Computing the Additive Complexity of Algebraic Circuits with Root Extracting

Dima Grigoriev [*] Marek Karpinski [†]

Abstract

We design an algorithm for computing the generalized (algebraic circuits with root extracting, cf. [P 81], [J 81], [GSY 93]) *additive complexity* of any rational function. It is the first computability result of this sort on the additive complexity of algebraic circuits.

Key words. Additive complexity, algebraic circuits, root extracting, minimal computation.
AMS subject classification. 68Q25, 68Q40, 68Q15, 26C15.

[*]Dept. of Computer Science, The Pensylvania State University, University Park, PA 16802. Research partially supported by NFS Grant CCR-9424358. Email: dima@cs.psu.edu.

[†]Dept. of Computer Science, University of Bonn, 53117 Bonn, and the International Computer Science Institute, Berkeley, California. Research partially supported by DFG Grant KA 673/4-1, by the ESPRIT BR Grants 7097 and EC-US030. Email: marek@cs.bonn.edu.

1 Introduction

It is a well known open problem in the theory of computation, whether the additive complexity of functions is computable. Note that both multiplicative and total complexities of functions are computable. In this paper we prove, somewhat surprisingly, the *computability* of the generalized additive complexity for algebraic circuits with root extraction. These circuits were considered in [J 81] where a lower bound on the number of root extracting operations for computing on algebraic functions has been proven. This was recently generalized in [GSY 93] for the algebraic circuits which contain in addition also exponential and logarithmic functions. Our result is the first computability result of this sort on the *additive* complexity of algebraic circuits.

Let us give the definition of the generalized additive complexity. $\bar{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$, the set of algebraic numbers. We say that a rational function $f \in \mathbb{Q}(X_1, \ldots, X_n)$ has a generalized additive complexity at most t, if there exists a sequence of algebraic functions:

$$u_{i+1} = \varepsilon^{(i+1)} X_1^{\alpha_1^{(i+1)}} \cdots X_n^{\alpha_n^{(i+1)}} u_1^{\beta_1^{(i+1)}} \cdots u_i^{\beta_i^{(i+1)}} + \kappa^{(i+1)} X_1^{\gamma_1^{(i+1)}} \cdots X_n^{\gamma_n^{(i+1)}} u_1^{\delta_1^{(i+1)}} \cdots u_i^{\delta_i^{(i+1)}}$$

for $0 \leq i \leq t$, where $\kappa^{(t+1)} = 0$, $f = u_{t+1}$ and all the exponents $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)} \in \mathbb{Q}$, $0 \leq i \leq t$ are rationals, coefficients $\varepsilon^{(i+1)}, \kappa^{(i+1)} \in \bar{\mathbb{Q}}$ are algebraic. The rationality of the exponents (rather than being integers) differs the *generalized* additive complexity from the usual *additive* complexity.In other words, we consider algebraic circuits in which (in addition to the usual arithmetic operations) extracting of arbitrary roots is allowed.

If t equals to the generalized additive complexity of f then we say that computation $u_1, \ldots, u_{t+1}$ of f is generalized additive-minimal.

In the section 2 we consider the computations in which the exponents $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)}$, $0 \leq i \leq t$ are allowed to be algebraic and refer to it as *the quasi-additive complexity.* The computation of the quasi-additive complexity is reduced (see lemma below) to the problem of quantifier elimination in the theory of differentially closed fields (solved in [Se 56], for its complexity see [G 89]).

In section 3 we prove (see proposition below) that any quasi-additive minimal computation of a rational function can be transformed into a generalized additive-minimal computation with the same number of additions which contains only rational exponents, thus quasi-additive and generalized additive complexities coincide. Moreover, the corollary in section 3 gives a possibility to construct the rational exponents of a generalized additive-minimal computation. In section 4 we describe an algorithm for producing a generalized additive-minimal computation. In the case of one variable ($n = 1$) we give an (elementary) complexity bound of the designed algorithm (see theorem below) as it uses the quantifier elimination algorithm from [G 89]. In the general case ($n \geq 2$) we do not give complexity bounds as the quantifier elimination method from [Se 56] is used which relies in turn on the efficient bounds in Hilbert's Idealbasissatz which are not known to be elementary.

Note that first lower bounds on the additive complexity of f in terms of the variety of real roots of f were obtained in [BC 76] and [G 83] (see also [Ri 85]). One can find in [G 83] also a survey on other lower bounds, in particular on the additive complexity (see also [G 82] [SW 80]). The lower bound from [G 83] is used (see the end of section 3) to show that there are polynomials with the generalized additive complexity equal to 3 and arbitrary large additive complexity.

Another interesting issue is the dependance of the (standard) additive complexity on the coefficents which are involved in *straight-line programs* (cf. [W 78]). If we allow only real algebraic coefficents (from $\bar{\mathbb{Q}} \cap \mathbb{R}$) instead of $\bar{\mathbb{Q}}$ (see above), then the additive complexity could jump drastically as the following example indicates. The polynominal $(1+iX)^n + (1-iX)^n \in \mathbb{Z}[x]$ (cf. [W 78]) has *evidently* the additive complexity at most 3 over $\bar{\mathbb{Q}}$. It has also all its roots in $\bar{\mathbb{Q}} \cap \mathbb{R}$, therefore its *additive complexity* over $\bar{\mathbb{Q}} \cap \mathbb{R}$ is greater than $\Omega(\log^{\frac{1}{2}} n)$ (cf. [G 83], [Ri 85]).

