Randomized Complexity Lower Bound for Arrangements and Polyhedra

D Grigoriev

Randomized Complexity Lower Bound for Arrangements and Polyhedra

D. Grigoriev

IRMAR, Université de Rennes
Campus de Beaulieu, 35042 Rennes, cedex France
dima@maths.univ-rennes1.fr

The complexity lower bound $\Omega(\log N)$ for randomized computation trees is proved for recognizing an arrangement or a polyhedron with N faces. This provides in particular, the randomized lower bound $\Omega(n \log n)$ for the DISTINCTNESS problem and generalizes [11] where the randomized lower bound $\Omega(n^2)$ was ascertained for the KNAPSACK problem. The core of the method is an extension of the lower bound from [8] on the multiplicative complexity of a polynomial.

Introduction.

The complexity lower bounds for deterministic algebraic computation trees were obtained in [26], [2], [4], [30], [31], [22] where the topological methods were developed. In particular, these methods provide the lower bound $\Omega(\log N)$ for recognizing (a membership to) 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 $\bigcup_{1 \le i < j \le n} \{X_i = X_j\} \subset \mathbb{R}^n$, EQUALITY SET problem $\{(x_1, \ldots, x_n, y_1, \ldots, y_n) : (x_1, \ldots, x_n)$ is a permutation of $(y_1, \ldots, y_n)\} \subset \mathbb{R}^{2n}$ and the lower bound $\Omega(n^2)$ for the KNAP-

SACK problem $\bigcup_{I\subset\{1,\ldots,n\}} \left\{\sum_{i\in I} x_i = 1\right\} \subset \mathbb{R}^n$. 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], [20], [9], [10] but for decade an open problem remained, to obtain nonlinear 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 [8] the proposed lower bound $\Omega(\log N)$ was proved for the randomized algebraic computation trees over an arbitrary field of zero characteristic, here the computation branches according to the signs $\{=,\neq\}$ unlike the more customary computation trees over the reals, studied in all previously mentioned papers including the present one, which branch according to the signs $\{\leq,>\}$. The core of the method of [8] was the lower bound $\Omega(\log N)$ on the multiplicative complexity of a polynomial (see e.g. [27]), where N is the number of the faces of an arrangement on which the polynomial vanishes.

In the present paper the latter lower bound $\Omega(\log N_1)$ on the multiplica-

tive complexity of a polynomial is extended (see the corollary in section 2) to a modified invariant N_1 of an arrangement, namely, the number of so-called *strongly singular* faces (see section 1) of the arrangement (now the polynomial does not necessary vanish on the arrangement). Relying on this lower bound on the multiplicative complexity, the proof of the complexity lower bound $\Omega(\log N)$ for RCT recognizing an arrangement or a polyhedron with N faces (see the theorem in section 3) becomes much simpler than the related ones in [13], [11]. In particular, this gives the lower bound $\Omega(n \log n)$ for RCT recognizing the DISTINCTNESS problem. The construction of RCT with the linear complexity $O(n)$ for the EQUALITY SET problem from [5] shows that the condition imposed in the present paper (as well as in [8]) that the recognized set is an arrangement, so a union of hyperplanes, rather than a union of planes of greater than 1 codimensions as in the EQUALITY SET problem, is essential. In the last section 4 we generalize the construction of [5] and design a RCT for recognizing the following problem $\{(x_1, \ldots, x_n, y_1, \ldots, y_m)$: each of the both differences of the multisets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ contains at most k elements $\} \subset \mathbb{R}^{n+m}$ which has a linear complexity when k is a constant. For arbitrary n, m the randomized complexity of this problem remains to be an open question.

Let us also mention the paper [12] where a complexity lower bound was established for the randomized *analytic* decision trees (rather than for more customary algebraic ones) and also the paper [7] 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 Strongly singular faces of an arrangement with respect to a polynomial.

By F we denote a field of zero characteristic. Let $H_1, \ldots, H_m \subset F^n$ be hyperplanes and let $\Gamma = H_{i_1} \cap \cdots \cap H_{i_{n-k}}$ have the dimension $\dim \Gamma = k$, so Γ is k-face of the arrangement $S = H_1 \cup \cdots \cup H_m$.

Fix arbitrary coordinates $Z_1, \ldots, Z_k$ in Γ. Then treating $H_{i_1}, \ldots, H_{i_{n-k}}$ 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 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

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

$0 \neq \alpha \in F$ with respect to the coordinate system $Z_1,\dots,Z_k,Y_1,\dots,Y_{n-k}$ as the minimal term in the lexicographical ordering $Z_1 > \cdots > Z_k > Y_1 > \cdots > Y_{n-k}$, namely 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

$$\begin{aligned} 0 \not\equiv f^{(1)} &= \left(\frac{f}{Y_{n-k}^{m_{n-k}}}\right)(Z_1,\dots,Z_k,Y_1,\dots,Y_{n-k-1},0) \in \\ & F[Z_1,\dots,Z_k,Y_1,\dots,Y_{n-k-1}] \end{aligned}$$

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 $0 \not\equiv f^{(2)} \in F[Z_1,\dots,Z_k,$ $Y_1,\dots,Y_{n-k-2}]$ 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}, $m_{n-k-1}, \ldots, m_1$ and the polynomials

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

$1 \leq l \leq n-k$, 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 f, in which occurs the monomial $Y_{n-k-l+2}^{m_{n-k-1+2}} \cdots Y_{n-k}^{m_{n-k}}$ for each $1 \leq l \leq n-k$. Notice that $m_{n-k}, \ldots, m_{n-k-l}$ depend only on the hyperplanes $H_{i_{n-k}}, \ldots, H_{i_{n-k-l}}$ 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 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 $H_{i_{n-k}}, \ldots, H_{i_{n-k-l}}$ 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 $H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}}$. Continuing, we define also $m'_k, \ldots, m'_1$. Observe that 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 [13], [11]).

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

For any polynomial $g \in F[X_1, \ldots, X_n]$ one can rewrite it in the coordinates $\overline{g}(Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k})$ and expand $\overline{g} = g_s + g_{s+1} + \cdots + g_{s_1}$, where $g_j \in F[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}]$, $s \leq j \leq s_1$ is homogeneous with respect to the variables $Y_1, \ldots, Y_{n-k}$ of degree j and $g_s = g_s^{(0)} \not\equiv 0$. Consider the leading term $lm(g_s) = \alpha Z_1^{m'_1} \cdots Z_k^{m'_k} Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$ and denote by $\mathrm{Var}^{(H_{i_1}, \ldots, H_{i_{n-k}})}(g)$ the number of positive (in other words, nonzero) integers among $m_{n-k}, \ldots, m_1$, note that $s = m_1 + \cdots + m_{n-k}$. Although $\mathrm{Var}^{(H_{i_1}, \ldots, H_{i_{n-k}})}(g)$ depends on the order of the hyperplanes $H_{i_1}, \ldots, H_{i_{n-k}}$, we will denote it sometimes by $\mathrm{Var}^{(\Gamma)}(g)$ for brevity when no ambiguity could happen. As we have shown above $\mathrm{Var}^{(H_{i_1}, \ldots, H_{i_{n-k}})}(g)$ is independent from the coordinates $Z_1, \ldots, Z_k$ of Γ. Obviously, $\mathrm{Var}^{(H_{i_1}, \ldots, H_{i_{n-k}})}(g)$ 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 $\{g_s^{(l)} = 0\} \cap H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}}$ contains the plane $H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}} \cap H_{i_{n-k-l}}$ (being a hyperplane in $H_{i_{n-k}} \cap \cdots \cap H_{i_{n-k-l+1}}$).

