An Exponential Lower Bound on the Size of Algebraic Decision Trees for MAX

Dima Grigoriev* **Marek Karpinski†**

Andrew C. Yao‡

TR-95-066

November 1995

Abstract

We prove an exponential lower bound on the size of any fixed-degree algebraic decision tree for solving MAX, the problem of finding the maximum of n real numbers. This complements the $n-1$ lower bound of Rabin [R72] on the depth of algebraic decision trees for this problem. The proof in fact gives an exponential lower bound on size for the polyhedral decision problem MAX= of testing whether the j-th number is the maximum among a list of n real numbers. Previously, except for linear decision trees, no nontrivial lower bounds on the size of algebraic decision trees for any familiar problems are known. We also establish an interesting connection between our lower bound and the maximum number of minimal cutsets for any rank-d hypergraphs on n vertices.

*Departments of Computer Science and Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802. The research of this author is supported in part by the Volkswagen-Stiftung. Email: `grigorie@cse.psu.edu`

†Department of Computer Science, University of Bonn, 53117 Bonn, and International Computer Science Institute, Berkeley, California. The research of this author is supported in part by the DFG Grant KA 673/4-1, and by the ESPRIT BR Grants 7097 and EC-US 030. Email: `marek@theory.cs.uni-bonn.de`

‡Department of Computer Science, Princeton University, Princeton, New Jersey 08544. The research of this author is supported in part by National Science Foundation under grant CCR-9301430. Email: `yao@cs.princeton.edu`

1 Introduction

The minimum depth of decision trees has been extensively studied for many computational problems in the literature. However, another natural complexity measure, the minimum *size* of decision trees is much less understood. For business applications (e.g. [GS79]) and for some computational problems, the size of decision trees gives a reasonable measure of the space required to implement the corresponding algorithms. For example, consider the membership problem for a given polyhedron in n dimensions. Unless the polyhedron has a highly-structured description, it is reasonable to expect that many decision trees (especially those with optimized depth) have to be stored in order for the membership queries to be processed with an efficiency reflecting the depths of the trees.

We focus our attention to computations in $\mathbb{R}^n$ that can be modeled by algebraic decision trees; these include many geometric and searching-sorting problems. Clearly, the size of a decision tree is no less than its depth, and thus a lower bound to the depth of all decisions trees for solving a problem is also a lower bound to the size of all such trees. Other than this obvious observation, the only lower bounds known are those for linear decision trees (where only linear functions are used for branching, see e.g., [DL75], [BLY92]), typically exponential in the depth. For higher degree algebraic decision trees, no superpolynomial lower bounds are known for natural problems, except with further constraints on the test polynomials.

In this paper we investigate the size complexity of algebraic decision trees for MAX, the problem of finding the maximum of n real numbers, which was studied extensively in the literature (cf., e.g., [K73], [R72], [TY94]). We use the standard degree-d ternary algebraic decision tree model in which each internal node performs a test $p(x_1, x_2, \cdots, x_n) : 0$ (where p is any real polynomial of degree d) with $<, =, >$ as the possible outcomes. Rabin [R72] established the sharp lower bound $n-1$ on the depth of any algebraic decision tree (for any d) solving this problem (see also [MPR94]). Except for linear decision trees ($d = 1$) and for cases with special restricted forms of polynomial tests (see Remark 1), no nonlinear lower bound is known on the size.

Let "MAX=" denote the problem of verifying $x_1 \geq x_k$ for all $1 \leq k \leq n$. The main result of the present paper is to show that, for any fixed d, the size of any degree-d algebraic decision tree for solving MAX= (and hence MAX) is at least $2^{e_d n}$ for some positive constant e_d. We will also establish an interesting connection between this lower bound and the maximum number of minimal cutsets for any rank-d hypergraphs on n vertices. This connection enables us to obtain better values of e_d. There are many interesting open problems suggested by our work, some of which are mentioned in the remarks below and at the end of Section 2.

