



# Randomized Complexity Lower Bounds

D Grigoriev

## ► To cite this version:

D Grigoriev. Randomized Complexity Lower Bounds. ACN Symposium Theory on Computing, 1998, Dallas, United States. hal-03049402

**HAL Id: hal-03049402**

**<https://hal.science/hal-03049402>**

Submitted on 9 Dec 2020

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

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

# Randomized Complexity Lower Bounds

D. Grigoriev<sup>1</sup>

Departments of Mathematics and Computer Science  
The Pennsylvania State University  
University Park, PA 16802  
dima@cse.psu.edu

The complexity lower bound  $\Omega(\log N)$  is proved for randomized computation trees (over reals with branching signs  $\{\leq, >\}$ ) for recognizing an arrangement or a polyhedron with  $N$  faces. A similar lower bound is proved for randomized computation trees over any zero-characteristic field with branching signs  $\{=, \neq\}$  for recognizing an arrangement. As consequences, this provides in particular, the randomized lower bound  $\Omega(n^2)$  for the KNAPSACK problem (which was proved in case of the randomized computation trees over reals in [11]) and also the randomized lower bound  $\Omega(n \log n)$  for the DISTINCTNESS problem (which is thereby the sharp bound). The technical core of the paper is a lower bound on the multiplicative complexity of a polynomial in terms of its singularities.

## Introduction.

The complexity lower bounds for deterministic algebraic computation trees were obtained in [26], [2], [4], [29], [30], [22] where the topological methods were developed. In particular, these methods provide the lower bound  $\Omega(\log N)$  for recognizing a union of planes (of different dimensions) with  $N$  faces, under a face we mean any nonempty intersection of several among these planes. As consequences we obtain the lower bound  $\Omega(n \log n)$  for the DISTINCTNESS problem  $\bigcup_{1 \leq i < j \leq n} \{X_i = X_j\} \subset \mathbb{R}^n$ , EQUALITY SET problem

$\{(x_1, \dots, x_n, y_1, \dots, y_n) : (x_1, \dots, x_n) \text{ is a permutation of } (y_1, \dots, y_n)\} \subset \mathbb{R}^{2n}$  and the lower bound  $\Omega(n^2)$  for the

KNAPSACK problem  $\bigcup_{I \subset \{1, \dots, n\}} \left\{ \sum_{i \in I} x_i = 1 \right\} \subset \mathbb{R}^n$ . In

[14], [15] a differential-geometric approach for recognizing polyhedra (to which the mentioned topological methods are not applicable) was proposed which gives the lower bound  $\Omega(\log N / \log \log N)$  where  $N$  is the number of faces of the polyhedron.

The first results on the randomized computation trees (RCT) appeared in [24], [19], [9], [10] but for decade an open

problem remained to obtain non-linear complexity lower bounds for recognizing natural problems by RCT. In [13] for the first time the nonlinear lower bound was obtained for somewhat weaker computational model of the randomized algebraic *decision* trees in which the testing polynomials in the branching nodes are of a fixed degree, rather than the *computation* trees in which the testing polynomials are computed along the path of the computation, so they could have in principle an exponential degree. The approach of [13] provides the lower bound  $\Omega(\log N)$  for recognizing an arrangement, i.e. a union of hyperplanes, and for recognizing a polyhedron, where  $N$  is again the number of faces. In particular, this leads to the lower bound  $\Omega(n \log n)$  for the DISTINCTNESS problem and  $\Omega(n^2)$  for the KNAPSACK problem. For the EQUALITY SET problem a complexity lower bound on a randomized algebraic decision tree seems to be an open question.

But the method of [13] does not provide a lower bound for more interesting model of RCT. Only in [11] a method was developed which gives in particular, a lower bound  $\Omega(n^2)$  for the KNAPSACK problem on RCT. This method relies on the obtained in [11] lower bound on the multiplicative border complexity of polynomials. The lower bound  $\Omega(\log N)$  of [11] holds for arrangements or polyhedra which satisfy some special conditions which fail, for example, for the DISTINCTNESS problem.

In this paper we consider RCT over an arbitrary zero-characteristic field  $F$  with branching signs  $\{=, \neq\}$  and also more customary RCT over reals with branching signs  $\{\leq, >\}$ . We remind (see e.g. [24], [19], [13]) that RCT  $T = \{T_\alpha\}_\alpha$  is a collection of computation trees  $T_\alpha$  which are chosen with the probabilities  $p_\alpha \geq 0, \sum_\alpha p_\alpha = 1$  such that  $T$  gives for any input a correct output with a probability greater than  $1 - \gamma$  for a certain  $\gamma < 1/2$  which is called the error probability of RCT.

Let  $H_1, \dots, H_m \subset F^n$  be a family of hyperplanes, denote by  $S = H_1 \cup \dots \cup H_m$  the arrangement. Under  $k$ -face of  $S$  we mean any nonempty intersection  $H_{i_1} \cap \dots \cap H_{i_{n-k}}$  of the dimension  $\dim(H_{i_1} \cap \dots \cap H_{i_{n-k}}) = k$ .

