COMPLEXITY LOWER BOUNDS FOR RANDOMIZED COMPUTATION TREES OVER ZERO CHARACTERISTIC FIELDS

D. Grigoriev

IMR Université Rennes-1
Beaulieu 35042 Rennes France
dima@maths.univ-rennes1.fr

We obtain a nonlinear complexity lower bounds for randomized computation trees with branching signs $\{=, \neq\}$ over zero characteristic fields. As consequences we get $\Omega(n \log n)$ lower bound for the distinctness problem and $\Omega(n^2)$ lower bound for the knapsack problem. For more customary randomized computation trees over reals with branching signs $\{\leq, >\}$ the similar bounds were proved: for the knapsack problem in [GK97] and for the distinctness problem in [G99].

Introduction.

Complexity lower bounds for algebraic decision and computation trees over the reals, where for the branching the signs $\{\leq, >\}$ are involved, were widely studied. In [SY82], [B83] the lower bound $\Omega(\log c - n)$ was obtained for recognizing a semialgebraic set with the number c of connected components in the set or in its complement. Afterwards in [CMP92] the lower bound was strengthened to $\Omega(\log c)$. In [BLY92], [Y92], [BL94] the lower bound $\Omega(\log \chi)$ was proved where χ is the Euler characteristic of the set. Finally, in [Y94], [MMP96] the strongest among these "topological" lower bounds $\Omega(\log b)$ was obtained, where b is the sum of Betti number of the set. For the sets with the trivial topology, like polyhedra, these bounds are not applicable and in [GKV97] the complexity lower bound $\Omega(\log N)$ was proved using a differential-geometric approach, for recognizing a polyhedron with N faces

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

(of all the dimensions). We mention also that for a parallel computation trees model the upper complexity bound $O(\sqrt{\log N \log\log N})$ close to the lower one $\Omega(\sqrt{\log N})$ [Y81], [MP93] was obtained in [G97] for small dimensions.

Another challenging problem which was open for many years, is obtaining complexity lower bounds for the randomized decision and computation algebraic trees. Recall (see e.g. [M85]) that in the randomized models for any input point the answer could be given with the probability of an error at most $\gamma < \frac{1}{2}$. In [GKMS96] a lower bound $\Omega(\log N)$ was proved for randomized *decision* trees recognizing an arrangement (i.e. a union of hyperplanes) or a polyhedron with N faces. This gives as corollaries the lower bound $\Omega(n \log n)$ for the distinctness problem $\cup_{1\leq i<j\leq n}\{X_i = X_j\}$ and the lower bound $\Omega(n^2)$ for the knapsack problem $\underset{I\subset\{1,\dots,n\}}{\cup}\left\{\sum_{i\in I} x_i = 1\right\}$ (both problems are treated as arrangements). In [GK97] the lower bound $\Omega(n^2)$ was proved for the knapsack problem for the more natural model of randomized *computation* trees. In [G99] the lower bound $\Omega(n \log n)$ was ascertained for the distinctness problem for the same model. The basic difference between the decision and computation trees is that in the former one the testing polynomials (usually, of some fixed degree) are given, while in the latter one the testing polynomials are computed along a branch of the tree, thus the degree of testing polynomials could grow exponentially, that provides major difficulties in proving the complexity lower bounds. In [GKS96] the complexity lower bounds were ascertained also for the randomized decision *analytic* tree, in which arbitrary analytic functions could be used as testing ones.

Decision and computation trees over other fields rather than $\mathbb{R}$ are not so well studied (see [S83], also [L90] where the case of recognizing an irreducible hypersurface was treated). In [B94] the trees with the signs $\{=, \neq\}$ in branching instructions over algebraically closed fields of positive characteristic were introduced and the lower bound $\Omega(\log_2 C)$ for recognizing a variety was obtained, where C is the degree of the Zeta-function of the variety. Also it is promised in [B94] to prove the analogue of this bound over the fields of zero characteristic in a future paper.

In the present paper we focus (apparently, for the first time) on the randomized computation trees over fields F of zero characteristic (the results were announced in [G98]). For the problem of recognizing an arrangement $S = \bigcup_{1\leq i\leq m} H_i$, where $H_i \subset F^n$ are hyperplanes, we prove the complexity lower bound $\Omega(\log \widetilde{N})$, here $\widetilde{N}$ is the lower bound for the number of faces in any subarrangement $\bigcup_{1\leq j\leq q} H_{\ell_j}$ of S where $q \geq \alpha m$ for an appropriate constant $\alpha > 0$ (theorem 2). As consequences we obtain the lower bounds $\Omega(n \log n)$ for the distinctness problem (corollary 2) and $\Omega(n^2)$ for the knapsack problem (corollary 3). Notice that a similar problem for obtaining a nonlinear lower bound for the distinctness problem for the randomized computations over the real field still remains open (see [GK97]).

It is interesting to observe that considering arrangements (so the varieties of codimension 1) is essential as shows the example from [BKL93], where a randomized computation tree with the linear complexity $O(n)$ is designed for recognizing the equality set problem $\{(x_1, \ldots, x_n, y_1, \ldots, y_n) \in F^{2n} : (x_1, \ldots, x_n)$ is a permutation of $(y_1, \ldots, y_n)\}$, being not an arrangement, but rather a union of n-dimensional planes in $2n$-dimensional space.

