Quadratic Randomized Lower Bound for the Knapsack Problem*

Dima Grigoriev † Marek Karpinski ‡

*A preliminary version of this paper appears in [GK97]

†Dept. of Computer Science and Mathematics, Penn State University, University Park.
Research partially supported by NSF Grant CCR-9424358. Email: dima@cse.psu.edu

‡Dept. of Computer Science, University of Bonn, 53117 Bonn, and the International Computer Science Institute, Berkeley. Research partially done while visiting Dept. of Computer Science, Princeton University. Research supported by DFG Grant KA 673/4-1, and by the ESPRIT BR Grants 7097 and EC-US 030. Email: marek@cs.uni-bonn.de

Marek Karpinski Email: marek@cs.uni-bonn.de

Abstract

We prove $\Omega(n^2)$ complexity lower bound for the general model of *randomized computation trees* solving the *Knapsack Problem*, and more generally *Restricted Integer Programming*. This is also the first *nontrivial* lower bound for *randomized computation trees*. The method of the proof depends crucially on the new technique for proving lower bounds on the *border complexity* of a polynomial which could be of independent interest.

0 Introduction

We prove for the first time nonlinear complexity lower bounds for randomized computation trees (*RCT*s) (see e.g. [MT82], [S83]) recognizing languages like *unions of hyperplanes* (i.e. *linear arrangements*) or *intersections of half-spaces* (polyhedra). As an application we prove a quadratic lower bound on *RCT*s solving the knapsack problem, or more general, the restricted integer programming.

Obtaining general lower bounds for randomized computations was an open question for a long time (see e.g. [M85a, b, c] and [KV88]). Only recently, a nonlinear lower bound was proven in [GKMS96] for a weaker model of randomized d-decision trees (d-*RDT*s), in which the testing polynomials have degrees at most d (for 2-dimensional case the lower bound was proven in [GK93] and for the generic arrangements a lower bound was proved in [GK94]). In particular, for d-*RDT*s in [GKMS96] the lower bound $\Omega(n \log n)$ was proven for the *Element Distinctness Problem* (i.e. whether all the numbers $x_1, \ldots, x_n$ are pairwise distinct), and the lower bound $\Omega(n^2)$ was proved for the *Knapsack problem.* Usually, the bound d on the degree in d-*RDT* is small enough, and the main difficulty while considering *RCT* is that the degree of testing polynomials in principle could be exponential in the depth. Therefore, we develop in the present paper a new method for obtaining complexity lower bounds for *RCT*s.

The method developed in the present paper is not applicable to the element distinctness problem. In [BKL93], [GKMS96] a linear depth *RCT* was constructed for a similar problem (*permutation problem*) beating its deterministic $\Omega(n\ \log n)^2$ lower bound [B83]). This example shows that the still open problem of complexity of an *RCT* for the element distinctness problem is quite delicate.

We also mention that a linear $\frac{n}{4}$ lower bound for an *RCT* recognizing the arrangement $\bigcup_{1 \le i \le n} \{X_i = 0\}$ or the "orthant" $\bigcap_{1 \le i \le n} \{X_i \ge 0\}$ was proved in [GKMS96]. For a stronger model of randomized analytic decision trees ($RADT$) a complexity upper bound $O(\log^2 n)$ for testing $\bigcap_{1\leq i\leq n}\{X_i \geq 0\}$ was proven in [GKS96] (for deterministic analytic decision trees the exact complexity bound n was proved in [R72], [MPR94]). Besides, in [GKS96] for $RADT$ a sublinear lower bound $\Omega(n^{1/2})$ was proved for the union of orthants $\bigcup\{\sigma_i X_i \geq 0,\ 1 \leq i \leq n\}$ where $\sigma_i \in \{-1, 1\}$ and the number of negative among σ_i is divided by a fixed q such that $q \neq 2^s$ for any s.

For deterministic models of the computation and decision trees several methods for obtaining complextity lower bounds were developed earlier. The "topological" methods based on the number of connected components ([SY82], [B83]), or more general, on the sum of Betti numbers ([BLY92], [Y94]), provide the lower bound $\Omega(n^2)$ for the knapsack problem and the lower bound $\Omega(n \log n)$ for the distinctness or the permutation problem. The already mentioned example from [BKL93] shows that these "topological" bounds cannot be directly extended to RCT.

For testing a polyhedron (to which the topological methods are not applicable), the differential-geometric method (involving the curvature) for obtaining complextity lower bounds for deterministic computations was developped in [GKV96], which provides $\Omega(\log N)$ lower bound for decision trees (see also [GKV95]) and $\Omega(\log N/\log\log N)$ for computation trees, where N is the number of all faces of the polyhedron.

We now briefly describe the content of the paper. In section 1 we introduce the notion of the *border complexity*, for the similar notations cf. [S90] [B79] [BCLR79], of a polynomial and prove a lower bound on it which is of independent interest, in terms of the number of connected components.

In section 2 we prove the main theorem which provides a complexity lower bound for RCT testing an arrangement or a polyhedron. For that purpose we use some tools (in particular, the tree of flags) from [GKMS96], but the proof differs from the one in [GKMS96] since the degree of RCTs could be exponential as we already mentioned.

In section 3 as an application of the main theorem we give a complexity quadratic lower bound $\Omega(n^2 \log j)$ for *RCT* testing the *Restricted Integer Programming*

$$L_{n,j} = \bigcup_{a \in \{0,\ldots,j-1\}^n} \{aX = 1\}$$

(which is an arrangement consisting of j^n hyperplanes). Notice that for $j = 2$ this problem coincides with the *Knapsack Problem*. In particular, in section 3 we give a lower bound $j^{\Omega(n^2)}$ on the number of faces of $L_{n,j}$ (and thereby, on the number of the connected components of the complement of $L_{n,j}$, which was also ascertained in [YI65], [M85b], [GKMS96], and [DL78]). Moreover, in section 3 we provide a stronger lower bound on the number of faces of subarrangements of $L_{n,j}$ (under a subarrangement we understand the restriction of a subset of hyperplanes from $L_{n,j}$ on a face of $L_{n,j}$). The analogue of this bound for subarrangements of the distinctness problem is wrong, that is why we cannot get a nonlinear complexity lower bound for *RCT*, solving the distinctness problem.

In the last section 4 we state the complexity lower bound for the deterministic computation trees recognizing a polyhedron under less restrictive conditions than for the randomized computation trees as in the theorem from section 2.

1 Lower bound on the border complexity

We start now with the technical development leading to the crucial lower bound on the *border complexity* of a polynomial.

Let $H_1, \ldots, H_{n-k} \subset \mathbb{R}^n$ be hyperplanes such that their intersection $\Gamma = H_1 \cap \cdots \cap H_{n-k}$ has the dimension $\dim \Gamma = k$. Fix arbitrary coordinates $Z_1, \ldots, Z_k$ in Γ. Then treating $H_1, \ldots, H_{n-k}$ as the coordinate hyperplanes of the coordinates $Y_1, \ldots, Y_{n-k}$, one gets the coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$ in $\mathbb{R}^n$.

For any polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ rewrite it in the coordinates $\overline{f}(Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k})$ and following [GKMS96], define its leading term

$$lm(f) = \alpha Z_1^{m_1'} \cdots Z_k^{m_k'} Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$$

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

$$0 \not\equiv f^{(1)} = \left(\frac{\overline{f}}{Y_{n-k}^{m_{n-k}}}\right)(Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-1}, 0) \in \mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-1}]$$

which could be viwed as a polynomial on the hyperplane H_{n-k}. Observe that m_{n-k} depends only on H_{n-k} and not on $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-1}$, since a linear transformation of the coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-1}$ changes the coefficients (being the polynomials from $\mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-1}]$) of the expansion of $\overline{f}$ 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 $\overline{f}$ 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 $\overline{f}$ 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 $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-2}$, since (as above) a linear transformation of the coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-2}$ changes the coefficients (being the polynomials from $\mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-2}]$) of the expansion of $\overline{f}$ 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 $0 \not\equiv f^{(2)} \in \mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-2}]$ the coefficient of the expansion of $\overline{f}$ at the monomial $Y_{n-k-1}^{m_{n-k-1}} Y_{n-k}^{m_{n-k}}$. Obviously

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

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

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

$$0 \not\equiv f^{(l)} \ \in \ \mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-l}]$$

$1 \leq l \leq n-k$, 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 $\overline{f}$, in which occurs the monomial $Y_{n-k-l+2}^{m_{n-k-l+2}} \cdots Y_{n-k}^{m_{n-k}}$ for each $1 \leq l \leq n-k$. Notice that $m_{n-k}, \ldots, m_{n-k-l}$ depend only on the hyperplanes $H_{n-k}, \ldots, H_{n-k-l}$ and not on $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-l-1}$. Then $f^{(l)}$ is the coefficient of the expansion of $\overline{f}$ at the monomial $Y_{n-k-l+1}^{m_{n-k-l+1}} \cdots Y_{n-k}^{m_{n-k}}$ and

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

Thus, $f^{(l)}$ depends only on $H_{n-k}, \ldots, H_{n-k-l}$ and not on $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-l-1}$. One could view $f^{(l)}$ as a polynomial on the $(n-l)$-dimensional plane $H_{n-k} \cap \cdots \cap H_{n-k-l+1}$. Continuing, we define also $m_k^{'}, \ldots, m_1^{'}$.

