JOURNAL OF COMPLEXITY **16**, 2–49 (2000)
doi:10.1006/jcom.1999.0526, available online at http://www.idealibrary.com on IDEAL®

Time-Space Tradeoffs in Algebraic Complexity Theory

M. Aldaz

Departamento de Matemática e Informática, Universidad Pública de Navarra, E-31006 Pamplona, Spain
E-mail: mikaldaz@unavarra.es

J. Heintz

Depto. de Matemáticas, Est. y Comp., Fac. de Ciencias, Universidad de Cantabria, E-39071 Santander, Spain; and Departamento de Matemática, Universidad de Buenos Aires, Ciudad Universitaria, Pab. I (1428) Buenos Aires, Argentina
E-mail: heintz@hall.matesco.unican.es, joos@mate.dm.uba.ar

G. Matera

Laboratorio de Computación, Universidad Favaloro, Solís 453 (1078) Buenos Aires, Argentina; and Instituto de Desarrollo Humano, Universidad Nacional de Gral. Sarmiento, Roca 850 (1663) San Miguel, Argentina
E-mail: gmatera@favaloro.edu.ar, gmatera@ungs.edu.ar

J. L. Montaña

Departamento de Matemática e Informática, Universidad Pública de Navarra, E-31006 Pamplona, Spain
E-mail: pepe@unavarra.es

and

L. M. Pardo

Depto. de Matemáticas, Est. y Comp., Fac. de Ciencias, Universidad de Cantabria, E-39071 Santander, Spain
E-mail: pardo@hall.matesco.unican.es

Received November 15, 1998

We exhibit a new method for showing lower bounds for time-space tradeoffs of polynomial evaluation procedures given by straight-line programs. From the tradeoff results obtained by this method we deduce lower space bounds for polynomial evaluation procedures running in optimal nonscalar time. Time, denoted by L, is measured in terms of nonscalar arithmetic operations and space, denoted by S, is measured by the maximal number of pebbles (registers) used during the given evaluation procedure. The time-space tradeoff function considered in this paper is

0885-064X/00 $35.00

LS^2. We show that for "almost all" univariate polynomials of degree at most d our time-space tradeoff functions satisfy the inequality $LS^2 \geqslant \frac{d}{8}$. From this we conclude that for "almost all" degree d univariate polynomials, any nonscalar time optimal evaluation procedure requires space at least $S \geqslant c\sqrt[4]{d}$, where $c > 0$ is a suitable universal constant. The main part of this paper is devoted to the exhibition of specific families of univariate polynomials which are "hard to compute" in the sense of time-space tradeoff (this means that our tradeoff function increases linearly in the degree).

Key Words: pebble game; time-space tradeoff; straight-line program; elimination theory.

1. INTRODUCTION

Computer oriented algorithmics often requires simultaneos optimization of more than one complexity measure. Although it is not easy to capture the programming reality in a theoretical model one feels compelled at least to attempt an effort in this direction. In this sense the present paper is devoted to the interplay between the (computational) issue of time and (necessary) space in the particular case of (numeric) evaluation of univariate polynomials. Our theoretical model is that of arithmetic circuits represented by directed acyclic graphs (DAGs) on which we play a pebble game (see the surveys [45, 49, 6]). Thus arithmetic operations are counted at unit cost and an intermediate result of our computation, mathematically being represented by a rational function, occupies just one unit of memory space when it is stored. More specifically when measuring time we shall take only nonscalar multiplications/divisions into account, linear operations, in particular additions, are free. This coarsening of the computational model is due to technical reasons and acceptable since we are interested just in *lower* bounds for the tradeoff between computation time and memory space necessary to evaluate a given univariate polynomial. A particularity of our model is that any polynomial can be evaluated in constant memory space (as one easily sees when analyzing Horner's rule, see also [4, 38] for more general results in this direction). However computation time cannot be compressed arbitrarily in polynomial evaluation, the logarithm of the degree being a universal lower bound. This motivates the study of *time-space tradeoffs* or alternatively the behaviour of memory space under the assumption of a time optimal algorithm. As said before our basic algorithmic model for time and space is that of a pebble game played on an arithmetic circuit represented by a DAG. There exists another model well suited for our purpose, which is not considered here, namely that of a branching program (see [6]). The reason for the omission of this model is that straight-line programs, although less relevant in computer science than branching programs, are better suited for the technical tools we are going to apply in this paper. These technical tools come mainly from geometric

and arithmetic intersection theory (see, e.g., [25, 18, 17, 27, 40, 34] and the references cited therein). For a similar reason (uniformity assumptions do not help for our techniques) we do not consider modeling of time and space by Turing machines.

Straight-line programs have been used in the past extensively in order to show lower bounds for time-space tradeoffs of many problems of different computational nature and taste. Examples of such problems with significant results are: sorting [57], language recognition [16], algebraic problems such as convolution, matrix-vector products and discrete Fourier transform [57, 47], binary integer multiplication [48], matrix multiplication and inversion, iterated matrix multiplication [24, 31, 46], range queries [61, 58]. The general question, namely whether it is possible to find efficient tradeoffs between time and space while pebbling an *arbitrary* (not necessarily computation) DAG was considered and negatively answered in [35, 42, 44].

The rather combinatorial branching program model is powerful enough to produce relevant lower bounds for time-space tradeoffs of algebraic problems. Results in this direction can be found in [63], where lower bounds for the time-space tradeoff of the discrete Fourier transform in the branching program model are established, and in [1], where such lower bounds for a large list of computational problems are given. This problem list includes the task of computing the convolution of two vectors, computing a matrix-vector product, matrix multiplication, matrix inversion, computing the product of three matrices and integer multiplication. Lower bounds for time-space tradeoffs in the branching program model are known in the case of the following counting problems: sorting [9, 7], element distinctness [8, 62] and finding unique elements [3].

In this paper we are concerned with the time-space complexity of evaluating univariate polynomials and the computation model we use is that of straight-line programs (or DAGs) together with pebble games played on them. Our method for obtaining lower bounds for time-space tradeoffs for polynomial evaluation is based on a geometrical interpretation of the notion of a straight-line program of given nonscalar time L and space S (see Section 2, Definitions 2, 3, and Lemmata 4, 5, 6).

First of all let us observe that the computation DAG associated to Horner's rule for the evaluation of an univariate polynomial P of degree d can be pebbled using exactly two pebbles in total time $2d$ and nonscalar time d. Let L and S denote nonscalar time and space used by the Horner algorithm for the evaluation of the polynomial P. With this notation we obtain the following obvious time-space tradeoff upper bound for the evaluation of the polynomial P:

$$L \cdot S^2 = 4 \cdot d.$$

Using a simple counting argument we show in Section 2 that this upper bound is, asymptotically, exact for almost all univariate degree d polynomials. In analogy with [55, 30, 20, 26] we call such polynomials *hard to compute* in terms of tradeoff.

In Section 3 we develop a global strategy which we shall follow in Section 4 to exhibit *specific* families of univariate polynomials which are hard to compute in the sense of time-space tradeoff. The new aspect of our strategy consists in a problem adapted analysis of the height of points lying on the fiber of a given $\mathbb{Q}$-definable algebraic morphism of affine spaces. The conclusions of this analysis constitute our main tool to establish time-space tradeoffs for univariate polynomials with integer coefficients (see Proposition 9). The case of polynomials with algebraic coefficients is treated using an adaptation of the degree method of [30] (see also [29, 27]). The following time-space tradeoff lower bounds are presented in Section 4:

(1) Polynomials with integer coefficients of the form $\sum_{0 \leqslant j \leqslant d} 2^{j!} X^j$ have a time-space tradeoff $LS^2 = \Omega(d)$.

(2) Polynomials with integer coefficients of the form $\prod_{1 \leqslant j \leqslant d} (X - 2^{2^j})$ have a time space tradeoff $LS^2 = \Omega(d/\log_2 d)$.

(3) Polynomials with algebraic coefficients of the form $\sum_{1 \leqslant j \leqslant d} \sqrt{p_j}\, X^j$ have a time-space tradeoff $LS^2 = \Omega(d/\log_2 d)$. (Here p_j denotes the jth prime number.)

(4) Polynomials with algebraic coefficients of the form $\prod_{1 \leqslant j \leqslant d} (X - \sqrt{p_j})$ have a time-space tradeoff $LS^2 = \Omega(d/\log_2 d)$.

In all these examples L denotes the number of nonscalar multiplications/divisions and S the number of pebbles (registers) used when evaluating the polynomial under consideration by a given straight-line program. Our time-space tradeoff results imply that any *nonscalar time optimal* algorithm which evaluates any of the mentioned polynomial families needs roughly space $S = \Omega(\sqrt[4]{d})$ (see Proposition 26). Finally let us observe that to our knowledge our method is the first one which is able to produce time-space tradeoff lower bounds for algebraic computation problems with just *one* output.

2. TIME AND SPACE FOR ARITHMETIC CIRCUITS

In this section we discuss how the complexity measures time and space can be suitably represented in our basic model of computation, namely the random access model of straight-line programs (also called arithmetic circuits). Intuitively one would say that computational time and space of a straight-line program find a natural representation playing a pebble game on the underlying computation graph (see, e.g., [6]). However, this combinatorial definition of our complexity measures is not well suited for the application of geometric methods to proofs of lower complexity bounds—the main subject of this paper.

For this reason we are going to transform the pebble game complexity model first in a register allocation model and then the register allocation model in a geometric model of computation.

2.1. *From the Pebble Game Complexity Model to the Register Allocation Model*

Let K be an infinite field and let $X_1, ..., X_n$ be indeterminates over K. By $K[X_1, ..., X_n]$ we denote the ring of n-variate polynomials over K and by $K(X_1, ..., X_n)$ its fraction field.

Let F be an element of $K(X_1, ..., X_n)$, i.e., a rational function over the field K in the variables $X_1, ..., X_n$. Let us recall the following standard notions of algebraic complexity theory (see [10; 56; 54; 26; 19; 40; 12, Chap. 4]).

DEFINITION 1. A straight-line program in $K(X_1, ..., X_n)$ which computes the rational function F is a sequence $\beta = (Q_1, ..., Q_r)$ of elements of the field $K(X_1, ..., X_n)$ with the following properties

(1) $Q_r = F$,

(2) for any $1 \leqslant \rho \leqslant r$, the rational function Q_ρ belongs to $K \cup \{X_1, ..., X_n\}$ or there exist $1 \leqslant \rho_1, \rho_2 < \rho$ and an arithmetic operation op_ρ in $\{+, -, *, /\}$ such that $Q_\rho = Q_{\rho_1}\, op_\rho\, Q_{\rho_2}$ holds.

The rational functions $Q_1, ..., Q_r$ are called intermediate results of the straight-line program β and the rational function $F = Q_r$ is called final result or output of β. In the sequel we shall assume without loss of generality that all intermediate results $Q_1, ..., Q_r$ of β are non-zero.

To a given straight-line program $\beta = (Q_1, ..., Q_r)$ in $K(X_1, ..., X_n)$ we associate as usually a labeled *directed acyclic graph* (computation *DAG* for short) which we denote by $\Gamma(\beta)$ and which we call the *computation graph* of the straight-line program β. The computation graph $\Gamma(\beta)$ has r vertices called nodes (or gates). Each node of $\Gamma(\beta)$ has indegree 0 or 2 and is labeled by an element of $K \cup \{X_1, ..., X_n\}$ in the first case and by an arithmetic operation in the latter case. Nodes of indegree 0 are called *source nodes* of $\Gamma(\beta)$. Source nodes labeled by a variable $X_1, ..., X_n$ are called *input nodes* and source nodes labeled by an element of K are called *parameter nodes*. The elements of K occurring in that way are called *parameters* of the computation graph $\Gamma(\beta)$ (or of the straight-line program β).

The nodes of $\Gamma(\beta)$ are numbered by $1 \leqslant \rho \leqslant r$. If for a node ρ of $\Gamma(\beta)$ there exist nodes $1 \leqslant \rho_1, \rho_2 < \rho$ and an arithmetic operation op_ρ such that $Q_\rho = Q_{\rho_1}\, op_\rho\, Q_{\rho_2}$ holds, then the node ρ is labeled by op_ρ, its indegree is 2 and $\Gamma(\beta)$ contains directed edges leading from the vertices ρ_1 and ρ_2 to the vertex ρ (the nodes ρ_1 and ρ_2 are called *predecessor nodes* of ρ). The nodes

which are not source nodes are called *internal nodes* of $\Gamma(\beta)$. The node r is called *output node* of the computation graph $\Gamma(\beta)$.

To each node ρ of $\Gamma(\beta)$ we associate the rational function Q_ρ appearing in the sequence β as intermediate result. This rational function is recursively computed by the graph $\Gamma(\beta)$ starting with the source nodes. In particular the rational function which corresponds to the output node r is $Q_r = F$.

We call a node ρ of $\Gamma(\beta)$ *nonscalar* if it has the following property: the node ρ has indegree 2, the arithmetic operation op_ρ is a multiplication or division and the intermediate results Q_{ρ_1}, Q_{ρ_2} of β associated to the predecessors nodes ρ_1, ρ_2 of ρ satisfy the condition $Q_{\rho_1}, Q_{\rho_2} \notin K$ if op_ρ is a multiplication and the condition $Q_{\rho_2} \notin K$ if op_ρ is a division.

On the directed acyclic graph $\Gamma(\beta)$ we may play a pebble game subject to the following rules (see [6]):

(P1) any source node can be pebbled,

(P2) if the predecessor nodes of a given node ρ of $\Gamma(\beta)$ are both pebbled, then ρ can be pebbled by a new pebble or just by moving a pebble from one of the predecessor nodes to ρ,

(P3) a pebble can always be removed from a pebbled node of $\Gamma(\beta)$.

The pebble game finishes when the output node of $\Gamma(\beta)$ is pebbled. In general various distinct pebble games can be played on a given computation graph $\Gamma(\beta)$. That means that the computation graph $\Gamma(\beta)$ typically does not admit just one pebble game, or with other words: pebble games are not uniquely determined by the underlying DAG.

For a particular pebble game on a given computation graph $\Gamma(\beta)$ we have the following complexity measures:

(C1) a *space* measure given by the maximum number of pebbles used at any moment of the game,

(C2) a *total time* measure given by the number of pebble placements performed during the game following rules (P1) and (P2),

(C3) a *nonscalar time* measure given by the number of pebble placements on the nonscalar nodes of $\Gamma(\beta)$ performed during the game following the rule (P2).

We extend our notion of straight-line program as follows: *from now on we shall understand by a straight-line program an arithmetic circuit β in the sense of Definition* 1 *together with a fixed pebble game played on its computation graph $\Gamma(\beta)$. We use the same notation, namely β, for the new mathematical object: the straight-line program together with a fixed pebble game.*

We introduce the following combinatorial complexity model which reflects sequential time and space in our arithmetic setting:

DEFINITION 2. Let $F \in K(X_1, ..., X_n)$ be a rational function. A straight-line program in the field of rational functions $K(X_1, ..., X_n)$ which evaluates

F using total time T, nonscalar time L and space S is a straight-line program β for F in the sense of Definition 1 together with a pebble game played on $\Gamma(\beta)$ in total time T, nonscalar time L and space S, where these complexity measures are determined following the conditions (C2), (C3), and (C1).

In this way we obtain a purely combinatorial complexity model measuring total and nonscalar time and space playing a pebble game on a computation DAG. Next, we are going to construct a register allocation model for our general purpose of deriving lower bounds on time-space tradeoffs for polynomial evaluation.

