SIAM J. Comput.
Vol. 3, No. 2, June 1974

POLYNOMIALS WITH RATIONAL COEFFICIENTS WHICH ARE HARD TO COMPUTE*

VOLKER STRASSEN†

Abstract. We present specific polynomials in $\mathbb{C}[x]$ with algebraic or rational coefficients which are hard to compute (even though arbitrary complex numbers are allowed as inputs for the computation). Examples are: $\sum_{\delta=0}^{d} e^{2\pi i/2^\delta} x^\delta$, $\sum_{\delta=0}^{d} 2^{2^\delta} x^\delta$. We also show that the minimum number of arithmetic operations to compute polynomials in $\mathbb{C}[x]$ is itself computable. Finally, we study computational complexity in finite-dimensional algebras over an algebraically closed field.

Key words. concrete complexity, polynomial evaluation, rational coefficients, trade-off

1. Introduction. Motzkin [5] and Belaga [1] have shown that the computation (evaluation) of polynomials $\alpha_d x^d + \cdots + \alpha_0 \in \mathbb{C}[x]$ using infinite-precision arithmetic "in general" requires d additions/subtractions and $d/2$ multiplications, even if arbitrary auxiliary complex numbers can be used without extra cost (the choice of these numbers—as well as the whole computation—will of course depend on the polynomial $\alpha_d x^d + \cdots + \alpha_0$, i.e., on its coefficients; in the literature, one therefore often speaks of the possibility of "preconditioning" the coefficients, or of the "preconditioning model"; in the terminology of [10], one is simply dealing with computations in $\mathbb{C}[x]$ considered as a ring over $\mathbb{C} \cup \{x\}$). "In general" may here be interpreted in two ways:

1. the quoted lower bounds hold for all polynomials of degree d except for a set of Lebesgue measure 0;

2. they hold for all polynomials with algebraically independent coefficients (over the rationals).

Since arbitrary polynomials in $\mathbb{C}[x]$ of degree d may in fact be computed with $3d/2 + 2$ arithmetical operations (see again Motzkin [5], Belaga [1]), the first interpretation gives rather precise information on the typical computational complexity of polynomials of degree d. On the other hand, if one is interested in the complexity of specific polynomials, the second interpretation applies, and the information is much less complete: most polynomials occurring in mathematics or in applications have rational or algebraic coefficients. For such polynomials, so far only the trivial lower bound $\log_2 d$ is available.

In the present paper we derive lower bounds for the computational complexity of polynomials with rational or algebraic coefficients. Here are a few examples: let β be a computation (for definitions and notation, see [10]) that computes

$$\sum_{\delta=0}^{d} 2^{2^{\delta d^2}} x^\delta$$

in the field $\mathbb{C}(x)$ over $\mathbb{C} \cup \{x\}$ (i.e., β may use division and may fetch arbitrary complex numbers). Then either β contains at least $d - 4$ additions/subtractions and at least $(d/2) - 2$ multiplications/divisions, or the total number of arithmetic operations in β is ridiculously large, namely $\geqq d^2/\log_2 d$ (Cor. 2.12). Thus in view

* Received by the editors January 17, 1973, and in final revised form September 21, 1973.

† A first version of this paper was written at the Matematisk Institut, University of Aarhus, Denmark, during the summer 1970. Now at Universität Zürich, Zürich, Switzerland.

of the results of Motzkin and Belaga, the above polynomial is practically as hard to compute as one with algebraically independent coefficients. The intuitive reason for this is, of course, the tremendous growth rate of the coefficient sequence. If we moderate this growth rate, we obtain weaker lower bounds. For example: the total number of arithmetic operations needed for computing

$$\sum_{\delta=0}^{d} 2^{2^\delta} x^\delta$$

is at least $\sqrt{d/(3 \log d)}$ for large d (Cor. 2.11). By contrast, $\sum_{\delta=0}^{d} 2^\delta x^\delta$ can obviously be computed with $O(\log d)$ operations.

Polynomials with fast growing integer coefficients occur as initial segments of generating functions in combinatorial mathematics. A slightly different example of a polynomial of complexity at least $\sqrt{d/\log d}$ is

$$\sum_{\delta=0}^{d} e^{2\pi i/2^\delta} x^\delta.$$

Concerning the proofs, we remark that already the investigations of Motzkin and Belaga imply the existence of a polynomial in $d + 1$ indeterminates $P(y_0, \cdots, y_d) \neq 0$ such that if $P(\alpha_0, \cdots, \alpha_d) \neq 0$, then $\alpha_d x^d + \cdots + \alpha_0$ is hard to compute (roughly speaking). It seems very difficult to actually exhibit such a polynomial P. We show, however, with the help of the Dirichlet–Siegel pigeonhole principle, that polynomials P exist which have moderate degree and integer coefficients of absolute value $\leqq 3$. Even such fragmentary information yields the abovementioned lower bounds for the complexity of specific polynomials.

So far we have talked about the results of § 2 of this paper. Before turning to § 3, let us discuss a somewhat different question in a slightly more general context. Let k be an algebraically closed field, $x_1, x_2, \cdots, x_n$ indeterminates over k. We interpret $k(\mathbf{x}) = k(x_1, \cdots, x_n)$ as a field over $k \cup \{x_1, \cdots, x_n\}$ (see [10]). Let z be an integer-valued proper operation-time (cost function) for the type of $k(\mathbf{x})$, which is strictly positive on $+$, $-$, $*$, $/$. The computational complexity L is a function from the set of finite subsets of $k(\mathbf{x})$ to $\mathbb{N} = \{0, 1, 2, \cdots\}$ (intuitively, $L(F)$ is the minimal amount of time that is sufficient to evaluate the set of rational functions F on a computer with a single processor when it takes $z(\omega)$ units of time to perform the operation ω; for details see [10]). We would like to know if L itself is computable. In other words: is it possible to decide if $L(F) \leqq t$ for finite subsets F of $k(\mathbf{x})$ and $t \in \mathbb{N}$?

We treat this question in more detail, even though the rest of the paper is logically independent of the following discussion. First we encode the elements of $k(\mathbf{x})$ into finite sequences over k: we represent rational functions as pairs of polynomials (this representation is not unique since we do not require that the polynomials are relatively prime; further, only pairs whose "denominator-polynomial" is not zero represent rational functions). Let t_0 be a large natural number. If $t \leqq t_0$, then in investigating the problem "$L(F) \leqq t$?" we can restrict our consideration to rational functions which allow a representation by polynomials of degree $\leqq 2^{t_0}$. We represent such polynomials by the $\binom{2^{t_0} + n + 1}{n + 1}$-

tuples of their coefficients. For $M = 2\cdot\binom{2^{t_0} + n + 1}{n + 1}$, every $f \in k^M$ whose last $M/2$ coordinates are not all zero corresponds to a rational function $\tilde{f}$.

Now we construct for every $(t, r) \in \mathbb{N}^2$ with $-\max\{z(+), z(-), z(*), z(/)\} \leqq t \leqq t_0$ a formula $\mathscr{A}_{t,r}(\phi_1, \cdots, \phi_r)$ of the elementary theory of fields (the ϕ_ρ's stand for pairwise distinct M-tuples of free variables) such that

$$\forall t \leqq t_0 \quad \forall r \quad \forall f_1, \cdots, f_r \in k^M, \tag{1.1}$$
$$[(\models_k \mathscr{A}_{t,r}(f_1, \cdots, f_r)) \Leftrightarrow (\tilde{f}_1, \cdots, \tilde{f}_r \text{ are defined and } L(\{\tilde{f}_1, \cdots, \tilde{f}_r\}) \leqq t)].$$

We do this by induction on (t, r) with respect to the lexicographical ordering:

$$\mathscr{A}_{t,r}(\phi_1, \cdots, \phi_r) :\equiv 0 = 0 \qquad \text{if } 0 \leqq t \leqq t_0, \quad r = 0,$$
$$\mathscr{A}_{t,r}(\phi_1, \cdots, \phi_r) :\equiv 0 \neq 0 \qquad \text{if } t < 0,$$

and for $0 \leqq t \leqq t_0, r > 0$:

$$\mathscr{A}_{t,r}(\phi_1, \cdots, \phi_r) :\equiv \bigvee_{\substack{\pi \text{ permutation} \\ \text{of } \{1, \cdots, r\}}} \mathscr{A}'_{t,r}(\phi_{\pi 1}, \cdots, \phi_{\pi r}),$$

where

$$\begin{aligned}
&\mathscr{A}'_{t,r}(\phi_1, \cdots, \phi_r) :\equiv \\
&\quad \bigvee \psi_1 \bigvee \psi_2 (\tilde{\phi}_r = \tilde{\psi}_1 + \tilde{\psi}_2 \wedge \mathscr{A}_{t,-z(+),r+1}(\phi_1, \cdots, \phi_{r-1}, \psi_1, \psi_2)) \\
&\qquad\qquad \vee (\tilde{\phi}_r = \tilde{\psi}_1 - \tilde{\psi}_2 \wedge \mathscr{A}_{t-z(-),r+1}(\phi_1, \cdots, \phi_{r-1}, \psi_1, \psi_2)) \\
&\qquad\qquad \vee (\tilde{\phi}_r = \tilde{\psi}_1 * \tilde{\psi}_2 \wedge \mathscr{A}_{t-z(*),r+1}(\phi_1, \cdots, \phi_{r-1}, \psi_1, \psi_2)) \\
&\qquad\qquad \vee (\tilde{\phi}_r = \tilde{\psi}_1 / \tilde{\psi}_2 \wedge \mathscr{A}_{t-z(/),r+1}(\phi_1, \cdots, \phi_{r-1}, \psi_1, \psi_2)) \\
&\qquad\qquad \vee ((\tilde{\phi}_r = x_1 \vee \cdots \vee \tilde{\phi}_r = x_n \vee \tilde{\phi}_r \text{ const.}) \wedge \mathscr{A}_{t,r-1}(\phi_1, \cdots, \phi_{r-1})).
\end{aligned}$$

Here the ϕ_ρ, ψ_ρ always stand for pairwise distinct M-tuples of logical variables. The expressions "$\tilde{\phi}_r = \tilde{\psi}_1 + \tilde{\psi}_2$, $\tilde{\phi}_r = \tilde{\psi}_1 - \tilde{\psi}_2$, $\tilde{\phi}_r = \tilde{\psi}_1 * \tilde{\psi}_2$, $\tilde{\phi}_r = \tilde{\psi}_1/\tilde{\psi}_2$, $\tilde{\phi}_r = x_j$, $\tilde{\phi}_r$ const." are abbreviations of formulas of the elementary theory of fields; the exact (and obvious) definition of these formulas is left to the reader. These formulas should also state that the rational functions are defined and that in the case of division, the denominator does not vanish.

