Theoretical Computer Science 64 (1989) 1-13
North-Holland

ON THE REPRESENTATION OF RATIONAL FUNCTIONS OF BOUNDED COMPLEXITY

Hans-Jörg STOß

Department of Mathematics, Universität Konstanz, Postfach 5560, Konstanz D-7750, Fed. Rep. Germany

Communicated by A. Schönhage
Received June 1986
Revised February 1988

Abstract. The main result of this article is the Representation Theorem which characterizes families of rational functions of bounded complexity by appropriate mappings. This description is not only independent of the characteristic of the underlying field but also of the specific complexity measure under consideration. As an application of the Representation Theorem we derive good lower complexity bounds.

1. Introduction

An important problem in complexity theory is to determine the complexity of evaluating a finite set of rational functions. A very powerful method to treat that problem was introduced by Strassen [12]. He discovered polynomial mappings which describe families of functions with bounded complexity. In the meantime this idea has been applied and modified in many cases, see, e.g., Borodin-Cook [1], Schnorr [8], Schnorr-van de Wiele [9], Heintz-Sieveking [6], Heintz-Schnorr [5], von zur Gathen-Strassen [3]. It is striking that all those articles need restrictions with respect to the complexity measures or the field of coefficients under consideration, let alone additional more technical assumptions.

In the present article we present a version of the Representation Theorem which does not only include the particular cases mentioned above, but also provides further results and holds completely independently of the complexity measure and the characteristic of the field. The main technical device in the proof is to replace the polynomial mappings, considered so far, by elements of an appropriate algebra (see Section 3).

As far as applications are concerned we restrict our considerations in this article to a simultaneous proof of lower bounds for the complexity of polynomials with algebraic coefficients. They turn out to be optimal with respect to the order of magnitude. These results have only been established in several special cases with specific proofs every time.

In a separate article [10] we give further applications of the Representation Theorem and prove lower complexity bounds which hold for large classes of polynomials, e.g., for polynomials with 0-1-coefficients, divisors or multiples of given polynomials. We use the following model of computation (see, e.g., Strassen [11], Borodin–Munro [2]).

Let G be a field with primefield E, $x_1,\dots,x_n$ indeterminates and $G(x)$ the field of rational functions in $x_1,\dots,x_n$. A computation sequence β in $G(x)$ is a sequence $\beta=(r_1,\dots,r_k)\in G(x)^k$ where for all $i=1,\dots,k$ either $r_i\in G\cup\{x_1,\dots,x_n\}$ or $r_i=r_j\circ r_l$ with $1\leq j$, $l\leq i$ and $\circ\in\{+,-,*,/\}$ and $r_l\neq 0$ in case of division. A set $\{f_1,\dots,f_m\}\subset G(x)$ is said to be computed by β if $\{f_1,\dots,f_m\}\subset\{r_1,\dots,r_k\}$. Let F be a subfield of G. We call an operation $r_i=r_j\circ r_l$ a F-nonscalar operation if r_j and $r_l\in G(x)\setminus F$ and $\circ=*$ or if $r_l\in G(x)\setminus F$ and $\circ=/$. We consider the complexity measures

$L_F(\beta):=\#$ of F-nonscalar operations in β,

$L_+(\beta):=\#$ of additions or subtractions in β,

$L_{\mathrm{tot}}(\beta):=\#$ of all arithmetic operations in β.

For $F=G$ the measure L_F is just the Ostrowsky complexity, L_E is essentially the measure which counts all multiplicative operations. For any complexity measure $L\in\{L_F, L_+, L_{\mathrm{tot}}\}$ and $f_1,\dots,f_m\in G(x)$ we define the complexity

$$L(f_1,\dots,f_m):=\min\{L(\beta)\mid\beta\text{ computes }\{f_1,\dots,f_m\}\}.$$

Before discussing the details we describe briefly the main ideas which lead to the Representation Theorem. First of all we combine generic computations for the complexity measures under consideration into one recursion scheme (see (2.1)) which, by specification of its free parameters, allows every family $(f_1,\dots,f_m)$ of functions with complexity say $\leq t$ to be represented.

The use of generic computations is a common technique for this subject but a more detailed analysis leads to technical complications. Therefore we replace that recursion scheme (2.1) by another scheme (2.5) which also allows all families $(f_1,\dots,f_m)$ with complexity $\leq t$ to be represented and is better adapted to our futher consideration. Next we expand rational functions into power series and obtain the desired mappings which describe families with complexity $\leq t$ from the coefficients of the power series expansions of certain functions defined by that recursion scheme (2.5).

In Section 3 we analyse the algebraic properties of those mappings. It turns out that in the case of the characteristic $\mathrm{char}(G)=0$ they are given by polynomials while in the general case we can describe them by elements in a tensor product of a ring of polynomials over the rational numbers and a full polynomial ring over the prime field E of G.

2. Recursions for functions of bounded complexity

Let β be a computation for $f_1,\dots,f_m\in G(x)$ with $L_F(\beta)=t$. We can transform β by collecting uncounted steps into the following recursion scheme:

$$P_{-n+j}:=x_j\quad(j=1,\dots,n),$$

$$T_i' := y_i' + \sum_{j=-n+1}^{i-1} v_{ij}' P_j, \qquad T_i'' := y_i'' + \sum_{j=-n+1}^{i-1} v_{ij}'' P_j,$$

$$P_i := z_i T_i' * T_i'' + (1 - z_i) T_i' / T_i'' \qquad (i = 1, \ldots, t),$$

$$f_\mu = T_{t+\mu} := y_{t+\mu} + \sum_{j=-n+1}^{t} v_{t+\mu,j} P_j \quad (\mu = 1, \ldots, m).$$

P_i $(i = 1, \ldots, t)$ are the results of the nonscalar steps, the parameters y_i', y_i'', $y_i \in G$, v_{ij}', v_{ij}'', $v_{ij} \in F$ express the uncounted scalar steps and $z_i \in \{0, 1\}$ gives the type of the ith nonscalar operation. This scheme is known as "generic computation".