**Theorem 1.** *Assume that for a certain constant  $c_0 < 1$  any subarrangement  $S_1 = H_{i_1} \cup \dots \cup H_{i_q}$  of  $S$  where  $q > c_0 m$ , has at least  $N^{(0)}$  faces of all the dimensions. Then the depth of any RCT over  $F$  recognizing  $S$ , is greater than  $\Omega(\log_2 N^{(0)} - 2n - \log_2 n)$ .*

**Corollary 1.1.** *Any RCT over  $F$  solving the DISTINCTNESS problem, has the complexity greater than  $\Omega(n \log n)$ .*

The idea of the proof of the necessary in theorem 1 lower bound on  $N^{(0)}$  one can find in [13]. Observe that the lower

<sup>1</sup>Supported by NSF Grant CCR-9424358.

bound in the corollary is nearly sharp since it is possible to compute (deterministically) the discriminant  $\prod_{1 \leq i < j \leq n} (X_i - X_j)$  with the complexity  $O(n \log^2 n)$  ([20], [27]).

If to count only *nonscalar* multiplications/divisions (i.e. to consider the multiplicative complexity) then the lower bound from the corollary becomes sharp also due to [20], [27].

**Corollary 1.2.** *Any RCT over  $F$  solving the KNAPSACK problem, has the complexity greater than  $\Omega(n^2)$ .*

The proof of the necessary lower bound on  $N^{(0)}$  one can find in [11].

Corollary 1.2 can be generalized to the complexity lower bound  $\Omega(n^2 \log j)$  for RCT solving the RESTRICTED INTEGER PROGRAMMING ([19])  $\bigcup_{\alpha \in \{0, \dots, j-1\}^n} \subset F^n$  (obviously, it converts into the KNAPSACK problem when  $j = 2$ ).

In case of more customary RCT over reals  $\mathbf{R}$  with the branching signs  $\{\leq, >\}$  we consider recognizing either an arrangement  $S = \bigcup_{1 \leq i \leq m} H_i \subset \mathbf{R}^n$  or a polyhedron  $S^+ = \bigcap_{1 \leq i \leq m} H_i^+ \subset \mathbf{R}^n$ , where  $H_i^+$  is a half-space bounded by the hyperplane  $H_i$ ,  $1 \leq i \leq m$ . We say that  $\Gamma = H_{i_1} \cap \dots \cap H_{i_{n-k}}$  is  $k$ -face of  $S^+$  if  $\dim(\Gamma \cap S^+) = k$ .

**Theorem 2.** *Let for some positive constants  $c, c_1$  and  $k \leq (1 - c_1)n$  an arrangement  $\mathcal{S} = S = \bigcup_{1 \leq i \leq m} H_i$  or a polyhedron  $\mathcal{S} = S^+ = \bigcap_{1 \leq i \leq m} H_i^+$  have at least  $\Omega(m^{c(n-k)})$   $k$ -faces. Then for any RCT recognizing  $\mathcal{S}$ , its depth is greater than  $\Omega(n \log m)$ .*

**Corollary 2.1.** *Any RCT over reals solving the DISTINCTNESS problem, has the complexity greater than  $\Omega(n \log n)$ .*

Similar to the case of RCT over a zero-characteristic field (cf. corollary 1.1) the complexity bound is sharp since one can (deterministically) sort the input real numbers  $x_1, \dots, x_n$  with the complexity  $O(n \log n)$ .

**Corollary 2.2.** (see also [11]). *Any RCT over reals solving the KNAPSACK problem, has the complexity greater than  $\Omega(n^2)$ .*

For the similar to the DISTINCTNESS problem SET DISJOINTNESS  $\{(x_1, \dots, x_n, y_1, \dots, y_n) : x_i \neq y_j\} \subset \mathbf{R}^{2n}$  (being a complement to an arrangement) one obtains (almost literally as in the corollaries 1.1, 2.1) the lower bound  $\Omega(n \log n)$  and the upper bound  $O(n \log^2 n)$  (relying on the computing of the resultant [20], [27]) on the randomized complexity.

In the next two sections we give sketches of the proofs of theorems 1, 2.

The construction from [5] of RCT with the linear complexity  $O(n)$  for the EQUALITY SET problem (which is the union of  $n$ -dimensional planes in  $2n$ -dimensional space, see above) shows that the consideration just of *hyperplanes* in theorems 1, 2 is crucial, and the non-linear randomized complexity lower bounds cannot be directly extended to unions of planes of arbitrary dimensions.

In [3] deterministic computation trees with the branching signs  $\{=, \neq\}$  over algebraically closed fields of *positive characteristics* were considered, and the complexity lower bound  $\Omega(\log C)$  for recognizing an algebraic variety was established, where  $C$  is the degree of the Zeta-function of the variety. It is an open question to obtain non-linear complexity lower bounds for *randomized* computation trees over the fields of positive characteristics.