The proof of theorem 2 relies on corollary 1 in which the lower bound $\Omega(\log N)$ is proved on the multiplicative complexity of any function f which vanishes on an arrangement with N faces. In its turn, the proof of the corollary 1 is based on the degree method [S73], on the complexity of computing the gradient [BS83] and on the technical core of the paper, namely theorem 1, in which a lower bound on the degree of the gradient map of f is ascertained in terms of N (over the algebraic closure $\overline{F}$ of F).

Basically, it is shown in the proof of theorem 1 that the limits of the gradients at the points tending to a singular point (namely, to a vertex of the arrangement in n-dimensional space), sweep the whole $(n-1)$-dimensional projective space. The difficulty, why the method of [BS83] could not be used in a more direct way, is that it is not excluded that the degree of the gradient map for a polynomial could be greater than the one for a multiple of this polynomial.

It would be interesting to get similar lower bounds for the randomized computation trees over the fields of positive characteristic.

1. Complexity of multiples of a product of linear functions.

Let F be an algebraically closed field of zero characteristic. Consider pairwise distinct hyperplanes $H_1, \dots, H_m \subset F^n$, let $L_i \in F[X_1, \dots, X_n]$ be a linear function such that its variety of zeroes $H_i = \{L_i = 0\}$, $1 \leq i \leq m$. By $S = \bigcup_{1 \leq i \leq m} H_i$ denote an arrangement, $L = \prod_{1 \leq i \leq m} L_i$, so $S = \{L = 0\}$.

If for some $1 \leq i_1 < \cdots < i_{n-k} \leq m$ the dimension $\dim(H_{i_1} \cap \cdots \cap H_{i_{n-k}}) = k$, the intersection $H_{i_1} \cap \cdots \cap H_{i_{n-k}}$ is called k-face of S. In this section by N we denote the number of 0-faces (in other words, vertices) of S.

Let a polynomial $0 \not\equiv f \in F[X_1, \dots, X_n]$ be a certain multiple of L. Similar to [S73], [L90] consider the graph of f joined by its gradient $\mathrm{grad}_f(x) = \left(\frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}\right)(x)$.

$$\begin{aligned} G = \{(x_1, \dots, x_n, x_0, y_1, \dots, y_n); (x_1, \dots, x_n) \in F^n, x_0 \\ = f(x_1, \dots, x_n), (y_1, \dots, y_n) = \mathrm{grad}_f(x)\} \subset F^{2n+1}. \end{aligned}$$

The main purpose of the present section is to prove a lower bound on the degree (see e.g. [M76], [S73], [S94]) $\deg G$ in terms of N (see theorem 1 below). As usual while studying the degree one considers the embedding of an affine variety $G \subset F^{2n+1} \subset \mathbb{P}^{2n+1} = \mathbb{P}^{2n+1}(F)$ into the projective space. Then $\deg G$ equals to the maximal possible (and simultaneously, typical) number of points of intersections of the projective closure $\overline{G} \subset \mathbb{P}^{2n+1}$ with linear subspaces, provided the intersection is finite.

Theorem 1. *$deg\, G \geq \frac{N}{2^{2n+1}}$*

Proof. Introduce the following rational map $\psi : F^{2n+1} \to \mathbb{P}^{n^2+2n-1}$ defined by the formula

$$\psi(x_1,\ldots,x_n,x_0,y_1,\ldots,y_n)=(\{x_iy_j\}:y_1:\cdots:y_n)\,;\;0\leq i\leq n\,,\;1\leq j\leq n$$

where $\{x_iy_j\}$ denote $n(n+1)$ projective coordinates. Observe that ψ is the composition of the canonical maps $F^{n+1}\times(F^n-0)\to F^{n+1}\times\mathbb{P}^{n-1}\to\mathbb{P}^{n+1}\times\mathbb{P}^{n-1}\to\mathbb{P}^{n^2+2n-1}$ where the latter one is the Segre embedding. Thus, ψ is defined when not all $y_1,\ldots,y_n$ vanish (the role of ψ is to make the coordinates of the gradient to be projective). Obviously $\dim\psi(G)=\dim G=n$.

Consider also a rational map $\sigma:\mathbb{P}^{n^2+2n-1}\to\mathbb{P}^{n-1}$, being a linear projection: $\sigma(\{z_{ij}\}:y_1:\cdots:y_n)=(y_1:\cdots:y_n)$ (its role is to distinguish the coordinates of the gradient).

First we remark that the theorem holds easily in case $n=1$. Indeed, the arrangement $S\subset F$ consists of N points being the zeroes of L, therefore $\deg f\geq N$ since $L\big|f$. The graph $G=\{(x,f(x),f'(x)):x\in F\}\subset F^3$ and its degree $\deg G\geq\deg f$. Henceforth, we assume that $n\geq 2$.

Besides, we suppose that $N\geq 1$, otherwise the theorem is evident.

