

Lower Bounds and Real Algebraic Geometry

Peter Bürgisser

ABSTRACT. Many relevant problems in symbolic computation and computational geometry can be formalized as semi-algebraic computation or decision problems, to be solved by means of algebraic computation trees. It is a general paradigm that a complicated geometrical, topological, or combinatorial structure of a problem should result in high computational complexity. This survey outlines some of the ideas leading to lower bounds in terms of degree, Betti numbers, and number of faces of an arrangement or a polyhedron, emphasizing the role of real algebraic geometry in this endeavour. The impact of randomization on decision complexity is briefly discussed.

1. Introduction

Computational decision problems can often be cast in the following form: Given real numbers x_1, \dots, x_n , determine whether they satisfy some fixed system of polynomial equalities and inequalities. In other words, we have to decide for a given point $x \in \mathbb{R}^n$, whether it is contained in a fixed semi-algebraic subset W of \mathbb{R}^n . Our goal is the systematic study of the computational complexity to solve such problems. In Section 2.1 we list some basic computational problems, which can be formulated in such a way. We then indicate that typically, these problems can be algorithmically solved much faster than one would expect naively. The optimality proof of these algorithms is one of the great successes of algebraic complexity theory. In this survey, we present some of the most important ideas leading to nonlinear complexity lower bounds and optimality proofs. As the underlying model of computation, we use algebraic computation trees, which are introduced in Section 2.2.

Given the semi-algebraic formulation of the problems considered, it is not surprising, that the main tools to understand their intrinsic complexity are provided by real algebraic geometry. The concept of the degree of a (real) algebraic variety, and methods to estimate this degree play a key role throughout these investigations. By the degree of a real variety we will understand the geometric degree of its complexification.

We start our journey with geometrical lower bounds in Section 3. Strassen's Degree Bound 3.2 [54] is historically the first result, which provides nonlinear lower

1991 *Mathematics Subject Classification.* 68Q17; 14Pxx, 52B05, 55-xx.

Key words and phrases. algebraic complexity, lower bounds, real algebraic geometry, algebraic topology, arrangements and polyhedra.

complexity bounds. This fundamental insight bounds the nonscalar complexity of a set of rational functions from below by the logarithm of the degree of the graph of the associated rational map. The proof is a rather straightforward consequence of Bézout's Inequality 3.1. Another important idea is the Derivative Inequality 3.3 due to Baur and Strassen [1], which relates the complexity of a rational function with those of its gradient.

So far, peculiarities of the reals played no role. This changes, when we move on to the discussion of the decision complexity of an irreducible, real algebraic set W . An algebraic computation tree, which recognizes W in \mathbb{R}^n , does not necessarily recognize the complexification of W . Nevertheless, it is possible to derive a lower bound on the decision complexity of W in terms of the logarithm of the degree of W . This Real Degree Bound 3.4 is due to Lickteig and Roy [36].

In Section 4 we address lower bounds on the decision complexity of a semi-algebraic set in terms of its topological invariants. The major tool to obtain such results is the Milnor-Thom Bound 4.2 [46, 42, 57], which provides upper bounds on the sum of Betti numbers of semi-algebraic sets in terms of the degrees of the defining polynomials. Steele and Yao [53] recognized that the Milnor-Thom Bound 4.2 can be applied to obtain nontrivial lower bounds in terms of the number of connected components for the model of algebraic decision trees. This was extended to algebraic computation trees by Ben-Or [2], who proved the Connected Component Bound 4.1.

The extension of this result to higher Betti numbers took quite a while. It was first established for polyhedral sets W in the model of linear decision trees by Björner et al. [6], who proved a lower bound in terms of the Euler characteristic of W , and then generalized to higher Betti numbers by Björner and Lovász [5]. Finally, Yao [62, 63] succeeded in extending these results to the model of algebraic computation trees by proving the Betti Number Bound 4.4. The key idea is to replace the Betti numbers by those with compact supports, which behave subadditively with respect to the union of certain sets. This issue is discussed rather detailed in Section 4.2. We remark that Montaña et al. [44] have proved an extension of the Betti Number Bound 4.4 to parallel complexity.

In Section 5 we investigate the complexity to test membership to polyhedra or to unions of hyperplane arrangements. For polyhedra, the Betti Number Bound 4.4 does not yield good lower bounds since polyhedra are contractible and thus have trivial topology. On the other hand, it seems plausible that membership testing to a polyhedron with many faces is difficult. This was confirmed by Grigoriev et al. [27], who proved a lower bound in terms of the number of faces. Their proof is based on concepts from differential geometry and the Milnor-Thom Bound 4.2. It exploits the idea that when deforming a polyhedron to a smooth hypersurface H_ϵ , the points of H_ϵ close to a vertex of the polyhedron must have large principal curvatures. We do not go into the details of this complicated argument, but instead sketch the proof of a stronger lower bound (Face Bound 5.4), which is a consequence of the methods developed in the work by Grigoriev [21, 23] about randomized computation trees. Some of the new ideas are best explained by first treating the situation of complex arrangements, which is done in Section 5.1 following Grigoriev [22]. The Degree Bound 3.2 and the Derivative Inequality 3.3 play a key role in this argument.

In Section 6 we briefly address randomized decision complexity. The problem to prove nonlinear lower bounds for the real knapsack problem in the randomized

computation tree model was open for about a decade. It was attacked and finally solved in a sequence of papers authored by Grigoriev, Karpinski, Meyer auf der Heide, and Smolensky [25, 24, 26, 22, 23] culminating in the paper [23] by Grigoriev. The proof technique outlined in Section 5 is a by-product of this endeavour.

Acknowledgments. I thank Martin Lotz for discussions and helpful comments.

2. Problems, Fast Algorithms, and Models of Computation

2.1. Fast Algorithms. We list here a couple of fundamental computational or decisional problems over the real numbers and indicate a rapid algorithmical solution for each of these problems. In the complexity bounds mentioned, the symbol $M(n)$ will stand for an upper bound on the complexity to multiply two univariate polynomials of degree n over \mathbb{R} . We have $M(n) = O(n \log n)$, when counting all arithmetic operations, and $M(n) = O(n)$, when only the nonscalar multiplications and divisions are counted.

1. *Element Distinctness.* One has to decide for given real numbers x_1, \dots, x_n , whether they are pairwise distinct. Note that this means to test membership to the complement of a certain arrangement of real hyperplanes. It can be solved by sorting the given real numbers with $O(n \log n)$ comparisons. An algebraic solution is to first compute the discriminant $\prod_{i < j} (x_i - x_j)^2$ with $O(M(n) \log n)$ arithmetic operations [1] and then testing the result for zero.

2. *Convex Hull.* We want to compute the convex hull of n given points in the real plane. The output of the algorithm should consist of those input points, which are extremal points of the convex hull. A related decision problem is to find out, whether all the input points are extremal. Basic algorithms in computational geometry show that this can be done with $O(n \log n)$ arithmetic operations and tests (cf. [47]).

3. *Root Verification.* Given n real numbers x_1, \dots, x_n and a real polynomial $p(t) = \sum_{i=0}^n (-1)^i y_i t^{n-i}$ by its coefficients $y_0 = 1, y_1, \dots, y_n$. We have to verify whether the collection of the x_i forms the complete set of roots of $p(t)$ (including multiplicities). If we denote by σ_i the i th elementary symmetric polynomial in the x -variables, then this question amounts to test whether $y_i = \sigma_i(x_1, \dots, x_n)$ for all i . There are algorithms, which compute all the elementary symmetric polynomials from the x -variables with $O(M(n) \log n)$ arithmetic operations [54].

4. *Real Knapsack.* This is a membership problem to the union of a certain arrangement of real hyperplanes. One has to decide for given real numbers x_1, \dots, x_n whether there is a set of indices $I \subseteq \{1, \dots, n\}$ such that $\sum_{i \in I} x_i = 1$. The corresponding problem over the rationals is NP-complete [31]. Therefore, it is quite astonishing that the Real Knapsack Problem can be solved by linear decision trees with $O(n^4 \log n)$ tests, as shown by Meyer auf der Heide [39]. (Extensions to arbitrary hyperplane arrangements have been obtained by Meiser [38].) It seems that the computation tree model is too powerful to capture the “true” complexity of this problem.

5. *Continued Fraction and GCD:* Given are univariate real polynomials A_1 and A_2 of the degrees $n = \deg A_1 \geq \deg A_2$ by their coefficients. We are required to compute the (coefficients of the) quotients Q_1, \dots, Q_{t-1} occurring in the Euclidean algorithm

$$A_i = Q_i A_{i+1} + A_{i+2}, \quad \deg A_{i+2} < \deg A_{i+1}, \quad A_{i+1} \neq 0, \quad 1 \leq i \leq t-1, \quad A_{t+1} = 0,$$

as well as the greatest common divisor A_t of A_1 und A_2 . Note that the sequence (Q_1, \dots, Q_{t-1}) constitutes the continued fraction expansion of A_1/A_2 . By the Euclidean representation of the pair (A_1, A_2) we understand the extension of this sequence by the gcd A_t and we call

$$d := (d_1, \dots, d_{t-1}, d_t) := (\deg Q_1, \dots, \deg Q_{t-1}, \deg A_t)$$

the corresponding degree pattern.

