$ (see the above process for producing P). After the tth step of the process the polygon $\mathbf{P}(y_t)$ will be constructed, where $y_t = \gamma_0 X^{\delta_0} + \gamma_{s_1} X^{\delta_1} + \ldots + \gamma_{s_{t-1}} X^{\delta_{t-1}}$, and $\mathbf{P}(y_t)$ has a unique edge e_t with a slope $\delta_t = \delta_0 - s_t/\nu$ less than δ_{t-1} for an appropriate natural number s_t and with the vertices $(j, 1), (j_t, 0)$. Corresponding to e_t is the polynomial $h_{e_t} = \beta_0 Z + \beta_t$, where $\beta_t = lc(\mathscr{R}(y_t))$, $j_t = \deg(\mathscr{R}(y_t))$, then $\delta_t = j_t - j$ and $\gamma_{s_t} = -\beta_t/\beta_0$.

Recall that

$$\mathscr{R}(y_t) = \sum_{0 \leq k \leq n} f_k \tau_k(y_t).$$

Assume that while calculating the coefficient β_t, a monomial occurs in the expression $\tau_k(y_t)$ such that this monomial contains a term $\gamma_0^{\kappa_0}\gamma_{s_1}^{\kappa_1} \ldots \gamma_{s_{t-1}}^{\kappa_{t-1}}$, then $\kappa_0 + \kappa_1 + \ldots \kappa_{t-1} \leq k$, furthermore, the degree relatively to the variable X of this monomial does not exceed

$$\kappa = \kappa_0 \delta_0 + \kappa_1 \delta_1 + \ldots + \kappa_{t-1}\delta_{t-1} < kd,$$

hence

$$\deg(f_k) + \kappa_0 \delta_0 + \ldots + \kappa_{t-1}\delta_{t-1} \geq j_t = \delta_0 - s_t/\nu + j.$$

In all $\tau_k(y_t)$ contains at most $(2t)^k$ monomials of the form $(c/\nu^k)\gamma_0^{\kappa_0}\gamma_{s_1}^{\kappa_1} \ldots \gamma_{s_{t-1}}^{\kappa_{t-1}} X^{\kappa'}$, where $\kappa' \leq \kappa$ and c is a natural number less than $(\kappa\nu)^k < (kdn)^k$. Suppose that the size of coefficients $l(\gamma_{s_t}) \leq M_t$. Then $M_0 \leq M\mathscr{P}(d_1, n)$ (see above) and

$$M_t \leq \max_{\kappa_0, \ldots, \kappa_{t-1}} \left\{ \sum_{0 \leq i \leq t-1} \kappa_i M_i \right\} + 0(n \log(ndt)) + M\mathscr{P}(d_1 n)$$

for $t \geq 1$. Since the point $(\deg(f_k), k)$ is situated in the polygon $\mathscr{P}$ which contains the edge e_0 with the slope δ_0 whose continuation $\mathbf{L}_{e_0}$ contains in its turn the point $(j, 1)$ (by virtue of Lemma 2.2 and non-peculiarity of Y), an inequality $\deg(f_k) + k\delta_0 \leq j + \delta_0$ is valid. Therefore,

$$-(k-1)\delta_0 + \kappa_0 \delta_0 + \kappa_1(\delta_0 - s_1/\nu) + \ldots + \kappa_{t-1}(\delta_0 - s_{t-1}/\nu) \geq \delta_0 - s_t/\nu.$$

When $\delta_0 \geq 0$ we obtain an inequality $\kappa_1 s_1 + \ldots + \kappa_{t-1} s_{t-1} \leq s_t$, whence by induction on $t \geq 1$ we deduce a bound

$$M_t \leq (2s_t - 1)\log(s_t + 1)(M + \log(d))\mathscr{P}(d_1, n).$$

The algorithm produces γ_{s_t} within time $\mathscr{P}(M, d, d_1, n, s_t) \leq \mathscr{P}(M, d, d_1, n)$.

When $\delta_0 < 0$ we infer by induction on $t \geq 1$ a bound

$$M_t \leq (2n^t - 1)(M + \log d)\mathscr{P}(d_1, n)$$

taking into account an inequality $\kappa_0 + \kappa_1 + \ldots + \kappa_{t-1} \leq k \leq n$. The algorithm produces γ_{s_t} within time $\mathscr{P}(M, d, d_1, n^t)$. Lemma 2.4. is proved.

Now we proceed to estimate the coefficients and the time required for their production while expanding a prefix of an arbitrary solution (5) of the equation $\mathscr{R}(Y) = 0$. Note that

the known methods for estimating the coefficients of power series solutions of the equation $\mathscr{R}(Y)=0$ and other types of ordinary differential equations (see, e.g. Mahler, 1976; Wasow, 1976) have essentially asymptotical features without taking into account the dependence on the parameters of the operator $\mathscr{R}$, and these methods do not allow us to get the required bounds on the opening coefficients of the series (cf. Lemma 2.5, below). Let us mention also that in Chistov (1986) bounds, stronger than in Lemma 2.5, on the coefficients of Newton–Puiseux series of a solution of algebraic equation are obtained (these bounds guarantee the polynomial complexity bound for the Newton–Puiseux expanding algorithm). Unfortunately, the method from Chistov (1986) cannot be generalized directly to differential equations.

Thus, represent uniquely a prefix $P=p_1+\ldots+p_s$ (see (5)), where

$$p_i=\sum_{j\geq 0}\gamma_{i,j}X^{\sigma_i-j/\nu},$$

herein $\gamma_{i,0}\neq 0$ for each $1\leq i\leq s$ and $p_1+\ldots+p_i$ is a prefix with a multiplicity m_i as well as a prefix $p_1+\ldots p_{i-1}+\gamma_{i,0}X^{\sigma_i}$. Evidently, $n\geq m_1>\ldots>m_s\geq 1$. Fix for a while $1\leq i\leq s$ and denote a prefix $p=p_1+\ldots+p_{i-1}$. By virtue of Lemma 2.3 the equation $\mathscr{R}^{(m_i-1)}(Y)=0$ has a unique solution with the prefix $p+p_i$, hence the equation $\mathscr{R}^{(m_i-1)}(Y+p)=0$ has a non-peculiar solution with a prefix p_i. Let the coefficients $\gamma_{l,t}$ for all $1\leq l<i$ generate, over F, a field $f_{i-1}=\mathbb{Q}[\eta_{i-1}]\simeq\mathbb{Q}(Z]/(\phi_{i-1})$, where $\phi_{i-1}\in\mathbb{Q}[Z]$ is a minimal polynomial of a primitive element η_{i-1}. Recall that $\deg(\phi_{i-1})<d_1n$ (see the remark just before Lemma 2.4) and

$$\eta_{i-1}=\eta+\sum_{l,t}\lambda_{l,t}\gamma_{l,t}$$

for suitable natural numbers $0\leq\lambda_{l,t}<d_1n$ (cf. corollary to Proposition 1.4). Assume the bounds $l(\phi_{i-1})$, $l(f_k)$, $l(\gamma_{l,t})$, $l(\eta)\leq\mu$ to be true for $1\leq l<i$, $0\leq k\leq n$.

Below we apply Lemma 2.4 to the equation $\mathscr{R}^{(m_i-1)}(Y+p)=0$. According to Lemma 2.1 (see also (4))

$$\mathscr{R}^{(m_i-1)}(Y+p)=\sum_{0\leq k\leq n-m_i+1}\frac{1}{k!}\tau_k\mathscr{R}^{(m_i+k-1)}(p)$$

and

$$\mathscr{R}^{(m_i+k-1)}(p)=(m_i+k-1)!\sum_{0\leq j\leq n-m_i-k+1}\binom{m_i+k+j-1}{j}f_{m_i+k+j-1}\tau_j(p).$$

The expression $\gamma_j(p)$ contains at most $(2nd)^j$ monomials of the form

$$(c_1/c_2)\left(\prod_{0\leq l\leq i;t}\gamma_{l,t}^{\kappa_{l,t}}\right)X^{\kappa/\nu},$$

where $\kappa_{l,t}\geq 0$, κ, c_1, c_2 are integers and $|c_1|\leq(nd)^j$, $|c_2|\leq n^s$ (cf. the proof of Lemma 2.4). Moreover,

$$\sum_{0\leq l<i;t}\kappa_{l,t}\leq j\quad\text{and}\quad -j\nu<\kappa<jd\nu.$$

Therefore, the size

$$l\left(\frac{1}{k!}\mathscr{R}^{(m_i+k-1)}(p)\right)\leq(\mu+\log(d))\mathscr{P}(d_1,n).$$

Provided that p is already constructed, these observations and the formula $\tau_{j+1}(p)=p\tau_j(p)+D\tau_j(p)$ show by induction on j that one can yield $\tau_j(p)$ and by the same token

$\mathscr{R}^{(m_i+k-1)}(p)$ within time $\mathscr{P}(\mu, d, d_1, n)$.

In order to prepare the way for applying Lemma 2.4 to the equation $\mathscr{R}^{(m_i-1)}(Y+p)=0$, multiply $\mathscr{R}^{(m_i-1)}(Y+p)$ by X^n and make the substitution $X_1=X^{1/\nu}$. As a result, we obtain an expression of the form $\sum_{o\le k\le n-m_i+1} g_k\tau_k$, where $g_k\in F_{i-1}[X_1]$ are polynomials satisfying the bounds $\deg_{X_1}(g_k)\le n(n+1)(d+1)$ and $l(g_k)\le(\mu+\log(d))\mathscr{P}(d_1, n)$. We infer from Lemma 2.4 that the coefficients $\gamma_{i,t}\in F_i=\mathbb{Q}[\eta_i]\simeq\mathbb{Q}[Z](\phi_i)$, moreover, $\deg(\phi_i)<d_1n$ and $l(\phi_i)$, $l(g_k)$, $l(\eta_{i-1})$, $l(\gamma_{l,t})\le(\mu+\log(d))\mathscr{P}(d_1, n)$ for $1\le l<i$. If $\sigma_i\ge 0$, then

$$l(\gamma_i, t)\le(\mu+\log(d))\mathscr{P}(d_1, n, t)\le\mu\mathscr{P}(d, d_1, n).$$

Whence by induction on i we deduce the bounds $l(\phi_i)$, $l(\gamma_{l,t})\le M\mathscr{P}((ddn)^t)$ for $1\le l\le i$ and taking into account that $i\le s\le n$ we conclude that $l(\phi_i)$, $l(\gamma_{l,t})\le M\mathscr{P}((dd_1n)^n)$ for $1\le l\le i$. Assume now that there exists an i_0 such that $\sigma_{i_0-1}\ge 0$, $\sigma_{i_0}<o$ and let p_i contain r_i terms when $i\ge i_0$, so $\sum_{i\ge i_0} r_i<\nu\le n$. Making use of Lemma 2.4 as above by induction on i one infers the bounds

$$l(\phi_i), l(\gamma_{l,t})\le M\mathscr{P}((dd_1n)^n(dd_1)^{(i-i_0+1)}n^{(\sum_{i_0\le j<\nu} rj)+t})\le M\mathscr{P}((dd_1n)^n)$$

for $i_0\le l\le i$. Thus, these bounds are true for all coefficients of P.