Lemma 1. *For any vertex $x^{(0)}=(x_1^{(0)},\ldots,x_n^{(0)})$ of S set $x_0^{(0)}=f(x_1^{(0)},\ldots,x_n^{(0)})=0$. Then $\dim(\sigma(\overline{\psi(G)}\cap\mathcal{H}^{(0)}))=n-1$, where $(n-1)$-dimensional projective linear subspace*

$$\mathcal{H}^{(0)}=\mathcal{H}(x^{(0)})=\{(\{x_i^{(0)}y_j\}:y_1:\cdots:y_n);(y_1:\cdots:y_n)\in\mathbb{P}^{n-1}\}\subset\mathbb{P}^{n^2+2n-1}$$

is determined by the linear equations $z_{ij}=x_i^{(0)}y_j$, $0\leq i\leq n$, $1\leq j\leq n$.

Remark. Lemma 1 implies that $\mathcal{H}^{(0)}\subset\overline{\psi(G)}$ and therefore, $\sigma(\overline{\psi(G)}\cap\mathcal{H}^{(0)})=\sigma(\mathcal{H}^{(0)})=\mathbb{P}^{n-1}$.

Proof of the lemma. W.l.o.g. we assume for the sake of simplifying the notations that $x^{(0)}=0$ and the hyperplanes $\{X_1=0\},\ldots,\{X_n=0\}\subset F^n$ are among $H_1,\ldots,H_m$ (this could be achieved by a suitable linear transformation of the coordinates).

Suppose that the conclusion in lemma is wrong. Then there exists a non-zero homogeneous polynomial $h \in F[Y_1, \dots, Y_n]$ such that $h(y_1, \dots, y_n) = 0$ for any point $(\{0\} : y_1 : \dots : y_n) \in \overline{\psi(G)}(\cap \mathcal{H}^{(0)})$.

Write $f = f_s + f_{s+1} + \dots + f_{s_1}$, where f_j is the homogeneous component of f of degree j and $f_s \not\equiv 0$. Since $X_1 \cdots X_n | f$ we have $s \geq n \geq 2$, moreover in the decomposition into the sum of homogeneous components $\frac{\partial f}{\partial X_j} = \frac{\partial f_s}{\partial X_j} + \frac{\partial f_{s+1}}{\partial X_j} + \dots + \frac{\partial f_{s_1}}{\partial X_j}$ the least component $\frac{\partial f_s}{\partial X_j}$ of degree $(s-1)$ does not vanish identically.

Let us show that for any line $\{(tx_1, \dots, tx_n)\}_{t \in F} \subset F^n$, where a point $0 \neq (x_1, \dots, x_n) \in F^n$, passing through $x^{(0)} = 0$, such that grad_{f_s} does not vanish on this line identically (and thus, does not vanish for any $t \neq 0$, as grad_{f_s} is homogeneous), it holds

$$\left(\{0\} : \frac{\partial f_s}{\partial X_1} : \dots : \frac{\partial f_s}{\partial X_n}\right) (x_1, \dots, x_n) \in \overline{\psi(G)} \tag{1}$$

Indeed, we have $\frac{\partial f}{\partial X_j}(tx_1, \dots, tx_n) = t^{s-1} \widetilde{f}_j(t, x_1, \dots, x_n) =$ $\left(t^{s-1} \frac{\partial f_s}{\partial X_j} + t^s \frac{\partial f_{s+1}}{\partial X_j} + \dots + t^{s_1 - 1} \frac{\partial f_{s_1}}{\partial X_j}\right) (x_1, \dots, x_n)$, $1 \leq j \leq n$ and $f(tx_1, \dots, tx_n) = t^s \widetilde{f}_0(t, x_1, \dots, x_n)$ for suitable polynomials $\widetilde{f}_0, \widetilde{f}_1, \dots, \widetilde{f}_n \in F[t, x_1, \dots, x_n]$. Then the point

$$\left(\left\{ tx_i \cdot t^{s-1} \widetilde{f}_j \right\}_{1 \leq i,j \leq n} : \left\{ t^s \widetilde{f}_0 \cdot t^{s-1} \widetilde{f}_j \right\}_{1 \leq j \leq n} : t^{s-1} \widetilde{f}_1 : \dots : t^{s-1} \widetilde{f}_n \right)$$

belongs to $\psi(G)$. Dividing all the coordinates over the common factor t^{s-1} and after that substituting $t = 0$ we get (1) for the resulting limit point.

Thus, for any point $(x_1, \dots, x_n) \in F^n$ we have $h\left(\left(\frac{\partial f_s}{\partial X_1}, \dots, \frac{\partial f_s}{\partial X_n}\right)(x_1, \dots, x_n)\right) = 0$ since h is homogeneous, i.e. $h\left(\frac{\partial f_s}{\partial X_1}, \dots, \frac{\partial f_s}{\partial X_n}\right) \equiv 0$.

Consider the monomial ordering *deglex*, according to which a monomial is higher than another one if either its total degree is greater or the degrees of both coincide and the monomial is higher in the lexicographical ordering (with respect to a certain fixed ordering of the variables $X_1, \dots, X_n$).