In order to prove (1.1), one shows first by induction on (t, r) (for $t \leqq t_0$)

$$\forall f_1, \cdots, f_r \in k^M,$$
$$(\models_k \mathscr{A}_{t,r}(f_1, \cdots, f_r) \Rightarrow \tilde{f}_1, \cdots, \tilde{f}_r \text{ are defined, and } L(\{\tilde{f}_1, \cdots, \tilde{f}_r\}) \leqq t),$$

and then by L-induction (see [10]) on the set variable F,

$$\forall t \leqq t_0 \quad \forall r \quad \forall f_1, \cdots, f_r \in k^M,$$
$$(\tilde{f}_1, \cdots, \tilde{f}_r \text{ are defined and } F = \{\tilde{f}_1, \cdots, \tilde{f}_r\} \text{ and } L(F) \leqq t \Rightarrow \models_k \mathscr{A}_{t,r}(f_1, \cdots, f_r)).$$

We apply quantifier-elimination to the formulas $\mathscr{A}_{t,r}(\phi_1, \cdots, \phi_r)$ (in the theory of algebraically closed fields; see [9]). This procedure assigns a quantifier-free formula $\mathscr{B}_{t,r}(\phi_1, \cdots, \phi_r)$ to every (t, r) with $t \leqq t_0$ such that $\vdash (\mathscr{A}_{t,r} \leftrightarrow \mathscr{B}_{t,r})$ and therefore

$$\forall f_1, \cdots, f_r \in k^M (\models_k \mathscr{A}_{t,r}(f_1, \cdots, f_r) \Leftrightarrow \models_k \mathscr{B}_{t,r}(f_1, \cdots, f_r)).$$

Therefore (1.1) remains valid if we replace $\mathscr{A}_{t,r}$ by $\mathscr{B}_{t,r}$. Since quantifier-elimination and the construction of $\mathscr{A}_{t,r}(\phi_1, \cdots, \phi_r)$ are effective procedures, the function

$$(t, r) \mapsto \mathscr{B}_{t,r}(\phi_1, \cdots, \phi_r)$$

is computable. Hence if we can decide if a rational expression in $f_1, \cdots, f_r \in k^M$ vanishes, then we can check for $\models_k \mathscr{B}_{t,r} f_1, \cdots, f_r)$ and hence for $L(\{\tilde{f}_1, \cdots, \tilde{f}_r\}) \leqq t$ (if the $f_1, \cdots, f_r$ are originally given as quotients of polynomials of some degree γ, then choose $t_0 \geqq \max\{t, \log_2 \gamma\}$).

In particular, this is the case for $k = \mathbb{C}$ if the coordinates of $f_1, \cdots, f_r$ are elements of $\mathbb{Q}$. The computational complexity over $\mathbb{C}(\mathbf{x})$ of a system of rational functions with rational coefficients is therefore a computable function of these coefficients. If we encode finite subsets F of $\mathbb{Q}(\mathbf{x})$ by means of the reduced quotient representation of rational functions bijectively by natural numbers $\langle F \rangle$, then L induces a number theoretic function. This function is recursive.

Of course, the situation is completely different if we replace the computational complexity over $\mathbb{C}(\mathbf{x})$ by the complexity over $\mathbb{Q}(\mathbf{x})$. Problem: is the diophantine relation

$$\{(\langle F \rangle, t) : L_{\mathbb{Q}(\mathbf{x})}(F) \leqq t\} \tag{1.2}$$

recursive?

In the discussion above, we can obviously replace the algebraically closed field k by a real closed field. Further, we can use the depth T instead of L (see [10]). We can also weaken the assumptions about z (e.g., we can allow z to assume values in $\mathbb{Q}$: $\mathbb{Q}$-valued operation times with finite range can always be changed to integer-valued operation times by multiplication with a natural number). Finally, we can interpret $k(\mathbf{x})$ as a k-field over $\{x_1, \cdots, x_n\}$ and choose, e.g., $z = 1_{\{*,/\}}$.

Statement (1.1) with $\mathscr{B}_{t,r}$ instead of $\mathscr{A}_{t,r}$ implies that the set $\{(f_1, \cdots, f_r) : L(\{\tilde{f}_1, \cdots, \tilde{f}_r\}) \leqq t\} \subset k^{Mr}$ is constructible in the sense of algebraic geometry (see [6]). In § 3 we prove an analogous statement (Thm. 3.1), without using logic, by means of algebraic geometry; we apply the theorem of Chevalley ([6, p. 97]) instead of quantifier-elimination (which we could have used as well). The situation in § 3 differs from the previous discussion as follows:

1. Division is not allowed, hence $k(\mathbf{x})$ simplifies to $k[\mathbf{x}]$.
2. $k[\mathbf{x}]$ is replaced by $k[\mathbf{x}]/(x_1, \cdots, x_n)^M$. $(x_1, \cdots, x_n)^M$ denotes the ideal which is generated by the monomials of degree M (since M can be chosen to be arbitrarily large, this does not restrict generality).
3. Besides $k[\mathbf{x}]/(x_1, \cdots, x_n)^M$, arbitrary finite-dimensional k-rings A are considered (which do not have to be commutative nor associative); these rings are interpreted as k-rings over a given system of generators.
4. The operation time is $z = 1_{\{*\}}$.

The encoding of A does not create difficulties: A is a finite dimensional k-vector space and therefore an affine space in the sense of algebraic geometry.

After showing that the set

$$\{(a_1, \cdots, a_r) : L(\{a_1, \cdots, a_r\}) \leqq t\} \subset A^r$$

is constructible for every r, t, it is desirable to close the set in the sense of the Zariski topology. We define a new function $\mathbf{L}$ from the set of finite subsets of A to $\mathbb{N}$ such that

$$(1.3) \{(a_1, \cdots, a_r) : \mathbf{L}(\{a_1, \cdots, a_r\}) \leqq t\} = \overline{\{(a_1, \cdots, a_r) : L(\{a_1, \cdots, a_r\}) \leqq t\}}$$

(overlining denotes closure). If we disregard the difference between $(a_1, \cdots, a_r)$ and $\{a_1, \cdots, a_r\}$, then $\mathbf{L}$ is the largest Zariski-lower-semicontinuous function $\leqq L$. Analogously we define $\mathbf{L}(F \bmod E)$ in terms of $L(F \bmod E)$ (see [10]) by forming the closure with respect to F. $\mathbf{L}(\cdot \bmod \cdot)$ has again the formal properties of L, i.e., $\mathbf{L}$ is a relative L-bound (Thm. 3.4). Theorem 3.5 is a general analogue of Theorem 1 of Paterson–Stockmeyer [7].

$\mathbf{L}$ is more manageable than L: e.g., the knowledge of L is equivalent to the knowledge of the formulas $\mathscr{B}_{t,r}(\phi_1, \cdots, \phi_r)$ or the constructible sets defined by them, whereas $\mathbf{L}$ is known if the much simpler closed sets (1.3) or the corresponding polynomial ideals are known. We will denote these polynomial ideals by $J_r(t)$.

In analogy with § 2, we show in § 3 that for $k = \mathbb{C}$, the ideal $J_r(t)$ contains a nonzero form of relatively small degree with integer coefficients which have absolute value $\leqq 3$. This yields, e.g., the following lower bounds: if we interpret $\mathbb{C}[\mathrm{x}]$ as a $\mathbb{C}$-ring over $\{x\}$, then for large d,

$$\mathbf{L}\left(* \,\middle|\, \sum_{\delta=0}^{d} e^{2\pi i/2^\delta} x^\delta\right) > \frac{1}{2} d^{1/3}, \tag{1.4}$$

$$\mathbf{L}\left(* \,\middle|\, \sum_{\delta=0}^{d} 2^{2^\delta} x^\delta\right) > \frac{1}{2} d^{1/3}, \tag{1.5}$$

and

$$\mathbf{L}\left(* \,\middle|\, \sum_{\delta=0}^{d} 2^{2^{\delta d^3}} x^\delta\right) > \sqrt{d} - 3 \tag{1.6}$$

(see Corollary 3.7).

The lower bound (1.6) is of optimal order as follows from Paterson–Stockmeyer [7, Thm. 4]. The existence of polynomials of degree d with integer coefficients which require at least $\sqrt{d}$ nonscalar multiplications for their computation is already proved in that paper [7, Thm. 1].

The emphasis of § 3 is on general developments. The language is therefore more abstract than in § 2. A reader who is mostly interested in concrete results may skip Theorems 3.3, 3.4 and 3.5 without logical loss.

The most interesting open problems in the present context are perhaps (i) to exhibit a "reasonable" polynomial with coefficients 0 or 1 which is hard to compute, (ii) to derive nontrivial lower bounds for the complexity of initial segments of the classical power series, e.g., $\sum(x^\delta/\delta!)$.

This paper assumes knowledge of [10]. In § 3 we also use notions and theorems of algebraic geometry (see [6, Chap. 1]).