Finally, the leading term $lm(f) = \alpha Z_1^{m_1^{'}} \cdots Z_k^{m_k^{'}} Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$ is the minimal term of $\overline{f}$ in the lexicographical ordering with respect to the ordering $Z_1 > \cdots > Z_k > Y_1 > \cdots > Y_{n-k}$. The leading term $lm(f^{(l)}) = \alpha Z_1^{m_1'} \cdots Z_k^{m_k'} Y_1^{m_1} \cdots Y_{n-k-l}^{m_{n-k-l}}$, we refer to this equality as the maintenance property (see also [GKMS96]).

Denote by $Var(f) = Var^{(H_1, \ldots, H_{n-k})}(f)$ the number of positive (i.e. nonzero) integers among $m_{n-k}, \ldots, m_1$. As we have shown above, $Var(f)$ is independent from the coordinates $Z_1, \ldots, Z_k$ of Γ. Obviously, $Var(f)$ coincides with the number of $1 \leq l \leq n-k$ such that $Y_{n-k-l} \mid f^{(l)}$, the latter condition is equivalent to that the variety $\{f^{(l)} = 0\} \bigcap (H_{n-k} \cap \cdots \cap H_{n-k-l+1})$ contains the plane $H_{n-k} \cap \cdots \cap H_{n-k-l+1} \cap H_{n-k-l}$ (being a hyperplane in $H_{n-k} \cap \cdots \cap H_{n-k-l+1}$).

It is convenient (see also [GKMS96]) to reformulate the introduced concepts by means of infinitesimals. Namely for a real closed field F (see e.g. [L65]) we say that an element ε 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 [L65]).

One could make the order in $\widetilde{F(\varepsilon)}$ clearer by embedding it in the larger real closed field $F((\varepsilon^{1/\infty}))$ of Puiseux series (cf. e.g. [GV88]). 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: $sgn(b) = sgn(\beta_{i_0})$. 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 $\varepsilon_1 > \varepsilon_2 > \ldots > \varepsilon_{n+2} > 0$ be infinitesimals, where ε_1 is an infinitesimal relative to $\mathbb{R}$; in general ε_{i+1} is an infinitesimal relative to $\widetilde{\mathbb{R}(\varepsilon_1, \ldots, \varepsilon_i)}$ for all $0 \leq i \leq n+1$. Denote the real closed field $\mathbb{R}_i = \widetilde{\mathbb{R}(\varepsilon_1, \ldots, \varepsilon_i)}$, in particular, $\mathbb{R}_0 = \mathbb{R}$. For an element $b \in \mathbb{R}_{n+2}$ for brevity denote the standard part $st_i(b) = st_{\varepsilon_{i+1}}(st_{\varepsilon_{i+2}} \cdots (st_{\varepsilon_{n+2}}(b) \cdots) \in \mathbb{R}_i$ (provided that it is definable).

Also we will use the Tarski's transfer principle [T51]. 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.

Tarski's transfer principle implies that a semialgebraic set $\{f_1 \geq 0, \ldots, f_{k_1} \geq 0, f_{k_1+1} > 0, \ldots, f_k > 0\} \subset F^n$, where the polynomials $f_i \in F[X_1, \ldots, X_n]$ have the degrees $deg(f_i) \leq d$, has at most

$(min\{2^k, (\frac{k}{n})^n\} d^n)^{O(1)}$ connected components (cf. [GV88]), relying on this bound in case $F = \mathbb{R}$ from [W68] (cf. also [BPR94]), which strenghtens the result of [M64].

Another application of Tarski's transfer principle is the concept of the completion. Let $F_1 \subset F_2$ be real closed fields and Ψ 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 Ψ 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 Ψ (obviously, $V \subset V^{(F_2)}$). Tarski's transfer principle entails, in particular, that the number of connected components of V is the same as the one of $V^{(F_2)}$ (cf. [GV88]).

One could easily see that for any point $(z_1, \dots, z_k) \in \mathbb{R}^k_{k+2}$ such that $f^{(n-k)}(z_1, \dots, z_k) \neq 0$ (we utilize the introduced above notations) the following equality for the signs

$$\sigma_1^{m_1} \dots \sigma_{n-k}^{m_{n-k}} sgn\left(f^{(n-k)}(z_1, \dots, z_k)\right) = sgn\left(\overline{f}(z_1, \dots, z_k, \sigma_1 \varepsilon_{k+3}, \dots, \sigma_{n-k}\varepsilon_{n+2})\right) \quad (1)$$

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:

$$f^{(n-k)}(Z_1, \dots, Z_k) = st_{k+2}\left(\frac{\overline{f}(Z_1, \dots, Z_k, \varepsilon_{k+3}, \dots, \varepsilon_{n+2})}{\varepsilon_{k+3}^{m_1} \cdots \varepsilon_{n+2}^{m_{n-k}}}\right) \quad (2)$$

For a family of hyperplanes $H_1, \dots, H_m \subset \mathbb{R}^n$ let $S = \cup_{1 \leq i \leq m} H_i$ be an arrangement, by $B_0(H_1, \dots, H_m)$ we denote the number of connected components of the complement $\mathbb{R}^n - S$.

Following e.g. [S90] we define the complexity $s = C(f)$ of a polynomial $f \in \mathbb{R}[X_1, \dots, X_n]$ as the length of the shortest straight-line program which computes f. Recall that the latter is a sequence of operations $u_1 = X_1, \dots, u_n = X_n$, then for every $n < j \leq s+n$ $u_j = \tilde{u}_{j_1} \odot \tilde{u}_{j_2}$, where for each $i = 1, 2$ either $\tilde{u}_{j_i} = u_{j_i}$ with $j_i < j$ or $\tilde{u}_{j_i} \in \mathbb{R}$ and either $\odot = \times$

or $\odot = +$. To every u_j by recursion on j one attaches in the natural way a polynomial $U_j \in \mathbb{R}[X_1, \ldots, X_n]$ (the value of u_j). The straight-line program computes f if $U_{s+n} = f$.

Observe that one could consider also the division $\odot = /$ and the resulting rational functions, but since we deal only with the signs of the testing functions in the computation trees (see below), we could consider separately the computations of the numerators and denominators of the rational functions by means of the straight-line programs without the divisions.

For a polynomial $g \in \mathbb{R}[Z_1, \ldots, Z_k]$ its *border complexity* $\overline{C}(g)$ (cf. [S90]) is the minimal $C(f)$ where $f \in \mathbb{R}[X_1, \ldots, X_n]$ for a certain $n \geq k$ such that $g = f^{(n-k)}$, for suitable coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$, which we treat as the linear forms in $X_1, \ldots, X_n$. Actually, one could literally extend the concept of the border complexity to the polynomials with the coefficients from an arbitrary field.

The main result of this section is the following lower bound on the border complexity.

Proposition: Let for a polynomial $g \in \mathbb{R}[Z_1, \ldots, Z_k]$ its border complexity $\overline{C}(g) \leq s$. Assume that $H_1, \ldots, H_m \subset \mathbb{R}^k$ are pairwise distinct hyperplanes such that the corresponding linear functions $L_{H_i} \mid g$, $1 \leq i \leq m$ (where the zero set of L_{H_i} is H_i). Then $B_0(H_1, \ldots, H_m) \leq 2^{O(s+k)}$.

Remark: In fact, one could formulate the proposition in a stronger setting as follows (the proof goes through literally). For a polynomial g with the border complexity less than s, the number of the connected components in the complement in $\mathbb{R}^k$ of the set $\{g = 0\}$ of zeroes of g does not exceed $2^{O(s+k)}$.

Proof: Let $u_i = X_i$, $1 \leq i \leq n$; $u_j = \tilde{u}_{j_1} \odot \tilde{u}_{j_2}$, $n + 1 \leq j \leq n + s$ be a straight-line program which computes a certain polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ such that $g = f^{(n-k)}$ for suitable coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$ (we utilize the introduced above notations). Express $X_i = \alpha_1^{(i)} Z_1 + \cdots + \alpha_k^{(i)} Z_k + \beta_1^{(i)} Y_1 + \cdots \beta_{n-k}^{(i)} Y_{n-k}$, $1 \le i \le n$, where $\alpha_j^{(i)}, \beta_j^{(i)} \in \mathbb{R}$. Remind that by $\overline{f}(Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k})$ we denote the polynomial f in the coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$.