In a similar way we can transform a computation β with $L_+(\beta) = t$ into a recursion. We collect uncounted steps into terms of the form

$$S_i' := y_i' \prod_{j=-n+1}^{i-1} P_j^{u_{ij}'}, \qquad S_i'' := y_i'' \prod_{j=-n+1}^{i-1} P_j^{u_{ij}''},$$

with y_i', $y_i'' \in G$, u_{ij}', $u_{ij}'' \in \mathbb{Z}$ and express the counted additions/subtractions by

$$P_i := S_i' + z_i S_i'' \quad \text{with } z_i \in \{+1, -1\}.$$

We combine these recursion schemes to the following generalized generic computation scheme where the parameters u_{ij}', u_{ij}'' range over $\mathbb{Z}$, all others over G.

Given m, n, $t \in \mathbb{N}$, define for $j = 1, \ldots, n$, $P_{-n+j} := x_j$ and for $i = 1, \ldots, t + m$ define $t(i) := \min\{i - 1, t\}$ and

$$S_i' := y_{i1}' \prod_{j=-n+1}^{t(i)} P_j^{u_{ij}'}, \qquad S_i'' := y_{i1}'' \prod_{j=-n+1}^{t(i)} P_j^{u_{ij}''},$$

$$T_i' := y_{i2}' + \sum_{j=-n+1}^{t(i)} v_{ij}' P_j, \qquad T_i'' := y_{i2}'' + \sum_{j=-n+i}^{t(i)} v_{ij}'' P_j, \tag{2.1}$$

$$P_i := y_{i3} S_i' + y_{i4} S_i'' + y_{i5} T_i' * T_i'' + y_{i6} T_i' / T_i'' + y_{i7} T_i'.$$

This recursion scheme contains

$$r := 2\left(\sum_{i=1}^{t} (n + i - 1) + \sum_{i=t+1}^{t+m} (n + t)\right) = (t + 2m)(t + 2n - 1) - 2m(n - 1) \tag{2.2}$$

exponents u, the same number of parameters v and say s' parameters y. Clearly, this recursion defines for every choice $(\mathring{u}, \mathring{v}, \mathring{y}) \in Z^r \times G^r \times G^{s'}$ rational functions $P_i(\mathring{u}, \mathring{v}, \mathring{y})(x)$, $S_i'(\mathring{u}, \mathring{v}, \mathring{y})(x), \ldots \in G(x)$ provided there is no division by zero. We call a choice admissible if all these functions are defined and not the zero element of $G(x)$. The construction of that recursion scheme easily yields this: if $L \in \{L_F, L_+, L_{\text{tot}}\}$ is a complexity measure and $f_1, \ldots, f_m \in G(x)$ are functions with $L(f_1, \ldots, f_m) \leq t$ then there is a choice $(\mathring{u}, \mathring{v}, \mathring{y})$ of parameters in (2.1) such that

$$f_\mu(x) = P_{t+\mu}(\mathring{u}, \mathring{v}, \mathring{y})(x) \quad (\mu = 1, \ldots, m)$$

holds. Moreover, this remains valid if we restrict the parameters u, v to certain sets $M(L) \subset \mathbb{Z}^r \times G^r$ depending on the complexity measure under consideration:

To model computations β with $L_F(\beta) \leq t$ it is enough to choose in (2.1) parameters

$$(\mathring{u}, \mathring{v}) \in M(L_F) := \{0\}^r \times F^r. \tag{2.3a}$$

Likewise, parameters

$$(\mathring{u}, \mathring{v}) \in M(L_+) := \mathbb{Z}^r \times \{0\}^r \tag{2.3b}$$

allow computations β with $L_+(\beta) \leq t$ to be modelled. Finally, we can model computations β with $L_{\text{tot}}(\beta) \leq t$. Here it is enough to choose

$$(\mathring{u}, \mathring{v}) \in M(L_{\text{tot}}) \tag{2.3c}$$

which consists of all pairs $(\mathring{u}, \mathring{v}) \in \{0, 1\}^r \times \{0, 1\}^r \subset \mathbb{Z}^r \times G^r$ where for all i at most one of the u'_{ij} equals 1 and ditto for the u''_{ij}, v'_{ij}, v''_{ij}. This set contains at most $(t+m+1)^{4(t+m)}$ elements.

From these observations the proof of the following lemma is quite simple.

Lemma 2.1. *Let $L \in \{L_F, L_+, L_{\text{tot}}\}$ be a complexity measure and $f_1, \ldots, f_m \in G(x)$ nontrivial functions with $L(f_1, \ldots, f_m) \leq t$. Then there is an admissible choice*

$$(\mathring{u}, \mathring{v}, \mathring{y}) \in M(L) \times G^{s'} \subset \mathbb{Z}^r \times G^r \times G^{s'}$$

for the parameters of the recursion (2.1) *such that*

$$f_\mu(x) = P_{t+\mu}(u, v, y)(x) \quad (\mu = 1, \ldots, m). \tag{2.4}$$

Our goal is to describe functions of bounded complexity. Lemma 2.1 is a first step in that direction. But though the definition of the recursion scheme (2.1) is quite natural the solutions P_i of (2.1) are only partially defined with respect to the parameters u, v, y and thus several technical complications arise for a more detailed analysis of the P_i.

