LOWER BOUNDS IN ALGEBRAIC COMPUTATIONAL COMPLEXITY

Dima Grigoriev

▶ **To cite this version:**

Dima Grigoriev. LOWER BOUNDS IN ALGEBRAIC COMPUTATIONAL COMPLEXITY. Journal of Soviet Mathematics, 1985. hal-03053161

HAL Id: hal-03053161
https://hal.science/hal-03053161

Submitted on 10 Dec 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

LOWER BOUNDS IN ALGEBRAIC COMPUTATIONAL COMPLEXITY

D. Yu. Grigor'ev

UDC 519.5

The present article is a survey of selected methods for obtaining lower bounds in algebraic complexity. We present the contents.

Introduction. 1. Basic concepts. Chapter I. Algebraic-geometric approach to obtaining lower bounds of computational complexity of polynomials. 2. Evaluating a polynomial with "general" coefficients. 3. Computational complexity of individual polynomials. 4. The degree method and its generalizations (the case of an infinite ground field). 5. The degree method (the case of a finite ground field). 6. Additive complexity and real roots. Chapter II. Lower bounds on multiplicative complexity for problems of linear algebra. 7. Multiplicative complexity and rank. 8. Rank of a pair of bilinear forms. 9. Multiplicative complexity of a bilinear form over a commutative ring. 10. Bounds on the rank of algebras. 11. Linearized multiplicative complexity. Chapter III. Complexity for straight-line programs of nonstandard types. 12. Irrational computational complexity of algebraic functions. 13. Monotone programs. 14. Time–space tradeoffs. 15. Graph-theoretic methods in algebraic complexity. 16. Additive complexity in triangular and directed computations and Bruhat decomposition.

INTRODUCTION

The problem of lower bounds is one of the most difficult ones in computational complexity theory, and it can be said without exaggeration that their obtaining constitutes the naturally fundamental topic of complexity theory, since the establishment of lower bounds, i.e., the construction of sufficiently fast algorithms, is, rather, the prerogative of the other mathematical sciences from which the concrete computational problems originate. In spite of the fact that the problem of obtaining nontrivial lower bounds (i.e., of proving the impossibility of sufficiently fast algorithms for given computational problems, and, by the same token, the penetration of the secrets of fast algorithms) is far from completely solved, in it there are certain interesting advances, particularly in that part of complexity theory which relates to the problems traceable to algebra, called algebraic complexity (see Bel'tyukov's survey in the present issue on lower bounds in some other sections of complexity theory).

Algebraic complexity is one of the oldest branches of complexity theory (but it is one that is being most intensively worked on at the present time); it has been around for nearly 25 years, but a sufficiently complete survey devoted to it has not yet appeared in Russian. Among the foreign publications we should note, in the first place, the book [27], as well as [1, 13], but lower bounds are in fact absent in the latter, while [27] does not go into the achievements of recent years.

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, Vol. 118, pp. 25-82, 1982.

 0090-4104/85/2904-1388$09.50 © 1985 Plenum Publishing Corporation

To no extent does the author pretend at completeness of the exposition of all the results in the area of obtaining lower bounds in algebraic computational complexity; rather, the present text is a survey of selected methods and achievements, whose aim is to fill in the gaps existing in the Russian literature. The methods that have already been widely propagated, as well as those that do not as yet have sufficiently strong applications, are presented in lesser detail. The number of proofs given in the present survey is comparatively small; a sufficiently complete list of references permits us to refer to appropriate literature when necessary.

The author tried to pay most attention to those methods of establishing lower bounds which are connected with nontrivial algebraic methods. The profound connections with classical algebra, as also the problem statements, being atypical of traditional algebra, are, in general, a characteristic feature of algebraic complexity, which can make it attractive for algebraists.

A survey of methods in algebraic complexity leaves a somewhat mosaiclike impression. This is due, it seems, to the fact this branch of mathematics is still quite young and as yet no unified ideas have been formulated in it, the problems are difficult and have to be approached individually. Therefore, the different chapters are formally little connected with each other (except Sec. 1 which gives the definitions needed for understanding what follows). Essentially, each section contains a description of an individual method; at the same time, the ordering of the material is not random and has definite historical and methodical reasons (if the ontogeny and phylogeny of algebraic complexity is desired). We note that the contents of Secs. 6, 11, 16, and a part of Sec. 15 are being published for the first time.

The numbering of the sections and of the formulas is consecutive; the theorems, lemmas, and corollaries are two-numbered, the first of which is the number of the corresponding section.

1. Basic Concepts

The basic computing model used in algebraic complexity is the straight-line program (see [1, 27], for example) which we now describe. Let there be given:

1) a collection of input variables $x_1,\dots,x_n$;

2) a ring K (usually this is a field which will be denoted by F) which is subsequently called the ground ring;

3) a set P of base operations (usually $P=\{+,\times,/\}\cup\{\times\gamma\}_{\gamma\in K}$, where $+,\times,/$ are binary arithmetic operations, $\times\gamma$ is a unary operation, viz., multiplication by γ).

The variables $x_1,\dots,x_n$ can be assumed or not to be pairwise commuting; often this is clear from the substance of the problem being analyzed.

4) a straight-line program (SLP) proper is a sequence of rows (instructions) the l-th of which has the following form:

$$z_l = f_l(z_{i_1},\dots,z_{i_u}, x_{j_1},\dots,x_{j_v}),$$

where $i_1<l,\dots,i_u<l$ and $f_l\in P$.

By induction on l there is naturally determined the term in the variables $x_1,\dots,x_n$ corresponding to the working variable z_l and called the value of z_l. We say that a

certain family of terms (or of functions) of $x_1,\dots,x_n$ is computed by a given SLP if the terms of the family being examined are encountered among the values of the working variables z_ℓ of this SLP.

We fix as well the integer-valued function $\lambda=\lambda_\odot : P \to N\cup\{0\}$, and the number $\lambda(f)$ for $f\in P$ is called the complexity of operation f. The complexity of a SLP β (we denote it $C(\beta)=C_\odot(\beta)$) is the sum of all $\lambda(f_\ell)$ over the instruction of this SLP. Finally, the complexity of a collection of terms (or functions) $g_1,\dots,g_K$ is the smallest complexity of the SLP's computing this family (we denote it $C(g_1,\dots,g_K)=C_\odot(g_1,\dots,g_K)$). Sometimes instead of the word "complexity" we shall use the terminology complexity measure. We cite one example of complexity. Let $\lambda_t(f)=1$ for every $f\in P$. Then the corresponding complexity C_t "counts" the number of all operations of the SLP and is called the total complexity.

Below we shall refer to the notation adopted in the present section, each time making concrete the K (or F), P, $\lambda=\lambda_\odot$.

CHAPTER I. ALGEBRAIC-GEOMETRIC APPROACH TO OBTAINING LOWER BOUNDS OF COMPUTATIONAL COMPLEXITY OF POLYNOMIALS

2. Evaluating a Polynomial with "General" Coefficients

One of the first problems examined in algebraic complexity was the evaluation of a polynomial with "general" coefficients at one point (see [18] and the references given there to the earlier literature). In other words: F is an algebraically closed field, $P=\{+,\times,/\}\cup\{\times\gamma\}_{\gamma\in F}$. We denote $\lambda_+(+)=1$, $\lambda_+(\times)=\lambda_+(/)=\lambda_+(\times\gamma)=0$ (the corresponding complexity C_+ is sometimes called additive); $\lambda_{\times/}(+)=0$, $\lambda_{\times/}(\times)=\lambda_{\times/}(/)=\lambda_{\times/}(\times\gamma)=1$. It is required to estimate $C_\odot(a_0+a_1x+\dots+a_nx^n)$ where $\odot=+$ or $\odot=\times/$; in the given case $\{x,a_0,\dots,a_n\}$ is a collection of pairwise-commuting input variables, where $x,a_0,\dots,a_n$ are algebraically independent over F; therefore, the coefficients are called "general" (in this case the SLP being examined were called, in [18], schemes without preliminary processing of the coefficients).

THEOREM 2.1 [18]. $C_+(a_0+\dots+a_nx^n)=C_{\times/}(a_0+\dots+a_nx^n)=n$. It is easy to see that in both cases the upper bounds are achieved with the aid of Horner's scheme.

Informally speaking, the idea for obtaining the lower bound is the following. The value of every working variable of the SLP, viz., a scheme without preliminary coefficient processing, is some rational function $g\in F(x,a_0,\dots,a_n)$ which can in some way be written as a function $g=(b_0+\dots+b_px^p)/(c_0+\dots+c_qx^q)$, where $b_i,c_i\in F(a_0,\dots,a_n)$. Then by induction on K it can be shown that if $C_\odot(g)\leq K$, then the degree of transcendence of field $F(b_0,\dots,b_p,c_0,\dots,c_q)$ over F does not exceed $K+1$ for a suitable choice of writing g as a fraction; whence the theorem now follows ($\odot$ can stand for either $+$ or $\times/$).

We note that from what has been proved there immediately follows the validity of Theorem 2.1 for the case of an arbitrary infinite field.

Another class of SLP that can be considered, called schemes with preliminary coefficient processing in [18], is defined, in the terminology of Sec. 1, thus: $F=\overline{\mathbb{Q}(a_0,\dots,a_n)}$ is the field of algebraic functions of variables algebraically independent over $\mathbb{Q}$; P and $\lambda_\odot$

are the same as above. It is required to estimate $C_{\odot}(a_0+\dots+a_n x^n)$; moreover, here the set of input variables is $\{x\}$. The interpretation is the following: if it is necessary to evaluate one and the same polynomial many times at different points, then it makes sense to compute certain auxiliary functions of the coefficients beforehand, i.e., a multiple evaluation of the values of the polynomial at different points compensates for the outlay on evaluating these algebraic functions. We denote $g=a_0+\dots+a_n x^n$.

THEOREM 2.2 [18, 41]. 1) $C_+(g)=n$;

2) $C_{x/}(g)=n/2+1$ for even n;

3) $C_{x/}(g)=(n+1)/2$ for odd $n\geqslant 9$;

4) $C_{x/}(g)=(n+3)/2$ for odd $n\leqslant 7$.

The proofs of the lower bounds are similar to those of the lower bounds in Theorem 2.1. The upper bounds in cases 2), 3), 4) (which have been proved only for algebraically closed fields F of characteristic zero and for real-closed fields) call for nontrivial constructions. Estimates of the joint behavior of $C_+(\beta)$ and $C_{x/}(\beta)$ for an SLP β computing g have been presented as well in [41].

Theorem 2.2 can be generalized to the case of several polynomials of one variable common to them all. To be precise, let $g_i=a_0^{(i)}+a_1^{(i)}x+\dots+a_{n_i}^{(i)}x^{n_i}$ $(1\leqslant i\leqslant K)$ and let $\{a_j^{(i)}\}$ be algebraically independent over $\mathbb{Q}$. We set $\sum_{1\leqslant i\leqslant K} n_i=N$; then we have

THEOREM 2.3 [18]. 1) $C_+(g_1,\dots,g_K)=N$;

2) $C_{x/}(g_1,\dots,g_K)=N/2+1$ for even N;

3) $(N-1)/2+1\leqslant C_{x/}(g_1,\dots,g_K)\leqslant(N-1)/2+2$ for odd N.

In [18] SLP have been constructed for which C_+ and $C_{x/}$ are simultaneously close to the lower bounds from Theorems 2.2 and 2.3.

The last type of SLP we shall consider in this section is defined as follows: $F=\overline{\mathbb{Q}(a_0,\dots,a_n)}$; $P=\{+,x,/\}\cup\{xy\}_{y\in F}$; $\lambda_m(+)=\lambda_m(xy)=0$, $\lambda_m(x)=\lambda_m(/)=1$; $\{x\}$ is the set of input variables. The complexity C_m thereby definable will be called multiplicative complexity (i.e., C_m "counts" the number of nonlinear operations). Below, $\asymp$ and $\precsim$ denote, respectively, equality and inequality to within a multiplicative constant.

THEOREM 2.4 [42]. $C_m(g)\asymp\sqrt{n}$.

The upper bound can be obtained on the basis of the following equality (without loss of generality we take it that $n=k^2$): $g=(a_0+a_1x+\dots+a_kx^k)+(a_{k+1}x+a_{k+2}x^2+\dots+a_{2k}x^k)x^k+\dots+(a_{n-k+1}x+\dots+a_nx^k)x^{n-k}$. The proof of the lower bound is analogous to that of the lower bounds in the preceding theorems.

3. Computational Complexity of Individual Polynomials

In the preceding section we examined SLP for the evaluation of the polynomial $g=a_0+a_1x+\dots+a_nx^n$ whose coefficients $a_0,\dots,a_n$ are algebraically independent over F. Of considerable interest is the case when the coefficients $a_0,\dots,a_n$ "have been constructed simply," for instance, they are integers or algebraic numbers. In other words, let $F=\overline{\mathbb{Q}}$; $P=\{+,x,/\}\cup\{xy\}_{y\in F};\lambda_+,\lambda_{x/},\lambda_m$ have the same sense as above; $\{x\}$ is the set of input variables. The problem is to estimate $C_{\odot}(g)$ for various $g\in F[x]$.

The proofs of Theorems 2.2 and 2.4 enable us to prove at the same time the following statement: the dimension of the variety (lying in F^{n+1}) of the coefficient vectors $(a_0,\dots,a_n)$ of polynomials g, for which either

$$C_+(g)\leqslant k \quad \text{or } C_{x/}(g)\leqslant k-n+\left[\frac{n}{2}\right]+1 \quad \text{or} \quad C_m(g)\leqslant\sqrt{k},$$

does not exceed $k+1$. In particular, almost all (in the sense of algebraic geometry, i.e., those whose coefficient vectors belong to an everywhere-dense set in the Zariski topology) polynomials g satisfy the inequalities

$$C_+(g)=n,\quad C_{x/}(g)\geqslant\left[\frac{n}{2}\right]+1,\quad C_m(g)\geqslant\sqrt{n}. \tag{1}$$

In spite of this circumstance we have not succeeded in solving satisfactorily even the following weakened variant of the above-stated problem on estimating $C_{\odot}(g)$ (although in recent years there has been significant progress in it, with which we deal below in the present section): "indicate explicitly" a polynomial g with "good" coefficients, satisfying inequalities (1) or at least one of them. This would shed light on the secrets of complexity. The words within the quotation marks require a more precise definition, but a reasonable problem statement (for example, the words "good" coefficients can signify coefficients from the set $\{0,1\}$) will be clear from the subsequent context.

Deviating somewhat, we remark that a similar situation, somewhat unusual for classical mathematics, when it is difficult to "indicate explicitly" even one simply constructed concrete element from a sufficiently natural everywhere-dense set (in the case at hand, the set of polynomials difficult to evaluate, i.e., polynomials satisfying inequalities (1) or even weaker inequalities), is very prevalent in algebraic complexity and is of great interest (see the next section as well). This not very precisely posed problem of the "explicit indication" of difficultly computable functions (polynomials or polynomial families in Chapter I) will be somewhat imprecisely called the problem of obtaining lower bounds.

We now go on to present certain advances in this problem, made recently. A number of papers (for example, [55, 50, 51]), the first ones on this topic, explicitly constructed polynomials which satisfy somewhat weakened inequalities (1) or some portion of them or their disjunction. The methods in these papers are very similar in their ideas, differing in a number of technical details, and they are weaker than the one elegant method of Heintz and Sieveking [36], which we present somewhat later in this section. Therefore, for completeness of the picture we briefly sketch the idea of these methods, following the first paper [55] in this cycle of papers. Thus, let the polynomial $g=a_0+\dots+a_d x^d$ be evaluated with the aid of a SLP β for which the inequalities $C_+(\beta)\leqslant u$, $C_x(\beta)\leqslant v_1$, $C_/(\beta)\leqslant v_2$ have been fulfilled (here, naturally, $\lambda_x(+)=\lambda_x(/)=0$, $\lambda_x(x)=\lambda_x(xy)=1$; $\lambda_/(+)=\lambda_/(x)=\lambda_/(xy)=0$, $\lambda_/(/)=1$). We set $m=\min\{u, 2(v_1+v_2)\}$. The maximum of the moduli of the polynomial's coefficients is called its weight.

THEOREM 3.1 [55]. Given a positive integer $h>d^{\frac{(u+v_1+v_2)^2}{d-m-2}}$. Then there exists a nontrivial form $H\in\mathbb{Z}[y_0,\dots,y_d]$, $\deg H\leqslant h$, with weight no greater than three, having the property that $H(a_0,\dots,a_d)=0$.

Sketch of the Proof. The coefficients of a rational function, being the value of the working variable z_ℓ of the SLP β (see the notation in Sec. 1), can be represented as rational functions of the parameters which are introduced in β as constants from F (i.e., each constant from β, newly introduced into F, is reckoned a parameter). Although it is not possible to "explicitly write out" these rational functions, by induction on ℓ it is not difficult to estimate explicitly in terms of ℓ (or in the final analysis, in terms of u, v_1, v_2) the degree and the weight of these rational functions. Hence it follows (here we make implicit use of the theorem on the avoidance of division in SLP evaluating polynomials [54]; in a weakened form we shall be dealing with it in Sec. 7) that the coefficient vector of polynomial q is the value of some vector of polynomials $(P_0, \ldots, P_d)$ with integer coefficients and with degrees and weights a priori bounded from above (in terms of u, v_1, v_2). Then the Dirichlet–Siegel lemma (see [55], for example) yields an upper bound on the degree of the nontrivial form H of weight three with integer coefficients, such that $H(P_0, \ldots, P_d) \equiv 0$ (direct computation yields the bound for $\deg H$ indicated in the theorem).

As a corollary of Theorem 3.1 we get that if the coefficients of a polynomial q of degree d do not satisfy the equating to zero of any form of degree $\leq h$ with integer coefficients and weight no greater than three, then the polynomial q cannot be evaluated by a SLP with parameters u, v_1, v_2. We present some applications of the indicated arguments and of arguments close to them:

$$C_m\Big(\sum_{0\leq k\leq d} 2^{2^{kd^3}} x^k\Big) > \sqrt{d} - 3 \qquad ([55]);$$

$$C_{\chi/}\Big(\sum_{1\leq k\leq d} \exp(2\pi i/2^{kd^2})\, x^k\Big) > \frac{d}{2} - 1 \qquad ([51]);$$

$$C_+\Big(\sum_{1\leq k\leq d} \exp(2\pi i/2^{kd^2})\, x^k\Big) \geq d - 2 \qquad ([51])$$

(compare with Theorems 2.2 and 2.4).