Due to (2) for any point $(z_1, \ldots, z_k) \in \mathbb{R}_2^k$ we have

$$g(z_1, \ldots, z_k) = st_2 \left(\frac{\overline{f}(z_1, \ldots, z_k, \varepsilon_{k+3}, \ldots, \varepsilon_{n+2})}{\varepsilon_{k+3}^{m_1} \cdots \varepsilon_{n+2}^{m_{n-k}}} \right) \tag{3}$$

Denote $u_i' = \alpha_1^{(i)} z_1 + \cdots + \alpha_k^{(i)} z_k + \beta_1^{(i)} \varepsilon_{k+3} + \cdots + \beta_{n-k}^{(i)} \varepsilon_{n+2}$, $1 \le i \le n$. Introduce a new variable Z_0 and two semialgebraic sets

$$\begin{aligned} \mathcal{V} = \Big\{ & (z_0, z_1, \ldots, z_k, u_{n+1}, \ldots, u_{n+s}) \in \mathbb{R}_{n+2}^{k+s+1} : \\ & u_j = \tilde{u}_{j_1}' \odot \tilde{u}_{j_2}', n+1 \le j \le n+s, \\ & \quad \text{where for each } i = 1,2 \text{ either } \tilde{u}_{j_i}' = u_{j_i}' \text{ when } 1 \le j_i \le n \text{ and } \tilde{u}_{j_i}' = u_{j_i} \text{ when } n < j_i < j, \text{ or } \tilde{u}_{j_i}' \in \mathbb{R} \text{ according to the straight-line program which computes } f; \\ & \Big(\big(\frac{u_{n+s}}{\varepsilon_{k+3}^{m_1} \cdots \varepsilon_{n+2}^{m_{n-k}}} \big)^2 - \varepsilon_1 \Big)^2 + \\ & \qquad \Big(z_0^2 + z_1^2 + \cdots + z_k^2 - \frac{1}{\varepsilon_1} \Big)^2 < \varepsilon_2 \Big\}; \end{aligned}$$

$$V = \left\{ (z_0, z_1, \ldots, z_k) \in \mathbb{R}_1^{k+1} : g^2(z_1, \ldots, z_k) = \varepsilon_1; z_0^2 + z_1^2 + \cdots + z_k^2 = \frac{1}{\varepsilon_1} \right\}$$

Denote by $\prod : \mathbb{R}_{n+2}^{k+s+1} \to \mathbb{R}_{n+2}^{k+1}$ the linear projection along the coordinates $u_{n+1}, \ldots, u_{n+s}$. The linear projection $\prod : \mathcal{V} \rightleftarrows \prod(\mathcal{V})$ is an isomorphism of the semialgebraic sets, since the projection

$$\prod(\mathcal{V}) = \left\{ (z_0, z_1, \ldots, z_k) \in \mathbb{R}_{n+2}^{k+1} : \left(\left(\frac{\overline{f}(z_1, \ldots, z_k, \varepsilon_{k+3}, \ldots, \varepsilon_{n+2})}{\varepsilon_{k+3}^{m_1} \cdots \varepsilon_{n+2}^{m_{n-k}}} \right)^2 - \varepsilon_1 \right)^2 + \right.$$
$$\left. (z_0^2 + z_1^2 + \cdots + z_k^2 - \frac{1}{\varepsilon_1})^2 < \varepsilon_2 \right\}$$

and the inverse mapping is given by the polynomial mapping $u_j = \tilde{u}'_{j_1} \odot \tilde{u}'_{j_2}$, $n+1 \leq j \leq n+s$.

Then $V \subset \prod(\mathcal{V})$ because of (3).

Furthermore, $st_1(\prod(\mathcal{V})) = V$; the left side is definable since for any point $(z_0, \dots, z_k) \in \prod(\mathcal{V})$ the square of its euclidean norm $\|z_o, \dots, z_k\|^2 = z_0^2 + \cdots + z_k^2 < \frac{1}{\varepsilon_1} + \varepsilon_2^{\frac{1}{2}} < \frac{1}{\varepsilon_1} + 1$. By the same reason lemma 1 from [GV88] states that the number N_3 of the connected components of V does not exceed the number N_4 of the connected components of $\prod(\mathcal{V})$, the latter coincides with the number of the connected components of $\mathcal{V}$ since it is isomorphic to $\prod(\mathcal{V})$.

We claim that for any connected component $W \subset \mathbb{R}^k$ (which is an open set in the euclidean topology) of the component $\mathbb{R}^k - \{g = 0\}$ and an arbitrary point $w_0 \in \partial W$ on the boundary, there exists a point $(z_1, \dots, z_k) \in W^{(\mathbb{R}_1)} \subset \mathbb{R}_1^k$ from the completion $W^{(\mathbb{R}_1)}$ (as we have seen above from Tarski's transfer principle, the connected components W of the complement are in the bijective correspondence with their completions $W^{(\mathbb{R}_1)} \supset W$, being the connected components of the complement $\{g = 0\}^{(\mathbb{R}_1)}$ in $\mathbb{R}_1^k$, the number of these connected components we denote by N_0) such that $g^2(z_1, \dots, z_k) = \varepsilon_1$ and $st_0(z_1, \dots, z_k) = w_0$ (cf. lemma 3 from [GV88]). Indeed, pick out an arbitrary point $w \in W$. Taking into account that $w_0 \in \partial(W^{(\mathbb{R}_1)})$, so $g(w_0) = 0$, and $0 < g^2(w) \in \mathbb{R}$ we conclude that g^2 attains on $W^{(\mathbb{R}_1)}$ any intermediate value from $\mathbb{R}_1$ between 0 and $g^2(w)$ (using Tarski's transfer principle), in particular, ε_1. Now take a point $w_1 \in W^{(\mathbb{R}_1)}$ being the nearest to w_0 such that $g^2(w_1) = \varepsilon_1$ (its existence follows again from Tarski's transfer principle). It suffices to prove that $st_0(w_1) = w_0$. Suppose the contrary. Then there exists $0 < r \in \mathbb{R}$ such that for any point $w_2 \in W^{(\mathbb{R}_1)}$ with the distance $\|w_0 - w_2\| \leq r$ the inequality $g^2(w_2) < \varepsilon_1$ holds. Since $w_0 \in \partial W$ there exists a point $w_3 \in W$ such that $\|w_0 - w_3\| \leq r$, then $0 < g^2(w_3) \in \mathbb{R}$ and we get a contradiction with the supposition, and that proves the claim.

Furthermore, since $w_0 \in \mathbb{R}^k$ and $st_0(z_1, \dots, z_k) = w_0$, there exists $0 < r_1 \in \mathbb{R}$ such that the norm $\|z_1, \dots, z_k\| \leq r_1$, a fortiori $\|z_1, \dots, z_k\|^2 \leq \frac{1}{\varepsilon_1}$.

Consider a semialgebraic set

$$V_0 = \left\{(z_1, \dots, z_k) \in \mathbb{R}_1^k : g^2\left(z_1, \dots, z_k\right) = \varepsilon_1\right\}$$

Denote by N_1 the number of the connected components of V_0 containing a point w_4 with the square of the euclidean norm $\|w_4\|^2 \leq \frac{1}{\varepsilon_1}$. The proved above claim states that the number N_0 does not exceed N_1, taking into account that

$$V_0 \subset \left(\mathbb{R}^k - \{g = 0\}\right)^{(\mathbb{R}_1)} = \mathbb{R}_1^k - (\{g = 0\})^{(\mathbb{R}_1)}$$

On the other hand, $B_0(H_1, \dots, H_m) \leq N_0$, since $\sqcap_{1 \leq i \leq m} L_{H_i} \mid g$ (evidently, in every connected component, being an open set in the euclidean topology, of the complement of the arrangement $\left(\mathbb{R}^k - \bigcup_{1 \leq i \leq m} H_i\right) \supset \left(\mathbb{R}^k - \{g = 0\}\right)$, there exists a point at which g does not vanish).

Obviously, N_1 is less than or equal to the number N_2 of the connected components of the set

$$V_1 = V_0 \cap \left\{(z_1, \dots, z_k) \in \mathbb{R}_1^k : \|z_1, \dots, z_k\|^2 \leq \frac{1}{\varepsilon_1}\right\}$$

In its turn $V_1 = \prod_0(V)$, where $\prod_0 : \mathbb{R}_1^{k+1} \to \mathbb{R}_1^k$ is the projection along the coordinate Z_0. Hence $N_2 \leq N_3$.

Gathering the obtained chain of inequalities $B_0(H_1, \dots, H_m) \leq N_0 \leq N_1 \leq N_2 \leq N_3 \leq N_4$ for the numbers of the connected components, we conclude that $B_0(H_1, \dots, H_m)$ does not exceed the number of connected components of $\mathcal{V}$. The latter is less than $2^{O(s+k)}$ according to [W68] and Tarski's transfer principle (see above).