2 Describing the quasi-additive complexity in terms of the first-order theory of differentially closed fields

We start with designing an algorithm for testing, whether there exist (and if so, also to produce) *algebraic* exponents $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)} \in \bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$) in the computation $u_1, \ldots, u_{t+1}$ providing an identity $u_{t+1} = f$ holds. In this case we say that f has the quasi-additive complexity at most t. For this purpose we introduce the (differential) unknowns

$$u_{i+1}, \tilde{\alpha}_1^{(i+1)}, \ldots, \tilde{\delta}_i^{(i+1)}, v_1^{(i+1)}, \ldots, v_n^{(i+1)}, w_1^{(i+1)}, \ldots, w_i^{(i+1)}, \tilde{v}_1^{(i+1)}, \ldots, \tilde{v}_n^{(i+1)}, \tilde{w}_1^{(i+1)}, \ldots, \tilde{w}_i^{(i+1)}$$

for all $0 \leq i \leq t$ and the system of (partial) differential equations (denote $D_i = \frac{d}{dX_i}$ and by D any of the operators $D_1, \ldots, D_n$, by $\delta(l,j)$ denote the Kronecker symbol):

$$D(\tilde{\alpha}_1^{(i+1)}) = \cdots = D(\tilde{\delta}_i^{(i+1)}) = 0 \qquad (1a)_{i+1}$$

$$D_j(v_l^{(i+1)}) = \frac{\tilde{\alpha}_l^{(i+1)}}{X_l} v_l^{(i+1)} \delta(l,j); \qquad D_j(\tilde{v}_l^{(i+1)}) = \frac{\tilde{\gamma}_l^{(i+1)}}{X_l} \tilde{v}_l^{(i+1)} \delta(l,j), \quad 1 \leq l,j \leq n \qquad (1b)_{i+1}$$

$$D(w_l^{(i+1)}) = \tilde{\beta}_l^{(i+1)} w_l^{(i+1)} \frac{Du_l}{u_l}; \qquad D(\tilde{w}_l^{(i+1)}) = \tilde{\delta}_l^{(i+1)} \tilde{w}_l^{(i+1)} \frac{Du_l}{u_l}, \qquad 1 \leq l \leq i \qquad (1c)_{i+1}$$

$$u_{i+1} = v_1^{(i+1)} \ldots v_n^{(i+1)} w_1^{(i+1)} \ldots w_i^{(i+1)} + \tilde{v}_1^{(i+1)} \ldots \tilde{v}_n^{(i+1)} \tilde{w}_1^{(i+1)} \ldots \tilde{w}_i^{(i+1)} \qquad (1d)_{i+1}$$

for all $0 \leq i \leq t$ together with the equation $u_{t+1} = f$. The resulting system we denote by (1).

Note that the equations $(1a)_{i+1}$ imply that $\tilde{\alpha}_1^{(i+1)}, \ldots, \tilde{\delta}_i^{(i+1)} \in \bar{\mathbb{Q}}$ are the constants; $(1b)_{i+1}$ imply that $v_l^{(i+1)} = \mu_l^{(i+1)} X_l^{\tilde{\alpha}_l^{(i+1)}}, \tilde{v}_l^{(i+1)} = \tilde{\mu}_l^{(i+1)} X_l^{\tilde{\gamma}_l^{(i+1)}}$ for the appropriate constants $\mu_l^{(i+1)}$, $\tilde{\mu}_l^{(i+1)} \in \bar{\mathbb{Q}}$; $(1c)_{(i+1)}$ imply that $w_l^{(i+1)} = \nu_l^{(i+1)} u_l^{\tilde{\beta}_l^{(i+1)}}, \tilde{w}_l^{(i+1)} = \tilde{\nu}_l^{(i+1)} u_l^{\tilde{\delta}_l^{(i+1)}}$ for the appropriate constants $\nu_l^{(i+1)}, \tilde{\nu}_l^{(i+1)} \in \bar{\mathbb{Q}}$.

Thus, the following lemma is proved.

Lemma. *The solvability of system (1) (in all its differential unknowns) is equivalent to the fact that the quasi-additive complexity of f is at most t.*

Now we consider the statement of solvability of the system (1) as an existentional formula of the first-order theory of differentially closed fields [Se 56]. Applying to it a quantifier elimination algorithm [Se 56] one can eliminate unknowns

$$u_{i+1}, v_1^{(i+1)}, \ldots, v_n^{(i+1)}, w_1^{(i+1)}, \ldots, w_i^{(i+1)}, \tilde{v}_1^{(i+1)}, \ldots, \tilde{v}_n^{(i+1)}, \tilde{w}_1^{(i+1)}, \ldots, \tilde{w}_i^{(i+1)} \text{for all } 0 \leq i \leq t.$$

As a result we get an (existentional) equivalent formula containing only the unknowns $\tilde{\alpha}_1^{(i+1)}$, $\ldots, \tilde{\delta}_i^{(i+1)}, 0 \leq i \leq t$. Because of (1a) the latter formula can be considered as a formula in the language of polynomials (so, without derivatives), thus as a system of polynomial equations and inequalities with integer coefficients.