We denote finite sequences $(a_1, \cdots, a_r)$ by $\mathbf{a}$, $\operatorname{Im} \mathbf{a}$ stands for $\{a_1, \cdots, a_r\}$. $\mathscr{E}(A)$ is the set of finite subsets of A. $\mathbb{N}'$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ stand for the set of positive natural numbers, nonnegative natural numbers, integers, rational numbers and complex numbers, respectively. Let x be a real number; $\exp(x)$ stands for e^x, $\lfloor x \rfloor$ is the greatest integer $\leqq x$, $\lceil x \rceil$ is the least integer $\geqq x$. If f and g are number-theoretic functions, then "$f(d) \lesssim g(d)$ for $d \to \infty$" means that for every $\varepsilon > 0$, finally $f(d) < (1 + \varepsilon)g(d)$. The abbreviation log always stands for $\log_2$.

2. Construction of polynomials over $\mathbb{Q}$ which are hard to compute (counting all operations).

We start with preliminaries.

DEFINITION 2.1. The *height* of a polynomial with integer coefficients is the maximum of the absolute values of the coefficients. The *weight* of such a polynomial is the sum of the absolute values of the coefficients.

The weight is subadditive and submultiplicative.

LEMMA 2.2 (pigeonhole lemma). *Let $N > M$. M linear forms $\in \mathbb{Z}[B_1, \cdots, B_N]$, each of weight $\leqq G$, have a common nontrivial zero $\langle b_1, \cdots, b_N \rangle \in \mathbb{Z}^N$ such that*

$$|b_i| \leqq \lfloor G^{M/(N-M)} \rfloor + 2$$

for all i.

Proof. See Schneider [8, p. 140].

LEMMA 2.3. *Let $m \geqq 1$, $c \geqq 2$, $f \geqq 4$ and $q \geqq 5$ be natural numbers, let $z_1, \cdots, z_m$ be indeterminates over $\mathbb{Z}$ and let*

$$P_1, \cdots, P_q \in \mathbb{Z}[z_1, \cdots, z_m]$$

be such that

$$\text{degree } P_\kappa \leqq c, \quad \text{weight } P_\kappa \leqq f$$

for all κ. If g is a natural number such that

$$g^{q-m-2} > c^m q^q \log f, \tag{2.1}$$

then there is a nontrivial form $H \in \mathbb{Z}[y_1, \cdots, y_q]$ of degree g and height $\leqq 3$ such that

$$H(P_1, \cdots, P_q) = 0.$$

Proof. To show: there are integers $b_{i_1,\cdots,i_q}$ (not all $= 0$) such that $|b_{i_1,\cdots,i_q}| \leqq 3$ and

$$\sum_{i_1 + \cdots + i_q = g} b_{i_1,\cdots,i_q} P_1^{i_1} \cdots P_q^{i_q} = 0. \tag{2.2}$$

First we replace the $b_{i_1,\cdots,i_q}$'s by indeterminates $B_{i_1,\cdots,i_q}$ and consider

$$Q := \sum_{i_1 + \cdots + i_q = g} B_{i_1,\cdots,i_q} P_1^{i_1} \cdots P_q^{i_q} \in \mathbb{Z}[\mathbf{B}, \mathbf{z}].$$

Evidently,

$$\text{degree}_{\mathbf{z}} Q \leqq gc,$$

and

$$\text{weight } Q \leqq f^g \binom{g + q - 1}{q - 1}.$$

If we write Q as a polynomial in $z_1, \cdots, z_m$, then the coefficients are linear forms $\in \mathbb{Z}[\mathbf{B}]$, of weight $\leqq f^g \binom{g+q-1}{q-1}$. There are at most $\binom{gc+m}{m}$ such forms. (2.2) says that the $b_{i_1, \cdots, i_q}$'s are common zeros of these. The pigeonhole lemma implies the existence of a nontrivial zero $b_{i_1, \cdots, i_q}$ with $|b_{i_1, \cdots, i_q}| \leqq 3$ if

$$\binom{g+q-1}{q-1} > \binom{gc+m}{m}$$

and

$$\left(f^g \binom{g+q-1}{q-1} \right)^{\binom{gc+m}{m}} < 2^{\binom{g+q-1}{q-1} - \binom{gc+m}{m}}. \tag{2.3}$$

The first inequality follows from the second one. The assumptions about m, c, q and $g \geqq 2$ (because of (2.1)) imply

$$\binom{gc+m}{m} \leqq (gc)^m + 1$$

and

$$\left(\frac{g}{q}\right)^{q-1} < \binom{g+q-1}{q-1} < g^q.$$

Suppose now that (2.3) is false. Then

$$(f^g g^q)^{(gc)^m + 1} \geqq 2^{(g/q)^{q-1}} - (gc)^m - 1,$$

and therefore

$$((gc)^m + 1) g (\log f + q) \geqq \left(\frac{g}{q}\right)^{q-1} - (gc)^m - 1,$$

which can be written as

$$((gc)^m + 1)(g(\log f + q) + 1) \geqq \left(\frac{g}{q}\right)^{q-1}.$$

This implies (note that $g \geqq 2$, $c \geqq 2$, $\log f \geqq 2$, $q \geqq 5$)

$$(gc)^m g q \log f \geqq \left(\frac{g}{q}\right)^{q-1}.$$

This inequality contradicts (2.1).

Let k be a field; $k[[x]]$ is the ring of formal power series in x interpreted as a ring with division by units over $k \cup \{x\}$. Therefore $k[[x]]$ has the type $\Omega = \{+, -, *, /\} \cup k \cup \{x\}$.

LEMMA 2.4. *Let β be a Ω-computation whose execution in $k[[x]]$ yields the sequence $(a_1, \cdots, a_l)$ of intermediate results. Assume*

$$a_i = \sum_{\delta \geqq 0} \alpha_{i\delta} x^\delta.$$

Let $L(\pm|\beta) = u$, $L(*|\beta) = v_1$, $L(/|\beta) = v_2$. *Put* $v = v_1 + v_2$ *and* $m = \min\{u, 2v\}$. *Then there are polynomials*

$$P_{i\delta} \in \mathbb{Z}[z_1, \cdots, z_m]$$

$(1 \leqq i \leqq l, 1 \leqq \delta < \infty)$ *such that*

$$\begin{aligned} \max_{1 \leqq \delta \leqq d} \text{degree } P_{i\delta} &\leqq (u+1)2^{v_1}(d^{v_2} + 3d^{v_2-1} + \cdots + 3d + 2) \\ &\leqq (u+1)2^{v_1+1}d^{v_2}, \end{aligned} \tag{2.4}$$

$$\sum_{1 \leqq \delta \leqq d} \text{weight } P_{i\delta} \leqq 3^{(u+1)2^{v_1}(d^{v_2}+\cdots+1)} - 1 \leqq 2^{(u+1)2^{v_1+1}d^{v_2}} \tag{2.5}$$

for $1 \leqq i \leqq l$, $d \geqq 5$, *and there are* $\gamma_1, \cdots, \gamma_m, \lambda_i \in k$ *such that* $\lambda_i \neq 0$ *and*

$$\lambda_i P_{i\delta}(\gamma_1, \cdots, \gamma_m) = \alpha_{i\delta}$$

for $1 \leqq i \leqq l, \delta \geqq 1$.

Proof. First we prove the lemma with $2v$ instead of m by induction on l arranging $\lambda_i = 1$ for all i. The initial step of the induction is obvious (empty computation). Let $\beta = (\beta_1, \cdots, \beta_l)$. By the induction hypothesis, there are $P_{i\delta}$ for $1 \leqq i \leqq l-1$, $1 \leqq \delta < \infty$, having the desired properties.

If $\omega_l \in k$, then we set $P_{l\delta} = 0$ for all δ.

If $\omega_l = x$, then we set $P_{l1} = 1$ and $P_{l\delta} = 0$ for $\delta > 1$.

If $\beta_l = (\pm, i, j)$, then we set $P_{l\delta} = P_{i\delta} \pm P_{j\delta}$.

If $\beta_l = (*, i, j)$, then we define the $P_{l\delta}$'s by

$$\begin{aligned} &\left(z_{2v-1} + \sum_{\delta \geqq 1} P_{i\delta}(z_1, \cdots, z_{2v-2})x^\delta\right)\left(z_{2v} + \sum_{\delta \geqq 1} P_{j\delta}(z_1, \cdots, z_{2v-2})x^\delta\right) \\ &\qquad = z_{2v-1}z_{2v} + \sum_{\delta \geqq 1} P_{l\delta}(z_1, \cdots, z_{2v})x^\delta. \end{aligned}$$

Further, we set $\gamma_{2v-1} = \alpha_{i0}$, $\gamma_{2v} = \alpha_{j0}$.

If $\beta_l = (/, i, j)$ then we define the $P_{l\delta}$'s by

$$\begin{aligned} &\left(z_{2v-1} + \sum_{\delta \geqq 1} P_{i\delta}(z_1, \cdots, z_{2v-2})x^\delta\right) \Big/ \left(1/z_{2v} + \sum_{\delta \geqq 1} P_{j\delta}(z_1, \cdots, z_{2v-2})z^\delta\right) \\ &\qquad = z_{2v-1}z_{2v} + \sum_{\delta \geqq 1} P_{l\delta}(z_1, \cdots, z_{2v})x^\delta. \end{aligned} \tag{2.6}$$

The $P_{l\delta}$'s are integer polynomials because of

$$\frac{1}{1/z_{2v} + \sum_{\delta \geqq 1} P_{j\delta}x^\delta} = z_{2v} \sum_{\sigma \geqq 0} \left(-z_{2v} \sum_{\delta \geqq 1} P_{j\delta}x^\delta\right)^\sigma. \tag{2.7}$$

Further, we set $\gamma_{2v-1} = \alpha_{i0}$, $\gamma_{2v} = 1/\alpha_{j0}$.