To avoid these problems our next step is to replace the recursion (2.1) by the recursion (2.5) below which has solutions for every choice of its parameters and again allows a result similar to Lemma 2.1 to be proved. In that scheme the parameters u range over $\mathbb{Z}$, the parameters v over G and the w's over H which denotes an extension field of G of infinite cardinality.

Given $m, n, t \in \mathbb{N}$, define for $j = 1, \ldots, n$, $R_{-n+j} := 1 + w_{j0}x_j$ and for $i = 1, \ldots, t+m$, define $t(i) := \min\{i-1, t\}$ and

$$\begin{aligned}
U'_i &:= \prod_{j=n+1}^{t(i)} R_j^{u'_{ij}}, \qquad U''_i := \prod_{j=n+1}^{t(i)} R_j^{u''_{ij}},\\
V'_i &:= 1 + \left[w'_{i1} \sum_{j=-n+1}^{t(i)} v'_{ij} w_{j2}(R_j - 1) \right],\\
V''_i &:= 1 + \left[w''_{i1} \sum_{j=-n+1}^{t(i)} v''_{ij} w_{j2}(R_j - 1) \right],\\
R_i &:= 1 + [w_{i3}(U'_i - 1) + w_{i4}(U''_i - 1) + w_{i5}(V'_i * V''_i - 1)\\
&\qquad + w_{i6}(V'_i / V''_i - 1) + w_{i7}(V'_i - 1)].
\end{aligned} \tag{2.5}$$

Finally, define for $\mu = 1, \dots, m, Q_\mu := w_{t+\mu,2} R_{t+\mu}$. This scheme (2.5) contains again r (see (2.2)) exponents u, the same number of parameters v and

$$s := 8(t+m)+2n \tag{2.6}$$

parameters w.

Proposition 2.2. *For every choice* $(\mathring{u}, \mathring{v}, \mathring{w}) \in \mathbb{Z}^r \times G^r \times G^s$ *of parameters recursion* (2.5) *defines functions*

$$R_i(\mathring{u}, \mathring{v}, \mathring{w})(x),\ U_i'(\mathring{u}, \mathring{v}, \mathring{w})(x), \dots, Q_i(\mathring{u}, \mathring{v}, \mathring{w})(x) \in H(x).$$

For the proof of this proposition and for later use observe the following fact.

Proposition 2.3. *For every choice of the parameters it holds that*

$$\begin{aligned} &R_i(\mathring{u}, \mathring{v}, \mathring{w})(0) = 1 && (i = -n+1, \dots, t+m), \\ &U_i'(\mathring{u}, \mathring{v}, \mathring{w})(0) = \cdots = V_i''(\mathring{u}, \mathring{v}, \mathring{w})(0) = 1 && (i = 1, \dots, t+m), \\ &Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(0) = w_{t+\mu,2} && (\mu = 1, \dots, m). \end{aligned}$$

The next proposition connects both recursions. The P_i are defined by (2.1), the Q_μ by (2.5).

Proposition 2.4. *Given an admissible choice* $(\mathring{u}, \mathring{v}, \mathring{y}) \in \mathbb{Z}^r \times G^r \times G^{s'}$ *of parameters for* (2.1) *there is a hypersurface* $K \subsetneq H^n$ *with coefficients in* G *with the following property*: *For every* $\lambda \in H^n \backslash K$ *we can choose* $\mathring{w} \in H^s$ *such that for* $\mu = 1, \dots, m$

$$P_{t+\mu}(\mathring{u}, \mathring{v}, \mathring{y})(x) = Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x - \lambda).$$

Proof. Let $(\mathring{u}, \mathring{v}, \mathring{y})$ be admissible for (2.1) and let P_i, S_i', etc. denote the functions defined by (2.1) with that choice. Then all these functions are well defined and nontrivial $\in G(x)$. We can represent these functions as quotients of polynomials $\in G[x]$ and the product of all these polynomials is a nontrivial polynomial $k \in G[x]$. Because H is infinite the zeros of k form a hypersurface $K \subsetneq H^n$ and for all $\lambda \in H^n \backslash K$ the values $P_i(\lambda)$ $(i = -n+1, \dots, t+m)$ respectively $S_i'(\lambda), \dots, T_i''(\lambda)$ $(i = 1, \dots, t+m)$ are defined and $\neq 0$. A straightforward induction shows that the normed functions

$$R_i(x) := \frac{P_i(x+\lambda)}{P_i(\lambda)}, \qquad U_i'(x) := \frac{S_i'(x+\lambda)}{S_i'(\lambda)}, \qquad U_i''(x) := \frac{S_i''(x+\lambda)}{S_i''(\lambda)},$$

$$V_i'(x) := \frac{T_i'(x+\lambda)}{T_i'(\lambda)}, \qquad V_i''(x) := \frac{T_i''(x+\lambda)}{T_i''(\lambda)}$$

are solutions of the recursion (2.5) if we choose the parameters (u, v) in (2.5) as $(\mathring{u}, \mathring{v})$ and define the w's as follows:

$$\mathring{w}_{j0} := \frac{1}{\lambda_j} \quad (j = 1, \dots, n),$$

$$\mathring{w}'_{i1} := \frac{1}{T_i'(\lambda)},$$

$$\mathring{w}''_{i1} := \frac{1}{T_i''(\lambda)} \quad (i = 1, \dots, t+m),$$

$$\mathring{w}_{i2} := P_i(\lambda) \quad (i = -n+1, \dots, t+m) \quad \text{and}$$