As already mentioned, the most powerful method for establishing lower complexity bounds on polynomial evaluation was proposed in [36], and we pass on to its exposition right away. As a preliminary we present a certain digest of facts from algebraic geometry (all of which can be found, say, in [15]) needed for this section and the text.

If X is an irreducible algebraic variety (over some algebraically closed field F), $X \subset \mathbb{P}^k$, where $\mathbb{P}^k$ is a k-dimensional projective space, then almost all (in the Zariski topology sense) linear spaces $\pi \subset \mathbb{P}^k$ of dimension $\dim \pi = k - \dim X$ have in the intersection $X \cap \pi$ one and the same finite number of points, called the degree $\deg X$ of variety X. We remark in passing that if $X \cap \pi$ consists of a finite number s of points, then $s \leq \deg X$. Every variety Y can be decomposed into irreducible components: $Y = X_1 \cup \ldots \cup X_t$; then: $\deg Y = \sum \deg X_i$. The concept of the degree $\deg X$ is invariant, i.e., is independent of the imbedding of X into the projective space. We note the subsequently useful Bezout inequality

$$\deg(Y \cap Z) \leq \deg Y \cdot \deg Z. \qquad (2)$$

Following [36], we introduce one more complexity (in the notation of Sec. 1), where $H \subset F$ is some infinite subfield of field F. We set $\lambda_H(+) = \lambda_H(x\gamma) = 0$ for $\gamma \in H$ and $\lambda_H(x\gamma) = \lambda_H(x) = \lambda_H(/) = 1$ for $\gamma \in F \setminus H$. In other words, free of charge we admit multiplications by elements of field H (see below for a typical example of application, when $F = \mathbb{C}$, $H = \mathbb{Q}$).

Let $v, d_1, \ldots, d_s$ be positive integers. Further, let C' be one of the complexity measures C_+, C_H, C_m (see Sec. 2 for the notation). We set $m = 2v$ when considering C_+ or C_H and $m = v^2 + 2v$ when considering C_m. Then we have

THEOREM 3.2 [50, 51]. For every $v, d_1, \ldots, d_s$ there exist polynomials $Q_{k,j} \in H[y_1, \ldots, y_m]$, where $d_k > j \geq 0$, $1 \leq k \leq s$, $\deg Q_{k,j} \leq 3jv + 2$, such that if $g_1, \ldots, g_s \in F[x]$, $\deg g_k \leq d_k$ $(1 \leq k \leq s)$, and $C'(g_1, \ldots, g_s) \leq v$, then for all $\xi \in A$, except for a finite number, we can find $\eta_1, \ldots, \eta_m \in F$ such that

$$g_k = \sum_{0 \leq j \leq d_k} Q_{k,j}(\eta_1, \ldots, \eta_m)(x - \xi)^j \quad (1 \leq k \leq s). \tag{3}$$

The idea of the proof is similar to that of the proof of Theorem 3.1.

Following [36], we consider a morphism Ψ of affine spaces $F^m \xrightarrow{\Psi} F^{d_1} \times \ldots \times F^{d_s} = F^d$ $(d = d_1 + \ldots + d_s)$, defined by the vector of polynomials $(Q_{1,1}, \ldots, Q_{1,d_1}, \ldots, Q_{s,1}, \ldots, Q_{s,d_s})$ from Theorem 3.2. We denote $W = \overline{\operatorname{Im}\Psi}$ to be the closure of the image of Ψ (in the Zariski topology). The variety $\operatorname{Im}\Psi$, and by the same token also W, are defined over field H ([15]). Below $\log$ denotes the binary logarithm, $|M|$ is the cardinality of set M.

LEMMA 3.3 [36]. $\frac{1}{6} \frac{\log \deg W}{\log d} \leq m$.

Proof. Let $\theta_1, \ldots, \theta_{\dim W}$ be hyperplanes such that $|\operatorname{Im}\Psi \cap \theta_1 \cap \ldots \cap \theta_{\dim W}| = \deg W$ (from the definition of degree). Then $\operatorname{codim} \Psi^{-1}(\theta_i) = 1$ and $\deg \Psi^{-1}(\theta_i) \leq 3dv + 2$ (the latter from Theorem 3.2). Let t be the number of components in the variety $U = \Psi^{-1}(\theta_1) \cap \ldots \cap \Psi^{-1}(\theta_{\dim W})$. Then by the Bézout inequality (2) we obtain $t \leq \deg U \leq \prod_{1 \leq i \leq \dim W} \deg \Psi^{-1}(\theta_i) \leq (3dv+2)^{\dim W}$. Since $\Psi(U) = W \cap \theta_1 \cap \ldots \cap \theta_{\dim W}$, we have $\deg W \leq t$ and, finally, $\deg W \leq (3dv+2)^{\dim W}$. This completes the lemma's proof since $\dim W \leq m$, and we can take it that $v \leq d$.

We denote the combined complexity $J = \min\{C_+, C_H, C_m^2\}$. Let $g_k = \sum_{0 \leq j \leq d_k} g_{k,j} x^j$ $(1 \leq k \leq s)$. We consider the point $x = (g_{1,1}, \ldots, g_{1,d_1}, \ldots, g_{s,d_s}) \in F^d$ and we let B be the closure of this point over field H in F^d (i.e., B is the smallest closed variety, defined over H, containing x: if F is algebraic over H, then B consists of a finite number of points). Let $\mathfrak{D}$ be a variety defined as the set of general coefficients of certain polynomials $P_1, \ldots, P_\tau$, where $\deg P_i \leq l$ $(1 \leq i \leq \tau)$ for some l, and let $B \underset{\text{comp}}{\subset} \mathfrak{D}$ (the latter relation signifies that all components of variety B are as well components of variety $\mathfrak{D}$).

THEOREM 3.4 [36]. $J(g_1, \ldots, g_s) \geq \frac{1}{24} \frac{\log \deg B}{\log(dl)}$.

Proof. We use Theorem 3.2 and the notation adopted in it. We assume that in equalities (3) we can set $\xi = 0$ (if we cannot, then we take an arbitrary admissible value $\xi = \xi_0$ and we reduce everything to the case being examined by making the change of variable $x' = x - \xi_0$). Then $x \in \operatorname{Im}\Psi \subset W$, and since W is closed and bounded over H, we have $B \subset W$, hence $B \underset{\text{comp}}{\subset} W \cap \mathfrak{D}$.

We can find a nontrivial linear combination $p^{(1)}=\sum_{1\leqslant i\leqslant r}\alpha_i^{(1)}p_i$ $(\alpha_i^{(1)}\in F)$ such that the variety of its zeros (we denote it $\{p^{(1)}=0\}$) does not contain (and by the same token, properly intersects (see [15]) any component of variety W which is not contained in $\mathfrak{D}$. Analogously taking $\dim W$ steps, we find the linear combinations $p^{(j)}=\sum_{1\leqslant i\leqslant r}\alpha_i^{(j)}p_i$ $(1\leqslant j\leqslant \dim W)$ such that $\mathfrak{D}\cap W\underset{\text{comp}}{\subset}\{p_1=\ldots=p_{\dim W}=0\}\cap \dim W=E$. Hence, by the Bézout inequality (2) we have

$$\deg B\leqslant \deg(\mathfrak{D}\cap W)\leqslant \deg E\leqslant \deg W\cdot l^{\dim W}\leqslant \deg W\cdot l^{m}.$$

Using the last inequality and Lemma 3.3, we obtain $m\geqslant(1/6)\log\deg B/\log(dl)$, whence follows the theorem.

Let us mention some applications of the theorem which cannot be obtained on the basis of Theorem 3.1 and of the method of [50, 51]; in the corollary below $F=\bar{\mathbb{Q}}$, $H=\bar{\mathbb{Q}}$.

COROLLARY 3.5 [36]. $\mathcal{J}(\sum_{1\leqslant j\leqslant d}\exp(2\pi i/\kappa_j)x^j)\geqslant \log \mathrm{LCM}(\kappa_1,\ldots,\kappa_d)/\log(d\cdot\max\{\kappa_1,\ldots,\kappa_d\})$, where κ_j are positive integers $(1\leqslant j\leqslant d)$, LCM is the least common multiple.

In the hypotheses of Theorem 3.4 we assume $\mathfrak{D}$ to be the variety of common zeros of the polynomials $\{y_1^{\kappa_1}-1=0,\ldots,y_d^{\kappa_d}-1=0\}$, by the same token $l=\max\{\kappa_1,\ldots,\kappa_d\}$. For example $\mathcal{J}(\sum_{1\leqslant j\leqslant d}\exp(2\pi i/j)x^j)\geqslant d/\log d$ [36] and $\mathcal{J}(\sum_{1\leqslant j\leqslant d}\exp(2\pi i/p_j)x^j)\geqslant d$ [36], where p_j is the j-th prime.

Using their own method, Heintz and Sieveking [36] proposed a method of estimating from below the complexity $C_H(\{\sum_{1\leqslant j\leqslant d}\alpha_{ij}x_j\}_{1\leqslant i\leqslant d})$ for a $d\times d$-family of linear forms. Analogously to the above, let B be the closure over field H of the point $x=(\alpha_{1,1},\ldots,\alpha_{d,d})\in F^{d^2}$ and let $\mathfrak{D}$ be as above. Then we have

Statement 3.6 [36]. $C_H(\{\sum_{1\leqslant j\leqslant d}\alpha_{ij}x_j\})\geqslant\dfrac{\log\deg B}{\log(dl)}$

Sketch of the Proof. Using [54, 64] we can take it (by increasing the complexity C_H by no more than twice) that the values of all the working variables of the SLP evaluating the family of linear forms are linear functions. Hence we conclude (arguing as in the proof of Theorem 3.1) that we can find polynomials $Q_{1,1},\ldots,Q_{d,d}\in H[y_1,\ldots,y_{2v}]$; $\deg Q_{ij}\leqslant 2v$ $(1\leqslant i,j\leqslant d)$, such that $x\in\mathrm{Im}\,\psi$, where $\psi=(Q_{1,1},\ldots,Q_{d,d})\colon F^{2v}\to F^{d^2}$. Let $W=\overline{\mathrm{Im}\,\psi}$, then, arguing analogously to the proof of Lemma 3.3, we obtain $\deg W\leqslant(2v)^{2v}$. From then on we follow the proof of Theorem 3.4.

Thus, we have constructed polynomials with coefficients from $\bar{\mathbb{Q}}$, relatively "simple" in structure, whose combined complexity $\mathcal{J}$ is close to the maximum possible $(O(d))$. This partially answers the question posed at the beginning of this section.

We recall as well that we have proved (ineffectively) the existence of difficultly computable polynomials with coefficients from set $\{0,1\}$ (see [50], for example). More precisely, we have proved the existence of d-degree polynomials with coefficients from set $\{0,1\}$ with a) a total complexity (see Sec. 1) of the order of $d/\log d$ (this estimate is exact, as follows from the method in [46]); b) a multiplicative complexity not less than $\sqrt{d/\log d}$ with respect to order (this estimate is close to exact, as follows from Theorem 2.4); c) an additive complexity not less than $\sqrt{d}/\log d$ with respect to order. The problem

of obtaining more exact bounds for the additive complexity of d-degree polynomials with rational coefficients remains unsolved. For it we know only a lower bound (i.e., examples with the lower bound indicated have been constructed) and an upper bound, respectively $\sqrt{d}$ and d with respect to order.

4. Degree Method and Its Generalization (Case of an Infinite Ground Field)

On the basis of the methods set forth in the preceding section, it has not been successful to prove lower bounds for the complexity of natural polynomials or of families of polynomials, since the basic instrument in the arguments is the establishment of some upper bound on the degree of extension (over a primitive field) of the field generated by the coefficients of the polynomial being evaluated, in terms of its complexity. In explicit form this exists in Strassen's method (Theorem 3.1) and, in a more veiled form (estimate of the degree of set B), in the Heintz–Sieveking method (Lemma 3.3 and Theorem 3.4).

In the present section we shall expound on methods based on the use of the concept and properties of the degree of a variety (see Sec. 3 above or [15]), yielding nonlinear (relative to the number of variables) lower bounds on the multiplicative complexity for certain natural families of polynomials of several variables (see the already-classic old paper [23]) and for individual polynomials (see [25, 50]).

Thus, in the terminology of Sec. 1, F is an algebraically closed field; $P=\{+,\times,/\} \cup \{x\gamma\}_{\gamma\in F}$; $\lambda=\lambda_m$. It is required to estimate the multiplicative complexity $C_m(g_1,\dots,g_k)$ of a family of rational functions of pairwise-commuting input variables $x_1,\dots,x_n$. The functions $g_1,\dots,g_k$ prescribe a rational mapping $F^n \xrightarrow{G=(g_1,\dots,g_k)} F^k$. We consider its graph $Graph(G)\subset F^{n+k}$ and by $W=\overline{Graph(G)}\subset P^{n+k}$ we denote its projective closure. We note that $Graph(G)$ is an open subset in the irreducible closed variety W; therefore, $\deg W = \deg Graph(G)$.

THEOREM 4.1 [23]. $C_m(g_1,\dots,g_k)\geq \log_2 \deg W$.

This theorem is rather widely known and, therefore, with regard to its proof we merely remark that it is carried out by induction on $C_m(g_1,\dots,g_k)$ and uses the Bézout inequality (2).

We mention certain applications of Strassen's theorem

$$C_m\Big(\sum_{1\leq i\leq d} a_i x_1^i,\dots,\sum_{1\leq i\leq d} a_i x_d^i\Big) \asymp d\log d$$

for every d-degree polynomial (i.e., $a_d\neq 0$) over F (the evaluation of a concrete polynomial of precisely degree d at d points, i.e., here the set of input variables (see Sec. 1) is $\{x_1,\dots,x_d\}$). Let $\sigma_i=\sum_{1\leq j_1<\dots<j_i\leq d} x_{j_1}\cdots x_{j_i}$ be an elementary i-degree symmetric function; then $C_m(\sigma_1,\dots,\sigma_d)\asymp d\log d$. Further, the interplation problem for a d-degree polynomial, i.e., the recovery of its coefficients from the values at $(d+1)$ distinct points, also has a multiplicative complexity $d\log d$ with respect to order. We remark that all bounds from the applications mentioned are true as well for an arbitrary infinite ground field F, since the SLP evaluating a family of polynomials over an infinite field evaluates this family over any extension of it.

Unfortunately, Theorem 4.1 does not yield a nontrivial estimate for the multiplicative complexity of an individual polynomial, since $\deg W \leq \prod_{1\leq i\leq k} \deg q_i$, where $\deg(g_1/g_2)=\max\{\deg g_1,(\deg g_2)+1\}$. This deficiency was first removed by Schnorr [50]; we proceed to present his method (as before we take field F to be algebraically closed).

Let $p=a_0(x_1,\ldots,x_n)+a_1(x_1,\ldots,x_n)y+\ldots+a_d(x_1,\ldots,x_n)y^d\in F[y,x_1,\ldots,x_n]$ and $C_m(p)=v$. We consider a SLP β evaluating p, such that $C_m(\beta)=v$. Informally speaking, we would want to transform the SLP β into some SLP $\tilde{\beta}$ evaluating the coefficients of polynomial p, i.e., the polynomials $a_0,\ldots,a_d\in F[x_1,\ldots,x_n]$. But if there is division in β, then this would make it difficult since the natural path to such a transformation is to evaluate all coefficients of powers (not exceeding d) of the variable y for all values (which can be treated as power series in y) of the working variables z_ℓ of the SLP β (see Sec. 1), which is impossible if it is required, for example, to decompose into series in y with a zero free term. In principle this defect can be eliminated by examining power series in the new variable $(y-\eta)$ (instead of y) for some $\eta\in F$ (even for almost all $\eta\in F$). Therefore, we can introduce η into the SLP as a new input variable; i.e., the rational function $f_\ell\in F(y,x_1,\ldots,x_n)$, being the value of some working variable z_{m_ℓ} of the SLP β (by m_ℓ we have denoted the number of the instruction in β at which the ℓ-binary multiplication or division is implemented; see item 4 of the definition in Sec. 1), is written as $f_\ell=\sum_{i\geq 0} b_{i,\ell}(\eta,x_1,\ldots,x_n)(y-\eta)^i$, where $b_{i,\ell}$ are rational functions.

Using no more than v operations $\times$ and $/$, we compute all $\{b_{0,\ell}\}_{1\leq\ell\leq v}$ by induction on ℓ, i.e., the free terms in the power series in the variable $(y-\eta)$, corresponding to the functions f_ℓ. Next, by induction on ℓ we can show that every coefficient $b_{i,\ell}$ can be represented as some polynomial $Q_{i,\ell}$ of degree no higher than $2i\ell$ (cf. Theorem 3.2) of the parameters $\eta,x_1,\ldots,x_n$ and $\{b_{0,\ell}\}_{1\leq\ell\leq v}$. We point out that actually we do not evaluate the coefficients $b_{i,\ell}$ (to counterbalance the informal exposition of the idea of Schnorr's method; see above), since this is rather labor-consuming, but we construct a certain representation suitable for them.

Let $p=\tilde{a}_0(\eta,x_1,\ldots,x_n)+\tilde{a}_1(\eta,x_1,\ldots,x_n)(y-\eta)+\ldots+\tilde{a}_d(\eta,x_1,\ldots,x_n)(y-\eta)^d$, we consider the rational mapping $F^{n+1}\xrightarrow{A=(\tilde{a}_0,\ldots,\tilde{a}_d)}F^{d+1}$ which can be decomposed into two rational mappings.

$$F^{n+1}\xrightarrow{\varphi=(x_1,\ldots,x_n,\eta,b_{0,1},\ldots,b_{0,v})}F^{n+1+v}\xrightarrow{\psi=(\tilde{a}_0,\ldots,\tilde{a}_d)}F^{d+1}.$$

According to Theorem 4.1 and what we have proved above, $\deg\mathrm{Graph}(\varphi)\leq 2^v$. Further, since $\tilde{a}_i=Q_i(\{\eta,\{x_i\},\{b_{0,\ell}\})$, where $Q_i=\sum_{1\leq j\leq v}\alpha_{ij}Q_{i,j}$ is some linear $(\alpha_{ij}\in F)$ combination of the above-mentioned polynomials, we have $\deg Q_i\leq 2vi$, whence $\deg\mathrm{Graph}(\psi)\leq(2vd)^d$. It is easy to verify that $\deg\mathrm{Graph}(\psi\circ\varphi)\leq\deg\mathrm{Graph}(\psi)\cdot\deg\mathrm{Graph}(\varphi)$, consequently, $\deg\mathrm{Graph}(A)\leq 2^v(2vd)^d$. On the other hand, $\mathrm{Graph}(a_0,\ldots,a_d)=\mathrm{Graph}(\tilde{a}_0,\ldots,\tilde{a}_d)\cap\pi\subset F^{n+d+2}$, where π is the hyperplane with equation $\eta=0$; therefore, according to the Bézout inequality (2), $\deg\mathrm{Graph}(a_0,\ldots,a_d)\leq\deg\mathrm{Graph}(\tilde{a}_0,\ldots,\tilde{a}_d)\leq 2^v(2vd)^d$. Thus, we have

THEOREM 4.2 [50]. Let $p=a_0(x_1,\ldots,x_n)+a_1(x_1,\ldots,x_n)y+\ldots+a_d(x_1,\ldots,x_n)y^d$. Then $C_m(p)>v$ for v such that $\deg\mathrm{Graph}(a_0,\ldots,a_d)>2^v(2vd)^d$.