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. [19]). 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 [19]).

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. [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: $sgn(b) = sgn(\beta_{i_0})$. 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 $\varepsilon_1 > \varepsilon_2 \cdots > \varepsilon_{n+1} > 0$ be infinitesimals, where ε_1 is an infinitesimal relative to $\mathbb{R}$; in general ε_{i+1} is an infinitesimal relative to $\mathbb{R}(\varepsilon_1, \ldots, \varepsilon_i)$ for all $0 \leq i \leq n$. 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 $b \in \mathbb{R}_{n+1}$ for brevity denote the standard part $st_i(b) = st_{\varepsilon_{i+1}}(st_{\varepsilon_{i+2}} \cdots (st_{\varepsilon_{n+1}}(b) \cdots)) \in \mathbb{R}_i$ (provided that it is definable).

Also we will use the Tarski's transfer principle [29]. 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 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, $V \subset V^{(F_2)}$).

One could easily see that for any point $(z_1, \ldots, z_k) \in \mathbb{R}_k^k$ and a polynomial $g \in \mathbb{R}[X_1, \ldots, X_n]$ such that $g_s^{(n-k)}(z_1, \ldots, z_k) \neq 0$ (we utilize the introduced above notations) the following equality for the signs

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

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:

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

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 $\mathrm{Var}^{(H_{i_1}, \dots, H_{i_{n-k}})}(g) \geq \eta(n-k)$. 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).

2 Multiplicative complexity and strongly singular faces.

Consider the graph (cf. [27], [18]) of the gradient map $G = \{(x, \mathrm{grad}_g(x)) : x \in F^n\} \subset F^{2n} = \{(x_1, \dots, x_n, v_1, \dots, v_n)\}$, so $v_i = \frac{\partial g}{\partial X_i}(x)$, $1 \leq i \leq n$. The notion of the degree deg was extended in [17] to constructible sets in an affine space from the usual case of closed projective sets ([25], [23]). We are now able to formulate the main technical tool of this section (cf. theorem 1 [8]).

Lemma 1 *For any $0 \leq k \leq n, 0 < \eta \leq 1$ and an arrangement $S = H_1 \cup \dots \cup H_m$ having N strongly singular k-faces with respect to a polynomial $g \in F[X_1, \dots, X_n]$ over an algebraically closed zero-characteristics field F, the following bound holds: $deg G \geq \Omega(N/(m^{(1-\eta)(n-k)} 2^{4n}))$*

Proof. w.l.o.g. we assume that $N \geq 1$, otherwise the lemma is trivial. We introduce a linear projection $\varphi : F^{2n} \to F^n$ where $\varphi(X_1, \dots, X_n, V_1, \dots, V_n) = (X_1, \dots, X_n)$. Also we introduce a rational map $\psi : F^{2n} \to \mathbb{P}^{n^2+n-1}$ where

$\mathbb{P}^{n^2+n-1}$ is the projective space with the coordinates $\{W_{i\ell}\}_{1\le i,\ell\le n} : \{W_\ell\}_{1\le \ell\le n}$, herewith ψ is given by the formulae $W_{i\ell} = X_iV_\ell, W_\ell = V_\ell, 1 \le i,\ell \le n$. Thus, ψ is defined for any point $(x,v) \in F^{2n}$ such that $v \neq 0$. In fact, ψ could be viewed as the composition of the following natural rational maps $F^{2n} \to F^n \times (F^n - 0) \to F^n \times \mathbb{P}^{n-1} \hookrightarrow \mathbb{P}^n \times \mathbb{P}^{n-1} \hookrightarrow \mathbb{P}^{n^2+n-1}$, where the latter one is the Segre embedding ([25], [23]). Finally, we denote by $\sigma : \mathbb{P}^{n^2+n-1} \to \mathbb{P}^{n-1}$ the linear projection, where $\sigma(\{W_{i\ell}\} : \{W_\ell\}) = \{W_\ell\}$. The role of σ is to distinguish the coordinates of the gradient.

For the time being fix a strongly singular k-face $\Gamma = H_{i_1} \cap \cdots \cap H_{i_{n-k}}$ of g. We recall that for any point ν from Γ the chosen coordinates $Y_1, \ldots, Y_{n-k}$ vanish at ν, herewith $H_{i_1}, \ldots, H_{i_{n-k}}$ are the coordinate hyperplanes for $Y_1, \ldots, Y_{n-k}$. We have an expansion $\overline{g} = g_s + g_{s+1} + \cdots + g_{s_1}$, where the polynomial $g_j \in F[Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}]$, $s \le j \le s_1$ is homogeneous of degree j with respect to the variables $Y_1, \ldots, Y_{n-k}$, and $g_s \not\equiv 0$. Let $Y_{\ell_1}, \ldots, Y_{\ell_p}$, $p \ge \eta(n-k)$ occur in $lm(g_s) = \alpha Z_1^{m'_1} \cdots Z_k^{m'_k} Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$. We remind that $m_1, \ldots, m_{n-k}$ do not depend on the coordinates $Z_1, \ldots, Z_k$, thereby on a particular point ν from Γ; also $g_s^{(n-k)} \in F[Z_1, \ldots, Z_k]$ is the coefficient at $Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$ of the expansion of g_s, herewith $lm(g_s^{(n-k)}) = \alpha Z_1^{m'_1} \cdots Z_k^{m'_k}$.

For the sake of simplifying the notations, we make a linear transformation of the coordinates $X_1, \ldots, X_n$ into $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$ and the same linear transformation we apply also to the coordinates $V_1, \ldots, V_n$ (keeping for them the same notation). Then in the new coordinates $G = \{(z_1, \ldots, z_k, y_1, \ldots, y_{n-k}, v_1, \ldots, v_n) : v_i = \frac{\partial \overline{g}}{\partial Z_i}(z_1, \ldots, z_k, y_1, \ldots, y_{n-k})$, $1 \le i \le k$; $v_{j+k} = \frac{\partial \overline{g}}{\partial Y_j}(z_1, \ldots, z_k, y_1, \ldots, y_{n-k})$, $1 \le j \le n-k\}$ and ψ is given by the same formulae $W_{i\ell} = Z_iV_\ell$, $W_{j+k,\ell} = Y_jV_\ell$, $W_\ell = V_\ell$ as above.

For a fixed point $\nu = (z_1, \ldots, z_k, 0, \ldots, 0) \in \Gamma$ consider $(n-1)$-dimensional plane $\mathcal{P} = \mathcal{P}_\nu = \psi(\varphi^{-1}(\nu)) \subset \mathbb{P}^{n^2+n-1}$. The following lemma is similar to lemma 1 [8].