Let $M = X_1^{i_1} \cdots X_n^{i_n}$ be the least monomial of f_s in *deglex* ordering (hence M is also the least monomial of f), then $i_1 \geq 1, \dots, i_n \geq 1$ since $X_1 \cdots X_n | f$. Therefore, the least monomial of $\frac{\partial f_s}{\partial x_j}$ is $\frac{M}{X_j}$. Let $h = \sum_K h_K Y_1^{K_1} \cdots Y_n^{K_n}$. In the expansion of $h\left(\frac{\partial f_s}{\partial X_1}, \cdots, \frac{\partial f_s}{\partial X_n}\right)$ the least monomials $\left(\frac{M}{X_1}\right)^{K_1} \cdots \left(\frac{M}{X_n}\right)^{K_n}$ of the items are pairwise distinct; indeed, assuming the contrary we have, $\left(\frac{M}{X_1}\right)^{p_1} \cdots \left(\frac{M}{X_n}\right)^{p_n} = 1$ for some integers $p_1, \dots, p_n$ not all of them being zeroes, then the vector $(p_1, \dots, p_n)$ is collinear with the vector $(i_1, \dots, i_n)$, thus $M^{i_1+\cdots+i_n} = M$, but $i_1 + \cdots + i_n \geq n \geq 2$ and we get a contradiction. Since the least monomials of the items are pairwise distinct, they cannot cancel each other, this leads to the contradiction with $h\left(\frac{\partial f_s}{\partial X_1}, \cdots, \frac{\partial f_s}{\partial X_n}\right) \equiv 0$ and proves the lemma.

Lemma 2. *deg* $\overline{\psi(G)} \geq N$

Proof. Consider a variety $V = \overline{\psi(G)} \cap \mathcal{P} \subset \mathbb{P}^{n^2+2n-1}$, where $\mathcal{P} = \{\{z_{ij}\}_{1 \leq i,j \leq n} : \{0\} : y_1 : \cdots : y_n\}$ is the subspace (of codimension n) obtained by means of substituting zeroes for the coordinates $\{z_{0i}\}_{1 \leq i \leq n}$.

Pick out any vertex $x^{(0)}$ of S (taking into account that $N \geq 1$), then $\overline{\psi(G)} \cap \mathcal{H}^{(0)} \subset V$ and lemma 1 entails that $\dim(\sigma(V \cap \mathcal{H}^{(0)})) = n-1$. On the other hand, consider a hyperplane $\{X_0 = 0\} \subset F^{2n+1}$, then $\psi(G) \cap \mathcal{P} \subset \psi(G \cap \{X_0 = 0\})$, hence $\dim\,(\psi(G) \cap \mathcal{P}) \leq \dim(G \cap \{X_0 = 0\}) \leq n-1$, therefore, no n-dimensional irreducible component of $\psi(G)$ lies entirely in $\mathcal{P}$ and because of that $\dim V \leq n-1$, thus $\dim V = n-1$.

The theorem on the dimensions of the fibres [S94], [M76] implies the existence (actually, an open set) of a point $y^{(0)} = (y_1^{(0)} : \cdots : y_n^{(0)}) \in \mathbb{P}^{n-1}$ such that the preimage $\sigma^{-1}(y^{(0)}) \cap V$ consists of a finite number of points and moreover, $y^{(0)} \in \sigma(V \cap \mathcal{H}^{(0)})$ for any vertex $x^{(0)}$ of S. Therefore, $\deg \overline{\psi(G)} \geq N$ since the intersection of V with the subspace $\{y_i y_j^{(0)} = y_j y_i^{(0)}\}_{1 \leq i,j \leq n}$ consists of a finite number of points $\sigma^{-1}(y^{(0)}) \cap V$, and for any of vertices $x^{(0)} = (x_1^{(0)}, \dots, x_n^{(0)})$ of S this intersection contains the point $(\{x_i^{(0)} y_j^{(0)}\}_{1 \leq i,j \leq n} : \{0\} : y_1^{(0)} : \cdots : y_n^{(0)})$ due to the choice of $y^{(0)}$ (cf. [S94],[S73]). Lemma 2 is proved.

To complete the proof of the theorem one could invoke the inequality deg $\overline{\psi(G)} \leq$

$\deg\psi\cdot\deg G$ (see [S73], [S94]), but in order to estimate $\deg\psi$ one should consider Graph ψ of the map ψ into the projective space $\mathbb{P}^{n^2+2n-1}$ and Segre embedding Graph ψ into $\mathbb{P}^{(2n+2)(n^2+2n)-1}$ (see [M76], [S94]) which would increase its degree. Instead of that, we give an alternative self-contained proof of the required inequality $\deg\overline{\psi(G)}\leq 2^{2n+1}\deg G$.

Take a subspace $P\subset\mathbb{P}^{n^2+2n-1}$ of the codimension n such that $P\cap\psi(G)$ consists of $\deg\psi(G)=\deg\overline{\psi(G)}$ points (such a subspace exists since for almost any n-codimensional subspace its intersection with $\overline{\psi(G)}$ consists of $\deg\overline{\psi(G)}$ points and for almost any subspace its intersection with the set $\overline{\psi(G)}-\psi(G)$ of dimension less than n is empty). Then $\psi(\psi^{-1}(P)\cap G)=P\cap\psi(G)$. Hence $\deg\overline{\psi(G)}$ does not exceed the number of irreducible components of the variety $\psi^{-1}(P)\cap G$ which in its turn is less or equal to $\deg(\psi^{-1}(P)\cap G)\leq\deg\psi^{-1}(P)\deg G$ according to the Bezout inequality for locally closed sets proved in [H83] which extends the more customary case of the closed projective sets intersecting completely, see e.g. [M76], [S94], also [S73]. The local closedness of the set $\psi^{-1}(P)$ follows from the next paragraph.