$$\mathring{w}_{i3} := \mathring{y}_{i3} \frac{S_i'(\lambda)}{P_i(\lambda)}, \qquad \mathring{w}_{i4} := \mathring{y}_{i4} \frac{S_i''(\lambda)}{P_i(\lambda)}, \qquad \mathring{w}_{i5} := \mathring{y}_{i5} \frac{T_i'(\lambda) * T_i''(\lambda)}{P_i(\lambda)},$$

$$\mathring{w}_{i6} := \mathring{y}_{i6} \frac{T_i'(\lambda)}{P_i(\lambda) T_i''(\lambda)}, \qquad \mathring{w}_{i7} := \mathring{y}_{i7} \frac{T_i'(\lambda)}{P_i(\lambda)} \quad (i = 1, \dots, t+m).$$

From this we get for $\mu = 1, \dots, m$

$$Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x) = \mathring{w}_{t+\mu,2} R_{t+\mu}(x) = P_{t+\mu}(\lambda) \frac{P_{t+\mu}(x+\lambda)}{P_{t+\mu}(\lambda)} = P_{t+\mu}(x+\lambda),$$

respectively,

$$Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x-\lambda) = P_{t+\mu}(x). \quad \square$$

By Proposition 2.4 we can replace in Lemma 2.1 the $P_{t+\mu}$ by the Q_μ. This yields the following lemma.

Lemma 2.5. *Let $L \in \{L_F, L_+, L_{\text{tot}}\}$ be a complexity measure and $f_1, \dots, f_m \in G(x)$ functions with $L(f_1, \dots, f_m) \leq t$. Then there are a $(\mathring{u}, \mathring{v}) \in M(L)$ (see (2.3)) and a hypersurface $K \subsetneq H^n$ with coefficients in G with the property that for every $\lambda \in H^n \backslash K$ there is a $\mathring{w} \in H^s$ such that*

$$f_\mu(x) = Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x-\lambda) \quad (\mu = 1, \dots, m). \tag{2.7}$$

Proof. Suppose all f_μ are nontrivial. By Lemma 2.1 there is a choice $(\mathring{u}, \mathring{v}, \mathring{y}) \in M(L) \times G^{s'}$ admissible for the recursion (2.1) with

$$f_\mu(x) = P_{t+\mu}(\mathring{u}, \mathring{v}, \mathring{y})(x) \quad (\mu = 1, \dots, m).$$

By Proposition 2.4 there is a hypersurface $K \subsetneq H^n$ and given $\lambda \in H^n \backslash K$ there is a $\mathring{w} \in H^s$ with $P_{t+\mu}(\mathring{u}, \mathring{v}, \mathring{y})(x) = Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x-\lambda)$ which yields

$$f_\mu(x) = Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x-\lambda) \quad (\mu = 1, \dots, m).$$

By the definition of the Q_μ in (2.5) that also holds if some of the f_μ are trivial. $\square$

For a more detailed analysis we switch from rational functions to power series. We call $\lambda \in H^n$ admissible for $g \in H(x)$ if there are polynomials h, $k \in H[x]$ with $h(\lambda) \neq 0$ and $g = k/h$. Given $\lambda = (\lambda_1, \ldots, \lambda_n) \in H^n$ admissible for $g_1, \ldots, g_m \in H(x)$ we can expand these functions into power series $\in H[[x-\lambda]]$

$$g_\mu(x) = \sum_{\nu_1,\ldots,\nu_n \geq 0} g_{\mu,\nu_1,\ldots,\nu_n}(\lambda)(x_1-\lambda_1)^{\nu_1} \cdots (x_n-\lambda_n)^{\nu_n} \tag{2.8}$$

and we denote, given $d \in \mathbb{N}$, by

$$\begin{aligned} &c(g_\mu \,|\, \mu = 1, \ldots, m; \lambda, d) \\ &\quad := (g_{\mu,\nu_1,\ldots,\nu_n}(\lambda) \,|\, \mu = 1, \ldots, m, \nu_1 + \cdots + \nu_n \leq d) \in H^{m\binom{n+d}{d}}, \end{aligned} \tag{2.9}$$

the vector built from the coefficients up to degree d of these series (2.8).

From Propositions 2.2, 2.3 and the definition of the Q_μ in (2.5) we have the following proposition.

Proposition 2.6. (i) *Given* $(\mathring{u}, \mathring{v}, \mathring{w}) \in \mathbb{Z}^r \times G^r \times H^s$, $\lambda := 0 \in H^n$ *is admissible for all functions* $R_i(\mathring{u}, \mathring{v}, \mathring{w})(x)$, $U_i'(\mathring{u}, \mathring{v}, \mathring{w})(x), \ldots, Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x)$.

(ii) *In the corresponding power series expansions*

$$Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x) = \sum_{\nu_1,\ldots,\nu_n \geq 0} Q_{\mu,\nu_1,\ldots,\nu_n}(\mathring{u}, \mathring{v}, \mathring{w}) x_1^{\nu_1} \cdots x_n^{\nu_n},$$

the coefficients define totally defined functions $Q_{\mu,\nu_1,\ldots,\nu_n} : \mathbb{Z}^r \times G^r \times H^s \to H$. *The same holds for the other functions* R_i, U_i', *etc. given by* (2.5).