The proposition is proved.

2 Lower bounds for randomized computation trees

Recall (see e.g. [B83]) that in the computation tree (CT) testing polynomials are computed along paths using the elementary arithmetic operations.

In particular, for a testing polynomial $f_i \in \mathbb{R}[X_1, \dots, X_n]$ at the level i (assuming that the root has the zero level) we have $C(f_i) \le i$. Under RCT (cf. [MT82], [S83], [M85a,b,c]) we mean a collection of CT $T = \{T_\alpha\}$ and a probabilistic vector $p_\alpha \ge 0$, $\sum_\alpha p_\alpha = 1$ such that T_α is chosen with the probability p_α. The main requirement is that for any input RCT gives a correct output with the probability $1 - \gamma > \frac{1}{2}$ (γ is called the error probability of RCT).

For a hyperplane $H \subset \mathbb{R}^n$ by $H^+ \subset \mathbb{R}^n$ denote the closed halfspace $\{L_H \ge 0\}$, where L_H is a certain linear function with the zero set H. For a family of hyperplanes $H_1, \dots, H_m$ the intersections $S^+ = \cap_{1 \le i \le m} H_i^+$ is called a polyhedron. An intersection $\Gamma = H_{i_1} \cap \cdots \cap H_{i_{n-k}}$ is called k-face of S^+ if $dim\ \Gamma = dim(\Gamma \cap S^+) = k$. By $\phi_k(S^+)$ we denote the number of k-faces of S^+. Similary (and even simpler) for the arrangement $S = \cup_{1 \le i \le m} H_i$ its k-face is any k-dimensional intersection of the form $\Gamma = H_{i_1} \cap \cdots \cap H_{i_{n-k}}$. By $\phi_k(S)$ we denote the number of k-faces of S.

Now we are able to formulate the main result of this paper.

Theorem: Let there exist positive constants c_1, c_2, c_3, c_4 such that $c_3(1 - c_1) < c_2$ and an arrangement $\mathcal{S} = S = \cup_{1 \le i \le m} H_i$ or a polyhedron $\mathcal{S} = S^+ = \cap_{1 \le i \le m} H_i^+$ satisfy the following properties:

1. $\phi_{[c_1 n]}(\mathcal{S}) \ge \Omega(m^{c_2 n})$;

2. for any k-face Γ of $\mathcal{S}$ with $k \ge c_1 n$ and any subfamily $H_{i_1}, \dots, H_{i_q}$ of $H_1, \dots, H_m$ with at least $q \ge m^{c_3}$ hyperplanes such that $H_{i_j} \not\supset \Gamma$ for each $1 \le j \le q$ and the hyperplanes $H_{i_1} \cap \Gamma, \dots, H_{i_q} \cap \Gamma$ in Γ are pairwise distinct, the number of the connected components $B_0^{(\Gamma)}(H_{i_1} \cap \Gamma, \dots, H_{i_q} \cap \Gamma)$ of the complement in Γ of the arrangement $\cup_{1 \le j \le q}(H_{i_j} \cap \Gamma)$ is greater than $\Omega(m^{c_4 n})$.

Then for any RCT recognizing $\mathcal{S}$, its depth is greater than $\Omega(n \log m)$.

Before proceeding to the proof of the theorem, we need some preparation.

First we fix the canonical representation of k-face Γ in two cases: namely, of S and of S^+, respectively (see [GKMS96]). In the case of S take the maximal $i_{n-k} \leq m$ such that $H_{i_{n-k}} \supset \Gamma$, then the maximal i_{n-k-1} such that $H_{i_{n-k-1}} \supset \Gamma$ and $dim(H_{i_{n-k}} \cap H_{i_{n-k-1}}) = n-2$ (obviously $i_{n-k-1} < i_{n-k}$) and so on we produce the indices $i_{n-k} > i_{n-k-1} > \cdots > i_1$ such that $\Gamma = H_{i_{n-k}} \cap \cdots \cap H_{i_1}$. As the representation of Γ we take the flag of planes: $H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \cdots \supset H_{i_{n-k}} \cap \cdots \cap H_{i_1} = \Gamma$.

Now consider the case of S^+. W.l.o.g. one could assume that $dim\ S^+ = n$. Under a hyperplane of a l-dimensional polyhedron we mean a $(l-1)$-plane which is $(l-1)$-face of the polyhedron. W.l.o.g. one could assume that all hyperplanes $H_1, \ldots, H_m$ are hyperfaces of S^+.

Take the maximal $i_{n-k} \leq m$ such that $H_{i_{n-k}} \supset \Gamma$. Denote the polyhedron $S_1^+ = H_{i_{n-k}} \cap S^+$. Obviously, Γ is its k-face and $dim\ S_1^+ = n-1$. By $\mathcal{H}_1$ denote the family of all hyperplanes H_i such that $H_i \supset \Gamma$ and $(H_{i_{n-k}} \cap H_i)$ is a hyperface of S_1^+ (thereby, it is $(n-2)$-face of S^+). Then $\mathcal{H}_1 \subset \{H_1, \ldots, H_{i_{n-k}-1}\}$ because of the choice of i_{n-k}. Since S_1^+ is a convex polyhedron, any of its faces is an intersection of some of its hyperfaces, in particular, any of its face Γ_1 which contains $\Gamma \subset \Gamma_1$, could be represented as $\Gamma_1 = H_{i_{n-k}} \cap (\bigcap_{H_i \in \mathcal{H}_1'} H_i)$ for a suitable subfamily $\mathcal{H}_1' \subset \mathcal{H}_1$.

Assume that by recursion on l it is already produced a sequence of indices $i_{n-k} > \cdots > i_{n-k-l+1}$, $1 \leq l \leq n-k-1$ such that $H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l_1+1}}$ is $(n-l_1)$-face of S^+ for every $1 \leq l_1 \leq l$. Denote $\Gamma^{(l)} = H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}}$ and the polyhedron $S_l^+ = \Gamma^{(l)} \cap S^+$. In addition, a family $\mathcal{H}_l \subset \{H_1, \ldots, H_{i_{n-k-l+1}-1}\}$ is produced such that for any $H_i \in \mathcal{H}_l$ $\Gamma^{(l)} \cap H_i$ contains Γ and is a hyperface of S_l^+, and vice versa any hyperface of S_l^+ has the form $\Gamma^{(l)} \cap H_i$ for a certain $H_i \in \mathcal{H}_l$. Hence any face $\Gamma_1 \supset \Gamma$ of S_l^+ has the form $\Gamma_1 = \Gamma^{(l)} \cap (\bigcap_{H_i \in \mathcal{H}_l'} H_i)$ for a suitable subfamily $\mathcal{H}_l' \subset \mathcal{H}_l$.

To carry out the recursive step, take as i_{n-k-l} the maximal index such that $H_{i_{n-k-l}} \in \mathcal{H}_l$ (obviously, $i_{n-k-l} < i_{n-k-l+1}$). Then $\Gamma^{(l+1)} = \Gamma^{(l)} \cap H_{i_{n-k-l}}$ is a hyperface of S_l^+ (and thereby is $(n-l-1)$-face of S^+). Denote the polyhedron $S_{l+1}^+ = H_{i_{n-k-l}} \cap S_l^+$. Take as $\mathcal{H}_{l+1}$ the family of all $H_i \in \mathcal{H}_l$ such that $\Gamma^{(l+1)} \cap H_i$ is a hyperface of S_{l+1}^+ (evidently, $\Gamma^{(l+1)} \cap H_i \supset \Gamma$ since $H_{i_{n-k-l}}, H_i \in$

$\mathcal{H}_l$). Due to the choice of i_{n-k-l} we have $\mathcal{H}_{l+1} \subset \{H_1, \dots, H_{i_{n-k-l}-1}\}$.

It remains to prove that for any hyperface Γ_2 of S^+_{l+1} such that $\Gamma_2 \supset \Gamma$, there exists $H_i \in \mathcal{H}_{l+1}$ for which $\Gamma_2 = \Gamma^{(l+1)} \cap H_i$. According to the property of $\mathcal{H}_l$ there exist $H_{j_1}, H_{j_2} \in \mathcal{H}_l$ such that $\Gamma_2 = \Gamma^{(l)} \cap H_{j_1} \cap H_{j_2}$. Since $\Gamma^{(l+1)} \supset \Gamma_2$ and $dim\ \Gamma^{(l+1)} = dim\ \Gamma_2 + 1 = n - l - 1$, either $\Gamma_2 = \Gamma^{(l+1)} \cap H_{j_1}$ or $\Gamma_2 = \Gamma^{(l+1)} \cap H_{j_2}$ is valid. In the former case $H_{j_1} \in \mathcal{H}_{l+1}$, in the latter case $H_{j_2} \in \mathcal{H}_{l+1}$. This completes the recursive step.