We remark that by Sturm's theorem (cf. [7]) one can compute the number of zeros of a squarefree polynomial A_1 in any real interval from the Euclidean representation of A_1 and its derivative $A_2 = A_1'$ by just $O(n)$ arithmetic operations. For more information about the Euclidean algorithm and its countless applications, we refer to [19].

The Knuth-Schönhage algorithm [33, 32, 48, 43] is a sophisticated efficient algorithm for computing the Euclidean representation of given polynomials A_1, A_2 with $O(M(n) \log n)$ arithmetic operations. A more detailed analysis of this algorithm was done by Strassen [55]. Let $H(d) := -\sum_{d_i > 0} \frac{d_i}{n} \log \frac{d_i}{n}$ denote the entropy of the degree pattern d . Then the Knuth-Schönhage algorithm in fact uses $O(n(1+H(d)))$ arithmetic operations on a pair of input polynomials (A_1, A_2) , whose Euclidean representation has degree pattern d . (For a comprehensive account of these results see also [10].)

2.2. Models of Computation. Algebraic computation trees over the reals provide a formal framework to describe computations involving arithmetic operations, as well as branchings according to sign tests. They can be defined as finite ternary trees whose simple nodes are labeled by arithmetic instructions, while their branching nodes are labeled by sign tests. On an input $x \in \mathbb{R}^n$, the arithmetic operations and sign tests are successively executed and accordingly, the computation follows a unique path in the tree from the root to a leaf (if no attempt to divide by zero is made). In general, the output consists of some of the real numbers computed along this path and of the information, in which leaf of the tree the computation has ended up. Over the complex numbers, the computation trees are binary, as only equality tests are allowed. For formal definitions we refer to [10]. (Note that the model there is slightly different as only binary trees are considered.)

When studying decision problems, which is our main focus, we require that the leaves carry a 'yes' or 'no'-label, which provides the corresponding information. It is obvious that the sets of inputs accepted by such computation trees are just the semi-algebraic sets. We also remark that when studying decision problems, then we may assume without loss of generality that there are no divisions, since a quotient p/q can be encoded by the pair (p, q) , and one arithmetic operations on such quotients can be simulated by at most 4 arithmetic operations on the numerators and denominators.

By the *decision complexity* $C(W)$ of a semi-algebraic set W , we will understand the minimal number of nonscalar multiplications and branchings sufficient to solve this membership problem by means of algebraic computation trees in the worst case. Thus additions, subtractions, and multiplications with real scalars are not counted, which is motivated by the lower bounds we are going to prove. In other words, $C(W)$ is the minimal depth of algebraic computation trees solving the membership problem to W , where depth refers to the number of nonscalar multiplication and branching nodes.

A more restricted (and less realistic) model is that of algebraic decision trees. These are ternary trees whose inner nodes v are labeled by polynomials f_v . On input x , the computation starts at the root and branches at node v according to the sign of $f_v(x)$. Again the leaves carry a ‘yes’ or ‘no’-label. In this model, we count only the number of branchings, but we put a restriction on the f_v by requiring that their degree is less than or equal to some a priori bound d . The model of linear decision trees is obtained by the restriction $d = 1$. Usually, lower bounds are considerably easier to prove in these restricted models.

3. Geometrical Lower Bounds

3.1. Strassen’s Degree Bound. We consider the algorithmical problem to compute real polynomials f_1, \dots, f_m in $\mathbb{R}[X_1, \dots, X_n]$ from variables X_1, \dots, X_n (considered as the inputs) and real constants by means of straight-line programs. For simplicity of exposition, we assume that there are no divisions. A straight-line program performing this task produces a sequence $g_{-n+1} = X_1, \dots, g_0 = X_n, g_1, \dots, g_r$ of intermediate results such that for all $1 \leq k \leq r$ there are $i, j < k$ satisfying

$$g_k = g_i \circ g_j \text{ or } g_k = \lambda g_i, \quad \circ \in \{+, -, *\}, \lambda \in \mathbb{R},$$

and such that all f_i occur among the intermediate results. The special treatment of scalar multiplications is motivated by the lower bound we are going to prove, which in fact holds for the minimal number of nonscalar multiplications sufficient for such a computation. This quantity is called the (*nonscalar*) *complexity* $L(f_1, \dots, f_m)$ of the polynomials to be computed.

Since the degree can at most double in a multiplication step, it is obvious that $\deg g_k \leq 2^{\mu_k}$, where μ_k denotes the number of nonscalar multiplication steps in the initial segment of the computation up to g_k . Therefore, the degree bound $L(f_m) \geq \log_2 \deg f_m$ holds. Our goal will be an extension of this elementary observation.

We first note that any straight-line program solving the computation problem over the reals, also works over the complex numbers, hence we may assume without loss of generality that $f_i \in \mathbb{C}[X_1, \dots, X_n]$ and that the computation takes place in the polynomial ring over \mathbb{C} . However, we remark that for decision problems solved by algebraic computation trees, it makes a big difference whether we work over \mathbb{R} or \mathbb{C} , see Section 3.2.

The *degree* $\deg V$ of an irreducible, affine variety $V \subseteq \mathbb{C}^n$ of dimension d can be characterized as the finite number of intersection points of V with a generic affine subspace of \mathbb{C}^n having the complementary dimension $n - d$. This is a well-defined notion, as shown in algebraic geometry (cf. [50, 45, 29]). In algebraic complexity theory, it is common to define the degree of an affine variety as the sum of the degrees of all of its irreducible components (as opposed to the sum of the degrees of the components of maximal dimension). This is advantageous for degree estimations.

Bézout’s theorem relates the degree of the intersection of two varieties with the degrees of the varieties themselves. In algebraic complexity theory, the Bézout Inequality 3.1 given below is a fundamental tool. It can be derived in a straightforward way from the version of Bézout’s theorem treating the intersection of an irreducible variety with an irreducible hypersurface, see for instance [29, Thm. I.7.7] and [10]. We remark that Bézout’s Inequality 3.1 does also hold for the intersection of any two locally closed subsets in projective space.

BÉZOUT INEQUALITY 3.1. *Let V be an affine variety in \mathbb{C}^n and H be a hypersurface. Then we have $\deg(V \cap H) \leq \deg V \cdot \deg H$.*

We assign to a sequence (f_1, \dots, f_m) of polynomials the graph of the corresponding polynomial map $f: \mathbb{C}^n \rightarrow \mathbb{C}^m$ and define the degree $\deg(f_1, \dots, f_m)$ as the degree of this graph. Note that this clearly extends the usual notion of degree for polynomials ($m = 1$). What is the growth of the degrees $d_k := \deg(g_{-n+1}, \dots, g_k)$ during a straight-line computation with intermediate results g_i ? We first note that $d_0 = 1$. If $g_k = g_i * g_j$, then we can write $G_k := \text{graph}(g_1, \dots, g_{k-1}, g_k)$ as the intersection of $G_{k-1} \times \mathbb{C}$ with the quadric given by the equation $Y_k - Y_i Y_j = 0$, where the Y_i denote the corresponding coordinate variables. Since a quadric has degree two, we conclude with the Bézout Inequality 3.1 that $d_k \leq 2d_{k-1}$. In the case $g_k = \lambda g_i + \mu g_j$, $\lambda, \mu \in \mathbb{C}$, we obtain by intersecting with a linear subspace that $d_k \leq d_{k-1}$ (in fact, equality holds). We conclude that $d_k \leq 2^{\mu_k}$, where again μ_k denotes the number of nonscalar multiplication steps in the initial segment of the computation up to g_k . Finally, one can show that the degree does not increase under projections, which implies that $\deg(f_1, \dots, f_m) \leq d_r$. We therefore obtain the following fundamental result:

DEGREE BOUND 3.2 (Strassen [54], 1973). *For polynomials f_i over \mathbb{C} we have*

$$L(f_1, \dots, f_m) \geq \log_2 \deg(f_1, \dots, f_m).$$

We remark that this lower bounds remain true for the computation of rational functions when allowing divisions.

The Degree Bound 3.2 implies the optimality with respect to nonscalar complexity of numerous basic algorithms [54], see also [10]. For instance, for the elementary symmetric polynomials σ_i , it is not hard to see that $\deg(\sigma_1, \dots, \sigma_n) = n!$. The Degree Bound 3.2 implies $L(\sigma_1, \dots, \sigma_n) \geq \log_2(n!) \geq n(\log_2 n - 2)$, which shows the optimality of the corresponding algorithm mentioned in Section 2.1 (up to a constant factor).