Thus, given a rational function f the algorithm tries $t = 1, 2, \ldots$, and for each t tests (using [CG 83], [C 86]), whether the above constructed system of polynomial equations and inequalities has a solution (over $\bar{\mathbb{Q}}$). For a minimal such t we take any of these solutions $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)} \in \bar{\mathbb{Q}}, 0 \leq i \leq t$. In the next section we show that in this case there exists as well a rational solution of this system and moreover we show how to construct it.

To solve the system (1) of differential equations we applied the algorithm from [Se 56] for which elementary complexity bound is unknown since it relies on an efficient bound in Hilbert's Idealbasissatz. But the complexity of quantifier elimination is elementary in the case of ordinary differential equations for the algorithm designed in [G 89], i. e. when $n = 1$, in another words when there is only one independent variable X. In this case the system (1) contains $O(t^2)$ unknows, the order of highest occurring derivatives in the equations is at most 1, the degree of the equations is at most $O(t) + \deg f$ and the number of equations is at most $O(t^2)$, the bit-size of the coefficients of the occuring equations is at most $O(1) + M$, where M is the bit-size of the coefficients of f. Therefore (see the bounds in [G 89]), one can eliminate quantifiers and produce a system of polynomial equations and inequalities with integer coefficients (see above) in the unknowns $\tilde{\alpha}_1^{(i+1)}, \ldots, \tilde{\delta}_i^{(i+1)}, 0 \leq i \leq t$ in time $\mathcal{N} = M^{O(1)}(degf)^{2^{2^{O(t^2)}}}$; the degrees of the polynomials occurring in this system do not exceed $\mathcal{N}_1 = (degf)^{2^{2^{O(t^2)}}}$ the number of these polynomials is at most $\mathcal{N}_1$ and the bit-size of (integer) coefficients occurring in this system can be bounded by $\mathcal{N}$.

Therefore to solve this system of polynomial equations and inequalities we apply the algorithm from [CG 83] (cf. also [C 86]) which requires time $M^{O(1)}(degf)^{2^{2^{O(t^2)}}}$. The algorithm from [CG 83] finds (provided that the system is solvable) a solution $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)} \in \bar{\mathbb{Q}}, 0 \leq i \leq t$ in the following form. The algorithm produces an irreducible over $\mathbb{Q}$ polynomial $\varphi(Z) \in \mathbb{Q}[Z]$, also

polynomials $\bar{\alpha}_1^{(i+1)}(Z),\ldots,\bar{\delta}_i^{(i+1)}(Z)\in\mathbb{Q}[Z], 0\le i\le t$ such that $\alpha_1^{(i+1)}=\bar{\alpha_1}^{(i+1)}(\theta),\ldots,\delta_i^{(i+1)}=\bar{\delta}_i^{(i+1)}(\theta)$ where $\theta\in\bar{\mathbb{Q}}$ is a root of $\varphi(\theta)=0$. From [CG 83] we obtain the following bounds:

$$\deg(\varphi),\deg(\bar{\alpha}_1^{(i+1)}),\ldots,\deg(\bar{\delta}_i^{(i+1)})\le(\deg f)^{2^{2^{O(t^2)}}}, 0\le i\le t$$

and the bit-size of every coefficient occurring in the listed polynomials does not exceed $M^{O(1)}$ $(degf)^{2^{2^{O(t^2)}}}$.

3 Rational exponents in the quasi-additive minimal computation

In this section we prove (see the proposition below) the equivalence of the generalized additive and quasi-additive complexities for rational functions. Moreover, we show (see Corollary below) how for given algebraic exponents of a quasi-additive minimal computation to produce the exponents of a certain generalized additive-minimal computation of the same rational function, thus containing only rational exponents. The similar statements were proved also for the rationality of the exponents in the minimal sparse representations of a rational function [GKS 92a] and of a real algebraic function [GKS 92a]. But the latter statements have different (from the one in the present paper) nature, also another difference is that we prove here the existence of the rational exponents rather than the rationality as it was the case in [GKS 92a], [GKS 92a].