Lemma 2 *It holds* $\dim(\sigma(\overline{\psi(G)} \cap \mathcal{P})) \ge \eta(n-k) - 1$. *Moreover, the linear (coordinate) functions* $W_{\ell_1}, \ldots, W_{\ell_p}$ *are algebraically independent on* $\overline{\psi(G)} \cap \mathcal{P}$.

Proof. Take a point $(z_1, \ldots, z_k, y_1, \ldots, y_{n-k}) \in F^n$ and consider a line $\{t_\lambda = (z_1, \ldots, z_k, \lambda y_1, \ldots, \lambda y_{n-k})\}_{\lambda \in F} \subset F^n$. Then $\frac{\partial \overline{g}}{\partial Y_\ell}(t_\lambda) = \left(\frac{\partial g_s}{\partial Y_\ell} + \frac{\partial g_{s+1}}{\partial Y_\ell} + \cdots + \frac{\partial g_{s_1}}{\partial Y_\ell}\right)(t_\lambda) = \lambda^{s-1}(\frac{\partial g_s}{\partial Y_\ell}(z_1, \ldots, z_k, y_1, \ldots, y_{n-k}) + \lambda \widetilde{g}^{(\ell)})$, where

$\widetilde{g}^{(\ell)} \in F[\lambda, z_1, \dots, z_k, y_1, \dots, y_{n-k}]$, $1 \le \ell \le n-k$. Similar, $\frac{\partial \overline{g}}{\partial Z_i}(t_\lambda) = \lambda^s \widehat{g}^{(i)}$, where $\widehat{g}^{(i)} \in F[\lambda, z_1, \dots, z_k, y_1, \dots, y_{n-k}]$. Denote $\mathrm{grad} = (\frac{\partial \overline{g}}{\partial Z_1}, \dots, \frac{\partial \overline{g}}{\partial Z_k}, \frac{\partial \overline{g}}{\partial Y_1}, \dots, \frac{\partial \overline{g}}{\partial Y_{n-k}})$.

Hence the point

$$\psi(t_\lambda, \mathrm{grad}(t_\lambda)) = \lambda^{s-1}(\dots : \frac{\partial g_s}{\partial Y_\ell}(z_1, \dots, z_k, y_1, \dots, y_{n-k}) + \lambda \widetilde{g}^{(\ell)} : \dots) \in \psi(G) \cap \mathcal{P}_{t_\lambda}$$

(provided that the point of the projective space is defined, i.e. $\mathrm{grad}(t_\lambda) \neq 0$). Divide all the coordinates of this point over their common factor λ^{s-1} and after that plug $\lambda = 0$. Then the resulting point $(\dots : \frac{\partial g_s}{\partial Y_\ell}(z_1, \dots, z_k, y_1, \dots, y_{n-k}) : \dots) \in \overline{\psi(G)} \cap \mathcal{P}_\nu$ (provided that not all $\frac{\partial g_s}{\partial Y_\ell}(z_1, \dots, z_k, y_1, \dots, y_{n-k})$ vanish).

For each $1 \le j \le \rho$ the leading term of the polynomial $\frac{\partial g_s}{\partial Y_{\ell_j}}(z_1, \dots, z_k, Y_1, \dots, Y_{n-k})$ equals to $g_s^{(n-k)}(z_1, \dots, z_k) m_{\ell_j} Y_1^{m_1} \cdots Y_{\ell_j - 1}^{m_{\ell_j - 1}} Y_{\ell_j}^{m_{\ell_j} - 1} Y_{\ell_j + 1}^{m_{\ell_j + 1}} \cdots Y_{n-k}^{m_{n-k}}$, provided that $g_s^{(n-k)}(z_1, \dots, z_k) \neq 0$ (recall that $m_{\ell_j} \ge 1$).

First we establish lemma 2 in case $\rho = 1$, then it suffices to verify that $\overline{\psi(G)} \cap \mathcal{P}_\nu \neq \emptyset$ because $\rho \ge \eta(n-k)$. Moreover, we prove that for any point $w_0 \in F^n$ we have $\overline{\psi(G)} \cap \mathcal{P}_{w_0} \neq \emptyset$. Indeed, take any point $w_1 \in F^n$ for which the gradient $\mathrm{grad}(w_1) \neq 0$. Then grad does not vanish almost everywhere on the line $\{w_\lambda = w_0 + \lambda(w_1 - w_0)\}_{\lambda \in F}$. Since (cf. above) the point $\psi(w_\lambda, \mathrm{grad}(w_\lambda)) \in \psi(G) \cap \mathcal{P}_{w_\lambda}$, provided that $\mathrm{grad}(w_\lambda) \neq 0$, we conclude that the limit of these points when $\lambda \to 0$, belongs to $\overline{\psi(G)} \cap \mathcal{P}_{w_0}$, which is thereby, nonempty.

Now let $\rho \ge 2$. If the statement of the lemma were wrong, there would exist a homogeneous polynomial $h = \sum_K h_K W_{\ell_1}^{K_1} \cdots W_{\ell_\rho}^{K_\rho} \in F[W_{\ell_1}, \dots, W_{\ell_\rho}]$ vanishing on $\overline{\psi(G)} \cap \mathcal{P}_\nu$ (or by the same token on $\sigma(\overline{\psi(G)} \cap \mathcal{P}_\nu)$). Therefore, $h(\frac{\partial g_s}{\partial Y_{\ell_1}}(z_1, \dots, z_k, Y_1, \dots, Y_{n-k}), \dots, \frac{\partial g_s}{\partial Y_{\ell_\rho}}(z_1, \dots, z_k, Y_1, \dots, Y_{n-k})) = 0$. Denote $Y^M = Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$. The leading monomial of the product $(\frac{\partial g_s}{\partial Y_{\ell_1}}(z_1, \dots, z_k, Y_1, \dots, Y_{n-k}))^{K_1} \cdots (\frac{\partial g_s}{\partial Y_{\ell_\rho}}(z_1, \dots, z_k, Y_1, \dots, Y_{n-k}))^{K_\rho}$ equals to $\left(\frac{Y^M}{Y_{\ell_1}}\right)^{K_1} \cdots \left(\frac{Y^M}{Y_{\ell_\rho}}\right)^{K_\rho}$.

For any two distinct integer multiindices $(K_1, \dots, K_\rho) \neq (Q_1, \dots, Q_\rho)$ we have $\left(\frac{Y^M}{Y_{\ell_1}}\right)^{K_1} \cdots \left(\frac{Y^M}{Y_{\ell_\rho}}\right)^{K_\rho} \neq \left(\frac{Y^M}{Y_{\ell_1}}\right)^{Q_1} \cdots \left(\frac{Y^M}{Y_{\ell_\rho}}\right)^{Q_\rho}$. Indeed, otherwise

$\left(\frac{Y^M}{Y_{\ell_1}}\right)^{K_1-Q_1}\cdots\left(\frac{Y^M}{Y_{\ell_\rho}}\right)^{K_\rho-Q_\rho}=1$, i.e. $Y^{M(K_1-Q_1+\cdots+K_\rho-Q_\rho)}=Y_{\ell_1}^{K_1-Q_1}\ldots Y_{\ell_\rho}^{K_\rho-Q_\rho}$, therefore the multiindices $(K_1-Q_1,\ldots,K_\rho-Q_\rho)=(K_1-Q_1+\cdots+K_\rho-Q_\rho)(m_{\ell_1},\ldots,m_{\ell_\rho})$ coincide, in particular, $K_1-Q_1+\cdots+K_\rho-Q_\rho\neq 0$, but the sums of the coordinates in both multiindices differ by the factor of $m_{\ell_1}+\cdots+m_{\ell_\rho}\geq\rho\geq 2$.