It is not difficult to see that the $P_{l\delta}$'s have the desired properties; we only show how to estimate degree and weight in the case of division. (2.6) and (2.7) imply

$$\left(z_{2v-1}+\sum_{\delta=1}^{d}P_{i\delta}x^{\delta}\right)z_{2v}\sum_{\sigma=0}^{d-1}\left(-z_{2v}\sum_{\delta=1}^{d}P_{j\delta}x^{\delta}\right)^{\sigma}+z_{2v-1}z_{2v}\left(-z_{2v}\sum_{\delta=1}^{d}P_{j\delta}x^{\delta}\right)^{d}$$

$$\equiv z_{2v-1}z_{2v}+\sum_{\delta=1}^{d}P_{l\delta}x^{\delta}\,(\operatorname{mod} x^{d+1}).$$

The bound for the degree follows immediately. If $\sum_{\delta=1}^{d}$ weight $P_{i\delta}\leqq t-1$ and $\sum_{\delta=1}^{d}$ weight $P_{j\delta}\leqq t-1$ for some $t\geqq 3$, then

$$\left(\sum_{\delta=1}^{d}\text{weight }P_{l\delta}\right)+1=\text{weight}\left(z_{2v-1}z_{2v}+\sum_{\delta=1}^{d}P_{l\delta}x^{\delta}\right)$$

$$\leqq t\sum_{\sigma=0}^{d-1}t^{\sigma}+t^{d}\leqq\frac{t^{d+1}}{t-1}+t^{d}\leqq 3t^{d}.$$

The induction step for the weight follows. We now prove the lemma with u instead of m. For simplicity, we assume that $a_i\neq 0$ for all i (it should not cause any problems for the reader to drop this assumption). Then every a_i can be written as

$$a_i=\sum_{\delta\geqq\delta_i}\alpha_{i\delta}x^{\delta},\qquad \alpha_{i\delta_i}\neq 0.$$

We construct not only the polynomials $P_{i\delta}$ for $\delta\geqq 1$, but also polynomials P_{i0} with integer coefficients such that (2.4) and (2.5) are satisfied with $\max_{0\leqq\delta\leqq d}$ and $\sum_{0\leqq\delta\leqq d}$. We also achieve that

$$P_{i0}=\cdots=P_{i,\delta_i-1}=0,\qquad P_{i\delta_i}=1.$$

Obviously, this forces $\lambda_i=\alpha_{i\delta_i}$. The proof goes again by induction on l.

If $\omega_l\in k-\{0\}$, then we set $P_{l0}=1$ and $P_{l\delta}=0$ for $\delta>0$.

If $\omega_l=x$, then we set $P_{l1}=1$ and $P_{l\delta}=0$ for $\delta\neq 1$.

If $\beta_l=(*,i,j)$, then we define the $P_{l\delta}$'s by

$$\sum_{\delta\geqq 0}P_{i\delta}x^{\delta}\sum_{\delta\geqq 0}P_{j\delta}x^{\delta}=\sum_{\delta\geqq 0}P_{l\delta}x^{\delta}.$$

If $\beta_l=(/,i,j)$, then we define the $P_{l\delta}$'s by

$$\sum_{\delta\geqq 0}P_{i\delta}x^{\delta}\Big/\sum_{\delta\geqq 0}P_{j\delta}x^{\delta}=\sum_{\delta\geqq 0}P_{l\delta}x^{\delta}.$$

Since a_j is a unit, we have $\alpha_{j0}\neq 0$ and hence $P_{j0}=1$. Therefore the $P_{l\delta}$'s have integer coefficients.

If $\beta_l=(+,i,j)$ then we distinguish 3 cases.

Case 1. $\delta_i=\delta_j=\delta_l$. We define the $P_{l\delta}$'s by

$$z_u\sum_{\delta\geqq 0}P_{i\delta}(z_1,\cdots,z_{u-1})x^{\delta}+(1-z_u)\sum_{\delta\geqq 0}P_{j\delta}(z_1,\cdots,z_{u-1})x^{\delta}$$

$$=\sum_{\delta\geqq 0}P_{l\delta}(z_1,\cdots,z_u)x^{\delta}.$$

Then $P_{l\delta}=0$ for $\delta<\delta_l$ and $P_{l\delta_l}=1$. Furthermore, we set

$$\gamma_u=\alpha_{i\delta_i}/(\alpha_{i\delta_i}+\alpha_{j\delta_j})$$

(the denominator is $=\alpha_{l\delta_l}$ and therefore $\neq 0$).

Case 2. $\delta_i = \delta_j < \delta_l$. Then $\alpha_{i\delta_i} = -\alpha_{j\delta_j}$. We set $P_{l\delta} = 0$ for $\delta < \delta_l$, $P_{l\delta_l} = 1$, and define the remaining $P_{l\delta}$'s by

$$z_u \sum_{\delta > \delta_l} P_{i\delta}x^\delta - z_u \sum_{\delta > \delta_l} P_{j\delta}x^\delta = \sum_{\delta > \delta_l} P_{l\delta}x^\delta.$$

Furthermore, we set $\gamma_u = \alpha_{i\delta_i}/\alpha_{l\delta_l}$.

Case 3. $\delta_i \neq \delta_j$, say $\delta_i < \delta_j$. Then $\delta_l = \delta_i$. We define the $P_{l\delta}$'s by

$$\sum_{\delta \geqq 0} P_{i\delta}x^\delta + z_u \sum_{\delta \geqq 0} P_{j\delta}x^\delta = \sum_{\delta \geqq 0} P_{l\delta}x^\delta.$$

Again $P_{l\delta} = 0$ for $\delta < \delta_l$ and $P_{l\delta_l} = 1$. Furthermore, we set $\gamma_u = \alpha_{j\delta_j}/\alpha_{i\delta_i}$. The case $\beta_l = (-, i, j)$ is treated analogously. The proof that the $P_{l\delta}$'s possess the desired properties goes along the lines of the first part of this proof.

THEOREM 2.5. *Let β compute*

$$a = \sum_{\delta=0}^{d} \alpha_\delta x^\delta, \qquad \alpha_\delta \in k,$$

in $k(x)$ interpreted as a field over $k \cup \{x\}$. Let $L(\pm|\beta) = u > 0$, $L(*/|\beta) = v > 0$,

$$m = \min\{u, 2v\}, \qquad s = u + v.$$

Let $q \geqq 5$, and let $\delta_1, \cdots, \delta_q$ be pairwise distinct natural numbers $\leqq d$. If g is a natural number such that

$$g^{q-m-2} > d^{s(m+1)}q^q, \tag{2.8}$$

then there is a nontrivial form $H \in \mathbb{Z}[y_1, \cdots, y_\gamma]$ of degree g and height $\leqq 3$ such that

$$H(\alpha_{\delta_1}, \cdots, \alpha_{\delta_q}) = 0.^{1}$$

Proof. We can assume without loss of generality that β is executable and that k has infinite degree of transcendence over its prime field. Let $(a_1, \cdots, a_l)$ be the sequence of results of β, $a_i \in k(x)$. In order to simplify the argument, we assume $a = a_l$. Let $\theta \in k$ be transcendental over $\alpha_1, \cdots, \alpha_d$ and be different from the zeros and poles of the nontrivial a_i. Then we can develop each a_i as a formal power series in $x - \theta$:

$$a_i = \sum_{\delta \geqq 0} \alpha_{i\delta}(x - \theta)^\delta.$$

For $a_i \neq 0$ we have $\alpha_{i0} \neq 0$. If we interpret the ring $k[[x - \theta]]$ of formal power series as a ring with division by units over $k \cup \{x\}$, then β is executable in this ring and has the sequence $(a_1, \cdots, a_l)$ of results. Therefore we can apply Lemma 2.4 (with $x - \theta$ instead of x). Lemma 2.4 implies the existence of polynomials $P_1, \cdots, P_q \in \mathbb{Z}[z_1, \cdots, z_m]$ and $\gamma_1, \cdots, \gamma_m, \lambda \in k$ with $\lambda \neq 0$ such that

$$\lambda P_\kappa(\gamma_1, \cdots, \gamma_m) = \alpha_{l\delta_\kappa},$$
$$\text{degree } P_\kappa \leqq 2(u + 1)d^v \leqq d^s,$$
$$\text{weight } P_\kappa \leqq 2^{2(u+1)d^v} \leqq 2^{d^s}$$

[1] Obviously the theorem will only be relevant for $q > m + 2$.

(the right inequalities follow from $d \geqq q \geqq 5$ and $u \geqq 1$). If we set $c = d^s, f = 2^{d^s}$ then by (2.8),

$$g^{q-m-2} > c^m g^q \log f.$$

By Lemma 2.3, there is a nontrivial form $H \in \mathbb{Z}[y_1, \cdots, y_\gamma]$ of degree g and height $\leqq 3$ such that

$$H(P_1, \cdots, P_q) = 0,$$

and therefore

$$\begin{aligned} 0 &= H(\alpha_{l\delta_1}, \cdots, \alpha_{l\delta_q}) \\ &= H\left(\sum_{\delta=\delta_1}^{d} \binom{\delta}{\delta_1} \alpha_\delta \theta^{\delta-\delta_1}, \cdots, \sum_{\delta=\delta_q}^{d} \binom{\delta}{\delta_q} \alpha_\delta \theta^{\delta-\delta_q}\right). \end{aligned}$$

The constant term of this polynomial in θ is $H(\alpha_{\delta_1}, \cdots, \alpha_{\delta_q})$. Since θ is transcendental over $\alpha_1, \cdots, \alpha_q$, we conclude

$$H(\alpha_{\delta_1}, \cdots, \alpha_{\delta_q}) = 0.$$

LEMMA 2.6. *Let* $\operatorname{char} k \notin \{2, 3\}$, k_0 = *prime field of* k, $\tau_1, \cdots, \tau_q \in k$, *and let* g *be a natural number such that*

$$[k_0(\tau_1, \cdots, \tau_\kappa) : k_0(\tau_1, \cdots, \tau_{\kappa-1})] > g$$

for all κ. *Then there is no form* $H \in \mathbb{Z}[y_1, \cdots, y_q]$, $H \neq 0$ *of degree* g *and height* $\leqq 3$ *such that*

$$H(\tau_1, \cdots, \tau_q) = 0.$$

Proof. Assume there is such a form. Let $\tilde{H}$ be the image of H under the canonical homomorphism $\mathbb{Z}[y_1, \cdots, y_q] \to k_0[y_1, \cdots, y_q]$. Since $\operatorname{char} k \notin \{2, 3\}$ and height $H \leqq 3$, $\tilde{H} \neq 0$. Choose κ such that

$$\tilde{H}(\tau_1, \cdots, \tau_\kappa, y_{\kappa+1}, \cdots, y_q) = 0,$$

but

$$\tilde{H}(\tau_1, \cdots, \tau_{\kappa-1}, y_\kappa, y_{\kappa+1}, \cdots, y_q) \neq 0.$$

We interpret $\tilde{H}(\tau_1, \cdots, \tau_{\kappa-1}, y_\kappa, y_{\kappa+1}, \cdots, y_q)$ as a polynomial in $y_{\kappa+1}, \cdots, y_q$ with coefficients $\in k_0(\tau_1, \cdots, \tau_{\kappa-1})[y_k]$. Let Q be a nonvanishing coefficient. Then $Q(\tau_\kappa) = 0$, and degree $Q \leqq$ degree $H = g$, and therefore

$$[k_0(\tau_1, \cdots, \tau_\kappa) : k_0(\tau_1, \cdots, \tau_{\kappa-1})] \leqq g,$$

which is a contradiction.