So, let

$$u_{i+1}=\varepsilon^{(i+1)}X_1^{\alpha_1^{(i+1)}}\cdots X_n^{\alpha_n^{(i+1)}}u_1^{\beta_1^{(i+1)}}\cdots u_i^{\beta_i^{(i+1)}}+\kappa^{(i+1)}X_1^{\gamma_1^{(i+1)}}\cdots X_n^{\gamma_n^{(i+1)}}u_1^{\delta_1^{(i+1)}}\cdots u_i^{\delta_i^{(i+1)}}$$

where $0\le i\le t, \kappa^{(t+1)}=0$ and all the exponents and coefficients

$$\alpha_1^{(i+1)},\ldots,\delta_i^{(i+1)},\varepsilon^{(i+1)},\kappa^{(i+1)}\in\bar{\mathbb{Q}}\ .$$

Proposition. *Assume that $f=u^{(t+1)}\in\bar{\mathbb{Q}}(X_1,\ldots,X_n)$ is a rational function and t is the minimal possible (so t equals to the quasi-additive complexity of f). Then there exist rational exponents $a_1^{(i+1)},\ldots,d_i^{(i+1)}\in\mathbb{Q}, 0\le i\le t$, respectively, providing also a computation of f (thus, t equals also to the generalized additive complexity).*

Proof. For each $1\le j\le n$ consider a $\mathbb{Q}$-basis $\bar{\theta}_j^{(1)},\bar{\theta}_j^{(2)},\ldots\in\bar{\mathbb{Q}}$ of the $\mathbb{Q}$-linear hull $\mathbb{Q}\{\alpha_j^{(s)},\gamma_j^{(s)}\}_{1\le s\le t+1}$. If 1 (thereby $\mathbb{Q}$) is contained in the latter linear hull, then we set $\bar{\theta}_j^{(1)}=1$. Denote $\{\theta_j^{(1)},\theta_j^{(2)},\ldots\}=\{\bar{\theta}_j^{(1)},\bar{\theta}_j^{(2)},\ldots\}\setminus\{1\}$.

Consider a differential field $F_j, 0\le j\le n$ generated over $\bar{\mathbb{Q}}(X_1,\ldots,X_n)$ by the elements $\log X_1, X_1^{\theta_1^{(1)}}, X_1^{\theta_1^{(2)}},\ldots,\log X_j, X_j^{\theta_j^{(1)}}, X_j^{\theta_j^{(2)}},\ldots$. Then in the terminology of [RC 79] each

$F_j, 0 \le j \le n$ is a log-explicit extension of its field of constants $\bar{\mathbb{Q}}$ (one can represent $X^\beta = \exp(\beta \log X)$).

We claim that the elements $X_{j+1}^{\theta_{j+1}^{(1)}}, X_{j+1}^{\theta_{j+1}^{(2)}}, \ldots \in F_{j+1}$ are algebraically independent over the field $F_j(\log X_{j+1})$. Assume the contrary. Then the corollary 3. 2 [RC 79] (see also [Ro 76]) implies the existence of a constant $\kappa \in \bar{\mathbb{Q}}$, rational numbers

$$l_1^{(0)}, l_1^{(1)}, \ldots, l_j^{(0)}, l_j^{(1)}, \ldots, l_{j+1}^{(0)}, l_{j+1}^{(1)}, \ldots \in \mathbb{Q}$$

such that not all $l_{j+1}^{(1)}, l_{j+1}^{(2)}, \ldots$ are zeroes and

$$X_{j+1}^{l_{j+1}^{(0)} + \sum_{k\ge 1} l_{j+1}^{(k)} \theta_{j+1}^{(k)}} = \kappa X_1^{l_1^{(0)} + \sum_{k\ge 1} l_1^{(k)} \theta_1^{(k)}} \cdots X_j^{l_j^{(0)} + \sum_{k\ge 1} l_j^{(k)} \theta_j^{(k)}}$$

but this leads to a contradiction since the derivative $\frac{d}{dX_{j+1}}$ of the left side is nonzero, but of the right side equals to zero.

For each $1 \le i \le t$ consider a $\mathbb{Q}$-basis $\bar{\eta}_i^{(1)}, \bar{\eta}_i^{(2)}, \ldots \in \bar{\mathbb{Q}}$ of the $\mathbb{Q}$-linear hull $\mathbb{Q}\{\beta_i^{(s)}, \delta_i^{(s)}\}_{i+1\le s\le t+1}$. If 1 (thereby $\mathbb{Q}$) is contained in the latter linear hull, then we set $\bar{\eta}_i^{(1)} = 1$. Denote $\{\eta_i^{(1)}, \eta_i^{(2)}, \ldots\} = \{\bar{\eta}_i^{(1)}, \bar{\eta}_i^{(2)}, \ldots\} \setminus \{1\}$.

Denote by E_i, $0 \le i \le t$ a field generated over F_n by the elements

$$\log u_1, u_1^{\eta_1^{(1)}}, u_1^{\eta_1^{(2)}}, \ldots, \log u_i, u_i^{\eta_i^{(1)}}, u_i^{\eta_i^{(2)}}, \ldots .$$

It is a log-explicit extension of its field of constants $\bar{\mathbb{Q}}$.