The obtained contradiction proves lemma 2 for the points $\nu=(z_1,\ldots,z_k,0,\ldots,0)$ such that $g_s^{(n-k)}(z_1,\ldots,z_k)\neq 0$. Now observe that for any point $u\in\mathbb{P}^{n^2+n-1}$ the set $\varphi(\psi^{-1}(u))$ consists of a single point when $u\in\psi(F^{2n})$ or else is empty. Thus, $\varphi\psi^{-1}:\overline{\psi(F^{2n})}\to F^n$ is a rational surjective map [25]. Finally, applying the theorem on dimension of fibers [25] to the restriction of the rational map $\varphi\psi^{-1}:\overline{\psi(G)}\cap(\varphi\psi^{-1})^{-1}\Gamma\to\Gamma$ being surjective as was shown above, we complete the proof of lemma 2. $\square$

Now we come back to the proof of lemma 1. Observe that $\overline{\psi(G)}\cap\mathcal{P}\subset\mathbb{P}^{n^2+n-1}$ (where $\mathcal{P}=\mathcal{P}_\nu$ for an arbitrary point $\nu\in\Gamma$, see above) is a closed projective variety and the projection σ is defined everywhere on this variety, so being a regular map, hence $\sigma(\overline{\psi(G)}\cap\mathcal{P})\subset\mathbb{P}^{n-1}$ is a closed projective variety (see [25], [23]).

There exists a subspace $B\subset\mathbb{P}^{n-1}$ with the dimension $\dim B=\lfloor n-\eta(n-k)\rfloor$ such that $\dim(\overline{\psi(G)}\cap\sigma^{-1}(B))\leq n-\eta(n-k)+1$ (actually, almost any subspace satisfies this property). This follows from the theorem of dimension of fibres [23] applying it to the rational dominating map $\sigma:\overline{\psi(G)}\to\overline{\sigma(\overline{\psi(G)})}$ and taking into account that $\dim\overline{\psi(G)}=\dim G=n$.

Since the intersection of two closed projective varieties of the complement dimensions (see lemma 2) $B\cap\sigma(\overline{\psi(G)}\cap\mathcal{P})$ is not empty [25], [23], we conclude that $\sigma^{-1}(B)\cap\overline{\psi(G)}\cap\mathcal{P}\neq\emptyset$, for any point ν from any strongly singular k-face Γ. Varying $\mathcal{P}=\mathcal{P}_\nu$ for different points ν from Γ, the latter implies in particular, that $\dim(\sigma^{-1}(B)\cap\overline{\psi(G)})\geq k$.

Therefore, the constructible set $U=\varphi(\psi^{-1}(\sigma^{-1}(B)\cap\overline{\psi(G)}))\subset F^n$ contains all strongly singular k-faces Γ. Observe that $\dim U\leq\dim(\sigma^{-1}(B)\cap\overline{\psi(G)})\leq n-\eta(n-k)+1$ since $\varphi\psi^{-1}$ is a rational map (cf. above).

For each strongly singular k-face $\Gamma=H_{i_1}\cap\cdots\cap H_{i_{n-k}}$ successively choose $j_1,j_2,\ldots\in\{i_1,\ldots,i_{n-k}\}$, such that for every $\ell\geq 0$ we have $\dim(U\cap H_{j_1}\cap\cdots\cap H_{j_\ell}\cap H_{j_{\ell+1}})\leq\dim(U\cap H_{j_1}\cap\cdots\cap H_{j_\ell})-1$ while $\dim(U\cap H_{j_1}\cdots\cap H_{j_\ell})>k$. After at most $q\leq n-\eta(n-k)+1-k$ steps we reach $j_1,\ldots,j_q$ for which $\dim(U\cap H_{j_1}\cap\cdots\cap H_{j_q})=k$, thus Γ is an irreducible component of

$U \cap H_{j_1} \cap \cdots \cap H_{j_q}$. Take also a $(n-k)$-dimensional plane $Q \subset F^n$ transversal to all k_1-faces of S for all $0 \le k_1 \le n$ and to all irreducible components of $U \cap H_{j_1} \cap \ldots \cap H_{j_q}$ for all $j_1, \ldots, j_q$. Then the point $Q \cap \Gamma$, being an irreducible component of 0-dimensional variety $U \cap H_{j_1} \cap \cdots \cap H_{j_q} \cap Q$, does not belong to other k-faces except Γ.

Consider constructible sets $\mathcal{H}_i = \psi(\varphi^{-1}(H_i))$, $\mathcal{Q} = \psi(\varphi^{-1}(Q)) \subset \mathbb{P}^{n^2+n-1}$, $1 \le i \le m$. Consider also

$$\mathcal{U} = \mathcal{U}_{j_1,\ldots j_q} = \sigma^{-1}(B) \cap \overline{\psi(G)} \cap \mathcal{H}_{j_1} \cap \cdots \cap \mathcal{H}_{j_q} \cap \mathcal{Q}. \tag{2}$$

Then $\varphi(\psi^{-1}(\mathcal{U})) = U \cap H_{j_1} \cap \cdots \cap H_{j_q} \cap Q = \{u_1, \ldots, u_\kappa\} \subset F^n$ is a finite collection of points. Therefore, every irreducible component of $\mathcal{U}$ is contained in one of the pairwise disjoint $(n-1)$-dimensional planes $\psi(\varphi^{-1}(u_1)), \ldots, \psi(\varphi^{-1}(u_\kappa)) \subset \mathbb{P}^{n^2+n-1}$, since the image of this irreducible component under the rational map $\varphi\psi^{-1} : \overline{\psi(F^{2n})} \to F^n$, being a subset of $\{u_1, \ldots, u_\kappa\}$, should be a point; moreover each of these planes contains a certain component of $\mathcal{U}$.

Thus, $\deg(\mathcal{U}) = \deg(\mathcal{U}_{j_1,\ldots,j_q}) \ge \kappa$; we define the degree of a constructible set as the degree of its projective closure $\overline{\mathcal{U}}$ [23], [25], i.e. the sum of the degrees of irreducible components of $\overline{\mathcal{U}}$.

Taking the sum of the latter inequalities over all $1 \le j_1, \ldots, j_q \le m$, $q \le (n-k)(1-\eta)+1$ and observing that each strongly singular k-face Γ gives a contribution into the right side of one of these inequalities, we conclude that

$$\sum_{1 \le j_1,\ldots,j_q \le m; q \le (n-k)(1-\eta)+1} \deg(\mathcal{U}_{j_1,\ldots,j_q}) \ge N \tag{3}$$

Another method for bounding from below the degree of a variety passing through a given set of points one can find in [28], but this method is not applicable here. To bound $\deg(\mathcal{U}_{j_1,\ldots,j_q})$ from above, we rely on the following lemma.