Some applications of the theorem [50]:

$$C_m\Big(\sum_{0\le i\le d} x_i^{\kappa} y^i\Big) \ge d\log\kappa, \qquad \text{if } d^4 < \kappa;$$

$$C_m\Big(\sum_{0\le i\le d} (x_1+\dots+x_i)^{\kappa} y^i\Big) \ge d\log\kappa, \qquad \text{if } d^4 < \kappa.$$

We remark that in the applications mentioned, as above in an analogous situation, when we discuss corollaries of Theorem 4.1 we can take it that $\mathbb{F}$ is an arbitrary infinite field.

A more elegant method, permitting in addition the obtaining of nonlinear lower bounds for the complexity of individual polynomials, was suggested by Baur and Strassen [25] and was based on the following estimate for the complexity of evaluation of the rational function $f\in\mathbb{F}(x_1,\dots,x_n)$ and all its first partial derivatives (here $\mathbb{F}$ is any field).

THEOREM 4.3 [25]. 1) $C_m\Big(f, \frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\Big) \le 3C_m(f)$;

2) $C_t\Big(f, \frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\Big) \le 5C_t(f)$. (See Sec. 1.)

We prove only the item 1). We consider a SLP β evaluating f with complexity $C_m(\beta)=C_m(f)=r$. Let $g_1,\dots,g_r$ be the values of the working variables in the SLP β, in the instructions containing binary multiplications or divisions (see item 4 of the definition in Sec. 1). Then for every i $g_i = u_i \odot v_i$ ($\odot = \times$ or $\odot = /$) and

$$u_i = \sum_{1\le j\le i-1} \beta_{ij} g_j + p_i; \quad v_i = \sum_{1\le j\le i-1} \gamma_{ij} g_j + q_i;$$
$$f = \sum_{1\le j\le r} \alpha_j g_j + m,$$

where $\alpha_i,\beta_{ij},\gamma_{ij}\in\mathbb{F}$; $\max\{\deg p_i, \deg q_i, \deg m\} \le 1$.

LEMMA 4.4 [25]. Let $0\ne y_i\in\mathbb{F}$ $(1\le i\le s)$; $\alpha_{ij}\in\mathbb{F}$ $(1\le j<i\le s)$; $w_1,\dots,w_s$ are variables. We define the h_i $(1\le i\le s)$ by induction on i: $h_1 = y_1 w_1,\dots, h_i = y_i\Big(\sum_{1\le j\le i-1}\alpha_{ij}h_j + w_i\Big),\dots$. We denote $h_s = \sum_{1\le\sigma\le s} d_\sigma w_\sigma$, $d_\sigma\in\mathbb{F}$. Then

$$d_s = y_s;\ d_j = \Big(\sum_{j+1\le\sigma\le s} d_\sigma \alpha_{\sigma j}\Big) y_j \quad \text{for} \quad 1\le j<s.$$

Proof of the Lemma. We denote $h_i = \sum_{1\le\sigma\le s} d_{i\sigma} w_\sigma$. We consider the lower-triangular matrices

$$\mathbb{D} = \begin{pmatrix} d_{11} & & 0 \\ \vdots & \ddots & \\ d_{s1} & \dots & d_{ss} \end{pmatrix},\quad A = \begin{pmatrix} 0 & & 0 \\ \alpha_{21} & \ddots & \\ \alpha_{s1} & \dots & \alpha_{s,s-1}\ 0 \end{pmatrix},\quad Y = \begin{pmatrix} y_1 & & 0 \\ & \ddots & \\ 0 & & y_s \end{pmatrix}.$$

Then the lemma's hypothesis is equivalent to the equality $\mathbb{D} = Y(A\mathbb{D}+E)$, where E is the unit matrix. Having multiplied this equality from the left by the matrix $\mathbb{D}Y^{-1}$, and from the right by $\mathbb{D}^{-1}Y$, we obtain $\mathbb{D} = (\mathbb{D}A+E)Y$, whence the lemma follows.

We return to the theorem's proof. We set $s = 3r+1$;

$$\alpha_{3i-2,l} = \begin{cases} \beta_{ij}, & \text{if } l=3j \\ 0, & \text{otherwise} \end{cases};\quad \alpha_{3i-1,l} = \begin{cases} \gamma_{ij}, & \text{if } l=3j \\ 0, & \text{otherwise} \end{cases};$$

$$\alpha_{3i,l}=\begin{cases}1 \text{ for } l=3i-2 \text{ or } l=3i-1\\ 0, \text{ otherwise}\end{cases} \quad \text{for } 1\le l<3i\le s \text{ and}$$

$$\alpha_{s,l}=\begin{cases}a_j, \text{ if } l=3j\\ 0, \text{ otherwise}\end{cases}$$

Further, if $g_i=u_i\cdot v_i$, then we set $y_{3i-2}=v_i, y_{3i-1}=u_i, y_{3i}=1$. However, if $g_i=u_i/v_i$, then $y_{3i-2}=1, y_{3i-1}=-u_i/v_i, y_{3i}=1/v_i$. Finally, we set

$$\xi_{3i-2,\nu}=\frac{\partial p_i}{\partial x_\nu},$$

$$\xi_{3i-1,\nu}=\frac{\partial q_i}{\partial x_\nu},\ \xi_{3i,\nu}=0\ (1\le i\le r);\ \xi_{s,\nu}=\frac{\partial m}{\partial x_\nu}.$$

Then by induction on i it is easily verified that if $h_1,\dots,h_s$ have been defined as in Lemma 4.4 for the indicated parameters α_{ij}, y_j, then $\frac{\partial g_i}{\partial x_\nu}=h_{3i}(\xi_{1,\nu},\dots,\xi_{s,\nu})$. Hence we obtain $\frac{\partial f}{\partial x_\nu}=h_s(\xi_{1,\nu},\dots,\xi_{s,\nu})=\sum_{1\le\sigma\le s} d_\sigma \xi_{\sigma,\nu}$. Therefore, $C_m\left(\frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\right)\le C_m(d_1,\dots,d_s)$, since $\xi_{\sigma,\nu}\in F$ for all σ,ν. By Lemma 4.4 the family $\{d_1,\dots,d_s\}$ is evaluated (if $g_1,\dots,g_r$ have already been evaluated) with the use of $(s-1)$ binary multiplications by $y_{s-1},\dots,y_1$ in succession. Since among the $\{y_1,\dots,y_{s-1}\}$ at least r equal unity, to evaluate $\frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}$ it is sufficient to use no more than $(s-1)-r=2r$ binary multiplications and divisions, which proves the theorem.

We mention some applications of Theorem 4.3.

COROLLARY 4.4 [25]. 1) $\frac{1}{3}n\log(m-1)\le C_m\left(\sum_{1\le i\le n} x_i^m\right)\le 2n\log m$;

2) $\frac{1}{3}\max\{q,n-q+1\}\log\min\{q-1,n-q\}\le C_m(\sigma_q)\le n\log\min\{q,n-q\}+2n$,

where $\sigma_1,\dots,\sigma_n$ are elementary symmetric functions of n variables (cf. the applications of Theorem 4.1);

3) $\frac{1}{3}n\log n\le C_m\left(\prod_{i,j}(x_i-y_j)\right)\le n(9\log n+1)$;

4) $\frac{1}{6}n\log n-\frac{2}{3}n\le C_m\left(\prod_{i\ne j}(x_i-x_j)\right)=O(n\log n)$;

5) let the matrix $(b_{ij})=(a_{ij})^{-1}$ $(1\le i,j\le n)$; then $C_m(\{b_{ij}\})\le 3C_m(\det(a_{ij}))+n^2$.

The proof of the lower bounds in items 1)-4) is carried out by applying Theorem 4.1 to the collection of partial derivatives of the functions being computed. The proof of item 5) relies on the representation $b_{l,k}=A_{k,l}/\det(a_{ij})$, where A_{ij} is the (i,j)-minor. On the other hand, by Cramer's rule, $\frac{\partial\det(a_{ij})}{\partial a_{kl}}=\pm A_{kl}$. Thus from item 5) and previously known results we obtain the coincidence (to within a multiplicative constant) of the complexities of matrix multiplication, matrix inversion, and determinant evaluation (also see Solodovnikov's survey in this issue).

We heed the fact that Theorem 4.3 cannot be generalized directly to the computation of the second partial derivatives (and by the same token, to families of several variables — $\{f_1,\dots,f_k\}$ — in contrast to one function $\{f\}$). As a counterexample we consider the polynomials $f=x_1\cdots x_n$. Then $\frac{\partial^2 f}{\partial x_i\partial x_j}=\frac{f}{x_ix_j}$ for $i\ne j$ and $C_m\left(\left\{\frac{f}{x_ix_j}\right\}\right)\ge\dim\left(\left\{\frac{f}{x_ix_j}\right\}_{i>j}\right)=\frac{n(n-1)}{2}$.

In concluding the present section we cite one application, due to Strassen, of the degree method for computing the Euclidean representation (or the continuous fraction) of a rational function by a computing model somwhat different from a SLP [57]. If $A_1, A_2 \in F[x]$, $\deg A_1 = n \geq \deg A_2 = m \geq 0$, then we apply the Euclid algorithm to A_1 / A_2 and obtain here the sequence of equalities

$$A_1 = Q_1 A_2 + A_3,\ A_2 = Q_2 A_3 + A_4, \ldots, A_{t-1} = Q_{t-1} A_t.$$

The vector of polynomials $(Q_1, Q_2, \ldots, Q_{t-1}, A_t)$ is called a Euclidean representation of the fraction A_1/A_2. The vector of degrees $(n_1, \ldots, n_t) = (\deg Q_1, \ldots, \deg Q_{t-1}, \deg A_t)$ is called the format of the fraction A_1/A_2 (or of the pair (A_1, A_2)). Obviously, $m = \sum_{2 \leq i \leq t} n_i$, $n = \sum_{1 \leq i \leq t} n_i$. By $\mathcal{D}(n_1, \ldots, n_t)$ we denote the set of pairs (A_1, A_2) having the format $(n_1, \ldots, n_t)$.

It is clear that a SLP is an unsuitable model for computing a Euclidean representation since different fractions can have different formats even for one and the same values of n and m, i.e., a different form of response. Therefore, the following computing model was introduced in [57], adequate for the given problem and called the branched tree program (BTP).* The BTP contains a tree T directed from the root to the leaves. Any vertex of tree T has one or two sons. At every vertex having two sons (it is called a branching vertex) there stands an arbitrary polynomial; at every vertex having one son (it is called an evaluating vertex) there stands some base operation (from $\mathfrak{P}$; see Sec. 1). The arguments of both the polynomial mentioned and the base operation are the results of some evaluating vertices located on a single branch from the root to the vertex being examined. A response consisting of the results of the evaluating vertices located above a leaf is delivered at the leaf.

The functioning of a BTP is unique. An input is fed in at the root of tree T and the computation takes place along some uniquely determined branch: an appropriate base operation is computed at every evaluating vertex; after the branching vertex at which a polynomial p stands, the evaluation proceeds along one of the branches depending on whether or not the value of polynomial p equals zero.

If a BTP with tree T computes a Euclidean representation, then every two inputs on which the computation takes place along one and the same branch of tree T have a like format, and by the same token, every branch (or an appropriate leaf) can have a format ascribed to it. If some weight $\lambda_\odot$ has been specified on the base operations (see Sec. 1), then the weight of a branch is the sum of the weights of the base operations at the vertices along this branch. We define the complexity of the BTP as a function of the format: $C_\odot(n_1, \ldots, n_t)$ is set equal to the largest of the weights of the braches with format $(n_1, \ldots, n_t)$. The normalized entropy [3] is defined as $-\frac{1}{n}\sum_{1 \leq i \leq t} n_i \log\left(\frac{n_i}{n}\right) = H(n_1, \ldots, n_t)$.

THEOREM 4.6 [57]. 1) (Knuth and Schönhage) A BTP can be constructed to compute the Euclidean representation with the bound

*Translator's Note: The literal phase used in Russian for a straight-line program is "unbranched program." At the time of writing I did not have access to Strassen's paper [57] and therefore I do not know what name he has given to this new program. I have made here a literal translation of the Russian phase. I would appreciate it greatly if someone who knows what Strassen used lets me know.

$$C_m(n_1,\dots,n_t)\leqslant 30n(H(n_1,\dots,n_t)+6{,}5).$$

2) Every BTP, computing a Euclidean representation over an algebraically closed ground field F, has the multiplicative complexity $C_m(n_1,\dots,n_t)\geqslant n(H(n_1,\dots,n_t)-2)$, i.e., for every $(n_1,\dots,n_t)$ there exists a set $\mathcal{U}$, open in $\mathcal{D}(n_1,\dots,n_t)$, on each element of which the BTP has a multiplicative complexity of not less than the magnitude indicated.

We note (see [57]) that the multiplicative complexity of the evaluation of the product of t polynomials in one variable (the same one for all) of degrees $n_1,\dots,n_t$, respectively, over an infinite ground field F is of the order of $nH(n_1,\dots,n_t)$. The proof of item 2) of Theorem 4.6 and of the lower bound in the last remark relies on Theorem 4.1.

5. Degree Method (Case of a Finite Ground Field)

The methods presented in the preceding section work only in the case of an infinite ground field, since essentially we use the fact that if some SLP β evaluates a polynomial (or a family of polynomials) over an infinite field, then β evaluates this same polynomial (or family) also over any extension of it, in particular, over its algebraic closure, for which we now apply an algebraic-geometric technique connected with the polynomial's degree. For the case of a finite ground field F, Strassen [56] suggested another method which nevertheless also uses Theorem 4.1 (see Sec. 4). The present section is devoted to its presentation.

Thus, let F be a finite field, $P=\{+,\times,/\}\cup\{x\gamma\}_{\gamma\in F}$; $\lambda=\lambda_m$. The problem consists in estimating $v=C_m(g_1,\dots,g_K)$ for $g_1,\dots,g_K\in F[x_1,\dots,x_n]$, where $\{x_1,\dots,x_n\}$ are pairwise-commuting input variables (see Sec. 1). Suppose that a SLP β evaluates $\{g_1,\dots,g_K\}$ and that $C_m(\beta)=v$. We denote $S=\mathrm{Graph}(F^n\xrightarrow{G=(g_1,\dots,g_K)}F^K)\subset F^{n+K}$. We shall treat the SLP β as a SLP $\bar\beta$ over the algebraic closure $\bar F$. The SLP $\bar\beta$ then evaluates certain polynomials $\bar g_1,\dots,\bar g_K\in F[x_1,\dots,x_n]$, such that the restriction $\bar g_i|_{F^n}=g_i$ $(1\leqslant i\leqslant K)$, and $\bar g_i$ possibly does not coincide with g_i on the whole $\bar F^n$ (this feature distinguishes the case of a finite ground field from that of an infinite one). Obviously, $C_m(\bar g_1,\dots,\bar g_K)\leqslant v$. We now consider the irreducible mapping $W=\mathrm{Graph}(\bar F^n\xrightarrow{\bar G=(\bar g_1,\dots,\bar g_K)}\bar F^K)\subset\bar F^{n+K}$. The inclusion $S\subset W$ is fulfilled (we take it that $F^{n+K}\subset\bar F^{n+K}$ is a natural embedding). The idea of Strassen's method consists in finding effective sufficient conditions on a finite set S_1 of points, under whose fulfillment every irreducible mapping $W_1\supset S_1$ would have a sufficiently large degree (for a fixed dimension $\dim W_1$), and then applying Theorem 4.1.

We say (see [56]) that a finite subset $S_1\subset\bar F^N$ is a t-set (t is some positive integer) if for all $0\leqslant d\leqslant N$ and for every irreducible closed subset $W_1\subset\bar F^N$ there is fulfilled $\deg W_1\geqslant|S_1\cap W_1|/t^{\dim W_1}$. The next lemma is of independent interest, it seems, also for specialists in algebraic geometry.

LEMMA 5.1 [56]. Let $S_1\subset\bar F^N$, t be a positive integer, $l_1,\dots,l_q$ be linear forms on $\bar F^N$ such that:

a) for every $1\leqslant i\leqslant q$ and any $c_1,\dots,c_{i-1}\in\bar F$ the linear form l_i takes no more than t values on set

$$S_1\cap\{y\in\bar F^N: l_1(y)=c_1,\dots,l_{i-1}(y)=c_{i-1}\};$$

b) if $l_i(y)=l_i(u)$ for some $y,u\in S_1$ and for all $1\le i\le q$, then $y=u$.

Then S_1 is a t-set.

The lemma can be proved by induction on q.

THEOREM 5.2 [56]. Let $g_1,\dots,g_K\in F[x_1,\dots,x_n]$ and let the set $S_1=S=\mathrm{Graph}(g_1,\dots,g_K)\subset F^{n+K}\subset \bar{F}^{n+K}$ satisfy the hypotheses of Lemma 5.1. Then $C_m(g_1,\dots,g_K)\ge \log(|S|/t^n)$.