Remark 1. A direct motivation for the present study is the close relation between the *size* of decision trees for MAX and the *depth* of decision trees for selecting the i largest elements. Let $a_{d,n}$ be the minimum size of any degree-d algebraic decision tree for solving MAX for almost all inputs (i.e., except for a measure-0 set). Then any degree-d algebraic decision tree for selecting the i largest elements must have depth greater than $\log_2(a_{d,n}\binom{n}{i-1})$. This approach to the selection problem was first formulated in [FG79] for the case $d = 1$. It is well known that Farkas Lemma implies $a_{d,n} = 2^{n-1}$ for $d = 1$. In [Y89] and [F93], it was proved that $a_{d,n} = 2^{n-1}$ *if* the test polynomials are restricted to $(x_j - x_k)(x_h - x_s)$ and

products of linear forms, respectively, leading to lower bounds $n + (i-1)\log_2 n + O(1)$ or the selection problems under such constraints.

Conjecture 1: $a_{d,n} = 2^{n-1}$ for all d, n.

A proof of this conjecture would imply that the depth complexity of algebraic decision tree for selecting the i largest elements among n is $n + (i-1)\log_2 n + \theta(1)$, which has been an open problem for some time. Even a proof of the conjecture for $d = 2$ will be of much interest.

Remark 2 All the known exponential lower bounds on decision tree size for MAX, as discussed in Remark 1, were proved with the following approach: show that every branch of the tree has to be of length $n-1$ or more. This is no longer possible for the general case even for $d = 2$, since a degree-2 decision tree with the root node testing $p = x_1 - x_2^2 - \cdots - x_n^2 - 1 : 0$ has a branch of length 1 (the branch with $p(x) > 0$ at the root). To our knowledge, no lower bound better than $n-1$ is known before this paper.

Remark 3 We consider in the paper standard ternary decision trees (cf. [SY82], [B83]) branching according to the signs $>, =, <$. Notice that for binary decision trees studied in [R72] (branching according to the signs $\leq, >$), MAX= has an $(n-1)$-size linear decision tree, namely the tree which successively tests $x_1 \geq x_2, \quad x_1 \geq x_3, \quad \ldots, \quad x_1 \geq x_{n-1}$. (More generally, this construction shows that the membership problem for any polyhedron defined by k inequalities has a linear decision tree of size $k+1$ in this binary tree model; compare this with the lower bound on the depth $\Omega(logN)$ of [GKV95] where N is the number of all the faces of a polyhedron). On the other hand, MAX does not seem to have any polynomial-size trees in the binary tree model.

Conjecture 2: Any *binary* algebraic decision tree (of any degree) for MAX must have size $2^{\Omega(n)}$.

It is not hard to see that Conjecture 1 implies Conjecture 2. We also mention that for the membership problem to a union of k hyperplanes $\bigcup_{1 \leq i \leq k} a_i X = b_i$, there is a ternary (as well as binary) algebraic decision tree of the size k. It simply tests $(a_1 X - b_1)^2$, then, if the sign is $>$, tests $(a_2 X - b_2)^2$, etc. Notice that this tree is nonlinear.

Remark 4 A more refined way to model space requirement is to consider *branching programs* (see e.g., [BFKLT81], [BFMUW87]) in which "equivalent" nodes are permitted to be merged together. Very little is known about branching programs with algebraic decision elements (however, see [Y82]).

2 Summary of Results

Consider an input n-tuple of real numbers $(x_1, \ldots, x_n) \in \mathbb{R}^n$. An *Algebraic Decision Tree* (ADT) T of degree d and dimension n for MAX (MAX=) is a ternary tree with each internal node perfoming a ternary test $p(x_1, x_2, \cdots, x_n) : 0$ where p is a polynomials of degree at most d, and branching according to the outcomes ($<, =$, or $>$). Each leaf of the tree is either labeled by a certain index $i \in \{1, \ldots, n\}$ (MAX), or by a label "yes"or "no" (MAX=). We say that the decision tree T *solves* MAX (MAX=) in dimension n if, for an arbitrary input vector $(x_1, \ldots, x_n) \in \mathbb{R}^n$, the path traversed in T terminates in a leaf labeled by i ("yes") if and only if $x_i = \max\{x_1, \ldots, x_n\}$ ($x_1 = \max\{x_1, \ldots, x_n\}$, respectively). The *size* (resp. *depth*) of T is the number of its leaves (resp. the maximum length of its paths). It is well-

known [R72] that the depth of an ADT for MAX is at least $n-1$. This bound is optimal as one can easily construct T with the depth $n-1$ and size 2^{n-1}.