One of the most beautiful applications of the Degree Bound 3.2 is the optimality of the Knuth-Schönhage algorithm (compare Section 2.1). Let $D(d)$ denote the set of all pairs (A_1, A_2) of complex polynomials, whose Euclidean representation has the degree pattern $d = (d_1, \dots, d_t)$. Strassen [55] proved that any algebraic computation tree over \mathbb{C} computing the Euclidean representation of given polynomials needs at least $n(H(d) - 2)$ nonscalar operations on all inputs (A_1, A_2) in a Zariski dense subset of $D(d)$. Schuster [49] proved a similar lower bound for the corresponding decision problem to test whether the Euclidean representation of a given input (A_1, A_2) has the degree pattern d . (This is based on the degree bound for decision complexity (3.3), cf. Section 3.2.)

The Degree Bound develops its full strength only in combination with the so-called Derivative Inequality, which relates the complexity of a polynomial f with the complexity of its gradient $\text{grad} f$ as follows:

DERIVATIVE INEQUALITY 3.3 (Baur and Strassen [1], 1983).

$$L(f, \text{grad} f) \leq 3L(f).$$

In combination with the Degree Bound 3.2 we obtain the lower bound

$$(3.1) \quad L(f) \geq \frac{1}{3} \log_2 \deg(f, \text{grad} f)$$

for the complexity of a polynomial f . This implies for instance the lower bound $L(\prod_{i < j} (X_i - X_j)^2) = \Omega(n \log_2 n)$ for the discriminant as a function of the roots [1], which we know to be optimal up to a constant factor from the discussion in Section 2.1.

3.2. Degree Bound over the Reals. Let $W \subset \mathbb{R}^n$ be an irreducible real algebraic set. We study the algorithmical problem to decide membership to W of input points $x \in \mathbb{R}^n$. Assume we are given an algebraic computation tree solving the membership problem to W . To each leaf v of this tree we can associate the *leaf set* D_v consisting of those inputs x in \mathbb{R}^n , whose computation in the tree ends up with the node v . The condition $x \in D_v$ can be expressed by sign conditions on the polynomials evaluated at x along the path to the leaf v . Each leaf set D_v may thus be written in the form

$$D_v = \{x \in \mathbb{R}^n \mid f_1(x) = 0, \dots, f_p(x) = 0, g_1(x) > 0, \dots, g_q(x) > 0\},$$

where the polynomials f_i and g_j are computed along the path of v and therefore have a nonscalar complexity bounded by $C(W) - p - q$. The set W is the union of all the leaf sets corresponding to ‘yes’-leaves. Hence there exists at least one leaf set D_v , which is Zariski dense in W . If we denote by U the open semi-algebraic set given by the corresponding conditions $g_j > 0, 1 \leq j \leq q$, and by $Z(f_1, \dots, f_p)$ the zero set of the f_i , we obtain that

$$(3.2) \quad W \cap U = D_v = Z(f_1, \dots, f_p) \cap U.$$

Over the complex numbers an analogous observation is true, we just have to replace the conditions $g_j > 0$ by the conditions $g_j \neq 0$, thus U is Zariski open in this case. In this situation, it is easy to obtain a lower bound on the decision complexity $C(W)$. Indeed, Equation (3.2) implies that W is an irreducible component of $Z(f_1, \dots, f_p)$, which relies on the general fact that a nonempty Zariski open subset of an irreducible algebraic set is Zariski dense in this algebraic set. By our definition of degree and the Bézout Inequality 3.1 we conclude $\deg W \leq \deg Z(f_1, \dots, f_p) \leq \deg(f_1, \dots, f_p)$. Thus from the Degree Bound 3.2, we obtain the following degree bound for the decision complexity $C(W)$ of an irreducible algebraic subset W of \mathbb{C}^n :

$$(3.3) \quad C(W) \geq \log_2 \deg W.$$

(Note that this lower bound is even valid for the number of nonscalar multiplications, irrespective of the number of branchings.)

This argument cannot be immediately transferred to the reals. In fact, a nonempty Euclidean open subset of an irreducible algebraic set V is Zariski dense in V iff it contains a regular point of V (cf. [7, §7.6]). (For instance, think of an irreducible, real elliptic curve having an isolated point; this point forms a Euclidean open subset of the curve.) Therefore, our argument gets stuck in the case where W is contained in the singular locus of $Z(f_1, \dots, f_p)$. As a way out, we define $f := f_1^2 + \dots + f_p^2$ and note that $L(f) \leq C(W)$ (we have traded the branchings for squaring operations). Note that $Z(f_1, \dots, f_p) = Z(f) = Z(f, \text{grad} f)$. The key observation is the following degree estimation

$$(3.4) \quad \deg W \leq \deg(f, \text{grad} f).$$

Hereby, the degree of the real irreducible algebraic set W is defined as the degree of its complexification $W_{\mathbb{C}}$, which we define as the Zariski closure of W in \mathbb{C}^n .

From this observation and the Derivative Inequality 3.3 we immediately obtain the desired degree bound over the reals:

REAL DEGREE BOUND 3.4 (Lickteig and Roy [36], 1996). *The decision complexity $C(W)$ of an irreducible real algebraic subset W of \mathbb{R}^n satisfies*

$$C(W) \geq \frac{1}{3} \log_2 \deg W.$$

The proof of the estimate (3.4) in [36] is based on a heavy machinery using the notion of the real spectrum. We are going to briefly explain the geometric idea behind the proof, without attempting to supply the subtle technical details. The basic idea is as follows: we perturb the equation $f = 0$ in order to achieve a nondegenerate situation (transversality) which can be easily handled, and then use a lower semi-continuity property of the degree.

We need the following general observation: Assume that V is an irreducible real algebraic set of dimension d and let h_1, \dots, h_{n-d} be polynomials vanishing on V , which intersect transversally in some point $\xi \in V$. Using the implicit function theorem, we see that the complex zero set of the given polynomials is a smooth, complex manifold of dimension d around ξ , and hence its complexification $V_{\mathbb{C}}$ is an irreducible component of the complex zero set $Z_{\mathbb{C}}(h_1, \dots, h_{n-d})$. By our definition of the real degree and the Bézout Inequality 3.1 we get

$$\deg V = \deg V_{\mathbb{C}} \leq \deg Z_{\mathbb{C}}(h_1, \dots, h_{n-d}) \leq \deg(h_1, \dots, h_{n-d}).$$

Let now W be a d -dimensional irreducible real algebraic set as in (3.2) and put $f := f_1^2 + \dots + f_p^2$. One can show that after some linear coordinate transformation, the system of perturbed equations

$$f = \epsilon, \partial_1 f = 0, \dots, \partial_{n-d-1} f = 0$$

defines for almost all $\epsilon > 0$ some d -dimensional irreducible component W_{ϵ} , in some of whose points these equations intersect transversally. (If the zero set of $f - \epsilon$ is compact, then this can be shown as in the proof of the Milnor-Thom Bound 4.2, see Section 4.1 and [10, Prop. 11.5].) Moreover, one can achieve that the family W_{ϵ} of real irreducible varieties “converges” to W as ϵ goes to zero. This convergence means that the limit of a sequence of polynomials vanishing on W_{ϵ} must vanish on W . One can show that the degree is lower semi-continuous with this respect. This can be done by replacing ϵ by an infinitesimal and by using the characterization of the degree of varieties by the leading coefficient of the corresponding Hilbert polynomials. (See [36] or [10, §8.5], where a similar problem is treated.) On the other hand, we have by the general observation from before that

$$\deg W_{\epsilon} \leq \deg(f - \epsilon, \partial_1 f, \dots, \partial_{n-d-1} f) \leq \deg(f, \text{grad} f),$$

which finishes our sketch of the proof.

As an application of the Real Degree Bound 3.4, we obtain the lower bound $\Omega(n \log n)$ for the complexity of the Root Verification problem, showing the optimality of the algorithm mentioned in Section 2.1.

The Real Degree Bound 3.4 allows to transfer the optimality results for the Knuth-Schönhage algorithm by Strassen [55] and Schuster [49] to the real setting. Thus it follows that any algebraic computation tree over \mathbb{R} computing the Euclidean representation of given polynomials needs at least $n(H(d) - 2)$ nonscalar operations on all inputs (A_1, A_2) in $D(d)$ outside a semi-algebraic subset of smaller dimension. This answers a question posed by Strassen [56].

To finish this section, we mention some further lower bound results involving concepts of real algebraic geometry. Lickteig [34, 35] proved a degree based lower bound on the decision complexity of irreducible real hypersurfaces, which is an extension of the lower bound (3.1) to the corresponding decision problem. In the papers [12, 13, 9] linear lower bounds are proved, which allow the determination of decision complexities in generic situations.