Given $d \in \mathbb{N}$ we introduce the mapping

$$\begin{aligned} &\Phi_d : \mathbb{Z}^r \times G^r \times H^s \to H^{m\binom{n+d}{d}} \\ &(u, v, w) \mapsto (Q_{\mu,\nu_1,\ldots,\nu_n}(u, v, w) \,|\, \mu = 1, \ldots, n; \nu_1 + \cdots + \nu_n \leq d), \end{aligned} \tag{2.10}$$

which maps every choice of parameters for recursion (2.5) into the coefficient vector of the corresponding functions $Q_\mu(u, v, w)(x)$. Now we can reformulate Lemma 2.5 in terms of power series. This yields the following lemma.

Lemma 2.7. *Let* $L \in \{L_F, L_+, L_{\text{tot}}\}$ *be a complexity measure and* $f_1, \ldots, f_m \in G(x)$ *functions with* $L(f_1, \ldots, f_m) \leq t$. *Then there are* $(\mathring{u}, \mathring{v}) \in M(L)$ (*see* (2.3)) *and a hypersurface* $K \subsetneq H^n$ *with the following properties*:

(i) *Every* $\lambda \in H^n \backslash K$ *is admissible for* $f_1, \ldots, f_m$.

(ii) *For every* $\lambda \in H^n \backslash K$ *and every* $d \in \mathbb{N}$ *we have*

$$c(f_\mu \,|\, \mu = 1, \ldots, m; \lambda, d) \in \operatorname{im} \Phi_d|_{\{\mathring{u}\} \times \{\mathring{v}\} \times H^s}.$$

Proof. If we choose $\mathring{u}$, $\mathring{v}$, K, λ and w according to Lemma 2.5 we have

$$f_\mu(x) = Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x - \lambda) \quad (\mu = 1, \ldots, m).$$

It follows from Proposition 2.6 that λ is admissible for $Q_\mu(\mathring{u}, \mathring{v}, \mathring{w})(x-\lambda)$ and therefore for the $f_\mu(x)$, too. Now we expand both sides of (2.7) into power series and compare coefficients up to degree d. This yields

$$c(f_\mu \mid \mu = 1, \ldots, m;\ \lambda, d) = c(Q_\mu(\mathring{u}, \mathring{v}, \mathring{w}) \mid \mu = 1, \ldots, m;\ 0, d)$$

and by (2.10) the right-hand side equals $\Phi_d(\mathring{u}, \mathring{v}, \mathring{w})$ which is in im $\Phi_d|_{\{\mathring{u}\}\times\{\mathring{v}\}\times H^s}$. □

The last step in this section is to eliminate the hypersurface K. This can be done if we replace im $\Phi_d|_{\{\mathring{u}\}\times\{\mathring{v}\}\times H^s} \in H^{m\binom{n+d}{d}}$ by its Zariski closure with respect to polynomials over the field H.

The rational functions $f_\mu \in G(x)$ have representations $f_\mu = k_\mu/h$ with polynomials k_μ $(\mu = 1, \ldots, m)$, $h \in G[x]$ and $h(\lambda) \neq 0$ for all admissible λ. Then the coefficients of the $(x-\lambda)$-expansions of the f_μ have a representation

$$\begin{aligned} &c(f_\mu \mid \mu = 1, \ldots, m;\ \lambda, d) \\ &\quad = (h(\lambda))^{-(d+1)}(g_{\mu,\nu_1,\ldots,\nu_n}(\lambda) \mid \mu = 1, \ldots, m;\ \nu_1 + \cdots + \nu_n \leq d) \end{aligned} \tag{2.11}$$

with polynomials $g_{\mu,\nu_1,\ldots,\nu_n}(\lambda) \in G[\lambda]$.

Let q denote a polynomial of degree say γ over the field H which vanishes on im $\Phi_d|_{\{\mathring{u}\}\times\{\mathring{v}\}\times H^s}$. Then by Lemma 2.7 we have for all $\lambda \in H^n \backslash K$

$$q(c(f_\mu \mid \mu = 1, \ldots, m;\ \lambda, d)) = 0. \tag{2.12}$$

On the other hand we get by (2.11) with some polynomial $\tilde{q}$ over H

$$q(c(f_\mu \mid \mu = 1, \ldots, m;\ \lambda, d)) = (h(\lambda))^{-\gamma(d+1)}\tilde{q}(\lambda).$$

By (2.12) $\tilde{q}$ has to be the zero polynomial and this implies that $c(f_\mu \mid \mu = 1, \ldots, m;\ \lambda, d)$ belongs to the Zariski closure of im $\Phi_d|_{\{u\}\times\{v\}\times H^s}$ whenever λ is admissible for all f_μ $(\mu = 1, \ldots, m)$.

This version of Lemma 2.7 is the first part of the desired theorem. For the convenience of the reader we present it in an (almost) self-contained form.

Theorem 2.8 (Representation Theorem Part 1). *Given m, n, $t \in \mathbb{N}$ define $r := (t+2m)(t+2n-1) - 2m(n-1)$, $s := 8(t+m)+2n$. Let G be a field with prime field E, H an extension field of infinite cardinality and $G(x)$ the field of rational functions in indeterminates $x_1, \ldots, x_n$ over G. Then there exists a family*

$$\Phi = (Q_{\mu,\nu_1,\ldots,\nu_n} \mid \mu = 1, \ldots, m;\ \nu_1, \ldots, \nu_n \in \mathbb{N}) \tag{2.13}$$