We prove an exponential lower bound on the size.

Theorem 1 Any algebraic decision tree of degree d solving MAX (MAX=) in dimension n has size at least $\Omega(2^{c'(d)n})$ where $c'(d) > 0$ depends only on d.

A *hypergraph* $\mathcal{F}$ on *vertex set* $\{1,\ldots,N\}$ is a family of subsets of $\{1,\ldots,N\}$. The *rank* of $\mathcal{F}$ is the maximum size of any member of $\mathcal{F}$. A *minimal cutset* of $\mathcal{F}$ is a set $V \subseteq \{1,\ldots,N\}$ which intersects every member set of $\mathcal{F}$ and no proper subset of V has this property. Let us denote by $m_{\mathcal{F}}$ the number of *minimal cutsets* of $\mathcal{F}$. Let $m_{d,N}$ be the maximum $m_{\mathcal{F}}$ for any hypergraphs $\mathcal{F}$ of rank d or less on N vertices. It is not hard to show that for $d=2$, $m_{2,N}$ is equal to the maximum number of maximal cliques of any N-vertex graph, which by a result of Moon and Moser [MM65] is equal to $\theta(3^{N/3})$.

A slight variation of the proof of Theorem 1 leads to an interesting connection of our lower bound to the combinatorial quantity $m_{d,N}$.

Theorem 2 Any algebraic decision tree of degree d solving MAX (MAX=) in dimension n has size at least $2^{n-1}/m_{d,n-1}$.

From the fact $m_{2,N} = \theta(3^{N/3})$, it follows then that any degree-2 algebraic decision tree for MAX (MAX=) must have size $\Omega(2^{c'(d)n})$ with $c'(2) = 1-(\log_2 3)/3 \approx 0.47$. This improves over the value $1-\frac{1}{1+\frac{1}{2}\log_2(\frac{4}{3})} \approx 0.18$ for $c'(2)$ obtained in the proof of Theorem 1 (see Section 3); it also improves all the $c'(d)$ for $d>2$, since the proof of Theorem 1 defines $c'(d)$ recursively.

Remark 5 An interesting open combinatorial question is to determine the smallest $\lambda(d)$ for which $m_{d,N} \leq O(2^{\lambda(d)N})$. By Theorem 2, we can then choose $c'(d)$ in Theorem 1 to be $1-\lambda(d)$. To our knowledge, even the best $\lambda(3)$ has not been determined.

3 Proof of Theorem 1

Clearly every decision tree for MAX can be easily converted into a decision tree for the MAX= by relabeling a leaf "yes" whenever it is originally leabled as "x_1 is maximum". Thus we only need to prove Theorem 1 for MAX=.

For any $\{1\} \subset I \subset \{1,\ldots,n\}$ consider the following ('wall') set $M_I = \{(x_1,\ldots,x_n) : x_i > x_j$ for all $i \in I, j \notin I$ and $x_{i_1} = x_{i_2}$ for all $i_1, i_2 \in I\}$. Denote the plane $P_I = \{(x_1,\ldots,x_n) : x_{i_1} = x_{i_2}$ for all $i_1, i_2 \in I\}$. Then $\dim P_I = n - |I| + 1$ and M_I is an open polyhedron in P_I. Note that $P_{\{1\}} = \mathbb{R}^n$ and all P_I are pairwise distinct. Obviously, the sets M_I are pairwise disjoint and form a partition of the set $x_1 = max\{x_1,\ldots,x_n\}$ with 2^{n-1} elements. Observe that the Euclidian closure $\overline{M_I}$ has a non-empty intersection with M_J if and only if $I \subset J$. Moreover, if $\overline{M_I} \bigcap M_J \neq \emptyset$ then $\overline{M_I} \supset M_J$. Thus, $\{M_I\}$ form a cellular decomposition of the set $x_1 = max\{x_1,\ldots,x_n\}$ and the boundary $\partial M_I = \bigcup_{J \supset I} M_J$ in the plane P_I.