Let us also mention the paper [12] where a complexity lower bound was established for the randomized *analytic* de-

cision trees (rather than for more customary algebraic ones) and also the paper [6] where a lower bound was ascertained for a randomized *parallel* computational model (rather than a sequential model considered in the quoted papers including the present one).

## 1 RCT over zero characteristic fields.

In this section we give a sketch of the proof of theorem 1 (the complete proof one can find in [7]).

Assume for the time being that the field  $F = \bar{F}$  is algebraically closed. Denote by  $N_0$  the number of 0-faces (in other words, vertices) of the arrangement  $S = H_1 \cup \dots \cup H_m$ .

Similar to [27], [17] consider the graph of the gradient map of a polynomial  $0 \neq g \in F[X_1, \dots, X_n]$

$$G = \{(x = (x_1, \dots, x_n), \frac{\partial g}{\partial X_1}(x), \dots, \frac{\partial g}{\partial X_n}(x))\} \subset F^{2n}$$

The main technical tool in the proof of theorem 1 is the following lower bound on the degree  $\deg G$  (defined as the degree of the projective closure of  $G$  [23], [25]).

**Lemma 1.1.**  $\deg G \geq \frac{N_0}{2^{2n}}$

Denote by  $C(g)$  the multiplicative complexity of  $g$ . The results from [27], [1] imply the inequality  $\deg G \leq 2^{3C(g)}$  which together with lemma 1.1 entail the following lower bound on the multiplicative complexity of  $g$ .

**Proposition 1.** *If a polynomial  $0 \neq g \in F[X_1, \dots, X_n]$  vanishes on the arrangement  $S$  with  $N_0$  vertices then  $C(g) \geq \frac{1}{3}(\log_2 N_0 - 2n)$ .*

We remark that if  $N_l$  denotes the number of  $l$ -faces of  $S$  then one obtains the similar lower bound  $\frac{1}{3}(\log_2 N_l - 2(n-l))$  by means of intersecting  $S$  with a  $(n-l)$ -dimensional plane.

Now let  $F$  be an arbitrary zero characteristic field. To complete the proof of theorem 1 observe that if RCT  $T = \{T_\alpha\}_\alpha$  recognizes  $S$  with an error probability  $\gamma < 1/2$ , then for every  $\alpha$  CT  $T_\alpha$  possesses the unique "thick" path (from the root to a leaf), along which all the testing polynomials  $f_1, \dots, f_k \in F[X_1, \dots, X_n]$  have the branching sign  $\neq$ . One can prove that with a probability greater than  $1 - 2\gamma > 0$  the product  $f_1 \dots f_k$  vanishes on at least  $q > \frac{1-2\gamma}{1+2\gamma}m$  of hyperplanes among  $H_1, \dots, H_m$ . Taking into account that  $\gamma$  could be made as close to zero as desired at the expense of increasing the depth of RCT by a suitable constant factor [19], we apply proposition 1 and the remark just after it to the polynomial  $f_1 \dots f_k$  (notice that the multiplicative complexity of the latter product does not exceed  $2k - 1$ ), and get a lower bound on  $k$ . Since the complexity of RCT under consideration is greater or equal to  $k$ , one completes the proof of theorem 1.

## 2 RCT over reals

In this section we give a sketch of the proof of theorem 2 (the complete proof one can find in [8]).

Again let  $F$  be a zero characteristic field and  $\Gamma = H_{i_1} \cap \dots \cap H_{i_{n-k}}$  be  $k$ -face of the arrangement  $S = H_1 \cap \dots \cap H_m$ . Fix arbitrary coordinates  $Z_1, \dots, Z_k$  in  $\Gamma$ . Then treating  $H_{i_1}, \dots, H_{i_{n-k}}$  as the coordinate hyperplanes of the coordinates  $Y_1, \dots, Y_{n-k}$ , one gets the coordinates  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k}$  in  $F^n$ . The next construction of the leading terms of a polynomial is similar to [13], [11].

For any polynomial  $f(Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k}) \in F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k}]$  following [13], [11] define its leading term

$$\alpha Z_1^{m'_1} \dots Z_k^{m'_k} Y_1^{m_1} \dots Y_{n-k}^{m_{n-k}}$$

$0 \neq \alpha \in F$  (with respect to the coordinate system  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k}$ ) as follows. First take the minimal integer  $m_{n-k}$  such that  $Y_{n-k}^{m_{n-k}}$  occurs in the terms of  $f = f^{(0)}$ . Consider the polynomial

$$0 \neq f^{(1)} = \left( \frac{f}{Y_{n-k}^{m_{n-k}}} \right) (Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-1}, 0) \\ \in F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-1}]$$

which could be viewed as a polynomial on the hyperplane  $H_{i_{n-k}}$ . Observe that  $m_{n-k}$  depends only on  $H_{i_{n-k}}$  and not on  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-1}$ , since a linear transformation of the coordinates  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-1}$  changes the coefficients (being the polynomials from  $F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-1}]$ ) of the expansion of  $f$  in the variable  $Y_{n-k}$ , and a coefficient vanishes identically if and only if it vanishes identically after the transformation. Then  $f^{(1)}$  is the coefficient of the expansion of  $f$  at the power  $Y_{n-k}^{m_{n-k}}$ .