of totally defined functions: $\mathbb{Z}^r \times G^r \times H^s \to H$ and for every complexity measure $L \in \{L_F, L_+, L_{\text{tot}}\}$ a set $M(L) \subset \mathbb{Z}^r \times G^r$, where $M(L_F) = \{0\}^r \times F^r$, $M(L_+) = \mathbb{Z}^r \times \{0\}^r$, $M(L_{\text{tot}}) \subset \{0, 1\}^r \times \{0, 1\}^r$, $\# M(L_{\text{tot}}) \leq (t+m+1)^{4(t+m)}$ with the following property: For every complexity measure $L \in \{L_F, L_+, L_{\text{tot}}\}$ and every m rational functions $f_1, \ldots, f_m \in G(x)$ with complexity $L(f_1, \ldots, f_m) \leq t$ there is a $(\mathring{u}, \mathring{v}) \in M(L)$ such that for all $\lambda \in H^n$ admissible for $f_1, \ldots, f_m$ and all $d \in \mathbb{N}$

$$c(f_\mu \mid \mu = 1, \ldots, m;\ \lambda, d) \in \overline{\text{im}\ \Phi_d|_{\{\mathring{u}\}\times\{\mathring{v}\}\times H^s}}. \tag{2.14}$$

Here $c(f_\mu \mid \mu = 1, \ldots, m; \lambda, d)$ denotes the coefficient vector of the power series expansion defined in (2.9), *Φ_d the mapping built from the family Φ according to* (2.10) *and the bar on the right-hand side denotes the Zariski closure with respect to polynomials over the field H.*

3. Algebraic properties of Φ

Part 1 of the Representation Theorem describes families of functions of bounded complexity in terms of the mapping Φ_d which is given by coefficients of the power series expansions of the Q_μ defined by recursion (2.5). To analyse the algebraic properties of that mapping we re-examine that recursion.

Let B denote the ring of all total functions $\mathbb{Z}^r \times G^r \times H^s \to H$. From Proposition 2.6 we know that all R_i, U_i', $\ldots$, V_i'', Q_μ given by (2.5) can be expanded into power series in x and the coefficients define functions in B, i.e. we can read them as power series in $B[[x]]$.

In $B[[x]]$ we have the usual ring operations $+$, $-$, $*$. Furthermore we know by Proposition 2.3 that all series R_i, U_i', U_i'', V_i', V'' have absolute terms $=1$ and therefore they are units in $B[[x]]$. For a unit $S \in B[[x]]$ the inverse series S^{-1} is defined and we can build general powers:

Proposition 3.1. *Given $\alpha \in \mathbb{Z}$ and $S = 1 + \sum_{\nu \geq 1} S_\nu \in B[[x]]$ where S_ν denotes the homogeneous part of degree ν, the series S^α is well defined by the formula*

$$S^\alpha = 1 + \sum_{\nu \geq 1} \left(\sum_{\rho=1}^{\nu} \binom{\alpha}{\rho} \sum_{\substack{\rho_1 + \cdots + \rho_\nu = \rho \\ 1 \cdot \rho_1 + \cdots + \nu \cdot \rho_\nu = \nu}} \frac{\rho!}{\rho_1! \cdots \rho_\nu!} S_1^{\rho_1} \cdots S_\nu^{\rho_\nu} \right). \tag{3.1}$$

From that it follows easily by induction that for fixed $\mathring{u} \in \mathbb{Z}^r$ the coefficients of the power series expansions of the $R_i(\mathring{u}, v, w)(x)$, $U_i'(\mathring{u}, v, w)(x), \ldots, Q_\mu(\mathring{u}, v, w)(x)$ are polynomials in the remaining variables v, w with coefficients in the prime field E.

But how do they depend on the exponents u?

In (3.1) the exponent α occurs only in the term

$$\binom{\alpha}{\rho} = \frac{1}{\rho!} \alpha(\alpha - 1) \cdots (\alpha - \rho + 1) \tag{3.2}$$

and this is a polynomial in α with coefficients in $\mathbb{Q}$. Therefore it seems that the coefficients of the $R_i(u, v, w)(x)$, etc. belong to some substructure of B which is combined from polynomials in u over $\mathbb{Q}$ and polynomials in v, w over E. This structure can be defined as given in the following.

Let I_u be the subring of $\mathbb{Q}[u]$ which consists of all polynomials that map $\mathbb{Z}^r$ into $\mathbb{Z}$. Observe that given $\rho \in \mathbb{N}$ the "binomial polynomial" $\binom{\alpha}{\rho}$ in (3.2) belongs to I_u if α denotes one of the indeterminates collected in u.

We form the tensor product

$$A := I_u \otimes E[v, w]. \tag{3.3}$$

With the natural operations, A is a commutative ring with unity and without zero divisors, which is an I_u- and an $E[v, w]$-algebra too and which allows a valuation

$$\deg_A \varphi := \min\left\{\max_i(\deg_u g_i + \deg_{v,w} h_i) \mid \varphi = \sum_i g_i \otimes h_i \in I_u \otimes E[v, w]\right\}, \tag{3.4}$$

where $\deg_u$ and $\deg_{v,w}$ respectively, denote the usual degree in I_u and $E[v, w]$ respectively.

Remark. This ring A behaves in essential properties like a ring of polynomials and in case the prime field E is $\mathbb{Q}$ it is actually the polynomial ring $\mathbb{Q}[u, v, w]$ with the usual degree valuation. Readers not familiar with tensor products may restrict themselves to that case.

Every element $\varphi = \sum_i g_i \otimes h_i \in A$ defines a function $\in B$ by

$$\mathbb{Z}^r \times G^r \times H^s \ni (\mathring{u}, \mathring{v}, \mathring{w}) \mapsto \sum_i g_i(\mathring{u}) \cdot h_i(\mathring{v}, \mathring{w}) \in H,$$

where the multiplication on the right-hand side is the natural action of $\mathbb{Z}$ on the field H. It is easy to see that this mapping is independent of the representation of φ by elementary tensors. In this sense A is a subring of B. This ring A is the proper structure to describe the mapping Φ_d.