Suppose that there is given a straight-line program β as above together with its computation graph $\Gamma(\beta)$. Suppose furthermore that there is given a pebble game on $\Gamma(\beta)$ which uses S pebbles say 1, ..., S and which can be played in total time T on the graph $\Gamma(\beta)$. In what follows we think the pebble game given as a time sequence of T register allocation instructions in which the new variables $R_1, ..., R_S$ appear as names of registers. The register allocation instructions are labeled by the symbols (1), ..., (T). We introduce them as follows:

1. If at time $1 \leqslant t \leqslant T$ of the game a source node ρ of $\Gamma(\beta)$ is pebbled following rule (P1) by pebble $1 \leqslant j \leqslant S$, then the register allocation instruction (t) has the form

$$R_j := X_i$$

in case that node ρ is labeled by the input variable X_i. In case that node ρ is labeled by the parameter $\alpha \in K$ the register allocation instruction (t) has the form

$$R_j := \alpha.$$

2. If at time $1 \leqslant t \leqslant T$ of the game the internal node ρ of $\Gamma(\beta)$ is pebbled following rule (P2) by pebble $1 \leqslant j \leqslant S$, then the register allocation instruction (t) has the form

$$R_j := R_k \, op_\rho \, R_l,$$

where op_ρ is the arithmetic operation associated with the node ρ and $1 \leqslant k, l \leqslant S$ are the pebbles already placed on the predecessor nodes ρ_1, ρ_2 of ρ.

According to the register allocation rules just introduced we may redefine the notion of a straight-line program of total time T (respectively nonscalar time L) and space S in the following way:

DEFINITION 3. A straight-line program β in $K(X_1, ..., X_n)$ using total time T and space S is a sequence of register allocation instructions labeled (1), ..., (T) such that for each $1 \leqslant t \leqslant T$ instruction (t) is one of the following two types:

(i) $R_j := a$ with $a \in K \cup \{X_1, ..., X_n\}$ and $1 \leqslant j \leqslant S$,

(ii) $R_j := R_k \; op \; R_l$ with $op \in \{+, -, *, /\}$ and $1 \leqslant k, l, j \leqslant S$.

Here $R_1, ..., R_S$ are the (distinct) register variables the straight-line program β uses.

The *total time* used by the straight-line program β is therefore the number T of register allocation instructions it contains. The *nonscalar time* used by β (or its *nonscalar length*) is the number of register allocation instructions of the form (ii) occurring in β which are subject to the following restrictions: the arithmetic operation op is a multiplication or division, the contents of the registers R_k, R_l—to be introduced below—do not belong to the parameter domain K in case op is a multiplication and the content of the register R_l does not belong to K if op is a division. In the sequel we shall write $L(\beta)$ for the *nonscalar time* and $S(\beta)$ for the *space* used by the straight-line program β.

Given a straight-line program β in the sense of Definition 3 one may define in the most obvious way for any time instance $1 \leqslant t \leqslant T$ and any register R_j with $1 \leqslant j \leqslant S$ its *content* R_j^t as a rational function of $K(X_1, ..., X_n)$ obtained applying step by step the register allocation instructions (1), ..., (T). In case that register j remains unspecified in this way at time t we define its content as the constant value 1 of the field K. Thus at any time any register content is the constant value $1 \in K$ or a rational function of $K(X_1, ..., X_n)$ which appears as intermediate result of the underlying arithmetic circuit β in the sense of Definition 1. We call $(R_j^t)_{1 \leqslant j \leqslant S,\ 1 \leqslant t \leqslant T}$ the *computation matrix* of the straight-line program β.

2.2. *From the Register Allocation Model to the Geometric Complexity Model*

In this subsection we introduce a geometric model of polynomial evaluation which reflects computational time and space when arithmetic operations are counted at unit cost. This model is somewhat coarse with regard to upper complexity bounds but it is well suited for the inference of lower bounds for the intrinsic time-space tradeoff function of a series of explicit polynomials which—we guess—are studied for the first time under the aspect of time versus space.

Our method to obtain lower bounds on time-space tradeoffs for polynomial evaluation is based on a geometrical interpretation of the notion of a straight-line program which uses nonscalar time and space not exceeding some prefixed quantities L and S, respectively. In the sequel we restrict ourselves to the case $n := 1$. This means that we are only dealing with univariate polynomials and rational functions defined over the field K. We denote by $X := X_1$ the only variable of the polynomials and rational functions occurring as intermediate results in the straight-line programs we are considering from now on.

First of all let us observe that the computation graph associated with Horner's rule for a univariate degree d polynomial $F \in K[X]$ can be pebbled in total time $2d$ and nonscalar time d using exactly two pebbles. Let L and S denote nonscalar time and space used by the Horner algorithm which evaluates the polynomial F. Then L and S satisfy the tradeoff relation $LS^2 = 4d$.

This consideration leads us to the following question: given *any* polynomial $F \in K[X]$ of degree at most d, do there exist straight-line programs β in $K(X)$ using nonscalar time $L(\beta)$ and space $S(\beta)$ such that the *time-space tradeoff* $LS^2(\beta) := L(\beta)\, S^2(\beta)$ is considerably smaller than d? Using a simple counting argument we shall find that the answer to this question is negative. This means that there exists a universal constant $c > 0$ such that (in some precise sense) *almost all* polynomials $F \in K[X]$ of degree bounded by d have the property that *any* straight-line program β in $K(X)$ evaluating F has a time-space tradeoff $LS^2(\beta)$ satisfying the inequality

$$LS^2(\beta) \geqslant cd$$

(see Theorem 7 below). In the sequel we shall abreviate such a statement as

$$LS^2(F) = \Omega(d).$$

Similarly as in [55, 26] we say that a family of univariate degree d polynomials $(F_d)_{d \in \mathbb{N}}$ is *hard to compute* in terms of time-space tradeoff if there exists a constant $c' > 0$ such that any family of arithmetic circuits $(\beta_d)_{d \in \mathbb{N}}$ in $K[X]$ with β_d evaluating the polynomial F_d satisfies the following time-space tradeoff inequality

$$LS^2(\beta_d) \geqslant d^{c'}.$$

In the sequel we shall abreviate such a statement as

$$LS^2(F_d) = d^{\Omega(1)}.$$

The geometrical method we are going to develop allows us to exhibit *specific* families of univariate polynomials which are hard to compute in this sense.

Let L and S be fixed natural numbers and let us suppose that we are given a straight-line program β which computes the rational function $F \in K(X)$ in nonscalar time $L(\beta) \leqslant L$ and space $S(\beta) \leqslant S$.

In order to homogenize notations let us start the computation formally at time zero fixing for $1 \leqslant j \leqslant S$ the content R_j^0 of each register R_j as $R_j^0 := 0$. Besides of space we shall take into account only *nonscalar* time as complexity measure. Nonscalar time will be indicated by the new parameter l

which ranges from 1 to L. Moreover, we shall use two extra registers R_{-1} and R_0 whose contents at any time instance $0 \leqslant l \leqslant L$ are fixed as $R^l_{-1} := 1$ and $R^l_0 := X$. Since in the nonscalar model K-linear operations are free and since we take in the straight-line program β only nonscalar operations into account, we may describe β by a recursive sequence of register allocation instructions (I^l_j) of the following type: for $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ the instruction (I^l_j) has the form

$$R^l_j := \left(\sum_{-1 \leqslant k \leqslant S} a^{(j,l)}_k R^{l-1}_k \right) op \left(\sum_{-1 \leqslant k \leqslant S} b^{(j,l)}_k R^{l-1}_k \right),$$

where *op* is a multiplication or division and where the $a^{(j,l)}_k$ and $b^{(j,l)}_k$ are suitable elements of K.

The output F of β is given by a final register allocation instruction (I), namely

$$F := \sum_{-1 \leqslant k \leqslant S} c_k R^L_k$$

with the c_k being suitable elements of K.

The elements $a^{(j,l)}_k$, $b^{(j,l)}_k$, c_k of K occurring in these register allocation instructions are called the *parameters* of the straight-line program β. Moreover, the intermediate results of β are given by the *computation matrix*

$$M(\beta) := (R^l_j)_{-1 \leqslant j \leqslant S,\, 0 \leqslant l \leqslant L}.$$

The circuit β itself is determined by its parameters and the indication which arithmetic operation, multiplication or division, is applied in each register allocation instruction (I^l_j).

We observe here that the register allocation instructions (I^l_j) do not exactly reflect a pebble game on the computation graph $\Gamma(\beta)$ since in our modeling all registers are assumed to change their contents simultaneously. Nevertheless, in a pebble game at any time instance only one register is affected and not all of them simultaneously.

Therefore, the modeling of a computation in $K(X)$ using given nonscalar time L and space S by register allocation rules of type (I^l_j) and of type (I) with $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ is somewhat coarser than the modeling given by Definition 2 and 3. This means that in this way there may appear rational functions as "outputs of the computations" which cannot be evaluated by a straight-line program which uses only nonscalar time L and

space S. Since our final aim is to prove *lower* bounds for the tradeoff between nonscalar time and space required to compute certain univariate polynomials, this coarsening of the complexity model will not affect the correctness of our results which we shall state in the sense of Definitions 2 and 3.

Let us also remark that the complexity model we have selected is somewhat arbitrary even within its own category. A moment's reflection shows that at least two alternative complexity models of the same type are thinkable. The first alternative model includes some parallelism admitting S simultaneous nonscalar multiplications/divisions at each step. Although this alternative complexity model is at first glance more general than the one we have chosen for our presentation, the time-space tradeoff lower bounds we are going to prove in this paper remain the same for this alternative model.

The second alternative model is more restrictive than ours. It allows only the change of just one register at each step and requires that this step represents a nonscalar multiplication/division. This second alternative complexity model produces slightly different time-space tradeoff lower bounds from those we are going to show (although the proving methods would be essentially the same). Whereas the time-space tradeoff function we are going to consider in this paper is always of the type LS^2, this second alternative complexity model yields a tradeoff function of type LS. It is surely a question of taste or personal preference, but in view of our proving methods the complexity model we have selected for this paper appears the most natural to us.

Let the quantities L and S be fixed. Let us think the parameters $a_k^{(j,l)}$, $b_k^{(j,l)}$, c_k occurring for $-1 \leqslant k \leqslant S$, $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ in the register allocation instructions (I_j^l) and (I) as varying, i.e., let us replace these parameters by new indeterminates. Then the entries of the computation matrix $M(\beta)$ and the rational function F representing intermediate results and output of the straight-line program β become rational expressions in the parameters of the circuit β (and of course in the variable X).

In this way the straight-line program β becomes a *generic computation scheme of nonscalar time L and space S* which is uniquely determined by the quantities L and S and the choice of the arithmetic operation (multiplication or division) done for each $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ in the register allocation instruction (I_j^l).

We are going to simplify somewhat further our computation scheme of nonscalar time L and space S. For this purpose we introduce for each $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ a new parameter $d^{(j,l)}$ which will be interpreted as follows: the value to be assigned to the parameter $d^{(j,l)}$ is 1 if the arithmetic operation occurring in the instruction (I_j^l) as *op* is a multiplication and the value is 0 if this arithmetic operation is a division.

Now we replace for each $1 \leqslant j \leqslant S$, $1 \leqslant l \leqslant L$ the register allocation instruction (I_j^l) by the following new one which we denote by (J_j^l):

$$R_j^l = \left(\sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_k^{l-1} \right) \cdot \left(d^{(j,l)} \left(\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1} \right) + (1 - d^{(j,l)}) \left(\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1} \right)^{-1} \right).$$

(Let us observe that taking in the register allocation instruction (J_j^l) the inverse of the subexpression $\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1}$ is consistent with our general assumption that the computations we consider do not contain the rational function zero as intermediate result.) Again we represent each parameter $d^{(j,l)}$ by a new indeterminate.

In this way we obtain a new generic computation scheme which depends only on the nonscalar time L and the space S. The parameters of this new computation scheme are $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$ and c_k with $-1 \leqslant k \leqslant S$, $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$.

Let us analyze how the output F depends on these parameters if F is a polynomial belonging to $K[X]$. To this end we use an idea going back to [55] (see also [50]).

In order to state the following technical result we recall that the *weight* of a polynomial with integer coefficients is the sum of the absolute values of its coefficients.

LEMMA 4. *Let d, L, S be given natural numbers, let $N := 8LS^2$ and let $Z_1, ..., Z_N$ be new indeterminates. There exist polynomials $P_d, ..., P_0 \in \mathbb{Z}[Z_1, ..., Z_N]$ of degree and weight bounded by*

$$\deg P_i \leqslant i(2L-1) + 2$$

and

$$\text{weight } P_i \leqslant (6(S+1))^{(i+1)^L},$$

with $0 \leqslant i \leqslant d$, such that the morphism of affine spaces

$$\Phi_{d,L,S} : K^N \to K^{d+1}$$

defined by these polynomials has the following property: for any polynomial $F \in K[X]$ of degree at most d which can be computed by a straight-line program in $K(X)$ using at most nonscalar time L and space S, there exists

a (nonempty) cofinite subset U_F of K such that for any element $\eta \in U_F$ the point $(f_d(\eta), ..., f_0(\eta)) \in K^{d+1}$ given by the representation

$$F = \sum_{0 \leqslant i \leqslant d} f_i(\eta)(X-\eta)^i$$

belongs to the image of the morphism $\Phi_{d,L,S}$.

Proof. Let β be an arbitrary straight-line program in $K(X)$ which computes a given polynomial $F \in K[X]$ of degree at most d using nonscalar time L and space S. We suppose that β is given as before by a sequence of register allocation instructions (J_j^l) with $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ and a final instruction (I). Thus the intermediate results of β are rational functions $R_k^l \in K(X)$ with $-1 \leqslant k \leqslant S$ and $0 \leqslant l \leqslant L$ which satisfy the following recursive relations:

- $R_{-1}^l = 1$ for any $0 \leqslant l \leqslant L$,
- $R_0^l = X$ for any $0 \leqslant l \leqslant L$,
- $R_j^0 = 0$ for any $1 \leqslant j \leqslant S$,

and

- $$R_j^l = \left(\sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_k^{l-1} \right) \cdot \left(d^{(j,l)} \left(\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1} \right) + (1 - d^{(j,l)}) \left(\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1} \right)^{-1} \right) \quad (1)$$

for any $1 \leqslant j \leqslant S$ and any $1 \leqslant l \leqslant L$.

Finally the output polynomial $F \in K[X]$ is representable as

$$F = \sum_{-1 \leqslant k \leqslant S} c_k R_k^L. \quad (2)$$

Here $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$, c_k are suitable elements of K with $-1 \leqslant k \leqslant S$, $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$, namely the parameters of the straight-line program β.