COROLLARY 2.7. *Let* β *compute*

$$a = \sum_{\delta=0}^{d} \exp(2\pi i/2^\delta) x^\delta$$

in the field $\mathbb{C}(x)$ *over* $\mathbb{C} \cup \{x\}$. *If we set* $L(\pm|\beta) = u$, $L(*/|\beta) = v$, $m = \min\{u, 2v\}$, $s = u + v$, *then*

$$s(m+2) \gtrsim d/\log d$$

for $d \to \infty$. *In particular*, $s > \sqrt{d/\log d}$ *for large* d.

Proof. Let

$$\begin{aligned} \alpha_\delta &= \exp(2\pi i/2^\delta), \\ q &= \lfloor d/((\log d)^2 + 3) \rfloor, \\ \delta_\kappa &= \kappa(\lceil \log d)^2 \rceil + 2), \qquad \kappa = 1, \cdots, q, \\ g &= 2\lceil (\log d)^2 \rceil. \end{aligned}$$

Then

$$[\mathbb{Q}(\alpha_{\delta_1}, \cdots, \alpha_{\delta_\kappa}) : \mathbb{Q}(\alpha_{\delta_1}, \cdots, \alpha_{\delta_{\kappa-1}})] = \begin{cases} 2^{\delta_\kappa - \delta_{\kappa-1}} & \text{for } \kappa > 1, \\ 2^{\delta_1 - 1} & \text{for } \kappa = 1, \end{cases}$$

which is $>g$ for all κ. Lemma 2.6 and Theorem 2.5 imply

$$g^{q-m-2} \leqq d^{s(m+1)} q^q.$$

The assertion follows by substituting.

COROLLARY 2.8. *Let β compute*

$$a = \sum_{\delta=0}^{d} \exp(2\pi i/2^{\delta^3}) x^\delta$$

in the field $\mathbb{C}(x)$ over $\mathbb{C} \cup \{x\}$. Then for large d, either

$$m > d/5,$$

or

$$s > d^2/(5 \log d).$$

(We use the notation of Corollary 2.7.)

Proof. Let

$$\begin{aligned} \alpha_\delta &= \exp(2\pi i/2^{\delta^3}) \\ q &= \lfloor d/4 \rfloor \\ \delta_\kappa &= \lceil (4\kappa d^2)^{1/3} \rceil \\ g &= 2^{d^2 - 4d}. \end{aligned}$$

Then

$$I_\kappa := [\mathbb{Q}(\alpha_{\delta_1}, \cdots, \alpha_{\delta_\kappa}) : \mathbb{Q}(\alpha_{\delta_1}, \cdots, \alpha_{\delta_{\kappa-1}})] = \begin{cases} 2^{\delta_\kappa^3 - \delta_{\kappa-1}^3} & \text{for } \kappa > 1 \\ 2^{\delta_1^3 - 1} & \text{for } \kappa = 1. \end{cases}$$

Since

$$\begin{aligned} \delta_\kappa^3 - \delta_{\kappa-1}^3 &\geqq 4\kappa d^2 - ((4(\kappa - 1)d^2)^{1/3} + 1)^3 \\ &\geqq 4d^2 - 3d^2 - 3d - 1 \\ &> d^2 - 4d \end{aligned}$$

and

$$\delta_1^3 - 1 > d^2 - 4d,$$

we infer

$$I_\kappa > g \quad \text{for all } \kappa.$$

Lemma 2.6 and Theorem 2.5 imply

$$g^{q-m-2} \leqq d^{s(m+1)} q^q.$$

The assertion follows easily.

LEMMA 2.9. (See Schneider [8, § 5].) *Let*

$$Q = \sum_{j=0}^{l} \sigma_j y^j \in \mathbb{Z}[y]$$

with $\delta_l \neq 0$ *and*

$$|\sigma_j| \leqq hc^{l-j} \quad \textit{for all } j.$$

Then for any root $\tau \in \mathbb{C}$ *of* Q,

$$|\tau| \leqq (h+1)c.$$

Proof. If $|\tau| \leqq c$, then we have nothing to prove. Therefore assume $|\tau| > c$.

$$\sigma_l \tau^l = -\sum_{j=0}^{l-1} \sigma_j \tau^j$$

implies

$$\begin{aligned} |\tau|^l &\leqq \sum_{j=0}^{l-1} |\sigma_j| |\tau|^j \\ &\leqq hc^l \sum_{j=0}^{l-1} (|\tau|/c)^j \\ &\leqq hc^l (|\tau|/c)^l / ((|\tau|/c) - 1), \end{aligned}$$

which in turn implies the assertion.

LEMMA 2.10. *Let* $\tau_1, \cdots, \tau_q \in \mathbb{Z}$, $q \geqq 5$, *and* $g \in \mathbb{N}$, $g \geqq 3$, *with*

$$|\tau_1| > 4$$

and

$$|\tau_\kappa| > |q\tau_{\kappa-1}|^g \quad \text{for } \kappa > 1.$$

Then there is no form $H \in \mathbb{Z}[y_1, \cdots, y_q]$, $H \neq 0$, *of degree* g *and height* $\leqq 3$ *such that*

$$H(\tau_1, \cdots, \tau_q) = 0.$$

Proof. Assume there is such a form. Choose κ such that

$$H(\tau_1, \cdots, \tau_\kappa, y_{\kappa+1}, \cdots, y_q) = 0,$$

but

$$H(\tau_1, \cdots, \tau_{\kappa-1}, y_\kappa, \cdots, y_q) \neq 0.$$

We interpret $H(\tau_1, \cdots, \tau_{\kappa-1}, y_\kappa, \cdots, y_q)$ as a polynomial in $y_{\kappa+1}, \cdots, y_q$ with coefficients in $\mathbb{Z}[y_\kappa]$. Let Q be a nonvanishing coefficient. The coefficients of Q are polynomials with integer coefficients in $\tau_1, \cdots, \tau_{\kappa-1}$ of degree $\leqq g$ and of height $\leqq 3$. Therefore

$$\text{height } Q \leqq \begin{cases} 3 & \text{if } \kappa = 1, \\ 3\binom{g + \kappa - 1}{\kappa - 1}|\tau_{\kappa-1}|^g & \text{for } \kappa > 1. \end{cases}$$

$Q(\tau_\kappa)$ is equal to zero. By Lemma 2.9 (with $c = 1$, $h = \text{height } Q$), we infer

$$|\tau_\kappa| \leqq \text{height } Q + 1 \leqq \begin{cases} 4 & \text{if } \kappa = 1, \\ |q\tau_{\kappa-1}|^g & \text{if } \kappa > 1. \end{cases}$$

This contradicts the assumptions about τ_κ.

COROLLARY 2.11. *Let β compute*

$$a = \sum_{\delta=0}^{d} 2^{2^\delta} x^\delta$$

in the field $\mathbb{C}(x)$ over $\mathbb{C} \cup \{x\}$. We set $u = L(\pm|\beta)$, $v = L(*/|\beta)$, $m = \min\{u, 2v\}$, $s = u + v$. Then

$$s(m + 2) \gtrsim d/(3 \log d)$$

for $d \to \infty$. In particular, $s > \sqrt{d/(3 \log d)}$ for large d.

Proof. Let $\varepsilon > 0, \alpha_\delta = 2^{2^\delta}, q = \lfloor d/(\log d)^2 \rfloor, \delta_\kappa = \kappa \lfloor (\log d)^2 \rfloor, g = \lfloor d^{(1-\varepsilon)\log d} \rfloor$. Then for large d,

$$|\alpha_{\delta_1}| > 4,$$

$$|\alpha_{\delta_\kappa}| > |q\alpha_{\delta_{\kappa-1}}|^g \qquad (\kappa > 1).$$

Lemma 2.10 and Theorem 2.5 imply

$$g^{q-m-2} \leqq d^{s(m+1)} q^q$$

Substitution yields $s(m + 2) \gtrsim (1 - \varepsilon)d/\log d$. The assertion follows since ε may be arbitrarily small.

COROLLARY 2.12. *Let β compute*

$$a = \sum_{\delta=0}^{d} 2^{2^{\delta d^3}} x^\delta$$

in the field $\mathbb{C}(x)$ over $\mathbb{C} \cup \{x\}$. Then for large d, either

$$m \geqq d - 4$$

or

$$s > d^2/\log d.$$

(We used the notations of the preceding corollary).

Proof. Let $\alpha_\delta = 2^{2^{\delta d^3}}$, $\delta_\kappa = \kappa$, $q = d$, $g = 2^{d^3 - d^2}$. Then for large d,

$$|\alpha_1| > 4$$

and

$$|\alpha_\kappa| > |q\alpha_{\kappa-1}|^g \qquad (\kappa > 1).$$

Lemma 2.10 and Theorem 2.5 imply

$$g^{q-m-2} \leqq d^{s(m+1)}q^q.$$

By substituting and taking logarithms, we get

$$d^4 - d^3 - d\log d \leqq (s\log d + d^3 - d^2)(m + 2).$$

If $s \leqq d^2/\log d$, then $m \geqq d - 4$.