Second, take the minimal integer  $m_{n-k-1}$  such that  $Y_{n-k-1}^{m_{n-k-1}}$  occurs in the terms of  $f^{(1)}$ . In other words,  $Y_{n-k-1}^{m_{n-k-1}}$  is the minimal power of  $Y_{n-k-1}$  occurring in the terms of  $f$  in which occurs the power  $Y_{n-k}^{m_{n-k}}$ . Therefore,  $m_{n-k}, m_{n-k-1}$  depend only on the hyperplanes  $H_{n-k}, H_{n-k-1}$  and not on  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-2}$ , since (as above) a linear transformation of the coordinates  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-2}$  changes the coefficients (being the polynomials from  $F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-2}]$ ) of the expansion of  $f$  in the variables  $Y_{n-k}, Y_{n-k-1}$  and a coefficient vanishes identically if and only if it vanishes identically after the transformation. Denote by  $0 \neq f^{(2)} \in F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-2}]$  the coefficient of the expansion of  $f$  at the monomial  $Y_{n-k-1}^{m_{n-k-1}} Y_{n-k}^{m_{n-k}}$ . Obviously

$$f^{(2)} = \left( \frac{f^{(1)}}{Y_{n-k-1}^{m_{n-k-1}}} \right) (Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-2}, 0)$$

One could view  $f^{(2)}$  as a polynomial on the  $(n-2)$ -dimensional plane  $H_{i_{n-k}} \cap H_{i_{n-k-1}}$ .

Continuing in the similar way, we obtain consecutively the (non-negative) integers  $m_{n-k}, m_{n-k-1}, \dots, m_1$  and the polynomials

$$0 \neq f^{(l)} \in F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-l}]$$

$1 \leq l \leq n-k$ , by induction on  $l$ . Herewith,  $Y_{n-k-l+1}^{m_{n-k-l+1}}$  is the minimal power of  $Y_{n-k-l+1}$  occurring in the terms of  $f$ , in which occurs the monomial  $Y_{n-k-l+2}^{m_{n-k-l+2}} \dots Y_{n-k}^{m_{n-k}}$  for each  $1 \leq l \leq n-k$ . Notice that  $m_{n-k}, \dots, m_{n-k-l}$  depend only on the hyperplanes  $H_{i_{n-k}}, \dots, H_{i_{n-k-l}}$  and not on  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-l-1}$ . Then  $f^{(l)}$  is the coefficient of the expansion of  $f$  at the monomial  $Y_{n-k-l+1}^{m_{n-k-l+1}} \dots Y_{n-k}^{m_{n-k}}$  and

$$f^{(l+1)} = \left( \frac{f^{(l)}}{Y_{n-k-l}^{m_{n-k-l}}} \right) (Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-l-1}, 0)$$

Thus,  $f^{(l)}$  depends only on  $H_{i_{n-k}}, \dots, H_{i_{n-k-l}}$  and not on  $Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k-l-1}$ . One could view  $f^{(l)}$  as a polynomial on the  $(n-l)$  dimensional plane  $H_{i_{n-k}} \cap \dots \cap H_{i_{n-k-l+1}}$ . Continuing, we define also  $m'_k, \dots, m'_1$ .

Finally, the leading term  $lm(f) = \alpha Z_1^{m'_1} \dots Z_k^{m'_k} Y_1^{m_1} \dots Y_{n-k}^{m_{n-k}}$  is the minimal term of  $f$  in the lexicographical ordering with respect to the ordering  $Z_1 > \dots > Z_k > Y_1 >$

$\dots > Y_{n-k}$ . The leading term  $lm(f^{(l)}) = \alpha Z_1^{m'_1} \dots Z_k^{m'_k} Y_1^{m_1} \dots Y_{n-k-l}^{m_{n-k-l}}$ , we refer to this equality as the maintenance property (see also [13], [11]).

From now on the construction and the definitions differ from the ones in [13], [11].