Thus, at the end of recursion we obtain a flag, which we treat as the claimed canonical representation of the k-face Γ:

$$H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \cdots \supset H_{i_{n-k}} \cap \cdots \cap H_{i_1} = \Gamma$$

such that for each $1 \leq l \leq k$ $H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}}$ is $(n-l)$-face of S^+ (the recursion on l implies that $dim(H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}}) = n - l$).

Fix k-face Γ of $\mathcal{S}$, where either $\mathcal{S} = S$ or $\mathcal{S} = S^+$. Let $H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \cdots \supset H_{i_{n-k}} \cap \cdots \cap H_{i_1} = \Gamma$ be a flag which represents Γ as described above. For a family of polynomials $f_1, \dots, f_s \in \mathbb{R}[X_1, \dots, X_n]$ we define $Var^{(\Gamma)}(f_1, \dots, f_s)$ to be the number of the variables among $Y_1, \dots, Y_{n-k}$ (we utilize the notations introduced in section 1) which occur in at least one of $lm(f_1), \dots, lm(f_s)$, where $H_{i_1}, \dots, H_{i_{n-k}}$ are the coordinate hyperplanes of the coordinates $Y_1, \dots, Y_{n-k}$, respectively. Since $lm(f_1 \cdots f_s) = lm(f_1) \cdots lm(f_s)$ we get that $Var^{(H_{i_1}, \dots, H_{i_{n-k}})}(f_1 \cdots f_s) = Var^{(\Gamma)}(f_1 \cdots f_s) = Var^{(\Gamma)}(f_1, \dots, f_s)$.

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

The following lemma was proved in [GKMS96].

Lemma 1: Let $T = \{T_\alpha\}$ be an RCT recognizing

a) an arrangement $S = \cup_{1 \leq i \leq m} H_i$ such that $\Gamma = \cap_{1 \leq j \leq n-k} H_{i_j}$ is k-face of S, or

b) a polyhedron $S^+ = \cap_{1\le i\le m} H_i^+$ such that for each $1 \le l \le n-k$ $\cap_{l\le j\le n-k} H_{i_j}$ is $(k+l-1)$-face of S^+ (denote $\Gamma = \cap_{1\le j\le n-k} H_{i_j}$)

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

Remark: Notice that the conditions in a), b) are fulfilled if $H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \cdots \supset H_{i_{n-k}} \cap \cdots \cap H_{i_1} = \Gamma$ is the canonical flag representation of Γ in both cases of S and S^+ (see above).

Proof of Lemma 1: Choose the coordinates $Z_1,\dots,Z_k,Y_1,\dots,Y_{n-k}$ such that $Z_1,\dots,Z_k$ are the coordinates in Γ and $H_{i_1},\dots,H_{i_{n-k}}$ are the coordinate hyperplanes of $Y_1,\dots,Y_{n-k}$, respectively (cf. section 1), which satisfy the following properties. The origin $\underbrace{(0,\dots,0)}_{n}$ of this coordinates system $Z_1,\dots,Z_k,Y_1,\dots,Y_{n-k}$ does not lie in any l-face with $l<k$ and besides, in the case b) $(0,\dots,0)$ belongs to the polyhedron S^+. Also we require that for any testing polynomial f from any CT T_α $f^{(n-k)}\underbrace{(0,\dots,0)}_{k} \ne 0$ holds (recall that $f^{(n-k)} \not\equiv 0$ depends only on $H_{i_1},\dots,H_{i_{n-k}}$, see section 1).

a) Consider the point $E = (\underbrace{0,\dots,0}_{k},\varepsilon_{k+3},\dots,\varepsilon_{n+2})$ and the points $E_i^{(0)} = (\underbrace{0,\dots,0}_{k},\varepsilon_{k+3},\dots,\varepsilon_{k+i+1},0,\varepsilon_{k+i+3},\dots,\varepsilon_{n+2})$, $1\le i\le n-k$. Then the point $E\notin S$ (because of the choice of the origin of the coordinates system $Z_1,\dots,Z_k,Y_1,\dots,Y_{n-k}$) and $E_i^{(0)} \in S$, $1\le i\le n-k$.

Easy counting yields that there is a fraction of $\frac{1-2\gamma}{2(1-\gamma)}$ of all T_α's that give the correct outputs for E and for at least $(1-2\gamma)^2(n-k)$ many among $E_i^{(0)}$, $1\le i\le n-k$. Take such T_{α_0} and some $1\le i_0\le n-k$ for which T_{α_0} gives the correct output.

Denote by $f_1,\dots,f_s$ the testing polynomials along the path in T_{α_0} followed by the input E. We claim that Y_{i_0} occurs in one of the leading terms $lm(f_1),\dots,lm(f_s)$ (thereby, Y_{i_0} occurs in $lm(f_1\cdots f_s) = lm(f_1)\cdots lm(f_s)$, see above).

Suppose the contrary. Let $lm(f_l) = Z_1^{m'_1} \cdots Z_k^{m'_k} Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$, then $m_{i_0} = 0$ by the supposition. Then (1) from section 1 implies that $sgn(f_l(E_{i_0}^{(0)})) = sgn(f_l^{(n-k)}(\underbrace{0, \ldots, 0}_{k})) \neq 0$ because of the choice of the origin of the coordinates system $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$. By the same token $sgn(f_l(E)) = sgn(f_l^{(n-k)}(\underbrace{0, \ldots, 0}_{k}))$. Therefore, $E_{i_0}^{(0)}$ satisfies all the tests along the path under consideration in T_{α_0} followed by the input E, hence the output of T_{α_0} for the input $E_{i_0}^{(0)}$ is the same as for the input E, so incorrect, that contradicts the choice of i_0.

b) First we show that $E \in S^+$. Take any hyperplane $H_l = \{\kappa_1 Z_1 + \ldots + \kappa_k Z_k + \beta_1 Y_1 + \ldots + \beta_{n-k} Y_{n-k} + \beta_0 = 0\}$, $1 \leq l \leq m$ given by a linear function L_{H_l} with the coefficients $\kappa_i, \beta_j \in \mathbb{R}$. We need to show that $L_{H_l}(E) \geq 0$. Let $0 \leq j_0 \leq n-k$ be the uniquely defined index such that $\beta_0 = \ldots = \beta_{j_0-1} = 0$, $\beta_{j_0} \neq 0$ (if all $\beta_0 = \ldots = \beta_{n-k} = 0$ then $L_{H_l}(E) = 0$). We prove that $\beta_{j_0} > 0$, this would entail that $sgn(L_{H_l}(E)) = sgn(\beta_{j_0}) > 0$. Pick out an arbitrary point $v_{n-j_0} = (\underbrace{0, \ldots, 0}_{k}, y_1^{(n-j_0)}, \ldots, y_{j_0}^{(n-j_0)}, 0, \ldots, 0) \in ((H_{i_n} \cap \ldots \cap H_{i_{j_0+1}}) \cap S^+) - H_{i_{j_0}}$. Then $y_{j_0}^{(n-j_0)} \neq 0$, therefore $y_{j_0}^{(n-j_0)} > 0$ since $v_{n-j_0} \in S^+$. Hence $0 < sgn\, L_{H_l}(v_{n-j_0}) = sgn(\beta_{j_0} \cdot y_{j_0}^{(n-j_0)})$, this implies that $sgn(\beta_{j_0}) > 0$. Thus $E \in S^+$.

Notice that the points
$E_i^{(+)} = (0, \ldots, 0, \varepsilon_{k+3}, \ldots, \varepsilon_{k+i+1}, -\varepsilon_{k+i+2}, \varepsilon_{k+i+3}, \ldots, \varepsilon_{n+2}) \notin S^+$, $1 \leq i \leq n-k$.

The rest of the proof is similar as in a), with replacing the role of the points $E_i^{(0)}$ by $E_i^{(+)}$. In a similar way if $m_{i_0} = 0$ then $sgn(f_l(E_{i_0}^{(+)})) = sgn(f_l^{(n-k)}(\underbrace{0, \ldots, 0}_{k})) = sgn(f_l(E)) \neq 0$ again because of (1) from section 1. Lemma 1 is proved.

An analogue of lemma 2 from [GKMS96] is the following lemma.

Lemma 2: Let $\mathcal{S} = S$ or $\mathcal{S} = S^+$ satisfy the condition 2. of the theorem. Assume that CT T' for some constant $c > 0$, satisfies the inequality $Var^{(\Gamma)}(T') \geq c(1-c_1)n$ for at least M $\lceil c_1 n \rceil$-faces Γ of $\mathcal{S}$. Then the depth t of T' fulfils either $t \geq \Omega(n \ \log m)$ or $M \leq O(3^t m^{(1-c+c_3+\delta)(1-c_1)n})$, where a constant $\delta > 0$ could be made as close to zero as desired.