Each of the rational functions $\sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_k^{l-1}$ and $\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1}$ occurring as subexpressions in Eq. (1) are defined and different from zero in all points of some cofinite subset U_F of K. Since by assumption K is infinite the set U_F is nonempty. Let η be an arbitrary point of U_F and let $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$. Then the rational functions $R_{-1}^{l-1}, ..., R_S^{l-1}$, $\sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_k^{l-1}$ and $\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1}$ are defined and different from zero in η. By a suitable change of the parameters $a_j^{(j,l)}$, $b_j^{(j,l)}$ and c_k in Eqs. (1) and (2) we may assume without loss of generality that $\sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_k^{l-1}(\eta) = 1$ and $\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1}(\eta) = 1$ holds. The parameter $d^{(j,l)}$ takes by

assumption only the values 0 or 1. This implies that the rational function R_j^l is defined in η and that $R_j^l(\eta)=1$ holds. This enables us to represent R_j^l as a formal power series in $X-\eta$ with coefficients in K. More precisely we may write the rational function R_j^l uniquely as power series

$$R_j^l = 1 + \sum_{i \geqslant 1} R_{j,i}^l (X-\eta)^i$$

with coefficients $R_{j,i}^l$ belonging to the field K. Observe that $R_0^l = X$ has also a power series representation of the form $R_0^l = \eta + (X-\eta) = \eta + \sum_{i \geqslant 1} R_{0,i}^l (X-\eta)^i$ with $R_{0,1}^l = 1$ and $R_{0,i}^l = 0$ for $i > 1$. From our assumptions we deduce

$$\begin{aligned} \sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_k^{l-1} &= \sum_{-1 \leqslant k \leqslant S} a_k^{(j,l)} R_{k,0}^{l-1}(\eta) + \sum_{0 \leqslant k \leqslant S} a_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i \\ &= 1 + \sum_{0 \leqslant k \leqslant S} a_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i \end{aligned} \tag{3}$$

and similarly

$$\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1} = 1 + \sum_{0 \leqslant k \leqslant S} b_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i. \tag{4}$$

Equation (4) implies

$$\left(\sum_{-1 \leqslant k \leqslant S} b_k^{(j,l)} R_k^{l-1} \right)^{-1} = 1 + \sum_{v \geqslant 1} \left(- \sum_{0 \leqslant k \leqslant S} b_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i \right)^v.$$

This enables us to express Eq. (1) in terms of power series. For $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$ we have

$$\begin{aligned} &1 + \sum_{i \geqslant 1} R_{j,i}^l (X-\eta)^i \\ &\quad = \left(1 + \sum_{0 \leqslant k \leqslant S} a_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i \right) \\ &\qquad \cdot \left(d^{(j,l)} \left(1 + \sum_{0 \leqslant k \leqslant S} b_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i \right) \right. \\ &\qquad \left. + (1 - d^{(j,l)}) \left(1 + \sum_{v \geqslant 1} \left(- \sum_{0 \leqslant k \leqslant S} b_k^{(j,l)} \sum_{i \geqslant 1} R_{k,i}^{l-1} (X-\eta)^i \right)^v \right) \right). \end{aligned} \tag{5}$$

From Eq. (5) we deduce inductively that the coefficients $R^l_{j,i}$ are polynomial expressions which integer coefficients in the parameters $a_k^{(j',l')}$, $b_k^{(j',l')}$, $d^{(j',l')}$ of the straight-line program β where the range of k, j' and l' is $0 \leqslant k \leqslant S$, $1 \leqslant j' \leqslant S$ and $1 \leqslant l' \leqslant l$. These polynomial expressions depend only on L and S and are independent of the particular choice of η and of the particular straight-line program β.

Since no ambiguity may appear, we shall denote such a polynomial expression by the same symbol as the power series coefficient that it represents, namely $R^l_{j,i}$.

Comparing coefficients in Eq. (5) we see that each coefficient $R^l_{j,i}$ is up to sign a sum of monomial expressions of one of the following two types,

$$(d^{(j,l)})^{\varepsilon} \prod_{1 \leqslant v \leqslant \mu} b_{k_v}^{(j,l)} R^{l-1}_{k_v, i_v} \tag{6}$$

or

$$a_{k_\mu}^{(j,l)} R^{l-1}_{k_\mu, i_\mu} (d^{(j,l)})^{\varepsilon} \prod_{1 \leqslant v < \mu} b_{k_v}^{(j,l)} R^{l-1}_{k_v, i_v}, \tag{7}$$

with $\sum_{1 \leqslant v \leqslant \mu} i_v = i$, $1 \leqslant i_v \leqslant i$, $1 \leqslant \mu \leqslant i$, $0 \leqslant k_v \leqslant S$ and $\varepsilon \in \{0, 1\}$.

From this observation we deduce the following recursive degree bound:

$$\deg R^l_{j,i} \leqslant \max \Bigg\{ \mu + 1 + \sum_{1 \leqslant v \leqslant \mu} \deg R^{l-1}_{k_v, i_v} : \sum_{1 \leqslant v \leqslant \mu} i_v = i,\ 1 \leqslant i_v \leqslant i,\ 1 \leqslant \mu \leqslant i,\ 0 \leqslant k_v \leqslant S \Bigg\}. \tag{8}$$

From our construction one deduces immediately that for any $0 \leqslant k \leqslant S$ and any $i \geqslant 1$ the estimate

$$\deg R^0_{k,i} \leqslant 0 \tag{9}$$

holds.

Solving the recurrence relations (8) and taking into account the initial conditions (9) yields

$$\deg R^l_{j,i} \leqslant i(2l-1) + 1 \tag{10}$$

for any $1 \leqslant j \leqslant S$, $1 \leqslant l \leqslant L$ and $i \geqslant 1$.

We are going to estimate the weight of the polynomials $R^l_{j,i}$. To this aim observe that the number of monomial expressions (6) and (7) appearing in

$R^l_{j,i}$ does not exceed $3(2(S+1))^i$. From this remark we deduce the following recursive weight bound:

$$\text{weight } R^l_{j,i} \leqslant 3(2(S+1))^i \max\left\{ \prod_{1 \leqslant v \leqslant \mu} \text{weight } R^{l-1}_{k_v, i_v} : \sum_{1 \leqslant v \leqslant \mu} i_v = i,\ 1 \leqslant i_v \leqslant i,\ 1 \leqslant \mu \leqslant i,\ 0 \leqslant k_v \leqslant S \right\}. \tag{11}$$

By direct inspection one verifies easily that for any $1 \leqslant l \leqslant L$ and any $1 \leqslant j \leqslant S$ the estimate

$$\text{weight } R^l_{j,1} \leqslant 4^l (S+1)^l \tag{12}$$

holds.

Solving the recurrence relations (11) for $i > 1$ and taking into account the initial conditions weight $R^0_{k,v} \leqslant 1$, with $0 \leqslant k \leqslant S$ and $v \geqslant 1$, yields

$$\text{weight } R^l_{j,i} \leqslant 3^{(i^l-1)/(i-1)}(2(S+1))^{i(i^l-1)/(i-1)} \leqslant (6(S+1))^{(i+1)^l-1}. \tag{13}$$

The coefficients $R^l_{j,i}$ of the power series occurring in Eq. (5) are polynomial expressions over the integers in the $2LS^2 + 3LS$ parameters $a^{(j,l)}_k$, $b^{(j,l)}_k$, $d^{(j,l)}$ with $0 \leqslant k \leqslant S$, $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$. Thus we shall consider them as $(2LS^2 + 3LS)$-variate polynomials over the integers.

The polynomial $F \in K[X]$ is of degree at most d and has therefore a finite Taylor series expansion in $(X-\eta)$, say

$$F = \sum_{0 \leqslant i \leqslant d} f_i(\eta)(X-\eta)^i$$

with coefficients $f_i(\eta)$ belonging to the field K.

From Eq. (2) we deduce

$$\begin{aligned} F &= \sum_{0 \leqslant i \leqslant d} f_i(\eta)(X-\eta)^i = \sum_{-1 \leqslant k \leqslant S} c_k R^L_k \\ &= \left(c_{-1} + c_0\eta + \sum_{1 \leqslant k \leqslant S} c_k \right) + \sum_{0 \leqslant k \leqslant S} c_k \left(\sum_{i \geqslant 1} R^L_{k,i}(X-\eta)^i \right) \\ &= \left(c_{-1} + c_0\eta + \sum_{1 \leqslant k \leqslant S} c_k \right) + \sum_{i \geqslant 1} \left(\sum_{0 \leqslant k \leqslant S} c_k R^L_{k,i} \right)(X-\eta)^i. \end{aligned}$$

This implies

$$f_i(\eta) = \sum_{0 \leqslant k \leqslant S} c_k R^L_{k,i} \tag{14}$$

for $1 \leqslant i \leqslant d$ and

$$f_0(\eta) = c_{-1} + c_0 \eta + \sum_{1 \leqslant k \leqslant S} c_k \tag{15}$$

for $i = 0$.

Observe that Eq. (14) is independent of the parameter c_{-1}. This allows us to consider $c_{-1} + c_0 \eta$ just as a new parameter c from which the straight-line program β depends and which replaces the old parameter c_{-1}. In this sense we can rewrite Eq. (15) as

$$f_0(\eta) = c + \sum_{1 \leqslant k \leqslant S} c_k. \tag{16}$$

The right hand side of Eqs. (14) and (16) are polynomial expressions in the $2LS^2 + 3LS + S + 2 \leqslant 8LS^2$ parameters c, c_k, $a_k^{(j,l)}$, $b_k^{(j,l)}$, $d^{(j,l)}$ with $0 \leqslant k \leqslant S$, $1 \leqslant j \leqslant S$ and $1 \leqslant l \leqslant L$. These polynomial expressions depend only on L and S and they are independent of the choice of the point $\eta \in U_F$.

Let $N := 8LS^2$ and let $Z_1, ..., Z_N$ be new indeterminates. From Eqs. (10), (13), (14), and (16) we deduce that there exist polynomials $P_0, ..., P_d \in \mathbb{Z}[Z_1, ..., Z_N]$ such that for any $0 \leqslant i \leqslant d$ degree and weight of P_i can be estimated by

$$\deg P_i \leqslant i(2L-1) + 2$$

and

$$\text{weight } P_i \leqslant (6(S+1))^{(i+1)^L - 1} (S+1) \leqslant (6(S+1))^{(i+1)^L}$$

and such that the following holds: for any polynomial $F \in K[X]$ of degree at most d which can be evaluated by a straight-line program using at most nonscalar time L and space S there exists a (nonempty) cofinite set U_F in K such that for any value $\eta \in U_F$ there is a point $z \in K^N$ with

$$F = \sum_{0 \leqslant i \leqslant d} f_i(\eta)(X-\eta)^i = \sum_{0 \leqslant i \leqslant d} P_i(z)(X-\eta)^i.$$

Let now

$$\Phi_{d,L,S}: K^N \to K^{d+1}$$

be the morphism of affine spaces defined by $\Phi_{d,L,S}(z) := (P_d(z), ..., P_0(z))$ for arbitrary $z \in K^N$. This morphism has all the properties announced in the statement of Lemma 4. ▌

In our applications we shall need a more comprehensive formulation of Lemma 4 in which the generic value η and the cofinite set U_F it belongs to do not appear anymore explicitely. Such a formulation can easily be obtained by including the generic value η in the list of parameters of the hypothetical straight-line program β analyzed in the proof of Lemma 4. From this observation we deduce our next result.

LEMMA 5. *Let d, L, S be given natural numbers, let $N := 8LS^2 + 1$ and let $Z_1, ..., Z_N$ be new indeterminates. There exist polynomials $P_d, ..., P_0 \in \mathbb{Z}[Z_1, ..., Z_N]$ of degree and weight bounded by*

$$2(Ld+1)$$

and

$$(12(S+1))^{(d+1)L}$$

respectively such that the morphism of affine spaces

$$\Phi_{d,L,S}: K^N \to K^{d+1}$$

defined by these polynomials has the following property: for any polynomial $F \in K[X]$ of degree at most d which can be computed by a straight-line program using at most nonscalar time L and space S, the point $(f_d, ..., f_0) \in K^{d+1}$ given by the representation $F = \sum_{0 \leqslant i \leqslant d} f_i X^i$ belongs to the image of $\Phi_{d,L,S}$.

In the sequel we shall identify any polynomial $F = \sum_{0 \leqslant i \leqslant d} f_i X^i \in K[X]$ of degree at most d with its coefficient vector $(f_d, ..., f_0)$ which we consider as a point of the affine space K^{d+1}. In this sense a statement like "$F \in K^{d+1}$" should be understood as "$(f_d, ..., f_0) \in K^{d+1}$."

From Lemma 4 we deduce the following geometric consequences which represent our main tool in deriving lower bounds for the intrisic time-space tradeoff of univariate polynomials (compare with [30]).

LEMMA 6. *Let d, L, S be given natural numbers. There exists a Zariski closed, irreducible and $\mathbb{Q}$-definable subset $W_{d,L,S}$ of K^{d+1} such that the following conditions are satisfied:*

(i) $\dim W_{d,L,S} \leqslant 8LS^2$.

(ii) $\deg W_{d,L,S} \leqslant (2(Ld+1))^{8LS^2}$.

(iii) *The coefficient vector of any polynomial $F \in K[X]$ of degree at most d which can be evaluated by a straight-line program in $K(X)$ using at most nonscalar time L and space S belongs to the algebraic variety $W_{d,L,S}$.*

Proof. Let $W := W_{d,L,S}$ be the Zariski-closure in K^{d+1} of the image of the morphism $\Phi := \Phi_{d,L,S}$ of Lemma 4. One sees immediately that W is a Zariski closed irreducible subset of the affine space K^{d+1}. This subset is also $\mathbb{Q}$-definable since the morphism Φ is given by the polynomials $P_d, ..., P_0$ which have integer coefficients. For the rest of the proof let us interprete Φ as a morphism of affine varieties which maps K^N into W. In this interpretation Φ is dominant. This implies $\dim W \leqslant N = 8LS^2$. Therefore the algebraic variety $W = W_{d,L,S}$ satisfies condition (i).

Let us verify condition (ii). Let $r := \dim W$. Since the morphism Φ is dominant there exists a nonempty, Zariski open subset of W which is contained in $im\Phi$, the image of Φ. Therefore we may deduce from [25] that there exist r affine hyperplanes $H_1, ..., H_r$ of K^{d+1} which intersect $im\ \Phi$ in $\deg W$ many points. Let $M = H_1 \cap \cdots \cap H_r \cap im\ \Phi$. By assumption we have $\# M = \deg W$. From Lemma 4 one deduces immediately that $\Phi^{-1}(H_1), ..., \Phi^{-1}(H_r)$ are hypersurfaces of K^N of degree at most $2(Ld+1)$. Let

$$\mathscr{C} := \{ C : C \text{ is an irreducible component of } \Phi^{-1}(H_1) \cap \cdots \cap \Phi^{-1}(H_r) \}.$$

By the Bézout Inequality (see [25, 18]) we have

$$\# \mathscr{C} \leqslant \sum_{C \in \mathscr{C}} \deg C \leqslant (2(Ld+1))^r \leqslant (2(Ld+1))^{8LS^2},$$

where $\deg C$ denotes the (geometric) degree of the irreducible closed subset C of K^N.

For any $C \in \mathscr{C}$ the Zariski closure of the image $\Phi(C)$ is an irreducible subset of K^{d+1} contained in M, hence a point of M. Since the set M is contained in $im\ \Phi$ we conclude

$$\deg W_{d,L,S} = \deg W = \# M \leqslant \# \mathscr{C} \leqslant (2(Ld+1))^{8LS^2}.$$

Finally we are going to verify condition (iii). Let $F = \sum_{0 \leqslant i \leqslant d} f_i X^i \in K[X]$ be a polynomial of degree at most d which can be evaluated by a straight-line program in $K(X)$ using at most nonscalar time L and space S. For any $\eta \in K$ let $F = \sum_{0 \leqslant i \leqslant d} f_i(\eta)(X-\eta)^i$ be the Taylor expansion of F in $X - \eta$. The vector $(f_d(\eta), ..., f_0(\eta))$ depends in a polynomial way on the

parameter η. Let $U := U_F$ be the nonempty, cofinite subset introduced in Lemma 4. For any $\eta \in U$ we have

$$(f_d(\eta), ..., f_0(\eta)) \in im\ \Phi_{d, L, S} = im\ \Phi \subset W,$$

by this lemma. Since U is infinite and W is Zariski closed in K^{d+1} we conclude that $(f_d, ..., f_0) = (f_d(0), ..., f_0(0))$ belongs to the algebraic variety $W = W_{d, L, S}$. ∎

From Lemma 6 we deduce now our first complexity result. This result characterizes the intrinsic time-space tradeoff complexity of "almost all" univariate polynomials of degree at most d generalizing thus the main outcome of [41] and showing that Horner's rule is asymptotically optimal in terms of time-space tradeoffs.