Lemma 3 *Let an affine Zariski closed set $\mathcal{V} \subset F^{2n}$. Then $deg(\psi(\mathcal{V})) \le 2^{2n} deg(\mathcal{V})$.*

Proof. (cf. the proof of theorem 1 [8]). First, one can reduce lemma to the case of an irreducible $\mathcal{V}$. Since $\dim(\overline{\psi(\mathcal{V})} - \psi(\mathcal{V})) < \dim(\psi(\mathcal{V}))$, there is a subspace $R \subset \mathbb{P}^{n^2+n-1}$ with $\dim R = n^2 + n - 1 - \dim \psi(\mathcal{V})$ for which

$R \cap \psi(\mathcal{V})$ consists of $\deg \psi(\mathcal{V}) = \deg \overline{\psi(\mathcal{V})}$ points (in fact, almost any subspace has $\deg \psi(\mathcal{V})$ common points with $\overline{\psi(\mathcal{V})}$, and almost any subspace has an empty intersection with $\overline{\psi(\mathcal{V})} - \psi(\mathcal{V})$). Because $\psi(\psi^{-1}(R) \cap \mathcal{V}) = R \cap \psi(\mathcal{V})$, the degree $\deg \psi(\mathcal{V})$ does not exceed the number of irreducible components of the variety $\psi^{-1}(R) \cap \mathcal{V}$, which in its turn is less or equal to $\deg(\psi^{-1}(R) \cap \mathcal{V})$. Then we apply the Bezout inequality $\deg(\psi^{-1}(R) \cap \mathcal{V}) \leq \deg(\psi^{-1}(R)) \cdot \deg \mathcal{V}$ which was proved for locally closed sets in [17], rather than for the usual case of projective closed varieties with the complete intersection [23], [25]. The local closedness of $\psi^{-1}(R)$ follows from the next paragraph.

It remains to bound $\deg(\psi^{-1}(R))$. If R is determined by several linear equations of the form $\sum_{1 \leq i, \ell \leq n} \alpha_{i\ell} W_{i\ell} + \sum_{1 \leq \ell \leq n} \beta_\ell W_\ell = 0$, then $\psi^{-1}(R)$ is determined by the quadratic equations $\sum_{1 \leq i, \ell \leq n} \alpha_{i\ell} X_i V_\ell + \sum_{1 \leq \ell \leq n} \beta_\ell V_\ell = 0$ out of the plane $L = \{V_1 = \cdots = V_n = 0\}$ on which ψ is not defined. One can choose $2n$ suitable linear combination of these equations $\zeta_1, \ldots, \zeta_{2n} \in F[X_1, \ldots, X_n, V_1, \ldots, V_n]$ such that the irreducible components of the locally closed set $\{\zeta_1 = \cdots = \zeta_{2n} = 0\} - L \subset F^{2n}$ contain all the irreducible components of $\psi^{-1}(R)$ and in addition, perhaps, few points, being its 0-dimensional components (cf. also [6]). Hence $\deg(\psi^{-1}(R)) \leq 2^{2n}$ again due to the Bezout inequality. This completes the proof of lemma 3.

Coming back to bounding $\deg(\mathcal{U}_{j_1, \ldots, j_q})$ from above, we note that $\mathcal{H}_{j_1} \cap \cdots \cap \mathcal{H}_{j_q} \cap \mathcal{Q} = \psi(\varphi^{-1}(H_{j_1} \cap \cdots \cap H_{j_q} \cap Q))$ (cf. (2)) and $\mathcal{H} = \varphi^{-1}(H_{j_1} \cap \cdots \cap H_{j_q} \cap Q) \subset F^{2n}$ being a plane, so of degree 1. Applying lemma 3 we obtain the bound

$$\deg(\psi(\mathcal{H})) \leq 2^{2n}. \tag{4}$$

For every $1 \leq i \leq n$ consider a principle affine Zariski open chart $\mathcal{A}_\ell = \{W_\ell \neq 0\} \subset \mathbb{P}^{n^2+n-1}$ and denote $\mathcal{A} = \cup_{1 \leq \ell \leq n} \mathcal{A}_\ell$. Observe that $\sigma^{-1}(B) \subset \mathcal{A}$ is closed in $\mathcal{A}$.

Let us also show that $\mathcal{H}_{j_1} \cap \cdots \cap \mathcal{H}_{j_q} \cap \mathcal{Q} = \psi(\mathcal{H}) \subset \psi(F^{2n}) \subset \mathcal{A}$ is closed in $\mathcal{A}$. Indeed, $\mathcal{H}$ is given by a system of linear equations $\{h_t = \sum_{1 \leq i \leq n} \gamma_{ti} X_i + \gamma_{t0} = 0\}_t$ which depend only on $X_1, \ldots, X_n$. We claim that $\psi(\mathcal{H}) =$

$$\mathcal{A} \cap \left\{ \sum_{1 \leq i \leq n} \gamma_{ti} W_{i\ell} + \gamma_{t0} W_\ell = 0 \right\}_{t, 1 \leq \ell \leq n} \cap \{W_{i\ell_1} W_{\ell_2} = W_{i\ell_2} W_{\ell_1}\}_{1 \leq i, \ell_1, \ell_2 \leq n}$$

The inclusion $\subset$ is obvious. To prove the inverse inclusion take a point $\{w_{i\ell}\}_{i,\ell} : \{w_\ell\}_\ell$ from the set at the right side. Then $w_{\ell_0} \neq 0$ for a cer-

tain $1 \leq \ell_0 \leq n$. From the equalities $w_{i\ell_1}w_{\ell_2} = w_{i\ell_2}w_{\ell_1}$ we get that $\{w_{i\ell}\}_{i,\ell} : \{w_\ell\}_\ell = \psi\left(\frac{w_{1\ell_0}}{w_{\ell_0}}, \cdots, \frac{w_{n\ell_0}}{w_{\ell_0}}, w_1, \ldots, w_n\right)$. Finally, the equalities $\left\{\sum_{1\leq i\leq n}\gamma_{ti}w_{i\ell_0} + \gamma_{t0}w_{\ell_0} = 0\right\}_t$ entail that $\left(\frac{w_{1\ell_0}}{w_{\ell_0}}, \cdots, \frac{w_{n\ell_0}}{w_{\ell_0}}, w_1, \ldots, w_n\right) \in \mathcal{H}$, which proves the inverse inclusion of the claim and thereby the closedness of $\psi(\mathcal{H})$ in $\mathcal{A}$.