For any polynomial  $g \in F[X_1, \dots, X_n]$  one can rewrite it in the coordinates  $\bar{g}(Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k})$  and expand  $\bar{g} = g_s + g_{s+1} + \dots + g_{s_1}$ , where  $g_j \in F[Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k}]$ ,  $s \leq j \leq s_1$  is homogeneous with respect to the variables  $Y_1, \dots, Y_{n-k}$  of degree  $j$  and  $g_s = g_s^{(0)} \neq 0$ . Consider the leading term  $lm(g_s) = \alpha Z_1^{m'_1} \dots Z_k^{m'_k} Y_1^{m_1} \dots Y_{n-k}^{m_{n-k}}$  and denote by  $\text{Var}^{(\Gamma)}(g) = \text{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(g)$  the number of positive (in other words, nonzero) integers among  $m_{n-k}, \dots, m_1$ , note that  $s = m_1 + \dots + m_{n-k}$ . As we have shown above  $\text{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(g)$  is independent from the coordinates  $Z_1, \dots, Z_k$  of  $\Gamma$ . Obviously,  $\text{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(g)$  coincides with the number of  $1 \leq l \leq n-k$  such that  $Y_{n-k-l} | g_s^{(l)}$ , the latter condition is equivalent to that the variety  $\{g_s^{(l)} = 0\} \cap H_{i_{n-k}} \cap \dots \cap H_{i_{n-k-l+1}}$  contains the plane  $H_{i_{n-k}} \cap \dots \cap H_{i_{n-k-l+1}} \cap H_{i_{n-k-l}}$  (being a hyperplane in  $H_{i_{n-k}} \cap \dots \cap H_{i_{n-k-l+1}}$ ).

It is convenient (see also [13], [11]) to reformulate the introduced concepts by means of infinitesimals in case of a real closed field  $F$  (see e.g. [18]). We say that an element  $\varepsilon$  transcendental over  $F$  is an infinitesimal (relative to  $F$ ) if  $0 < \varepsilon < a$  for any element  $0 < a \in F$ . This uniquely induces the order on the field  $F(\varepsilon)$  of rational functions and further on the real closure  $\widetilde{F(\varepsilon)}$  (see [18]).

One could make the order in  $F(\varepsilon)$  clearer by embedding it in the larger real closed field  $F((\varepsilon^{1/\infty}))$  of Puiseux series (cf. e.g. [16]). A nonzero Puiseux series has the form  $b = \sum_{i \geq i_0} \beta_i \varepsilon^{i/\delta}$ , where  $-\infty < i_0 < \infty$  is an integer,  $\beta_i \in F$  for every integer  $i$ ;  $\beta_{i_0} \neq 0$  and the denominator of the rational exponents  $\delta \geq 1$  is an integer. The order on  $F((\varepsilon^{1/\infty}))$  is defined as follows:  $\text{sgn}(b) = \text{sgn}(\beta_{i_0})$ . When  $i_0 \geq 1$ , then  $b$  is called an infinitesimal, when  $i_0 \leq -1$ , then  $b$  is called infinitely large. For any not infinitely large  $b$  we define its standard part  $st(b) = st_\varepsilon(b) \in F$  as follows: when  $i_0 = 0$ , then  $st(b) = \beta_{i_0}$ , when  $i_0 \geq 1$ , then  $st(b) = 0$ . In the natural way we extend the standard part to the vectors from  $(F((\varepsilon^{1/\infty})))^n$  and further to subsets in this space.

Now let  $\varepsilon_1 > \varepsilon_2 > \dots > \varepsilon_{n+1} > 0$  be infinitesimals, where  $\varepsilon_1$  is an infinitesimal relative to  $\mathbf{R}$ ; then  $\varepsilon_{i+1}$  is an infinitesimal relative to  $\mathbf{R}(\varepsilon_1, \dots, \varepsilon_i)$  for all  $0 \leq i \leq n$ . Denote the real closed field  $\mathbf{R}_i = \mathbf{R}(\varepsilon_1, \dots, \varepsilon_i)$ , in particular,  $\mathbf{R}_0 = \mathbf{R}$ . For an element  $b \in \mathbf{R}_{n+1}$  for brevity denote the standard part  $st_i(b) = st_{\varepsilon_{i+1}}(st_{\varepsilon_{i+2}} \dots (st_{\varepsilon_{n+1}}(b) \dots)) \in \mathbf{R}_i$  (provided that it is definable).

Also we will use the Tarski's transfer principle [28]. Namely, for two real closed fields  $F_1 \subset F_2$  a closed (so, without free variables) formula in the language of the first-order theory of  $F_1$  is true over  $F_1$  if and only if this formula is true over  $F_2$ .

An application of Tarski's transfer principle is the concept of the completion. Let  $F_1 \subset F_2$  be real closed fields and  $\Psi$  be a formula (with quantifiers and, perhaps, with  $n$  free variables) of the language of the first-order theory of the field  $F_1$ . Then  $\Psi$  determines a semialgebraic set  $V \subset F_1^n$ . The completion  $V^{(F_2)} \subset F_2^n$  is a semialgebraic set determined by the same formula  $\Psi$  (obviously,  $V \subset V^{(F_2)}$ ).