THEOREM 7. *Let d be a given natural number. There exists a nonempty Zariski open subset U of K^{d+1} such that for any polynomial $F \in K[X]$ of degree at most d with $F \in U$ the tradeoff estimate $LS^2(F) \geqslant \frac{d}{8}$ holds.*

Proof. Let d be fixed. For any positive rational number $t \leqslant d$ we consider the Zariski closed subset $W_{d, t}$ of K^{d+1} defined by

$$W_{d, t} := \bigcup_{\substack{L, S \in \mathbb{N} \\ LS^2 \leqslant t}} W_{d, L, S}.$$

From Lemma 6(i) we deduce

$$\dim W_{d, t} \leqslant \max\{\dim W_{d, L, S} : L, S \in \mathbb{N}, LS^2 \leqslant t\} \leqslant 8t.$$

Thus for $t := \frac{d}{8}$ we have

$$\dim W_{d, d/8} \leqslant d.$$

This implies that the Zariski open set $U := K^{d+1} \setminus W_{d, d/8}$ is nonempty. From Lemma 6(iii) we deduce finally that for any polynomial F of $K[X]$ whose degree does not exceed d and which belongs to the set U the tradeoff estimate $LS^2(F) \geqslant \frac{d}{8}$ holds. ∎

Following [41] there exists a constant $c > 0$ such that any polynomial $F \in K[X]$ of arbitrary degree d can be evaluated by a straight-line program in $K[X]$ in nonscalar time not exceeding $c\sqrt{d}$. Combining this result with Theorem 7 we are able to make the following conclusion:

COROLLARY 8. *There exists a constant $c' > 0$ with the following property: let d be a given natural number and let U be the nonempty Zariski open subset*

of K^{d+1} introduced in Theorem 7. Then for any polynomial $F \in K[X]$ of degree at most d satisfying the condition $F \in U$ and for any straight-line program β in $K(X)$ which evaluates F in optimal nonscalar time the space $S(\beta)$ required by the procedure β is bounded from below by

$$S(\beta) \geqslant c' \sqrt[4]{d}.$$

We may paraphrase the content of Corollary 8 as follows: almost all polynomials of $K[X]$ of degree at most d require space $c' \sqrt[4]{d}$ if they are evaluated optimally with respect to nonscalar time. On the other hand following [41] there exists a constant $c'' > 0$ such that almost all polynomials of $K[X]$ of degree at most d need nonscalar time $c'' \sqrt{d}$ for their evaluation. This explains in which sense Theorem 7 contains the best possible *generic* time-space tradeoff result we may hope for.

3. TOOLS FROM GEOMETRIC ELIMINATION AND INTERSECTION THEORY

In this paper we shall often face situations like the following one: assume that there is given a polynomial $F \in K[X]$ of degree d. Only from the knowledge of the coefficients of F we have to deduce a lower bound for the quantity LS^2 where L and S are arbitrary natural numbers satisfying the condition $F \in W_{d,L,S}$ or the condition $F \in im\, \Phi_{d,L,S}$ with $W_{d,L,S}$ and $\Phi_{d,L,S}$ defined as in Lemma 6 and Lemma 5 respectively. These two Lemmas establish a relation between the size of the complexity parameters L and S and the degree or height of the algebraic variety $W_{d,L,S}$ or the algebraic morphism $\Phi_{d,L,S}$. Therefore we need a tool which allows us to estimate these geometric invariants, namely degree and height of $W_{d,L,S}$ and $\Phi_{d,L,S}$ respectively from the knowledge of just one specific point belonging to the algebraic variety $W_{d,L,S}$ or to the image of the morphism $\Phi_{d,L,S}$. We are going to develop such a tool making use of suitable Nullstellensätze and Bézout Inequalities from geometric and arithmetic elimination and intersection theory (compare [41, 55, 50, 30, 20, 29, 26, 54, 53, 36, 27, 39, 2] for a similar viewpoint).

In this technical section we are going to explain the results of elimination and intersection theory we shall apply in the sequel. Let us start recalling that the *height* of a polynomial with integer coefficients is the maximum absolute value of its coefficients. Similarly the *logarithmic height* of this polynomial is the maximum bit length of its coefficients. The logarithmic height of a polynomial over the integers is therefore roughly speaking the logarithm at base two of its height plus one.

The main result of this section is the following one:

PROPOSITION 9. *Let N, d, D and η be given natural numbers and let $\Phi := (P_d, ..., P_0): \mathbb{C}^N \to \mathbb{C}^{d+1}$ be a morphism of affine spaces with $P_0, ..., P_d$ being polynomials belonging to $\mathbb{Z}[Z_1, ..., Z_N]$. Let F be a given point of $\mathbb{Z}^{d+1}$. Consider the Φ-fiber $V := \Phi^{-1}(F)$ of the point F as a $\mathbb{Q}$-definable Zariski closed subvariety of $\mathbb{C}^N$. Suppose that V is nonempty. Let $h_1, ..., h_s \in \mathbb{Z}[Z_1, ..., Z_N]$ be polynomials satisfying the following conditions*:

(1) $V = \{z \in \mathbb{C}^N : h_1(z) = 0, ..., h_s(z) = 0\}$,

(2) $\max\{\deg h_i : 1 \leqslant i \leqslant s\} \leqslant D$, *and*

(3) $\max\{\text{logheight } h_i : 1 \leqslant i \leqslant s\} \leqslant \eta$.

Then, there exists a point $\theta = (\theta_1, ..., \theta_N)$ of the fiber V satisfying the estimate

$$\log_2 \max\{|\theta_i| : 1 \leqslant i \leqslant N\} \leqslant D^{cN}(\log_2 s + \eta),$$

where $c > 0$ is a suitable universal constant.

The rest of this section is devoted to the proof of this result. To this aim we need a series of intermediate technical results from geometric elimination theory. The first one is a suitable form of an effective Nullstellensatz.

In order to keep exposition more transparent we have choosen a "classical" version of this type of result implying rather coarse lower complexity bounds in our applications. Such Nullstellensatz versions can be found in [11, 13, 14, 32].

Let us remark that recent "intrinsic" Nullstellensätze as in [23, 21, 22, 33, 52] would allow a slight improvement of our tradeoff bounds.

THEOREM 10 (Effective Nullstellensatz). *Let $D \geqslant 3$ and $N \geqslant 3$ be given natural numbers and let $h_1, ..., h_s \in \mathbb{Z}[Z_1, ..., Z_N]$ be polynomials of degree at most D. Consider the ideal $\mathscr{I} = (h_1, ..., h_s)$ generated by these polynomials in $\mathbb{Q}[Z_1, ..., Z_N]$. Then the ideal $\mathscr{I}$ is trivial (i.e., $\mathscr{I} = (1)$) if and only if there exists polynomials $g_1, ..., g_s \in \mathbb{Q}[Z_1, ..., Z_N]$ satisfying the degree bound*

$$\max\{\deg g_i : 1 \leqslant i \leqslant s\} \leqslant D^N - D$$

such that the Bézout identity

$$1 = \sum_{1 \leqslant i \leqslant s} g_i h_i \tag{17}$$

holds.

For a proof of this result see [32, 17, 43]. The bound on the degree of the polynomials $g_1, ..., g_s$ in Theorem 10 allows us to reduce the question

of the emptyness of the algebraic variety V defined by the polynomials $h_1, ..., h_s$ to the question of solving an inhomogeneous system of linear equations of size $D^{N^2} \times sD^{N^2}$ over the rational numbers. The entries of this linear equation system are given by the coefficients of the polynomials $h_1, ..., h_s$. This linear system of equations allows us to compute a suitable polynomial of bounded degree which expresses a certain elimination property of the variety V. This observation leads us to the next result.

LEMMA 11. *Let $D \geqslant 3$ and $N \geqslant 3$ be given natural numbers and let V be a $\mathbb{Q}$-definable Zariski closed subset of $\mathbb{C}^N$ having positive dimension r. Suppose that V is given as the locus of zeroes of finitely many polynomials in $\mathbb{Z}[Z_1, ..., Z_N]$ of degree at most D. Let us introduce for $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant N+1$ new indeterminates $T_{i,j}$ and polynomials*

$$L_i := T_{i,1} Z_1 + \cdots + T_{i,N} Z_N + T_{i,N+1}.$$

Under these assumptions there exists a non-zero polynomial $E \in \mathbb{Z}[T_{i,j}; 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant N+1]$ of degree at most D^{N^2} having the following property: for any matrix $t = (t_{i,j})_{1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant N+1}$ of $\mathbb{C}^{r \times (N+1)}$ defining r affine linear polynomials

$$\begin{aligned} L_1(t, Z_1, ..., Z_N) &= t_{1,1} Z_1 + \cdots + t_{1,N} Z_N + t_{1,N+1}, \\ &\vdots \\ L_r(t, Z_1, ..., Z_N) &= t_{r,1} Z_1 + \cdots + t_{r,N} Z_N + t_{r,N+1}, \end{aligned}$$

the intersection of V with the affine linear subspace of $\mathbb{C}^N$ given by these polynomials, namely

$$V \cap \{z \in \mathbb{C}^N : L_1(t, z) = 0, ..., L_r(t, z) = 0\},$$

is nonempty if the (consistent) Zariski open condition $E(t) \neq 0$ holds.

Notation 12. For the rest of this section let us fix the notations

$$T := (T_{i,j})_{1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant N+1} \qquad \text{and} \qquad Z := (Z_1, ..., Z_N).$$

Proof of Lemma 11. By hypothesis there exist finitely many, say s, polynomials $h_1, ..., h_s \in \mathbb{Z}[Z_1, ..., Z_N]$ of degree at most D which define the variety V. Since r is the (positive) dimension of V there exists a nonempty Zariski open subset U of $\mathbb{C}^{r \times (N+1)}$ such that for any $t \in U$ the intersection

$$V \cap \{z \in \mathbb{C}^N : L_1(t, z) = 0, ..., L_r(t, z) = 0\},$$

contains at least one point (see, e.g., [25, Lemma 1]). This implies that the ideal $\mathscr{J}$ generated by the polynomials $h_1, ..., h_s, L_1, ..., L_r$ in the polynomial ring $\mathbb{Q}(T)[Z]$ is proper. From Theorem 10 we deduce therefore that there cannot exist polynomials $g_1, ..., g_{r+s} \in \mathbb{Q}(T)[Z]$ such that for any $1 \leqslant k \leqslant r+s$ the polynomial g_k has the form

$$g_k(Z) := \sum_{v_1 + \cdots + v_N \leqslant D^N - D} Y^{(k)}_{v_1, ..., v_N} Z_1^{v_1} \cdots Z_N^{v_N}$$

with coefficients $Y^{(k)}_{v_1, ..., v_N}$ in the field $\mathbb{Q}(T)$ and such that the Bézout identity

$$\begin{aligned} 1 = {} & g_1(Z)\, h_1(Z) + \cdots + g_s(Z)\, h_s(Z) \\ & + g_{s+1}(Z)\, L_1(T, Z) + \cdots + g_{s+r}(Z)\, L_r(T, Z) \end{aligned} \tag{18}$$

holds in $\mathbb{Q}(T)[Z]$.

We may interpret the (inconsistent) polynomial identity (18) as an inhomogeneous linear equation system in the unknowns $Y^{(k)}_{v_1, ..., v_N}$ appearing as coefficients of the "potential" polynomials $g_1, ..., g_{r+s}$ in the variables $Z_1, ..., Z_N$. This equation system has roughly size $D^{N^2} \times sD^{N^2}$ and its matrix, which we denote by A, contains as entries only coefficients of the polynomials $h_1, ..., h_s$ and $L_1, ..., L_r$ with respect to the variables $Z_1, ..., Z_N$.

Thus the matrix A is built up by integers and indeterminates $T_{i,j}$. Let us write

$$A \cdot Y = B \tag{19}$$

for the inhomogeneous linear equation system representing the polynomial identity (18). Here B and Y are column vectors of length at most D^{N^2} and sD^{N^2} respectively, all entries of B are 0 except one which is 1, and Y is the column vector of unknowns of the system. These unknowns can be written as $Y^{(k)}_{v_1, ..., v_N}$ with $1 \leqslant k \leqslant r+s$ and $v_1 + \cdots + v_n \leqslant D^N$. The inconsistency of the polynomial identity (18) implies the inconsistency of the linear equation system (19). Therefore the rank of the matrix A is strictly smaller than the rank, say m, of the matrix A^* obtained by adding to the matrix A the column vector B. This means that A^* contains a regular $m \times m$ minor with nonzero determinant $E \in \mathbb{Z}[T]$ whereas all $m \times m$ minors of A are singular. This determinant $E(T)$ expresses a suitable elimination property of the algebraic variety defined in $\mathbb{C}^{r \times (N+1)} \times \mathbb{C}^N$ by the polynomials $h_1(Z), ..., h_s(Z), L_1(T, Z), ..., L_r(T, Z)$ if we project this variety into the affine space $\mathbb{C}^{r \times (N+1)}$. The following arguments contain the precise sense of this statement and its justification: for any $t \in \mathbb{C}^{r \times (N+1)}$ such that $E(t) \neq 0$ holds the

linear equation system we obtain from (19) specializing the generic matrix T into t is inconsistent. In view of Theorem 10 this means that the ideal generated by the polynomials $h_1(Z), ..., h_s(Z), L_1(t, Z), ..., L_r(t, Z)$ in the polynomial ring $\mathbb{C}[Z]$ is proper. Therefore the variety

$$V \cap \{z \in \mathbb{C}^N : L_1(t, z) = 0, ..., L_r(t, z) = 0\}$$
$$= \{z \in \mathbb{C}^N : h_1(z) = 0, ..., h_s(z) = 0, L_1(t, z) = 0, ..., L_r(t, z) = 0\}$$

is nonempty.

Observe now that the entries of the matrix A^* are constants or linear polynomials of $\mathbb{Z}[T]$ and that it contains at most D^{N^2} rows what implies $m \leqslant D^{N^2}$. Therefore the degree of the polynomial $E(T)$ is bounded by D^{N^2}. ∎

Lemma 11 represents the main step in the proof of the next result.

LEMMA 13. *Let $D \geqslant 3$ and $N \geqslant 3$ be natural numbers and let V be a $\mathbb{Q}$-definable Zariski closed subset of $\mathbb{C}^N$ having positive dimension r. Suppose that V is given as the locus of zeroes of finitely many polynomials of $\mathbb{Z}[Z_1, ..., Z_N]$ of degree at most D. Then there are r affine linear polynomials $L_1, ..., L_r \in \mathbb{Z}[Z_1, ..., Z_N]$ of logarithmic height bounded by $N(N+1)\log_2 D$, such that for any $1 \leqslant k \leqslant r$ the algebraic variety*

$$V \cap \{z \in \mathbb{C}^N : L_1(z) = 0, ..., L_k(z) = 0\}$$

is nonempty of dimension $r - k$.