4. Topological Lower Bounds

4.1. Connected Components. Our goal is now to derive lower bounds on the decision complexity $C(W)$ of a semi-algebraic set W in \mathbb{R}^n in terms of topological invariants of the set W . The simplest such invariant is the the number $b_0(W)$ of connected components of W . If we focus on polyhedral sets W and restrict the model of computation to linear decision trees, then it is an easy exercise to show that at least $\log_3 b_0(W)$ sign tests are needed for deciding membership to W (each sign test decomposes the set under consideration into at most three connected components). It is a nontrivial result that this lower bound can be extended to the model of algebraic computation trees.

CONNECTED COMPONENT BOUND 4.1 (Ben-Or [2], 1983). *The decision complexity of a semi-algebraic set W in \mathbb{R}^n satisfies*

$$C(W) \geq \frac{1}{2}(\log_3 b_0(W) - n).$$

This result implies lower bounds of order $\Omega(n \log n)$ for the Element Distinctness or the Convex Hull problem and thus proves the optimality of the algorithms mentioned in Section 2.1. For the Knapsack problem, one obtains the lower bound $\Omega(n^2)$. For the determination of the number of connected components in these cases we refer to [15] or [10, Chap. 11].

The proof of the Connected Component Bound 4.1 relies on the fundamental bounds on the Betti numbers of real algebraic varieties due to Oleinik [46], Milnor [42], and Thom [57]. It will be convenient to denote the sum of all Betti numbers of a semi-algebraic set W by $b(W) := \sum_{k \in \mathbb{N}} b_k(W)$. The following bound on $b(W)$ given by Milnor is particularly useful for us.

MILNOR-THOM BOUND 4.2 (Milnor [42], 1964). *Assume W is the zero set of the polynomials $f_1, \dots, f_p \in \mathbb{R}[X_1, \dots, X_n]$ of degree at most d . Then we have*

$$b(W) \leq d(2d - 1)^{n-1}.$$

The proof ideas of this result are used at various places. For instance, they form the basis for the asymptotically fastest known algorithms for dealing with semi-algebraic sets, compare Grigoriev and Vorobjov [28] and the survey by Heintz et al. [30]. We remark that we have already used similar ideas in the proof of the Real Degree Bound 3.4.

Because of its importance, we briefly outline the main ideas of the proof of the Milnor-Thom Bound 4.2, for more details the reader may consult the original paper [42] or [7, 3]. First, the case of a smooth, compact hypersurface given by one equation $f = 0$ of degree $2d$ is settled. One shows that by a linear coordinate transformation, it can be achieved that the system of equations

$$f = 0, \partial_1 f = 0, \dots, \partial_{n-1} f = 0$$

has only nondegenerate solutions. This means that the restriction to W of the projection $\mathbb{R}^n \rightarrow \mathbb{R}$ onto the last coordinate is a Morse function, whose critical points are just the solutions of the above system of equations. By the Bézout Inequality 3.1, the number of critical points is bounded by $2d(2d-1)^{n-1}$. The Morse inequalities (cf. [41]) bound the sum $b(W)$ of Betti numbers by the number of critical points and thus provide the estimate in the special case considered (up to a factor of two).

In the general case, we set $f := f_1^2 + \dots + f_p^2$ and consider the compact sets $K_{\epsilon,r}$ given by the inequality $f(X) + \epsilon^2 \|X\|^2 \leq \epsilon^2 r^2$ with boundary $W_{\epsilon,r}$ described by the equation $f(X) + \epsilon^2 \|X\|^2 = \epsilon^2 r^2$. If $W_{\epsilon,r}$ is a smooth hypersurface, then we can bound its sum of Betti numbers as before. Moreover, Alexander duality [52, p. 296] implies for the complement $E_{\epsilon,r}$ of $K_{\epsilon,r}$ in \mathbb{R}^n that $\tilde{H}_k(E_{\epsilon,r}) \simeq H^{n-k-1}(K_{\epsilon,r})$ (the symbol \tilde{H}_k denotes the reduced homology). On the other hand, by Mayer-Vietoris, we have $\tilde{H}_k(W_{\epsilon,r}) \simeq \tilde{H}_k(K_{\epsilon,r}) \oplus \tilde{H}_k(E_{\epsilon,r})$. This implies that $b(W_{\epsilon,r}) = 2b(K_{\epsilon,r})$ and we obtain the upper bound $b(K_{\epsilon,r}) \leq d(2d-1)^{n-1}$.

We fix now $r > 0$ and use Sard's lemma (cf. [7]) to choose monotonically decreasing sequences $\epsilon_i \rightarrow 0$ and $r_i \rightarrow r$ such that all W_{ϵ_i, r_i} are smooth. The intersection W_r of W with the closed ball of radius r around the origin equals $W_r = \bigcap_i K_{\epsilon_i, r_i}$. Using standard facts from algebraic topology [52, §6.1] and the result that semi-algebraic sets can be triangulated (cf. [7, 3]), we see that for each k the cohomology group $H^k(W_r)$ is the direct limit of the $H^k(K_{\epsilon_i, r_i})$ as $i \rightarrow \infty$. This implies $b_k(W_r) \leq \liminf_i b_k(K_{\epsilon_i, r_i}) \leq d(2d-1)^{n-1}$. Finally, it is not hard to see that W_r is a deformation retract of W if r is chosen sufficiently large, which finishes the proof.

COROLLARY 4.3. *Assume that the semi-algebraic set W in \mathbb{R}^n is given by the conditions $f_1 = 0, \dots, f_p = 0, g_1 > 0, \dots, g_q > 0$, where f_i, g_j are polynomials of degree at most d . Then we have $b(W) \leq d(2d-1)^{n+q-1}$.*

In order to show this, let $\epsilon > 0$ and consider the subset W_ϵ of \mathbb{R}^n given by the conditions $f_i = 0, g_j \geq \epsilon$. This set is homeomorphic to the algebraic subset of \mathbb{R}^{n+q} described by the equations $f_i = 0, g_j = \epsilon + Y_j^2$, to which we can apply the Milnor-Thom Bound 4.2. Finally, we note that $W = \bigcap_{\epsilon > 0} W_\epsilon$ and use the semicontinuity property of the Betti numbers as above.

The proof of the Connected Component Bound 4.1 is now fairly simple. Recall the definition of the leaf set D_v of a computation tree corresponding to a leaf v given at the beginning of Section 3.2. We are going to bound the number of connected components of D_v . Fix a leaf v and consider the corresponding path in the tree. Forgetting for the moment about the test instructions, this path defines a straight-line program with intermediate results $g_{-n+1} = X_1, \dots, g_0 = X_n, g_1, \dots, g_r$. Similarly as in the proof of the Degree Bound 3.2, we can describe the graph of (g_{-n+1}, \dots, g_r) by a system of linear and quadratic equations in the variables $X_1, \dots, X_n, Y_1, \dots, Y_r$. We can make this description more concise by eliminating the Y -variables belonging to linear operations. Then the graph is homeomorphic to a subset of \mathbb{R}^{n+m} given by linear and quadratic equations, where m denotes the number of multiplication instructions along the path. By adding the linear inequalities corresponding to the sign tests, we obtain a subset of \mathbb{R}^{n+m} , which is homeomorphic to the leaf set D_v . If we assume that there are q sign tests along the path of v , then we obtain from Corollary 4.3 that $b_0(D_v) \leq 2 \cdot 3^{n+m+q-1}$

Suppose now that an algebraic computation tree solves the membership problem to the set W in \mathbb{R}^n . Then W is the union of all the leaf sets corresponding to ‘yes’-leaves and we have the estimate $m + q \leq C(W)$ for each path, since we count only the multiplications and the sign tests. The number of connected components behaves subadditively with respect to the union of sets. Therefore, as there are at most $3^{C(W)}$ leaves, we get

$$b_0(W) \leq \sum_v b_0(D_v) \leq 3^{C(W)} \cdot 2 \cdot 3^{n+C(W)-1} \leq 3^{n+2C(W)},$$

which finishes the proof of the Connected Component Bound 4.1.

4.2. Betti Numbers. Since the Milnor-Thom Bound 4.2 is valid for the sum of all Betti numbers, it is natural to ask whether the Connected Component Bound 4.1 can be extended correspondingly. The difficulty is that the higher Betti numbers do not behave subadditively with respect to the formation of unions (see Figure 1). The key idea is to work with a variant of Betti numbers, which behaves subadditively. This can be achieved by considering cohomology with compact supports. For the following facts from algebraic topology see [16, Chap. 8 §6].

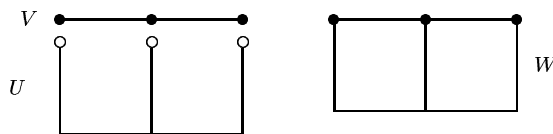


FIGURE 1. Betti numbers are not subadditive.