Let $\mathcal{U} = \sigma^{-1}(B)\cap\overline{\psi(G)}\cap\psi(\mathcal{H}) = \cup_j\mathcal{U}_j \subset \mathcal{A}$ (cf. (2)) be the decomposition of $\mathcal{U}$, being the intersection of three Zariski closed in $\mathcal{A}$ subsets as was just proved, into its irreducible components $\mathcal{U}_j$. For every $1 \leq i \leq n$ we have the induced decomposition of the intersection

$$(\sigma^{-1}(B) \cap \mathcal{A}_i) \cap (\overline{\psi(G)} \cap \mathcal{A}_i) \cap (\psi(\mathcal{H}) \cap \mathcal{A}_i) = \cup_j(\mathcal{U}_j \cap \mathcal{A}_i)$$

of three Zariski closed affine sets (in $\mathcal{A}_i$) into its irreducible components $\mathcal{U}_j \cap \mathcal{A}_i$, provided that $\mathcal{U}_j \cap \mathcal{A}_i \neq \emptyset$. Moreover, in the latter case the closure $\overline{\mathcal{U}_j \cap \mathcal{A}_i} = \overline{\mathcal{U}_j} \subset \mathbb{P}^{n^2+n-1}$ because $\mathcal{A}_i$ is open in $\mathbb{P}^{n^2+n-1}$, in particular $\deg(\mathcal{U}_j \cap \mathcal{A}_i) = \deg\mathcal{U}_j$. Applying the affine version of the Bezout inequality [17], we obtain

$$\begin{aligned}\sum_j \deg\mathcal{U}_j &\leq \deg(\sigma^{-1}(B) \cap \mathcal{A}_i)\deg(\overline{\psi(G)} \cap \mathcal{A}_i).\\ \deg(\psi(\mathcal{H}) \cap \mathcal{A}_i) &\leq \deg\overline{\psi(G)} \cdot \deg\psi(\mathcal{H})\end{aligned}$$

where the summation ranges over j for which $\mathcal{U}_j \cap \mathcal{A}_i \neq \emptyset$. Summing up these inequalities for all $1 \leq i \leq n$, we conclude

$$\deg\mathcal{U} = \sum_j \deg\mathcal{U}_j \leq n \cdot \deg\overline{\psi(G)} \cdot \deg\psi(\mathcal{H})$$

which together with the bounds (3), (4) gives the inequality

$$N \leq \left(\begin{array}{c} m \\ \lfloor(n-k)(1-\eta)\rfloor + 1 \end{array}\right) \cdot (n-k)(1-\eta)n \cdot \deg\overline{\psi(G)} \cdot 2^{2n},$$

hence taking into account the inequality $\deg\overline{\psi(G)} \leq 2^{2n}\deg G$ following from lemma 3, we finally get

$$\deg G \geq \Omega\left(\frac{N}{m^{(n-k)(1-\eta)}2^{4n}}\right),$$

that completes the proof of lemma 1.

Corollary. (cf. corollary 1 [8]). *Let a polynomial $g \in F[X_1, \ldots, X_n]$ have N strongly singular k-faces in an arrangement $H_1 \cup \cdots \cup H_m \subset F^n$. Then the multiplicative complexity $C(g) \geq 1/3(\log N - (n-k)(1-\eta)\log m - 4n - const)$.*

The results from [27], [1] imply that $\deg G \leq 2^{3C(g)}$, then make use of lemma 1.

3 Lower bound for randomized computation trees

Recall (see e.g. [2]) that in the computation tree (CT) testing polynomials are computed along paths using the elementary arithmetic operations. In particular, for a testing polynomial $f_i \in \mathbb{R}[X_1, \ldots, X_n]$ at the level i (assuming that the root has the zero level) we have the obvious bound on its complexity, a fortiori multiplicative complexity $C(f_i) \leq i$. Under RCT (cf. [24], [20]) we mean a collection of CT $T = \{T_\alpha\}$ and a probabilistic vector $p_\alpha \geq 0$, $\sum_\alpha p_\alpha = 1$ such that CT T_α is chosen with the probability p_α. The depth of an RCT (treated as its complexity) is defined as the maximum of the depths of all T_α's (actually the equivalent complexity classes one gets if to define the depth of RCT as the expectation of the depths of T_α's, [24]). 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 $\{L_H \geq 0\}$, where L_H is a certain linear function with the zero set H. For a family of hyperplanes $H_1, \ldots, H_m$ the intersection $S^+ = \cap_{1 \leq i \leq m} H_i^+$ is called a polyhedron. An intersection $\Gamma = H_{i_1} \cap \cdots \cap H_{i_{n-k}}$ is called k-face of S^+ if for each $1 \leq l \leq n-k+1$ we have $\dim(H_{i_l} \cap \cdots \cap H_{i_{n-k}}) = \dim(H_{i_l} \cap \cdots \cap H_{i_{n-k}} \cap S^+) = k+l-1$ (then clearly $H_{i_l} \cap \cdots \cap H_{i_{n-k}}$ is $(k+l-1)$-face of S^+). Recall (see section 1) that Γ is k-face of the arrangement $S = \cup_{1 \leq i \leq m} H_i$ if $\dim \Gamma = k$.

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

Theorem. *For any positive constants c, c_1, c_2 there exists $c_0 > 0$ satisfying the following. Let for some $k \leq (1-c_1)n$ an arrangement $\mathcal{S} = S = \cup_{1 \leq i \leq m} H_i$ or a polyhedron $\mathcal{S} = S^+ = \cap_{1 \leq i \leq m} H_i^+$ have at least $c_2(m^{c(n-k)})$ k-*

faces. Then for any RCT recognizing $\mathcal{S}$, its depth is greater than $c_0(n \log m)$.

For a family of polynomials $f_1, \ldots, f_t \in \mathbb{R}[X_1, \ldots, X_n]$ we define $\mathrm{Var}^{(\Gamma)}(f_1, \ldots, f_t)$ to be the number of the variables among $Y_1, \ldots, Y_{n-k}$ (we utilize the notations introduced in section 1) which occur in at least one of the leading terms $lm(f_{1,s_1}), \ldots, lm(f_{t,s_t})$, where $H_{i_1}, \ldots, H_{i_{n-k}}$ are the coordinate hyperplanes of the coordinates $Y_1, \ldots, Y_{n-k}$, respectively; $\overline{f}_j(Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}) = f_j(X_1, \ldots, X_n)$ and $\overline{f}_j = f_{j,s_j} + f_{j,s_j+1} + \cdots$, herewith $f_{j,l}$ is homogeneous with respect to the variables $Y_1, \ldots, Y_{n-k}$ of degree l and $f_{j,s_j} \not\equiv 0$, $1 \leq j \leq t$. Because the expansion into the homogeneous components $\overline{f}_1 \cdots \overline{f}_t = (f_{1,s_1} \cdots f_{t,s_t}) + \cdots$ starts with $f_{1,s_1} \cdots f_{t,s_t}$, we have $lm(f_{1,s_1} \cdots f_{t,s_t}) = lm(f_{1,s_1}) \cdots lm(f_{t,s_t})$ and hence $\mathrm{Var}^{(H_{i_1}, \ldots, H_{i_{n-k}})}(f_1 \cdots f_t) = \mathrm{Var}^{(\Gamma)}(f_1 \cdots f_t) = \mathrm{Var}^{(\Gamma)}(f_1, \cdots, f_t)$.

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

The following lemma is similar to lemma 1 [13], [11], but differs from it due to the different definition of the leading term lm.