We observe here that the results of [34, Subsect. 4.8] imply an improvement of the estimate for the logarithmic height of the affine linear polynomials $L_1, ..., L_r$ in Lemma 13 to $cN \log_2 D$ where $c > 0$ is a suitable universal constant. However we prefer to work with the coarser height bound in the statement of Lemma 13, since the impact of the mentioned improvement on our complexity results is rather modest and since this coarse bound is much easier to prove.

In the following proof we shall make again use of the matrix

$$T := (T_{i,j})_{1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant N+1}$$

of indeterminates $T_{i,j}$ introduced above.

Proof of Lemma 13. Applying Lemma 11 we construct recursively in the dimension r of the variety V affine linear polynomials $L_1, ..., L_r \in \mathbb{Z}[Z]$ satisfying the requirements of the lemma to show.

Before starting this recursive construction let us observe that the assumption V being given by N-variate polynomials of degree at most D and the Bézout Inequality (see, e.g., [25, Theorem 1; 18, Example 8.4.6]) imply together that the degree of V is bounded by D^N (in the sequel we shall denote the degree of V by deg V).

Let us first consider the case $r := 1$.

Since $\deg V \leqslant D^N$ holds we may choose a set Γ of at most D^N points of V such that for each irreducible component of maximal dimension $r = 1$ of V there exists at least one point in this component belonging to Γ. Let

$$Q := \prod_{(\gamma_1, \ldots, \gamma_N) \in \Gamma} (\gamma_1 T_{1,1} + \cdots + \gamma_N T_{1,N} + T_{1,N+1}) \in \mathbb{C}[T_{1,1}, \ldots, T_{1,N+1}]$$

and let $E_1 \in \mathbb{Z}[T_{1,1}, \ldots, T_{1,N}]$ be the elimination polynomial of Lemma 11. Thus QE_1 is a nonzero polynomial of $\mathbb{C}[T_{1,1}, \ldots, T_{1,N+1}]$ of degree at most $D^{N^2} + D^N < D^{N(N+1)}$. Therefore there exists in the set

$$\{(t_{1,1}, \ldots, t_{1,N+1}) \in \mathbb{Z}^{N+1} : \max\{|t_{1,j}| : 1 \leqslant j \leqslant N+1\} \leqslant D^{N(N+1)}\}$$

a point $(t_{1,1}, \ldots, t_{1,N+1})$ such that $QE_1(t_{1,1}, \ldots, t_{1,N+1}) \neq 0$ holds. Let $L_1 := t_{1,1} Z_1 + \cdots + t_{1,N} Z_N + t_{1,N+1}$. From $Q(t_{1,1}, \ldots, t_{1,N+1}) \neq 0$ we deduce that the affine hyperplane $\{z \in \mathbb{C}^N : L_1(z) = 0\}$ cuts properly all irreducible components of V of maximal dimension $r = 1$ and $E_1(t_{1,1}, \ldots, t_{1,N+1}) \neq 0$ implies that $V \cap \{z \in \mathbb{C}^N : L_1(z) = 0\}$ is nonempty. Therefore by the Dimension Theorem (see, e.g., [51]) the dimension of the algebraic variety $V \cap \{z \in \mathbb{C}^N : L_1(z) = 0\}$ is $r - 1 = 0$. Moreover the logarithmic height of the affine linear polynomial L_1 satisfies the requirements in the conclusion of Lemma 13.

In the general case $r > 1$ we proceed similarly. We assume inductively that we are able to find for any closed subvariety of $\mathbb{C}^N$ of dimension $r - 1$ which is definable by polynomials of $\mathbb{Z}[Z_1, \ldots, Z_N]$ of degree at most D, a set of $r - 1$ affine linear polynomials of $\mathbb{Z}[Z_1, \ldots, Z_N]$ satisfying the requirements in the conclusion of Lemma 13.

Again we choose a set Γ of at most D^N points of V such that for each component of maximal dimension r of V there exists at least one point in this component belonging to Γ.

Let

$$Q := \prod_{(\gamma_1, \ldots, \gamma_N) \in \Gamma} (\gamma_1 T_{1,1} + \cdots + \gamma_N T_{1,N} + T_{1,N+1}) \in \mathbb{C}[T_{1,1}, \ldots, T_{1,N+1}]$$

and let $E_r \in \mathbb{Z}[T]$ be the elimination polynomial of Lemma 11. Thus QE_r is again a nonzero polynomial of $\mathbb{C}[T]$ of degree strictly less than $D^{N(N+1)}$. Therefore there exists in the set

$$\{(t_{i,j})_{1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant N+1} \in \mathbb{Z}^{r \times (N+1)} : \max\{|t_{i,j}| : 1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant N+1\} \leqslant D^{N(N+1)}\}$$

a point $t = (t_{i,j})_{1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant N+1}$ such that $QE_r(t) \neq 0$ holds. Let $L_1 := t_{1,1}Z_1 + \cdots + t_{1,N}Z_N + t_{1,N+1}$. From $Q(t) = Q(t_{1,1}, ..., t_{1,N+1}) \neq 0$ we deduce that the affine hyperplane $\{z \in \mathbb{C}^N : L_1(z) = 0\}$ cuts properly all components of V of maximal dimension r. On the other hand, if we write T^* for the matrix obtained from T replacing the first row vector $(T_{1,1}, ..., T_{1,N+1})$ in T by $(t_{1,1}, ..., t_{1,N+1})$, we are able to infer from $E_r(t) \neq 0$ that the $(r-1)(N+1)$-variate polynomial $E_r(T^*)$ is nonzero. From Lemma 11 one deduces easily that any selection of $r-1$ affine linear polynomials of $\mathbb{C}[Z_1, ..., Z_n]$ whose coefficients satisfy the nonempty Zariski open condition $E_r(T^*) \neq 0$ define a nonempty intersection with the algebraic variety $W := V \cap \{z \in \mathbb{C}^N : L_1(z) = 0\}$. This implies that W is nonempty and that $\dim W = r-1$ holds. On the other hand W is definable by polynomials of $\mathbb{Z}[Z_1, ..., Z_N]$ of degree at most D. Thus applying the induction hypothesis to the variety W we find affine linear polynomials $L_2, ..., L_r \in \mathbb{Z}[Z_1, ..., Z_N]$ of logarithmic height bounded by $N(N+1)\log_2 D$ such that for any $2 \leqslant k \leqslant r$ the Zariski closed subset

$$W \cap \{z \in \mathbb{C}^N : L_2(z) = 0, ..., L_k(z) = 0\} = V \cap \{z \in \mathbb{C}^N : L_1(z) = 0, ..., L_k(z) = 0\}$$

is nonempty of dimension $\dim W - (k-1) = (r-1) - (k-1) = r-k$. Putting all this information together we see that the affine linear polynomials $L_1, ..., L_r$ satisfy the requirements in the conclusion of Lemma 13. ∎

In order to finish the proof of Proposition 9 we need now the following result which estimates the absolute value of the coordinates of the isolated points of a $\mathbb{Q}$-definable Zariski closed subset of the affine space $\mathbb{C}^N$.

PROPOSITION 14. *Let N, D, η and s be given natural numbers with $D \geqslant N$ and let $h_1, ..., h_s$ be polynomials of degree at most D and logarithmic height at most η belonging to $\mathbb{Z}[Z_1, ..., Z_N]$. Let V be the Zariski closed subset of $\mathbb{C}^N$ defined by these polynomials, i.e., let*

$$V := \{z \in \mathbb{C}^N : h_1(z) = 0, ..., h_s(z) = 0\}.$$

Then any isolated point $\theta := (\theta_1, ..., \theta_N)$ *of* V *satisfies the estimate*

$$\max\{\log_2 |\theta_i| : 1 \leqslant i \leqslant N\} \leqslant D^{c'N}(\log_2 s + \eta),$$

where $c' > 0$ *is a suitable universal constant.*

For a proof of this result see [34, Corollary 7]. We are now able to show Proposition 9:

Proof of Proposition 9. Let $r := \dim V$. Since V is nonempty by assumption we have $0 \leqslant r \leqslant N$. In case $r = 0$ all points of V are isolated and we may apply directly Proposition 14 to get a point θ of V satisfying the required estimate. Let us therefore suppose $r > 0$. From Lemma 13 we deduce that there exist r affine linear polynomials in $\mathbb{Z}[Z_1, ..., Z_N]$, say $L_1, ..., L_r$, of logarithmic height at most $N(N+1)\log_2 D$ such that

$$\begin{aligned} W &:= V \cap \{z \in \mathbb{C}^N : L_1(z) = 0, ..., L_r(z) = 0\} \\ &= \{z \in \mathbb{C}^N : h_1(z) = 0, ..., h_s(z) = 0, L_1(z) = 0, ..., L_r(z) = 0\} \end{aligned}$$

is a zero-dimensional algebraic subvariety of $\mathbb{C}^N$. In particular W is nonempty. The variety W is defined by $s + r \leqslant s + N$ polynomials which belong to $\mathbb{Z}[Z_1, ..., Z_N]$ and which have degree at most D and logarithmic height at most $\max\{\eta, N(N+1)\log_2 D\}$. Let $\theta = (\theta_1, ..., \theta_N)$ be any point of W. Applying Proposition 14 to the variety W we deduce the estimate

$$\begin{aligned} \max\{\log_2 |\theta_i| : 1 \leqslant i \leqslant N\} &\leqslant D^{c'N}(\log_2 (s+N) \\ &\quad + \max\{\eta, N(N+1)\log_2 D\}) \\ &\leqslant D^{cN}(\log_2 s + \eta), \end{aligned}$$

where $c > 0$ is a suitable universal constant (here we use the assumption $D \geqslant N$). Since W is contained in V the point θ belongs to the variety V. Moreover the absolute values of the coordinates of θ satisfy the requirements in the conclusion of Proposition 9. ∎

4. POLYNOMIALS WHICH ARE HARD TO COMPUTE

In this last section we are going to exhibit some examples of *specific* time-space tradeoff hard families of univariate polynomials. In these examples we shall be able to exhibit significant lower bounds for the space requirements of any nonscalar time optimal procedure which evaluates these polynomials. We may divide our examples in two main groups following the criterion

whether the polynomials under consideration are given by their coefficients or by their roots. The interest of the latter group of examples is motivated by the search for lower complexity bounds in geometric elimination theory where the representation of polynomials given by their roots arises naturally (see [27]). A second division of our examples in two classes will be given by the distinction whether the polynomials under consideration have algebraic or only rational coefficients. We have tried to find an almost unified presentation for these example classes.

4.1. *Polynomials Given by Their Coefficients*

We present in this section a series of techniques for showing lower bounds for time-space tradeoffs and apply them to specific families of polynomials with integer and algebraic coefficients. We start with two particular families of polynomials with *integer coefficients* and show that these families are hard to compute in terms of time-space tradeoff. Then the same kind of result is proved for a specific family of polynomials with *algebraic coefficients*. Finally we show that there exist many families of polynomials with $\{0, 1\}$-*coefficients* which are hard to compute in terms of time-space tradeoff.

4.1.1. *Polynomials with Integer Coefficients.* In [55] there are presented several explicit families of polynomials with integer coefficients which are shown to be hard to compute in the sense of sequential time complexity. This kind of result is extended and improved in [50, 54]. We apply Proposition 9 in order to obtain time-space tradeoff results in the spirit of the above cited references.

EXAMPLE 15. Let $\mathscr{F}_1 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{Z}[X]$ of degree d defined by

$$F_d := \sum_{0 \leqslant j \leqslant d} 2^{j!} X^j.$$

Then this family $\mathscr{F}_1$ is hard to compute in the sense of time-space tradeoff. More precisely, we have

$$LS^2(F_d) = \Omega(d).$$

Proof. Let d be fixed and let $F := F_d$. Furthermore, let L and S be arbitrary natural numbers such that the polynomial F can be computed by a straight-line program in $\mathbb{Q}(X)$, using non-scalar time L and space S. Thus the polynomial F belongs to the image of the morphism

$$\Phi := \Phi_{d, L, S} := (P_d, ..., P_0) : \mathbb{C}^N \to \mathbb{C}^{d+1}$$

introduced in Lemma 5, with $N := 8LS^2 + 1$ and $P_0, ..., P_d \in \mathbb{Z}[Z_1, ..., Z_N]$. (Remember that we identify the polynomial $F \in \mathbb{Z}[X]$ with the point

$$(f_j)_{0 \leqslant j \leqslant d} := (2^{j!})_{0 \leqslant j \leqslant d}$$

of $\mathbb{C}^{d+1}$ given by the vector of coefficients of F.) We observe that $(f_j)_{0 \leqslant j \leqslant d}$ is the only point of $\mathbb{C}^{d+1}$ contained in the algebraic variety

$$\{(f_d, ..., f_0) \in \mathbb{C}^{d+1} : f_0 - 2 = 0, f_1 - f_0 = 0, ..., f_d - f_{d-1}^d = 0\}.$$

Let $Z = (Z_1, ..., Z_N)$ and consider the polynomials $Q_0, ..., Q_d \in \mathbb{Z}[Z]$ defined by $Q_0(Z) := P_0(Z) - 2$ and $Q_j(Z) := P_j(Z) - P_{j-1}^j(Z)$ with $1 \leqslant j \leqslant d$. Note that the Φ-fiber $V := \Phi^{-1}(F)$ of the point $F \in \mathbb{C}^{d+1}$ is the algebraic set

$$V = \{z \in \mathbb{C}^N : Q_0(z) = 0, ..., Q_d(z) = 0\}.$$

Let

$$D := \max\{\deg Q_i : 0 \leqslant j \leqslant d\}$$

and

$$\eta := \max\{\text{logheight } Q_j : 0 \leqslant j \leqslant d\}.$$

From Lemma 5 we deduce that

$$\deg Q_j \leqslant j \cdot \deg P_j \leqslant 2j(Ld + 1) \leqslant 2d(Ld + 1)$$

holds for $0 \leqslant j \leqslant d$.