We claim that for $0 \le i \le t-1$ the elements $u_{i+1}^{\eta_{i+1}^{(1)}}, u_{i+1}^{\eta_{i+1}^{(2)}}, \ldots \in E_{i+1}$ are algebraically independent over the field $E_i(\log u_{i+1})$. Assume the contrary. Then again using corollary 3.2 [RC 79] we conclude that there exist a constant $\varepsilon \in \bar{\mathbb{Q}}$, rational numbers

$$p_1, p_1^{(1)}, p_1^{(2)}, \ldots, p_n, p_n^{(1)}, p_n^{(2)}, \ldots, z_1, z_1^{(1)}, z_1^{(2)}, \ldots, z_{i+1}, z_{i+1}^{(1)}, z_{i+1}^{(2)}, \ldots \in \mathbb{Q}$$

such that not all $z_{i+1}^{(1)}, z_{i+1}^{(2)}, \ldots$ are zeroes and

$$u_{i+1}^{z_{i+1} + \sum_{j\ge 1} z_{i+1}^{(j)} \eta_{i+1}^{(j)}} = \varepsilon X_1^{p_1 + \sum_{j\ge 1} p_1^{(j)} \theta_1^{(j)}} \cdots X_n^{p_n + \sum_{j\ge 1} p_n^{(j)} \theta_n^{(j)}} u_1^{z_1 + \sum_{j\ge 1} z_1^{(j)} \eta_1^{(j)}} \cdots u_i^{z_i + \sum_{j\ge 1} z_i^{(j)} \eta_i^{(j)}} .$$

This provides an expression of u_{i+1} as a product of powers of $X_1, \ldots, X_n, u_1, \ldots u_i$ and thereby we can diminish t by one in the computation of f, this contradiction with the minimality of t proves the algebraic independency of $u_{i+1}^{\eta_{i+1}^{(1)}}, u_{i+1}^{\eta_{i+2}^{(2)}}, \ldots$ over $E_i(\log u_{i+1})$.

Consider the expansions

$$\begin{aligned} \alpha_j^{(s)} &= a_j^{(s)} + \sum_{k\ge 1} a_{j,k}^{(s)} \theta_j^{(k)}, \gamma_j^{(s)} = \quad c_j^{(s)} + \sum_{k\ge 1} c_{j,k}^{(s)} \theta_j^{(k)}, \quad 1 \le j \le n, \qquad 1 \le s \le t+1 \\ \beta_i^{(s)} &= b_i^{(s)} + \sum_{k\ge 1} b_{i,k}^{(s)} \eta_i^{(k)}, \delta_i^{(s)} = \quad d_i^{(s)} + \sum_{k\ge 1} d_{i,k}^{(s)} \theta_i^{(k)}, \quad 1 \le i \le t+1, \quad i < s \le t+1 \end{aligned} \tag{2}$$

where $a_j^{(s)},\dots,d_{i,k}^{(s)}\in\mathbb{Q}$ are suitable rationals. Remark that if $1\notin\{\bar\theta_j^{(1)},\bar\theta_j^{(2)},\dots\}$ then $a_j^{(s)}=c_j^{(s)}=0$, also if $1\notin\{\bar\eta_i^{(1)},\bar\eta_i^{(2)},\dots\}$ then $b_i^{(s)}=d_i^{(s)}=0$. Then the initial computation $u_1,u_2,\dots$ we can rewrite as follows:

$$\begin{aligned}u_{i+1}=\ &\varepsilon^{(i+1)}X_1^{a_1^{(i+1)}}(X_1^{\theta_1^{(1)}})^{a_{1,1}^{(i+1)}}(X_1^{\theta_1^{(2)}})^{a_{1,2}^{(i+1)}}\cdots X_n^{a_n^{(i+1)}}(X_n^{\theta_n^{(1)}})^{a_{n,1}^{(i+1)}}\cdots\\ &u_1^{b_1^{(i+1)}}(u_1^{\eta_1^{(1)}})^{b_{1,1}^{(i+1)}}(u_1^{\eta_1^{(2)}})^{b_{1,2}^{(i+1)}}\cdots u_i^{b_i^{(i+1)}}(u_i^{\eta_i^{(1)}})^{b_{i,1}^{(i+1)}}(u_i^{\eta_i^{(2)}})^{b_{i,2}^{(i+1)}}\cdots+\\ &\kappa^{(i+1)}X_1^{c_1^{(i+1)}}(X_1^{\theta_1^{(1)}})^{c_{1,1}^{(i+1)}}(X_1^{\theta_1^{(2)}})^{c_{1,2}^{(i+1)}}\cdots X_n^{c_n^{(i+1)}}(X_n^{\theta_n^{(1)}})^{c_{n,1}^{(i+1)}}\cdots\\ &u_1^{d_1^{(i+1)}}(u_1^{\eta_1^{(1)}})^{d_{1,1}^{(i+1)}}(u_1^{\eta_1^{(2)}})^{d_{1,2}^{(i+1)}}\cdots u_i^{d_i^{(i+1)}}(u_i^{\eta_i^{(1)}})^{d_{i,1}^{(i+1)}}(u_i^{\eta_i^{(2)}})^{d_{i,2}^{(i+1)}}\cdots\end{aligned}\tag{3}$$