One could easily see that for any point  $(z_1, \dots, z_k) \in \mathbf{R}_k^k$  and a polynomial  $g \in \mathbf{R}[X_1, \dots, X_n]$  such that

$g_s^{(n-k)}(z_1, \dots, z_k) \neq 0$  (we utilize the introduced above notations) the following equality for the signs

$$\sigma_1^{m_1} \dots \sigma_{n-k}^{m_{n-k}} \operatorname{sgn}(g_s^{(n-k)}(z_1, \dots, z_k)) = \operatorname{sgn}(\bar{g}(z_1, \dots, z_k, \sigma_1 \varepsilon_{k+1} \varepsilon_{n+1}, \dots, \sigma_{n-k} \varepsilon_n \varepsilon_{n+1})) \quad (1)$$

holds for any  $\sigma_1, \dots, \sigma_{n-k} \in \{-1, 1\}$ . For any  $1 \leq i \leq n-k$  such that  $m_i = 0$  (1) holds also for  $\sigma_i = 0$ , agreeing that  $0^0 = 1$ . Moreover, the following polynomial identity holds:

$$g_s^{(n-k)}(Z_1, \dots, Z_k) = st_k \left( \frac{\bar{g}(Z_1, \dots, Z_k, \varepsilon_{k+1} \varepsilon_{n+1}, \dots, \varepsilon_n \varepsilon_{n+1})}{\varepsilon_{k+1}^{m_1} \dots \varepsilon_n^{m_{n-k}} \varepsilon_{n+1}^s} \right)$$

Now let  $F$  be an algebraically closed field of zero characteristic. Take a certain  $0 < \eta \leq 1$  (it will be specified later). We call  $k$ -face  $\Gamma = H_{i_1} \cap \dots \cap H_{i_{n-k}}$  of the arrangement  $S$  *strongly singular* (with respect to a polynomial  $g \in F[X_1, \dots, X_n]$ ) if  $\operatorname{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(g) \geq \eta(n-k)$ . Denote by  $N$  the number of strongly singular  $k$ -faces of  $S$  with respect to  $g$  (since  $g$  will be fixed for the time being, in the sequel we omit mentioning of  $g$  in this context).

The following lower bound on the degree of the graph  $G$  of the gradient map of  $g$  (see section 1) strengthens lemma 1.1, being the main technical tool in the proof of theorem 2.

**Lemma 2.1**  $\deg G \geq \Omega(N/(m^{(1-\eta)(n-k)} 2^{4n}))$

Similar to proposition 1 from section 1 this lemma implies the following proposition.

**Proposition 2.** *Let a polynomial  $g \in F[X_1, \dots, X_n]$  have  $N$  strongly singular  $k$ -faces in an arrangement  $H_1 \cup \dots \cup H_m \subset F^n$ . Then the multiplicative complexity  $C(g) \geq 1/3(\log N - (n-k)(1-\eta) \log m - 4n - \text{const})$ .*

For a family of polynomials  $f_1, \dots, f_t \in \mathbb{R}[X_1, \dots, X_n]$  we define  $\operatorname{Var}^{(\Gamma)}(f_1, \dots, f_t)$  to be the number of the variables among  $Y_1, \dots, Y_{n-k}$  which occur in at least one of the leading terms  $lm(f_{1,s_1}), \dots, lm(f_{t,s_t})$ , where  $H_{i_1}, \dots, H_{i_{n-k}}$  are the coordinate hyperplanes of the coordinates  $Y_1, \dots, Y_{n-k}$ , respectively;  $f_j(Z_1, \dots, Z_k, Y_1, \dots, Y_{n-k}) = f_j(X_1, \dots, X_n)$  and  $\bar{f}_j = f_{j,s_j} + f_{j,s_j+1} + \dots$ , herewith  $f_{j,l}$  is homogeneous with respect to the variables  $Y_1, \dots, Y_{n-k}$  of degree  $l$  and  $f_{j,s_j} \neq 0$ ,  $1 \leq j \leq t$ . Because the expansion into the homogeneous components  $\bar{f}_1 \dots \bar{f}_t = (f_{1,s_1} \dots f_{t,s_t}) + \dots$  starts with  $f_{1,s_1} \dots f_{t,s_t}$ , we have  $lm(f_{1,s_1} \dots f_{t,s_t}) = lm(f_{1,s_1}) \dots lm(f_{t,s_t})$  and hence  $\operatorname{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(f_1 \dots f_t) = \operatorname{Var}^{(\Gamma)}(f_1 \dots f_t) = \operatorname{Var}^{(\Gamma)}(f_1, \dots, f_t)$ .

For any CT  $T_1$  we denote by  $\operatorname{Var}^{(\Gamma)}(T_1) = \operatorname{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(T_1)$  the maximum of the  $\operatorname{Var}^{(\Gamma)}(f_1 \dots f_t)$  taken over all the paths of  $T_1$ , whose  $f_1, \dots, f_t$  are testing polynomials along the path.

The proof of the following "local" (i.e. concerning a single face) lemma relies on the relation (1) and is similar to lemma 1 [13], [11], but differs from it due to the different definition of the leading term  $lm$ .