Lemma 4 *Let $T = \{T_\alpha\}$ be an RCT recognizing*

a) an arrangement $S = \cup_{1 \leq i \leq m} H_i$ such that $\Gamma = H_{i_1} \cap \cdots \cap H_{i_{n-k}}$ 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^+ (so, see above, for each $1 \leq l \leq n-k+1$ we have $\dim(\cap_{l \leq j \leq n-k} H_{i_j}) = \dim(\cap_{l \leq j \leq n-k} H_{i_j} \cap S^+) = k + l - 1$)

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

Proof of Lemma 4: Choose the coordinates $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$ such that $Z_1, \ldots, Z_k$ are the coordinates in Γ and $H_{i_1}, \ldots, H_{i_{n-k}}$ are the coordinate hyperplanes of $Y_1, \ldots, Y_{n-k}$, respectively (cf. section 1), which satisfy the following properties. The origin $\underbrace{(0, \ldots, 0)}_{n}$ of this coordinates system $Z_1, \ldots, Z_k, Y_1, \ldots, Y_{n-k}$ does not lie in any l-face with $l < k$ and besides, in the case b) $(0, \ldots, 0)$ belongs to the polyhedron S^+. Also we require that for any testing polynomial f from any CT T_α the inequality $f_s^{(n-k)} \underbrace{(0, \ldots, 0)}_{k} \neq 0$ holds (recall that $f_s^{(n-k)} \not\equiv 0$ depends only on

$H_{i_1}, \ldots, H_{i_{n-k}}$ and $f = f_s + f_{s+1} + \cdots$ where f_j is homogeneous with respect to the variables $Y_1, \ldots, Y_{n-k}$ of degree j, see section 1).

Observe that RCT T treated over the field $\mathbb{R}_{n+1}$ recognizes the completion $S^{(\mathbb{R}_{n+1})} \subset (\mathbb{R}_{n+1})^n$ (respectively, $S^{+(\mathbb{R}_{n+1})}$) due to the Tarski transfer principle (see section 1). For the sake of simplicity of the notations we keep the notations S (respectively, S^+) for the completions.

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

We show 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 $E_i^{(0)}$, $1 \leq i \leq n-k$. Indeed, assuming the contrary we partition all T_α's into three (disjoint) pieces. In the first one the output for E is incorrect (its fraction is at most γ). In the second one (which is desirable for our goal) the fraction of correct outputs for $E_i^{(0)}, 1 \leq i \leq n-k$ is at least $(1-2\gamma)^2$ (its fraction is at most $\frac{1-2\gamma}{2(1-\gamma)}$ by the assumption). The rest of T_α's comprise the third piece. Thus, the total fraction of correct outputs for all $E_i^{(0)}, 1 \leq i \leq n-k$ together does not exceed $(\gamma + \frac{1-2\gamma}{2(1-\gamma)}) + (1-2\gamma)^2(1-\gamma-\frac{1-2\gamma}{2(1-\gamma)}) = 1-2\gamma+4\gamma^2-4\gamma^3 < 1-\gamma$, that contradicts to the requirement on the error probability γ.

Take such T_{α_0} and some $1 \leq i_0 \leq n-k$ for which T_{α_0} gives the correct output. Denote by $f_1, \ldots, f_t$ 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 $lm(f_{1,s_1}), \ldots, lm(f_{t,s_t})$ (thereby, Y_{i_0} occurs in $lm(f_{1,s_1} \ldots f_{t,s_t}) = lm(f_{1,s_1}) \ldots lm(f_{t,s_t})$, see above).

Suppose the contrary. Let $lm(f_{l,s_l}) = \beta Z_1^{m'_1} \cdots Z_k^{m'_k} Y_1^{m_1} \cdots Y_{n-k}^{m_{n-k}}$, then $m_{i_0} = 0$ for each $1 \leq l \leq t$ by the supposition. Then (1) from section 1 implies that $sgn(\overline{f_l}(E_{i_0}^{(0)})) = sgn(f_{l,s_l}^{(n-k)}\underbrace{(0, \ldots, 0)}_{k}) \neq 0$ 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 $sgn(\overline{f_l}(E)) = sgn(f_{l,s_l}^{(n-k)}\underbrace{(0, \ldots, 0)}_{k})$. 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 $H_l = \{\kappa_1 Z_1 + \ldots + \kappa_k Z_k + \beta_1 Y_1 + \ldots + \beta_{n-k} Y_{n-k} + \beta_0 = 0\}$, $1 \le l \le m$ given by linear function L_{H_l} with the coefficients $\kappa_i, \beta_j \in \mathbb{R}$. We need to show that $L_{H_l}(E) \ge 0$. Let $0 \le j_0 \le n-k$ be the uniquely defined index such that $\beta_0 = \ldots = \beta_{j_0-1} = 0$, $\beta_{j_0} \ne 0$ (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 $sgn(L_{H_l}(E)) = sgn(\beta_{j_0}) > 0$. Because $\dim(H_{i_{n-k}} \cap \cdots \cap H_{i_{j_0+1}} \cap S^+) = k + j_0$ and $\dim(H_{i_{n-k}} \cap \cdots \cap H_{i_{j_0+1}} \cap H_{i_{j_0}}) = k + j_0 - 1$ (see the beginning of this section), there exists a point $v_{n-j_0} \in (H_{i_{n-k}} \cap \cdots \cap H_{i_{j_0+1}} \cap S^+) - H_{i_{j_0}}$, notice that in the chosen coordinate system $v_{n-j_0} = (\underbrace{0, \ldots, 0}_{k}, y_1^{(n-j_0)}, \ldots, y_{j_0}^{(n-j_0)}, 0, \ldots, 0)$. Then $y_{j_0}^{(n-j_0)} \ne 0$, 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 $E_i^{(+)} = (\underbrace{0, \ldots, 0}_{k}, \varepsilon_{k+1}\varepsilon_{n+1}, \ldots, \varepsilon_{k+i-1}\varepsilon_{n+1},$ $-\varepsilon_{k+i}\varepsilon_{n+1}, \varepsilon_{k+i+1}\varepsilon_{n+1}, \ldots, \varepsilon_n\varepsilon_{n+1}) \notin S^+$, $1 \le i \le n-k$.

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 $sgn(\overline{f_l}(E_{i_0}^{(+)})) = sgn(f_{l,s_l}^{(n-k)}(\underbrace{0, \ldots, 0}_{k})) = sgn(\overline{f_l}(E)) \ne 0$ again because of (1) from section 1.

Lemma 4 is proved.

An analogue of lemma 2 from [13], [11] is the following lemma.

Lemma 5 *For any positive constants c, c_1, c_2, c_3 there exists $c_4 > 0$ satisfying the following. Let $\mathcal{S} = S$ or $\mathcal{S} = S^+$ fulfill the conditions of the theorem. Assume that CT T' for some constant $\eta > 1 - c$, satisfies the inequality $Var^{(\Gamma)}(T') \ge \eta(n-k)$ for at least $M \ge c_3(m^{c(n-k)})$ of k-faces Γ of $\mathcal{S}$. Then the depth t of T' is greater than $c_4(n \log m)$.*

The proof of lemma 5 differs from the proof of the analogous lemma 2 from [13] 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. Also it differs from the proof of lemma 2 [11] where the main tool was the lower bound on the border complexity. Here the

proof of lemma 5 is much easier than in [13], [11] and relies on the corollary (see section 2) in which the multiplicative complexity of a polynomial is bounded from below in terms of the number of strongly singular faces of an arrangement.