This implies

$$D \leqslant 2d(Ld + 1). \tag{20}$$

Furthermore, from Lemma 5 we conclude

$$\begin{aligned} \text{logheight } Q_0 &\leqslant 2 + \log_2 \text{weight } P_0 \\ &\leqslant 2 + (d+1)^L \log_2 (12(S+1)), \end{aligned}$$

and

$$\begin{aligned}\text{logheight } Q_j &\leqslant 1 + \log_2 \text{weight } P_j + \log_2 (\text{weight } P_{j-1})^j \\ &\leqslant 1 + (j+1) \log_2 (12(S+1))^{(d+1)^L} \\ &\leqslant 1 + (d+1)^{L+1} \log_2 (12(S+1))\end{aligned}$$

for $1 \leqslant j \leqslant d$. This implies the height bound

$$\eta \leqslant 1 + (d+1)^{L+1} \log_2 (12(S+1)). \tag{21}$$

Applying Proposition 9 to the algebraic variety V above and taking into account the degree and height estimates (20) and (21), we conclude that V contains a point $\theta = (\theta_1, ..., \theta_N)$ satisfying the estimate

$$\log_2 \max\{|\theta_i| : 1 \leqslant i \leqslant N\} \leqslant D^{cN}(\log_2 (d+1) + \eta)\},$$

where $c > 0$ is a suitable universal constant. Let us write $|\theta| := \max\{|\theta_i| : 1 \leqslant i \leqslant N\}$. In order to finish the proof let us consider for $0 \leqslant j \leqslant d$ the jth coefficient f_j of the polynomial F. Since the image of the point θ under the morphism Φ is F, we have $f_j = P_j(\theta)$ for $0 \leqslant j \leqslant d$. Thus, by Lemma 5 the absolute value of f_j is bounded as

$$\begin{aligned}\log_2 |f_j| &\leqslant \log_2 \text{weight } P_j + \deg P_j \cdot \log_2 |\theta| \\ &\leqslant (d+1)^L \log_2 (12(S+1)) + 2(Ld+1)\, D^{cN}(\log_2 (d+1) + \eta).\end{aligned}$$

From Horner's rule we deduce that we may assume without loss of generality that $LS^2 \leqslant c_1 d$ holds for a suitable universal constant c_1. Combining this observation with the estimates (20) and (21) for D and η, we conclude that the absolute values of the coordinates $f_0, ..., f_d$ of the polynomial F satisfy the inequalities

$$d! \leqslant \max\{\log_2 |f_j| : 0 \leqslant j \leqslant d\} \leqslant d^{c_2 N},$$

where $c_2 > 0$ is a suitable universal constant. Thus we obtain $d! \leqslant d^{c_2 N}$ on one hand and $N = 8LS^2 + 1$ on the other. This implies $c_3 d \leqslant LS^2$ for a suitable universal constant $c_3 > 0$. Since L and S are the time and space requirements of an arbitrary straight-line program evaluating the polynomial $F = F_d$ we finally obtain $LS^2(F_d) = \Omega(d)$. ∎

EXAMPLE 16. Let $\mathscr{F}_2 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{Z}[X]$ of degree d defined by

$$F_d := \sum_{0 \leqslant j \leqslant d} 2^{2^j} X^j.$$

Then this family $\mathscr{F}_2$ is hard to compute in the sense of time-space tradeoff. More precisely, we have

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right).$$

The proof of this bound can be established in the same way as in Example 15. For given $d, L, S \in \mathbb{N}$ one has to consider the algebraic variety

$$\{(f_d, ..., f_0) \in \mathbb{C}^{d+1} : f_0 - 2 = 0, f_1 - f_0^2 = 0, ..., f_d - f_{d-1}^2 = 0\}$$

whose only point is the coefficient vector of the polynomial F_d. The $\Phi_{d, L, S}$-fiber of this variety is defined by $P_0(Z) - 2$ and the polynomials $P_j(Z) - P_{j-1}^2(Z)$ with $1 \leqslant j \leqslant d$. The remaining arguments are the same as in the proof of the lower bound of Example 15.

Let us remark that Example 16 is analyzed in [55] where the sequential time lower bound $L(F_d) = \Omega(\sqrt[3]{d}/\log_2 d)$ is shown.

4.1.2. *Polynomials with Algebraic Coefficients.* In this subsection we adapt two general methods for proving lower time-complexity bounds for polynomials with non-rational coefficients to the context of time-space tradeoffs. The first method we present was recently introduced by W. Baur (see [2]). The description of a similar idea can be found in [12, Chap. 9, Exercise 9.11].

PROPOSITION 17. *There exists a universal constant $c > 0$ with the following property: let D be a given natural number and let*

$$F := \sum_{0 \leqslant j \leqslant d} f_j X^j$$

be a polynomial of degree at most d with complex coefficients. Suppose that there exist polynomials $g_1, ..., g_m \in \mathbb{Q}[Y_d, ..., Y_0]$ of degree at most D, such that the complex values $g_1(f_d, ..., f_0), ..., g_m(f_d, ..., f_0)$ are $\mathbb{Q}$-linearly independent. Under these assumptions we have

$$LS^2(F) \geqslant c \cdot \frac{\log_2 m}{\log_2 d + \log_2 D}.$$

Proof. Let be given an arbitrary straight-line program β in $\mathbb{C}(X)$ which evaluates the polynomial F in nonscalar time L and space S. As before we deduce from Horner's rule that we may assume without loss of generality that $L \leqslant d$ holds. Let $N := 8LS^2 + 1$ and $\delta := 2(Ld + 1)$. Let $Z_1, ..., Z_N$ be new indeterminates. Then by Lemma 5 there exist polynomials $P_d, ..., P_0 \in \mathbb{Z}[Z_1, ..., Z_N]$ of degree at most δ such that the coefficient vector $(f_d, ..., f_0)$ of F is in the image of the morphism of affine spaces $\Phi_{d, L, S}: \mathbb{C}^N \to \mathbb{C}^{d+1}$ given by $(P_d, ..., P_0)$. Since by assumption the complex values $g_1(f_d, ..., f_0), ..., g_m(f_d, ..., f_0)$ are $\mathbb{Q}$-linearly independent and since there exists a point $\theta \in \mathbb{C}^N$ such that

$$(f_d, ..., f_0) = (P_d(\theta), ..., P_0(\theta))$$

holds, we conclude that the polynomials $g_1(P_d, ..., P_0), ..., g_m(P_d, ..., P_0)$ must be $\mathbb{Q}$-linearly independent too. Note that these polynomials have degree bounded by δD. This implies that the $\mathbb{Q}$-vector space

$$\mathscr{P} := \{ G \in \mathbb{Q}[Z_1, ..., Z_N] : \deg G \leqslant \delta D \}$$

has dimension at least m. On the other hand we have

$$\dim \mathscr{P} = \binom{N + \delta D}{N} \leqslant (\delta D)^N.$$

Taking into account $L \leqslant d$ we deduce from this the estimate

$$m \leqslant (\delta D)^N = (2(Ld + 1)\, D)^{8LS^2 + 1} \leqslant (2(d^2 + 1)\, D)^{8LS^2 + 1}.$$

Taking logarithms, we conclude that there exists a universal constant $c > 0$ such that

$$LS^2 \geqslant c \cdot \frac{\log_2 m}{\log_2 d + \log_2 D}$$

holds. Since β was an arbitrary straight-line program in $\mathbb{C}(X)$ computing the polynomial F in nonscalar time L and space S, Proposition 17 follows. ∎

The second method for showing lower bounds for time-space tradeoffs of polynomials with nonrational coefficients goes back to [30].

PROPOSITION 18. *There exists a universal constant $c>0$ with the following property: let D be a given natural number and let*

$$F := \sum_{0 \leqslant j \leqslant d} f_j X^j$$

be a polynomial of degree at most d with complex algebraic coefficients. Let ρ be the cardinality of the orbit of the point $(f_d, ..., f_0) \in \mathbb{C}^{d+1}$ under the action of the group of automorphisms of $\mathbb{C}$ over $\mathbb{Q}$. Suppose that there exist polynomials $g_1, ..., g_m \in \mathbb{Q}[Y_d, ..., Y_0]$ of degree at most D, such that the locus of common zeroes of these polynomials in $\mathbb{C}^{d+1}$ is finite and contains the point $(f_d, ..., f_0)$. Under these assumptions we have

$$LS^2(F) \geqslant c \cdot \frac{\log_2 \rho}{\log_2 d + \log_2 D}.$$

Proof. Let β be an arbitrary straight-line program in $\mathbb{C}(X)$ which evaluates the polynomial F in nonscalar time L and space S. Observe that the coefficient vector $(f_d, ..., f_0)$ of the polynomial F belongs to the algebraic subvariety $W := W_{d, L, S}$ of $\mathbb{C}^{d+1}$ introduced in Lemma 6. Let $r := \dim W$ and observe that $r \leqslant 8LS^2$ holds by the same lemma. We choose now r generic $\mathbb{Q}$-linear combinations

$$B_k := \beta_1^{(k)} g_1 + \cdots + \beta_m^{(k)} g_m \in \mathbb{Q}[Y_d, ..., Y_0]$$

of the polynomials $g_1, ..., g_m$ with $1 \leqslant k \leqslant r$ and coefficients $\beta_1^{(k)}, ..., \beta_m^{(k)} \in \mathbb{Q}$. The genericity of this choice and the fact that the polynomials $g_1, ..., g_m$ define a nonempty finite subset (i.e., a zero-dimensional subvariety) of $\mathbb{C}^{d+1}$ imply together with $r = \dim W$ that the set

$$V := W \cap \{(y_d, ..., y_0) \in \mathbb{C}^{d+1} : B_1(y_d, ..., y_0) = 0, ..., B_r(y_d, ..., y_0) = 0\}$$

is finite. Observe that $(f_d, ..., f_0) \in V$ holds and that $B_1, ..., B_r$ are polynomials of $\mathbb{Q}[Y_d, ..., Y_0]$ of degree at most D.

Therefore V is a zero-dimensional $\mathbb{Q}$-definable subvariety of $\mathbb{C}^{d+1}$ which contains the whole orbit of the point $(f_d, ..., f_0)$ under the action of the automorphism group of $\mathbb{C}$ over $\mathbb{Q}$. This implies $\rho \leqslant \# V = \deg V$.

From the Bézout Inequality and Lemma 6(ii) we infer

$$\deg V \leqslant \deg W \cdot D^r \leqslant \deg W \cdot D^{8LS^2} \leqslant (2(Ld+1)D)^{8LS^2}.$$

As before we may assume without loss of generality that $L \leqslant d$ holds. Putting all this information together we obtain the estimate

$$\rho \leqslant (2(d^2+1)\, D)^{8LS^2}.$$

Taking logarithms, we conclude that there exists a universal constant $c > 0$ such that $LS^2 \geqslant c \cdot (\log_2 \rho/(\log_2 d + \log_2 D))$ holds.

Since β was an arbitrary straight-line program in $\mathbb{C}(X)$ computing the polynomial F in nonscalar time L and space S, Proposition 18 follows. ∎

Using Propositions 17 and 18 we are now going to exhibit two families of polynomials with algebraic coefficients which are hard to compute in the sense of time-space tradeoff. These families were already analyzed in [30] and [20, Application 2] from the point of view of sequential time complexity.

EXAMPLE 19. (1) Let $\mathscr{F}_3 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{R}[X]$ of degree d defined by

$$F_d := \sum_{1 \leqslant j \leqslant d} \sqrt{p_j}\, X^j,$$

where p_j denotes the jth prime number. Then this family $\mathscr{F}_3$ is hard to compute in the sense of time-space tradeoff. More precisely, we have

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right).$$

(2) Let $\mathscr{F}_4 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{C}[X]$ of degree d defined by

$$F_d := \sum_{1 \leqslant j \leqslant d} e^{2\pi i/j} X^j$$

where $e^{2\pi i/j}$ stands for the (canonical) jth root of unity contained in $\mathbb{C}$. Then this family $\mathscr{F}_4$ is hard to compute in the sense of time-space tradeoff. More, precisely, we have

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right).$$

Proof. Let $Y_d, \ldots, Y_0$ be new indeterminates.

First we discuss the asymptotical lower bound for the family $\mathscr{F}_3$. We are going to apply Proposition 17.

For any $S \subseteq \{1, ..., d\}$ we consider the polynomial

$$g_S := \prod_{j \in S} Y_j \in \mathbb{Q}[Y_d, ..., Y_0].$$

Observe that the degree of g_S is bounded by d. From [20] we deduce easily that the family of complex values

$$(g_S(\sqrt{p_1}, ..., \sqrt{p_d}) : S \subseteq \{1, ..., d\})$$

is $\mathbb{Q}$-linearly independent. The lower bound for the time-space tradeoff of the family $\mathscr{F}_4$ follows now easily from Proposition 17 setting $m := 2^d$ and $D := d$.

As for the family $\mathscr{F}_3$, we will apply Proposition 18. Let us consider the polynomials

$$g_1 := Y_0, \qquad g_2 := Y_1 - 1, \qquad g_3 := Y_2^2 - 1, ..., g_{d+1} := Y_d^d - 1.$$

Observe that these polynomials vanish at the point $\theta := (0, e^{2\pi i/1}, ..., e^{2\pi i/d}) \in \mathbb{C}^{d+1}$ which represents the coefficients of the dth member of the family $\mathscr{F}_4$, namely the polynomial $F_d = \sum_{1 \leqslant j \leqslant d} e^{2\pi i/j} X^j$. Moreover, the polynomials $g_1, ..., g_{d+1}$ belong to $\mathbb{Q}[Y_d, ..., Y_0]$ and have degree at most d. They define a finite subset of $\mathbb{C}^{d+1}$. Let ρ be the cardinality of the orbit of the point θ under the action of the group of automorphisms of $\mathbb{C}$ over $\mathbb{Q}$. Let us denote by φ the Euler function and by $[1, ..., d]$ the least common multiple of the numbers $1, ..., d$. With this notation one sees easily that

$$\rho = [\mathbb{Q}(e^{2\pi i/1}, ..., e^{2\pi i/d}) : \mathbb{Q}] = \varphi([1, ..., d])$$

holds. From the Prime Number Theorem (see, e.g., [15]) one infers

$$\log_2 \rho = \log_2 \varphi([1, ..., d]) = \Omega(d).$$

The lower bound for the time-space tradeoff of the family $\mathscr{F}_4$ follows now easily from Proposition 18 setting $D := d$. ∎

4.1.3. *Polynomials with* $\{0, 1\}$*-Coefficients.* In this subsection we show that almost all polynomials with $\{0, 1\}$-coefficients are hard to compute in the sense of time-space tradeoff. The method we are going to use for the proof of this result was applied in a slightly different way in [29] in order to prove a lower bound for the nonscalar time complexity of these polynomials. Let us introduce the following notation.

For any natural number d let

$$LS^2_{\{0,1\}}(d) := \max\left\{LS^2\left(\sum_{0\leqslant j\leqslant d} f_j X^j\right) : (f_d, ..., f_0) \in \{0,1\}^{d+1}\right\}.$$

THEOREM 20. *Let $d \geqslant 2$ and k be natural numbers with $d > k \log_2 d$. Then the following holds*:

(i) $\#\{(f_d, ..., f_0) \in \{0,1\}^{d+1} : LS^2(\sum_{0\leqslant j\leqslant d} f_j X^j) \leqslant \frac{1}{16}(d/\log_2 d - k)\} \leqslant 2^d/d^k$,

(ii) $LS^2_{\{0,1\}}(d) \geqslant \frac{1}{16}(d/\log_2 d)$.