The proof of lemma 2 differs from the proof of the analogous lemma 2 from [GKMS96] proved for *d-decision* trees, in which the degrees of the testing polynomials do not exceed d, rather than *computation* trees (considered in the present paper), in which the degrees of the testing polynomials could be exponential in the depth t of CT. Therefore the main tool in the proof of lemma 2 is the lower bound on the border complexity from the proposition (see section 1).

Before proving lemma 2 we show how to deduce the theorem from lemmas 1 and 2. Consider RCT $\{T_\alpha\}$ recognizing $\mathcal{S}$ with error probability $\gamma < \frac{1}{2}$. Denote $k = \lceil c_1 n \rceil$. Lemma 1, condition 1. of the theorem and counting imply the existence of T_{α_0} such that the inequality $Var^{(\Gamma)}(T_{\alpha_0}) \geq (1-2\gamma)^2(n-k)$ is true for $M = \frac{1-2\gamma}{2(1-\gamma)}\Omega(m^{c_2 n})$ k-faces Γ of $\mathcal{S}$. Apply lemma 2 to CT $T' = T_{\alpha_0}$ with $c = (1-2\gamma)^2$. If $t \geq \Omega(n \ \log m)$ the theorem is proved, else since the error probability γ could be made a positive constant as close to zero as desired at the expence of increasing by a constant factor the depth of RCT [M85a,c], take γ such that $(1-c+\delta) < \frac{c_2 - c_3(1-c_1)}{1-c_1}$. Then lemma 2 entails that $t \geq \Omega(n \ \log m)$, which proves the theorem. Thus, it remains to prove lemma 2.

Proof of lemma 2: To each k-face Γ of $\mathcal{S}$ satisfying the inequality $Var^{(\Gamma)}(T') \geq c(n-k)$, we correspond a path in T' with the testing polynomials $f_1, \dots, f_s \in \mathbb{R}[X_1, \dots, X_n]$ such that $Var^{(\Gamma)}(f_1 \cdots f_s) \geq Var^{(\Gamma)}(T')$. Denote $f = f_1 \cdots f_s$. Consider a canonical representation of Γ by a flag (see above)

$$H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \dots \supset H_{i_{n-k}} \cap \dots \cap H_{i_1} = \Gamma$$

Fix this path of T' for the time being and consider all k-faces Γ to which corresponds this path. We arrange the representing flags of all these k-faces in a tree $\mathcal{T}$ which we call the tree of flags (cf. the proof of lemma 2 from [GKMS96]). $\mathcal{T}$ has a root with the zero level, each its path has the same length $n-k$ (such trees are called regular), some of its vertices are labeled.

We construct $\mathcal{T}$ by induction on the level of its vertices. The base of induction. For each k-face Γ to which corresponds the fixed path of T', construct a vertex, being a son of the root of $\mathcal{T}$, and to this vertex (of level 1) attach the hyperplane $H_{i_{n-k}}$ (we utilize inroduced above notations). Thus, to different sons of the root different hyperplanes are attached. We label the constructed vertex if and only if $Y_{n-k}|f$ (the latter means that the linear function or the variable Y_{n-k} gives a contribution into $Var^{(\Gamma)}(f)$). Besides, we assign to the constructed vertex the polynomial $f^{(1)} \in \mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-1}]$ (see section 1).

Now assume by induction on l that $l < n-k$ levels of $\mathcal{T}$ are already constructed. Consider any vertex v of $\mathcal{T}$ at l-th level. To the vertex v leads the partially labeled path (from the root), to whose vertices the beginning elements of a flag are attached successively:

$$H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \ldots \supset H_{i_{n-k}} \cap \ldots \cap H_{i_{n-k-l+1}} = \Gamma_1 \qquad (4)$$

Finally, the polynomial $f^{(l)} \in \mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-l}]$ is assigned to the vertex v. Recall (see section 1) that $f^{(l)}$ is defined on $(n-l)$-plane Γ_1. Besides, v is either labeled or not labeled.

Thus, to different vertices at the level l are attached the different beginnings of flags.

At the inductive step we construct the sons of v. Namely, for any k-face Γ with the same beginning (4) of its representing flag consider the next element of its flag, let it be $\Gamma_1 \cap H_{i_{n-k-l}}$. Construct a son of v to which we attach $\Gamma_1 \cap H_{i_{n-k-l}}$ and assign the polynomial $f^{(l+1)} \in \mathbb{R}[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k-l-1}]$. We label this vertex if and only if $Y_{n-k-l}|f^{(l)}$ (recall that due to the maintainance property, see section 1, the latter condition means that the linear form or the variable Y_{n-k-l} gives a contribution into $Var^{(\Gamma)}(f)$).

This completes the inductive construction of $\mathcal{T}$. The leaves (or paths) of $\mathcal{T}$ correspond bijectively to k-faces of $\mathcal{S}$ to which the fixed path of T' corresponds. To each leaf (or path) of $\mathcal{T}$ which corresponds to k-face Γ the flag representing Γ $H_{i_{n-k}} \supset H_{i_{n-k}} \cap H_{i_{n-k-1}} \supset \ldots \supset H_{i_{n-k}} \cap \ldots \cap H_{i_1} = \Gamma$ is attached along the path (which is partially labeled).

Now we proceed to estimating the number of leaves of $\mathcal{T}$. For a vertex v consider all its labeled sons (we utilize the introduced above notations). Each labeled son corresponds to a hyperplane H_i such that the linear function $L_{\Gamma_1 \cap H_i} | f^{(l)}$, where $L_{\Gamma_1 \cap H_i}$ is a certain linear function on $(n-l)$-plane Γ_1 with the zero set $\Gamma_1 \cap H_i$, being a hyperplane in Γ_1, and to different sons correspond different hyperplanes $\Gamma_1 \cap H_i$. Consider the family $\mathcal{H}$ of all such hyperplanes H_i. First assume that it contains at least m^{c_3} hyperplanes. Then the condition 2. of the theorem implies that the number of the connected components $b = B_0^{(\Gamma_1)}(\{H_i \cap \Gamma_1\}_{H_i \in \mathcal{H}})$ of the complement in Γ_1 of the arrangement $\bigcup_{H_i \in \mathcal{H}} (H_i \cap \Gamma_1)$ is greater than $\Omega(m^{c_4 n})$. On the other hand the proposition (see section 1) entails that $b \leq 2^{O(s+n-l)} \leq 2^{O(s+n)}$, taking into account that the complexity $C(f) = C(f_1 \cdots f_s) \leq 2s-1$. This provides the lower bound on the depth of T', namely, $t \geq s \geq \Omega(n \log m)$, that proves lemma 2. Thus, we can assume that any vertex v of $\mathcal{T}$ has less than m^{c_3} labeled sons. Besides the labeled sons, each vertex could have at most m unlabeled sons. Furthermore, due to the maintenance property, along each path of $\mathcal{T}$ at least $c(1-c_1)n$ vertices are labeled (see the inductive step above).

To estimate the number of leaves in $\mathcal{T}$ introduce an auxiliary magnitude $M(R,Q)$ to be the maximal possible number of the leaves in a regular tree (actually, we could stick with subtrees of $\mathcal{T}$, so they are partially labeled) with the length of any path equal to R and with at most Q unlabeled vertices along the path. One can assume w.l.o.g. that $Q \leq R \leq m$ (if $Q > R$ then set $M(R,Q) = 0$, the inequality $R \leq m$ holds since we consider the subtrees of $\mathcal{T}$, and to each path of $\mathcal{T}$ a flag of the length at most m is attached).

Considering such a tree and its subtrees with the roots being the sons (both unlabeled and labeled) of the root of the tree, we get the following inductive inequality:

$$M(R,Q) \leq m \cdot M(R-1,Q-1) + m^{c_3} M(R-1,Q)$$

For the base of induction, obviously $M(0,0) = 1$. By induction on R we obtain the bound $M(R,Q) \leq \beta \cdot m^Q \cdot m^{(c_3+\delta_1)R}$ for arbitrary $\delta_1 > 0$ and a suitable $\beta > 0$.

Substituting $R = n - \lceil c_1 n \rceil$, $Q = (1-c)(n - \lceil c_1 n \rceil)$, we conclude that the number of the leaves of $\mathcal{T}$ is less than $O(m^{(1-c)(1-c_1)n+(c_3+\delta)(1-c_1)n})$ for arbitrary $\delta > 0$.

To complete the proof of lemma 2 it remains to notice that the tree of flags $\mathcal{T}$ was constructed for a fixed path of CT T'; there are at most 3^t paths of T'. On the other hand, every k-face Γ of $\mathcal{S}$, satisfying the inequality $Var^{(\Gamma)}(T') \geq c(1-c_1)n$, corresponds to one of the leaves of a tree of flags constructed for one of the paths of T'. Hence the number of such k-faces $M \leq O(3^t \cdot m^{(1-c+c_3+\delta)(1-c_1)n})$.