It remains to estimate $\deg\psi^{-1}(P)$. If P is determined by linear equations of the form $\sum_{0\leq i\leq n,1\leq j\leq n}\alpha_{ij}z_{ij}+\sum_{1\leq i\leq n}\alpha_i y_i=0$, then $\psi^{-1}(P)\subset F^{2n+1}$ is determined (out of the plane $L=\{y_1=\cdots=y_n=0\}$ where ψ is not defined) by quadratic equations of the form

$$\sum\alpha_{ij}x_iy_j+\sum\alpha_iy_i=0 \tag{2}$$

By induction on $0\leq q\leq 2n$ one could choose the linear combinations $g_1,\ldots,g_q\in F[X_1,\ldots,X_n,X_0,Y_1,\ldots,Y_n]$ of the equations of the form (2) satisfying the property that any irreducible component of codimension less than q of the locally closed set $\{g_1=\cdots=g_q=0\}-L$ is also an irreducible component of $\psi^{-1}(P)$. As q_{q+1} one can choose a linear combination of the equations of the form (2) such that g_{q+1} does not vanish identically on any irreducible component of $\{g_1=\cdots=g_q=0\}$, not being an irreducible component of $\psi^{-1}(P)$. At the end of this process $\psi^{-1}(P)$

is a union of several irreducible components of $\{g_1 = \cdots = g_{2n+1} = 0\}$ (the latter variety could contain few extra its 0-dimensional irreducible components). Hence $\deg \psi^{-1}(P) \leq \deg \{g_1 = \cdots = g_{2n+1} = 0\} \leq 2^{2n+1}$ again due to the Bezout inequality.

Finally, $\deg \overline{\psi(G)} \leq 2^{2n+1} \deg G$, together with lemma 2 this proves the theorem 1.

In the following corollary we utilize introduced above notations. From now on let F be an arbitrary field of zero characteristic.

Corollary 1. *Let $L|f$, $f \not\equiv 0$, then the multiplicative complexity C of f is greater or equal to $\frac{1}{3}(\log_2 N - 2n - 1)$*

For the proof we treat the polynomials L, f over the algebraic closure $\overline{F}$ of F. Notice that the [BS83] implies that the multiplicative complexity of the family of polynomials (f, grad_f) is less or equal to $3C$, hence [S73] entails that $\deg G \leq 2^{3C}$ (cf. also [L90]), which together with the theorem 1 proves the corollary.

2. Complexity lower bound for randomized computation trees

Let us consider first a deterministic algebraic computation tree (CT) T' which recognizes an arrangement S. Prune from T' all possible degenerate branches which lead to the sign $\neq$ for identically vanishing testing functions. After that the resulting CT (which we still denote by T') possesses the unique (we call it "thick") branch with the testing polynomials $f_1, \dots, f_k \in F[X_1, \dots, X_n]$, respectively, such that all the signs along this branch are $\neq$. Denote $f = f_1 \cdots f_k$. Obviously, the set $W = \{f \neq 0\} \subset \overline{F}^n$ of the points satisfying the tests along the "thick" branch is open and dense in the Zariski topology (see e.g. [M76]). Evidently, the total complexity of the sequence $f_1, \dots, f_k$ does not exceed k, therefore, the complexity of f being the product of this sequence, does not exceed $2k - 1$. The output of the "thick" branch should be "no", i.e. $W \cap S = \phi$, hence $L|f$.

For any $0 \leq r \leq n-1$ denote by $\varphi_r(S)$ the number of r-faces of S.

Proposition. The complexity of a deterministic computation tree recognizing an arrangement S is greater than $\frac{1}{6}(\log_2 \varphi_r(S) - 2(n-r))$.

Remark. Moreover, we show that a certain branch (in fact, the "thick" one) of a computation tree contains at least $\frac{1}{6}(\log_2 \varphi_r(S) - 2(n-r))$ *multiplications.*

To prove the proposition take a $(n-r)$-dimensional plane $P \subset F^n$ in generic position and restrict CT T' and S on P. Then the multiplicative complexity of the restriction $f|_P$ is still less or equal than $2k-1$ and the arrangement $S \cap P \subset P$ has $\varphi_r(S)$ vertices. Since $L|_P \mid f|_P$, one applies the corollary 1 and concludes that $(2k-1) \geq \frac{1}{3}(\log_2 \varphi_r(S) - 2(n-r) - 1)$, thus the proposition is proved.

But our main issue are the randomized algebraic computation trees (RCT, see e.g. [M85], [GKMS96], [GK97]). Under RCT we mean a collection of CT $T = \{T_\alpha\}$ and a probabilistic vector $p_\alpha \geq 0$, $\sum\limits_\alpha p_\alpha = 1$ 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 are obtained if to define the depth of an RCT as the expectation of the depths of T_α's [M85]). The main requirement is that for any input an RCT gives a correct output with probability at least $1 - \gamma > \frac{1}{2}$ (γ is called the error probability of RCT, see e.g. [M85], [GKMS96]).