Theorem 3.2 (Representation Theorem Part 2). *Let $A := I_u \otimes E[v, w]$ denote the ring defined in* (3.3), (3.4) *where u and v collect r indeterminates each, w collects s indeterminates. Then the functions $Q_{\mu,\nu_1,\ldots,\nu_n}$ of the family Φ in* (2.13) *belong to A and the following degree bound holds*:

$$\deg_A Q_{\mu,\mu_1,\ldots,\nu_n} \leq (4t+5)(\nu_1 + \cdots + \nu_n) + 1$$
$$(\mu = 1, \ldots, m;\ \nu_1, \ldots, \nu_n \in \mathbb{N}). \tag{3.5}$$

The first step in the proof is given in Proposition 3.3.

Proposition 3.3. *For indeterminates u, v, w the recursion* (2.5) *defines power series $R_i(u, v, w)(x)$, $U_i'(u, v, w)(x), \ldots, Q_\mu(u, v, w)(x) \in A[[x]]$.*

Proof. The proof rests on the following observations: for $j = 1, \ldots, n$ we have

$$R_{-n+j}(u, v, w)(x) = 1 + w_{j0}x_j \in A[[x]].$$

Therefore the assertion is true for the basis of the recursion (2.5) and these R_{-n+j} are units with absolute term 1. To compute the R_i, $U_i', \ldots, V_i''$ $(i = 1, \ldots, t+m)$

from these we have to perform the ring operations +, −, $*$. Furthermore we have to take powers like $R_j^{u'_{ij}}$ or $(V''_i)^{-1}$. Proposition 2.3 ensures that all these series have absolute term $=1$. Therefore (see (3.1)) these operations can be performed by in A well-defined operations on the coefficients. Finally, it follows from the formula $Q_\mu(u, v, w)(x) = w_{t+\mu,2} R_{t+\mu}(u, v, w)(x)$, (2.5), that the assertion holds for the Q_μ, too. □

It remains to prove the degree bound (3.5). For a power series

$$S = \sum_{\nu_1, \ldots, \nu_n \geq 0} S_{\nu_1 \cdots \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n} \in A[[x]]$$

we denote by

$$S_\nu := \sum_{\nu_1 + \cdots + \nu_n = \nu} S_{\nu_1 \cdots \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n} \quad (\nu \in \mathbb{N})$$

the homogeneous part of degree ν with respect to x and define by the valuation $\deg_A$ on A:

$$\deg_A S_\nu := \max\{\deg_A S_{\nu_1 \cdots \nu_n} \mid \nu_1 + \cdots + \nu_n = \nu\}. \tag{3.6}$$

By the definition of the ring operations in $A[[x]]$ and by (3.1), (3.2) the estimations given in Proposition 3.4 are easy to verify.

Proposition 3.4. *For power series S, $S' \in A[[x]]$ it holds that*

(i) $\deg_A(S \pm S')_\nu \leq \max\{\deg_A S_\nu, \deg_A S'_\nu\}$; (3.7)

(ii) $\deg_A(S \cdot S')_\nu \leq \max\{\deg_A S_\rho + \deg_A S'_{\nu-\rho} \mid 0 \leq \rho \leq \nu\}$; (3.8)

(iii) *for $S_0 = 1$ we have*

$$\deg_A(S^{-1})_\nu \leq \max\left\{ \sum_{\sigma=1}^{\nu} \rho_\sigma \deg_A S_\sigma \;\middle|\; \sum_{\sigma=1}^{\nu} \sigma\rho_\sigma = \nu \right\}; \tag{3.9}$$

(iv) *for $S_0 = 1$ is*

$$\deg_A(S^\alpha)_\nu \leq \nu + \max\left\{ \sum_{\sigma=1}^{\nu} \rho_\sigma \deg_A S_\sigma \;\middle|\; \sum_{\sigma=1}^{\nu} \sigma\rho_\sigma = \nu \right\}, \tag{3.10}$$

where α denotes one of the indeterminates collected in u. (Remember $A = I_u \otimes E[v, w]$.)

From these estimations it follows by induction that for the homogeneous parts $R_{j\nu}$ of the series R_j:

$$\deg_A R_{j\nu} \leq (4i+1)\nu \quad (-n+1 \leq j \leq i;\, 0 \leq i \leq t+1) \tag{3.11}$$

holds. For $i=0$ this is obvious by the definition of the R_j $(-n+1 \leq j \leq 0)$. For the induction step we assume that (3.11) holds for $i-1$. Repeated application of (3.10) and (3.8) yield $\deg_A U'_{i\nu} \leq 4i\nu$, $\deg_A U''_{i\nu} \leq 4i\nu$. Similarly repeated applications of (3.7), (3.8) yield $\deg_A V'_{i\nu} \leq 4i\nu$, $\deg_A V''_{i\nu} \leq 4i\nu$ and from this (3.11) follows immediately for i.

For $j=i=t+1$, (3.11) yields $\deg_A R_{t+1,\nu} \leqslant (4t+5)\nu$. But the $R_{t+\mu}$ $(\mu=2,\dots,m)$ are computed from R_j $(j\leqslant t)$ in exactly the same way as R_{t+1} by merely using other variables. Therefore we have

$$\deg_A R_{t+\mu,\nu} \leqslant (4t+5)\nu \quad (\mu=1,\dots,m).$$

Then the formula $Q_\mu = w_{t+\mu,2}R_{t+\mu}$ $(\mu=1,\dots,m)$ of (2.5) immediately yields the desired bound (3.5). □

4. An application

As an example for applications of the Representation Theorem we prove lower bounds for the complexity of single univariate polynomials.