The method of our proof is based on the analysis of a "touching frequency" of the sets computed along the branches of a tree T with the 'wall sets' M_I.

Consider any *branch* B (i.e., a path from the root to some leaf) of the tree T, and let the testing polynomials together with their signs along this branch be $f_1 = \cdots = f_k = 0, \quad g_1 > 0, \ldots, g_l > 0$. Let $W_B \subset \mathbb{R}^n$ denote the (semialgebraic) set of all $x = (x_1, x_2, \cdots, x_n)$

satisfying $\{f_1(x) = \cdots = f_k(x) = 0, \quad g_1(x) > 0, \ldots, g_l(x) > 0\}$. We say that W_B *touches* M_I if $\dim(W_B \bigcap M_I) = \dim M_I = n - |I| + 1$. Observe that if W_B touches M_I then the label of B is "yes". Since for every M_I there exists B such that W_B touches M_I, Theorem 1 follows immediately from the Main Lemma below.

Main Lemma. For any branch B of T, W_B can touch at most $2^{c(d)n}$ sets M_I for some constant $c(d) < 1$ dependent only on d.

Define $c(d)$ recursively as follows. Let $c(1) = 0$, and $c(d) = c(d-1) + \frac{(1-c(d-1))^2}{1-c(d-1)+\frac{1}{d}\log_2(\frac{2^d}{2^d-1})}$ for $d \geq 2$. It is straightforward to verify that $0 \leq c(d) < 1$ for all d.

We now prove the Main Lemma by a series of Propositions.

Proposition 1. W_B cannot touch M_I, M_J such that $I \underset{\neq}{\supset} J$.

Proof. Assume the contrary. Let $\{j_1, \ldots, j_{n-|J|}\} = \{1, \ldots, n\} \setminus J$. For any polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ denote $f^{(J)}(X_1, X_{j_1}, \ldots, X_{j_{n-|J|}}) = f|_{X_j = X_1, j \in J} \in \mathbb{R}[X_1, X_{j_1}, \ldots, X_{j_{n-|J|}}]$. (From now on, we sometimes use the notation X_i instead of x_i when they are considered as formal variables instead of numbers.) One could consider $f^{(J)}$ as the restriction of f on the plane P_J with the coordinates $X_1, X_{j_1}, \ldots, X_{j_{n-|J|}}$, where $X_1 = X_j$ for each $j \in J$. Then $f_1^{(J)}, \ldots, f_k^{(J)}$ vanish identically because these polynomials vanish on the semialgebraic set $W_B \bigcap M_J$ of full dimension in the plane P_J.

By assumption there exists a point $x \in M_I$ such that $g_1(x) > 0, \ldots, g_\ell(x) > 0$. There exists a ball $B_x(r)$ with a radius $r > 0$ centered in x such that $g_1, \ldots, g_l$ are positive everywhere on $B_x(r)$. As $x \in M_I \subset \partial\overline{M_J}$ there exists a point $x' \in (B_x(r) \bigcap P_J) \setminus \overline{M_J}$. The decision tree T being applied to x' goes through the branch B, since $x' = (x'_1, \ldots, x'_n) \in W_B$. Since branch B leads to a "yes" leave, the input x' is accepted by the decision tree. This is a contradiction, as $\max(x'_1, \ldots, x'_n)$ is not x'_1 ($x' \notin \overline{M_J}$). $\square$

Remark 6. In fact we proved a stronger statement. Namely, if W_B touches M_J then $W_B \bigcap M_I = \emptyset$ for any $I \underset{\neq}{\supset} J$.

Proposition 2. If W_B touches M_I then I is a minimal (with respect to the inclusion) among the subsets $\{1\} \subset J \subset \{1, \ldots, n\}$ such that $f_1^{(J)}, \ldots, f_k^{(J)}$ vanish identically.