If we do not permit divisions, then the proofs are simpler and the results somewhat sharper. If one is only interested in s, i.e., in $L(1|\alpha)$, then one can eliminate all but one division by computing with unreduced numerators and denominators and executing one division at the end of the computation.

The proof of Theorem 2.5 shows that one can replace d by $\max_\kappa \delta_\kappa$ in (2.8). This implies that every lower bound for the computational complexity of a specific polynomial a of degree d which is proved using Theorem 2.5 is equally valid for all polynomials of higher degrees which have a as the initial segment of degree d.

Furthermore, Theorem 2.5 is valid for the values of a polynomial a at the points $\delta_1, \cdots, \delta_q$ (instead of the coefficients $\alpha_{\delta_1}, \cdots, \alpha_{\delta_q}$) if one assumes $\alpha_0 = 0$ and uses a stronger version of (2.8). This follows from the fact that Lemma 2.4 immediately implies a corresponding lemma for the values of the polynomials $\sum_{\delta=1}^{d} \alpha_{i\delta}x^\delta$ at the arguments $1, \cdots, d$. Using this version of the lemma, one can show, for example, that every polynomial which approximates the function e^{e^x-1} (the generating function of the number of partitions) at the points $1, \cdots, d$ reasonably well has to be hard to compute.

3. The computation of polynomials when linear operations are free. In this section, $k_0 \subset k$ are fields, k_0 is perfect and k is algebraically closed. Let $x_1, \cdots, x_n$ be indeterminates over k. The Galois group $\mathrm{Gal}(k/k_0)$ operates on $k[\mathbf{x}] = k[x_1, \cdots, x_n]$ as well as on k^n.

We need some definitions and facts about rationality.

R1. Let V be a Zariski-closed subset of k^n. V is called *k_0-closed* (or *defined over k_0*) if one of the following equivalent conditions is satisfied:

(i) the ideal of V is generated by polynomials belonging to $k_0[\mathbf{x}]$;

(ii) V is the set of common zeros of polynomials belonging to $k_0[\mathbf{x}]$;

(iii) V is stable with respect to $\mathrm{Gal}(k/k_0)$, i.e.,

$$\forall\sigma \in \mathrm{Gal}(k/k_0), \sigma V = V.$$

Proof. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) is trivial. For (iii) $\Rightarrow$ (i), see [2, §§ 12, 14] or [4, p. 74].

R2. Let C be a constructible subset of k^n. We say that C is *defined over k_0* if one of the following equivalent conditions is satisfied:

(i) C is a member of the Boolean algebra generated by the k_0-closed sets;

(ii) $\forall\sigma \in \mathrm{Gal}(k/k_0), \sigma C = C$.

Proof. (ii) $\Rightarrow$ (i): Let C be constructible and invariant with respect to $\mathrm{Gal}(k/k_0)$. Let U be the largest subset of C which is open in $\bar{C}$, i.e.,

$$U = \bigcup_{\substack{U' \subset C \\ U' \text{ open in } \bar{C}}} U'.$$

$\bar{C}$ and U are invariant, and therefore $\bar{C} - U$ is invariant. Hence $U = \bar{C} - (\bar{C} - U)$ belongs to the Boolean algebra generated by the k_0-closed sets. It is therefore sufficient to prove (i) for $C - U$ instead of C. It is easy to prove that the maximal dimension of the components of $C - U$ is strictly smaller than the maximal dimension of the components of C. We can therefore conclude by induction.

R3. Let V be a k_0-closed, irreducible subset of k^n and let $\boldsymbol{\alpha} \in V$. Then

$$\dim V \geqq \operatorname{trdg}_{k_0} k_0(\boldsymbol{\alpha})$$

(where trdg stands for transcendence degree).

Proof. Let $\alpha_1, \cdots, \alpha_m$ be algebraically independent over k_0 and let J be the ideal of V. It is sufficient to show that $x_1 + J, \cdots, x_m + J$ are algebraically independent over k in $k[x_1, \cdots, x_n]/J$. Assume otherwise. Then there is a nontrivial $P \in k[x_1, \cdots, x_m]$ which is an element of J. Let $P_1, \cdots, P_l$ be the different polynomials which are generated by the application of the Galois group on P; $Q = \prod_{\lambda=1}^{l} P_\lambda$. Q is invariant under $\operatorname{Gal}(k/k_0)$. Since k_0 is perfect, Q is a nontrivial polynomial in $k_0[x_1, \cdots, x_m] \cap J$. In particular, $Q(\alpha_1, \cdots, \alpha_m) = 0$; this contradicts the algebraic independence of $\alpha_1, \cdots, \alpha_m$ over k_0.

R4. We say a morphism $k^n \to k^m$ is *defined over* k_0 if it is given by polynomials belonging to $k_0[x_1, \cdots, x_n]$.

It is clear how to apply these concepts to a finite-dimensional k-vector space V if some basis is distinguished. If V is given as scalar extension of a k_0-vector space V_0, $V = V_0 \otimes_{k_0} k$, then it is easy to prove that the definitions do not depend on the basis chosen, if one restricts oneself to bases coming from V_0: one says that V possesses a k_0-structure by virtue of the representation $V = V \otimes_{k_0} k$.

Let A_0 be a p-dimensional k_0-ring, i.e., a k_0-ring (not necessarily commutative) which has finite dimension p as a k_0-vector space (the associative law is not essential for the following). All computations will be done in

$$A = A_0 \otimes_{k_0} k;$$

A is interpreted as a k-ring. We use the operation-time $z = 1_{\{*\}}$. We can assume that A_0 is a subset of A. If we neglect the multiplication in A, then A is a k-vector space with k_0-structure.

THEOREM 3.1. *Let* $\mathbf{a} = (a_1, \cdots, a_r)$, $\mathbf{b} = (b_1, \cdots, b_s)$, $N = (s + t + 1)(s + t + r) - s(s + 1)$. *The set*

$$C_{r,s}(t) := \{(\mathbf{a}, \mathbf{b}) \in A^r \times A^s : L(\operatorname{Im} \mathbf{a} \bmod \operatorname{Im} \mathbf{b}) \leqq t\}$$

is the projection to $A^r \times A^s$ *of the graph of the morphism*

$$\phi : A^r \leftarrow A^s \times k^N$$

defined over k_0. *In particular,* $C_{r,s}(t)$ *is an irreducible constructible subset of* $A^r \times A^s$ *defined over* k_0. *Also, for* $E \in \mathscr{E}(A)$,

$$C_{r,E}(t) := \{\mathbf{a} \in A^r : L(\operatorname{Im} \mathbf{a} \bmod E) \leqq t\}$$

is irreducible and constructible, and

$$\dim \overline{C_{r,E}(t)} \leqq N.$$

If $E \in \mathscr{E}(A_0)$, *then* $C_{r,E}(t)$ *is defined over* k_0.

Proof. Let $(e_1, \cdots, e_p)$ be a basis of the k_0-vector space A_0 and therefore also a basis of the k-vector space A. Then

$$e_i e_j = \sum_{l=1}^{p} \sigma_{ij}^{(l)} e_l, \qquad \sigma_{ij}^{(l)} \in k_0. \tag{3.1}$$

Further, let $y_j^{(i)}$ $(i = 1, \cdots, p, j = 1, \cdots, s)$, $z_{1j}^{(i)}, z_{2j}^{(i)}$ $(i = 0, \cdots, j-1, j = s+1, \cdots, s+t)$ and $z_j^{(i)}$ $(i = 0, \cdots, s+t, j = s+t+1, \cdots, s+t+r)$ be indeterminates over k. Then $B = A \otimes_k k[\mathbf{y}, \mathbf{z}]$ is a $k[\mathbf{y}, \mathbf{z}]$-ring. Again we can assume that A is a subset of B. $(e_1, \cdots, e_p)$ is then also a basis of the $k[\mathbf{y}, \mathbf{z}]$-module B, and (3.1) is valid in B. We define a sequence $f_0, \cdots, f_{s+t+r}$ of elements of B (a "generic" sequence of intermediate results):

$$f_0 = 1,$$

$$f_j = \sum_{i=1}^{p} y_j^{(i)} e_i \qquad \text{for } 1 \leqq j \leqq s,$$

$$f_j = \sum_{i=0}^{j-1} z_{1j}^{(i)} f_i \sum_{i=0}^{j-1} z_{2j}^{(i)} f_i \quad \text{for } s+1 \leqq j \leqq s+t,$$

and

$$f_j = \sum_{i=0}^{s+t} z_j^{(i)} f_i \qquad \text{for } s+t+1 \leqq j \leqq s+t+r.$$

We will write

$$f_{s+t+\rho} = \sum_{\nu=1}^{p} P_\rho^{(\nu)} e_\nu, \qquad P_\rho^{(\nu)} \in k[\mathbf{y}, \mathbf{z}] \quad \text{for } 1 \leqq \rho \leqq r.$$

(3.1) implies

$$P_\rho^{(\nu)} \in k_0[\mathbf{y}, \mathbf{z}]. \tag{3.2}$$

These polynomials define a morphism

$$\phi : A^r \leftarrow A^s \times k^N;$$

we interpret the y's as coordinate variables of A^s and the z's as coordinate variables of k^N. In order to prove the first assertion of the theorem, we have to show: let $b_1, \cdots, b_s \in A$ with

$$b_j = \sum_{i=1}^{p} \eta_j^{(i)} e_i.$$

Then

$$L(a_1, \cdots, a_r \bmod b_1, \cdots, b_s) \leqq t \tag{3.3}$$

if and only if there are $\zeta_{1j}^{(i)}, \zeta_{2j}^{(i)} \in k$ $(0 \leqq i \leqq j-1,\ s+1 \leqq j \leqq s+t)$ and $\zeta_j^{(i)}$ $(i = 0, \cdots, s+t, j = s+t+1, \cdots, s+t+r)$ such that

$$a_\rho = \sum_{\nu=1}^{p} P_\rho^{(\nu)}(\boldsymbol{\eta}, \boldsymbol{\zeta}) e_\nu.$$