**Lemma 2.2.** *Let  $T = \{T_\alpha\}$  be an RCT recognizing*

- a) *an arrangement  $S = \cup_{1 \leq i \leq m} H_i$  such that  $\Gamma = H_{i_1} \cap \dots \cap H_{i_{n-k}}$  is  $k$ -face of  $S$ , or*
- b) *a polyhedron  $S^+ = \cap_{1 \leq i \leq m} H_i^+$  such that  $\Gamma = \cap_{1 \leq j \leq n-k} H_{i_j}$  is  $k$ -face of  $S^+$*

*with error probability  $\gamma < \frac{1}{2}$ . Then  $\operatorname{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(T_\alpha) \geq (1 - 2\gamma)^2(n-k)$  for a fraction of  $\frac{1-2\gamma}{2-2\gamma}$  of all  $T_\alpha$ 's.*

The following "global" (i.e. concerning the set of all faces) lemma is similar to lemma 2 from [13], [11], but its proof is considerably simpler.

**Lemma 2.3.** *Let  $S = S$  or  $S = S^+$  satisfy the conditions of the theorem 2. Assume that CT  $T'$  for some constant  $\eta > 1 - c$ , satisfies the inequality  $\operatorname{Var}^{(\Gamma)}(T') \geq \eta(n-k)$  for at least  $M \geq \Omega(m^{c(n-k)})$  of  $k$ -faces  $\Gamma$  of  $S$ . Then the depth  $t$  of  $T'$  is greater than  $\Omega(n \log m)$ .*

**Proof of lemma 2.3:** To each  $k$ -face  $\Gamma$  of  $S$  satisfying the inequality  $\operatorname{Var}^{(\Gamma)}(T') \geq \eta(n-k)$ , we correspond a path in  $T'$  with the testing polynomials  $f_1, \dots, f_{t_0} \in \mathbb{R}[X_1, \dots, X_n]$ ,  $t_0 \leq t$  such that  $\operatorname{Var}^{(\Gamma)}(f_1 \dots f_{t_0}) \geq \operatorname{Var}^{(\Gamma)}(T')$  (in other words,  $\Gamma$  is strongly singular  $k$ -face for  $f_1 \dots f_{t_0}$ , see section 1). Denote  $f = f_1 \dots f_{t_0}$ .

Assume that  $3^t \leq O(m^{(n-1+c)(n-k)/2})$ , otherwise we are done. Then there exists a path of  $T'$  (let us keep the notation  $f_1, \dots, f_{t_0}$  for the testing polynomials along this path) which corresponds to at least  $N = \Omega(m^{(c-\eta+1)(n-k)/2})$  of strongly singular  $k$ -faces  $\Gamma$  for  $f$  (because there are most  $3^t$  paths in  $T'$ ). Proposition 2 implies that the multiplicative complexity  $C(f) \geq \frac{1}{3}((\eta-1+c)(n-k) \log m - 4n - \text{const})$ . Obviously  $C(f) \leq t + t_0 - 1 \leq 2t - 1$  (cf. the proof of theorem 1 in section 1). Hence  $t \geq \Omega(n \log m)$  that proves lemma 2.3.

Finally we show how to deduce the theorem 2 from lemmas 2.2 and 2.3. Consider RCT  $\{T_\alpha\}$  recognizing  $S$  with error probability  $\gamma < \frac{1}{2}$ . Lemma 2.2 and counting imply the existence of  $T_{\alpha_0}$  such that the inequality  $\operatorname{Var}^{(\Gamma)}(T_{\alpha_0}) \geq (1 - 2\gamma)^2(n-k)$  is true for  $M = \frac{1-2\gamma}{2(1-\gamma)} \Omega(m^{c(n-k)})$  of  $k$ -faces  $\Gamma$  of  $S$ . Apply lemma 2.3 to CT  $T' = T_{\alpha_0}$  with  $\eta = (1 - 2\gamma)^2$ . Since the error probability  $\gamma$  could be made a positive constant as close to zero as desired at the expense of increasing by a constant factor the depth of RCT [19], take  $\gamma$  such that  $\eta > 1 - c$ . Then lemma 2.3 entails that  $t \geq \Omega(n \log m)$ , which proves theorem 2.

### 3 Deterministic computation trees

Treating a deterministic computation tree (CT) as a particular case of RCT one can release the restriction on subarrangements in theorem 1 and obtain the following result.

**Corollary 1.3** *If a CT (over a zero characteristic field) recognizes an arrangement with  $N$  faces (of all the dimensions) then its depth exceeds  $\Omega(\log N)$ .*

For CT over reals in a similar way one can release the restriction on the number of faces in theorem 2.

**Corollary 2.3** *If a CT (over reals) recognizes either an arrangement or a polyhedron  $S$  with  $N$  faces (of all the dimensions) then its depth exceeds  $\Omega(\log N)$ .*

In case of an arrangement one could deduce corollary 2.3 from [2], in case of a polyhedron the corollary strengthens the result from [15].