Theorem 4.1. *Let $F \subsetneq G$ be fields with prime field E, $f(x)=\sum_{\nu=0}^{d} \gamma_\nu x^\nu \in G[x]$ a polynomial of degree $d \geqslant 24$ with the property that for $\kappa = \mathrm{C},\dots,d$*

$$[F(\gamma_0,\dots,\gamma_\kappa) : F(\gamma_0,\dots,\gamma_{\kappa-1})] \geqslant (d+1)^{3(d+1)}. \tag{4.1}$$

Then

$$\min\{L_F(f), L_+(f), L_{\text{tot}}(f), L_G(f)^2\} > \tfrac{1}{14}d.$$

These lower bounds are optimal up to a constant factor. This is trivial for L_F, L_+, L_{tot} and follows for L_G from the Paterson–Stockmeyer algorithm [7]. Lower bounds of the same order may be found, e.g., in [8, 9, 12]. An elegant proof for L_+ is given in [4]. The new things are that these bounds hold for fields of any characteristic and the uniform proof.

For the proof we need the following lemma which may be found, e.g., in [8].

Lemma 4.2. *Given integers d, k, c with $d \geqslant k$ a field F and polynomials $\psi_0,\dots,\psi_d \in F[z_1,\dots,z_k]$ of degree $\leqslant c$, there is a nontrivial polynomial $q \in F[y_0,\dots,y_d]$ of degree $\leqslant 2c^k(d+1)^{(d+1)}$ with $q(\psi_0,\dots,\psi_d)=0$.*

We give the proof of Theorem 4.1 only for complexity measures $L \in \{L_F, L_+, L_{\text{tot}}\}$ $(F \subsetneq G)$. We choose L, assume that $L(f) \leqslant \frac{1}{14}d$ and apply the Representation Theorem with $m := n := 1$, $t := \lfloor \frac{1}{14}d \rfloor$ and an arbitrary infinite field $H \supset G$. Relation (2.14) yields

$$(\gamma_0,\dots,\gamma_d) \in \overline{\operatorname{im} \Phi_d|_{\{\mathring{u}\}\times\{\mathring{v}\}+H^s}},$$

where $(\mathring{u}, \mathring{v}) \in M(L) \subset \mathbb{Z}^r \times F^r$. Therefore the mapping $\Phi_d|_{\{u\}\times\{v\}\times H^s}$ is given by $d+1$ elements $\psi_0,\dots,\psi_d \in \mathbb{Z} \otimes F[w] = F[w]$ of degree less than

$$(4t+5)d+1 \leqslant (\tfrac{4}{14}d+5)d+1 \leqslant d^2 \quad (d \geqslant 24)$$

which use only

$$s = 8(t+1)+2 \leqslant \tfrac{8}{14}d + 10 < d \quad (d \geqslant 24)$$

variables. Lemma 4.2 for $k := d$, $c := d^2$ yields a nontrivial polynomial $q \in F[y_0, \ldots, y_d]$ of degree $\leqslant 2d^{2d}(d+1)^{d+1} < (d+1)^{3(d+1)}$ with $q(\psi_0, \ldots, \psi_d) = 0$. This q vanishes on $\overline{\operatorname{im} \Phi_{d|_{\{\mathring{u}\}\times\{\mathring{v}\}\times H^s}}}$ and we get $q(\gamma_0, \ldots., \gamma_d) = 0$.

Together with $q \in F[y_0, \ldots, y_d]$, $\deg q < (d+1)^{3(d+1)}$ this is a contradiction to (4.1).

The proof for the measure L_G follows the same line. □

Further applications which yield new results on lower complexity bounds will be given in a separate paper [10].

References

[1] A. Borodin and S. Cook, On the number of additions to compute specific polynomials, *SIAM J. Comp.* **5** (1976) 146-157.

[2] A. Borodin and I. Munro, *The Computational Complexity of Algebraic and Numeric Problems* (Elsevier, New York, 1975).

[3] J. Von zur Gathen and V. Strassen, Some polynomials that are hard to compute, *Theoret. Comput. Sci.* **11** (1980) 331-335.

[4] J. Heintz, Private communication (1984).

[5] J. Heintz and C.P. Schnorr, Testing polynomials which are easy to compute, in: *Proc. 12th Ann. ACM Symp. on Computing* (1980) 262-280.

[6] J. Heintz and M. Sieveking, A new method to show lower bounds for polynomials which are hard to compute, *Theoret. Comput. Sci.* **11** (1980) 321-330.

[7] M.S. Paterson and L.J. Stockmeyer, On the number of nonscalar multiplications necessary to evaluate polynomials, *SIAM J. Comp.* **2** (1973) 60-66.

[8] C.P. Schnorr, Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials, *Theoret. Comput. Sci.* **7** (1978) 251-261.

[9] C.P. Schnorr and J.P. van de Wiele, On the additive complexity of polynomials, *Theoret. Comput. Sci.* **10** (1980) 1-18.

[10] H.-J. Stoß, Lower bounds on the complexity of polynomials, *Theoret. Comput. Sci.* **64** (1989) 15-23 (this issue).

[11] V. Strassen, Berechnung und Programm I, *Acta Inform.* **1** (1972) 320-334.

[12] V. Strassen, Polynomials with rational coefficients which are hard to compute, *SIAM J. Comp.* **3** (1974) 129-149.