From the latter expression one can show by induction on i that u_{i+1} (and thereby each of the previous elements $u_1,\dots,u_i$) is algebraic over the field $E_i'\subset E_i$ generated over $\bar{\mathbb{Q}}(X_1,\dots,X_n)$ by the elements

$$X_1^{\theta_1^{(1)}},X_1^{\theta_1^{(2)}},\dots,X_n^{\theta_n^{(1)}},X_n^{\theta_n^{(2)}},\dots,u_1^{\eta_1^{(1)}},u_1^{\eta_1^{(2)}},\dots,u_i^{\eta_i^{(1)}},u_i^{\eta_i^{(2)}},\dots$$

Above we have proved that the latter elements are algebraically independent over $\bar{\mathbb{Q}}(X_1,\dots,X_n)$. As $u_{t+1}=f\in\bar{\mathbb{Q}}(X_1,\dots,X_n)$ we can substitute in the expression (3) instead of the elements

$$X_1^{\theta_1^{(1)}},X_1^{\theta_1^{(2)}},\dots,X_n^{\theta_n^{(1)}},X_n^{\theta_n^{(2)}},\dots,u_1^{\eta_1^{(1)}},u_1^{\eta_1^{(2)}},\dots,u_t^{\eta_t^{(1)}},u_t^{\eta_t^{(2)}},\dots$$

almost (in the sense of Zariski topology) arbitrary constants

$$y_1^{(1)},y_1^{(2)},\dots,y_n^{(1)},y_n^{(2)},\dots,z_1^{(1)},z_1^{(2)},\dots,z_t^{(1)},z_t^{(2)},\dots\in\bar{\mathbb{Q}},$$

respectively, with the mere requirement that in the intermediate computations of $u_1,u_2,\dots,u_{t+1}=f$ there is no taking nonpositive powers of zero (each time we choose some branch of a rational power).

As a result we get a computation of $\tilde u_1,\tilde u_2,\dots,\tilde u_{t+1}=f$ in which only rational exponents occur, namely

$$\tilde u_{i+1}=\tilde\varepsilon^{(i+1)}X_1^{a_1^{(i+1)}}\cdots X_n^{a_n^{(i+1)}}\tilde u_1^{b_1^{(i+1)}}\cdots\tilde u_i^{b_i^{(i+1)}}+\tilde\kappa^{(i+1)}X_1^{c_1^{(i+1)}}\cdots X_n^{c_n^{(i+1)}}\tilde u_1^{d_1^{(i+1)}}\cdots\tilde u_i^{d_i^{(i+1)}}\tag{4}$$

for some $\tilde\varepsilon^{(i+1)},\ \tilde\kappa^{(i+1)}\in\bar{\mathbb{Q}}$. The proposition is proved.

From the proof of the proposition we extract the

Corollary. *For every $1\le i\le t$, $1\in\mathbb{Q}\{\beta_i^{(s)},\delta_i^{(s)}\}_{i+1\le s\le t+1}$. For any $\mathbb{Q}$-basis $\bar\theta_j^{(1)},\bar\theta_j^{(2)},\dots$ of $\mathbb{Q}\{\alpha_j^{(s)},\gamma_j^{(s)}\}_{1\le s\le t+1}$ and any $\mathbb{Q}$-basis $\bar\eta_i^{(1)},\bar\eta_i^{(2)},\dots$ of $\mathbb{Q}\{\beta_i^{(s)},\delta_i^{(s)}\}_{i+1\le s\le t+1}$ we get the rational exponents of the resulting computation of $\tilde u_1,\dots,\tilde u_{t+1}$ (see (4)) from the expansions (2).*

In order to show that $1\in\mathbb{Q}\{\beta_i^{(s)},\delta_i^{(s)}\}_s$ observe that otherwise $b_i^{(s)}=d_i^{(s)}=0$ for all $i+1\le s\le t+1$ and we could diminish t by deleting $\tilde u_i$ from the computation $\tilde u_1,\dots,\tilde u_{t+1}$ and get a contradiction with a minimality of t.

Remark that the corollary together with lemma 12 [GKS 92a] entail that for any i the constructible set of all the possible exponent vectors $(\beta_i^{(i+1)}, \ldots, \beta_i^{(t+1)}, \delta_i^{(i+1)}, \ldots, \delta_i^{(t)}) \in \bar{\mathbb{Q}}^{2t-2i+1}$ is contained in a finite union of the hyperplanes of the kind

$$\sum_{i+1 \le j \le t+1} \hat{b}_i^{(j)} \beta_i^{(j)} + \sum_{i+1 \le j \le t} \hat{d}_i^{(j)} \delta_i^{(j)} = \hat{d}$$

where $\hat{b}_i^{(j)}, \hat{d}_i^{(j)}, \hat{d} \in \mathbb{Z}$. The similar holds also for the vectors $(\alpha_i^{(1)}, \ldots, \alpha_i^{(t+1)}, \gamma_i^{(1)}, \ldots, \gamma_i^{(t)}) \in \bar{\mathbb{Q}}^{2t+1}$. But we will not use this remark.