Proof. Let be given natural numbers d, k, L, S subject to the conditions $d \geqslant 2$, $d > k \log_2 d$ and $LS^2 \leqslant \frac{1}{16}(d/\log_2 d - k)$. Observe that the set $\{0,1\}^{d+1}$ can be defined as the intersection of $d+1$ hypersurfaces of $\mathbb{C}^{d+1}$ of degree 2, namely as

$$\{0,1\}^{d+1} = \{(f_d, ..., f_0) \in \mathbb{C}^{d+1} : f_d^2 - f_d = 0, ..., f_0^2 - f_0 = 0\}.$$

Applying [29, Proposition 2.3] and Lemma 6 of Section 2 we deduce from the Bézout Inequality the estimates:

$$\begin{aligned}\#(W_{d,L,S} \cap \{0,1\}^{d+1}) &\leqslant \deg W_{d,L,S} \cdot 2^{\dim W_{d,L,S}} \leqslant (4(Ld+1))^{8LS^2} \\ &\leqslant (8Ld)^{8LS^2} \leqslant (8LS^2 d)^{8LS^2}.\end{aligned}$$

Taking logarithms and using the assumption $LS^2 \leqslant \frac{1}{16}(d/\log_2 d - k)$, we conclude

$$\begin{aligned}\log_2(\#(W_{d,L,S} \cap \{0,1\}^{d+1})) &\leqslant 8LS^2 \log_2(8LS^2 d) \\ &\leqslant \frac{1}{2}\left(\frac{d}{\log_2 d} - k\right)\log_2\left(\frac{1}{2}\left(\frac{d}{\log_2 d} - k\right)d\right) \\ &\leqslant \frac{1}{2}\left(\frac{d}{\log_2 d} - k\right)\log_2\left(\frac{1}{2}d^2\left(\frac{1}{\log_2 d} - \frac{k}{d}\right)\right).\end{aligned}$$

Thus,

$$\begin{aligned}&\log_2(\#(W_{d,L,S} \cap \{0,1\}^{d+1})) \\ &\quad\leqslant \frac{1}{2}\left(\frac{d}{\log_2 d} - k\right)\left(2\log_2 d + \log_2\left(\frac{1}{2}\left(\frac{1}{\log_2 d} - \frac{k}{d}\right)\right)\right).\end{aligned}$$

From the assumption $d > k \log_2 d$ we deduce $0 < \frac{1}{2}(1/\log_2 d - k/d) < 1$. This implies

$$\log_2 (\#(W_{d,L,S} \cap \{0,1\}^{d+1})) \leqslant d - k \log_2 d.$$

From Lemma 6(iii) we infer now that

$$\#\left\{(f_d, ..., f_0) \in \{0,1\}^{d+1} : LS^2\left(\sum_{0 \leqslant j \leqslant d} f_j X^j\right) \leqslant \frac{1}{16}\left(\frac{d}{\log_2 d} - k\right)\right\} \leqslant \frac{2^d}{d^k}$$

holds, i.e., assertion (i) of the theorem. Assertion (ii) follows from (i) putting $k := 0$ and observing that the set $\{0,1\}^{d+1}$ has 2^{d+1} elements. ∎

4.2. *Polynomials Given by Their Roots*

The study of lower complexity bounds for the computation of families of polynomials given by their roots is motivated by their relationship with the intrinsic complexity of quantifier elimination procedures. Evidence for this relationship can be found in [27, 40]. In this subsection we exhibit two examples of families of polynomials given by their roots which are hard to compute in terms of time-space tradeoff.

Let $Y_{d-1}, ..., Y_0$ be new indeterminates and let

$$G := X^d + Y_{d-1} X^{d-1} + \cdots + Y_0$$

be the generic monic polynomial in the variable X with coefficients $Y_{d-1}, ..., Y_0$. Furthermore let $D(Y_{d-1}, ..., Y_0)$ be the discriminant of the polynomial G with respect to the variable X.

LEMMA 21. *Let $\mathscr{F}_5 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{Z}[X]$ of degree d defined by*

$$F_d := \prod_{1 \leqslant j \leqslant d} (X - 2^{2^j}).$$

Then F_d is the only monic polynomial $F = X^d + f_{d-1} X^{d-1} + \cdots + f_0$ of degree d with real coefficients which satisfies the following four conditions:

(1) $F(0) \neq 0$, $F(1) \neq 0$, $F(-1) \neq 0$.

(2) $D(f_{d-1}, ..., f_0) \neq 0$ (*this means that F has only simple roots*).

(3) *The polynomial F has only real roots.*

(4) *There exists a real number* t_0 *with* $t_0^2 \neq 4$ *such that*

$$(-1)^d 4f_0 = t_0^2$$

and

$$(-1)^d \cdot F(X) \cdot F(-X) \cdot (X^2 - 4) = (X^2 - t_0^2) \cdot F(X^2)$$

holds.

Proof. Putting $t_0 := 2^{2^d}$ one easily checks that the polynomial F_d satisfies the four conditions of the lemma. Therefore it is sufficient to show that there exists at most one monic polynomial $F = X^d + f_{d-1}X^{d-1} + \cdots + f_0 \in \mathbb{R}[X]$ of degree d which satisfies the conditions. Suppose now that such a polynomial F is given and fix a real number t_0 which satisfies the fourth condition with respect to this F. This condition implies that for any root x of F either $x^2 = t_0^2$ or $F(x^2) = 0$ holds. Thus for any root x of F one of the following two cases may occur:

(i) there exists a natural number k with $x^{2^k} = t_0^2$, or

(ii) any element of the set $S(x) := \{x^{2^m} : m \in \mathbb{N}\}$ is a root of F.

In case (ii) our assumptions on F imply that the set $S(x)$ is infinite. This rules out this case since F is monic. Therefore any root x of F satisfies (i). One easily sees $F(4) = 0$. Let r be a maximal nonnegative integer such that $2^2, 2^{2^2}, ..., 2^{2^r}$ are roots of F. From $F(4) = 0$ and $\deg F = d$ one concludes $1 \leqslant r \leqslant d$. The maximality of r implies $F(2^{2^{r+1}}) \neq 0$ whence $2^{2^{r+1}} = t_0^2 = (-1)^d 4f_0$. Thus we have $|t_0| > 1$.

We are now going to show that $r = d$ holds. Suppose that this is not the case. Since by assumption F has only simple roots which are all real there must exist $d - r$ distinct real zeroes $x_{r+1}, ..., x_d$ of F not contained in the set $\{2^2, 2^{2^2}, ..., 2^{2^r}\}$. Thus the roots of F are the real numbers $2^2, 2^{2^2}, ..., 2^{2^r}$, $x_{r+1}, ..., x_d$. This implies

$$2^{2^{r+1}} = (-1)^d \cdot 4 \cdot f_0 = 4 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^r} \cdot x_{r+1} \cdots x_d$$

and consequently $\prod_{r<i\leqslant d} x_i = 1$.

Let $r < m \leqslant d$. Since the root x_m of F satisfies (i) there exists a natural number k_m such that $x_m^{2^{km}} = t_0^2$ holds. Thus as $|t_0| > 1$ we have $|x_m| > 1$ for any $r < m \leqslant d$. But this contradicts our conclusion $\prod_{r<i\leqslant d} x_i = 1$.

That finishes the proof of the assertion $r = d$, saying that $2^2, 2^{2^2}, ..., 2^{2^d}$ are all roots of the monic polynomial F of degree d. With other words we have

$$F = \prod_{1 \leqslant j \leqslant d} (X - 2^{2^j}) = F_d. \quad \blacksquare$$

Let n be a natural number and let $X_1, ..., X_n$ be indeterminates over $\mathbb{Z}$. A subset S of $\mathbb{R}^n$ is called *semialgebraic* if there exists a finite set of polynomials $\mathscr{G} \subset \mathbb{Z}[X_1, ..., X_n]$ such that S is definable as a boolean expression built up from atomic formulas of type $G = 0$ or $G > 0$ with $G \in \mathscr{G}$. In this case we shall also say that S is *$\mathscr{G}$-definable* semialgebraic. A semialgebraic set has only finitely many connected components which are in turn semialgebraic (for more details see [5]).

In the sequel we shall use the following estimate which can be found in [59] (compare also [28, Theorem 4]):

PROPOSITION 22. *There exists a universal constant $c_0 > 0$ with the following property: Let n, D, s, h be natural numbers and let $\mathscr{G}$ be a set of s polynomials of $\mathbb{Z}[X_1, ..., X_n]$ having degree at most D and logarithmic height at most h, which defines a semialgebraic subset S of $\mathbb{R}^n$. Then the ball of $\mathbb{R}^n$ of radius $2^{h(sD)^{c_0 n}}$ centered at the origin intersects with every connected component of S at least in one point.*

We are now ready to prove that the family $\mathscr{F}_5$ is hard to compute in the sense of time-space tradeoff if we restrict ourselves to the field of parameters $K := \mathbb{R}$ (see Subsection 2.2):

PROPOSITION 23. *There exists a universal constant $c > 0$ with the following property: Let d, L, S be natural numbers and let*

$$F := \prod_{1 \leqslant j \leqslant d} (X - 2^{2^j}).$$

Let γ be a straight-line program in $\mathbb{R}(X)$ which computes the polynomial F using nonscalar time L and space S. Then we have

$$LS^2 \geqslant c \cdot \frac{d}{\log_2 d}.$$

Proof. Let us write $F = f_d X^d + f_{d-1} X^{d-1} + \cdots + f_0$ with $(f_d, ..., f_0) \in \mathbb{Z}^{d+1}$ and $f_d = 1$. Observe that F and $(f_{d-1}, ..., f_0)$ satisfy the four conditions of Lemma 21. We apply now Lemma 5 with $K := \mathbb{R}$. Following this

result and its proof, there exist for $N := 8LS^2 + 1$ polynomials $P_d, ..., P_0 \in \mathbb{Z}[Z_1, ..., Z_N]$ of degree at most $2(Ld+1)$ and weight at most $(12(S+1))^{(d+1)^L}$ such that the morphism of affine spaces $\Phi_{d,L,S}: \mathbb{R}^N \to \mathbb{R}^{d+1}$ introduced in this lemma maps the parameters of the straight-line program γ on $(f_d, ..., f_0) \in \mathbb{Z}^{d+1}$. Let $(\zeta_1, ..., \zeta_N)$ be the point of $\mathbb{R}^N$ representing the parameters of γ, let $\Phi := \Phi_{d,L,S}$ and let $V := \Phi^{-1}((f_d, ..., f_0))$ be the Φ-fiber of the integer point $(f_d, ..., f_0)$. Since $(\zeta_1, ..., \zeta_N)$ is contained in V, we conclude that V is nonempty. One verifies immediately that V is a semialgebraic subset of $\mathbb{R}^N$. Let $T, U_1, U_2, U_3, U_4, U_5$ be new indeterminates. Using the notation of Lemma 21 we consider the following polynomial equation system,

$$P_d - 1 = 0$$

$$P_0 U_1 - 1 = 0$$

$$\left(\sum_{0 \leqslant j \leqslant d} P_j \right) U_2 - 1 = 0$$

$$\left(\sum_{0 \leqslant j \leqslant d} (-1)^j P_j \right) U_3 - 1 = 0$$

$$D(P_{d-1}, ..., P_0)\, U_4 - 1 = 0$$

$$(T^2 - 4)\, U_5 - 1 = 0$$

$$(-1)^d 4P_0 - T^2 = 0$$

$$(-1)^d R(k)\, R(-k)(k^2 - 4) = (k^2 - T^2)\, R(k^2)$$

for $0 \leqslant k \leqslant 2d+2$ with $R := P_d X^d + \cdots + P_0$. Observe that the polynomials occurring in the above system belong to the ring $\mathbb{Z}[Z_1, ..., Z_N, T, U_1, ..., U_5]$ having degree at most $D := c' L d^3$ and logarithmic height at most $h := c'(d+1)^{L+1} \log_2(12(S+1))$ for a suitable universal constant $c' > 0$ and that there are at most $s := c'd$ of them. These polynomials codify the four conditions of Lemma 21. They define a semialgebraic subset W of $\mathbb{R}^N \times \mathbb{R}^6$. Let $\pi: \mathbb{R}^N \times \mathbb{R}^6 \to \mathbb{R}^N$ be the canonical projection which maps each point of $\mathbb{R}^N \times \mathbb{R}^6$ onto its first N components. From Lemma 21 and 5 one deduces easily that $\pi(W) = V$ holds. In particular W is nonempty. Applying Proposition 22 we see that W contains a point $\omega := (\theta_1, ..., \theta_N, t, u_1, u_2, u_3, u_4, u_5) \in \mathbb{R}^N \times \mathbb{R}^6$ with

$$\|\omega\| := (\theta_1^2 + \cdots + \theta_N^2 + t^2 + u_1^2 + u_2^2 + u_3^2 + u_4^2 + u_5^2)^{1/2} \leqslant 2^{h(sD)^{c_0}(N+6)},$$

where $c_0 > 0$ is the universal constant of this proposition. This implies that the semialgebraic set contains a point $\theta := (\theta_1, ..., \theta_N) \in \mathbb{R}^N$, namely $\theta = \pi(\omega)$, which satisfies

$$\log_2 |\theta| = \log_2 \max\{|\theta_i| : 1 \leqslant i \leqslant N\} \leqslant h(sD)^{c_0(N+6)}.$$

Without loss of generality we may suppose $L \leqslant d$. Therefore, taking into account $N = 8LS^2 + 1$, $s = c'd$, $D = c'Ld^3$ and $h = c'(d+1)^{L+1} \log_2 (12(S+1))$ we conclude that there exists a universal constant $c'' > 0$ such that the estimate $\log_2 |\theta| \leqslant d^{c''LS^2}$ holds. Since the point θ belongs to the Φ-fiber V of $(f_d, ..., f_0)$ we have $(-1)^d 2^{2^{d+1}-2} = (-1)^d \prod_{1 \leqslant j \leqslant d} 2^{2^j} = f_0 = P_0(\theta)$.

Reasoning as in the proof of the tradeoff lower bound of Example 15 we obtain the inequalities

$$\begin{aligned} \log_2 |f_0| = 2^{d+1} - 2 &\leqslant \log_2 \text{weight } P_0 + \deg P_0 \cdot \log_2 |\theta| \\ &\leqslant (d+1)^L \log_2 (12(S+1)) + 2(Ld+1)\, d^{c''LS^2}. \end{aligned}$$

Taking logarithms in these inequalities we deduce from $L \leqslant d$ that there exists a universal constant $c > 0$ such that

$$LS^2 \geqslant c \cdot \frac{d}{\log_2 d}$$

holds. ∎

EXAMPLE 24. Let as before $\mathscr{F}_5 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{Z}[X]$ of degree d defined by

$$F_d := \prod_{1 \leqslant j \leqslant d} (X - 2^{2^j}).$$

Then this family $\mathscr{F}_5$ is hard to compute in the sense of time-space tradeoff. More precisely we have

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right).$$

Proof. The lower bound we claim in this example refers to straight-line programs in $\mathbb{C}(X)$ and not in $\mathbb{R}(X)$ as in Proposition 23. However, one deduces this lower bound easily from that proposition: it is sufficient to observe that any straight-line program β in $\mathbb{C}(X)$ which computes for given $d \in \mathbb{N}$ the polynomial F_d, can be transformed into a straight-line program γ which evaluates F_d in nonscalar time $5L(\beta)$ and space $4S(\beta)$ using only

real parameters. One obtains this straight-line program γ by computing the real and imaginary part of each intermediate result of β separately (note that in view of [37] our time and space estimates for γ are even rather coarse). Our claim then follows easily from Proposition 23. ▮

We consider now a second example of a family of polynomials given by their roots which is hard to compute in the sense of time-space tradeoff. The polynomials of this second family will have algebraic coefficients. A similar example was analyzed in [27] from the point of view of sequential time complexity.