Let k_0 be the complexity (depth) of T, then any testing polynomial in T has the degree at most 2^{k_0}. Take $N = \left\lceil \frac{2^{k_0+2}}{1-2\gamma} \right\rceil$ and arbitrary N pairwise distinct elements $\alpha_1, \dots, \alpha_N \in F$. Consider a grid $R = \{\alpha_1, \dots, \alpha_N\}^{n-1} \subset F^{n-1}$. Then for any polynomial $0 \not\equiv g \in F[X_1, \dots, X_{n-1}]$ of degree at most 2^{k_0+1} the number of zeroes of g on R does not exceed $2^{k_0+1} \cdot N^{n-2} \leq \frac{1-2\gamma}{2} N^{n-1}$ (see [S80]).

Now embed the grid R into each hyperplane H_i, $1 \leq i \leq m$ (in an arbitrary way), one can assume w.l.o.g. that the embeddings in the different hyperplanes have no common points. The union of all these embeddings we denote by $\Delta \subset S$.

Observe that for the "thick" branches of T the output "yes" could be given with the probability at most γ. Indeed, there exists a point which belongs to the open sets W_α which correspond to the "thick" branches of T_α for all α and to the complement $F^n - S$; for this point the incorrect output "yes" could appear with a probability at most γ.

Therefore, there exists α such that CT T_α gives the output "no" for its "thick" branch and besides, gives the correct output (so, "yes") for at least $(1-2\gamma)|\Delta| = (1-2\gamma)m\ N^{n-1}$ points among Δ, denote this set of points by $\Delta_0 \subset \Delta$. Indeed, otherwise the correct output for the points from Δ is given with an expectation less than $(1-2\gamma)+\gamma$, the latter summand γ refers to α such that the "thick" branch of T_α gives the output "yes" (see above); that would contradict to the definition of γ. Let $f_1, \ldots, f_k$ be the testing polynomials along the "thick" branch of T_α, then $f = f_1 \cdots f_k$ vanishes at Δ_0 (obviously, $k \leq k_0$, $\deg f_i \leq 2^i$, $\deg f \leq 2^{k_0+1}$ and the complexity of f does not exceed $2k-1$).

Assume that there are exactly number q of hyperplanes $H_{i_1}, \ldots, H_{i_q}$ among $H_1, \ldots, H_m$ such that each of them contains more than $\frac{1-2\gamma}{2} N^{n-1}$ points from Δ_0. Then $(m-q)\frac{1-2\gamma}{2} \cdot N^{n-1} + qN^{n-1} \geq (1-2\gamma)m\ N^{n-1}$, whence $q \geq \frac{1-2\gamma}{1+2\gamma}m$. Observe now that f vanishes on each of hyperplanes $H_{i_1}, \ldots, H_{i_q}$ (due to the choice of N). Denote by $\widetilde{L} \in F[X_1, \ldots, X_n]$ the product of q linear functions which define $H_{i_q}, \ldots, H_{i_q}$. Then $\widetilde{L}|f$. Finally, applying corollary 1 as in the proof of the proposition (i.e. to the restriction of $\widetilde{L}$ and f onto a certain plane), we obtain the following lower bound on the complexity of RCT.

Theorem 2. *Assume that for any $\left\lceil \frac{1-2\gamma}{1+2\gamma}m \right\rceil$ hyperplanes among $H_1, \ldots, H_m$, the arrangement $\widetilde{S} \subset S = \bigcup_{1 \leq i \leq m} H_i$ being a union of these hyperplanes, has at least $\widetilde{N}$ faces of all the dimensions. Then the complexity of RCT with error probability $\gamma < \frac{1}{2}$ which recognizes S, is greater than $\frac{1}{6}(\log_2 \widetilde{N} - 2n - \log_2 n)$.*

Remark. In fact, one could replace $\frac{1-2\gamma}{1+2\gamma}$ by any other constant less than $1-2\gamma$.

Now we give two application of theorem 2.

Corollary 2. *Any RCT recognizing the distinctness, i.e. the arrangement $S =$*

$\bigcup_{1\leq i<j\leq n}\{X_i=X_j\}$ *has the complexity at least* $\Omega(n\log n)$.

The proof exploits an idea from [GKMS96]. Fix any constant $1\geq\beta>0$ and take at least $\beta\frac{n(n-1)}{2}$ hyperplanes $H_1,\dots,H_q$ among $\{X_i=X_j\}$, $1\leq i<j\leq n$. Let us show that the arrangement $H_1\cup\dots\cup H_q$ has at least $n^{\Omega(n)}$ faces, then theorem 2 would entail the corollary. For the sake of simplicity of notations suppose that n is even.

Consider all possible subsets $I\subset\{1,\dots,n\}$ for which $|I|=\frac{n}{2}$. By the argument of counting in average there exists a subset I such that among $\left(\frac{n}{2}\right)^2$ hyperplanes of the kind $\{X_i=X_j\}$ where $i\in I$, $j\notin I$ there are at least $\beta\frac{n^2}{4}$ from $H_1,\dots,H_q$. Denote $\alpha=\frac{1}{2}(1-\sqrt{1-\beta})>0$. There exist at least αn numbers $i_1,\dots,i_t\in I$ such that for any i_{t_1}, $1\leq t_1\leq t$ there are at least αn hyperplanes of the kind $\{X_{i_{t_1}}=X_j\}$, $j\notin I$ among $H_1,\dots,H_q$. Indeed, otherwise among the hyperplanes of the kind $\{X_i=X_j\}$, $i\in I$, $j\notin I$ one could find at least $\left(\frac{n}{2}-\alpha n\right)^2=\frac{n^2}{4}(1-\beta)$ hyperplanes which are not among $H_1,\dots,H_q$.