We now show that one can estimate the time required for producing P by $\mathscr{P}(M, (dd_1n)^n)$. At each step of producing P (see the beginning of the section) after producing a prefix p (for convenience of notations we suppose the parameters of p to satisfy the same bounds as above, in particular the coefficients of p generate a field $F_{i-1}=\mathbb{Q}[\eta_{i-1}]\simeq\mathbb{Q}[Z]/(\phi_{i-1})$). In order to produce the next term γX^δ, a polynomial

$$h_e=\sum_{(\deg(\mathscr{R}^{(k)}(p)), k)\in e}\frac{1}{k!}lc(\mathscr{R}^{(k)}(p))Z^k,$$

corresponding to an edge e with the slope δ, is considered. With the help of Proposition 1.4, the algorithm finds a factor $\tilde{h}_e\in F_{i-1}[Z]$ of h_e, irreducible over F_{i-1}, such that $\tilde{h}_e(\gamma)=0$ (in fact the algorithm looks over all the irreducible factors, cf. the beginning of the proof of Lemma 2.4). As it was shown above, one can construct $\mathscr{R}^{(k)}(p)$ and thereby the polynomial h_e within time $\mathscr{P}(\mu, d, d_1, n)$, furthermore, $l(h_e)\le(\mu+\log(d))\mathscr{P}(d_1, n)$. By virtue of Proposition 1.4, the algorithm factors the polynomial h_e over F_{i-1} and so finds $\tilde{h}_e$ within time $\mathscr{P}(\mu, \log(d), d_1, n)$, moreover, $l(\tilde{h}_e)\le(\mu+\log(d))\mathscr{P}(d_1, n)$. Involving the corollary from Proposition 1.4, the algorithm yields a field $\tilde{F}_{i-1}=F_{i-1}[\gamma]\simeq F_{i-1}[Z]/(\tilde{h}_e)$ in the form $\tilde{F}_{i-1}=\mathbb{Q}[\tilde{\eta}_{i-1}]\simeq\mathbb{Q}[Z]/(\tilde{\phi}_{i-1})$, where $\tilde{\phi}_{i-1}\in\mathbb{Q}[Z]$ is the minimal polynomial (over $\mathbb{Q}$) of a primitive element $\tilde{\eta}_{i-1}=\eta_{i-1}+\lambda\gamma$ for an appropriate integer $0\le\lambda<d_1n$. The algorithm then yields $\tilde{\phi}_{i-1}$, λ and the expressions γ, $\gamma_{l,t}$ for $1\le l\le i-1$ in the field $\tilde{F}_{i-1}$ within time $\mathscr{P}(\mu+\log(d), d_1, n)$, furthermore, $l(\tilde{\phi}_{i-1})$, $l(\gamma)$, $l(\gamma_{l,t})\le(\mu+\log(d))P(d_1, n)$. Therefore, by the previously proved bound $\mu=M\mathscr{P}((dd_1n)^n)$, we achieve the required time bound for producing P (observe that the bound on μ was ascertained with respect to another primitive element of the form $\sum_{l,t}\lambda_{l,t}\gamma_{l,t}$ of the field F_{i-1} rather than η_{i-1}, however, both primitive elements are expressible with respect to each other within the same size bounds, cf. Chistov & Grigor'ev (1983)).

In order to find ρ in the solution (5) of the equation $\mathscr{R}(Y)=0$, apply formula (3) and get

$$\mathscr{R}(P+\rho X^{-1})=\sum_{0\le k\le n}\frac{1}{k!}\tau_k(\rho X^{-1})\mathscr{R}^{(k)}(P).$$

Then $lc(\tau_k(\rho X^{-1}))$ is a polynomial in ρ of degree k with the integer coefficients, whose absolute values do not exceed $\exp(\mathscr{P}(k))$. Using what was shown above and the corollary to Proposition 1.4, we conclude that $\gamma_t, \rho \in \mathbb{Q}[\eta_1] \simeq \mathbb{Q}[Z]/(\phi_1)$, where ϕ_1 is a minimal over $\mathbb{Q}$ polynomial of a primitive element η_1 (cf. above), moreover, $l(\phi_1), l(\gamma_t), l(\rho) \leq M\mathscr{P}(dd_n n)^n)$. Recall that $\deg(\phi_1) < d_1 n$. One can estimate the time required for producing $\phi_1, \eta_1, \gamma_t, \rho$ as above by $\mathscr{P}(M, (dd_1 n)^n)$.

Finally, return back to considering an arbitrary singular point b of the operator L, i.e. $f_n(b) = 0$ (see (2) and the beginning of the Introduction). The algorithm factors f_n over the field F with the aid of Proposition 1.4. Let $\tilde{f}_n \in F[X]$ be a certain irreducible multiplier and $\tilde{f}_n(b) = 0$. Then $l(\tilde{f}_n) \leq M \cdot \mathscr{P}(d, d_1)$ (see (1)). Replacing the variables $X_1 = 1/(X-b)$, we obtain an operator L_1 with a singular point $X_1 = \infty$. Apply the already proven bounds to L_1, taking into account that the role of the field F is now played by a field $F[b] \simeq \mathbb{Q}[Z]/(\varphi_2)$ where a minimal polynomial $\varphi_2 \in \mathbb{Q}[Z]$ can be constructed again with the help of the corollary to Proposition 1.4, and, furthermore, $\deg(\varphi_2) < d_1 d$ and $l(\varphi_2) \leq M\mathscr{P}(d, d_1)$. Summarising the results of the present section, we formulate the following

LEMMA 2.5. *One can design an algorithm which, for any operator L (satisfying the bounds (1), see the Introduction) and its singular point b, produces an irreducible (over $\mathbb{Q}$) polynomial $\varphi_0 \in \mathbb{Q}[Z]$ determining a field $F_0 \simeq \mathbb{Q}[Z]/(\varphi_0)$ such that $b \in F_0$, produces an integer $1 \leq \nu \leq n$, produces a fractional-power polynomial*

$$\int P = \sum_{j>0} \gamma_j (X-b)^{-j/\nu} \in F_0[(X-b)^{-1/\nu}]$$

(respectively $\int P \in F_0[X^{1/\nu}]$ when the singular point $b = \infty$) and an exponent $\rho \in F_0$, so that there is a fundamental solution $v = \exp(\int P)(X-b)^{\rho}\Xi$ (see (2)) of the equation $Lv = 0$. Moreover, the following bounds hold: $\deg(\varphi_0) < dd_1 n$; $\deg_{(X-b)^{-1/\nu}}(\int P) \leq d\nu$, i.e. the indices $j \leq d\nu \leq dn$; the sizes of coefficients $l(\varphi_0), l(b), l(\gamma_j), l(\rho) \leq M\mathscr{P}((dd_1 n)^n)$. The algorithm runs within time $\mathscr{P}(M, (dd_1 n)^n)$.

COROLLARY. *The complex absolute value $|\rho| \leq \exp(M\mathscr{P}((dd_1 n)^n))$. For the proof observe that any root η_0 of the polynomial φ_0 satisfies a bound of the same form as well as the coefficients $\rho_i \in \mathbb{Q}$ of the expansion*

$$\rho = \sum_{0 \leq i < \deg(\varphi_0)} \rho_i \eta_0^i.$$

3. Estimating the Degree of a Divisor of a Linear Differential Operator

Firstly, assume that an operator L has a (right) divisor of the first order, i.e. $L = L_0(D-g)$ where $g \in \mathbb{C}(X)$, then $v = \exp(\int g)$ is a solution of the equation $Lv = 0$, hence $\mathscr{R}(g) = 0$. Consider a certain pole $a \in \mathbb{C}$ of the rational function g. If a is not a singular point of the operator L, then the function v is regular in a neighbourhood of the point a (see, e.g. Olver, 1974) and v_a regular in a neighbourhood of a such that $v_a(a) \neq 0$, so

$$g = \frac{m}{(X-a)} + \frac{Dv_a}{v_a},$$

where the function Dv_a/v_a is regular in a neighbourhood of a, i.e. $m = res_a(g)$ is the residue

of the function g in the point a. Therefore (see Schlesinger, 1897; Singer, 1981),

$$g = P + \sum_{1 \le j \le r} \frac{m_j}{X - a_j} + \sum_{1 \le i \le s} \sum_{1 \le t \le n_i} \frac{\beta_{i,t}}{(X-b_i)^t}$$

is an expansion into partial fractions, where $P \in \mathbb{C}[X]$ is a polynomial, $b_1, \ldots, b_s$ are all finite singular points of L, numbers $m_j \ge 1$ are natural, $\beta_{i,t} \in \mathbb{C}$, the points $a_1, \ldots, a_r$ are all poles of g that are not singular points of L. Note that $s \le \deg(f_n) < d$ (see (1)).

For $1 \le i \le s$ consider the power series expansion

$$g = \sum_{1 \le t \le n_i} \frac{\beta_{i,t}}{(X-b_i)^t} + g_i,$$

where g_i is regular in a neighbourhood of the point b_i. Using Lemma 2.5 we get the bounds $n_i \le d_i$; $l(\beta_{i,t}) \le M\mathscr{P}((dd_1 n)^n)$, in particular, the corollary of Lemma 2.5 implies the bound on the absolute value of the residue

$$|res_{b_i}(g)| = |\beta_{i,1}| \le \exp(M\mathscr{P}((dd_1 n)^n)).$$

Considering the expansion

$$g = P + \left(\sum_{1 \le j \le r} m_j + \sum_{1 \le i \le s} \beta_{i,1} \right) X^{-1} + g_\infty$$

in a neighbourhood of ∞, where the series g_∞ contains only the powers $X^{-\kappa}$ for $\kappa \ge 2$, again from Lemma 2.5 we deduce the bounds

$$\deg(P) \le d;\ l(P),\ l\left(\sum_{1 \le j \le r} m_j + \sum_{1 \le i \le s} \beta_{i,1} \right) \le \exp(M\mathscr{P}((dd_1 n)^n)).$$

Hence,

$$r \le \sum_{1 \le j \le r} m_j \le \exp(MP((dd_1 n)^n)).$$

This proves the following

LEMMA 3.1. *Let $L = L_0(D-g)$ where $g \in \mathbb{C}(X)$, then the degree* $\deg(g)$ *as well as the sum of absolute values of the residues*

$$\sum_{c \in \mathbb{C}} |res_c(g)| = \sum_{1 \le j \le r} m_j + \sum_{1 \le i \le s} |\beta_{i,1}|$$

of the function g over all the finite complex points do not exceed $\exp(M\mathscr{P}((dd_1 n)^n))$.

Now we proceed to complete the proof of Theorem 1.2 (see the Introduction), following the method from Schlesinger (1897) (see also Singer, 1981). Let $L = Q_0 Q$ where the operators $Q_0, Q \in \mathbb{C}(X)[D]$, the order $0 < ord(Q) = k < n$ and the leading coefficient $lc(Q) = 1$. Consider some basis $v^{(1)}, \ldots, v^{(k)}$ over $\mathbb{C}$ of the linear space of solutions of the equation $Qv = 0$. Then $QY = Wr(Y, v^{(1)}, \ldots, v^{(k)})/Wr$, where

$$Wr = Wr(v^{(1)}, \ldots, v^{(k)}) = \det(D^i v^{(j)})_{0 \le i \le k-1,\, 1 \le j \le k}$$

is the Wronskian (see, e.g. Schlesinger, 1897). Hence

$$Q = \sum_{0 \le i \le k} (q_i / Wr) D^i,$$

where $q_{k-1} = -D(Wr)$. Note

$$(Dq_i)/q_i = (D(q_i/Wr))(Wr/q_i) + D(Wr)/Wr \in \mathbb{C}(X)$$

is a rational function for each $0 \leq i \leq k$.

We now estimate the parameters of appropriate linear operators $R_0, \ldots, R_{k-1} \in F(X)[D]$ such that $R_{k-1}(Wr) = 0$; $R_i(q_i) = 0$ for all $0 \leq i \leq k-2$. For integers $0 \leq \varepsilon_1, \ldots, \varepsilon_k$ denote the $k \times k$ minor $\Delta_{\varepsilon_1, \ldots, \varepsilon_k} = \det(D^{\varepsilon_i} v^{(j)})_{1 \leq i, j \leq k}$. Observe that $Wr = \Delta_{0,1,\ldots,k-1}$, $q_i = (-1)^i \Delta_{0,1,\ldots,\hat{i},\ldots,k}$, here the roof means omitting the index. Let us prove by induction on m that, for any k-tuple $0 \leq \varepsilon_1^{(0)} < \ldots < \varepsilon_k^{(0)} < n$, the mth derivative $D^m \Delta_{\varepsilon_1^{(0)}, \ldots, \varepsilon_k^{(0)}}$ is expressible as a linear combination of the form $f_n^{-m} \sum_\varepsilon g_\varepsilon \Delta_\varepsilon$ where the sum ranges over all k-tuples $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k)$ such that $0 \leq \varepsilon_1 < \ldots < \varepsilon_k < n$, and $g_\varepsilon \in [X]$. Let the bounds $\deg(g_\varepsilon) \leq d^{(m)}$, $l(g_\varepsilon) \leq \mu^{(m)}$ hold. Obviously, $d^{(0)} = 0$, $\mu^{(0)} = 1$. Then

$$D(f_n^{-m} g_\varepsilon \Delta_\varepsilon) = (f_n^{-m} D g_\varepsilon - m g_\varepsilon f_n^{-m-1} D f_n) \Delta_\varepsilon + f_n^{-m} g_\varepsilon \sum_{1 \leq i \leq k} \Delta_{\varepsilon_1, \ldots, \varepsilon_{i-1}, \varepsilon_i + 1, \varepsilon_{i+1}, \ldots, \varepsilon_k}.$$