To prove the theorem it is enough to note that an irreducible closed n-dimensional mapping $\bar{W}=\overline{\mathrm{Graph}(G)}$ contains a t-set S; therefore, $\deg W\ge |S|/t^n$, and applying Theorem 4.1, we obtain

$$r\ge C_m(\bar{g}_1,\dots,\bar{g}_K)\ge \log\deg W\ge \log(|S|/t^n).$$

As an application of Theorem 5.2 (see [56]) we get that

$$C_m\Big(\sum_{1\le i\le n}a_ix_1^i,\dots,\sum_{1\le i\le n}a_ix_n^i\Big)\asymp O(n\log(\min\{n,|F|\})).$$

$(a_n\ne 0)$. For the problem of interpolating an n-th degree polynomial from values at $(n+1)$ points (the problem makes sense if $|F|>n$), its multiplicative complexity also equals $n\log n$ in order (we recall that we would have the same bound for these two problems in the case of an infinite field — see the applications of Theorem 4.1). The matter is different for elementary symmetric functions: in [17] it is shown that even the total complexity $C_t(\sigma_1,\dots,\sigma_n)$ is linear in n over a finite field F (cf. Sec. 4).

It is interesting to note that the reverse situation occurs in certain natural cases, i.e., the complexity of evaluation of a family of polynomials over a finite field can be greater than the complexity of evaluation of this family over an infinite field. For example, the multiplicative complexity of the multiplication of two n-th degree polynomials over an infinite field F equals $2n+1$ (see [31], for instance); in the case of a field F of two elements a lower bound of $3{,}52n$ was proved in [28] for the multiplicative complexity in this problem (the best known upper bound for it to-date is $n\cdot g(n)$, where g is some function growing more slowly than any fixed iteration of the logarithm; see [8, 9, 32, 33]).

6. Additive Complexity and Real Roots

In the preceding two sections we established lower bounds for the multiplicative complexity $C_m(g_1,\dots,g_K)$ of a family of polynomials in terms of a power of the graph $W=\mathrm{Graph}_{(\bar{F}^n\to\bar{F}^K)}\bar{G}=(\bar{g}_1,\dots,\bar{g}_K)$. Since $\deg W$ is not less than the number N_1 of discrete roots of the system $\bar{g}_1=\dots=\bar{g}_K=0$ over field $\bar{F}$, we have $C_m(g_1,\dots,g_K)\ge\log N_1$ (cf. Theorem 4.1).

In the present section, on the basis of Khovanskii's work in [21], we shall find a lower bound for the additive complexity $C_+(g_1,\dots,g_n)$ in terms of the number of roots of the system $g_1=\dots=g_n=0$. In this section, in the notation of Sec. 1, $F=\mathbb{R}$; $P=\{+,\times,/\}\cup\{x^y\}_{y\in\mathbb{R}}$; $\lambda=\lambda_+$ (see the beginning of Sec. 2); $g_1,\dots,g_n\in\mathbb{R}[x_1,\dots,x_n]$. Below, unless otherwise stipulated, all the polynomials are assumed real. The existence of the bound mentioned was assumed a long time ago and this assumption was based on the Descartes principle: the number of nonnegative roots of a polynomial in one variable does not exceed the number of its monomials. For one polynomial g in one variable a bound weaker than the one established below was obtained in [26] (it appears that the method of proof of the main theorem in this paper is of independent interest). By $\mathbb{R}^*$ we denote the set of nonzero real roots.

THEOREM 6.1 [21]. The system of equations $g_1=\ldots=g_n=0 (g_1,\ldots,g_n\in\mathbb{R}[x_1,\ldots,x_n])$ has no more than $2^{n}(n+2)^{K}2^{K(K+1)/2}$ discrete roots in $(\mathbb{R}^*)^n$, where K is the total number of monomials in all the polynomials $g_1,\ldots,g_n$.

COROLLARY 6.2. If the system $g_1=\ldots=g_n=0$ has N simple (i.e., of multiplicity one) discrete roots in $(\mathbb{R}^*)^n$, then $C_+(g_1,\ldots,g_n)\geqslant\frac{\sqrt{\log N}-2n}{3}$.

Proof of the Corollary. Let $y_1,\ldots,y_N$ be the simple roots mentioned of the system $g_1=\ldots=g_n=0$ (the roots from $(\mathbb{R}^*)^n$ will be called nontrivial). To derive the corollary from the theorem we make use of the well-known canonic form for the SLP (see [26], for example) containing no more than $v=C_+(g_1,\ldots,g_n)$ multiplications:

$$\begin{aligned}
&\vdots\\
&T_{l+1}=T_1^{i_1^{(l+1)}}\ldots T_l^{i_l^{(l+1)}}x_1^{u_1^{(l+1)}}\ldots x_n^{u_n^{(l+1)}}+T_1^{j_1^{(l+1)}}\ldots T_l^{j_l^{(l+1)}}x_1^{w_1^{(l+1)}}\ldots x_n^{w_n^{(l+1)}}\\
&\vdots\\
&G_1=T_1^{p_1^{(1)}}\ldots T_v^{p_v^{(1)}}x_1^{q_1^{(1)}}\ldots x_n^{q_n^{(1)}}\\
&\vdots\\
&G_n=T_1^{p_1^{(n)}}\ldots T_v^{p_v^{(n)}}x_1^{q_1^{(n)}}\ldots x_n^{q_n^{(n)}},
\end{aligned}\tag{4}$$

where the i,j,u,w,p,q with subscripts are integers; T_l is the SLP's working variable (see Sec. 1) in the instruction in which the l-th multiplication operation, by count, takes place; the value of the working variable G_i equals $g_i\,(1\leqslant l\leqslant v,\ 1\leqslant i\leqslant n)$.

Let us show that we can so modify system (4) by replacing $G_1,\ldots,G_n$ by nonzero real numbers $\varepsilon_1,\ldots,\varepsilon_n$ sufficiently small is modulus, respectively, that the modified system of $(v+n)$ equations in $(v+n)$ unknowns $x_1,\ldots,x_n,T_1,\ldots,T_v$ would have no fewer than N nontrivial roots. Since $y_1,\ldots,y_N$ are simple roots, by the implicit function theorem the mapping $\mathbb{R}^n\xrightarrow{G=(g_1,\ldots,g_n)}\mathbb{R}^n$ is bijective for each $1\leqslant i\leqslant N$ in some neighborhood $Y_i\ni y_i$, namely, having narrowed down the neighborhood Y_i, we can take it that the neighborhoods of zero $G(Y_i)=Q$ coincide and $Y_i\subset(\mathbb{R}^*)^n$ for all $1\leqslant i\leqslant N$. We consider the mapping $Y_i\xrightarrow{T_{l+1}^{(i)}=T_{l+1}}\mathbb{R}$ (here we identify the working variable T_{l+1} with its value). It is not identically zero (otherwise, the $(l+1)$-st instruction of the SLP is superfluous and can be deleted); therefore, the preimage of zero $(T_{l+1}^{(i)})^{-1}(0)=M_{i,l+1}\subset Y_i$ is a real algebraic variety of dimension less than n. We consider $M=\bigcup_i Q_i G(M_{i,l+1})$, viz., a subvariety of dimension less than n (since G/Y_i is a bijective morphism) of a neighborhood Q of zero in $\mathbb{R}^n$. Now as $(\varepsilon_1,\ldots,\varepsilon_n)$ we take an arbitrary point in Q outside M and the coordinate hyperplanes. By virtue of the choice of $(\varepsilon_1,\ldots,\varepsilon_n)$ the modified system has not less than N nontrivial roots (in neighborhoods $\{Y_i\}_{1\leqslant i\leqslant N}$ of the points $\{y_i\}_{1\leqslant i\leqslant N}$).

The modified system contains $K=(2n+3v)$ monomials. Having substituted this value of K into Theorem 6.1 and noted that $2^n(n+2)^K<2^{K(K+1)/2}$ in our case, we complete the corollary's proof.

As an application we consider the polynomial $P_d(x)=(x-1)\ldots(x-d)$ and the family of polynomials $\{P_d(x_1),\ldots,P_d(x_n)\}$ in the variables $x_1,\ldots,x_n$ for $d\geqslant 2^{3n}$; then $C_+(P_d(x_1),\ldots,P_d(x_n))\geqslant\sqrt{n\log d}$ (under the restrictions mentioned this bound is nonlinear in n).

Kushnirenko has conjectured (see [21]) that under the hypotheses of Theorem 6.1 a stronger upper bound is true for the number of nontrivial roots: to be precise, $2^{n}(\kappa_1-1)\dots(\kappa_n-1)$, where κ_i is the number of monomials in g_i. The conjecture remains unproved as yet for $n>1$. The validity of the conjecture would yield the bound $C_+(g_1,\dots,g_n)\geq \log N$, which would be an elegant analog of Strassen's Theorem 4.1.

By modifying the proof of Theorem 4.2 we can obtain a lower bound for the additive complexity for individual polynomials. Let $g=\sum_{1\leq i\leq n} g_i y^i$, where $g_1,\dots,g_n\in\mathbb{R}[x_1,\dots,x_n]$.

THEOREM 6.3. Let N be the number of simple nontrivial roots of the system of equations $g_1=\dots=g_n=0$. Then $C_+(g)\geq(\log N)^{1/2(n+2)}-n$.

Let a SLP β be such that $v=C_+(\beta)=C_+(g)$ and β evaluates g. We assume that the values of all working variables z_ℓ of the SLP β, which are rational functions from $\mathbb{R}(x_1,\dots,x_n,y)$, have been determined at a point $y_0=\eta\in\mathbb{R}$. Then we make the change of variable $y_1=y-\eta$. Each value of a working variable z_{a_ℓ}, where a_ℓ is the number of an instruction in the SLP β (see Sec. 1 and the proof of Corollary 3.2), containing the ℓ-th by count addition operation, will be treated as a power series in y_1, i.e., $T_\ell=\sum_{i\geq 0} b_i^{(\ell)} y_1^i$ (see (4)); in addition, we set $T_0=y=y_1+\eta$.

We restructure the SLP β into a SLP β_1, computing by recursion on ℓ the collection $\{b_i^{(\ell)}\}_{0\leq i\leq n}$ (in this the present proof differs from that of Theorem 4.2 wherein the collection of coefficients of the powers of y_1 were not actually computed). At first, as in the proof of Theorem 4.2, we construct a SLP containing v additions and evaluating $\{b_0^{(\ell)}\}_{1\leq\ell\leq v}$. Let (see (4) $T_{\ell+1}=T_{\ell+1,1}/T_{\ell+1,2}+T_{\ell+1,3}/T_{\ell+1,4}$, where $T_{\ell+1,j}=T_1^{\beta_{1,j}^{(\ell+1)}}\dots T_\ell^{\beta_{\ell,j}^{(\ell+1)}} x_1^{\gamma_{1,j}^{(\ell+1)}}\dots x_n^{\gamma_{n,j}^{(\ell+1)}}$, and $\beta_{p,j}^{(\ell+1)}$, $\gamma_{p,j}^{(\ell+1)}$ $(1\leq j\leq 4)$ are nonnegative integers. We denote $T_{\ell+1,j}=\sum_{i\geq 0} b_{i,j}^{(\ell+1)} y_1^i$. Then

$$b_{i,j}^{(\ell+1)}=\Big(\sum_{i_1+\dots+i_\ell=i} A_{i_1,\dots,i_\ell,j}\, b_{i_1}^{(1)}\dots b_{i_\ell}^{(\ell)}\Big) x_1^{\gamma_{1,j}^{(\ell+1)}}\dots x_n^{\gamma_{n,j}^{(\ell+1)}},$$

where $A_{i_1,\dots,i_\ell,j}$ is some positive integer. The number of summands in the last sum does not exceed $\binom{i+\ell-1}{i}\leq\binom{n+v}{v}$. The evaluation of $b_i^{(\ell+1)}$ in terms of $b_{i,j}^{(\ell+1)}$ and $b_0^{(\ell+1)}$ $(1\leq j\leq 4)$ requires no more than n^2 additions in succession. At the end of the SLP β_1 we return to the evaluation of $g_1,\dots,g_n$, having the computed $\overline{g}_0,\dots,\overline{g}_n$ such that $\sum_{0\leq i\leq n}\overline{g}_i(y-\eta)^i=\sum_{1\leq i\leq n} g_i y^i$, which requires no more than n^2 additions in succession.

As a result, $C_+(\beta_1)\leq n(v+1)\binom{n+v}{n}$. Hence by Corollary 6.2 we obtain $(n+v)^{n+2}\geq n(v+1)\binom{n+v}{n}\geq C_+(g_1,\dots,g_n)\geq\frac{\sqrt{\log N}-2n}{3}$ whence the theorem follows.

We mention here that the analog of Strassen's Theorem 4.3 is not true for C_+. For example, let $f=x_1\cdots x_n+x_1x_2^2\cdots x_n^n$; then $C_+(f)=1$. It can be proved that $C_+\left(\frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\right)=n$, since if $i\neq j$, then GCD $\left(\frac{\partial f}{\partial x_i},\frac{\partial f}{\partial x_j}\right)=(x_1\cdots x_n)/(x_ix_j)$, and to continue the proof we should make use of representation (4).

To complete the picture we remark that the analog of Corollary 6.2 for the evaluations over the complex ground field $F=\mathbb{C}$ is not true. In [63], for every n there was constructed an example of a polynomial $f\in\mathbb{R}[x]$ having n distinct real zeros, for which $C_+^{(\mathbb{C})}(f)\leq 3$. In this same paper [63] it was noted that the additive (over $\mathbb{R}$) complexity

of the Chebyshev polynomial of degree 3^k with 3^k distinct real zeros does not exceed k. By the same token, the bound in Corollary 6.2 is exact to within the extraction of a square root, while from the validity of the above-mentioned Kushnirenko conjecture there would ensue an exact bound in order.

In concluding this section the author would like to point out that many results of Arnol'd and his pupils (see [2, 21], for instance), touching on estimates of certain other topological characteristics of real algebraic varieties (besides the bounds we have used for the number of zero-dimensional components), for example, Betti numbers, the Euler characteristic, etc., in terms of the number k of monomials occurring in the polynomials defining a given variety, can it seems yield other interesting applications to the estimates of additive complexity, which is closely related to k, as was seen in the proof of Corollary 6.2. More profound estimates of additive complexity apparently exist in terms of the Newton polyhedron of the (real) polynomials being evaluated. Arnol'd hypothecated that all "reasonable" invariants of polynomials are expressed in terms of their Newton polyhedra; see [2], for example, where it has been proved that the number of roots of the general system coincides with Minkowski's mixed volume of the Newton polyhedra of the polynomials of this system. It remains to ascertain whether complexity (say, additive) is a "reasonable" invariant.

In concluding Chap. I we remark that in it we have presented methods for obtaining nonlinear lower complexity bounds for polynomials (and families of polynomials) of relatively high degree (in comparison with the number of variables). One of the unsolved and most interesting problems in this area is the obtaining of nonlinear lower bounds for polynomials of small (for example, constant, i.e., independent of the number of variables) degrees. Apparently, the solution of this problem calls for the development of a principally new technique.

CHAPTER II. LOWER BOUNDS ON MULTIPLICATIVE COMPLEXITY FOR PROBLEMS OF LINEAR ALGEBRA

7. Multiplicative Complexity and Rank

Throughout the whole chapter (excepting Sec. 11) we shall be dealing with the following situation (in the notation of Sec. 1): $P=\{+,x\}\cup\{xy\}_{y\in K}$ or $P=\{+,x,/\}\cup\{xy\}_{y\in F}$, if $K=F$ is a field (in Secs. 8 and 10, $K=F$); $\lambda=\lambda_m$ is the multiplicative complexity; the input variables $\{x_1,\dots,x_n\}\cup\{y_1,\dots,y_m\}$ are not assumed commuting.

The problem to be examined in this chapter is the estimation of $C_m(A_1,\dots,A_p)$, where $A_\ell=\sum_{i,j}a_{ij\ell}x_iy_j$ $(1\le\ell\le p)$ are bilinear forms $(a_{ij\ell}\in K)$. The same letter A_ℓ will denote the $n\times m$ -matrix of coefficients $(a_{ij\ell})_{1\le i\le n,\,1\le j\le m}$. The following concept of the rank of a family of bilinear forms (matrices) proved to be fruitful (one of the first papers in which it appeared explicitly was [64]):

$$Rg_K(A_1,\dots,A_p)=\min\{N:\{A_1,\dots,A_p\}\subset KC_1K+\dots+KC_NK,^*\ \text{where } C_i=u_iv_i\ (1\le i\le N)\ \text{for certain } n\times1\text{ -columns } u_1,\dots,u_N \text{ and } 1\times m\text{ -rows } v_1,\dots,v_N \text{ over } K\}.$$

*Translator's Note: The Russian word for rank is "rang" and hence the abbreviation "Rg" used here. Since this appears quite often in what follows, I have chosen to retain it rather than to change it everywhere to "Rk."

Let the tensor $\tau \in K^n \otimes K^m \otimes K^p$, we define its rank:

$$Rg_K(\tau) = \min\{N : \tau = u_1 \otimes v_1 \otimes w_1 + \ldots + u_N \otimes v_N \otimes w_N\}.$$

For matrices $A_1, \ldots, A_p$ we set up the $n \times m \times p$-tensor $\tau = (a_{ijl})$, then it is not difficult to verify that $Rg_K(\tau) = Rg_K(A_1, \ldots, A_p)$. Analogously we can determine $Rg_K(\tau)$ for any $\tau \in M_1 \otimes_K M_2 \otimes_K \ldots \otimes_K M_s$, where M_i is a K-module $(1 \leq i \leq s)$, but we do not here need so general a definition. The role of the concept introduced of the rank becomes apparent in the following theorem which algebrizes the multiplicative complexity in the situation being examined.

THEOREM 7.1 [54]. $C_m(A_1, \ldots, A_p) = Rg_K(A_1, \ldots, A_p)$.

Proof. At first let $K = F$ be a field. We eliminate division with the aid of the method in [54] (it is described briefly in [9] as well). A similar method was already applied in the proofs of Theorems 4.2 and 6.3. Suppose that a SLP β evaluates $A_1, \ldots, A_p$. By means of a change of variables of the type $x_i \to x_i - \eta_i = \bar{x}_i$ we can achieve that the free terms in the values of all working variables z_l in the SLP β are nonzero. The value of every variable z_l can be represented as a series $\sum_{i \geq 0} b_{i,l}$, where $b_{i,l}$ is a form of degree i (in the noncommuting variables $\bar{x}_1, \ldots, \bar{x}_n, \bar{y}_1, \ldots, \bar{y}_m$). We restructure β into the SLP $\bar{\beta}$ evaluating by recursion on l the forms $b_{0,l}, b_{1,l}, b_{2,l}$ (in the general case when β evaluates a family of polynomials $\{g_1, \ldots, g_p\}$ of arbitrary degrees, the SLP $\bar{\beta}$ must evaluate $b_{i,l}$ for all $i \leq \max\{\deg g_1, \ldots, \deg g_p\}$). It is not difficult to see that the restructuring mentioned does not increase the multiplicative complexity in the case being examined, i.e., $C_m(\bar{\beta}) \leq C_m(\beta)$.