Before proving lemma 5 we show how to deduce the theorem from lemmas 4 and 5. Consider RCT $\{T_\alpha\}$ recognizing $\mathcal{S}$ with error probability $\gamma < \frac{1}{2}$. Lemma 4 and counting imply the existence of T_{α_0} such that the inequality $\mathrm{Var}^{(\Gamma)}(T_{\alpha_0}) \geq (1-2\gamma)^2(n-k)$ is true for $M = \frac{1-2\gamma}{2(1-\gamma)}\Omega(m^{c(n-k)})$ of k-faces Γ of $\mathcal{S}$. Apply lemma 5 to CT $T' = T_{\alpha_0}$ with $\eta = (1-2\gamma)^2$. Since the error probability γ 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 [20], take γ such that $\eta > 1-c$. Then lemma 5 entails that $t \geq \Omega(n \log m)$, which proves the theorem. Thus, it remains to prove lemma 5.

Proof of lemma 5: To each k-face Γ of $\mathcal{S}$ satisfying the inequality $\mathrm{Var}^{(\Gamma)}(T') \geq \eta(n-k)$, we correspond a path in T' with the testing polynomials $f_1, \ldots, f_{t_0} \in \mathbb{R}[X_1, \ldots, X_n], t_0 \leq t$ such that $\mathrm{Var}^{(\Gamma)}(f_1 \cdots f_{t_0}) = \mathrm{Var}^{(\Gamma)}(T')$ (in other words, Γ is strongly singular k-face for $f_1 \cdots f_{t_0}$, see section 1). Denote $f = f_1 \cdots f_{t_0}$

Assume that $3^t \leq O(m^{(\eta-1+c)(n-k)/2})$, otherwise we are done. Then there exists a path of T' (let us keep the notation $f_1, \ldots, f_{t_0}$ 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 Γ for f (because there are most 3^t paths in T'). Corollary from section 2 implies that the multiplicative complexity $C(f) \geq \frac{1}{3}((\eta-1+c)(n-k)\log m - 4n - \mathrm{const})$. Obviously $C(f) \leq t + t_0 - 1 \leq 2t-1$ (cf. the proof of theorem 2 [8]). Hence $t \geq \Omega(n \log m)$ that proves lemma 5.

4 Applications and open problems

As a consequence of the theorem from the previous section we deduce the complexity lower bound $\Omega(n \log n)$ for any RCT, recognizing the DISTINCTNESS problem $\cup_{1 \leq i < j \leq n}\{X_i = X_j\} \subset \mathbb{R}^n$ (for the necessary in the theorem estimation of the number of $\left[\frac{n}{2}\right]$-faces see [13]).

Also we get the lower bound $\Omega(n^2)$ for the KNAPSACK problem $\cup_{I \subset \{1,\ldots,n\}}\{\sum_{i \in I} x_i = 1\}$, this result was already obtained in [11]. It would be interesting to extend the obtained bound to other types of sets, rather than considered in the theorem polyhedra and the unions of hyperplanes.

The linear $O(n)$ complexity RCT from [5] for the SET EQUALITY problem $\{(x_1, \ldots, x_n, y_1, \ldots, y_n) : \{x_1, \ldots, x_n\}$ is a permutation of $\{y_1, \ldots, y_n\}\} \subset \mathbb{R}^{2n}$ provides an evidence that the lower bound from the theorem could not be directly extended even to such quite natural sets like the unions of planes.

Generalizing the construction of [5] we design RCT for recognizing the following set: $\Delta_{n,m}^{(k)} = \{(x_1, \ldots, x_n, y_1, \ldots, y_m)$: each of the both differences of the multisets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ contains at most k elements$\} \subset \mathbb{R}^{n+m}$. Evidently, $k \geq |n - m|$. Denote the polynomials $f(X) = (X - x_1) \cdots (X - x_n)$, $g(X) = (X - y_1) \cdots (X - y_m)$. First compute (deterministically) $f(z_i), g(z_i)$ at $2k + 1$ random points, $0 \leq i \leq 2k$ with the complexity $O(k(n + m))$. Then (deterministically) interpolate the rational function $h = f/g$, being (presumably) a quotient of two monic polynomials both of degrees at most k by means of its values $(f/g)(z_i)$, $1 \leq i \leq 2k$ with the complexity $O(k \log^2 k)$ [3]. Finally, (deterministically) check whether the value of the obtained rational function $h(z_0)$ coincides with $f(z_0)/g(z_0)$. The complexity $O(k(n + m))$ of the designed RCT is better than the complexity $O((n + m) \log(n + m))$ of an obvious CT based on a sorting algorithm when k is small enough.

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] D. Bini, V. Pan, Polynomial and matrix computations, Birkhauser, 1994

[4] A. Bjorner, L. Lovasz, A. Yao, Linear decision trees: volume estimates and topological bounds, Proc. ACM Symp. Th.Comput. 1992, pp. 170–177.

[5] P. Buergisser, M. Karpinski, T. Lickteig, On randomized algebraic test complexity, J. Complexity, Vol. 9, 1993, pp. 231–251.

[6] A. Chistov, D. Grigoriev, Solving systems of algebraic equations in subexponential time I, II, Preprints LOMI E-9-83, E-10-83, Leningrad, 1983

[7] D.Grigoriev, Nearly sharp complexity bounds for multiprocessor algebraic computations, J. Complexity, Vol. 13,1, 1997, pp.50-64

[8] D.Grigoriev, Complexity lower bounds for randomized computation trees over algebraically closed fields, to appear in Computational Complexity

[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, Computational Complexity, 1997, vol. 6, 4, pp. 376–388

[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, 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., Vol. 5, 1988, pp. 37–64

[17] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theor. Comput. Sci., Vol. 24, 1983, pp. 239-277

[18] T. Lickteig, On semialgebraic decision complexity, Preprint TR-0–052 ICSI, Berkeley, 1990.

[19] S. Lang, Algebra, Addison-Wesley, New York, 1965

[20] F. Meyer auf der Heide, Simulating probabilistic by deterministic algebraic computation trees, Theor. Comput. Sci., Vol. 41, 1985, pp. 325–330.

[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, Nondetemrinistic 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 Berechnungskomplexitaet von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten, Numer. Math., Vol. 20, 1973, pp. 238–251.

[28] V. Strassen, Computational complexity over finite fields, SIAM J. Comput. 5, 2, 1976, pp. 324–331

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

[30] A. Yao, Algebraic decision trees and Euler characteristic, Proc. IEEE Symp. Found. Comput. Sci., 1992, pp. 268–277.

[31] A. Yao, Decision tree complexity and Betti numbers, Proc. ACM Symp. Th. Comput., 1994, pp. 615–624.