Note that if $0 \leq \varepsilon_1 < \ldots < \varepsilon_{k-1} < n$, then

$$\Delta_{\varepsilon_1, \ldots, \varepsilon_{k-1}, n} = -f_n^{-1} \sum_{0 \leq i < n} f_i \Delta_{\varepsilon_1, \ldots, \varepsilon_{k-1}, i}$$

(see the Introduction). Therefore $d^{(m+1)} \leq d^{(m)} + d$ and

$$\mu^{(m+1)} \leq \mu^{(m)} + 0(Md_1 + n + \log(d^{(m+1)})) + \mathscr{P}(d_1)$$

by virtue of (1), whence by induction on m we conclude that $d^{(m+1)} \leq (m+1)d$ and

$$\mu^{(m+1)} \leq (M + \log(d))(m+1)\mathscr{P}(d_1, n) + 0((m+1)\log(m+1)).$$

Hence, involving the bounds (see, e.g. Heintz (1983), also the proof of Lemma 4.1 in section 4, below) on the parameters of solutions of a suitable linear algebraic system whose unknowns are the coefficients of the desired operators R_i, $0 \leq i \leq k-1$, the following bounds are valid:

$$ord(R_i) \leq \binom{n}{k} = o(2^n); \deg(R_i) \leq d2^{2n}, \quad l(R_i) \leq (M + \log(d))\mathscr{P}(d_1, 2^n)$$

taking into account that in the above $m+1 \leq ord(R_i)$. By applying Lemma 3.1 to the operators $R_0, \ldots, R_{k-1}$ one infers that the degrees $\deg(D(Wr)/Wr)$, $\deg(D(q_i)/q_i)$ as well as the sums over all finite complex points of absolute values of the residues of the rational functions $D(Wr)/Wr$, $D(q_i)/q_i$ do not exceed $\exp(M(dd_1 2^n)^{\circ(2^n)})$.

Let the rational function $q_i/Wr = c\Pi_j (X - \alpha_{j,i})^{\kappa_{j,i}}$ for $0 \leq i \leq k-2$; $c, \alpha_{j,i} \in \mathbb{C}$; $\kappa_{j,i} \in \mathbb{Z}$, then

$$D(q_i/Wr)Wr/q_i = \sum_j \kappa_{j,i}(X - \alpha_{j,i})^{-1} = D(q_i)/q_i - D(Wr)/Wr.$$

One concludes from what was proved above, that the sum of the absolute values of the residues $\sum_j |\kappa_{j,i}|$ is less than $\exp(M(dd_1 2^n)^{\circ(2^n)})$. Therefore a similar bound is true for

$$\deg(Q) \leq \sum_{0 \leq i \leq k-2} \sum_j |\kappa_{j,i}| + \deg(D(Wr)/Wr).$$

One can find the coefficients of the operator Q_0 considering the equality $L = Q_0 Q$ as a linear system with the unknown being the coefficients of Q_0, and because of that,

$$\deg(Q_0) \leq n(n + \deg(Q)) \leq \exp(M(dd_1 2^n)^{\circ(2^n)}).$$

In order to complete the proof of Theorem 1.2 observe that if $L = Q_1 Q_2 Q_3$, then by the just proved bound $\deg(Q_3)$, $\deg(Q_2 Q_3) \leq \exp(M(dd_1 2^n)^{o(2^n)})$ and hence (cf. above) also $\deg(Q_2) \leq \exp(M(dd_1 2^n)^{o(2^n)})$.

4. Factoring a Linear Differential Operator and Its Complexity Analysis

In what follows N denotes a number taken from the conditions of Theorem 1.1. Fix a certain integer $0 < k < n$, introduce $(k+1)(N+1)$ indeterminates $c_{0,0}, \ldots, c_{0,N}, \ldots, c_{k,N}$ and a linear operator

$$Q = \sum_{0 \leq i \leq k} \left(\sum_{0 \leq j \leq N} c_{i,j} X^j \right) D^i \in \mathbb{Q}[c_{0,0}, \ldots, c_{k,N}][X, D]$$

of order k, where $Dc_{j,i} = 0$. For the fields F, F_1 denote by $F(F_1)$ their composite field (provided this is reasonable).

LEMMA 4.1. *Assume Q_0 is a linear operator in $F_1[X, D]$ for some field F_1. One can construct an operator R_0 in $F(F_1)[X, D]$ such that for any solution v of the equation $Lv = 0$ we have $R_0 Q_0 v = 0$. Furthermore, the following bounds hold:*

$$ord(R_0) \leq n,\ \deg(R_0) < (n+1)\deg(Q_0) + (ord(Q_0)+1)d.$$

In the case when the operator $Q_0 = Q$ the degree $\deg_{c_{0,0},\ldots,c_{k,N}}(R) \leq n+1$, the size $l(R) \leq (M + \log(Nd))\mathscr{P}(d_1, n)$ and it suffices $\mathscr{P}(M, (Nd)^n, d, d_1)$ time to construct R.

PROOF. Considering v as a differential variable, express $Q_0 v, DQ_0 v, \ldots, D^n Q_0 v, Lv, DLv, \ldots, D^{ord(Q_0)} Lv$ as linear combinations in $v, Dv, \ldots, D^{n+ord(Q_0)} v$ with coefficients from the rings $F_1[X]$ or $F[X]$, respectively. These coefficients constitute an $(n+ord(Q_0)+2) \times (n+ord(Q_0)+1)$ matrix B_0. Therefore, for suitable minors $g_0, \ldots, g_n, h_0, \ldots, h_{ord(Q_0)}$ of the matrix B_0, we have

$$\sum_{0 \leq i \leq n} g_i D^i Q_0 v + \sum_{0 \leq j \leq ord(Q_0)} h_j D^j Lv = 0.$$

Define an operator

$$R_0 = \sum_{0 \leq i \leq n} g_i D^i.$$

Then

$$\deg(R_0) < (n+1)\deg(Q_0) + (ord(Q_0)+1)d.$$

Furthermore, in the case when $Q_0 = Q$ the inequality $\deg_{c_{0,0},\ldots,c_{k,N}}(R) \leq n+1$ is evident. For each entry $b_{i,j}$ of the matrix B for $0 \leq i \leq n$ the size $l(b_{i,j}) = 0(n \log(N))$ and for $n+1 \leq i \leq n+k+2$ the size $l(b_{i,j}) \leq M + 0(k \log(d))$. Hence, $l(R) \leq (M + \log(Nd))\mathscr{P}(d_1, n)$ because of the bounds on the parameters of a determinant (see, e.g. Heintz, 1983; also Chistov & Grigor'ev, 1983, 1984).

The coefficients of the operator R are the minors of the matrix B. We can carry out their calculation with the aid of the Gaussian algorithm. Define (see Heintz, 1983; Chistov & Grigor'ev, 1983, 1984; Grigor'ev, 1986) a variant of Gaussian algorithm (VGA) Γ as a succession of pairs of indices $(\alpha_0, \beta_0), \ldots, (\alpha_{\omega-1}, \beta_{\omega-1})$ where $\alpha_0, \ldots, \alpha_{\omega-1}$ are pairwise distinct as well as $\beta_0, \ldots, \beta_{\omega-1}$. VGA Γ generates a chain of matrices $B^{(0)} = B, B^{(1)}, \ldots, B^{(\omega)}$ each obtained from the preceding one by an elementary transformation of the rows, denote

$B^{(\nu)} = (b^{(\nu)}_{\alpha,\beta})$. We have $b^{(\nu+1)}_{\alpha,\beta} = b^{(\nu)}_{\alpha,\beta} - b^{(\nu)}_{\alpha,\beta_\nu} b^{(\nu)}_{\alpha_\nu,\beta} / b^{(\nu)}_{\alpha_\nu,\beta_\nu}$ for $\alpha \neq \alpha_0, \ldots, \alpha_\nu$ distinguished from $\alpha_0, \ldots, \alpha_\nu$, moreover $b^{(\nu)}_{\alpha_\nu,\beta_\nu} \neq 0$. Then $b^{(\nu)}_{\alpha,\beta_\mu} = 0$ when $\mu < \nu$, provided that $\alpha \neq \alpha_0, \ldots, \alpha_\mu$. For $\alpha \neq \alpha_0, \ldots, \alpha_{\nu-1}$, $\beta \neq \beta_0, \ldots, \beta_{\nu-1}$ denote by $\Delta_{\alpha,\beta}$ the determinant (the minor) of the $(\nu+1)\times(\nu+1)$ submatrix of the matrix B formed by the rows $\alpha_0, \ldots, \alpha_{\nu-1}, \alpha$ and the columns $\beta_0, \ldots, \beta_{\nu-1}, \beta$. Then $b^{(\nu)}_{\alpha,\beta} = \Delta^{(\nu)}_{\alpha,\beta} / \Delta^{(\nu-1)}_{\alpha_{\nu-1},\beta_{\nu-1}}$ (see, e.g. Bereiss, 1968; Heintz, 1983). Because of this, while carrying out Gaussian algorithm every entry of an intermediate matrix $B^{(\nu)}$ is a ratio of two minors of the initial matrix B, that implies a bound on the degrees and on the sizes of coefficients of an entry and also on the time-bound of carrying our VGA and of calculating any minor of the matrix B. The time-bound is polynomial in the maximal bit-size of the minors of B. Therefore, the time required to calculate R does not exceed $\mathscr{P}(M, (Nn)^n, d, d_1)$, this completes the proof of Lemma 4.1.

COROLLARY. *Let the operator R_0 correspond to the operators L, Q_0 as in Lemma* 4.1, *a field $F_1 \subset \mathbb{C}$, a point $a \in \mathbb{C}$ be non-singular both for the operator L and for the operator R_0. Let v be some solution of the equation $Lv = 0$. Consider an expansion of the regular function*

$$Q_0 v = \sum_{i \geq 0} q_i (X-a)^i$$

in a neighbourhood on the complex plane of the point a, where $q_i \in \mathbb{C}$ (note that v and hence $Q_0 v$ are both regular in a neighbourhood of a, see Olver, 1974). *The equality $Q_0 v = 0$ is true iff $q_0 = \ldots = q_{n-1} = 0$.*

PROOF. Apply the uniqueness of the solution of an equation with given values at the point a for its kth derivatives where $0 \leq k \leq n-1$ (see, e.g. Olver, 1974) to the operator R_0. Taking into account that $R_0 Q_0 v = 0$, this proves the corollary.

Now we proceed to describing a factoring algorithm. Introduce indeterminates $a, v^{(1)}_0, \ldots, v^{(1)}_{n-1}, \ldots, v^{(k)}_0, \ldots, v^{(k)}_{n-1}$ algebraically independent over the field $F(c_{0,0}, \ldots, c_{0,N}, \ldots, c_{k,0}, \ldots, c_{k,N})$. Let R correspond to the operators L, Q according to Lemma 4.1. Our next goal is to express in a parametric form the condition that for given complex numbers $\tilde{c}_{0,0}, \ldots, \tilde{c}_{k,N}, \tilde{a}, \tilde{v}^{(1)}_0, \ldots, \tilde{v}^{(1)}_{n-1}, \ldots, \tilde{v}^{(k)}_0, \ldots, \tilde{v}^{(k)}_{n-1}$ the point $\tilde{a}$ is non-singular for the operators L and $\tilde{R}$ which corresponds to the operator

$$\tilde{Q} = \sum_{0 \leq i \leq k} \left(\sum_{0 \leq j \leq N} \tilde{c}_{i,j} X^j \right) D^i$$

according to Lemma 4.1, and also that the solutions

$$\tilde{v}^{(m)} = \tilde{v}^{(m)}_0 + \tilde{v}^{(m)}_1 (X-\tilde{a}) + \ldots + \tilde{v}^{(m)}_{n-1} (X-\tilde{a})^{n-1} + \ldots$$

of the equation $Lv = 0$ for $1 \leq m \leq k$ constitute a basis of the space (over $\mathbb{C}$) of solutions of the equation $\tilde{Q}v = 0$. It is well known (see, e.g. Olver, 1974) that for any $\tilde{v}_0, \ldots, \tilde{v}_{n-1}$ there exists a unique solution of the equation $Lv = 0$ of the form $\tilde{v}_0 + \tilde{v}_1 (X-\tilde{a}) + \ldots + \tilde{v}_{n-1} (X-\tilde{a})^{n-1} + \ldots$. In the following, while parametrically expressing the desired condition, we shall omit tilde in the notations of indeterminates and operators and sometimes use the same notations for an indeterminate and for its complex value, when this does not lead to misunderstanding.