For i_1 choose one of the possible of at least $[\alpha n]$ hyperplanes of the kind $\{X_{i_1}=X_{j_1}\}$, $j_1\notin I$ among $H_1,\dots,H_q$; after that for i_2 choose one of the possible of at least $([\alpha n]-1)$ hyperplanes of the kind $\{X_{i_2}=X_{j_2}\}$, $j_2\neq j_1$, $j_2\notin I$ among $H_1,\dots,H_q$ and so on. Finally, for $i_{[\alpha n]}$ we have at least 1 possibility for $j_{[\alpha n]}$. Any possible intersection of the hyperplanes $\{X_{i_1}=X_{j_1}\}\cap\dots\cap\{X_{i_{[\alpha n]}}=X_{j_{[\alpha n]}}\}$ provides a face of the codimension $[\alpha n]$, and there are at least $[\alpha n]!$ such faces.

Remark. For the more customary trees over the real field $F=\mathbb{R}$ with the signs $\{\leq,>\}$ at the testing nodes, lower bound $\Omega(n\log n)$ for the distinctness problem was proved in [GKMS96] in case of the randomized algebraic *decision* trees. In case of the randomized *computation* trees the complexity of the distinctness problem was posed as an open question in [GK97].

Corollary 3. *Any RCT recognizing the restricted integer programming (RIP)* $\bigcup_{a\in\{0,\dots,j-1\}^n}\{aX=1\}\subset F^n$ *has the complexity at least* $\Omega(n^2\log j)$.

Notice that in the particular case $j = 2$ this problem coincides with the knapsack problem.

The corollary follows from theorem 2 and from [GK97] where it is proved in particular, that for some $\sigma > 0$ any subarrangement of the RIP consisting of $\lfloor j^{\sigma n} \rfloor$ hyperplanes of the form $\{aX = 1\}$ has at least $j^{\lambda n^2}$ faces for a suitable $\lambda > 0$.

Remark. Actually, the corollary 3 in case of an algebraically closed field F can be deduced directly from the complexity lower bound $\Omega(n^2 \log j)$ for the RIP for the randomized computation trees over the real field $F = \mathbb{R}$ with the signs $\{\leq, >\}$ [GK97]. Indeed, in case of the field $F = \mathbb{C}$ (or algebraic numbers $F = \overline{\mathbb{Q}}$) one can easily convert RCT T into RCT $T^{(\mathbb{R})}$ over $F = \mathbb{R}$ (respectively, $F = \overline{Q} \cap \mathbb{R}$), representing each computed polynomial g in RCT T as $g = g_1 + \sqrt{-1}\ g_2$ where $g_1, g_2 \in \mathbb{R}[X_1, \dots, X_n]$ and computing both g_1, g_2 in $T^{(\mathbb{R})}$. This gives the corollary 3 in case of $\mathbb{F} = \mathbb{C}$ or $F = \overline{\mathbb{Q}}$.

For an arbitrary algebraically closed field F one can write the condition of the non-existence of a RCT with a fixed low enough complexity and fixed probabilities p_α which recognizes RIP, as a formula of the first order theory of algebraically closed fields with the coefficients in $\overline{\mathbb{Q}}$ (provided that $p_\alpha \in \overline{\mathbb{Q}}$). This formula is true over $F = \mathbb{C}$ (and over $F = \overline{\mathbb{Q}}$), hence it is true over an arbitrary algebraically closed field F.

Remark. The results of this paper can be extended from the considered above arrangements to the so-called "distorted" arrangements. Namely, for irreducible polynomials $h_1, \dots, h_m \in F[X_1, \dots, X_n]$ (here we assume F to be algebraically closed) a "distorted" arrangement is a variety $W = \{h_1 \cdots h_m = 0\} \subset F^n$. A "distorted" k-face of W is an irreducible k-dimensional variety $W_k \subset F^n$ for which there exist $1 \leq i_1, \dots, i_{n-k} \leq m$ such that W_k is an irreducible component of the variety $\{h_{i_1} = \dots = h_{i_{n-k}} = 0\}$ and in addition, for almost any (in Zariski topology) point $x \in W_k$ the gradients $\mathrm{grad}_{h_{i_1}}(x), \dots, \mathrm{grad}_{h_{i_{n-k}}}(x)$ are linearly independent.

Let $f \in F[X_1, \dots, X_n]$ vanish on W and N denote the number of 0-faces of W.

Then the inequality from theorem 1 still holds. Indeed, for any 0-face $x \in W$ we make a linear transformation of the coordinates, after which the gradient $\mathrm{grad}_{h_{i_j}}(x)$ becomes orthogonal to the coordinate hyperplane $\{X_j = 0\}, 1 \le j \le n$ and x becomes the origin of the coordinates. Then the least homogeneous component of h_{i_j} (at the point x) equals to $c_j X_j, c_j \ne 0, 1 \le j \le n$. Hence the least homogeneous component of $h_{i_1} \cdots h_{i_n}$ equals to $(c_1 \cdots c_n) X_1 \cdots X_n$, therefore $X_1 \cdots X_n$ divides the least homogeneous component of the polynomial f, and the proof of theorem 1 goes through for the polynomial f almost literally, thereby as well the proof of corollary 1.