A locally closed subset of \mathbb{R}^n is defined as the intersection of an open with a closed subset of \mathbb{R}^n . Let $V \subseteq W$ be locally closed semi-algebraic subsets of \mathbb{R}^n . The *cohomology group with compact supports* $H_c^k(W, V)$ of the pair (W, V) is defined as the direct limit of the cohomology groups $H^k(W, V')$ over all subsets V' , ordered by reverse inclusion, such that $V \subseteq V' \subseteq W$ and $W \setminus V'$ is compact. By the *k*th *Betti number with compact supports* $b_{c,k}(W)$ of W we will understand the rank of $H_c^k(W) := H_c^k(W, \emptyset)$, and we write $b_c(W) := \sum_{k \in \mathbb{N}} b_{c,k}(W)$ for the sum of these Betti numbers. (We remark that the definition of $H_c^k(W, V)$ given in [16] refers to the Čech-cohomology. However, this coincides with the singular cohomology for semi-algebraic sets V, W , since the latter can be triangulated.)

If V is closed in W and $U := W \setminus V$, one can show that $H_c^k(W, V) = H_c^k(U)$ by excision. Under this assumption, we obtain from the long exact sequence

$$\dots \rightarrow H_c^k(W, V) \rightarrow H_c^k(W) \rightarrow H_c^k(V) \rightarrow H_c^{k+1}(W, V) \rightarrow \dots$$

the long exact sequence

$$\dots \rightarrow H_c^k(U) \rightarrow H_c^k(W) \rightarrow H_c^k(V) \rightarrow H_c^{k+1}(U) \rightarrow \dots$$

This implies the following crucial subadditivity property of the Betti numbers with compact supports:

$$(4.1) \quad b_{c,k}(W) \leq b_{c,k}(U) + b_{c,k}(V) \quad \text{if } V \text{ is closed in } W.$$

In order to compute the numbers $b_{c,k}(W)$ for a noncompact locally closed set W , we may use the Alexandrov compactification \hat{W} of W , which compactifies W by

adding a “point at infinity” ∞ . Since $\dot{W} = W \cup \{\infty\}$ and W is open in \dot{W} , we get $H_c^k(W) = H^k(\dot{W}, \{\infty\})$ and therefore

$$b_{c,k}(W) := b_k(\dot{W}) \text{ for } k > 0 \text{ and } b_{c,0}(W) = b_0(\dot{W}) - 1.$$

On the other hand, if W is compact, we have $H_c^k(W) = H^k(W)$ and thus $b_{c,k}(W) = b_k(W)$. For instance, we obtain $b_c(V) = b(V) = 1$, $b_c(W) = b(W) = 3$, $b_c(U) = 2$ for the example in Figure 1, thus verifying relation (4.1).

We remark that the Betti numbers with compact supports may also be interpreted as the rank of Borel-Moore homology groups ([8], [7, §11.7]).

The Connected Component Bound 4.1 now generalizes as follows:

BETTI NUMBER BOUND 4.4 (Yao [63], 1994). *The decision complexity of a locally closed semi-algebraic set W in \mathbb{R}^n satisfies*

$$C(W) \geq \frac{1}{2}(\log_3 b_c(W) - n - 1).$$

For the proof, we need an extension of Corollary 4.3 to Betti numbers with compact supports.

COROLLARY 4.5. *Assume that the locally closed semi-algebraic set W in \mathbb{R}^n is given by the conditions $f_1 = 0, \dots, f_p = 0, g_1 > 0, \dots, g_q > 0$, where f_i, g_j are polynomials of degree at most d . Then we have $b_c(W) \leq d(2d - 1)^{n+q}$.*

In order to show this, assume first that $q = 0$, hence W is closed. We may realize the compactification of W by the inverse of the stereographic projection $S^n \setminus \{(0, \dots, 0, 1)\} \xrightarrow{\sim} \mathbb{R}^n, x \mapsto y$ given by the equations $y_i = x_i / (1 - x_{n+1})$. Then \dot{W} is described by the equations $(1 - x_{n+1})^d f_i(x_i / (1 - x_{n+1})) = 0$ of degree d and the Milnor-Thom Bound 4.2 implies the assertion. The extension to inequalities can be done as in the proof of Corollary 4.3.

The proof of the Betti Number Bound 4.4 is completely analogous to the one of the Connected Component Bound 4.1. The only remaining issue is to prove that indeed $b_{c,k}(W) \leq \sum_v b_{c,k}(D_v)$ for an algebraic computation tree deciding membership to a locally closed semi-algebraic set W . To a node u of a such a tree we assign the semi-algebraic set W_u consisting of the points $x \in W$ whose path in the tree passes through u . It is obvious that W_u is locally closed. Let L_u denote the set of ‘yes’-leaves corresponding to paths passing through u . Then we have $W_u = \cup_{v \in L_u} D_v$. We prove now by reverse induction on the depth of u that

$$(4.2) \quad b_{c,k}(W_u) \leq \sum_{v \in L_u} b_{c,k}(D_v).$$

If u is a leaf, then there is nothing to show. Otherwise, let u be a node with the descendents u_-, u_0, u_+ corresponding to the outcome of the sign test with a polynomial f , thus $W_{u_-} = W \cap \{f < 0\}$, $W_{u_0} = W \cap \{f = 0\}$, $W_{u_+} = W \cap \{f > 0\}$. Since W_{u_0} is closed in $W_{u_-} \cup W_{u_0}$ and this set is closed in W_u , we may apply the subadditivity relation (4.1) twice, in order to obtain that $b_{c,k}(W_u) \leq b_{c,k}(W_{u_-}) + b_{c,k}(W_{u_0}) + b_{c,k}(W_{u_+})$. This shows the claim (4.2) and completes the proof of the Betti Number Bound 4.4.

A nice application of the Betti Number Bound 4.4 is the “ k -equal problem” considered in Björner et al. [6, 5]: Given n real numbers, decide whether k of them are equal ($k \geq 2$). Using a sorting argument, one can show that $O(n \log \frac{n}{k})$ comparisons are sufficient to solve this problem (in the linear decision tree model). The Betti Number Bound 4.4 shows that this is optimal, even in the model of

algebraic computation trees. One can compute the Betti numbers of subspace arrangements with the formula of Goresky and MacPherson [20], which characterizes the Betti numbers of the complement of a subspace arrangement by its intersection semi-lattice. For more information on this, we refer to the excellent survey by Björner [4].

We are currently investigating how the Betti Number Bound 4.4 performs on problems traditionally treated by Degree Bounds. An intriguing open problem is the decision complexity of the discriminant of univariate polynomials (as a function of the coefficients). The Knuth-Schönhage algorithm yields the upper bound $O(M(n) \log n)$ for this problem.

PROBLEM 4.6. Prove a lower bound of order $n \log n$ on the complexity to decide whether a given complex polynomial of degree n has a multiple root!

Degree bounds provide only lower bounds of order $\Omega(n)$ for this problem (compare [10, Ex. 8.24] for a related discussion for the resultant). The cohomology of the complement of the complex discriminant variety is intimately linked with the braid group and has been determined by Fuchs [18] (see also Vassiliev [60]). Unfortunately, the Betti numbers turn out to be too small to answer the above problem.

We remark that an interesting topological method to prove lower bounds was introduced by Smale [51] in connection with the problem to approximatively compute the roots of a complex polynomial. He also uses the model of algebraic computation trees over the reals, but considers as complexity measure the number of all branching nodes in the tree (a quantity typically exponentially larger than the complexity we consider in this article). The topology of the complement of the discriminant variety plays a central role in Smale's approach. Vassiliev has considerably improved and extended these results [58, 59, 60, 61].

5. Combinatorial Lower Bounds

5.1. Complex Arrangements. We consider an arrangement given by complex hyperplanes H_1, \dots, H_m in \mathbb{C}^n and let W denote the union of these hyperplanes. In Section 4 we have discussed how to bound the decision complexity by topological invariants of W (or its complement). It seems plausible, that also a complicated combinatorial structure leads to high computational complexity, and it turns out that this is indeed the case. By a k -dimensional face of the given arrangement, we understand a k -dimensional intersection of some of the given hyperplanes; a vertex is a 0-dimensional face. Let $N_k(W)$ denote the number of k -dimensional faces of W .

Suppose we have a computation tree deciding membership to W . There is a (unique) leaf set D_v , which is Zariski dense in $\mathbb{C}^n \setminus W$. We call the corresponding path generic, since Zariski almost all inputs follow this path in the tree. Suppose that f_1, \dots, f_r are the nonzero test polynomials computed along the generic path. Then the leaf set D_v is disjoint from W and it is described by the conditions $f_1 \neq 0, \dots, f_r \neq 0$. This implies that on each hyperplane H_i , some of the f_j must vanish, thus the product polynomial $f := f_1 \cdots f_r$ vanishes on W . This means that f is a multiple of $\ell_1 \cdots \ell_m$ if H_i is the zero set of the affine linear polynomial ℓ_i . Note that $L(f) \leq C(W)$ (trading multiplications for branchings).