The condition that a is a non-singular point of the operator L can be written as $f_n(a) \neq 0$,

the condition that a is a non-singular point of R can be written in the form $(lc(R))(a) \neq 0$, by virtue of Lemma 4.1

$$\deg_a(lc(R)) < (n+1)N + (k+1)d,$$

$$\deg_{c_{0,0},\ldots,c_{k,N}}(lc(R)) \leq n+1,\ l(lc(R)) \leq (M+\log(Nd))\mathscr{P}(d_1, n).$$

Lastly, pick out an arbitrary $k \times k$ minor in $k \times n$ matrix $(v_i^{(m)})_{1 \leq m \leq k,\, 0 \leq i \leq n-1}$ and denote by

$$\psi \in F[c_{0,0}, \ldots, c_{k,N}, a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)}]$$

the product of this minor with the polynomials $f_n(a)$ and $lc(R)$. Then

$$\deg_a(\psi) \leq (n+1)(N+d);\quad \deg_{c_{0,0},\ldots,c_{k,n}}(\psi) \leq n+1;$$

$$\deg_{v_0^{(1)},\ldots,v_{n-1}^{(k)}}(\psi) \leq k < n;\quad l(\psi) \leq (M+\log(Nd))\mathscr{P}(d_1, n).$$

The algorithm yields the polynomial ψ within time $\mathscr{P}(M, (Nn)^n, d, d_1)$ because of Lemma 4.1. Thus, we have to express the condition that $Qv^{(m)} = 0$ for $1 \leq m \leq k$ (recall that $Lv^{(m)} = 0$) and that $\psi \neq 0$. Observe that if $(lc(R))(a) \neq 0$ then $Q \not\equiv 0$, since $lc(R)$ is a certain $(n+k+1) \times (n+k+1)$ minor of the matrix B (see the proof of Lemma 4.1).

One can express v_s for $s \geq 0$ via $v_0, \ldots, v_{n-1}$ such that

$$v = \sum_{s \geq 0} v_s (X-a)^s$$

satisfies the equation $Lv = 0$. Rewrite the operator

$$L = \sum_{0 \leq i \leq n} \left(\sum_{0 \leq j < d} (X-a)^j \sum_{0 \leq t < d-j} \binom{t+j}{j} f_{i,t+j} a^t \right) D^i,$$

where the polynomial

$$f_i = \sum_{0 \leq j < d} f_{i,j} X^j.$$

Then

$$Lv = \sum_{s \geq 0} (X-a)^s \left(\sum_{0 \leq i \leq n} \sum_{0 \leq j < d;\, j \leq s} \sum_{0 \leq t < d-j} \binom{t+j}{j} f_{i,t+j} a^t \binom{s+i-j}{i} i!\, v_{s+i-j} \right).$$

The equation $Lv = 0$ entails a linear system in the unknowns v_t for $t \geq n$, that is triangular: namely, in the sth equation ($s \geq 0$) only v_t for $t \leq s+n$ occur and, furthermore, the coefficient of the unknown v_{s+n} equals

$$f_n(a) \binom{s+n}{n} n! \neq 0.$$

Therefore, solving this linear system the algorithm can find for $s = 0, 1, \ldots$ successively

$$v_{s+n} = (f_n(a))^{-s-1} \sum_{0 \leq i \leq n} v_i g_{s+n,i},$$

where the polynomials $g_{s+n,i} \in F[a]$. Moreover, the following bounds are valid (cf. the proof of Lemma 4.1):

$$\deg_a(g_{s+n,i}) < (s+1)d;\quad l(g_{s+n,i}) \leq (M+d)\mathscr{P}(d_1, n, s),$$

and the algorithm can find $g_{s+n,i}$ within time $\mathscr{P}(M, d, d_1, n, s)$.

Similarly,

$$Q = \sum_{0 \leq i \leq k} \left(\sum_{0 \leq j \leq N} (X-a)^j \sum_{0 \leq t \leq N-j} \binom{t+j}{j} c_{i,t+j} a^t \right) D^i,$$

write

$$Qv = q_s = \sum_{0\le i\le k;\,0\le j\le N;\,j\le s;\,0\le t\le N-j} \binom{t+j}{j} c_{i,t+j}a^t \binom{s+i-j}{i} i!\, v_{s+i-j}$$

$$= (f_n(a))^{-s} \sum_{0\le i\le n;\,0\le j\le k;\,0\le t\le N} c_{j,t}v_i g_{s,i,j,t}$$

for suitable polynomials $g_{s,i,j,t}\in F[a]$, furthermore,

$$\deg_a(g_{s,i,\,j,t}) < N+(s+1)d; \quad l(g_{s,i,j,t}) \le (M+d+N)\mathscr{P}(d_1, n, s)$$

algorithm can find $g_{s,i,j,t}$ within time $\mathscr{P}(M, N, d, d_1, n, s)$. For the solution

$$v^{(m)} = \sum_{i\ge 0} v_i^{(m)}(X-a)^i$$

of the equation $Lv=0$, $1\le m\le k$, one can write analogously

$$Qv^{(m)} = \sum_{s\ge 0} q_s^{(m)}(X-a)^s$$

and express $q_s^{(m)}$ via $v_0^{(m)}, \ldots, v_{n-1}^{(m)}$. Involving the corollary from Lemma 4.1, we summarise in the following lemma what we proved above (keeping the same notation as above). Note that the operator $Q\not\equiv 0$ is a right divisor of the operator L iff any solution of the equation $Qv=0$ satisfies the equation $Lv=0$.

LEMMA 4.2. *An operator L has a right divisor of order k in the ring $\mathbb{C}(X)[D]$ iff there exist $c_{0,0}, \ldots, c_{0,N}, \ldots, c_{k,0}, \ldots, c_{k,N}, a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)} \in \mathbb{C}$ and that the following equalities hold (see above the formula for q_s):*

$$(f_n(a))^s q_s^{(m)} \equiv \sum_{0\le i\le n;\,0\le j\le k;\,0\le t\le N} c_{j,t}v_i^{(m)}g_{s,i,j,t} = 0 \quad \text{for } 1\le m\le k,\ 0\le s<n. \tag{6}$$

Note that under the conditions formulated in the lemma, $ord(Q)=k$ is true, since $Q\not\equiv 0$ and the equation $Qv=0$ has k linearly independent solutions $v^{(1)}, \ldots, v^{(k)}$ because of the corollary from Lemma 4.1.

We shall consider (6) as a system of kn linear (algebraic) equations in $(k+1)(N+1)$ indeterminates $c_{0,0}, \ldots, c_{k,N}$ with coefficients in the field $F(a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)})$ and we denote the matrix of this linar system by $A=(a_{\alpha,\beta})$. To parametrically solve this system (see Heintz, 1983; also Chistov & Grigor'ev, 1984; Grigor'ev, 1986) the algorithm yields recursively a succession of VGA $\Gamma_1, \Gamma_2, \ldots$ (cf. the proof of Lemma 4.1) and a corresponding succession of the polynomials $P_1, P_2, \ldots \in F[a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)}]$. Assume that $\Gamma_1, \ldots, \Gamma_l$; $P_1, \ldots, P_l$ are already found for a certain $l\ge 0$. While yielding Γ_{l+1} (and P_{l+1}) we utilize the same notations as above for Γ with the matrix B being replaced by A (see the proof of Lemma 4.1). Let the pairs of indices $(\alpha_0, \beta_0), \ldots, (\alpha_\nu, \beta_\nu)$ be already produced. Then the next pair $(\alpha_{\nu+1}, \beta_{\nu+1})$ is taken with the property that the product $\prod_{0\le\mu\le\nu+1}\Delta^{(\mu)}_{\alpha_\mu,\beta_\mu}$ (cf. the proof of Lemma 4.1) is linearly independent over the field F with the polynomials $P_1, \ldots, P_l$. When it is impossible to take $(\alpha_{\nu+1}, \beta_{\nu+1})$ satisfying this property, we consider VGA $\Gamma_{l+1} = \{(\alpha_0, \beta_0), \ldots, (\alpha_\nu, \beta_\nu)\}$ to be already completed and set $P_{l+1} = \prod_{0\le\mu\le\nu}\Delta^{(\mu)}_{\alpha_\mu,\beta_\mu}$. If it is impossible even to take (α_0, β_0), i.e. each entry of the matrix A is linearly dependent over F with the polynomials $P_1, \ldots, P_l$, then the algorithm ends yielding $\Gamma_1, \ldots, \Gamma_l$; $P_1, \ldots, P_l$. Let VGA $\Gamma_\kappa = \{(\alpha_0^{(\kappa)}, \beta_0^{(\kappa)}), \ldots, (\alpha^{(\kappa)}_{\omega_\kappa-1}, \beta^{(\kappa)}_{\omega_\kappa-1})\}$.

Consider a quasi-projective (see Shafarevich, 1974) variety

$$W_\kappa = \{w = (a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)}) \in \mathbb{C}^{kn+1} : P_\kappa(w) \neq 0, P_1(w) = \ldots = P_{\kappa-1}(w) = 0\}$$

for $1 \leq \kappa \leq l$ and $W_{l+1} = \{w : P_1(w) = \ldots = P_l(w) = 0\}$.

Obviously, $\cup_{1 \leq \kappa \leq l+1} W_\kappa = \mathbb{C}^{kn+1}$ and $W_{\kappa_1} \cap W_{\kappa_2} = \phi$ for $\kappa_1 \neq \kappa_2$. Observe that for any point $w \in W_\kappa$ VGA Γ_κ can be applied correctly to the matrix $A(w)$ obtained from A by plugging the co-ordinates of the point w instead of indeterminates $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$, and the result of applying Γ_κ is the matrix $A^{(\omega_\kappa)}(w) = (a_{\alpha,\beta}^{(\omega_\kappa)}(w))$. Note that the matrix $A^{(\omega_\kappa)}$ depends as a matter of fact on κ. For $1 \leq \kappa \leq l$ holds $a_{\alpha,\beta}^{(\omega_\kappa)}(w) = 0$ if $\alpha \neq \alpha_0^{(\kappa)}, \ldots, \alpha_{\omega_\kappa - 1}^{(\kappa)}$, apart from that $a_{\alpha_\mu^{(\kappa)}, \beta_\nu^{(\kappa)}}^{(\omega_\kappa)}(w) = 0$ when $\mu < \nu$. In other words the matrix $A^{(\omega_\kappa)}(w)$ has a form of trapezium, moreover, $\omega_\kappa \times \omega_\kappa$ minor $\Delta^{(\omega_\kappa - 1)}_{\alpha_0^{(\kappa)}, \ldots, \alpha_{\omega_\kappa - 1}^{(\kappa)}, \beta_0^{(\kappa)}, \ldots, \beta_{\omega_\kappa - 1}^{(\kappa)}}(w) \neq 0$ and the rank $rg(A(w)) = rg(A^{(\omega_\kappa)}(w)) = \omega_\kappa$.

In particular, $\omega_\kappa \leq kn$ (see (6)). For a point $w \in W_{l+1}$ the matrix $A(w) = 0$, so let $\omega_{l+1} = 0$.