Note also that in the resulting computation (4) the rational exponents depend on the choice of the $\mathbb{Q}$-basis (see the corollary). The following simple example demonstrates that the dependency really can happen:

$$u_1 = X^{\alpha}(X+1), u_2 = X^{-a\alpha} u_1^a + X^{-b\alpha} u_1^b = (X+1)^a + (X+1)^b$$

where $\alpha \in \bar{\mathbb{Q}} \setminus \mathbb{Q}, a, b \in \mathbb{Q}$. Choosing a basis $\alpha + z, 1 \in \mathbb{Q}\{1, \alpha\}$, for arbitrary $z \in \mathbb{Q}$, we get

$$\begin{aligned} u_1 &= (X^{\alpha+z})X^{1-z} + (X^{\alpha+z})X^{-z} \\ u_2 &= (X^{\alpha+z})^{-a} X^{za} u_1^a + (X^{\alpha+z})^{-b} X^{zb} u_1^b \end{aligned}$$

and by the corollary

$$\begin{aligned} u_1 &= wX^{1-z} + wX^{-z} \\ u_2 &= w^{-a} X^{za} u_1^a + w^{-b} X^{zb} u_1^b \end{aligned}$$

for arbitrary $w \in \bar{\mathbb{Q}} \setminus \{0\}$.

4 Constructing a generalized additive-minimal computation

The previous two sections (see lemma and corollary) give us a possibility to compute a generalized additive complexity t of a rational function f. Now we complete an algorithm which finds some generalized additive-minimal circuit computing f. Using the corollary from the section 3 the algorithm finds rational exponents $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)} \in \mathbb{Q}, 0 \le i \le t$, it remains to find the coefficients $\varepsilon^{(i+1)}, \kappa^{(i+1)} \in \bar{\mathbb{Q}}, 0 \le i \le t$.

Denote by $\mathcal{M}$ a bound on the bit-sizes of the rational exponents $\alpha_1^{(i+1)}, \ldots, \delta_i^{(i+1)} \in \mathbb{Q}, 0 \le i \le t$. Then by induction on i one can easily show that each $u_{i+1}, v_1^{(i+1)}, \ldots, \tilde{w}_i^{(i+1)}$, $0 \le i \le t$ is an algebraic function of the degree (i.e. the degree of a minimal polynomial to which satisfies

the function) at most $N = (\exp(\mathcal{M}))^{t^{O(t)}}$. Hence the coefficients $\varepsilon^{(i+1)}, \kappa^{(i+1)}$, $0 \le i \le t$ fit if and only if for every $1 \le x_1, \ldots, x_n \le N^2$ for which all the intermediate computations of the circuit are definable, the equality $u_{t+1}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ holds. So, for every fixed $1 \le x_1, \ldots, x_n \le N^2$ we introduce the variables

$$u_{t+1}(x_1, \ldots, x_n), v_1^{(i+1)}(x_1, \ldots, x_n), \ldots, \tilde{w}_i^{(i+1)}(x_1, \ldots, x_n),\ 0 \le i \le t$$

and write down a system of polynomial equations and inequalities expressing all the operations of the circuit (provided that they are all definable) and finally the relation $u_{t+1}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Then the algorithm invoking [CG 83] solves this system in $N^{2n} + 2t + 1$ variables and finds in particular $\varepsilon^{(i+1)}, \kappa^{(i+1)} \in \bar{\mathbb{Q}}, 0 \le i \le t$. More precisely, for each subset $J \subset \{1, \ldots, N^2\}^n$ we consider a system as above including in it just the points $(x_1, \ldots, x_n) \in J$ (so, J plays the role of the set of points in which the computation is defined). The algorithm solves this system and takes J with the maximal cardinality for which the system is solvable. In a more sophisticated way we can partition the cube $\{1, \ldots, N^2\}^n$ into N^n subcubes with sides equal to N and as J take each of these subcubes, but this improvement does not change the complexity bounds below.

In the ordinary case ($n = 1$) we can bound the complexity of the described algorithm. First, observe that in this case $\mathcal{M} \le M^{O(1)}(degf)^{2^{2^{O(t^2)}}}$ (see the end of the section 1). Therefore, the system of polynomial equations and inequalities constructed above contains $\exp(M^{O(1)}(degf)^{2^{2^{O(t^2)}}})$ polynomials of degrees at most $\exp(M^{O(1)}(degf)^{2^{2^{O(t^2)}}})$in $\exp(M^{O(1)}(degf)^{2^{2^{O(t^2)}}})$ variables. Hence one can solve it using the algorithm from [CG 83] in time $\exp(\exp(M^{O(1)}(degf)^{2^{2^{O(t^2)}}}))$ and find $\varepsilon^{(i+1)}, \kappa^{(i+1)} \in \bar{\mathbb{Q}}, 0 \le i \le t$ representing them as algebraic numbers as at the end of section 1 with the size bounded also by the latter value. Summarizing, we formulate

Theorem.

a) There is an algorithm calculating the generalized additive complexity of a rational function $f \in \mathbb{Q}(x_1, \ldots, x_n)$ and constructing a generalized additive-minimal circuit computing f;

b) In the case of one-variable rational functions f the running time of the algorithm from a) can be bounded by $\exp(\exp(M^{O(1)}(degf)^{2^{2^{O(t^2)}}}))$*, where M bounds the bit-size of each (rational) coefficient of f. The absolute values of the numerators and denominators of the found rational exponents in a generalized additive-minimal circuit computing f do not exceed* $\exp(M^{O(1)}(degf)^{2^{2^{O(t^2)}}})$.