Let us now consider (see [64], for instance) a division-free SLP β (the case of an arbitrary ring K is covered by the same token) evaluating $A_1, \ldots, A_p$. The value of each working variable z_l of the SLP β can be represented as $b_0^{(l)} + b_x^{(l)} + b_y^{(l)} + b_{xx}^{(l)} + b_{xy}^{(l)} + b_{yx}^{(l)} + b_{yy}^{(l)} + b_3^{(l)}$ where, for example, $b_{xy}^{(l)}$ is a sum of monomials (with coefficients from K) of the form $x_i y_j$ etc., $b_3^{(l)}$ is a sum of monomials of degrees no less than three. We restructure the SLP β into a SLP β_1 evaluating $b_0^{(l)}, b_x^{(l)}, b_y^{(l)}, b_{xy}^{(l)}$ by recursion on l for all l. If, for example, the l-th instruction (see Sec. 1) of the SLP β had the form $z_l = z_s z_t$ (where $s, t < l$), then $b_0^{(l)} = b_0^{(s)} b_0^{(t)}$; $b_x^{(l)} = b_x^{(s)} b_0^{(t)} + b_0^{(s)} b_x^{(t)}$; $b_y^{(l)} = b_y^{(s)} b_0^{(t)} + b_0^{(s)} b_y^{(t)}$; $b_{xy}^{(l)} = b_x^{(s)} b_y^{(t)} + b_{xy}^{(s)} b_0^{(t)} + b_0^{(s)} b_{xy}^{(t)}$. This shows that $C_m(\beta_1) \leq C_m(\beta)$, moreover, β_1 contains only the nonlinear multiplication operations $\times$ of the form $(\sum_i \alpha_i x_i) \times (\sum_j \gamma_j y_j)$, namely, one such multiplication corresponds to the product of a column by a row in matrix terminology. Hence follows the inequality $C_m(A_1, \ldots, A_p) \geq Rg_K(A_1, \ldots, A_p)$. This completes the theorem's proof since the reverse inequality is obvious.

Thus, the study of the multiplicative complexity of a family of bilinear forms is reduced to the estimation of the rank $Rg_K(A_1, \ldots, A_p)$ of a family of matrices. If $K = F$ is a field, then $Rg_F(A)$ is the usual rank of matrix A, and it is independent of the choice of F, which is false for $p > 1$ (i.e., $Rg_F(A_1, \ldots, A_p) \geq Rg_H(A_1, \ldots, A_p)$ under the extension of field $F \subseteq H$, and the inequality can be strict; see [9], for instance). The investigation of rank when $p > 1$ proved to be a very difficult problem (the results of studying it when $p = 2$, obtained by the author, are stated in Sec. 8). In the present chapter we present

certain bounds in this direction which have been obtained. The paper [30] (in Dutch) contains a more complete survey on rank.

In ending this introductory section we limit ourselves to some general remarks and to the properties of rank. Obviously, $Rg_K(A_1,\dots,A_p)\leq \sum_{1\leq i\leq p} Rg_K(A_i)$. In contrast to the rank of one matrix, $Rg_F(A_1,\dots,A_p)$ is not an upper-semicontinuous function of $A_1,\dots,A_p$ when $p>1$ (see [9], for example). If F is algebraically closed, then it is easy to see that $Rg_F(A_1,\dots,A_p)$ equals "almost everywhere" (in the sense of the Zariski topology) a certain number $r_q(m,n,p)$ depending only on m,n,p (and is not changed under any permutation of them) and on the characteristic q of field F. Certain estimates on $r_q(m,n,p)$ have been presented in [9], viz., $mnp/(m+n+p-2)\leq r_q(m,n,p)\leq \lceil m/2\rceil \min\{2n,p\}$ for $n\leq p$ (the upper bound follows from Corollary 8.3 below). When $m=n=p$ the order of growth of $r_q(n,n,n)$ is between $n^2/3$ and $n^2/2$ (the author does not know more exact bounds). Further, it was shown in [9] that for certain $n\times n$ -matrices $A_1,\dots,A_n$ with coefficients from the set $\{0,1\}$ the order of growth of $Rg_F(A_1,\dots,A_n)$ differs from n^2 by no more than a multiplicative constant (in contrast to the situation of polynomials — see the end of Sec. 3 — with coefficients from the set $\{0,1\}$, the order of growth of whose complexity is less than maximum at least in the multiplicative logarithm). In the plan of the general study of rank we note that the group of linear transformations preserving the tensor's rank has been computed as well in [9].

8. Rank of a Pair of Bilinear Forms

In this section we summarize the results due to the author on the estimates of $Rg_F(A,B)$, where F is a field, following [9, 32, 33]. We take it below that all matrices have been defined over F.

We define the relation $C\preccurlyeq D$ between matrices if $Rg_F(C,D)=Rg\,D$. Further, we introduce the relative rank $Rg_F(A/B)=\min_{C\preccurlyeq B} Rg(A-C)$, where the minimum ranges over all $C\preccurlyeq B$.

THEOREM 8.1 [9]. $Rg_F(A,B)=Rg\,B+Rg_F(A/B)$.

Now, up to the end of the section, let F be algebraically closed. We derive an explicit formula for $Rg_F(A,B)$ in terms of the canonic form of the pair (A,B) relative to the transformations $(A,B)\to(CAD,CBD)$, where C,D are nonsingular, which is called the Weierstrass–Kronecker canonic form of the matrix sheaf $\lambda A+\mu B$ (for example, see [5]; from this same book we have borrowed the terminology needed in the next theorem).

THEOREM 8.2 [8, 9, 32, 33]. In the sheaf $\lambda A+\mu B$ let the nonzero minimal indices equal $a_1,\dots,a_s$ for the columns and $b_1,\dots,b_k$ for the rows. Further, let the regular $p\times p$ "kernel" $\lambda A_0+\mu B_0$ of sheaf $\lambda A+\mu B$ have, for each $\gamma\in F\cup\{\infty\}$, d_γ elementary divisors of the form $(\alpha\lambda+\beta\mu)^\delta$, where $\alpha/\beta=\gamma$. We set $d=\max d_\gamma$. Then

$$Rg_F(A,B)=\sum_i(a_i+1)+\sum_j(b_j+1)+p+d.$$

The theorem's proof relies on Theorem 8.1. A result close to Theorem 8.2 has been obtained independently in [38]. Further, $m\leq n$ in the formulations.

COROLLARY 8.3 [9]. For $m \times n$ -matrices:

1) $Rg_F(A,B)$ almost everywhere equals $\min\{n, 2m\} - r_q(2,n,m)$ (in the notation of Sec. 7);

2) $\max_{A,B} Rg_F(A,B) = \min\{m + [n/2], 2m\}$.

From this corollary we see, in particular, that $Rg_F(A,B)$ is not an upper-semicontinuous function of A, B.

9. Multiplicative Complexity of a Bilinear Form Over a Commutative Ring

If in the case when $K = F$ is the ground field the difficulties were due to the estimation of the rank $Rg_F(A,B)$ of a pair of matrices (see Sec.8), then over an arbitrary commutative ring K the difficulties are due now to the estimation of $Rg_K(A)$ (by Theorem 7.1 the latter quantity coincides with the multiplicative complexity of a bilinear form A over K). Thus, let K be a commutative Noether ring with unity and A be an $m \times n$ -matrix over K. In this section we present the author's results on the bounds for $Rg_K(A)$ (see [10, 34]). By rgA we denote the usual rank of matrix A, equal to the size of the largest nonzero minor in it. Obviously, $rgA \leq Rg_K(A)$. Let us explicitly describe those rings K (we call them Rg *-rings*) for which the equality $Rg_K(A) = rgA$ is fulfilled for any A over K. The concepts from homological algebra used below can be found in [14]. By $gldh(K)$ we denote the global homological dimension of ring K.

THEOREM 9.1 [10, 34]. Ring K is an Rg-ring if and only if $K = K_1 \oplus \ldots \oplus K_s$ for some uniquely defined integer rings $K_1, \ldots, K_s$ such that:

1) $gldh(K_i) \leq 2$ $(1 \leq i \leq s)$;

2) every projective K_i -module is free $(1 \leq i \leq s)$.

COROLLARY 9.2 [10]. $F[z_1, z_2]$ is an Rg -ring.

How does $Rg_K(A)$ behave for the polynomial ring $K = K_d = F[z_1, \ldots, z_d]$ when $d \geq 3$? This question has been resolved practically completely in the case of matrices of the form $A = z_1 A_1 + \ldots + z_d A_d$, where A_i $(1 \leq i \leq d)$ is a matrix over field F (such matrices are called *square-free* and, up to the end of the present section, excepting the last paragraph in it, we retain for them the notation A with or without indices). We denote $R_d(r) = \sup_{rgA = r} Rg_{K_d}(A)$ and $R(r) = \sup_d R_d(r)$.

THEOREM 9.3 [10, 34]. 1) $R(r_1 + r_2) \geq R(r_1) + R(r_2)$;

2) $R(r) < 2r$;

3) $\lim_{r \to \infty} \frac{R(r)}{r} = 2$;

4) $R_3(r) = [3/2\, r]$.

An example of a matrix family $\{A_i\}$ on which the sequence $Rg_{K_d}(A_i)/rg(A_i) \xrightarrow[i \to \infty]{} 2$ is constructed as follows. We consider the Koszul complex (see [14, 15]) of the ring $K = K_d$ relative to the element system $\{z_1, \ldots, z_d\}$:

$$0 \to K^1 \xrightarrow{A_{1,d}} K^d \ldots K^{\binom{d}{i}} \xrightarrow{A_{i,d+1-i}} K^{\binom{d}{i+1}} \ldots K^d \xrightarrow{A_{d,1}} K^1 \to 0.$$

It can be shown [10] that

$$Rg_K(A_{i,d+1-i})=\min\left\{\binom{d}{i},\binom{d}{i+1}\right\};\ rg(A_{i,d+1-i})=\binom{d-1}{i}.$$

As the sequence $\{A_i\}$ we can take the middle terms of the Koszul complexes, i.e., $A_i=A_{i,i}$.

In concluding this section we mention that additivity is not fulfilled for $Rg_K(A)$ for all rings K relative to the direct sum of matrices, defined as $A\oplus B=\begin{pmatrix}A&0\\0&B\end{pmatrix}$ (cf. Strassen's conjecture of the additivity of rank, mentioned in the next section). For example, let $K=\mathbb{Z}[\sqrt{5}]$ and $A=\begin{vmatrix}\frac{\sqrt{5}-1}{2}&2\\ \sqrt{5}+1&\end{vmatrix}$. Then $Rg_K(A)=2$, but $Rg_K(A\oplus\ldots\oplus A)\leq p+1$, where p is the number of summands in the direct sum mentioned. At the same time, the additivity of $Rg_K(A)$ holds over a polynomial ring and for square-free matrices [10]. The author permits himself to make two conjectures: a) the additivity of a rank is fulfilled over the polynomial ring for any matrices; b) for every regular ring K (i.e., $gldh(K)<\infty$) we can find a number c_K such that $Rg_K(A)\leq c_K\,rg\,A$ for an arbitrary matrix A over K.

10. Bounds on the Rank of Algebras

Various complexity problems of linear algebra, for example, the multiplication of matrices or polynomials, lead to estimating the rank of certain algebras. The rank of an algebra $\mathfrak{A}$ over a field F (we denote it $Rg_F(\mathfrak{A})$) is defined as the rank of its structure tensor in some base of this algebra, and is independent of the choice of the base (see [54]). The rank $Rg_F(\mathfrak{A})$ can be interpreted as the multiplicative complexity of the multiplication of two elements of algebra $\mathfrak{A}$, i.e., to find, from the expansion of the factors with respect to the base, the expansion of their products. Let $\mathfrak{M}_n$ be the algebra of $n\times n$-matrices. Then $Rg_F(\mathfrak{M}_n)$ equals the multiplicative complexity of the multiplication of $n\times n$-matrices, i.e., $C_m(\{\sum_{1\leq i\leq n}x_{ki}y_{il}\}_{1\leq k,l\leq n}$. The next theorem is due to Alder and Strassen.

THEOREM 10.1 [24]. $Rg_F(\mathfrak{A})\geq 2\dim_F(\mathfrak{A})-K$, where K equals the number of maximal ideals in $\mathfrak{A}$.

The proof is broken up into the following two lemmas.

LEMMA 10.2 [24]. $Rg(\mathfrak{A}\oplus\mathfrak{B})\geq Rg((\mathfrak{A}/rad\,\mathfrak{A})\oplus\mathfrak{B})+2\dim rad\,\mathfrak{A}$ ($rad\,\mathfrak{A}$ is the radical of algebra $\mathfrak{A}$).

LEMMA 10.3 [24]. If $\mathfrak{A}$ is a simple algebra, then $Rg(\mathfrak{A}\oplus\mathfrak{B})\geq 2\dim\mathfrak{A}-1+Rg(\mathfrak{B})$ (we recall that an algebra is called simple if its only ideal is the zero ideal).

Since $\mathfrak{M}_n$ is a simple algebra, we obtain

COROLLARY 10.4 [24]. $Rg_F(\mathfrak{M}_n)\geq 2n^2-1$.

We note that Theorem 10.1 (as also the three assertions following it) has been proved in [24] actually in a stronger form, viz., for the multiplicative complexity C'_m of multiplication in the algebra under the assumption of commutation of the input variables $x_iy_j=y_jx_i$ of bilinear forms (see the beginning of Sec. 7). It is easily seen (see [64], for instance) that $C'_m\leq Rg=C_m\leq 2C'_m$ for families of bilinear forms.

We mention two further useful inequalities for the rank of tensors:

$$Rg_K(\tau_1\oplus\tau_2)\leq Rg_K(\tau_1)+Rg_K(\tau_2) \tag{5}$$

$$Rg_K(\tau_1 \otimes_K \tau_2) \leq Rg_K(\tau_1) Rg_K(\tau_2). \qquad (6)$$

Inequality (6) is applied in the following form for obtaining upper bounds for $Rg_F(m_n)$ (see [52, 54], for example): if $Rg_K(m_{n_0}) \leq N_0$ for some n_0, N_0, then $Rg_K(m_n) = O(n^{\log_{n_0} N_0})$ (inequality (6) is used here in the form $Rg_K(m_{n_1 n_2}) \leq Rg_K(m_{n_1}) Rg_K(m_{n_2})$, taking it that $m_{n_1 n_2} = m_{n_1} \otimes m_{n_2}$). Here it is appropriate to mention an estimate, asymptotically the best one known up to the moment of writing the present survey, for the complexity of matrix multiplication:

THEOREM 10.5 [29]. $Rg_F(m_n) = O(n^{2,18555\ldots})$.

The proof of this estimate relies on the following concept, interesting in its own right, of the *boundary rank* $\overline{Rg}(\tau)$ (see [29, 52], for example). To be precise, we define

$$\overline{Rg}(\tau) = \min\{N : \varepsilon^K(\tau + \varepsilon\sigma) = u_1 \otimes v_1 \otimes w_1 + \ldots + u_N \otimes v_N \otimes w_N\},$$

where K is some positive integer; u_i, v_i, w_i are some vectors over the ring $F[\varepsilon]$; σ is a tensor over ring $F[\varepsilon]$. Informally we say that the inequality $\overline{Rg}(\tau) \leq p$ signifies that tensors of rank not exceeding p exist "arbitrarily close" (in the Zariski topology sence) to tensor τ. The main instrument in the use of $\overline{Rg}$ is the boundary analog of inequality (6) [52]: if $\overline{Rg}(m_{n_0}) \leq N_0$ for some n_0, N_0, then $Rg(m_n) = O(n^{\log_{n_0} N_0})$. A number of examples of such kind of bounds for suitable n_0, N_0 have been constructed in [29, 52].

Strassen [54] has conjectured that $Rg_F(\tau_1 \otimes \tau_2) = Rg_F(\tau_1) + Rg_F(\tau_2)$ (cf. inequality (5)). It is false for the boundary rank (see [52]).

By $A_K = \sum_{0 \leq i \leq K} x_i y_{K-i}$ we denote a bilinear form expressing the coefficient (in terms of the coefficients of the cofactor) of the K-th power in the product of two n-th-degree polynomials, i.e., $Rg_F(A_0, \ldots, A_{2n})$ is the multiplicative complexity of the multiplication of two polynomials. The results mentioned at the end of Sec. 5 can be reformulated in the language adopted in the present section as follows:

THEOREM 10.6. 1) [31] $Rg_F(F[z]/(f)) = 2n - K$, where F is an infinite field, $\deg f = n$ and $f = f_1^{m_1} \ldots f_K^{m_K}$; moreover, $f_i \in F[z]$ is irreducible over $F (1 \leq i \leq K)$ and the $\{f_i\}$ are pairwise relatively prime.

2) [8, 9, 32, 33] $Rg_F(A_0, \ldots, A_{2n}) \leq ng(n)$ for a finite field F and for some function g growing more slowly than any fixed iteration of the logarithm.

3) [28] $Rg_F(A_0, \ldots, A_{2n}) \geq (3,52)n$ for a field F of two elements. Obviously, $Rg_F(F[z]/(f)) \leq Rg_F(A_0, \ldots, A_{2n}) \leq Rg_F(F[z]/(h))$, where $\deg h = 2n$. The estimate $Rg_F(A_0, \ldots, A_{2n}) = O(n \log n)$ for any field F followed from [22]. The upper bound in item 1) follows from inequality (5) and the isomorphism $F[z]/(f) = \bigoplus_{1 \leq i \leq K} F[z]/(f_i^{m_i})$; the lower bound follows from Theorem 10.1.