Thereafter, the algorithm finds the general form of the solution $C = (c_{0,0}, \ldots, c_{0,N}, \ldots, c_{k,0}, \ldots, c_{k,N})$ of the linear system (6) for the points $w \in W_\kappa$. Namely, denote $N_1 = (N+1)(k+1) - \omega_\kappa$ and introduce new indeterminates $c_1, \ldots, c_{N_1}$ corresponding to the columns of the matrix A different from $\beta_0^{(\kappa)}, \ldots, \beta_{\omega_\kappa - 1}^{(\kappa)}$. Then the vector C contains co-ordinates $c_1, \ldots, c_{N_1}$ at the places distinguished from $\beta_0^{(\kappa)}, \ldots, \beta_{\omega_\kappa - 1}^{(\kappa)}$, respectively. The co-ordinate at the place $\beta_j^{(\kappa)}$ for $0 \leq j \leq \omega_\kappa - 1$ of the vector C equals to $\sum_{1 \leq t \leq N_1} c_t \Delta_{j,t} / \Delta_{\alpha_0^{(\kappa)}, \ldots, \alpha_{\omega_\kappa - 1}^{(\kappa)}, \beta_0^{(\kappa)}, \ldots, \beta_{\omega_\kappa - 1}^{(\kappa)}}$ where $\Delta_{j,t}$ is a minor of the matrix A formed by the rows $\alpha_0^{(\kappa)}, \ldots, \alpha_{\omega_\kappa - 1}^{(\kappa)}$ and by the columns $\beta_0^{(\kappa)}, \ldots, \beta_{j-1}^{(\kappa)}, \beta_{j+1}^{(\kappa)}, \ldots, \beta_{\omega_\kappa - 1}^{(\kappa)}$ and by the column corresponding to the indeterminate c_t. For any minor Δ of the matrix A the following bounds are valid (see (6) and the proof of Lemma 4.1):

$$\deg_a(\Delta) < (N + (n+1)d)n^2;$$

$$\deg_{v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)}}(\Delta) < n^2; \quad l(\Delta) \leq (M + d + N)\mathscr{P}(d_1, n)$$

by virtue of the bounds on the parameters of $g_{s,i,j,t}$ indicated just before Lemma 4.2. Hence,

$$\deg_a(P_\kappa) < (N + (n+1)d)n^4;$$

$$\deg_{v_0^{(1)}, \ldots, v_{n-1}^{(k)}}(P_\kappa) < n^4; \quad l(P_\kappa) \leq (M + d + N)\mathscr{P}(d_1, n).$$

Because of that the number l of the polynomials $P_1, \ldots, P_l$ is at most $(N + (n+1)d)n^4 n^{4n^2} \leq (N+d)\mathscr{P}(n^{n^2})$ since they are linearly independent over F. Therefore, the time required to yield all $\Gamma_1, \ldots, \Gamma_l$; $P_1, \ldots, P_l$ and the general solution C of the linear system (6) does not exceed $\mathscr{P}(M, N, d, d_1, n^{n^2})$, taking into account that every entry of an intermediate (while carrying out some VGA) matrix is a ratio of two appropriate minors of the initial matrix A (cf. the proof of Lemma 4.1).

Fix some $1 \leq \kappa \leq l+1$. Consider a closed (here and further the Zariski topology is meant, see, e.g. Shafarevich, 1974) variety

$$\{w = (a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)}) \in \mathbb{C}^{kn+1} : P_1(w) = \ldots = P_{\kappa-1}(w) = 0\}$$

and relying on Proposition 1.5 (see the Introduction) find its irreducible components $\bar{V}_{\kappa,s}$ over the field F (when $\kappa = 1$ the single component $\bar{V}_{1,1} = \mathbb{C}^{kn+1}$). Evidently, $W_\kappa = \cup_s (\bar{V}_{\kappa,s} \setminus \{w : P_\kappa(w) = 0\})$. The algorithm from Proposition 1.5 represents every component $\bar{V} = \bar{V}_{\kappa,s}$ of a dimension $0 \leq p \leq kn+1$ by its general point (see (*) before Proposition 1.5), i.e. it gives the following isomorphism of the field $F(\bar{V})$ of rational functions on the variety $\bar{V}$:

$$F(T_1, \ldots, T_p)[\Theta_0] \simeq F(a, v_0^{(1)}, \ldots, v_{n-1}^{(1)}, \ldots, v_0^{(k)}, \ldots, v_{n-1}^{(k)}) = F(\bar{V}), \tag{7}$$

where $T_1, \ldots, T_p \in \{a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}\}$ are algebraically independent over F, the element Θ_0 is

algebraic over $F(T_1, \ldots, T_p)$ with $\phi(Z) \in F[T_1, \ldots, T_p][Z]$ is its minimal polynomial, and

$$\Theta_0 \leftarrow \lambda a + \sum_{0 \le i \le n-1,\, 1 \le m \le k} \lambda_i^{(m)} v_i^{(m)}$$

by isomorphism (7) for appropriate integers $1 \le \lambda, \lambda_i^{(m)} \le \deg_Z(\phi)$ (here $a, v_i^{(m)}$ are considered as the rational (co-ordinate) functions on $\bar{V}$).

The algorithm represents the isomorphism (7) by means of the images of the co-ordinate functions $a_1/a_2 \leftarrow a, v_{0,1}^{(1)}/v_{0,2}^{(1)} \leftarrow v_0^{(1)}, \ldots, v_{n-1,1}^{(1)}/v_{n-1,2}^{(k)} \leftarrow v_{n-1}^{(k)}$ under the isomorphism (7), where $a_2, v_{0,2}^{(1)}, \ldots, v_{n-1,2}^{(k)} \in F[T_1, \ldots, T_p]$ and $a_1, v_{0,1}^{(1)}, \ldots, v_{n-1,1}^{(k)} \in F[T_1, \ldots, T_p, \Theta_0]$. The algorithm also specifies $\lambda, \lambda_i^{(m)}$ and $T_1, \ldots, T_p$. Proposition 1.5 implies the following bounds (taking into account the bounds on the parameters of the polynomials $P_1, \ldots, P_l$):

$$\deg_Z(\phi) \le (Nd)^{n^2} \mathscr{P}(n^{n^2});$$

$$\deg_{T_1,\ldots,T_p}(\phi), \deg_{T_1,\ldots,T_p}(a_1/a_2), \deg_{T_1,\ldots,T_p}(v_{i,1}^{(m)}/v_{i,2}^{(m)}) \le \mathscr{P}((Ndn)^{n^2}, d_1);$$

$$l(\phi), l(a_1/a_2), l(v_{i,1}^{(m)}/v_{i,2}^{(m)}) \le M \mathscr{P}((Ndn)^{n^2}, d_1).$$

The time required to produce isomorphism (7) does not exceed $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2})$.

The algorithm then checks to see if the quasi-projective variety

$$V = \bar{V} \setminus \{w : P_\kappa(w) = 0\} \subset W_\kappa$$

is non-empty (in this case $\bar{V}$ is the closure of V). We have, by virtue of Chistov & Grigor'ev (1983) (cf. also Shafarevich, 1974) $V = \phi$ iff after plugging in the polynomial P_κ instead of the indeterminates $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$ the images $a_1/a_2, v_{0,1}^{(1)}/v_{0,2}^{(1)}, \ldots, v_{n-1,1}^{(k)}/v_{n-1,2}^{(k)} \in F(T_1, \ldots, T_p)[\Theta_0]$ respectively, under isomorphism (7), the zero element of the field $F(T_1, \ldots, T_p)[\Theta_0]$ would be obtained (cf. below, Lemma 4.3). We now assume that $V = \emptyset$. Then the algorithm finds the discriminant $\mathscr{D} \in F[T_1, \ldots, T_p]$ of the polynomial ϕ relatively to the variable Z by calculating the determinant of the Sylvester matrix (see, e.g. van der Waerden, 1971; Loos, 1982, and also section 5, below) of the polynomials $\phi, D\phi$ (certainly $\mathscr{D} \not\equiv 0$ since ϕ is irreducible). Hence, for the parameters of the polynomial $\mathscr{D}$ similar bounds as for ϕ (see above) are valid (see the proof of Lemma 4.1).

Next, for the polynomial ψ that we have constructed (see Lemma 4.2 and the construction preceding it) replace the indeterminants $c_{0,0}, \ldots, c_{k,N}$ by the general form C of the solution of the linear system (6). As a result one obtains a rational function of the form ψ_0/P_κ^λ for a suitable natural number $\lambda \le n+1$, where the polynomial $\psi_0 \in F[c_1, \ldots, c_{N_1}, a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}]$, furthermore, in force of the proved above bounds the following bounds are true:

$$\deg_{c_1,\ldots,c_{N_1}}(\psi_0) \le n+1; \quad \deg_a(\psi_0) \le (N+d)\mathscr{P}(n);$$

$$\deg_{v_0^{(1)},\ldots,v_{n-1}^{(k)}}(\psi_0) \le \mathscr{P}(n); \quad l(\psi_0) \le (M+d+N)\mathscr{P}(d_1, n).$$

The number of terms of the polynomial ψ_0 is at most $\mathscr{P}(N^n, n^{n^2}, d, d_1)$, therefore one can produce the polynomial ψ_0 within time $\mathscr{P}(M, N^n, n^{n^2}, d, d_1)$.

According to Lemma 4.2, in order to find out whether there is a right divisor of L with the order k, it suffices to test for the existence of a point $w \in V$ such that after plugging its co-ordinates into the polynomial ψ_0 for the indeterminates $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$ respectively, the new polynomial $\psi_0(w) \in \mathbb{C}[c_1, \ldots, c_{N_1}]$ does not vanish identically (then use any $c_1, \ldots, c_{N_1} \in \mathbb{C}$ such that $\psi_0(w)(c_1, \ldots, c_{N_1}) \neq 0$). Provided that there exists such a point w, the variety of the points with the desired property contains an open dense subset V_0 in V, since the closure $\bar{V}$ is irreducible (see Shafarevich, 1974). Therefore, if some set $V_1 \subset V$

contains an open dense subset in V, then it is sufficient to seek a point w with the desired property (i.e. from V_0) just in the set V_1 as $V_0 \cap V_1 \neq \phi$ contains again an open dense subset in V. The algorithm then produces explicitly a certain open dense subset $V_1 \subset V$ in the following manner.

Consider the quasi-projective variety

$$U = \{u = (\tilde{T}_1, \ldots, \tilde{T}_p, \tilde{\theta}) \in \mathbb{C}^{p+1} : \phi(u) = 0, (\mathscr{D} lc_Z(\phi) a_2 v_{0,2}^{(1)} \ldots v_{n-1,1}^{(k)})(u) \neq 0\}$$

(cf. (7)) and a rational mapping $\pi : \mathbb{C}^{p+1} \to \mathbb{C}^{kn+1}$ defined by the formula

$$\pi(u) = (a_1/a_2, v_{0,1}^{(1)}/v_{0,2}^{(1)}, \ldots, v_{n-1,1}^{(k)}/v_{n-1,2}^{(k)})(u).$$

Note that $\mathscr{D} lc_Z(\phi) a_2 v_{0,2}^{(1)}, \ldots, v_{n-1,2}^{(k)}$ depends only on $\tilde{T}_1, \ldots, \tilde{T}_p$.

LEMMA 4.3. *$\pi(U) \subset V$ and $\pi(U)$ contains an open dense set in $\bar{V}$.*

PROOF. If $h \in F[a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}]$ vanishes everywhere on $\bar{V}$, then $h(a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}) = 0$ where $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$ are now thought of as elements of $F(\bar{V})$. Taking (7) into account, if we replace $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$ with the rational functions $a_1(Z)/a_2, v_{0,1}^{(1)}(Z)/v_{0,2}^{(1)}, \ldots, v_{n-1,1}^{(k)}(Z)/v_{n-1,2}^{(k)} \in F[T_1, \ldots, T_p][Z]$, where the element Θ_0 is replaced by the variable Z, we obtain a rational function $E_h \in F[T_1, \ldots, T_p][Z]$ whose denominator is a monomial in $a_2, v_{0,2}^{(1)}, \ldots, v_{n-1,2}^{(k)}$.

Since the field $F(T_1, \ldots, T_p)[\Theta_0] \simeq F(T_1, \ldots, T_p)[Z]/(\phi)$, the polynomial ϕ divides E_h in the ring $F(T_1, \ldots, T_p)[Z]$. Dividing E_h by ϕ yields the equality $E_h = \phi E$ where the denominator of the rational function $E \in F(T_1, \ldots, T_p)[Z]$ is a monomial in $lc_Z(\phi), a_2, v_{0,2}^{(1)}, \ldots, v_{n-1,2}^{(k)}$. Hence, for every point $u \in U$ the following is correct

$$h((a_1/a_2, v_{0,1}^{(1)}/v_{0,2}^{(1)}, \ldots, v_{n-1,1}^{(k)}/v_{n-1,2}^{(k)})(u)) = E_h(u) = \phi(u) = 0.$$

In other words, $h(\pi(U)) = 0$, whence $\pi(U) \subset \bar{V}$ in force of arbitrariness of the choice of h vanishing on $\bar{V}$ (see, e.g. Shafarevich, 1974).

Observe that the mapping π gives an isomorphism of the fields of rational functions $F(\bar{V})$ and $F(U)$ by virtue of (7). Therefore, $\dim(\bar{V}) = \dim(\pi(U))$ and $\pi(U)$ contains an open dense subset in $\bar{V}$ (see Shafarevich, 1974). Lemma 4.3 is proved.