3 Quadratic complexity lower bound for RCTs solving the restricted integer programming

The restricted integer programming is the arrangement

$$L_{n,j} = \bigcup_{a \in \{0,\ldots,j-1\}^n} \{aX = 1\} \subset \mathbb{R}^n$$

of $m = j^n$ hyperplanes for some $j \geq 2$ (see e.g. [M85b]). For $j = 2$ $L_{n,2}$ is the knapsack problem.

As an application of the theorem we prove the following corollary.

Corollary: For any RCT solving the restricted integer programming $L_{n,j}$, its depth is greater than $\Omega(n^2 \log j)$.

To check the conditions 1., 2. of the theorem first take $\frac{3}{4} < c_1 < 1$. Any $k = \lceil c_1 n \rceil$-face Γ of $L_{n,j}$ can be given by $n-k$ linear equations $g_1, \dots, g_{n-k}$ of the form $aX = 1$ from $L_{n,j}$. If other linear equations $g'_1, \dots, g'_{n-k}$ from the family $L_{n,j}$ give the same k-face Γ then their linear hulls coincide: $\mathcal{L}(g_1, \dots, g_{n-k}) = \mathcal{L}(g'_1, \dots, g'_{n-k})$.

Take a prime $j \le p < 2j$. Let us show that the linear hull $\mathcal{L}(g_1, \dots, g_{n-k})$ contains at most p^{n-k} linear equations from the family $L_{n,j}$. Consider the linear equations from $(\mathcal{L}(g_1, \dots, g_{n-k}) \cap L_{n,j}) \bmod p$ (we treat the linear equations as their vectors of the coefficients). Then the results are pairwise distinct vectors, they constitute a family $\mathcal{F} \subset \mathbb{F}_p^{n+1}$, choose among the elements from $\mathcal{F}$ a basis over $\mathbb{F}_p$, it contains at most $n-k$ elements (otherwise, the preimages of $\mathcal{F}$ prior taking *modp* would be linear independent as well). All the vectors from $\mathcal{F}$ are the linear combinations over $\mathbb{F}_p$ of the elements of the basis, therefore, $\mathcal{F}$ contains at most p^{n-k} elements, thus the cardinality $|\mathcal{L}(g_1, \dots, g_{n-k}) \cap L_{n,j}| = |\mathcal{F}| \le p^{n-k}$.

Any $(n-k)$-tuple of the linearly independent linear equations from $L_{n,j}$ provides a k-face. Therefore, any k-face is provided by less or equal to

$$\binom{p^{n-k}}{n-k} \le p^{(n-k)^2} \le (2j-1)^{(n-k)^2}$$

number of $(n-k)$-tuples because of the shown above. On the other hand, denote by I_l, $1 \le l \le n$ the number of linearly independent l-tuples from $L_{n,j}$. Obviously, $I_1 = j^n - 1$. By induction on l for $l \le n-1$ we have $I_{l+1} \ge \frac{I_l(j^n - p^l)}{l+1}$ again because of the shown above. Hence,

$$I_l \ge (j^n-1)(j^n-p)(j^n-p^2)\cdots(j^n-p^{l-1})\frac{1}{l!} \quad >$$

$$(j^n-1)(j^n-2j)(j^n-(2j)^2)\cdots(j^n-(2j)^{l-1})\frac{1}{l!} \quad >$$

$$j^{nl}\left(1 - \frac{1+(2j)+(2j)^2+\cdots+(2j)^{l-1}}{j^n}\right)\frac{1}{l!} \quad =$$

$$j^{nl}\left(1-\frac{(2j)^l-1}{(2j-1)j^n}\right)\frac{1}{l!}$$

If $l \le \frac{n}{2}$ we have $\frac{(2j)^l-1}{(2j-1)j^n} \le \frac{1}{3}$, i.e. $I_l > \Omega(\frac{j^{nl}}{l!})$. Substituting $l = n-k$, we conclude that the number of k-faces $\phi_k(L_{n,j})$ is greater than

$$\Omega\left(\frac{j^{(1-c_1-\delta_1)n^2}}{(2j)^{(1-c_1)^2n^2}}\right) \ge \Omega\left(j^{((1-c_1)(2c_1-1)-\delta_1)n^2}\right)$$

for arbitrary $\delta_1 > 0$. Thus, to satisfy the condition 1. in the theorem one can take $c_2 = (1-c_1)(2c_1-1)-\delta_1$.

To justify the condition 2. in the theorem take any k_1-face Γ of $L_{n,j}$ where $k_1 \ge k$ given by $n-k_1$ linear equations $g_1, \dots, g_{n-k_1}$ from $L_{n,j}$, and besides, $q \ge j^{c_3 n}$ linear equations $h_1, \dots, h_q$ from $L_{n,j}$. Take a certain $0 < c_5 < 1$ which will be specified later. Denote $k_2 = \lceil c_5 n \rceil$. There are $\binom{q}{k_2} \ge \Omega(j^{c_5(c_3-\delta)n^2})$ k_2-tuples from $h_1, \dots, h_q$ for arbitrary $\delta > 0$. If two k_2-tuples $h_{i_1}, \dots, h_{i_{k_2}}$ and $h_{l_1}, \dots, h_{l_{k_2}}$ give the same face in Γ (i.e. a face of $L_{n,j}$, being a subset of Γ), the linear hulls coincide:

$$\mathcal{L}(g_1, \dots, g_{n-k_1}, h_{i_1}, \dots, h_{i_{k_2}}) = \mathcal{L}(g_1, \dots, g_{n-k_1}, h_{l_1}, \dots, h_{l_{k_2}})$$

(cf. above). Therefore, for any face in Γ there are at most $\binom{p^{n-k_1+k_2}}{k_2} \le (2j)^{c_5(n-k_1+c_5n)n}$ such k_2-tuples (since the latter linear hull contains at most $p^{n-k_1+k_2}$ linear equations from $L_{n,j}$, see above). Furthermore, $(2j)^{c_5(n-k_1+c_5n)n} \le j^{2c_5(1-c_1+c_5)n^2}$. Thus, the number of faces in Γ of the subarrangement $S^{(\Gamma)} = \bigcup_{1\le i\le q}(\Gamma \cap \{h_i = 0\})$ is greater than $\Omega\left(j^{c_5(c_3-\delta-2+2c_1-2c_5)n^2}\right)$.

Now take $c_3 = \frac{1}{2}$, then the requirement $c_3(1-c_1) < c_2$ is fulfilled for small enough $\delta_1 > 0$. Since $c_3 - 2 + 2c_1 > 0$, one could choose $c_5 > 0$ and $\delta > 0$ small enough to provide $c_4' = c_5(c_3 - \delta - 2 + 2c_1 - 2c_5) > 0$.

Thus, we have proved so far that the number of faces in Γ in the subarrangement $S^{(\Gamma)}$ is greater than $\Omega(j^{c_4'n^2})$. Take any $0 < c_4 < c_4'$. The required bound 2. of the theorem on the number of the connected components of the complement in Γ of the subarrangement $S^{(\Gamma)}$ $B_0^{(\Gamma)}(\Gamma \cap \{h_1 = 0\}, \dots, \Gamma \cap \{h_q = 0\}) \geq \Omega(j^{c_4 n^2})$ (and thereby the corollary) follows from the following general remark (this can be deduced also from [B92], but for the sake of selfcontainess we give a short and elementary proof of it).

Remark: For any arrangement $S = \bigcup_{1 \leq i \leq m} H_i \subset \mathbb{R}^n$ and $0 \leq k \leq n-1$ the number of k-faces in the arrangement $\phi_k(S) < B_0(H_1, \dots, H_m)$.

Proof: Intersecting S with a generic $(n-k)$-plane, we reduce the remark to the case $k = 0$.

Thus $k = 0$. Choose a generic hyperplane H and shift it parallel to itself. When it contains a vertex v of S we show that there "appears" a new (in other words, not yet swept) connected component of the complement $\mathbb{R}^n - S$ with a vertex v and situated completely on one side of H. Indeed, let $v = \bigcap_{1 \leq j \leq n} H_{i_j}$ for some $H_{i_1}, \dots, H_{i_n}$. Take the coordinates system with the coordinate hyperplanes $H_{i_1}, \dots, H_{i_n}$. Let H have an equation in these coordinates $\alpha_1 X_1 + \dots + \alpha_n X_n = 0$, each $\alpha_i \neq 0$, $1 \leq i \leq n$, since H is generic. Then the "orthant" $\{\alpha_i X_i \geq 0; 1 \leq i \leq n\}$ (which is situated completely on one side of H) contains a connected component of the complement $\mathbb{R}^n - S$ with a vertex in v.

So, to each vertex v of S corresponds a connected component of the complement $\mathbb{R}^n - S$. In addition, to the first (in the order of shifting H) vertex v_1 corresponds also at least one more connected component situated in the "orthant" $\{\alpha_i X_i \leq 0; 1 \leq i \leq n\}$ (so on the other side of H) with a vertex in v_1, this implies the strict inequality in the remark.