We now sketch the proof of item 3). We fix a certain $0 \leq j \leq n$. Obviously, $Rg_F(A_0, \ldots, A_{2n}) \geq Rg_F(A_{j-1}, \ldots, A_{2n-j+1}) = p_j$. By Theorem 7.1, $p = p_j$ equals the smallest number $C_1, \ldots, C_p$ of bilinear forms of rank 1, whose linear hull, linear over F, contains the linear hull $\mathcal{L} = \mathcal{L}(A_{j-1}, \ldots, A_{2n-j+1})$ of the bilinear forms being examined. On the other hand, for any bilinear form $0 \neq A \in \mathcal{L}$ the inequality $rg\, A \geq j$ is fulfilled; therefore, $\mathcal{L}$ can be treat-

ed as a linear code in the linear hull $\mathcal{L}(C_1,\dots,C_p)$ (with base $\{C_1,\dots,C_p\}$); moreover, the code distance of this code is not less than j (for the required concepts from coding theory see [19], for example). Therefore, to bound p from below we can apply the Varshamov–Gilbert bounds (see [19, Chap. 4]), which leads to the inequality $p\geqslant(3,52)n$ for a suitable choice of j.

The strengthening of the bounds for items 2) and 3) of the theorem is apparently a subtle number-theoretic problem.

11. Linearized Multiplicative Complexity

In the preceding sections of Chap. II we examined the rank of the elements of a tensor product of vector spaces (more precisely, of a product of three spaces, but, in principle, of a larger number; see the remark in Sec. 7). In the present section we consider the analog of rank for the elements of a symmetric product (more precisely, of a symmetric d_1-dimensional n-th-degree vector space over a field F; in other words, of the space of homogeneous forms forms of degree d_1 in the polynomial ring $F[x_1,\dots,x_n]$). Namely, for every form $f\in F[x_1,\dots,x_n]$ of degree d_1 the quantity $\min\left\{N: f=\sum_{1\leqslant i\leqslant N} l_1^{(i)}\dots l_{d_1}^{(i)}\right.$, where $\left.l_j^{(i)}\right.$ is a linear form$\}$ is called its *linearized multiplicative complexity* $C_l(f)$. We set forth a method for obtaining nonlinear lower bounds on $C_l(f)$; the method yields nonlinear bounds when $d_1\geqslant 4$. Below we take it that the degree $d_1=2d$ is even; this assumption has been made for convenience of notation (without a great loss of generality on account of the nature of the bounds being proposed in this section).

We shall examine auxiliary matrices A of dimension $n^d\times n^d$. Their rows and columns are numbered by all possible vectors $I=(i_1,\dots,i_d)$, where $1\leqslant i_1,\dots,i_d\leqslant n$; in this notation $A=(a_{I,J})$. By x^I we denote the d-th-degree monomial $x_{i_1}\dots x_{i_d}$ and by $|I|$ we denote the number $\kappa_1!\dots\kappa_n!$, where κ_i is the number of occurrences of the number i in vector I.

On the space of $n^d\times n^d$-matrices we define a linear operator L (we call it the *commutation operator*), having set $L(A)=B$, where $b_{P,Q}=\left(\sum_{x^Ix^J=x^Px^Q=x^K} a_{I,J}\right)|K|$, i.e., $x^Px^Q=x^K$ and the summation is over all pairs of vectors I,J such that $x^Ix^J=x^K$. Every matrix A can be associated with a form $g_A=\sum_{I,J} a_{I,J}x^Ix^J$ of degree $2d$, where the summation is over all pairs of vectors I,J. Conversely, every form g can be associated with a matrix A such that $g_A=g$, but now nonuniquely; namely, we have

LEMMA 11.1. The equality $g_A=g_B$ of forms is equivalent to $L(A)=L(B)$.

With every (ordered) family of linear forms $\{l_1,\dots,l_{2d}\}$ we can associate an $n^d\times n^d$-matrix $A=A_{l_1,\dots,l_{2d}}$ of rank 1, having set up its element $a_{I,J}=l_{1,i_1}\dots l_{d,i_d}l_{d+1,j_1}\dots l_{2d,j_d}$, where the form $l_i=\sum_{1\leqslant j\leqslant n} l_{i,j}x_j$ and $I=(i_1,\dots,i_d)$, $J=(j_1,\dots,j_d)$. Obviously, the form $g_{A_{l_1,\dots,l_{2d}}}=l_1\dots l_{2d}$ is a product of linear forms. We clarify the action of the commutation operator on the matrix $A_{l_1,\dots,l_{2d}}$ constructed.

LEMMA 11.2. $L(A_{l_1,\dots,l_{2d}})=\sum_{\pi\in S_{2d}} A_{l_{\pi(1)},\dots,l_{\pi(2d)}}$, where the summation is over all permutations of π.

Consequently, $\operatorname{rg}(L(A_{l_1,\dots,l_{2d}})) \leq (2d)!$

Now let $C_l(f) \leq N$ and $f = \sum_{1 \leq i \leq N} l_1^{(i)} \dots l_{2d}^{(i)}$. By A_i we denote the matrix $A_{l_1^{(i)},\dots,l_{2d}^{(i)}}$. Then $f = g_{A_1} + \dots + g_{A_N} = g_{A_1 + \dots + A_N}$. By Lemma 11.1 the matrix $L(A_1 + \dots + A_N) = L(f)$ is an invariant of form f. Finally, by Lemma 11.2,

$$\operatorname{rg}(L(A_1 + \dots + A_N)) \leq \operatorname{rg} L(A_1) + \dots + \operatorname{rg} L(A_N) \leq N(2d)!,$$

and as a result we obtain

THEOREM 11.3. For every form f of degree $2d$,

$$C_l(f) \geq \frac{\operatorname{rg} L(f)}{(2d)!}.$$

We present an example of the application of the theorem, demonstrating the presence of a large gap between the linearized multiplicative complexity and the total complexity C_t (see Sec. 1). Let $f = (x_1\overline{x_1} + \dots + x_n\overline{x_n})^d$ be a $2d$-th-degree form in the $2n$ variables $x_1, \dots, x_n$, $\overline{x_1}, \dots, \overline{x_n}$. For every vectors $I, \bar{J}$ we denote $x^I = x_{i_1} \dots x_{i_d}$, $\overline{x}^{\bar{J}} = \overline{x_{j_1}} \dots \overline{x_{j_d}}$. In the matrix $L(f)$ we pick out a submatrix B of dimension $n^d \times n^d$, spanned by a row of form I and a column of form $\bar{J}$ (over all $I, \bar{J}$ of the form indicated above). Now in matrix B we pick out a submatrix C spanned by any such maximal collection of rows $\{I\}$ for which all monomials x^I are pairwise distinct; we choose the columns with corresponding indices $\{\bar{I}\}$ * as for the rows. Then the square matrix C has $\binom{n+d-1}{n-1}$ rows and it is diagonal with nonzero elements on the diagonal; $\operatorname{rg} C = \binom{n+d-1}{n-1}$. According to Theorem 11.3, $C_l(f) \geq \binom{n+d-1}{n-1}/(2d)!$.

On the other hand, $C_t(f) \leq 2n + \log d$. It is clear that for d sufficiently small in comparison with n (to be precise, here we can take $n \succ d^6$) the quantity $C_l(f) \succ (n/d^5)^d$ is not bounded from above by, say, any polynomial of $C_t(f)$, i.e., of n.

For completeness we remark here that in [37] it has been shown that the multiplicative complexity $C_m(f)$ of a form f (here two cases can be examined: with commuting and noncommuting input variables) of degree d_1 can be bounded from above in terms of the following quantity (whose definition is close in spirit to the definitions of rank and of $C_l(f)$ examined in the present chapter): $\min\left\{N : f = \sum_{1 \leq i \leq N} g_i h_i\right.$, where g_i, h_i are forms and $\left.\frac{d_1}{3} \leq \deg g_i, \deg h_i \leq \frac{2d_1}{3}\right\}$. A method was proposed in [37] for estimating this quantity from below (and, by the same token, the multiplicative complexity) in the case when it is not assumed that the input variables are commuting. As yet it is not clear how to obtain lower bounds for this quantity in the case of commuting variables.

In concluding Chap. II we say a few words on the fact that the rank of a family of bilinear forms harbors in the meanwhile many mysteries. One of the most interesting unsolved problems is the obtaining of nonlinear (in the number of variables and the number of forms) lower bounds for the rank of some natural families of forms (here we can refer to practically everything we said at the beginning of Sec. 3 on the computational complexity of polynomials),

*Translator's note: This might be a misprint; I feel it ought to be $\{\bar{J}\}$.

for example, for problems, arousing great interest, of the multiplication of polynomials (over a finite field) or of the multiplication of matrices (see Sec. 10). The author cherishes the hope that for rank a breakthrough in obtaining nonlinear lower bounds occurs faster than in the other directions of algebraic complexity, which apparently requires a further algebraization of the concept of the rank of a family of bilinear forms.

CHAPTER III. COMPLEXITY FOR STRAIGHT-LINE PROGRAMS OF NONSTANDARD TYPES

In the last chapter the sections are less interrelated than in the preceding two chapters. What connects them is perhaps the fact that in them we examine SLP and complexity measures of nonstandard types, satisfying (excepting Sec. 12) some restrictions (different ones in different sections) in comparison with SLP of a sufficiently general form studied in Chapters I and II. The adoption of precisely these restrictions sometimes has practical grounds and is explainable by the possibility of obtaining lower bounds which we have been unable to obtain as yet for SLP of general form. Frequently for nonstandard (restricted) computing models we have succeeded in revealing the connection of the complexity with objects classical for mathematics (it is precisely on this basis that the author chose the material for the present chapter). In addition, the restrictions sometimes permit us to trace the influence of individual factors on the total complexity (see Sec. 1), which is useful for penetration into the secrets of complexity lower bounds.

12. Irrational Computational Complexity of Algebraic Functions

In this section we examine SLP of the following type (in the terminology of Sec. 1): F is a ground field of characteristic other than two; $P=\{+,\times,/,\sqrt{\ }\}\cup\{x_\gamma\}_{\gamma\in F}$; $\lambda=\lambda_{\sqrt{\ }}$, $\lambda(+)=\lambda(\times)=\lambda(/)=\lambda(x_\gamma)=0$, $\lambda(\sqrt{\ })=1$; the set of input variables is empty (somewhat modifying the definition from Sec. 1, we take it that constants from field F can stand as the arguments of the base operation in item 4 of the definition). Here the sign $\sqrt{\ }$ denotes the unary operation of taking the square root; rational operations are freely allowed; therefore, *complexity measures* of the kind indicated are naturally called *irrational*.

If $f\in F$ then the element $\sqrt{f}$ of the extension of field F is called a simple radical. Let $\{g_1,\dots,g_K\}\subset F(\sqrt{f_1},\dots,\sqrt{f_\ell})$, where $f_1,\dots,f_\ell\in F$; the problem examined in the present section is the estimation of the irrational complexity $C_{\sqrt{\ }}(g_1,\dots,g_K)$. The extension of field $F\subseteq F(g_1,\dots,g_K)$ is the Abelian Galois extension of degree 2^c (for some c) with the Galois group $Z_2\times\dots\times Z_2$ (the direct product of c copies of the cyclic group Z_2 of order two). It is not difficult to see that $c=C_{\sqrt{\ }}(g_1,\dots,g_K)$. The inequality $c\leqslant C_{\sqrt{\ }}(g_1,\dots,g_K)$ follows from the fact that the addition of one new simple radical increases the extension's degree by no more than twice; on the other hand, each floor (of degree two) of the tower of field $F=F_0\subset F_1\subset\dots\subset F_c=F(g_1,\dots,g_K)$ is obtained from the preceding one by the addition of one new radical, whence follows the opposite inequality.

We present an example, coming from antiquity. Let $F=\mathbb{R}(y_1,y_2)$, and then $C_{\sqrt{\ }}(g_1,\dots,g_K)$ equals precisely the necessary number of applications of a compass for the construction of $g_1,\dots,g_K$ with the aid of compass and straightedge.

The difficulty is that often in the interesting examples it is not clear how to estimate a priori from below the degree of the field extension. Therefore, a method for estimating $C_{\sqrt{}}$ was proposed in [53] for the case when $F = F_0(x_1,\dots,x_n)$ where $F_0 \subseteq \mathbb{C}$, and it was shown that $C_{\sqrt{}}(g) \geqslant \log N$ where N is the number of sheets of the Riemann surface of the analytic function g. The complete rigorous proof of this result requires a cumbersome technique (not carried out to the end in [53]), and we restrict ourselves here to the more elementary method, convenient for applications, suggested in [45].

Let $\tau=\{\tau_1,\dots,\tau_K\}$ be the set of simple radicals; we denote $\tau_I=\prod_{i\in I}\tau_i$ for $\varnothing\neq I \subseteq\{1,\dots,K\}$ ($\tau_\varnothing=1$). We say that set τ is radical-independent if $\tau_I\notin F$ for every $I\neq\varnothing$. By $R(\tau)$ we denote the radical dimension of set τ, i.e., the largest number of radical-independent elements among $\tau_1,\dots,\tau_K$. It is not difficult to show ([45]) that in any maximal-by-inclusion radical-independent subset of r there are $R(\tau)$ elements, i.e., the radical dimension possesses the same general (matroid) properties as does the usual dimension of a vector space: degree of transcendence of the field extension, etc. In connection with this, $R(\tau)$ is convenient for computation.

If τ is a radical-independent set, then the elements $\{\tau_I\}_{I\subset\{1,\dots,K\}}$ constitute the base of the extension of $F\subset F(\tau)$, whose degree, by the same token, equals 2^K [45]. Let $g=\{g_1,\dots,g_K\}\subset F(\tau)$, then the support $S(g,\tau)$ of family g is the set of τ_I such that for some $1\leqslant i\leqslant K$ in the (unique) decomposition $g_i=\sum_{J\subseteq\{1,\dots,K\}} c_{i,J}\tau_J$, where $c_{i,J}\in F$, the coefficient $c_{i,I}$ of τ_I is nonzero.

LEMMA 12.1 [45]. If τ is a radical-independent set and $g\subset F(\tau)$, then $F(g)=F(S(g,\tau))$.

LEMMA 12.2 [45]. If σ is some set of simple radicals, then $C_{\sqrt{}}(\sigma)=R(\sigma)=\log[F(\sigma):F]$.

As a corollary we obtain

THEOREM 12.3 [45]. Let τ be a radical-independent set and $g\subset F(\tau)$, then $C_{\sqrt{}}(g)=R(S(g,\tau))$.

Since in applications often $g\subset F(\sigma)$, where σ is some given set of simple radicals, the theorem yields the following path to the computation of $C_{\sqrt{}}(g)$, which sometimes proves effective. From σ it is necessary to pick out an arbitrary maximal-by-inclusion radical-independent set $\tau\subset\sigma$; further, having decomposed g_i with respect to the base from $\{\tau_I\}$, it is necessary to find $S(g,\tau)$, which is some set of simple radicals, and finally, to pick out in it a maximal-by-inclusion radical-independent subset; its cardinality also equals $C_{\sqrt{}}(g)$.

We give one concrete application of the theorem [45]. Let $F=F_0(\{y_i,z_i\}_{1\leqslant i\leqslant N})$, then

$$C_{\sqrt{}}\left(g=\sum_{1\leqslant i<j\leqslant N}\sqrt{(y_i-y_j)^2+(z_i-z_j)^2}\right)=\binom{N}{2}.$$

In the case given the set of simple radicals $\sigma=\tau=\left\{\sqrt{(y_i-y_j)^2+(z_i-z_j)^2}\right\}_{1\leqslant i<j\leqslant N}$ is radical-independent; this follows from the fact that the functions $\{(y_i-y_j)^2+(z_i-z_j)^2\}_{1\leqslant i<j\leqslant N}$ are pairwise relatively prime. As a result $\tau=S(g,\tau)$ and $R(\tau)=\binom{N}{2}$.

13. Monotone Programs

Monotone computations are a rather narrow but sufficiently natural class of SLP for which we have managed to obtain complexity lower bounds and even to compute then explicitly for certain cases. This was done for various problems in a large series of papers. Here we present Schnorr's theorem [49] which generalizes the arguments contained in many of these papers.

Thus, a monotone SLP is the name given to a SLP (using the notation from Sec. 1) in which the role of the ground ring K is played by a certain semiring $S \subset F \setminus \{0\}$ for some field F (the semiring forms a monoid with respect to addition and a monoid with respect to multiplication); $P = \{+, \times\} \cup \{+\gamma, \times\gamma\}_{\gamma \in S}$; $\lambda = \lambda_+$ (see Sec. 2), i.e., $\lambda(+) = \lambda(+\gamma) = 1$, $\lambda(\times) = \lambda(\times\gamma) = 0$; $\{x_1, \ldots, x_n\}$ is some set of input variables; the corresponding (monotone) complexity measure is denoted C_{mon}. For example, if $F = \mathbb{R}$, then as S we can take all positive numbers.

For every polynomial g, by $Mon(g)$ we denote the set of monomials occurring in g with nonzero coefficients. A subset of monomials $B \subset Mon(g)$ is called separating if for every $s, t \in B$ and $r \in Mon(g)$, if there is fulfilled $r \mid st$ (the vertical bar signifies the divisibility relation), then either $r = s$ or $r = t$. Schnorr showed that $C_{mon}(g) \geq |B| - 1$ (here and below we assume $C_{mon}(g) = \infty$ if it has not been defined). Furthermore, for the purposes of [49] the following strengthening of this result was proved. Let σ be some mapping from the set of variables to the set of monomials; then for every monomial q we denote by q^σ the result of replacing in q every variable x_j by the monomial $\sigma(x_j)$.

THEOREM 13.1 [49]. For every polynomial g $C_{mon}(g) \geq |B| - 1$ for any separating set B of polynomial g^σ.

As applications it was shown in [49] that $C_{mon}\left(\left\{\sum_{k+l=s} x_k y_l\right\}_{0 \leq s \leq 2n}\right) = (n+1)^2$ is fulfilled for the computation of the product of n-th degree polynomials and $C_{mon}\left(\left\{\sum_{1 \leq i \leq n} x_{ki} \cdot y_{il}\right\}_{1 \leq k, l \leq n}\right) = n^3 - n^2$ for the multiplication of $n \times n$-matrices (compare with Sec. 10). Further, we consider the polynomial

$$CL_{n,k} = \sum_{1 \leq v_1 < \ldots < v_k \leq n} \prod_{1 \leq i < j \leq k} x_{v_i, v_j}$$

of degree $\binom{k}{2}$ in the $\binom{n}{2}$ variables $\{x_{i,j}\}_{1 \leq i < j \leq n}$. From Theorem 13.1 it follows that $C_{mon}(CL_{n,k}) = \binom{n}{k} - 1$. On the other hand, the question on the presence of a polynomial upper bound for the total complexity $C_t(CL_{n,k})$ (see Sec.1) is closely connected with the $P \stackrel{?}{=} NP$ problem, since the polynomial $CL_{n,k}$ corresponds to the NP-universal problem on the existence of a k-clique in an n-vertex graph (for example, see [1, Chap. 10]).