Therefore, for the subset $V_1 \subset V$ promised above, one can now take $\pi(U) \cap V$. Thus, the algorithm has to find out whether there exists a point $w \in \pi(U) \cap V$ such that $\psi_0(w) \not\equiv 0$. The latter is fulfilled iff for an appropriate point $u \in U$ an inequality $(P_\kappa \psi_0)(\pi(u)) \not\equiv 0$ is true. Replace the indeterminants $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$ in the polynomial $P_\kappa \psi_0$ by the rational functions $a_1(Z)/a_2\ v_{0,1}^{(1)}(Z)/v_{0,2}^{(1)}, \ldots, v_{n-1,1}^{(k)}(Z)/v_{n-1,2}^{(k)}$, in which Θ_0 (see (7)) is replaced by Z (cf. the proof of Lemma 4.3). As a result a rational function ξ/ζ is obtained, where the polynomial $\xi \in F[c_1, \ldots, c_{N_1}, T_1, \ldots, T_p, Z]$ and the denominator ζ is a monomial in $a_2, v_{0,2}^{(1)}, \ldots, v_{n-1,2}^{(k)}$. The algorithm divides ξ by ϕ with a remainder (with the aid of, e.g. Loos, 1982): $\xi = \phi\xi_1/(lc_Z(\phi))^{t_1} + \xi_2/(lc_Z(\phi))^{t_2}$ where $t_1, t_2 \geq 0$ are natural numbers, the polynomials $\xi_1, \xi_2 \in F[c_1, \ldots, c_{N_1}, T_1, \ldots, T_p, Z]$ and $\deg_Z(\xi_2) < \deg_Z(\phi)$.

Obviously, for any point $u \in U$ the following equivalence is valid: $\xi(u) \equiv 0$ iff $\xi_2(u) \equiv 0$ (evidently, $(P_\kappa \psi_0)(\pi(u)) = (\xi/\zeta)(u)$). Denote the polynomial

$$\Omega = \xi_2 \mathscr{D} lc_Z(\phi) a_2 v_{0,2}^{(1)} \ldots v_{n-1,2}^{(k)} \in F[c_1, \ldots, c_{N_1}, \ldots, T_1, \ldots, T_p, Z].$$

The following bounds hold:

$$\deg_Z(\Omega) < \deg_Z(\phi) \le (Nd)^{n^2}\mathscr{P}(n^{n^2}), \quad \deg_{c_1,\ldots,c_{N_1}}(\Omega) \le n+1;$$

$$\deg_{T_1,\ldots,T_p}(\Omega) \le \mathscr{P}((Ndn)^{n^2}, d_1); \quad l(\Omega) \le M\mathscr{P}((Ndn)^{n^2}, d_1)$$

and the algorithm produces Ω within time $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2})$, taking into account that the coefficients of the remainder after dividing by ϕ (i.e. while calculating ξ_2) are, in fact, suitable minors of the Sylvester matrix of the polynomials ϕ, ξ (see van der Waerden, 1971; Loos, 1982, also section 5, below), and then using the same argument as above in the proof of Lemma 4.1.

Using Lemmas 4.2, 4.3 and continuing with the above notations one can deduce the following:

LEMMA 4.4. *An operator L has a right divisor of order k in the ring $\mathbb{C}(X)[D]$ iff for an appropriate $k \times k$ minor of the $k \times n$ matrix $(v_i^{(m)})$, and index $1 \le \kappa \le l+1$ and an irreducible component $\bar{V} = \bar{V}_{\kappa,s}$ (such that $V = \bar{V} \setminus \{w : P_\kappa(w) = 0\} \neq \emptyset$) there exist $\tilde{c}_1, \ldots, \tilde{c}_{N_1}, \tilde{T}_1, \ldots, \tilde{T}_p, \tilde{\theta} \in \mathbb{C}$ for which $\phi(\tilde{T}_1, \ldots, \tilde{T}_p, \tilde{\theta}) = 0$ and $0 \neq \Omega(\tilde{c}_1, \ldots, \tilde{c}_{N_1}, \tilde{T}_1, \ldots, \tilde{T}_p, \tilde{\theta})$ (under these conditions a point $w = \pi(\tilde{T}_1, \ldots, \tilde{T}_p, \tilde{\theta}) \in \pi(U) \cap V$).*

Furthermore, we show, provided that $\Omega \not\equiv 0$, that there exist integers $0 \le \tilde{c}_1, \ldots, \tilde{c}_{N_1} \le n+1$; $0 \le \tilde{T}_1, \ldots, \tilde{T}_p \le \mathscr{P}((Ndn)^{n^2}, d_1)$ and $\tilde{\theta} \in \mathbb{C}$ satisfying Lemma 4.4 and describe an algorithm for producing them. Denote the indeterminates $Z_j = c_j$ for $1 \le j \le N_1$ and $Z_{N_1+i} = T_i$ for $1 \le i \le p$, and construct a succession of polynomials $\Omega_0, \ldots, \Omega_{N_1+p}$ such that $0 \not\equiv \Omega_j \in F[Z_1, \ldots, Z_j]$ and $\Omega_{j-1} = lc_{Z_j}(\Omega_j)$ for $1 \le j \le N_1 + p$. Furthermore, $\Omega_{N_1+p} = lc_Z(\Omega)$ (obviously, the parameters of Ω_j satisfy similar bounds as those of Ω, see above). Assume that by recursion on j (for $1 \le j \le N_1 + p$) the integers $\tilde{Z}_1, \ldots, \tilde{Z}_{j-1}$ are already produced satisfying the specified bounds above and such that $\Omega_{j-1}(\tilde{Z}_1, \ldots, \tilde{Z}_{j-1}) \neq 0$. Denote $\tilde{Z} = (\tilde{Z}_1, \ldots, \tilde{Z}_{j-1})$. Replacing the indeterminants Z_j in the polynomial $\Omega_j(\tilde{Z}, Z_j) \in F[Z_j]$ with integers z_j where either $0 \le z_j \le \deg_{c_1,\ldots,c_{N_1}}(\Omega) \le n+1$ when $1 \le j \le N_1$ or $0 \le z_j \le \deg_{T_1,\ldots,T_p}(\Omega) \le \mathscr{P}((Ndn)^{n^2}, d_1)$ when $N_1 + 1 \le j \le N_1 + p$, the algorithm finds $\tilde{Z}_j$ such that $\Omega_j(\tilde{Z}, \tilde{Z}_j) \neq 0$ since $\deg_{Z_j}(\Omega_j(\tilde{Z}, Z_j)) \le \deg_{Z_j}(\Omega)$, this completes the recursive step. Taking into account that Ω contains at most $\mathscr{P}((Ndn)^{n^4}, d_1^{n^2})$ terms, the size $l(\Omega_j(\tilde{Z}, Z_j)) \le M\mathscr{P}((Ndn)^{n^2}, d_1)$, hence, the algorithm produces the vectors $\tilde{c} = (\tilde{c}_1, \ldots, \tilde{c}_{N_1})$, $\tilde{T} = (\tilde{T}_1, \ldots, \tilde{T}_p)$ (where $(\tilde{c}, \tilde{T}) = (\tilde{Z}_1, \ldots, \tilde{Z}_{N_1+p})$) for which $\Omega_{N_1+p}(\tilde{c}, \tilde{T}) \neq 0$, within time $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2})$.

From the definition of Ω we have $(\mathscr{D} lc_Z(\phi))(\tilde{T}) \neq 0$.

Consider the polynomials $\tilde{\Omega}(Z) = \Omega(\tilde{c}, \tilde{T}, Z)$, $\tilde{\phi}(Z) = \phi(\tilde{T}, Z) \in F[Z]$, then $lc_Z(\tilde{\Omega}) = (lc_Z(\Omega))(\tilde{c}, \tilde{T}) \neq 0$ and $lc_Z(\tilde{\phi}) = (lc_Z(\phi))(\tilde{T}) \neq 0$, and because of this $\deg_Z(\tilde{\Omega}) = \deg_Z(\Omega) < \deg_Z(\phi) = \deg_Z(\tilde{\phi})$. The algorithm produces $\tilde{\Omega}, \tilde{\phi}$ within time $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2})$ (cf. above). The polynomial $\tilde{\phi}$ has no multiple roots, as its discriminant $\mathscr{D}(\tilde{T}) \neq 0$. Relying on Proposition 1.4 (see the Introduction), the algorithm factors $\tilde{\phi}$ over the field F within time $\mathscr{P}(M, (Ndn)^{n^2}, d_1)$. There is an irreducible (over F) factor $\tilde{\phi}_0 | \tilde{\phi}$ which is relatively prime to $\tilde{\Omega}$ (since $\deg(\tilde{\Omega}) < \deg(\tilde{\phi})$) and the latter can be tested with the help of calculating GCDs (see, e.g. Loos, 1982, also section 5, below) within time $\mathscr{P}(M, (Ndn)^{n^2}, d_1)$, taking into account that Proposition 1.4 implies the bound $l(\tilde{\phi}_0) \le M\mathscr{P}((Ndn)^{n^2}, d_1)$. Letting $\tilde{\theta} \in \mathbb{C}$ be a root of the polynomial $\tilde{\phi}_0$, the tuple $(\tilde{c}, \tilde{T}, \tilde{\theta})$ satisfies Lemma 4.4, which was to be shown (see the claim just after Lemma 4.4). Using the corollary from Proposition 1.4, the algorithm constructs a primitive element η_2 over $\mathbb{Q}$ of the field $F[Z]/(\tilde{\phi}_0) \simeq F[\tilde{\theta}]$ and its

minimal polynomial $\varphi_2 \in \mathbb{Q}[Z]$, so that $F[\tilde{\theta}] = \mathbb{Q}[\eta_2] \simeq \mathbb{Q}[Z]/(\varphi_2)$. Then

$$\deg_Z(\varphi_2) \le d_1[F[\tilde{\theta}]:F] \le d_1(Nd)^{n^2}\mathscr{P}(n^{n^2}); \quad l(\varphi_2), l(\tilde{\theta}), l(\eta) \le M\mathscr{P}((Ndn)^{n^2}, d_1)$$

and the time required to construct η_2, φ_2 does not exceed $\mathscr{P}(M, (Ndn)^{n^2}, d_1)$.

Expressing

$$(\tilde{a}, \tilde{v}_0^{(1)}, \ldots, \tilde{v}_{n-1}^{(k)}) = w = \pi(\tilde{T}, \tilde{\theta}) = (a_1/a_2, v_{0,1}^{(1)}/v_{0,2}^{(1)}, \ldots, v_{n-1,1}^{(k)}/v_{n-1,2}^{(k)})^{(k)}(\tilde{T}, \tilde{\theta}) \in (\mathbb{Q}[\eta_2])^{kn+1},$$

the algorithm calculates $\tilde{c}_{0,0}, \ldots, \tilde{c}_{k,n}$ as linear combinations of the form $\sum_{1 \le i \le N_1} \tilde{c}_i \Delta_i/\Delta \in \mathbb{Q}[\eta_2]$ where Δ_i, Δ are suitable minors of the matrix $A(w)$ obtained from the matrix A by replacing $a, v_0^{(1)}, \ldots, v_{n-1}^{(k)}$ with the co-ordinates of w, respectively (this is correct because of Lemma 4.4).

We then have $l(w), l(\Delta_i), l(\Delta), l(\tilde{c}_{j,t}) \le M\mathscr{P}((Ndn)^{n^2}, d_1)$ by the proposition proved above. The algorithm produces all $\tilde{a}, v_i^{(m)}, \tilde{c}_{j,t}$ and also an operator

$$Q = \sum_{0 \le j \le k} \left(\sum_{0 \le t \le N} \tilde{c}_{j,t} X^t \right) D^j$$

that is a right divisor of the operator L (provided such a Q exists, cf. Lemma 4.4 and the claim just after it) within time $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2})$.

Apart from that (see Lemma 4.4) the algorithm looks over all possible $k \times n$ matrix $(v_i^{(m)})$, indices $1 \le \kappa \le l+1$ and irreducible components $\bar{V}$; this also can be realized within the latter time-bound, taking into account that the number of components $\bar{V}$ of the variety W_κ is at most $\mathscr{P}((Ndn)^{n^2})$ by virtue of the Bezout inequality (see Shafarevich, 1974; Heintz, 1983, also Chistov & Grigor'ev, 1983). In the following lemma, we summarize what was proved in the present section.