At the end we demonstrate that there could be a big gap between the the additive complexity

and generalized additive complexity. Consider a polynomial

$$f_n = (1 + X^{\frac{1}{2}})^n + (1 - X^{\frac{1}{2}})^n \in \mathbb{Z}[X]$$

with the generalized additive complexity at most 3. As all its $\lfloor \frac{n}{2} \rfloor$ roots are negative reals, the additive complexity of f_n is at least $\Omega((\log n)^{\frac{1}{2}})$ because of the result of [G 83] (see also [Ri 85]) based on the method from [Kh 91].

5 Further Research

It remains an interesting open problem on improving the complexity bounds of our algorithm. It will be also very interesting to shed some more light on the status of the problem of computing *standard additive* complexity of rational functions. At this point we do not know much about this problem.

Acknowledgments

We are thankful to Richard Cleve for starting us up to think about the additive complexity of polynomials, and to Allan Borodin, Joachim von zur Gathen, Thomas Lickteig, Michael Singer, Volker Strassen, and Andy Yao for many interesting discussions.

References

[BC 76] Borodin, A., and Cook, S., *On the number of additions to compute specific polynominals*, SIAM J. Computing **5** (1976), pp. 146-157.

[C 86] Chistov, A., *Algorithms of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Soviet Math. **34** (1986), pp. 1838-1882.

[CG 83] Chistov, A., and Grigoriev, D., *Subexponential-time solving systems of algebraic equations*, LOMI Preprints E-9-83, E-10-83, Steklov Math. Institute, 1983.

[G 82] Grigoriev, D., *Additive complexity in directed computations*, Theor. Comp. Sci., **19** 1982, pp. 39-67.

[G 83] Grigoriev, D., *Lower bounds in algebraic complexity*, Transl. in J. Soviet Math. **29**, 1985, pp. 1388-1425.

[G 89] Grigoriev, D., *Complexity of quantifier elimination in the theory of differential equations*, Lect. Notes Comput. Sci. **378**, 1989, pp. 11-25.

[GK 91] Grigoriev, D., and Karpinski, M., *Algorithms for Sparse Rational Interpolation*, Proc. ACM ISSAC, 1991, pp. 7-13.

[GKS 90] Grigoriev, D., Karpinski, M., and Singer, M., *Interpolation of Sparse Rational Functions without Knowing Bounds on Exponents*, Proc. 31^{st} IEEE FOCS, 1990, pp. 840-846.

[GKS 92a] Grigoriev, D., Karpinski, M., and Singer, M., *Computational complexity of sparse rational interpolation*, SIAM J. Computing **23** (1994), pp. 1-11.

[GKS 92b] Grigoriev, D., Karpinski, M., and Singer, M., *Computational complexity of sparse real algebraic function interpolation*, to appear in Proc. MEGA '92, Nice, 1992, Progr. in Math. Birkhäuser. Vol. **109** (1993), pp. 91-104.

[GSY 93] Grigoriev, D., Singer, M., and Yao, A., *On Computing Algebraic Functions using Logarithmus and Exponentials*, SIAM J. Computing **24** (1995), pp. 242-246.

[J 81] Ja'Ja', J., *Computations of algebraic functions with root extractios*, Proc. 22^{nd} IEEE FOCS, 1981, pp. 95-100.

[KW 93] Karpinski, M., Werther, Th., *VC Dimension and Uniform Learnability of Sparse Polynomials and Rational Functions*, SIAM J. Computing **22** (1993), pp. 1276-1285.

[Kh 91] Khovanski, A., *Fewnomials*, AMS Transl. Math. Monogr. **88**, 1991.

[P 81] Pippenger, N., *Computational Complexity of Algebraic Functions*, J. of Computer and System Sciences **22**, 1981, pp. 454-470.

[Ri 85] Risler, J. J., *Additive complexity and zeros of real polynomials*, SIAM J. Comput. **14**, 1985, pp. 178-183.

[Ro 76] Rosenlicht, M., *On Liouville's theory of elementary functions*, Pacif. J. Math. **65**, N 2, 1976, pp. 485-492.

[RC 79] Rothstein, M., and Caviness, B., *A structure theorem for exponential and primitive functions*, SIAM J. Comput. **8**, N 3, 1979, pp. 357-366.

[Se 56] Seidenberg, A., *An elimination theory for differential algebra*, Univ. of Calif. Press **3**, N 2, 1956, pp. 31-66.

[SW 80] Schnorr, C., and Wiele van de, J., *On the additive complexity of polynomials*, Theor. Comp. Sci. **10**, 1980, pp. 1-18.

[W 78] van de Wiele, J.P., *Complexité additive et zéros des polynômes à coefficents réels et complexes*, Rapport de Recherce Laboria N$^{\text{o}}$ 292 (Mars 1978).