By Equation (3.1) we know that $L(f) \geq \frac{1}{3} \log_2 \deg(f, \text{grad} f)$. The core of the method consists in the following important lower bound on the degree of $(f, \text{grad} f)$ in terms of the number of vertices of W .

THEOREM 5.1 (Grigoriev [22], 1999). *If a nonzero polynomial f vanishes on the union W of a complex hyperplane arrangement in \mathbb{C}^n , then we have*

$$\deg(f, \text{grad} f) \geq N_0(W)/2^{2n+1}.$$

This implies a lower bound on $C(W)$ in terms of $N_0(W)$. By intersecting W with a generic $(n - k)$ -dimensional hyperplane V and noting that $N_0(W \cap V) = N_k(W)$, we even obtain a lower bound in terms of the number of k -dimensional faces.

COROLLARY 5.2. *The decision complexity of the union W of a complex hyperplane arrangement in \mathbb{C}^n satisfies for all $0 \leq k \leq n$*

$$C(W) \geq \frac{1}{3}(\log_2 N_k(W) - 2(n - k) - 1).$$

It remains to outline the proof of Theorem 5.1. The essential idea behind is the quite intuitive observation that for each vertex x of the arrangement, each direction in \mathbb{C}^n can be obtained as a limit of the directions of $\text{grad} f(x^{(j)})$ for a suitable sequence of points $x^{(j)}$ tending to x . Hereby, a direction means a line in \mathbb{C}^n through the origin, that is, a point in the complex projective space \mathbb{P}^{n-1} .

In order to state this observation more succinctly, consider the graph G of $(f, \text{grad} f)$, which is the affine variety in $\mathbb{C}^{n+1} \times \mathbb{C}^n$ defined by

$$G := \{(x_0, x_1, \dots, x_n, y_1, \dots, y_n) \mid x_0 = f(x_1, \dots, x_n), y_i = \partial_i f(x_1, \dots, x_n)\}.$$

Clearly, $\dim G = n$. Let G_1 denote the closure of the image of $G \cap (\mathbb{C}^{n+1} \times (\mathbb{C}^n \setminus 0))$ under the canonical morphism $\mathbb{C}^{n+1} \times (\mathbb{C}^n \setminus 0) \rightarrow \mathbb{C}^{n+1} \times \mathbb{P}^{n-1}$. Then the above observation can be stated as follows. We omit the proof (cf. [22]):

LEMMA 5.3. *$(0, x_1, \dots, x_n) \times \mathbb{P}^{n-1}$ is contained in G_1 for any vertex $x = (x_1, \dots, x_n)$ of the arrangement.*

Let \mathcal{H} denote the zero set of the coordinate function X_0 in $\mathbb{C}^{n+1} \times \mathbb{P}^{n-1}$. The above lemma implies that $(0, x_1, \dots, x_n) \times \mathbb{P}^{n-1}$ is an irreducible component of $G_1 \cap \mathcal{H}$. We conclude that $G_1 \cap \mathcal{H}$ has at least as many irreducible components as there are vertices in the arrangement.

In order to proceed with a degree estimation, we embed $\mathbb{C}^{n+1} \times (\mathbb{C}^n \setminus 0)$ in a projective space using the Segre embedding:

$$\psi: \mathbb{C}^{n+1} \times (\mathbb{C}^n \setminus 0) \hookrightarrow \mathbb{P}^{n+1} \times \mathbb{P}^{n-1} \hookrightarrow \mathbb{P}^{2n^2+2n-1},$$

which maps the point $(x_0, x_1, \dots, x_n, y_1, \dots, y_n)$ to the point with homogeneous coordinates $((x_i y_j)_{0 \leq i \leq n, 1 \leq j \leq n} : y_1 : \dots : y_n)$. Let G'_1 and \mathcal{H}' be the images of G_1 and \mathcal{H} under this embedding, respectively. Then $G'_1 \cap \mathcal{H}'$ has at least $N_0(W)$ irreducible components, and we conclude that $N_0(W) \leq \deg(G'_1 \cap \mathcal{H}') \leq \deg G'_1$ using the Bézout Inequality 3.1 in projective space and $\deg \mathcal{H}' = 1$. By employing the fact that the coordinate functions of ψ are polynomials of degree at most two, it is not hard to see that $\deg G'_1 \leq 2^{2n+1} \deg G$ (cf. [22]). This implies the assertion of Theorem 5.1.

5.2. Real Arrangements and Polyhedra. We try to extend the previous results to real arrangements given by hyperplanes H_1, \dots, H_m in \mathbb{R}^n . With such an arrangement, we associate the union W of the hyperplanes, as well as the polyhedron W^+ defined as the intersection of the closed halfspaces H_i^+ corresponding to H_i . To be specific: if H_i is the zero set of the affine linear polynomial ℓ_i , then $H_i^+ = \{\ell_i \geq 0\}$. We always assume that W^+ is n -dimensional. Our focus will be on the decision complexity of the polyhedron W^+ , but the union W can be treated similarly (even in a simpler way). Note that the Betti Number Bound 4.4 does not provide a meaningful lower bound for the decision complexity of a polyhedron W^+ since it is contractible and thus $b_c(W^+) \leq 1$.

We denote by $N_k(W^+)$ the number of k -dimensional faces of the polyhedron W^+ . Yao and Rivest [64] proved that at least $\Omega(\log_2 N_k(W^+))$ sign tests are needed in the linear decision tree model for deciding membership to W^+ . It is possible to extend this result to the model of algebraic computation trees, answering Problem 11.1 in [10]. The Face Bound 5.4 below is a consequence of the methods developed in the work by Grigoriev [21, 23] about randomized computation trees. As mentioned in the Introduction, this result has been preceded by a weaker one due to Grigoriev et al. [27]. The proof in that paper is based on completely different concepts and considerably more complicated.

FACE BOUND 5.4. *The decision complexity of a polyhedron W^+ in \mathbb{R}^n given as an intersection of m closed halfspaces satisfies for any $0 \leq k \leq n$*

$$C(W^+) \geq \frac{1}{2}(\log_8 N_k(W^+) - \log_8 m - 2n).$$

This implies for the Element Distinctness problem and for the Knapsack problem lower bounds of the same order of magnitude as the Connected Component Bound 4.1. However, the Face Bound 5.4 has the advantage that it can be extended to the model of randomized computation trees (cf. Section 6).

We will now sketch the proof of the Face Bound 5.4. For simplicity of exposition, we restrict ourselves to the case of vertices ($k = 0$) and remark that the proof technique extends to higher dimensional faces without much difficulty.

Let H_1, \dots, H_n be hyperplanes in \mathbb{R}^n with $H_1 \cap \dots \cap H_n = \{0\}$. In order to simplify notation, we assume that $H_i = \{X_i = 0\}$ are the coordinate hyperplanes. We denote by $\text{tc}_n(f)$ the homogeneous part of lowest degree of a nonzero polynomial f in the variables X_1, \dots, X_n . Furthermore, we assign to f nonzero homogeneous polynomials $\text{tc}_i(f) \in \mathbb{R}[X_1, \dots, X_i]$ and multiplicities $\nu_i(f) \in \mathbb{N}$ by reverse induction on i : we define $\text{tc}_{i-1}(f)$ as the trailing coefficient of $\text{tc}_i(f)$ in the expansion with respect to the variable X_i , that is, the coefficient of the power of X_i of smallest degree in this expansion. We call this smallest degree the i th multiplicity $\nu_i(f)$. In suggestive notation we have

$$\text{tc}_i(f) = \text{tc}_{i-1}(f) X_i^{\nu_i(f)} + O(X_i^{\nu_i(f)+1}).$$

We note that $\deg \text{tc}_n(f) = \sum_{i=1}^n \nu_i(f)$ and $\nu_i(fg) = \nu_i(f) + \nu_i(g)$. We call a nonzero polynomial f *strongly singular* at the point 0 iff $\nu_i(f) > 0$ for all $1 \leq i \leq n$. Of course, this notion depends on the chosen hyperplanes H_i as well as on their order. (We remark that the definition in [23] is more general, which is necessary for coping with randomized trees.) Any nonzero multiple of a polynomial, which is strongly singular at 0, is strongly singular at 0 as well.

We define now what it means for a polynomial f to be strongly singular at a vertex of an arrangement (or of a polyhedron W^+). To simplify notation, we assume that the vertex is the origin 0. One can show that there exists a system of hyperplanes H_{i_1}, \dots, H_{i_n} of the underlying arrangement such that

$$(5.1) \quad \dim(W^+ \cap H_{i_1} \cap \dots \cap H_{i_n}) = \ell - 1 \quad \text{for } 1 \leq \ell \leq n + 1.$$

We say that the polynomial f is strongly singular at the vertex 0 of the given arrangement, iff it is strongly singular at 0 with respect to such a system of hyperplanes.