LEMMA 4.5. *One can design an algorithm which for any $0 < k < n$ yields a field $\mathbb{Q}[Z]/(\varphi_2) \simeq \mathbb{Q}[\eta_2] \supset F$ and some right divisor (provided that it exists) $Q \in \mathbb{Q}[\eta_2](X)[D]$ of the order k of the operator L (cf. Theorem 1.1 in the Introduction), where φ_2 is a minimal polynomial over $\mathbb{Q}$ of the primitive element η_2, within time $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2})$. Moreover, the following bounds are valid:*

$$\deg(\varphi_2) \le d_1[\mathbb{Q}[\eta_2]:F] \le d_1(Nd)^{n^2}\mathscr{P}(n^{n^2}); \quad l(\varphi_2), l(Q) \le M\mathscr{P}((Ndn)^{n^2}, d_1).$$

Finally, we describe an algorithm for factoring an operator L. For each $0 < k < n$ with the aid of Lemma 4.5 the algorithm yields a right divisor Q (if it exists) of order k of the operator L. There are two cases. In the first one, such a divisor exists for a certain $n/3 \le k \le 2n/3$; in this case let $L = Q_0 Q$. Otherwise, choose the largest $k_3 < n/3$ for which there exists a right divisor Q_3 of the order k_3, let $L = Q_4 Q_3$; then apply Lemma 4.5 to the operator Q_4 and choose the least $k_2 \ge 1$, for which there exists a right divisor Q_2 of the order k_2. Let $Q_4 = Q_1 Q_2$. The operator Q_2 is irreducible and $ord(Q_1) < n/3$. Thereupon the algorithm continues applying the described procedure in the first case to the operators Q_0, Q and in the second one to the operators Q_1, Q_3, etc. Observe that because of Theorem 1.2 (see the Introduction) at any step of the described procedure the same number N is taken.

After executing $s \ge 1$ steps of the described procedure a factorization $L = Q^{(1)} \ldots Q^{(t)}$ is obtained, where for every $1 \le i \le t$ the operator $Q^{(i)}$ is either irreducible or $ord(Q^{(i)}) \le n(2/3)^s$. Furthermore, relying on Lemma 4.5, and recursion on s, for every $1 \le i \le t$ a field $F^{(i)} \ni \mathbb{Q}[\eta^{(i)}] \simeq \mathbb{Q}[Z]/(\varphi^{(i)})$ is yielded, where $\varphi^{(i)}$ is a minimal polynomial over $\mathbb{Q}$ of a

primitive element $\eta^{(i)}$, such that the operator $Q^{(i)} \in F^{(i)}(X)[D]$. Based on the bounds from Lemma 4.5 one can infer (by induction on s) the following bounds:

$$\deg(\varphi^{(i)}) \leq d_1[F^{(i)}:F] \leq d_1 \mathscr{P}((Ndn)^{n^2\gamma_s});$$

$$l(\varphi^{(i)}), l(Q^{(i)}) \leq M\mathscr{P}((Ndn)^{n^2 s}, d_1^s)$$

where

$$\gamma_s = \sum_{0 \leq j < s} (4/9)^j < 2.$$

The algorithm yields the operators $Q^{(1)}, \ldots, Q^{(t)}$ within time $\mathscr{P}(M, (Ndn)^{n^4}, d_1^{n^2+s})$ again in force of Lemma 4.5.

After at most $s \leq \log_{3/2}(n)$ steps of the procedure a factorization $L = L_1 \ldots L_m$ into irreducible divisors will be produced together with the corresponding fields $H_1, \ldots, H_m$ such that $L_i \in H_i(X)[D]$. Here $H_i = Q[\mu_i] \simeq Q[Z]/(\psi_i)$, where ψ_i is the minimal polynomial over $\mathbb{Q}$ of the primitive element μ_i. Using Proposition 1.4 (see the Introduction) the algorithm factors the polynomial ψ_i over the field F and then finds a unique irreducible factor $h_i \in F[Z]$ of the polynomial ψ_i for which $h_i(\mu_i) = 0$; evidently $H_i = F[\mu_i] \simeq F[Z]/(h_i)$. Thereupon applying the corollary of Proposition 1.4 to the polynomials $h_1, \ldots, h_m$ the algorithm produces all possible fields $F_1 = \mathbb{Q}[\eta_1] \simeq \mathbb{Q}[Z]/(\varphi_1) \supset F$ where $\varphi_1(\eta_1) = 0$, with the property that there exists an embedding of the fields $\sigma_i : H_i \to F_1$ *over* F (see, e.g. van der Waerden, 1971) for each $1 \leq i \leq m$ and, moreover, $F_1 = F(\sigma_1(H_1), \ldots, \sigma_m(H_m))$, within time

$$\mathscr{P}\left(M, (Ndn)^{n^2} d_1^{\log(n)}, \prod_{1 \leq i \leq m} \deg(h_i)\right) \leq \mathscr{P}(M, (Ndn)^{n^3} d_1^{\log(n)}).$$

The field F_1 yields the operators $\sigma_1(L_1) \in \sigma_1(H_1)(X)[D], \ldots, \sigma_m(L_m) \in \sigma_m(H_m)(X)[D]$ and the algorithm tests, whether $L = \sigma_1(L_1) \ldots \sigma_m(L_m) \in F_1(X)[D]$? One of the possible fields F_1 fits and gives a factorization of L. Furthermore, a primitive element $\eta_1 = \eta + \sum_{1 \leq i \leq m} \lambda_i^{(1)} \mu_i$ exists for appropriate integers

$$0 \leq \lambda_i^{(1)} \leq [F_1 : \mathbb{Q}] \leq d_1[F_1 : F] \leq d_1 \prod_{1 \leq i \leq m} \deg(h_i) \leq d_1 \mathscr{P}((Ndn)^{n^3})$$

and the following bounds hold:

$$l(\varphi_1), l(\eta), l(\mu_i), l(\sigma_i(L_i)) \leq M\mathscr{P}((Ndn)^{n^3} d_1^{\log(n)}).$$

Theorem 1.1 is now proven.

5. Calculating the GCD of a Family of Linear Differential Operators

While calculating the GCD of a family of (usual) univariate polynomials it is reasonable to partition the family into pairs, calculate the GCD for each pair using the Euclidean algorithm, and bound the coefficients of the intermediate polynomials with the help of subresultants (see, e.g. Loos, 1982). The resulting polynomials are again partitioned into pairs, etc., GCDs of sub-families of the input family of polynomials appear in intermediate calculations and, taking into account that the GCD is a divisor of any of the polynomials from the subfamily, the coefficients of the GCD can be bounded as the coefficients of a divisor. In the case of (usual) polynomials the size of the coefficients of a divisor can be bounded by a polynomial in the size of the coefficients of the initial polynomials (see, e.g. Proposition 1.4 in the Introduction). In the case of the linear differential operators a similar (polynomial) bound is not known (cf. Theorem 1.2), therefore for calculating the

greatest common right divisor (GCRD) of a family of operators one has to estimate *a priori* the size of the coefficients of GCRD.

The coefficients of the GCD of two polynomials equal suitable minors (subresultants, see, e.g. Loos, 1982) of the Sylvester matrix (see, e.g. van der Waerden, 1971) of these two polynomials. Later on we generalize the construction of the Sylvester matrix and this property to a family of the polynomials, as a matter of fact, we prove it for the case of interest to us, that is, linear differential operators (however, it can be transferred in a similar way to the case of the polynomials). This will supply us with the required bound on the size of the coefficients of GCRD of a family of the operators.

Assume that the operators $Q_1, \ldots, Q_s \in F(X)[D]$ of orders $r_1, \ldots, r_s \leq n$ respectively, satisfy the same bounds (1) as the operator L in the Introduction. Denote $r = r_1 + \ldots + r_s$. For integers $v_1 \geq 0, \ldots, v_s \geq 0$ consider a matrix $B = B_{v_1, \ldots, v_s}$ (being a generalization of the Sylvester matrix) with entries in the field $F(X)$, whose rows are the coefficients of the expansions of the operators $Q_1, DQ_1, \ldots, D^{r-r_1+v_1}Q_1, Q_2, DQ_2, \ldots, D^{r-r_2+v_2}Q_2, \ldots, Q_s, DQ_s, \ldots, D^{r-r_s+v_s}Q_s$ in the basis consisting of the operators $D^{r+\max\{v_1,\ldots,v_s\}}, \ldots, D^2, D, 1$ (i.e. the first column corresponds to the operator $D^{r+\max\{v_1,\ldots,v_s\}}$). Pick out an arbitrary operator Q_{s_0} (we call it a leading operator) such that $v_{s_0} = \max\{v_1, \ldots, v_s\}$ and $r_{s_0} = \min_{v_i = v_{s_0}}\{r_i\}$ where the latter minimum ranges over all indices i for which $v_i = v_{s_0}$.

For any pair of operators Q_j, Q_{s_0} (here $j \neq s_0$), one has a unique right remainder $rem(Q_j, Q_{s_0}) = R_j \in F(X)[D]$. This is found by dividing Q_j by Q_{s_0} and satisfies the properties that $r_j^{(1)} = ord(R_j) < r_{s_0}$; $r_j^{(1)} \leq r_j$ (provided $R_j \neq 0$) and $Q_j = K_j Q_{s_0} + R_j$ for a certain $K_j \in F(X)[D]$; when $r_{s_0} = 0$, the operator $R_j = 0$. For uniformity of notation, we let $r_{s_0}^{(1)} = r_{s_0}$. Taking into account that, for arbitrary k, we have $D^k K_j Q_{s_0} = \sum_{i \geq 0} h_i D^i Q_{s_0}$ for suitable $h_i \in F(X)$, one can perform appropriate elementary transformations (over $F(X)$) of the rows of the matrix B so that the rows of the resulting matrix $\tilde{B}^{(1)}$ are the coefficients of the expansion (in the basis $D^{r+v_{s_0}}, \ldots, D^2, D, 1$) of the operators $R_j, DR_j, \ldots, D^{r-r_j+v_j}R_j$ for all $j \neq s_0$ and also of the operators $Q_{s_0}, DQ_{s_0}, \ldots, D^{r-r_{s_0}+v_{s_0}}Q_{s_0}$. In the first column of the matrix $\tilde{B}^{(1)}$ there is exactly one non-zero entry corresponding to the operator $D^{r-r_{s_0}+v_{s_0}}Q_{s_0}$, since for $j \neq s_0$ we have $ord(D^{r-r_j+v_j}R_j) \leq r + v_j \leq r + v_{s_0}$ (provided that $R_j \neq 0$) and both equalities are possible iff $r_j^{(1)} = r_j$ and $v_j = v_{s_0}$, in which case $r_j = r_j^{(1)} < r_{s_0}$, and we get a contradiction with the choice of the leading operator Q_{s_0}. Because of this $ord(D^{r-r_j+v_j}R_j) < r + v_{s_0}$; in other words, the entries in the first column corresponding to the operators $R_j, \ldots, D^{r-r_j+v_j}R_j$ all equal zero.

Since in what follows we shall consider only the minors of the matrix B containing among others some fixed set of several initial columns, we consider instead of the matrix $\tilde{B}^{(1)}$ the matrix $B^{(1)}$ obtained from $\tilde{B}^{(1)}$ by deleting all zero rows (they correspond to zero operators R_l) and also by deleting the first column and the row corresponding to the operator $D^{r-r_{s_0}+v_{s_0}}Q_{s_0}$. Furthermore, in what follows, all the minors in the matrix $B^{(1)}$ are to be multiplied by the leading coefficient $lc(Q_{s_0}) \neq 0$ in order to achieve a minor of the initial matrix B. At every step of the process we again delete from the current matrix all zero rows and also the first column and a certain row containing a unique non-zero entry in the first column of this current matrix.

We can do this and also keep track of a fixed set of initial columns in the matrix B. These columns would appear in a fixed set of minors of the matrix B.