In other words (by the definition of the $P_\rho^{(\nu)}$'s): (3.3) is valid iff there are $\bar{f}_{s+1}, \cdots, \bar{f}_{s+t} \in A$ such that $\bar{f}_{s+\tau}$ is the product of two k-linear combinations of $1, b_1, \cdots, b_s, \bar{f}_{s+1}, \cdots, \bar{f}_{s+\tau-1}$ $(1 \leqq \tau \leqq t)$ and such that a_ρ is a k-linear combination of $1, b_1, \cdots, b_s, \bar{f}_{s+1}, \cdots, \bar{f}_{s+t}$ $(1 \leqq \rho \leqq r)$. This is easy to prove as follows: if (3.3) is valid and if β computes $a_1, \cdots, a_r \bmod b_1, \cdots, b_s$ in A and $L(*|\beta) = t$, then let $\bar{f}_{s+1}, \cdots, \bar{f}_{s+t}$ be the results of the computational steps β_i with $\omega_i = *$ in the given order. On the other hand, if there exist $\bar{f}_{s+1}, \cdots, \bar{f}_{s+t}$ with the desired properties, then (3.3) is a consequence of the transitivity theorem (using the trivial Lemma 2.1 of [11]). Therefore $C_{r,s}(t)$ is the projection of graph(ϕ) on $A^r \times A^s$. Hence $C_{r,s}(t)$ is irreducible and constructible (by the theorem of Chevalley). (3.2) implies that ϕ is defined over k_0; hence graph(ϕ) is stable with respect to Gal (k/k_0). Therefore $C_{r,s}(t)$ is stable with respect to Gal(k/k_0); i.e., $C_{r,s}(t)$ is defined over k_0. Let $E \in \mathscr{E}(A)$, $E = \{b_1, \cdots, b_s\}$ with $b_j = \sum_{i=1}^{p} \eta_j^{(i)} e_i$. Then $C_{r,E}(t) = \{\mathbf{a} : (\mathbf{a}, \mathbf{b}) \in C_{r,s}(t)\}$ is evidently the image of the morphism

$$\phi(\eta, \cdot) : k^N \to A^r. \tag{3.4}$$

The remaining assertions follow.

Definition 3.2. A function

$$\lambda(\cdot \bmod \cdot) : \mathscr{E}(A)^2 \to \mathbb{N} \cup \{\infty\}$$

is *lower semicontinuous* (in the first variable) if the set

$$\{\mathbf{a} \in A^r : \lambda(\operatorname{Im} \mathbf{a} \bmod E) \leqq t\}$$

is Zariski-closed for all $r \in \mathbb{N}'$, $E \in \mathscr{E}(A)$ and $t \geqq 0$.

Theorem 3.3. *If*

$$\lambda(\cdot \bmod \cdot) : \mathscr{E}(A)^2 \to \mathbb{N} \cup \{\infty\}$$

is monotonic in its first argument, then there is a function

$$\boldsymbol{\lambda}(\cdot \bmod \cdot) : \mathscr{E}(A)^2 \to \mathbb{N} \cup \{\infty\}$$

such that

$$\{\mathbf{a} \in A^r : \boldsymbol{\lambda}(\operatorname{Im} \mathbf{a} \bmod E) \leqq t\} = \overline{\{\boldsymbol{\alpha} \in A^r : \lambda(\operatorname{Im} \mathbf{a} \bmod E) \leqq t\}} \tag{3.5}$$

for all $r \in \mathbb{N}'$, $E \in \mathscr{E}(A)$ and $t \geqq 0$. $\boldsymbol{\lambda}$ is the largest lower semicontinuous function $\leqq \lambda$.

Proof. We set

$$D_r(t) := \{\mathbf{a} \in A^r : \lambda(\operatorname{Im} \mathbf{a} \bmod E) \leqq t\}.$$

(3.5) is equivalent to

$$\boldsymbol{\lambda}(\operatorname{Im} \mathbf{a} \bmod E) = \min \{t : \mathbf{a} \in \overline{D_r(t)}\}$$

for all $\mathbf{a} \in A^r$. We can use this line as definition of $\boldsymbol{\lambda}$, if we know that the right side depends only on Im $\mathbf{a}$. Therefore it is sufficient to show:

$$(a_1, \cdots, a_r) \in D_r(t) \Rightarrow (a_{\pi 1}, \cdots, a_{\pi r}) \in D_r(t)$$

for arbitrary permutations π,

$$(a_1, \cdots, a_r) \in \overline{D_r(t)} \Rightarrow (a_1, \cdots, a_r, a_r) \in \overline{D_{r+1}(t)},$$

$$(a_1, \cdots, a_r) \in \overline{D_r(t)} \Rightarrow (a_1, \cdots, a_{r-1}) \in \overline{D_{r-1}(t)}.$$

The three implications follow from the observation that the set of $\mathbf{a} \in A^r$, for which the right sides are valid, is closed and contains $D_r(t)$. The remaining assertions are trivial.

THEOREM 3.4. $\mathbf{L}(\cdot \bmod \cdot)$ *is the largest lower semicontinuous relative L-bound.*

Proof. Because of Theorem 3.3 and [10, Thm. 4.8] it suffices to show that $\mathbf{L}$ is a relative $\mathbf{L}$-bound.

Monotonicity. We only prove that it is monotonic in the first argument.

It suffices to show

$$(a_1, \cdots, a_r) \in \overline{C_{r,E}(t)} \Rightarrow (a_1, \cdots, a_{r-1}) \in \overline{C_{r-1,E}(t)}. \tag{3.6}$$

This follows from the fact that

$$\{(a_1, \cdots, a_r) : (a_1, \cdots, a_{r-1}) \in \overline{C_{r-1,E}(t)}\}$$

is closed and contains $C_{r,E}(t)$.

Transitivity. First we show that $\mathbf{L}(\cdot \bmod D)$ is an L-bound for the canonical D-expansion of A. Since $L(\cdot \bmod D)$ is such an L-bound, the following is valid:

$$L(F \cup \{\omega\mathbf{a}\} \bmod D) \leqq L(F \cup \operatorname{Im} \mathbf{a} \bmod D) + z(\omega)$$

for $\mathbf{a} \in \operatorname{dom} \omega$, $\omega \in \{0, 1, +, -, *\} \cup k \cup D$. For $F = \{f_1, \cdots, f_r\}$, $\mathbf{a} = (a_1, \cdots, a_s)$, this means

$$(f_1, \cdots, f_r, a_1, \cdots, a_s) \in C_{r+s,D}(t) \Rightarrow (f_1, \cdots, f_r, \omega\mathbf{a}) \in C_{r+1,D}(t + z(\omega))$$

for all t. Evidently $\omega : A^s \to A$ is a morphism. Therefore,

$$\{(f_1, \cdots, f_r, a_1, \cdots, a_s) : (f_1, \cdots, f_r, \omega\mathbf{a}) \in \overline{C_{r+1,D}(t + z(\omega))}\}$$

is a closed set containing $C_{r+s,D}(t)$ and hence containing $\overline{C_{r+s,D}(t)}$. This means

$$(f_1, \cdots, f_r, a_1, \cdots, a_s) \in \overline{C_{r+s,D}(t)} \Rightarrow (f_1, \cdots, f_r, \omega\mathbf{a}) \in \overline{C_{r+1,D}(t + z(\omega))},$$

or in other words,

$$\mathbf{L}(F \cup \operatorname{Im} \mathbf{a} \bmod D) \leqq t \Rightarrow \mathbf{L}(F \cup \{\omega\mathbf{a}\} \bmod D) \leqq t + z(\omega).$$

Since this is valid for all t, we infer

$$\mathbf{L}(F \cup \{\omega\mathbf{a}\} \bmod D) \leqq \mathbf{L}(F \cup \operatorname{Im} \mathbf{a} \bmod D) + z(\omega).$$

Therefore $\mathbf{L}(\cdot \bmod D)$ is an L-bound mod D. To prove transitivity we can assume $u := \mathbf{L}(E \bmod D) < \infty$ without loss of generality. Then

$$\mathbf{L}(F \cup E \bmod D) - u$$

(fixed E, D) is also an L-bound mod $E \cup D$; hence

$$\mathbf{L}(F \cup E \bmod D) - u \leqq L(F \bmod E \cup D).$$

This means ($F = \{f_1, \cdots, f_r\}$, $E = \{b_1, \cdots, b_s\}$)

$$(f_1, \cdots, f_r) \in C_{r,E \cup D}(t) \Rightarrow (f_1, \cdots, f_r, b_1, \cdots, b_s) \in \overline{C_{r+s,D}(t + u)}.$$

Obviously

$$\{(f_1, \cdots, f_r) : (f_1, \cdots, f_r, b_1, \cdots, b_s) \in \overline{C_{r+s,D}(t + u)}\}$$

is a closed set containing $C_{r,E\cup D}(t)$ and therefore $\overline{C_{r,E\cup D}(t)}$. This means

$$(f_1,\cdots,f_r)\in\overline{C_{r,E\cup D}(t)}\Rightarrow(f_1,\cdots,f_r,b_1,\cdots,b_s)\in\overline{C_{r+s,D}(t+u)}$$

and thus

$$\mathbf{L}(F \bmod E\cup D)\leqq t\Rightarrow\mathbf{L}(F\cup E \bmod D)\leqq t+u.$$

Since this is valid for all t, we can infer

$$\mathbf{L}(F\cup E \bmod D)\leqq\mathbf{L}(F \bmod E\cup D)+\mathbf{L}(E \bmod D).$$