In spite of the fact that many different lower bounds were obtained for C_{mon}, the question of how large can the gap be between $C_t(g)$ and $C_{mon}(g)$ for a polynomial g remained open for some time. In [62] it was shown that this gap can be exponential. To be precise, we construct a family of plane graphs $\{G_n\}$ by induction on n:

$$G_1 = \Delta, \ldots, G_{n+1} = \quad \ldots,$$

i.e., G_n forms a regular triangle with side n, decomposed into a parquet of regular triangles with side 1.

Every set of edges of graph G_n, not having pairwise-common vertices and covering in aggregate all vertices (in particular, the number $(n+1)(n+2)/2$ of vertices must be even), is called a perfect matching of the graph. To each edge of graph G_n we assume its own variable, and for each set I of edges we denote by h_I the monomial equal to the product of the variables assigned to the edges of I. We define the polynomial g_n as the sum $\sum_I h_I$ over all perfect matchings I of graph G_n.

THEOREM 13.2 [62]. For some constant $c>1$, $C_{mon}(g_n) > c^n$ is fulfilled for all n.

On the other hand, according to one result of Kasteleyn (see [62], for example) we can effectively construct (the construction suits every plane graph) for every n a skew-symmetric matrix A_n such that $g_n = \mathrm{Pfaffian}(A_n) = \sqrt{\det A_n}$, which proves that $C_t(g_n)$ can be bounded from above by a polynomial of n (see [1, Chap. 6]). In combination with Valiant's Theorem 13.2 this answers the question posed above on the gap between total and monotone complexities.

For completeness we remark that in the Boolean case, i.e., when field F consists of two elements, monotone computations have been very intensively studied (for example, see [7] and the literature cited therein).

14. Lower Bounds for Time–Space Tradeoff

In this section we deviate somewhat from the concept of SLP adopted in Sec. 1, in order to introduce the concept of a SLP with storage S (see [6, Sec. 2]). Let F be the ground field, $P = \{+, \times, /\} \cup \{x^\gamma\}_{\gamma \in F}$; $\{x_i\}_{1 \le i \le n}$ be a collection of input variables. Every instruction of a SLP β with storage S (where S is some positive integer) has the form

$$z_{s_0} = f(z_{i_1}, \ldots, z_{i_u}, x_{j_1}, \ldots, x_{j_v}),$$

where $f \in P$, $1 \le s_0, i_1, \ldots, i_u \le S$ (it is important to note that the indices $i_1, \ldots, i_u$ can be greater than s_0, in contrast to the SLP defined in Sec. 1).

Let a SLP β with storage S (further in this section we shall sometimes omit these latter words) consist of T instructions and let the instruction written out be the t_0-th in order in the program for some $1 \le t_0 \le T$. For each $1 \le t \le T$ and $1 \le s \le S$ it is natural to determine, by induction on t, a rational function $Z_s^{(t)} \in F(x_1, \ldots, x_n)$ called the value of the working variable z_s at instant t. The induction base $Z_s^{(0)} = 0$ for any $1 \le s \le S$. If $Z_s^{(t)}$ has already been determined for all $t < t_0$, then in the case being examined $Z_{s_0}^{(t_0)} = f(Z_{i_1}^{(t_0-1)}, \ldots, Z_{i_u}^{(t_0-1)}, x_{j_1}, \ldots, x_{j_v})$ and $Z_s^{(t_0)} = Z_s^{(t_0-1)}$ for all $s \ne s_0$. We say that the functions $g_1, \ldots, g_K \in F(x_1, \ldots, x_n)$ are computed by the given β if for every $1 \le \nu \le K$ we can find $1 \le s \le S$ and $1 \le t \le T$ such that $Z_s^{(t)} = g_\nu$. It is natural to interpret the number S as space and T as time.

Let F be a field of two elements, $P=\{+,\times\}\cup\{+1\}$. In this case, a method was suggested in Sec. 2 of [6] for establishing a lower bound on the product ST for the SLP computing the family of polynomials $g_1,\dots,g_K\in F[x_1,\dots,x_n]$ satisfying some condition of l-independence $(1\leq l\leq K)$. Let us state the following two variants 1) and 2) of it (as a matter of fact, the first is a corollary of the second). For $g\in F[x_1,\dots,x_n]$ we denote by R_g the partioning of the n-dimensional cube F^n into two sets:

$$R_g^{(0)}=\{X\in F^n: g(X)=0\},\ R_g^{(1)}=\{X\in F^n: g(X)=1\}.$$

We say that the family $\{g_1,\dots,g_K\}$ possesses the property of l-independence if for every $1\leq v\leq l$ and for every $1\leq j_1<\dots<j_v\leq n$ and $1\leq i_1<\dots<i_{l-v}\leq K$ one of the following two conditions is fulfilled (see the remark above):

1) a collection of values of the variables $x_{j_1}=x_{j_1}^{(0)},\dots,\ x_{j_v}=x_{j_v}^{(0)}$ can be found such that for these fixed values the function vector $(g_{i_1},\dots,g_{i_{l-v}})$ takes more than 2^{l-v-1} values (as the remaining variables vary);

2) $H(R_{g_{i_1}}\vee\dots\vee R_{g_{i_{l-v}}}/R_{x_{j_1}}\vee\dots\vee R_{x_{j_v}})>l-v-1$,

where H is the conditional entropy in uniform measure on the cube F^n, and the symbol $\vee$ is the atomization of partitionings (see [3]).

THEOREM 14.1 [6, Sec. 2]. Let the family $\{g_1,\dots,g_K\}$ satisfy the l-independence condition. Then for every SLP with storage S computing this family $ST\geq Kl/8$ is fulfilled.

In many of the results in the present section we encounter a lower bound on the product ST which can be looked upon as a certain analog of the uncertainty principle, called a time–space tradeoff for the storage (space) and time.

As an application of the theorem we get (see [16]) that $ST\geq n^2/16$ for the problem of multiplying n-th-degree polynomials (cf. Theorem 10.6) and $ST\geq n^3/8$ for the matrix multiplication problem (cf. Corollary 10.4 and Theorem 10.5).

In a number of subsequent papers the method of proof of Theorem 14.1 was generalized to arbitrary fields F. To state the generalization we restrict ourselves to the case of SLP with space S computing a family of linear forms, i.e., $P=\{+\}\cup\{xy\}_{y\in F}$ and we denote the function $\lambda=\lambda_t$ corresponding to the complexity measure (time or number of instructions) by T_{ad} (the subscript is the abbreviation of the word "additive"). The problem consists of estimating $T_{ad}(A_1,\dots,A_n)$, where $A_j=\sum_{1\leq i\leq n}\alpha_{ij}x_i$ is a linear form $(1\leq j\leq n)$. We denote the $n\times n$-matrix of coefficients of these forms by $A=(\alpha_{ij})$.

THEOREM 14.2 [58]. Let all minors (see [5]) of matrix A be nonzero. Then for every SLP with space S, computing the family $\{A_1,\dots,A_n\}$, there is fulfilled $ST_{ad}\geq n^2$.

The idea of the proof goes back to [6, 47, 48, 59] and relies on the concept of a superconcentrator (see [44, 59], for example), which is a certain strengthening of the concept of a concentrator introduced independently in [16, 43]. Superconcentrators played a significant role in the establishment of lower complexity bounds; therefore, we consider them here in somewhat greater detail.

Let G be a directed graph without directed loops (graphs of this type are precisely those which have a partial ordering at vertices, and we shall call them ordered graphs). Vertices of graph G into which arcs do not enter are called input vertices $w_1,\dots,w_n$; vertices of graph G from which arcs do not leave are called output vertices $v_1,\dots,v_m$. Let $m=n$. We say that G is an n-superconcentrator if for every $1\leq k\leq n$ and for every two k-element sets $I,J\subset\{1,\dots,n\}$, in graph G we can trace k directed paths pairwise nonintersecting at vertices, where the starts of the paths lie in I and the ends in J. The motivation for this definition will be clear from what follows.

Here and in the next section an extended construction which associates with every SLP β (of the usual type, as defined in Sec. 1) some ordered graph G_β will be useful (for example, see [6, 58, 59]). Graph G_β has n input vertices, one for each input variable $x_1,\dots,x_n$. Further, to each instruction $z_l=f(z_{i_1},\dots,z_{i_u},x_{j_1},\dots,x_{j_v})$ (see Sec. 1) there corresponds a vertex into which enter arcs from vertices corresponding to the working variables $z_{i_1},\dots,z_{i_u}$ and to the input variables $x_{j_1},\dots,x_{j_v}$ (thus, T is the number of noninput vertices of graph G_β). Having made trivial transformations, we can take it that the input vertices of graph G_β correspond precisely to functions computable by the SLP β. Below in the present section, by SLP we shall understand as well SLP with space, which can be looked upon as a special case of the usual SLP (forgetting about the restriction on the space).

LEMMA 14.3 [59]. If a SLP β computes a family of linear forms with an $n\times n$ coefficient matrix A all of whose minors are nonzero, then G_β is an n-superconcentrator.

We remark, as was shown in [16, 43, 44, 59], that there exists a family of n-superconcentrators with a number, linear in n, of edges (an upper bound of $29n$ on the number of edges is given in [44]); therefore, by itself Lemma 14.3 does not lead directly to nonlinear lower bounds on the complexity.

LEMMA 14.4 [58]. If β is a SLP with space S and G_β is an n-superconcentrator, then $ST\geq n^2$.

Theorem 14.2 now follows easily from these two lemmas.

As an application of the theorem (besides it, still other additional arguments are brought in to prove the results listed below) we cite the following examples:

COROLLARY 14.5. 1) [58] for the problem of multiplication on n-th-degree polynomials (over any field), $ST\geq n^2$;

2) [47, 58] for the computation of the discrete Fourier transform, i.e., of a family of linear forms with an $n\times n$ coefficient matrix $(\exp(2\pi ijk))_{1\leq j,k\leq n}$, there is fulfilled $ST\geq n^2$ (to eliminate possible ambiguities we remark that here $i^2=-1$);

3) [58, 39] for the multiplication of $n\times n$-matrices, $ST\geq n^3$, and for the inversion of $n\times n$-matrices, $ST\geq n^4$;

4) [48] for the multiplication of integers not exceeding 2^n (i.e., for finding the binary digits of the product of n-digit numbers) there is fulfilled $ST\geq n^2$.

15. Graph-Theoretic Methods in Algebraic Complexity

The applications of graph theory in algebraic complexity are based on the construction of the ordered graph G_β described in the preceding section. One such application (to the

establishment of the "uncertainty principle") was considered above (see Sec. 14). In the present section we set forth fewer applications of graph theory than in Sec. 14, but, in the author's opinion, the methods and the problem statements themselves are of interest.

We shall not begin (as we usually did above) by fixing the class of SLP β (i.e., the parameters from the definition in Sec. 1), since the main object of consideration will be the graph G_β. We shall merely assume that the complexity measure $C=C_\lambda$ is defined in terms of a function λ equal to unity (compare with total complexity; see Sec. 1) for each base operation from $\mathfrak{P}$ (i.e., $C(\beta)$ equals the number of noninput vertices of graph G_β). The number of input variables of the SLP is denoted by n. We note here one important difference in the construction of the graph $G=G_\beta$ from that presented in Sec. 14. Namely (this is based on the constraint (7) stated below on the class of SLP to be examined), we shall reckon that graph G can have more than n input vertices and that one input variable can correspond to several input vertices (this assumption only widens the class of admissible SLP).

In the first application with which we deal the graph $G=G_\beta$ will satisfy the following constraint (see [6, Sec. 1]). By T_v we denote the subgraph of graph G containing the vertices located in it above vertex v (and containing all arcs from G, both ends of which lie in these vertices), i.e., vertices from which there are directed paths to v (in the language of orderings T_v contains vertices less than or equal to v). The constraint is that

T_v is a tree for every vertex v. (7)

We say that the family of functions $\{g_1,\dots,g_m\}$ (according to what we said above, the nature of the functions is not essential) is (θ,η)-separable if for every SLP β, satisfying constraint (7) and computing the family $\{g_1,\dots,g_m\}$, when deleting any G_β vertices from graph θ we can find η different pairs of vertices such that one member of each pair is some input vertex of graph G_β and the other is an output vertex, and between the vertices — members of every pair — we can draw in G_β a path (according to (7) such a path is unique) not passing through the deleted vertices (informally speaking, even if θ arbitrary functions are used "free of charge," then for many indices $i(1\leq i\leq m)$ it is required to address many inputs for computing the output g_i). The concept formulated was already essentially contained in Sec. 1 of [6] and is very close to the concept of the $(n,\eta(\theta))$-*grate* proposed independently in [60].

The separability condition (just as the concept of *grate*) has been described in the language, constructed with respect to computable functions, of a sufficiently wide class of SLP, which, undoubtedly, complicates the verification of its fulfillment. In [60] there was cited a certain more intrinsic property of the family of linear forms $\{A_1,\dots,A_m\}$, under whose fulfillment this family is a *grate* (and satisfies as well the separability condition) for suitable values of parameters. To be precise, by A we denote the coefficient matrix of family $\{A_1,\dots,A_m\}$, and for every matrix $\mathfrak{D}$, such that $\operatorname{rg}\mathfrak{D}\leq\theta$, let there be no fewer than η nonzero elements in matrix $(A+\mathfrak{D})$. Then the family $\{A_1,\dots,A_m\}$ is (θ,η)-separable. Two open questions were posed in [60], whose essence reduces to the following (together they can be looked upon as some scheme along the way to obtaining lower bounds):

1) to construct (explicitly — compare with the beginning of Sec. 3) an example of a family of functions $\{g_1,\dots,g_m\}$ satisfying the (θ,η)-separability condition for "nontrivial" values of θ and η (for example, $\theta\times m,\eta\times mn$);

2) to show that the complexity $C(\beta)$ is nonlinear in $\max\{m,n\}$ for certain θ and η (we take it that β computes a family of functions satisfying the (θ,η)-separability condition).

The following theorem, due to the author, serves as a partial answer to Valiant's question 2); the method for proving this theorem is contained in Sec. 1 of [6] (it was proved there for the case $\theta\sim\frac{m}{2}$, $\eta\times mn$ and was stated in a less general form).

THEOREM 15.1. If the family $\{g_1,\dots,g_m\}$ is (θ,η)-separable, then for every SLP β computing this family and whose graph G_β satisfies constraint (7), there is fulfilled $C(\beta)\geqslant M$ where M is the unique positive solution of the equation

$$M=(\eta/m)^{\left(1+\frac{\theta}{M\ln 2}\right)}.$$

We remark that for $\theta\times m\times n$ and $\eta\times m^2$ there is fulfilled $M\times m\log m/\log\log m$. The method for proving the theorem was used as well in [7] to obtain lower bounds (now without constraints of type (7)) for the monotone complexity of a family of disjunctives (cf. Sec. 13).

In Sec. 1 of [6] we proposed applying the theorem to estimating the additive complexity of computing a family of linear forms over $\mathbb{R}$ (as before, under assumption (7)), where $P=\{+\}\cup\{x\gamma\}_{|\gamma|\leq 1}$; $\lambda_{11}=\lambda_t$ is the total complexity (see Sec. 1). Let the family of vectors $a_1,\dots,a_m\in\mathbb{R}^n$ be such that

$$\forall I(\varnothing\neq I\subsetneq\{1,\dots,m\}\Rightarrow\rho_1(\mathrm{Conv}\{a_i\}_{i\in I},\ \mathrm{Conv}\{a_j\}_{j\notin I})\geqslant c),$$

where Conv denotes the convex hull, ρ_1 is the metric corresponding to the norm $l_1(\alpha_1,\dots,\alpha_n)=\sum_{1\leq i\leq n}|\alpha_i|$ (in Sec. 1 of [6] such a family of vectors was called an (m,c)-system). On the basis of Radon's theorem (see [12]) it was shown in Sec. 1 of [6] that the family $a_1,\dots,a_m$ (having the stated property) satisfies an $(m/2,\ mc/4)$-separability condition in the situation being examined. Hence, by Theorem 15.1 we get that $C_{11}(a_1,\dots,a_m)\geqslant M$, where M is taken from the theorem for the parameters $\theta=m/2$, $\eta=mc/4$. It would be interesting to try a condition analogous to the one stated, to be used in situations where there are no theorems of the type of Helly's theorem ([12]) and there is not even a direct analog of convexity (in the case being considered Radon's theorem was actually used to answer Valiant's question 1 posed above).

A SLP over $\mathbb{R}$ (or $\mathbb{C}$) with the same P as in the preceding paragraph (here and below we can forget about condition (7)) was examined in [40] where it was noted that in case $m=n$ the complexity $C_{11}(a_1,\dots,a_n)\geqslant\log\det(a_1,\dots,a_n)$. The bound from the preceding paragraph is weaker, in the interesting cases, than Morgenstern's bound, but possibly the realization made of the path suggested in Valiant's questions 1) and 2) is of independent interest (recall Theorem 15.1).

In [61] Valiant gave another partial answer to the question 2) posed above. The largest length of a directed path in an ordered graph G is called the depth $d(G)$ of graph G.

THEOREM 15.2 [61]. For some $\varepsilon > 0$ let some (θ,η) -separable family, where $\eta \geq \theta^{1+\varepsilon}$, be computed by a SLP β for which the depth $d(G_\beta) = O(\log\theta)$. Then

$$C_t(\beta) \geq \theta \log\log\theta / \log\log\log\theta .$$

16. Additive Complexity in Triangular and Directed Computations and Bruhat Decomposition

In this last section we introduce two classes of SLP (triangular and directed), computing families of linear forms (see [35]). For triangular SLP a method for establishing nonlinear complexity lower bounds is proposed below. For directed computations, besides lower bounds, we propose, furthermore, an explicit formula for the complexity on the basis of the technique developed by the author in the theory of Chevalley groups (the information needed here is presented in such a way that no preliminary information on Chevalley groups is assumed).