EXAMPLE 25. Let $\mathscr{F}_6 := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials $F_d \in \mathbb{R}[X]$ of degree d defined by

$$F_d := \prod_{1 \leqslant j \leqslant d} (X - \sqrt{p_j}),$$

where p_j denotes the jth prime number. Then this family $\mathscr{F}_6$ is hard to compute in the sense of time-space tradeoff. More precisely we have

$$LS^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right).$$

Proof. The lower bound we claim follows by adapting an argument first introduced in [2] to the context of time-space tradeoffs. Let $d \in \mathbb{N}$ be given and let $F := F_d$. For $1 \leqslant j \leqslant d$ we write σ_j for the jth elementary symmetric function in d arguments and $f_j := \sigma_j(\sqrt{p_1}, ..., \sqrt{p_d})$ for its value in the point $(\sqrt{p_1}, ..., \sqrt{p_d}) \in \mathbb{R}^d$. We have

$$F = \prod_{1 \leqslant j \leqslant d} (X - \sqrt{p_j}) = X^d - f_1 X^{d-1} + \cdots + (-1)^d f_d$$

for suitable real algebraic numbers $f_1, ..., f_d$. Let $X_1, ..., X_d$ and $Y_1, ..., Y_d$ be new indeterminates and let $1 \leqslant j \leqslant d$. The polynomial $N_j := X_1^{2j+1} + \cdots + X_d^{2j+1}$ is symmetric and hence there exists a (unique) polynomial $Q_j \in \mathbb{Z}[Y_1, ..., Y_d]$ of degree at most $2j+1$ such that

$$N_j(X_1, ..., X_d) = Q_j(\sigma_1(X_1, ..., X_d), ..., \sigma_d(X_1, ..., X_d))$$

holds (see, e.g., [60]). Let b_j be the real value

$$b_j := Q_j(f_1, ..., f_d).$$

One verifies immediately that

$$b_j = N_j(\sqrt{p_1}, ..., \sqrt{p_d}) = p_1^j \sqrt{p_1} + \cdots + p_d^j \sqrt{p_d}$$

holds. Thus the values $b_1, ..., b_d$ can be written as $\mathbb{Z}$-linear combinations of the values $\sqrt{p_1}, ..., \sqrt{p_d}$. The corresponding matrix is the nonsingular Vandermonde matrix $(p_k^j)_{1 \leqslant j,k \leqslant d}$. This implies that there exist $\mathbb{Q}$-linear forms $H_1, ..., H_d$ in d arguments such that $\sqrt{p_j} = H_j(b_1, ..., b_d)$ holds for $1 \leqslant j \leqslant d$. For any set $S \subseteq \{1, ..., d\}$ consider the polynomial

$$g_S := \prod_{j \in S} H_j(Q_1(Y_1, ..., Y_d), ..., Q_d(Y_1, ..., Y_d)).$$

Observe that $\deg g_S \leqslant d(2d+1)$ and

$$g_S(f_1, ..., f_d) = \prod_{j \in S} \sqrt{p_j}$$

holds. Thus

$$(g_S(f_1, ..., f_d) : S \subset \{1, ..., d\})$$

forms a family of 2^d real values which are $\mathbb{Q}$-linear independent. The lower bound for the time-space tradeoff of the family $\mathscr{F}_6$ follows now easily from Proposition 17 setting $m := 2^d$ and $D := d(2d+1)$. ∎

4.3. *Space Lower Bounds for Time Optimal Evaluation*

From Horner's rule follows that any univariate polynomial can be computed in constant space (see in this context also [4]). Therefore space can be arbitrarily small in polynomial evaluation if time is free.

However, restricting ourselves to time optimal procedures we obtain as an immediate consequence of our tradeoff results the following statement concerning space lower bounds (compare also Corollary 8):

PROPOSITION 26. *Let* $1 \leqslant i \leqslant 6$ *and let* $\mathscr{F}_i := (F_d^{(i)})_{d \in \mathbb{N}}$ *be any of the families of polynomials* $F_d^{(i)} \in \mathbb{C}[X]$ *introduced in the Examples* 15, 16, 19, 24, 25. *Then there exists a universal constant* $c > 0$ *with the following property*: *For any sequence* $(\beta_d)_{d \in \mathbb{N}}$ *of arithmetic circuits in* $\mathbb{C}(X)$ *such that* β_d *evaluates the polynomial* $F_d^{(i)}$ *in nonscalar time* $L(\beta_d) \leqslant \sqrt{d}$ *the space* $S(\beta_d)$ *used by* β_d *satisfies the lower bound*

$$S(\beta_d) \geqslant c \cdot \frac{\sqrt[4]{d}}{\sqrt{\log_2 d}}.$$

For the case of the family $\mathcal{F}_1$ this bound can be even improved to

$$S(\beta_d) \geqslant c \cdot \sqrt[4]{d}.$$

ACKNOWLEDGMENTS

This work was partially supported by the Spanish and Argentinian research grants: DGICYT PB96-0671-C02-02, Gobierno Foral de Navarra "Desarrollo e implementación de la estructura de datos *straight-line program*" (1996), UBACYT TW 80, ANPCyT 03-00000-01593, PIP CONICET 4571/96. Thanks go also to Klemens Hägele for his language corrections of a first draft of this paper.

REFERENCES

1. K. Abrahamson, Time-space tradeoffs for algebraic problems on general sequential machines, *J. Comput. System. Sci.* **43** (1991), 269–289.
2. W. Baur, Simplified lower bounds for polynomials with algebraic coefficients, *J. Complexity* **13** (1997), 38–41.
3. P. Beame, A general sequential time-space tradeoff for finding unique elements, *SIAM J. Comput.* **20** (1991), 270–277.
4. M. Ben-Or and R. Cleve, Computing algebraic formulas using a constant number of registers, *SIAM J. Comput.* **21** (1992), 54–58.
5. J. Bochnak, M. Coste, and M.-F. Roy, "Géométrie Algébrique Réelle," Ergebnisse der Mathematik und iher Grenzgebiete, Springer-Verlag, New York/Berlin, 1987.
6. A. Borodin, Time-space tradeoffs (getting closer to the barrier?), *in* "Algorithms and Computation, Proc. of the 4th ACM-SIGSAM Int. Symp. ISAAC'93" (K. W. Ny, Ed.), Lecture Notes in Computer Science, Vol. 762, pp. 209–220, Springer-Verlag, New York/Berlin, 1993.
7. A. Borodin and S. Cook, A time-space tradeoff for sorting on a general sequential model of computation, *SIAM J. Comput.* **11** (1982), 287–297.
8. A. Borodin, F. Fich, F. Meyer auf der Heide, E. Upfal, and A. Wigderson, A time-space tradeoff for element distinctness, *SIAM J. Comput.* **16** (1987), 97–99.
9. A. Borodin, M. J. Fischer, D. G. Kirkpatrick, N. A. Lynch, and M. Tompa, A time-space tradeoff for sorting on non-oblivious machines, *J. Comput. System Sci.* **22** (1981), 351–364.
10. A. Borodin and I. Munro, "The Computational Complexity of Algebraic and Numeric Problems," Elsevier, Amsterdam, 1975.
11. D. W. Brownawell, Bounds for the degree in the Nullstellensatz, *Ann. of Math.* **126** (1987), 577–591.
12. P. Bürgisser, M. Clausen, and M. A. Shokrollahi, "Algebraic Complexity Theory," Comprehensive Studies in Mathematics, Vol. 315, Springer-Verlag, New York/Berlin, 1997.
13. L. Caniglia, A. Galligo, and J. Heintz, Borne simplement exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque, *C. R. Acad. Sci. Paris Sér. I Math.* **307** (1988), 255–258.

14. L. Caniglia, A. Galligo, and J. Heintz, Some new effectivity bounds in computational geometry, *in* "Proceedings 6th International Symposium AAECC-6" (T. Mora, Ed.), Lecture Notes in Computer Science, Vol. 357, pp. 131–152, Springer-Verlag, New York/Berlin, 1989.
15. K. Chandrasekharan, "Introduction to Analytic Number Theory," Grundlehren der Math. Wissenschaften, Springer-Verlag, New York/Berlin, 1968.
16. P. Duris and Z. Galil, A time-space tradeoff for language recognition, *in* "Proceedings of the 22nd Annual IEEE Symposium on Foundations of Computer Science, 1981," pp. 53–57.
17. N. Fitchas and A. Galligo, Nullstellensatz effectif et Conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel, *Math. Nachr.* **149** (1990), 231–253.
18. W. Fulton, "Intersection Theory," Ergebnisse der Mathematik und iher Grenzgebiete, Vol. 24, Springer-Verlag, New York/Berlin, 1984.
19. J. von zur Gathen, "Parallel Linear Algebra," pp. 573–617, Morgan Kaufmann, San Mateo, CA, 1993.
20. J. von zur Gathen and V. Strassen, Some polynomials which are hard to compute, *Theoret. Comput. Sci.* **11** (1980), 331–335.
21. M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo, Lower bounds for diophantine approximation, *J. Pure Appl. Algebra* **117–118** (1997), 277–317.
22. M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo, Straight-line programs in geometric elimination theory, *J. Pure Appl. Algebra* **124** (1997), 101–146.
23. M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo, When polynomial equation systems can be "solved" fast?, *in* "Proceedings 11th International Symposium AAECC-11" (G. Cohen, M. Giusti, and T. Mora, Eds.), Lecture Notes in Computer Science, Vol. 948, pp. 205–231, Springer-Verlag, New York/Berlin, 1995.
24. D. Yu. Grigor'ev, An application of separability and independence notions for proving lower bounds of circuit complexity, Notes of Scientific Seminars of LOMI 60, Leningrad Departament, Steklov Mathematical Institute, 1976.
25. J. Heintz, Fast quantifier elimination over algebraically closed fields, *Theoret. Comput. Sci.* **24** (1983), 239–277.
26. J. Heintz, On the computational complexity of polynomials and bilinear mappings: A survey, *in* "Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-5" (L. Huget and A. Poli, Eds.), Lecture Notes in Computer Science, Vol. 356, pp. 269–300, Springer-Verlag, New York/Berlin, 1989.
27. J. Heintz and J. Morgenstern, On the intrinsic complexity of elimination theory, *J. Complexity* **9** (1993), 471–498.
28. J. Heintz, M.-F. Roy, and P. Solernó, Sur la complexité du principe de Tarski–Seidenberg, *Bull. Soc. Math. France* **118** (1990), 101–126.
29. J. Heintz and C. P. Schnorr, Testing polynomials which are easy to compute, *in* "Proceedings 12th Annual ACM Symposium on Theory of Computing, 1982," pp. 262–268.
30. J. Heintz and M. Sieveking, Lower bounds for polynomials with algebraic coefficients, *Theoret. Comput. Sci.* **11** (1980), 321–330.
31. J. Ja'Ja', Time-space tradeoffs for some algebraic problems, *J. Assoc. Comput. Math.* **30** (1983), 657–667.
32. J. Kollár, Sharp effective Nullstellensatz, *J. Amer. Math. Soc.* **1** (1988), 963–975.
33. T. Krick, J. Sabia, and P. Solernó, On intrinsic bounds in the Nullstellensatz, *Appl. Algebra Engrg. Comm. Comput.* **8** (1997), 125–134.

34. T. Krick and L. M. Pardo, A computational method for diophantine approximation, *in* "Proceedings MEGA'94 Algorithms in Algebraic Geometry and Applications, 1996" (L. González-Vega and T. Recio, Eds.), pp. 193–254.
35. T. Lengauer and R. E. Tarjan, Upper and lower bounds on time-space tradeoffs, *in* "Proceedings 11th Annual ACM Symposium on Theory of Computing, 1979," pp. 262–277.
36. T. M. Lickteig, "On Semialgebraic Decision Complexity," Habilitationsschrift, Universität Tübingen TR-90-052, Int. Comp. Sc. Inst., Berkeley, 1990.
37. T. M. Lickteig and K. Werther, How can a complex square root be computed in an optimal way? *Comput. Complexity* **5** (1995), 222–236.
38. C. Michaux, Une remarque à propos des machines sur $\mathbb{R}$ introduites par Blum, Shub et Smale, *C. R. Acad. Sci. Paris Sér. I Math.* **309** (1989), 435–437.
39. J. L. Montaña and L. M. Pardo, Lower bounds for arithmetic networks, *Appl. Algebra Engrg. Comm. Comput.* **4** (1993), 1–24.
40. L. M. Pardo, How lower and upper complexity bounds meet in elimination theory, *in* "Proceedings 11th International Symposium AAECC-11" (G. Cohen, M. Giusti, and T. Mora, Eds.), Lecture Notes in Computer Science, Vol. 948, pp. 33–69, Springer-Verlag, New York/Berlin, 1995.
41. M. S. Paterson and L. J. Stockmeyer, On the number of nonscalar multiplications necessary to evaluate polynomials, *SIAM J. Comput.* **2** (1973), 60–66.
42. W. J. Paul and R. E. Tarjan, Time-space tradeoffs in a pebble game, *Acta Inform.* **10** (1978), 111–115.
43. P. Philippon, Théorème des zéros effectif, d'après J. Kollár, Publications de l'Université Pierre et Marie Curie, Paris VI, 88, Groupe d'étude sur les Problèmes diophentiens 1988–1989, Exposé, 1989.
44. N. Pippenger, A time-space tradeoff, *J. Assoc. Comput. Match.* **25** (1978), 509–515.
45. N. Pippenger, Pebbling, *in* "Proceedings 5th IBM Symposium on Mathematical Foundations on Computer Science, 1980."
46. J. E. Savage, Space-time tradeoffs for banded matrix problems, *J. Assoc. Comput. Mach.* **31** (1984), 422–437.
47. J. E. Savage and S. Swamy, Space-time tradeoffs on the FFT algorithm, *IEEE Trans. Inform. Theory* **24** (1978), 563–568.
48. J. E. Savage and S. Swamy, Space-time Tradeoffs for Oblivious Integer Multiplication, *in* "Lecture Notes in Computer Science," Vol. 71, pp. 240–251, Springer-Verlag, New York/Berlin, 1979.
49. J. E. Savage, Space-time tradeoffs—A survey, *in* "Proceedings 3rd Hungarian Computer Science Conference, 1981."
50. C. P. Schnorr, Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials, *Theoret. Comput. Sci.* **7** (1978), 251–261.
51. I. R. Shafarevich, "Basic Algebraic Geometry I: Varieties in Projective Space," Springer-Verlag, New York/Berlin, 1994.
52. M. Sombra, Bounds for the Hilbert function of polynomials ideals and for the degrees in the Nullstellensatz, *J. Pure Appl. Algebra* **117–118** (1997), 565–599.
53. H. J. Stoss, Lower bounds for the complexity of polynomials, *Theoret. Comput. Sci.* **64** (1989), 15–23.
54. H. J. Stoss, On the representation of rational functions of bounded complexity, *Theoret. Comput. Sci.* **64** (1989), 1–13.

55. V. Strassen, Polynomials with rational coefficients which are hard to compute, *SIAM J. Comput.* **3** (1974), 128–149.
56. V. Strassen, Algebraic complexity, *in* "Handbook of Theoretical Computer Science," Chap. 11, pp. 634–672, Elsevier, Amsterdam, 1990.
57. M. Tompa, Time-space tradeoffs for computing functions using conectivity of their circuits, *J. Comput. System Sci.* **20** (1980), 118–132.
58. P. M. Vaidya, Space-time tradeoffs for orthogonal range queries, *in* "Proceedings 17th Annual ACM Symposium on Theory of Computing, 1985," pp. 169–174.
59. N. Vorobjov, Bounds of real roots of a system of algebraic equations, Notes of Scientific Seminars 137, Leningrad Department, Steklov Mathematical Institute, 1984.
60. B. L. van der Waerden, "Algebra I," Auflage der Modernen Algebra, Springer-Verlag, New York/Berlin, 1960.
61. A. C. Yao, Space-time tradeoff for answering range queries, *in* "Proceedings 14th Annual ACM Symposium on Theory of Computing, 1982," pp. 128–136.
62. A. C. Yao, Near optimal time-space tradeoff for element distinctness, *in* "Proceedings 29nd Annual IEEE Symposium on Foundations of Computer Science, 1988," pp. 183–187.
63. Y. Yesha, Time-space tradeoffs for matrix multiplication and the discrete Fourier transform on any sequential random access computer, *J. Comput. System Sci.* **29** (1984), 183–197.