The proof of theorem 2 also goes through for "distorted" arrangements. Instead of the grid R in the proof one should take a suitable finite subset of points from a hypersurface $\{h_i = 0\} \subset F^n, 1 \le i \le n$ to guarantee that if any polynomial $g \in F[X_1, \dots, X_n]$ of a given degree vanishes at any fraction of $\beta > 0$ among these points then $h_i | g$ (of course, the number of points in this finite subset depends on β and on the degree of g). For example, one could consider a linear projection $\pi : F^n \to F^{n-1}$ such that $\dim(\pi\{h_i = 0\}) = n - 1$, take an appropriate grid $R_1 \subset F^{n-1}$, then the preimage $\pi^{-1}(R_1)$ could replace R in the proof.

References

[BS83] W. Baur, V. Strassen, *The complexity of partial derivatives*, Theor. Comput. Sci. **22** (1983), 317–330.

[B83] M. Ben-Or, *Lower bounds for algebraic computation trees*, Proc. ACM Symp. Th. Comput. (1983), 80–86.

[B94] M. Ben-Or, *Algebraic computation trees in characteristic $p > 0$*, Proc. IEEE Symp. Found. Comput.Sci. (1994), 534–539.

[BL94] A. Bjorner, L. Lovasz, *Linear decision trees, subspace arrangements and Moebius functions*, J. AMS **7, 3** (1994), 677–705.

[BLY92] A. Bjorner, L. Lovasz, A. Yao, *Linear decision trees: volume estimates and topological bounds*, Proc. ACM Symp. Th.Comput. (1992), 170–177.

[BKL93] P. Buergisser, M. Karpinski, T. Lickteig, *On randomized algebraic test complexity*, J. Complexity **9** (1993), 231–251.

[CMP92] F. Cucker, J.L. Montana, L.M. Pardo, *Time bounded computations over the reals*, Int. Journal of Algebra and Computation **2, 4** (1992), 395–408.

[G97] D. Grigoriev, *Nearly sharp complexity bounds for multiprocessor algebraic computations*, J. Complexity **13, 1** (1997), 50–64.

[G98] D. Grigoriev, *Randomized complexity lower bounds*, Proc. ACM Symp. Th. Comput. (1998), 219–223.

[G99] D. Grigoriev, *Randomized complexity lower bounds for arrangements and polyhedra*, Discrete and Computational Geometry (1999).

[GK97] D. Grigoriev, M. Karpinski, *Randomized quadratic lower bound for knapsack*, Proc. ACM Symp. Th. Comput. (1997), 76–85.

[GKS96] D. Grigoriev, M. Karpinski, R. Smolensky, *Randomization and the computational power of analytic and algebraic decision trees*, Computational Complexity **6, 4** (1997), 376–388.

[GKMS96] 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), 612–619.

[GKV97] D. Grigoriev, M. Karpinski, N. Vorobjov, *Lower bound on testing membership to a polyhedron by algebraic decision and computation trees*, Discrete and Computational Geometry **17,2** (1997), 191–215.

[H83] J.Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comput. Sci. **24** (1983), 239–277.

[L90] T. Lickteig, *On semialgebraic decision complexity*, Preprint TR-0–052 ICSI, Berkeley, 1990.

[M85] F. Meyer auf der Heide, *Simulating probabilistic by deterministic algebraic computation trees*, Theor. Comput. Sci. **41** (1985), 325–330.

[MP93] J. Montana, L. Pardo, *Lower bounds for arithmetic networks*, Appl. Algebra in Eng. Commun. Comput. **4** (1993), 1–24.

[MMP96] J.Montana, J.Morais, L.Pardo, *Lower bounds for arithmetic network II: sum of Betti numbers*, Appl. Algebra in Eng. Commun. Comput. **7** (1996), 41-51.

[M76] D. Mumford, *Algebraic geometry*, Springer, 1976.

[S80] T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27** (1980), 701–717.

[S94] I. R. Shafarevich, *Basic algebraic geometry*, V. 1 – Springer, 1994.

[SY82] M. Steele, A. Yao, *Lower bounds for algebraic decision trees*, J. Algorithms **3** (1982), 1–8.

[S73] V. Strassen, *Die Berechnungskomplexitaet von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten*, Numer. Math. **20** (1973), 238–251.

[S83] V. Strassen, *The complexity of continued fractions*, SIAM J. Comput. **12,1** (1983), 1–27.

[Y81] A. Yao, *On the parallel complexity for the knapsack problem*, Proc. ACM Symp. Th. Comput. (1981), 123–127.

[Y92] A. Yao, *Algebraic decision trees and Euler characteristic*, Proc. IEEE Symp. Found. Comput. Sci. (1992), 268–277.

[Y94] A. Yao, *Decision tree complexity and Betti numbers*, Proc. ACM Symp. Th. Comput. (1994), 615–624.