In the matrix $B^{(1)}$, for each $j \neq s_0$ (provided that $R_j \neq 0$), there are

$$r - r_j + v_j + 1 = r_1^{(1)} + \ldots + r_{j-1}^{(1)} + r_{j+1}^{(1)} + \ldots + r_s^{(1)} + v_j^{(1)} + 1$$

rows corresponding to the operators $R_j, DR_j, \ldots, D^{r-r_j+v_j}R_j$ for a suitable $v_j^{(1)}$ (in the latter

sum $r_i^{(1)}$ is omitted if the corresponding operator $R_i = 0$). Observe that $v_j^{(1)} \geq v_j$ since $r_m^{(1)} \leq r_m$ for all m (when $R_m = 0$ one can adopt temporarily just for this argument that $r_m^{(1)} = 0$). Furthermore, in the matrix $B^{(1)}$ there are

$$r - r_{s_0} + v_{s_0} = r_1^{(1)} + \ldots + r_{s_0-1}^{(1)} + r_{s_0+1}^{(1)} + \ldots + r_s^{(1)} + v_{s_0}^{(1)} + 1$$

rows (the same remark as above concerns the latter sum) corresponding to the operators $Q_{s_0}, DQ_{s_0}, \ldots, D^{r-r_{s_0}+v_{s_0}-1}Q_{s_0}$ for an appropriate $v_{s_0}^{(1)}$. We now show that $v_{s_0}^{(1)} \geq 0$. If

$$r_1^{(1)} + \ldots + r_{s_0-1}^{(1)} + r_{s_0+1}^{(1)} + \ldots + r_s^{(1)} < r - r_{s_0},$$

then $v_{s_0}^{(1)} \geq v_{s_0} \geq 0$. Suppose this is not the case, that is,

$$r_1^{(1)} + \ldots + r_{s_0-1}^{(1)} + r_{s_0+1}^{(1)} + \ldots + r_s^{(1)} = r - r_{s_0}.$$

We then have $r_j^{(1)} = r_j$ or $r_j = 0$ for each $j \neq s_0$. We first assume that $r_{s_0} > 0$. In this case $r_j = r_j^{(1)} < r_{s_0}$ (if $r_j = 0$, then trivially $r_j^{(1)} = r_j = 0 < r_{s_0}$) and therefore $v_{s_0} > v_j$ because of the choice of the leading operator Q_{s_0}. This implies $v_{s_0} \geq 1$ (provided $s \geq 2$) and so $v_{s_0}^{(1)} = v_{s_0} - 1 \geq 0$. Note that we have also shown that, under the assumptions $r_{s_0} > 0$ and $s \geq 2$, the matrix $B^{(1)}$ contains at least one row corresponding to the operator Q_{s_0}. Assume now that $r_{s_0} = 0$. We then have $r_j = 0$ for all j (see above) and the matrix $B^{(1)}$ either consists of v_{s_0} rows corresponding to the operators $Q_{s_0}, DQ_{s_0}, \ldots, D^{v_{s_0}-1}Q_{s_0}$ if $v_{s_0} \geq 1$ or $B^{(1)}$ is the zero matrix if $v_{s_0} = 0$. In the former case $v_{s_0}^{(1)} = v_{s_0} - 1 \geq 0$, in the latter one $v_j = 0$ for all j (by virtue of the choice of Q_{s_0}) and the matrix B consists of a single column. Finally, we consider the case $s = 1$, then $r = r_{s_0}$ and either the matrix $B^{(1)}$ contains $v_{s_0} = v_{s_0}^{(1)} + 1 \geq 1$ rows, i.e. one row less than the matrix B, or $B^{(1)}$ is the zero matrix. In the former case $v_{s_0}^{(1)} \geq 0$, in the latter one B consists of a single row. Thus, we have shown the inequalities $v_j^{(1)} \geq 0$ for all j (provided that $B^{(1)} \neq 0$) and, moreover, if $B^{(1)} = 0$ then the matrix B consists of either one row or one column.

Let $r^{(1)} = r_1^{(1)} + \ldots + r_{s_1}^{(1)}$ (here we have condensed the lower indices retaining only the addends corresponding to $s_1 < s$ non-zero operators Q_{s_0} and R_j for $j \neq s_0$). Summarizing the above assertions, we have proved that the matrix $B^{(1)} = B_{v_1^{(1)}, \ldots, v_{s_1}^{(1)}}^{(1)}$ provided that $B^{(1)} \neq 0$) satisfies the same properties as the initial matrix B (in particular, the integers $v_1^{(1)} \geq 0, \ldots, v_{s_1}^{(1)} \geq 0$), whereas $B^{(1)}$ contains one column less and at least one row less than the matrix B; moreover, $G = GCRD(\{R_j\}_{j \neq s_0}, Q_{s_0}) = GCRD(Q_1, \ldots, Q_s)$, in other words, the GCRD of the operators corresponding to the rows of the matrix does not change after the described elementary transformations.

We continue the above process until we get the last matrix $B^{(t)}$ that does not vanish. By what was proven above, $B^{(t)}$ consists of either one column and then $G = 1$ or $B^{(t)}$ consists of one row corresponding to the operator Q_0 and then $G = Q_0$ (up to a factor from $F(X)^*$). Observe that in both cases $B^{(t)}$ contains $ord(G) + 1$ columns.

Recall that during the process of producing the matrix $B^{(t)}$ in all t initial columns were deleted. Therefore the number of columns in the initial matrix B equals

$$r + \max\{v_1, \ldots, v_s\} + 1 = t + ord(G) + 1.$$

For any set I, consisting of $t+1$ rows of the matrix B, denote by $b_I \in (F(X))^{ord(G)+1}$ a vector, whose ith co-ordinate equals a minor of the matrix B formed by the rows from the set I and by the initial t columns and by $(t+i)$th column, where $1 \leq i \leq ord(G)+1$. Consider a linear space $\mathscr{B} = \mathscr{B}(B) \subset (F(X))^{ord(G)+1}$ spanned over the field $F(X)$ by the vectors b_I for all possible sets I. After the elementary transformations on the rows of the matrix B the space $\mathscr{B}$ does not change (when considering it for the transformed matrix). Add back to the

matrix $B^{(t)}$ all t deleted columns and rows and call this new matrix $\tilde{B}^{(t)}$. The corresponding space $\mathscr{B}(\tilde{B}^{(t)})$ coincides with $\mathscr{B}$, since $\tilde{B}^{(t)}$ can be obtained from B by suitable elementary transformations on the rows.

Obviously rank $(B) = rank(\tilde{B}^{(t)}) = t+1$. On the other hand, the space $\mathscr{B}(\tilde{B}^{(t)})$ is one-dimensional and spanned by a vector b_{I_0} (where I_0 contains t non-zero rows added back to the matrix $\tilde{B}^{(t)}$). The vector b_{I_0} is collinear with a vector whose ith co-ordinate $(1 \le i \le ord(G)+1)$ equals $g_{ord(G)+1-i} \in F(X)$, where

$$G = GCRD(Q_1, \ldots, Q_S) = \sum_{0 \le i \le ord(G)} g_i D^i.$$

Hence, this vector is collinear with any vector b_I, this completes the proof of the following lemma (one has to put $v_1 = \ldots = v_s = 0$ in the initial matrix $B = B_{0,\ldots,0}$).

LEMMA 5.1. *Denote by B a matrix over the field $F(X)$ with the rows being the coefficients of the expansions of the operators Q_1, $DQ_1, \ldots$, $D^{r-r_1}Q_1$, Q_2, $DQ_2, \ldots$, $D^{r-r_2}Q_2, \ldots$, Q_s, $DQ_s, \ldots$, $D^{r-r_s}Q_S$, where $r = r_1 + \ldots + r_s$, in the basis consisting of the operators $D^r, \ldots, D^2, D, 1$. Let*

$$G = GCRD(Q_1, \ldots, Q_s) = \sum_{0 \le i \le m} g_i D^i,$$

then $m = ord(G) = r + 1 - rank(B)$. Furthermore, for any set I consisting of $rank(B)$ rows of the matrix B, a vector b_I, whose ith co-ordinate equals the minor of the matrix B formed by the rows from the set I and by the initial $r-m$ columns and by the $(r-m+i)$th column $(1 \le i \le m+1)$, is collinear with the vector $(g_m, \ldots, g_1, g_0)$. In addition, there is a set I such that the vector $b_I \ne 0$. Moreover, we have the bounds:

$$\deg_X(G) < dr \le dns, \quad l(G) \le (M + \log(d))\mathscr{P}(d_1, n, s)$$

(see (1)).

The latter bounds follow from the bounds on the size of the determinant (cf. e.g. Heintz, 1983, *and the proof of Lemma* 4.1. *in section* 4).

The algorithm for calculating $G = GCRD(Q_1, \ldots, Q_s)$ finds a set I, consisting of $rank(B)$ rows of the matrix B, such that the submatrix of B formed from the rows of I and the initial $rank(B)$ columns is non-singular. Such a set I exists by Lemma 5.1 The algorithm then calculates the vector b_I, which gives the coefficients of the operator G (see Lemma 5.1). The algorithm executes the described calculations using a variant of the Gaussian algorithm (see the proof of Lemma 4.1 in section 4). Hence, its running time can be bounded by a polynomial in M, d, d_1, n and s. This completes the proof of Theorem 1.3 (see the Introduction).

References

Bereiss, E. H. (1968). Sylvester's identity and multistep integer preserving Gaussian elimination. *Math. Comp.* **22**, 565–566.

Chistov, A. L. (1986). Polynomial complexity of Newton–Puiseux algorithm. *Proc. Symp. Math. Found. Comput. Sci., Bratislava* (Lect. Notes Comput. Sci.) **233**, 247–255.

Chistov, A. L., Grigor'ev, D. Yu. (1982). Polynomial-time factoring of multivariable polynomials over a global field. *Preprint LOMI* E-5-82, Leningrad.

Chistov, A. L., Grigor'ev, D. Yu. (1983). Subexponential-time solving systems of algebraic equations. I, II. *Preprints LOMI* E-9-83, E-10-83, Leningrad.

Chistov, A. L., Grigor'ev, D. Yu. (1984). Complexity of quantifier elimination in the theory of algebraically closed fields. *Proc. Symp. Math. Found. Comput. Sci., Prague* (Lect. Notes Comput. Sci.) **176,** 17–31.

Cohn, P. M. (1971). *Free Rings and Their Relations.* Academic Press.

Della Dora, J., di Crescenzo, Cl., Tournier, E. (1982). An algorithm to obtain formal solutions of a linear homogeneous differential equation at an irregular singular point. *Proc. Symp. EUROCAM '82* (Lect. Notes Comput. Sci.) **144,** 273–280.

Grigor'ev, D. Yu. (1986). Computational complexity in polynomial algebra. *Proc. Int. Congr. Mathem., Berkeley* **2,** 1452–1460.

Grigor'ev, D. Yu. (1989). Complexity of factoring a linear ordinary differential operator. *Soviet Math. Dokl.* **38,** 452–457.

Grigor'ev, D. Yu., Chistov, A. L. (1984). Fast decomposition of polynomials into irreducible ones and the solution of systems of algebraic equations. *Soviet Math. Dokl.* **29,** 380–383.

Heintz, J. (1983). Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.* **24,** 239–278.

Kaltofen, E. (1982*a*). A polynomial reduction from multivariate to bivariate integral polynomial factorization. *Proc. STOC, ACM,* pp. 261–266.

Kaltofen, E. (1982*b*). A polynomial-time reduction from bivariate to univariate integral polynomial factorization. *Proc. FOCS, IEEE,* pp. 57–64.

Kaltofen, E. (1985). Polynomial-time reductions from multivariate to bi- and univariate integral factorization. *SIAM J. Computing* **14,** 469–489.

Lenstra, A. K., Lenstra, H. W., Lovasz, L. (1982). Factoring polynomials with rational coefficients. *Math. Ann.* **261,** 515–534.

Loos, R. (1982). Generalized polynomial remainder sequences. In: *Computer Algebra. Symbolic and Algebraic Computation.* Springer.

Mahler, K. (1976). Lectures on transcendental numbers. *Lect. Notes Mathem.* **546.**

Olver, F. (1974). *Introduction to Asymptotics and Special Functions.* Academic Press.

Schlesinger, L. (1897). *Handbuch für Theorie der linearen Differentialgleichungen II.* Leipzig: Teubner.

Shafarevich, I. R. (1974). *Basic Algebraic Geometry.* Springer.

Singer, M. (1981). Liouvillian solutions of n-th order homogeneous linear differential equations. *Amer. J. Math.* **103,** 661–682.

van der Waerden, B. L. (1971). *Algebra I.* Springer.

Wasow, W. (1976). *Asymptotic Expansions for Ordinary Differential Equations.* New York: Krieger Publ. Co.