**Acknowledgement.** I would like to thank Marek Karpinski for useful discussions.

### References

- [1] W. Baur, V. Strassen, The complexity of partial derivatives, Theor. Comput. Sci., Vol. 22, 1983, pp. 317–330
- [2] M. Ben-Or, Lower bounds for algebraic computation trees, Proc. ACM Symp. Th. Comput., 1983, pp. 80–86
- [3] M. Ben-Or, Algebraic computation trees in characteristic  $p > 0$ , Proc. IEEE Symp. Found. Comput. Sci., 1994, pp. 534–539.

- [4] A. Björner, L. Lovász, A. Yao, Linear decision trees: volume estimates and topological bounds, *Proc. ACM Symp. Th. Comput.* 1992, pp. 170–177.
- [5] P. Bürgisser, M. Karpinski, T. Lickteig, On randomized algebraic test complexity, *J. Complexity*, Vol. 9, 1993, pp. 231–251.
- [6] D. Grigoriev, Nearly sharp complexity bounds for multiprocessor algebraic computations, *J. Complexity*, vol. 13, 1997, pp. 50–64.
- [7] D. Grigoriev, Complexity lower bounds for randomized computation trees over algebraically closed fields, submitted to *Computational Complexity*
- [8] D. Grigoriev, Randomized Complexity Lower Bounds for Arrangements and Polyhedra, to appear in *Discrete and Computational Geometry*
- [9] D. Grigoriev, M. Karpinski, Lower Bounds on Complexity of Testing Membership to a Polygon for Algebraic and Randomized Computation Trees, Technical Report TR-93-042, International Computer Science Institute, Berkeley, 1993
- [10] D. Grigoriev, M. Karpinski, Lower Bound for Randomized Linear Decision Tree Recognizing a Union of Hyperplanes in a Generic Position, Research Report No. 85114-CS, University of Bonn, 1994
- [11] D. Grigoriev, M. Karpinski, Randomized quadratic lower bound for knapsack, *Proc. ACM Symp. Th. Comput.*, 1997, pp. 76–85
- [12] Grigoriev, M. Karpinski, R. Smolensky, Randomization and the computational power of analytic and algebraic decision trees, to appear in *Computational Complexity*, 1997
- [13] D. Grigoriev, M. Karpinski, F. Meyer auf der Heide, R. Smolensky, A lower bound for randomized algebraic decision trees, *Proc. ACM Symp. Th. Comput.*, 1996, pp. 612–619
- [14] D. Grigoriev, M. Karpinski, N. Vorobjov, Improved Lower Bound on Testing Membership to a Polyhedron by Algebraic Decision Trees, *Proc. 36th IEEE FOCS*, 1995, pp. 258–265
- [15] D. Grigoriev, M. Karpinski, N. Vorobjov, Lower bound on testing membership to a polyhedron by algebraic decision and computation trees, *J. Discrete and Computational Geometry*, Vol. 17, 2, 1997, pp. 191–215.
- [16] D. Grigoriev, N. Vorobjov, Solving Systems of Polynomial Inequalities in Subexponential Time, *Journal of Symbolic Comp.*, 5, 1988, pp. 37–64
- [17] T. Lickteig, On semialgebraic decision complexity, Preprint TR-0-052 ICSI, Berkeley, 1990.
- [18] S. Lang, *Algebra*, Addison-Wesley, New York, 1965
- [19] F. Meyer auf der Heide, Simulating probabilistic by deterministic algebraic computation trees, *Theor. Comput. Sci.*, Vol. 41, 1985, pp. 325–330.
- [20] R. Moenck, A. Borodin, Fast modular transforms via division *Proc. IEEE Symp. Switching and Automata Theory* 1972 pp. 90–96
- [21] J. Montana, L. Pardo, Lower bounds for arithmetic networks, *Appl. Algebra in Eng. Commun. Comput.*, Vol. 4, 1993, pp. 1–24.
- [22] J. Montana, J. Morais, L. Pardo, Lower bounds for arithmetic network II: sum of Betti numbers, *Appl. Algebra in Eng. Commun. Comput.*, Vol. 7, 1996, pp. 41–51.
- [23] D. Mumford, *Algebraic geometry*, Springer, 1976.
- [24] U. Manber, M. Tompa, Probabilistic, Nondeterministic and Alternating Decision Trees, *Proc. 14th ACM STOC*, 1982, pp. 234–244
- [25] I. R. Shafarevich, *Basic algebraic geometry*, V. 1 – Springer, 1994.
- [26] M. Steele, A. Yao, Lower bounds for algebraic decision trees, *J. Algorithms*, Vol. 3, 1982, pp. 1–8.
- [27] V. Strassen, Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten, *Numer. Math.*, Vol. 20, 1973, pp. 238–251.
- [28] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, University of California Press, 1951.
- [29] A. Yao, Algebraic decision trees and Euler characteristic, *Proc. IEEE Symp. Found. Comput. Sci.*, 1992, pp. 268–277.
- [30] A. Yao, Decision tree complexity and Betti numbers, *Proc. ACM Symp. Th. Comput.*, 1994, pp. 615–624.