Thus, we examine the following somewhat modified SLP. In the notation of Sec. 1, F is the ground field, $\{x_1,\dots,x_n\}$ are the input variables, $P = \{a \to a + \alpha b\}_{\alpha\in F} \cup \{x\alpha\}_{\alpha\in F}$. In matrix terminology, elementary operations correspond naturally to these instructions. There are also N variables $z_1,\dots,z_N$ (which can be treated as storage) from which we can pick out n variables $z_{i_1},\dots,z_{i_n}$ $(1 \leq i_1 < \dots < i_n \leq N)$, which are called basic (the rest are called auxiliary). The SLP β itself is a sequence of rows, and for every $1 \leq t \leq T$ and $1 \leq j \leq N$ there is naturally determined by induction on t (analogously to Sec. 14) a linear form $Z_j^{(t)}$ in the variables $x_1,\dots,x_n$ with coefficients from F. At the initial instant $(t=0)$ we set $Z_{i_j}^{(0)} = x_j$ $(1 \leq j \leq n)$ for the basic variables and $Z_j^{(0)} = 0$ $(j \neq i_1,\dots,i_n)$ for the auxiliary ones. By definition we take it that β computes the family of n linear forms $Z_{i_1}^{(T)},\dots,Z_{i_n}^{(T)}$. This restriction, i.e., reckoning at the end of the computation of the outputs at the place where there were inputs at the initial instant, which is not essential for SLP of general form, is very important in our case.

At first we turn to triangular computations. By definition, every instruction of a triangular SLP β has the form $z_j = z_j + \alpha z_i$, where $i > j$ or $z_j = \alpha z_j$ $(\alpha \in F)$. These instructions (in matrix language) correspond to upper-triangular elementary transformations. We set the function $\lambda = \lambda_\Delta$ (see Sec. 1) equal to one on instructions of the first type and to zero on instructions of the second type. The complexity measure C_Δ resulting here (see Sec. 1) is called triangular. If A is an $n \times n$ -matrix of the coefficients of the family of linear forms $a_1,\dots,a_n$, then we denote $C_\Delta(A) = C_\Delta(a_1,\dots,a_n)$. We remark that in justification of its name the triangular complexity $C_\Delta(A)$ has been defined only for upper-triangular matrices A (i.e., matrices with zeros below the diagonal).

THEOREM 16.1 [35]. Let an upper-triangular matrix A be represented in the form $A = \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}$, where A_1, A_2 are upper-triangular. Then

$$C_\Delta(A) \geq C_\Delta(A_1) + C_\Delta(A_2) + \operatorname{rg} B .$$

As an application of the theorem we consider a family of upper-triangular matrices $\{A_n\}$, where $A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \dots, A_{n+1} = \begin{pmatrix} A_n & E \\ 0 & A_n \end{pmatrix}, \dots$; here E is the unit matrix (i.e., A_n has the dimension $2^n \times 2^n$). Then we have

COROLLARY 16.2 [35]. $C_\Delta(A_n) = n \cdot 2^{n-1}$.

In other words, the growth of the triangular complexity $C_\Delta(A_n)$ is nonlinear in the dimension of the matrices.

The second class of SLP which we consider here is that of directed SLP. Every instruction of a directed SLP β has the form

$$z_{K+1} = z_{K+1} + \alpha z_K \quad \text{or} \quad z_j = z_j + \alpha z_i \ , \ \text{where} \ j \leq i \ (\alpha \in F).$$

We set the function $\lambda = \lambda_d$ equal to unity on instructions of the first type and to zero on instructions of the second type. The complexity measure C_d resulting here (see Sec. 1) is called directed. In contrast to triangular complexity, the directed complexity $C_d(A)$ (we use the notation introduced above) is defined for any quadratic $(n \times n)$ matrix A.

For $C_d(A)$ it is not difficult to obtain nonlinear (in n) lower bounds, but we have succeeded in doing considerably more: to obtain an explicit formula for $C_d(A)$. To state this result we need certain preliminary information, which we now present.

Let S_n be a symmetric group (i.e., the group of all permutations of an n-element set) which we shall simultaneously treat as a subgroup of the group GL_n of nonsingular matrices (all matrices encountered here and later are of dimension $n \times n$). By T we denote the manifold of upper-triangular matrices and by $B = T \cap GL_n$ the subgroup of all nonsingular upper-triangular matrices. A Bruhat decomposition (see Sec. 3 of [20]) consists in that for every matrix $A \in GL_n$ there exists and is unique a permutation $w_A \in S_n$ such that $A \in B w_A B$. On group S_n there is defined (see Sec. 1 of Chap. 4 in [4]) a length function $l(w)$, where $w \in S_n$, as the smallest l such that $w = \sigma_{j_1} \dots \sigma_{j_l}$, where $\sigma_j = (j \ j+1)$ is the transposition of two adjacent indices $(1 \leq j < n)$. Every decomposition of w into a product of transpositions of form σ_j with the smallest number of factors equal to $l = l(w)$ is called reduced. It is easy to see that $l(w)$ coincides with the number of inversions in w , i.e., the number of pairs $i < j$ for which $w(i) > w(j)$. We denote $l(A) = l(w_A)$, we define the function l on GL_n (on nonsingular matrices).

On group S_n we introduce (see Sec. 8 of [20]) the relation $\leq$ of partial ordering: $w_1 \leq w_2 \ (w_1, w_2 \in S_n)$ if w_1 equals some subproduct (with preservation of order of factors) of some reduced decomposition of element w_2 . It can be shown (see Sec. 8 of [20]) that the determination of the order is independent of the choice of the reduced decomposition of w_2 . The order shows its worth in the following theorem (see Sec. 8 of [20]): $\overline{BwB} = \bigcup_{w_1 \leq w} B w_1 B$, where the bar signifies closure in the Zariski topology (here it is assumed that field F is infinite). As follows from the Bruhat decomposition, under the union sign there stand pairwise-nonintersecting sets.

It is easy to see that $C_d(A) \leq l(A)$ for nonsingular matrices A . In order to establish the reverse inequality, the author had to extend the function l from GL_n to M_n (M_n denotes the manifold of all $n \times n$ -matrices), to prove an analog of the Bruhat decomposition (see Theorem 16.3 below) and an analog of the Chevalley theorem (see Corollary 16.4 below) for M_n , then to establish a certain monotonicity property of the resultant function l (see Lemma 16.5 below), and, finally, to prove the equality $C_d(A) = l(A)$ now for all $A \in M_n$.

THEOREM 16.3 [11, 35]. For every $A \in \mathcal{M}_n$ there exists and is unique a permutation $w_A \in S_n$ such that:

1) $A \in \mathcal{T} w_A \mathcal{T}$;

2) if $A \in \mathcal{T} w \mathcal{T}$ for some $w \in S_n$, then $w_A \preccurlyeq w$.

Permutation w_A is constructed in time $O(n^3)$ from A. Now, on the theorem's basis we can extend function ℓ to $\mathcal{M}_n$, having set $\ell(A) = \ell(w_A)$.

COROLLARY 16.4 [11, 35]. 1) $\overline{\mathcal{T} w \mathcal{T}} = \bigcup_{w_1 \preccurlyeq w} \mathcal{T} w_1 \mathcal{T}$;

2) function ℓ is upper-semicontinuous on $\mathcal{M}_n$.

In contrast to the nonsingular case, the sets occurring in the union in item 1) of the corollary may intersect.

We say that the $n \times n$ -matrix A is a principal submatrix of the $m \times m$ -matrix D $(n \leqslant m)$, if A is a submatrix of matrix D and its diagonal lies on the diagonal of matrix D; in other words, submatrix A is picked out from matrix D with the aid of rows and columns having one and the same indices.

LEMMA 16.5 [11, 35]. If A is a principal submatrix of matrix D, then $\ell(A) \leqslant \ell(D)$.

Finally, having proved a number of assertions for function ℓ (see [11, 35]) and relying on 16.3, 16.4, 16.5, we obtain as a result the promised explicit formula for $C_d(A)$.

THEOREM 16.6 [35]. $C_d(A) = \ell(A)$.

We remark that Theorems 16.3 and 16.6 and Lemma 16.5 are true also over a finite ground field F.

In conclusion, we mention that Theorem 16.3 and Corollary 16.4, and partially also Lemma 16.5, generalize (in invariant form) to arbitrary classical Chevalley groups ([11]).

LITERATURE CITED

1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley, Reading, MA (1974).
2. D. N. Bernshtein, "The number of roots of a system of equations," Funkts. Anal. Prilozhen., 9, No. 3, 1-4 (1975).
3. P. Billingsley, Ergodic Theory and Information, Wiley, New York (1965).
4. N. Bourbaki, Éléments de Mathématique. Groupes et Algèbres de Lie. Chapitres 4, 5, et 6, Masson, Paris (1981).
5. F. R. Gantmakher, The Theory of Matrices, Chelsea Publ., New York (1959).
6. D. Yu. Grigor'ev, "Application of separability and independence notions for proving lower bounds of circuit complexity," J. Sov. Math., 14, No. 5, 1450-1456 (1980).
7. D. Yu. Grigor'ev, "On a lower bound of the computation complexity of a family of disjunctives in a monotone basis," J. Sov. Math., 15, No. 1, 11-13 (1981).
8. D. Yu. Grigor'ev, "Rank of a pair of matrices and convolutions," Usp. Mat. Nauk, 34, No. 2, 193-194 (1979).
9. D. Yu. Grigor'ev, "Algebraic computational complexity of a family of bilinear forms," Zh. Vyshisl. Mat. Mat. Fiz., 19, No. 3, 563-580 (1979).
10. D. Yu. Grigor'ev, "Relation of rank and multiplicative complexity of a bilinear form over a Noetherian commutative ring," J. Sov. Math., 17, No. 4, 1987-1998 (1981).
11. D. Yu. Grigor'ev, "Analog of the Bruhat decomposition for the closure of the cone of the Chevalley group of a classical series," Dokl. Akad. Nauk SSSR, 257, No. 5, 1040-1044 (1981).
12. L. Danzer, B. Grünbaum, and V. Klee, Helly's Theorem and Its Relatives, Proc. Sympos. Pure Math., Vol. VII, Am. Math. Soc., Providence, RI (1963), pp. 101-180.
13. D. E. Knuth, The Art of Computer Programming, Vol. 2, Addison-Wesley, Reading, MA (1973).
14. S. MacLane, Homology, Springer-Verlag, Berlin (1963).
15. Yu. I. Manin, Lectures on Algebraic Geometry. Part I: Affine Schemes, Moscow State Univ. (1970).

16. G. A. Margulis, "Explicit construction of concentrators," Probl. Peredachi Inf., 9, No. 4, 71-80 (1973).
17. M. V. Mikhailyuk, "On the computational complexity of elementary symmetric functions in finite fields," Dokl. Akad. Nauk SSSR, 244, No. 5, 1072-1076 (1979).
18. V. Ya. Pan, "On methods for computing the values of polynomials," Usp. Mat. Nauk, 21, No. 1, 103-134 (1966).
19. W. W. Peterson, Error-Correcting Codes, MIT Press, Cambridge, MA (1962).
20. R. Steinberg, Lectures on Chevalley Groups, Yale Univ. Notes, New Haven, CT (1967).
21. A. G. Khovanskii, "On a class of systems of transcendental equations," Dokl. Akad. Nauk SSSR, 255, No. 4, 804-807 (1980).
22. A. Schönhage and V. Strassen, "Schnelle Multiplikation Großer Zahlen," Computing (Arch. Elektron. Rechnen), 7, 281-292 (1971).
23. V. Strassen, "Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten," Numer. Math., 20, 238-251 (1972/73).
24. A. Alder and V. Strassen, "On the algorithmic complexity of associative algebras," Theor. Comput. Sci., 15, 201-211 (1981).
25. W. Baur and V. Strassen, "The complexity of partial derivatives," Preprint Univ. Zurich (1981).
26. A. Borodin and S. Cook, "On the number of additions to compute specific polynomials," SIAM J. Comput., 5, No. 1, 146-157 (1976).
27. A. Borodin and I. Munro, The Computational Complexity of Algebraic and Numeric Problems, Elsevier, New York (1975).
28. M. R. Brown and D. P. Dobkin, "An improved lower bound on polynomial multiplication," IEEE Trans. Comput., C-29, No. 5, 337-340 (1980).
29. D. Coppersmith and S. Winograd, "On the asymptotic complexity of matrix multiplication," SIAM J. Comput., 11, 472-492 (1982).
30. P. van Emde Boas, "Berekeningskomplexiteit van bilineaire en kwadratische vormen," Preprint Univ. van Amsterdam (1980).
31. C. M. Fiduccia and Y. Zalcstein, "Algebras having linear multiplicative complexity," J. Assoc. Comput. Mach., 24, No. 2, 311-331 (1977).
32. D. Yu. Grigor'ev, "Some new bounds on tensor rank," LOMI Preprint E-2-78, Leningrad (1978).
33. D. Yu. Grigor'ev, "Multiplicative complexity of a pair of bilinear forms and of the polynomial multiplication," in: Mathematical Foundations of Computer Science 1978, J. Winkowski (ed.), Lect. Notes Comput. Sci., 64, Springer-Verlag, Berlin–Heidelberg–New York (1978), pp. 25-256.
34. D. Yu. Grigor'ev, "Multiplicative complexity of a bilinear form over a commutative ring," in: Mathematical Foundations of Computer Science 1981, J. Gruska and M. Chytil (eds.), Lect. Notes Comput. Sci., 118, Springer-Verlag, Berlin–Heidelberg–New York (1981), pp. 281-286.
35. D. Yu. Grigor'ev, "Additive complexity in directed computations," Theor. Comput. Sci., 19, No. 1, 39-67 (1982).
36. J. Heintz and M. Sieveking, "Lower bounds for polynomials with algebraic coefficients," Theor. Comput. Sci., 11, No. 3, 321-330 (1980).
37. L. Hyafil, "The power of commutativity," 18th Ann. Sympos. Foundations Comput. Sci., IEEE Computer Soc., Long Beach, CA (1977), pp. 171-174.
38. J. Ja' Ja', "Optimal evaluation of pairs of bilinear forms," Conf. Record Tenth Ann. ACM Sympos. Theory Comput., Assoc. Comput. Mach., New York (1978), pp. 173-183.
39. J. Ja' Ja', "Time–space tradeoffs for some algebraic problems," Conf. Proc. Twelfth Ann. ACM Sympos. Theory Comput., Assoc. Comput. Mach., New York (1980), pp. 339-350.
40. J. Morgenstern, "Note on a lower bound of the linear complexity of the fast Fourier transform," J. Assoc. Comput. Mach., 20, No. 2, 305-306 (1973).
41. V. Ya. Pan, "Computational complexity of computing polynomials over the fields of real and complex numbers," Conf. Record Tenth Ann. ACM Sympos. Theory Comput., Assoc. Comput. Mach., New York (1978), pp. 162-172.
42. M. S. Paterson and L. J. Stockmeyer, "On the number of nonscalar multiplications necessary to evaluate polynomials," SIAM J. Comput., 2, 60-66 (1973).
43. M. S. Pinsker, "On the complexity of a concentrator," Seventh Int. Teletraffic Congr., Stockholm (1973).
44. N. Pippenger, "Superconcentrators," SIAM J. Comput., 6, No. 2, 298-304 (1977).
45. N. Pippenger, "Computational complexity in algebraic function fields (preliminary version)," 20th Ann. Sympos. Foundations Computer Sci., IEEE Computer Soc., New York (1979), pp. 61-65.

46. J. E. Savage, "An algorithm for the computation of linear forms," SIAM J. Comput., 3, No. 2, 150-158 (1974).
47. J. E. Savage and S. Swamy, "Space–time tradeoffs on the FFT algorithm," IEEE Trans. Inf. Theory, IT-24, No. 5, 563-568 (1978).
48. J. E. Savage and S. Swamy, "Space–time tradeoffs for oblivious sorting and integer multiplication," Tech. Rep. CS-32, Brown Univ., Providence, RI (1978).
49. C. P. Schnorr, "A lower bound on the number of additions in monotone computations," Theor. Comput. Sci., 2, 305-315 (1976).
50. C. P. Schnorr, "On the additive complexity of polynomials and some new lower bounds," in: Theoretical Computer Science, Lect. Notes Comput. Sci., K. Weihrauch (ed.), Vol. 67, Springer-Verlag, Berlin–Heidelberg–New York (1979), pp. 286-297.
51. C. P. Schnorr and J. P. Van de Wiele, "On the additive complexity of polynomials," Theor. Comput. Sci., 10, 1-18 (1980).
52. A. Schönhage, "Partial and total matrix multiplication," SIAM J. Comput., 10, No. 3, 434-455 (1981).
53. M. I. Shamos and G. Yuval, "Lower bounds from complex function theory," 17th Ann. Sympos. Foundations Comput. Sci., IEEE Computer Soc., Long Beach, CA (1976), pp. 268-273.
54. V. Strassen, "Vermeidung von Divisionen," J. Reine Angew. Math., 264, 184-202 (1973).
55. V. Strassen, "Polynomials with rational coefficients that are hard to compute," SIAM J. Comput., 3, No. 2, 128-149 (1974).
56. V. Strassen, "Computational complexity over finite fields," SIAM J. Comput., 5, No. 2, 324-331 (1976).
57. V. Strassen, "The computational complexity of continued fractions," Proc. 1981 ACM Sympos. Symbolic and Algebraic Comput., Assoc. Comput. Mach., New York (1981), pp. 51-67.
58. M. Tompa, "Time–space tradeoffs for computing functions, using connectivity properties of their circuits," Conf. Record Tenth Ann. ACM Sympos. Theory Comput., Assoc. Comput. Mach., New York (1978), pp. 196-204.
59. L. G. Valiant, "On nonlinear lower bounds in computational complexity," Seventh Ann. ACM Sympos. Theory Comput., Assoc. Comput. Mach., New York (1975), pp. 45-53.
60. L. G. Valiant, "Some conjectures relating to superlinear complexity bounds," Tech. Rep. N 85, Univ. Leeds (1976).
61. L. G. Valiant, "Graph-theoretic arguments in low-level complexity," Comput. Sci. Rep. 13-77, Univ. Edinburgh (1977).
62. L. G. Valiant, "Negation can be exponentially powerful," Teor. Comput. Sci., 12, 303-314 (1980).
63. J. P. Van de Wiele, "Complexité additive et zéros des polynômes à coefficients réels et complexes," Proc. First Meet. AFCET-SMT Appl. Math. (1978).
64. S. Winograd, "On the number of multiplications necessary to compute certain functions," Commun. Pure Appl. Math., 23, 165-179 (1970).

(The results were announced January 21 and 23, 1981.)