Normalization. Since $\mathbf{L}(\,\cdot \bmod D)$ is an L-bound for the canonical D-expansion of A, we have (putting $D=\mathrm{Im}\,\mathbf{a}$)

$$\mathbf{L}(\omega\mathbf{a} \bmod \mathrm{Im}\,\mathbf{a})\leqq\mathbf{L}(\mathrm{Im}\,\mathbf{a} \bmod \mathrm{Im}\,\mathbf{a})+z(\omega)\leqq z(\omega).$$

THEOREM 3.5. *Let* $\mathbf{a}\in A^r$, $\mathbf{b}\in A^s$. *If* $(e_1,\cdots,e_p)$ *is a* k_0*-basis of* A_0 *and therefore a k-basis of A, and if*

$$a_j=\sum_{i=1}^{p}\alpha_j^{(i)}e_i$$

with $\alpha_j^{(i)}\in k$, *then*

$$\mathbf{L}(\mathrm{Im}\,\mathbf{a} \bmod \mathrm{Im}\,\mathbf{b})\geqq(\mathrm{trdg}_{k_0}k_0(\boldsymbol{\alpha}))^{1/2}-(r+s).$$

Proof. Let

$$\mathbf{L}(\mathrm{Im}\,\mathbf{a} \bmod \mathrm{Im}\,\mathbf{b})=t. \tag{3.7}$$

By Theorem 3.1, $\overline{C_{r,\mathrm{Im}\,\mathbf{b}}(t)}$ is an irreducible subvariety of A_r such that

$$\begin{aligned}\dim\overline{C_{r,\mathrm{Im}\,\mathbf{b}}(t)}&\leqq(s+t+1)(s+t+r)-s(s+1)\\&\leqq(t+r+s)^2.\end{aligned}\tag{3.8}$$

Theorem 3.1 also states that $C_{r,\mathrm{Im}\,\mathbf{b}}(t)$ is stable with respect to $\mathrm{Gal}\,(k/k_0)$. Since the elements $\sigma\in\mathrm{Gal}\,(k/k_0)$ are continuous, $\overline{C_{r,\mathrm{Im}\,\mathbf{b}}(t)}$ is also stable. Therefore $\overline{C_{r,\mathrm{Im}\,\mathbf{b}}(t)}$ is k_0-closed. (By 3.7)

$$\mathbf{a}\in\overline{C_{r,\mathrm{Im}\,\mathbf{b}}(t)}.$$

Using R.3, we get

$$\dim\overline{C_{r,\mathrm{Im}\,\mathbf{b}}(t)}\geqq\mathrm{trdg}_{k_0}k_0(\boldsymbol{\alpha}).$$

The assertion follows now from (3.8).

In the following, we assume $k_0=\mathbb{Q}$. Further, let $(e_1,\cdots,e_p)$ be a basis of the k_0-vector space A_0 such that $e_1=1$ and

$$\sigma_{i,j}^{(l)}\in\mathbb{Z} \tag{3.9}$$

(see (3.1)). We set

$$\lambda:=\max_{i,j}\sum_{l}|\sigma_{ij}^{(l)}| \tag{3.10}$$

and assume $\lambda \geqq 1$. Further, let $\mathbf{b} = (b_1, \cdots, b_s) \in A_0^s$, $b_j = \sum_{i=1}^{p} \eta_j^{(i)} e_i$ with $\eta_j^{(i)} \in \mathbb{Z}$. We set

$$\gamma := \sum_{i,j} |\eta_j^{(i)}| \tag{3.11}$$

and assume $\gamma \geqq 1$. Using the basis $(e_1, \cdots, e_p)$, we can identify the affine space A^r with $k^{pr} = k^p \times \cdots \times k^p$. If $y_1, \cdots, y_{pr}$ are its coordinate variables, then its coordinate ring is the polynomial ring $k[y_1, \cdots, y_{pr}]$. Then $\overline{C_{r,\operatorname{Im}\mathbf{b}}(t)}$ is a closed irreducible subvariety of k^{pr}; we denote its ideal by $J(t)$.

THEOREM 3.6. *Let $r, s \geqq 1$, $q \geqq 5$, $1 \leqq \delta_1, \cdots, \delta_q \leqq pr$; let g be a natural number such that*

$$g^{q-(t+r+s)^2} > 2^{(t+r+s)^2(t+1)} q^q \log(\lambda(\gamma + 1)). \tag{3.12}$$

Then there exists a nontrivial form

$$H \in J(t) \cap \mathbb{Z}[y_{\delta_1}, \cdots, y_{\delta_q}]$$

such that

$$\text{height } H \leqq 3, \quad \text{degree } H = g.$$

Proof. We use the proof of Theorem 3.1. By replacing the $y_j^{(i)}$ of that proof by $\eta_j^{(i)}$, we get polynomials $P_\rho^{(\nu)}(\boldsymbol{\eta}, \cdot) \in \mathbb{Q}[\mathbf{z}]$. The construction implies that these polynomials are elements of $\mathbb{Z}[\mathbf{z}]$. If we set

$$P_{(\rho-1)p+\nu} := p_\rho^{(\nu)}(\boldsymbol{\eta}, \cdot),$$

then by (3.4) the systems of values of $P_1, \cdots, P_{pr}$ form exactly the set $C_{r,\operatorname{Im}\mathbf{b}}(t) \subset k^{pr}$. An element $H \in \mathbb{Z}[y_{\delta_1}, \cdots, y_{\delta_q}]$ is therefore contained in $J(t)$ if and only if

$$H(P_{\delta_1}, \cdots, P_{\delta_q}) = 0. \tag{3.13}$$

The construction of the polynomials $P_\rho^{(\nu)}(\boldsymbol{\eta}, \cdot)$ also yields (the proof goes by induction on t) that

$$\max_{1 \leqq \nu \leqq p} \text{degree } P_\rho^{(\nu)}(\boldsymbol{\eta}, \cdot) \leqq 2^{t+1} - 1$$

and

$$\sum_{\nu=1}^{p} \text{weight } P_\rho^{(\nu)}(\boldsymbol{\eta}, \cdot) \leqq 2^{\log(\lambda(\gamma+2))2^t - \log\lambda} - 1$$

for all ρ. We can apply Lemma 2.3 with $m = N, c = 2^{t+1}, f = 2^{\log(\lambda(\gamma+1))2^{t+1}}$. Since (2.1) is a consequence of (3.12), there is a nontrivial form $H \in \mathbb{Z}[y_{\delta_1}, \cdots, y_{\delta_q}]$ of degree g and height $\leqq 3$ satisfying (3.13), i.e., H is an element of $J(t)$.

COROLLARY 3.7. *Interpret $\mathbb{C}[x]$ as $\mathbb{C}$-ring over $\{x\}$. Then for $d \to \infty$ (for large d, respectively)*

$$L\left(* \,\middle|\, \sum_{\delta=0}^{d} \exp(2\pi i/2^\delta) x^\delta\right) \gtrsim d^{1/3}, \tag{3.14}$$

$$L\left(* \,\middle|\, \sum_{\delta=0}^{d} 2^{2^\delta} x^\delta\right) \gtrsim d^{1/3} \tag{3.15}$$

$$L\left(* \,\middle|\, \sum_{\delta=0}^{d} 2^{2^{\delta d 3}} x^\delta\right) > \sqrt{d} - 3. \tag{3.16}$$

Proof. Let $a \in \mathbb{C}[x]$ be of degree d. Then

$$L_{\mathbb{C}[x]}(*|a) \geqq L_A(*|a \bmod \xi),$$

where $A = \mathbb{C}[x]/x^{d+1}\mathbb{C}[x]$ is interpreted as a $\mathbb{C}$-ring and ξ is the residue class of x. Furthermore,

$$A = (\mathbb{Q}[x]/x^{d+1}\mathbb{Q}[x]) \otimes_{\mathbb{Q}} \mathbb{C}.$$

Therefore we can apply Theorem 3.6 with $p = d + 1$, $e_1 = \xi^{i-1}$,

$$\sigma_{ij}^{(l)} = \begin{cases} 1 & \text{if } i + j - 1 = l, \\ 0 & \text{otherwise,} \end{cases}$$

$\lambda = 1$, $s = 1$, $b_1 = \xi$, $\gamma = 1$ and $r = 1$. One concludes now as in the proofs of Corollaries 2.7, 2.11 and 2.12.

In a similar way, Theorem 3.6 applies to polynomial rings in several variables.

Acknowledgments. Many thanks go to Walter Baur and to the referee for their careful reading of the paper and their helpful remarks.

REFERENCES

[1] E. G. BELAGA, *Some problems involved in the computation of polynomials*, Dokl. Akad. Nauk SSSR, 123 (1958), pp. 775–777.

[2] A. BOREL, *Linear Algebraic Groups*, W. A. Benjamin, New York, 1969.

[3] J. EVE, *The evaluation of polynomials*, Numer. Math., 6 (1964), pp. 17–21.

[4] S. LANG, *Introduction to Algebraic Geometry*, Interscience, New York, 1958.

[5] T. S. MOTZKIN, *Evaluation of polynomials and evaluation of rational functions*, Bull. Amer. Math. Soc., 61 (1955), p. 163.

[6] D. MUMFORD, *Introduction to Algebraic Geometry*, Harvard Lecture Notes.

[7] M. PETERSON AND L. STOCKMEYER, *Bounds on the evaluation time for rational polynomials*, IEEE Conference Record of the 12th Ann. Sympos. of Switching and Automata Theory, 1971, pp. 140–143.

[8] T. SCHNEIDER, *Einführung in die Transzendenten Zahlen*, Springer-Verlag, Berlin, 1957.

[9] J. R. SHOENFIELD, *Mathematical Logic*, Addison-Wesley, Reading, Mass., 1967.

[10] V. STRASSEN, *Berechnung und Programm I*, Acta Informat., 1 (1972), pp. 320–335.

[11] ———, *Vermeidung von Divisionen*, Crelle Journal für die Reine und Angew. Mathematik, 264 (1973), pp. 184–202.