LEMMA 5.5. *Assume that an algebraic computation tree T decides membership to the polyhedron W^+ . Then for each vertex of W^+ there is a leaf v of the tree such that the product g_v of the (nonzero) test polynomials computed along the path to v is strongly singular at this vertex.*

For the proof it will be convenient to work with infinitesimals. If K is an ordered field, then we may extend this order to the rational function field $K(\epsilon)$ by defining an element $f = \alpha_r \epsilon^r + \alpha_{r+1} \epsilon^{r+1} + \dots$ of $K[\epsilon]$ to be positive iff the trailing coefficient α_r is positive. As $0 < \epsilon < a$ for all positive $a \in K$, the element ϵ can be interpreted as a positive infinitesimal with respect to K . We set now $K_0 := \mathbb{R}$ and successively define ordered fields $K_i = K_{i-1}(\epsilon_i)$ for $1 \leq i \leq n + 1$ by adjoining infinitesimals ϵ_i . Note that $\epsilon_1 > \dots > \epsilon_{n+1}$. From this construction of the orders it follows that for $f \in \mathbb{R}[X_1, \dots, X_n]$, for signs $\sigma_j \in \{-1, 1\}$ and $0 \leq i \leq n$ we have

$$(5.2) \quad \operatorname{sgn} f(\sigma_1 \epsilon_1 \epsilon_{n+1}, \dots, \sigma_n \epsilon_n \epsilon_{n+1}) = \sigma_{i+1}^{\nu_{i+1}(f)} \dots \sigma_n^{\nu_n(f)} \operatorname{sgn} \operatorname{tc}_i(f)(\sigma_1 \epsilon_1, \dots, \sigma_i \epsilon_i).$$

We note that the polyhedron W^+ can be naturally extended to a polyhedron contained in K_{n+1}^n , which we denote by the same symbol. Also, we may feed points in K_{n+1}^n as inputs to an algebraic computation tree.

We are now going to prove Lemma 5.5 and assume as before that the vertex considered is the origin, and that the hyperplanes H_{i_j} are as in (5.1). Without loss of generality, we assume that $H_{i_j}^+ = \{X_j \geq 0\}$. We have for all $1 \leq i \leq n$ that

$$E := \epsilon_{n+1}(\epsilon_1, \dots, \epsilon_n) \in W^+, \quad E_i := \epsilon_{n+1}(\epsilon_1, \dots, \epsilon_{i-1}, -\epsilon_i, \epsilon_{i+1}, \dots, \epsilon_n) \notin W^+$$

(in order to show that $E \in W^+$ use condition (5.1)). Let v be the leaf of the computation tree T corresponding to the input E , let f_1, \dots, f_r be the (nonzero) test polynomials computed along this path, and put $g_v := f_1 \dots f_r$. For each i , the path on input E_i is distinct from the path on input E . Hence there is a test polynomial f_ρ such that the signs of $f_\rho(E)$ and $f_\rho(E_i)$ are distinct. By (5.2), this implies that $\nu_i(f_\rho)$ must be odd, hence positive, hence $\nu_i(g_v) > 0$. As the index i was chosen arbitrarily, we conclude that g_v is strongly singular at the vertex 0 of the arrangement. This proves Lemma 5.5.

One can show the following analogue of Theorem 5.1.

THEOREM 5.6 (Grigoriev [23], 1999). *The number $N_0(W, f)$ of vertices of a real arrangement, at which a nonzero, real polynomial f is strongly singular, satisfies*

$$\deg(f, \operatorname{grad} f) \geq \frac{N_0(W, f)}{m 16^n}.$$

For the proof, the only thing to check is that Lemma 5.3 remains valid for vertices of the arrangement at which the polynomial f is strongly singular. We omit the details, which can be found in [23].

The proof of the Face Bound 5.4 for $k = 0$ is now an easy consequence. Suppose that we have an algebraic computation tree solving the membership problem to W^+ . By Lemma 5.5, Theorem 5.6, and Equation (3.1) we obtain

$$N_0(W^+) \leq \sum_v N_0(W, g_v) \leq 3^{C(W^+)} m 16^n 8^{C(W^+)} \leq m 8^{2n+2C(W^+)},$$

which shows the assertion.

6. Randomized Decision Complexity

Randomization is an important technique for algorithm design and can sometimes speed up computations considerably. One can generalize the model of algebraic computation trees to include randomization for instance by introducing “guess nodes”. We say that such a tree decides membership to W if the (two-sided) error probability is less than some positive $\epsilon < 1/2$. We abstain from giving a formal definition here. General results about the simulation of randomized by deterministic computation trees can be found in [40, 14].

Here is an example [11], which provably shows that randomization can help. The Root Verification problem has been previously shown to be of (deterministic) decision complexity $\Theta(n \log n)$. When allowing for randomization, this problem has complexity $O(n)$, which can be seen as follows: Choose $t \in \mathbb{R}$ uniformly at random in a set of $2n + 1$ points. Evaluate the polynomials $f(t) = t^n + \sum_{i=1}^n (-1)^i y_i t^{n-i}$ and $g(t) = \prod_{i=1}^n (t - x_i)$ with $O(n)$ operations, and test whether these values are equal. If $y_i = \sigma_i(x)$ for all $1 \leq i \leq n$, then $f(t) = g(t)$. Otherwise, $f(t) \neq g(t)$ with probability less than $1/2$.

This simple example already shows that the previously discussed lower bounds on decision complexity in terms of degree or Betti numbers in general do not extend to the randomized model! Interestingly, some lower bounds for irreducible hypersurfaces can be extended. For instance, randomized checking of the value of a middle elementary symmetric polynomial, i.e., whether $y_{n/2} = \sigma_{n/2}(x)$, requires $\Omega(n \log n)$ operations [11]. In the same paper, it is also proven that randomization does not help to check the value of the determinant (while checking matrix multiplication seems to be easier using randomization [17]).

What can be said about the randomized decision complexity of hypersurfaces with many irreducible components, say hyperplane arrangements? Recall that the Element Distinctness and the Knapsack problem are of this type. For the model of randomized linear decision trees, Manber and Tompa [37] obtained lower bounds of the same order of magnitude as the deterministic ones. In the model of algebraic computation trees, the situation is considerably more complicated. In a sequence of papers authored by Grigoriev, Karpinski, Meyer auf der Heide, and Smolensky [25, 24, 26, 22, 23] this problem was treated, first in the model of randomized algebraic decision trees, and then for randomized algebraic computation trees. So far, the last word was spoken by Grigoriev [23], who obtained a bound in terms of the number of faces of a polyhedron, or of an arrangement of real hyperplanes. The proof of this result is an extension of the ideas explained in Section 5, which were in fact developed in order to tackle this question! We do not state Grigoriev’s result [23], as it is rather technical. As an application, one obtains lower bounds for the Element Distinctness and the Knapsack problem, which are of the same order of magnitude as the deterministic ones.

These lower bounds for hyperplane arrangements in the randomized model in general cannot be extended to subspace arrangements of higher codimension, as the following example shows. Consider the Set Equality problem to decide for two given sequences of reals $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ whether there exists a permutation π such that $y_i = x_{\pi(i)}$. This means that the elementary symmetric polynomials have the same value on x and y . The Connected Component Bound 4.1 shows that the deterministic decision complexity of the Set Equality problem is $\Theta(n \log n)$. However, using randomization, Set Equality can be checked with $O(n)$ operations by the same idea as for the Root Verification problem. (However, the bound $\Omega(n \log n)$ for Set Equality is optimal in the linear decision tree model [37].)

Despite the recent impressive progress it seems that the impact of randomization on algebraic decision complexity is still far from being understood.