4 Lower bound on the complexity of deterministic computation trees

For CT T' which recognizes either an arrangement $\mathcal{S} = S$ or a polyhedron $\mathcal{S} = S^+$ given by the hyperplanes $H_1, \dots, H_m$, we can give the similar complexity lower bound $\Omega(\log N)$ as in the theorem, where N is the number of k-faces of $\mathcal{S}$, without the restriction $N \geq m^{\Omega(n)}$ imposed in the theorem.

Theorem 2: Let CT T' with the depth t recognize $\mathcal{S}$ with N k-faces, and $\mathcal{S}$ satisfy the following condition. For any k_1-face Γ of $\mathcal{S}$ with $k_1 \geq k$ and any subset $H_{i_1}, \dots, H_{i_s}$ with $s \geq N^{c_3/(n-k)}$ for a certain $c_3 < 1$ such that the planes $H_{i_1} \cap \Gamma, \dots, H_{i_s} \cap \Gamma$ are pairwise distinct from Γ, the number of connected componets of the complement in Γ of the arrangement $B_0^{(\Gamma)}(H_{i_1} \cap \Gamma, \dots, H_{i_s} \cap \Gamma) \geq N^{c_4}$ for a suitable $c_4 > 0$. Then $t \geq \Omega(\log N)$.

The proof follows the proof of the theorem with considerable simplifications. Namely, in lemma 1 one states that $Var^{(\Gamma)}(T') = n - k$. In lemma 2 we have either the bound $2^t \geq N^{\Omega(c_4)}$ or the bound $N \leq 3^t N^{c_3}$ due to the estimation $M(n-k, 0) \leq N^{c_3}$.

Notice that the Theorem 2 in case of an arrangement $\mathcal{S} = S$ follows from [SY82], [B83] without the condition in the Theorem 2. In case of a polyhedron $\mathcal{S} = S^+$ a weaker complexity lower bound $\Omega(\log N / \log\log N)$ was proved in Theorem 2 from [GKV96] without the condition of Theorem 2.

5 Open Problem

We were not able to prove any superlinear lower bound or a linear upper bound on the *Element Distinctness*(cf. [M85a], [GKMS96]) for randomized computational trees. Note that the corresponding lower bound for randomized decision trees is $\Omega(n \log n)$, [GKMS96].

Acknowledgement

We thank Friedhelm Meyer auf der Heide, Volker Strassen, and Andy Yao for many stimulating discussions.

References

[B83] M. Ben-Or, *Lower Bounds for Algebraic Computation Trees*, Proc. 15th ACM STOC (1983), pp. 80–86.

[B79] D. Bini, *Border Rank of a $p \times q \times 2$ Tensor and the Optimal Approximation of a Pair of Bilinear Forms*, Proc. ICALP 80, Lecture Notes in Computer Science Vol. 85, Springer-Verlag, 1980, pp. 98–108.

[BCLR79] D. Bini, M. Capovani, G. Lotti, F. Romassi, *$O(n^{2.7799})$ Complexity for $n \times n$ Approximate Matrix Multiplication*, Inform. Processing Letters **8** (1979), pp. 234–235.

[B92] A. Björner, Subspace Arrangements, Proc. First European Congress of Mathematicians, Progress in Mathematics, Vol. 119, Birkhäuser, 1992, pp. 321–370.

[BLY92] A. Björner, L. Lovasz and A. Yao, *Linear Decision Trees: Volume Estimates and Topological Bounds*, Proc. 24th ACM STOC (1992), pp. 170–177.

[BKL93] P. Buergisser, M. Karpinski, T. Lickteig, *On Randomized Algebraic Test Complexity*, J. of Complexity **9** (1993), pp. 231–251.

[BPR94] S. Basu, R. Pollack, M.-R. Roy, *On the Combinatorial and Algebraic Complexity of Quantifier Elemination*, Proc. 35th IEEE FOCS, 1994, pp. 632–641.

[CKKLW95] F. Cucker, M. Karpinski, P. Koiran, T. Lickteig, K. Werther, *On Real Turing Machines That Toss Coins*, Proc. 37th ACM STOC (1995), pp. 335–342.

[DL78] D.P. Dobkin, R.J. Lipton, *A Lower Bound of $\frac{1}{2}n^2$ on Linear Search Programms for the Knapsack Problem*, J. Comput. Syst. Sci. **16** (1978), pp. 413–417.

[GK93] 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.

[GK94] 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.

[GK97] D. Grigoriev, M. Karpinski, *Randomized $\Omega(n^2)$Lower Bound for Knapsack*, Proc. 29th ACM STOC (1997).

[GKMS96] D. Grigoriev, M. Karpinski, F. Meyer auf der Heide, R. Smolensky, *A Lower Bound for Randomized Algebraic Decision Trees*, Proc. 28th ACM STOC (1996), pp. 612–619; submitted to Computational Complexity.

[GKS96] D. Grigoriev, M. Karpinski, R. Smolensky, *Randomization and the Computational Power of Analytic and Algebraic Decision Trees*; submitted to Computational Complexity.

[GKV95] 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; also to appear in Discrete and Computational Geometry, 1996.

[GKV96] D. Grigoriev, M. Karpinski, N. Vorobjov, *Lower Bound on Testing Membership to a Polyhedron by Algebraic Decision and Computation Trees*, Discrete and Computational Geometry, 1996.

[GKY96] D. Grigoriev, M. Karpinski, A. Yao, *An Exponential Lower Bound on the Size of Algebraic Decision Trees for the MAX*, submitted to J. Computational Complexity.

[GV88] D. Grigoriev, N. Vorobjov, *Solving Systems of Polynomial Inequalities in Subexponential Time*, Journal of Symbolic Comp. **5** (1988), pp. 37–64.

[KV88] M. Karpinski, R. Verbeek, *Randomness, Provability, and the Separation of Monte Carlo Time and Space*, LNCS, **270** (1988), Springer-Verlag, 1988, pp. 189–207.

[L65] S. Lang, *Algebra*, Addison–Wesley, New York, 1965.

[MT82] U. Manber, M. Tompa, *Probabilistic, Nondeterministic and Alternating Decision Trees*, Proc. 14th ACM STOC (1982), pp. 234–244.

[M64] J. Milnor, *On the Betti Numbers of Real Varieties*, Proc. AMS, 1996, v. 15, pp. 275–280.

[M84] F. Meyer auf der Heide, *A Polynomial Linear Search Algorithm for the n-Dimensional Knapsack Problem*, J. ACM **31** (1984), pp. 668–676.

[M85a] F. Meyer auf der Heide, *Nondeterministic versus Probabilistic Linear Search Algorithms*, Proc. IEEE FOCS (1985), pp. 65–73.

[M85b] F. Meyer auf der Heide, *Lower Bounds for Solving Linear Diophantic Equations on Random Access Machines*, J. ACM **32** (1985), pp. 929–937.

[M85c] F. Meyer auf der Heide, *Simulating Probabilistic by Deterministic Algebraic Computation Trees*, Theoretical Computer Science **41** (1985), pp. 325–330.

[MPR94] L. Montana, L. Pardo, T. Recio, *A Note on Rabin's Width of a Complete Proof*, Computational Complexity, 1994, v. 4, p. 12–36.

[MT82] U. Manber, M. Tompa, *Probabilistic, Nondeterministic and Alternating Decision Trees*, Proc. 14th ACM STOC (1982), pp. 234-244.

[R72] M. Rabin, *Proving Simultaneous Positivity of Linear Forms*, J. Comput. Syst. Sci., 1972, v. 6, p. 639–650.

[S83] M. Snir, *Lower Bounds for Probabilistic Linear Decision Trees*, Research Report 83-6, Dept. of Computer Science, Hebrew University of Jerusalem, 1983.

[S90] V. Strassen, *Algebraic Complexity Theory*, in Handbook of Theoretical Computer Science, vol. A, 1990, Elsevier, pp. 633–672.

[SY82] J. M. Steele and A. C. Yao, *Lower Bounds for Algebraic Decision Trees*, J. of Algorithms **3** (1982), pp. 1–8.

[T51] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, University of California Press, 1951.

[W68] H. Warren, *Lower Bounds for Approximation of Nonlinear Manifolds*, Trans. AMS, 1968, v. 133, pp. 167–178.

[Y92] A. Yao, *Algebraic Decision Trees and Euler Characteristics*, Proc. 33rd IEEE FOCS (1992), pp. 268–277.

[Y94] A. Yao, *Decision Tree Complexity and Betti Numbers*, Proc. 26th ACM STOC (1994), pp. 615–624.

[YI65] S. Yajima, T. Ibarak, *A Lower Bound on the Number of Threshold Functions*, IEEE EC, 1965, V. 14, pp. 926–929.