References

- [1] W. Baur and V. Strassen, *The complexity of partial derivatives*, Theoret. Comp. Sci. **22** (1983), 317–330.
- [2] M. Ben-Or, *Lower bounds for algebraic computation trees*, Proc. 15th ACM STOC, Boston, 1983, pp. 80–86.
- [3] R. Benedetti and J.-J. Risler, *Real algebraic and semi-algebraic sets*, Hermann, 1990.
- [4] A. Björner, *Subspace arrangements*, Proc. of 1st European Congress of Mathematics (Paris, 1992), Birkhäuser, 1992, pp. 321–370.
- [5] A. Björner and L. Lovász, *Linear decision trees, subspace arrangements and Möbius functions*, J. Amer. Math. Soc. **7** (1994), no. 3, 677–706.
- [6] A. Björner, L. Lovász, and A.C. Yao, *Linear decision trees: volume estimates and topological bounds*, Proc. 24th ACM STOC, 1992, pp. 171–177.
- [7] J. Bochnak, M. Coste, and M.F. Roy, *Géométrie algébrique réelle*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 12, Springer Verlag, 1987.
- [8] A. Borel and J.C. Moore, *Homology theory for locally compact spaces*, Michigan Math. J. **7** (1960), 137–159.
- [9] P. Bürgisser, *Decision complexity of generic complete intersections*, Research Report 8578-CS, Institut für Informatik der Universität Bonn, 1992.
- [10] P. Bürgisser, M. Clausen, and M.A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der mathematischen Wissenschaften, vol. 315, Springer Verlag, 1997.
- [11] P. Bürgisser, M. Karpinski, and T. Lickteig, *On randomized semialgebraic decision complexity*, J. Compl. **9** (1993), 231–251.
- [12] P. Bürgisser and T. Lickteig, *Verification complexity of linear prime ideals*, J. Pure Appl. Alg. **81** (1992), 247–267.
- [13] P. Bürgisser, T. Lickteig, and M. Shub, *Test complexity of generic polynomials*, J. Compl. **8** (1992), 203–215.
- [14] F. Cucker, M. Karpinski, P. Koiran, T. Lickteig, and K. Werther, *On real Turing machines that toss coins*, Proc. 27th ACM STOC, Las Vegas, 1995, pp. 335–342.
- [15] D. Dobkin and R.J. Lipton, *A lower bound of $\frac{1}{2}n^2$ on linear search programs for the knapsack problem*, J. Comp. Syst. Sci. **16** (1978), 413–417.
- [16] A. Dold, *Lectures on algebraic topology*, Grundlehren der mathematischen Wissenschaften, vol. 200, Springer Verlag, 1972.
- [17] R. Freivalds, *Fast probabilistic algorithms*, LNCS, no. 74, Springer Verlag, 1979, pp. 57–69.
- [18] D.B. Fuchs, *Cohomology of the braid group mod 2*, Funct. Anal. Appl. **4(2)** (1970), 46–59.
- [19] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, 1999.
- [20] M. Goresky and R.D. MacPherson, *Stratified Morse theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 14, Springer Verlag, 1988.
- [21] D.Yu. Grigoriev, *Randomized complexity lower bounds*, Proc. 30th ACM STOC, 1998, pp. 219–223.

- [22] ———, *Complexity lower bounds for randomized computation trees over zero characteristic fields*, *Comp. Compl.* **8** (1999), 316–329.
- [23] ———, *Randomized complexity lower bound for arrangements and polyhedra*, *Discrete Comput. Geom.* **21(3)** (1999), 329–344.
- [24] D.Yu. Grigoriev and M. Karpinski, *Randomized quadratic lower bound for knapsack*, *Proc. 29th ACM STOC*, 1997, pp. 76–85.
- [25] D.Yu. Grigoriev, M. Karpinski, F. Meyer auf der Heide, and R. Smolensky, *A lower bound for randomized algebraic decision trees*, *Proc. 37th STOC*, 1996, pp. 612–619.
- [26] D.Yu. Grigoriev, M. Karpinski, and R. Smolensky, *Randomization and the computational power of analytic and algebraic decision trees*, *Comp. Compl.* **6** (1996/97), no. 4, 376–388.
- [27] D.Yu. Grigoriev, M. Karpinski, and N. Vorobjov, *Lower bound on testing membership to a polyhedron by algebraic decision and computation trees*, *Discrete Comput. Geom.* **17** (1997), 191–215.
- [28] D.Yu. Grigoriev and N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, *J. Symb. Comp.* **5** (1988), 37–64.
- [29] R. Hartshorne, *Algebraic geometry*, GTM, Springer Verlag, 1977.
- [30] J. Heintz, T. Recio, and M.F. Roy, *Algorithms in real algebraic geometry and applications to computational geometry*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **6** (1991), 137–163.
- [31] R.M. Karp, *Reducibility among combinatorial problems*, *Complexity of Computer Computations* (R.E. Miller and J.W. Thatcher, eds.), New York, 1972, pp. 85–104.
- [32] D.E. Knuth, *The analysis of algorithms*, Actes du congrès international des Mathématiciens, Nice, vol. 3, 1970, pp. 269–274.
- [33] D.H. Lehmer, *Euclid’s algorithm for large numbers*, *Amer. Math. Monthly* **45** (1938), 227–233.
- [34] T. Lickteig, *On semialgebraic decision complexity*, Tech. Report TR-90-052, Int. Comp. Sc. Inst., Berkeley, 1990, Habilitationsschrift, Universität Tübingen.
- [35] ———, *Semi-algebraic decision complexity, the real spectrum, and degree*, *J. Pure Appl. Alg.* **110** (1996), 131–184.
- [36] T. Lickteig and M.F. Roy, *Semi-algebraic complexity of quotients and sign determination of remainders*, *J. Compl.* **12** (1996), 545–571.
- [37] U. Manber and M. Tompa, *Probabilistic, nondeterministic, and alternating decision trees*, *Proc. 14th ACM STOC*, 1982, pp. 234–244.
- [38] S. Meiser, *Point location in arrangements of hyperplanes*, *Information and Computation* **106** (1993), 286–303.
- [39] F. Meyer auf der Heide, *A polynomial linear search algorithm for the n-dimensional knapsack problem*, *J. ACM* **31** (1984), 668–676.
- [40] ———, *Simulating probabilistic by deterministic algebraic computation trees*, *Theoret. Comp. Sci.* **41** (1985), 325–330.
- [41] J. Milnor, *Morse theory*, *Annals of Math. Studies*, no. 51, Princeton University Press, 1963.
- [42] ———, *On the Betti numbers of real varieties*, *Proc. AMS*, vol. 15, 1964, pp. 275–280.
- [43] R.T. Moenck, *Fast computation of GCDs*, *Proc. 5th ACM STOC*, 1973, pp. 142–151.
- [44] J.L. Montaña, J.E. Morais, and L.M. Pardo, *Lower bounds for arithmetic networks II: Sum of Betti numbers*, *AAECC* **7** (1996), 41–51.
- [45] D. Mumford, *Algebraic geometry I: Complex projective varieties*, Springer Verlag, 1976.
- [46] O.A. Oleĭnik, *Estimates of the Betti numbers of real algebraic hypersurfaces*, *Math. Sb. (N.S.)* **28 (70)** (1951), 635–640.
- [47] F.P. Preparata and M.I. Shamos, *Computational geometry, an introduction*, Texts and Monographs in Computer Science, Springer Verlag, 1985.
- [48] A. Schönhage, *Schnelle Berechnung von Kettenbruchentwicklungen*, *Act. Inf.* **1** (1971), 139–144.
- [49] P. Schuster, *Interpolation und Kettenbruchentwicklung. Die Komplexität einiger Berechnungsaufgaben*, Ph.D. thesis, Univ. Zürich, 1980.
- [50] I.R. Shafarevich, *Basic algebraic geometry*, Springer Verlag, 1974.
- [51] S. Smale, *On the topology of root finding*, *J. Compl.* **3** (1987), 81–89.
- [52] E. Spanier, *Algebraic topology*, MacGraw-Hill, 1966.
- [53] J.M. Steele and A.C. Yao, *Lower bounds of algebraic decision trees*, *J. Algorithms* **3** (1982), 1–8.

- [54] V. Strassen, *Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten*, Num. Math. **20** (1973), 238–251.
- [55] ———, *The computational complexity of continued fractions*, SIAM J. Comp. **12** (1983), 1–27.
- [56] ———, *Algebraic complexity theory*, Handbook of Theoretical Computer Science (J. van Leeuwen, ed.), vol. A, Elsevier Science Publishers B. V., Amsterdam, 1990, pp. 634–672.
- [57] R. Thom, *Sur l'homologie des variétés algébriques réelles*, Differential and Combinatorial Topology (S.S. Cairns, ed.), Princeton Univ. Press, 1965, pp. 255–265.
- [58] V.A. Vassiliev, *Cohomology of braid groups and complexity of algorithms*, Funct. Anal. Appl. **22** (1988), 15–24.
- [59] ———, *Topological complexity of algorithms of approximate solving the systems of polynomial equations*, Algebra Anal. **1** (1989), 198–213.
- [60] ———, *Complements of discriminants of smooth maps: Topology and applications*, Transl. of Math. Monographs, no. 98, AMS, 1992.
- [61] ———, *Cohomology of braid groups and complexity*, From Topology to Computation: Proceedings of the SMALEFEST, Springer Verlag, 1993, pp. 359–367.
- [62] A.C. Yao, *Algebraic decision trees and Euler characteristic*, Proc. 33rd FOCS, 1992.
- [63] ———, *Decision tree complexity and Betti numbers*, Proc. 26th ACM STOC, 1994.
- [64] A.C. Yao and R.L. Rivest, *On the polyhedral decision problem*, SIAM J. Comp. **9** (1980), 343–347.

DEPT. OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF PADERBORN, D-33095
PADERBORN, GERMANY

E-mail address: buergisser@upb.de