Proof. First, as we have seen in the proof of Proposition 1 that $f_1^{(I)}, \ldots, f_k^{(I)}$ vanish identically. Second, assume that $J \underset{\neq}{\subset} I$ such that $f_1^{(J)}, \ldots, f_k^{(J)}$ vanish identically. As W_B touches M_I, there exists a point $x \in M_I \bigcap W_B$; by defintion, $g_1(x) > 0, \ldots, g_l(x) > 0$. Then $g_1, \ldots, g_l$ are positive everywhere in a ball $B_x(r)$ for a suitable $r > 0$. Since $x \in M_I \subset \partial\overline{M_J}$, the open set $B_x(r) \bigcap M_J$ in P_J is nonempty, and $B_x(r) \bigcap M_J \subset W_B$ by definition of W_B. Thus, W_B touches M_J and we get a contradiction with Proposition 1, which proves the proposition. $\square$

The Main Lemma follows immediately from Proposition 2 and the following proposition.

Proposition 3. For any polynomials $h_1, \ldots, h_m \in \mathbb{R}[X_1, \ldots, X_n]$ with degrees $\deg(h_i) \leq d$, the number of sets minimal (with respect to the inclusion) among the subsets $\{1\} \subset I \subset \{1, \ldots, n\}$ such that $h_1^{(I)}, \ldots, h_m^{(I)}$ vanish identically, does not exceed $2^{c(d)n}$.

We prove the proposition by induction on d. For $d = 1$, each $h_i = \sum_{1 \leq j \leq n} \alpha_{ij} X_j + \alpha_i$, $1 \leq i \leq m$, is a linear polynomial. Let $\{1\} \subset I \subset \{1, \ldots, n\}$ be a minimal set for which

$h_1^{(I)}, \ldots, h_m^{(I)}$ vanish identically. Then for each $1 \le i \le m$, $\alpha_i = 0$, $\sum_{1 \le j \le n} \alpha_{ij} = 0$, and I must contain all j with $\alpha_{ij} \neq 0$. Thus, either no such I exists, or there is a unique such I consisting of $\{1\}$ and all $j \in \{1, \ldots, n\}$ for which there exists $1 \le i \le m$ such that $\alpha_{ij} \neq 0$. This proves the proposition for the induction base $d = 1$.

Inductive step. Let $d > 1$. Consider two cases. Denote $0 < c = \frac{1-c(d-1)}{1-c(d-1)+\frac{1}{d}\log_2(\frac{2^d}{2^d-1})} < 1$. A set $V \subset \{X_2, \ldots, X_n\}$ is called *a cover set* if each monomial $X_1^{\beta_1}, \ldots, X_n^{\beta_n}$ occurring in at least one of the polynomials $h_1, \ldots, h_m$ contains a variable from $V \cup \{X_1\}$.

1. In the first case there does NOT exist a cover set V of size $|V| \le cn$. We construct a set $\{b_1, b_2, \ldots, b_l\}$ of monomials occurring in at least one of $h_1, \ldots, h_m$ such that they are pairwise disjoint in the variables and contain only the variables from $\{X_2, \ldots, X_n\}$. We add $b_1, b_2, \cdots$ sequentially until no additional monomial can be added without violating the property stated above. Clearly, $b_1, \ldots, b_l$ contain at most dl variables among $\{X_2, \ldots, X_n\}$, and that these variables constitute a cover set. By assumption, we must have $dl > cn$.

   Observe that for any set $\{1\} \subset I \subset \{1, \ldots, n\}$ such that $h_1^{(I)}, \ldots, h_m^{(I)}$ vanish identically, the set $\{X_i, i \in I\}$ should have a common variable with each monomial $b_1, \ldots, b_l$. Therefore, the number of all such sets I does not exceed

$$2^n \left(\frac{2^d - 1}{2^d}\right)^l \le 2^n \left(\frac{2^d - 1}{2^d}\right)^{\frac{cn}{d}}. \tag{1}$$

2. In the second case there exists a cover set V with $|V| \le cn$. Consider any minimal $\{1\} \subset I$ such that $h_1^{(I)}, \ldots, h_m^{(I)}$ vanish identically. Let $I_0 = V \setminus \{X_i, i \in I\}$ and $I_1 = V \cap \{X_i, i \in I\}$. We uniquely expand $h_j^{(I_1 \cup \{1\})} = X_1 h_{j,X_1} + \sum_{\gamma=(\cdots\gamma_i\cdots)} (\prod_{i \in I_0} X_i^{\gamma_i}) P_{j,\gamma}$, $1 \le i \le m$, where the polynomials $P_{j,\gamma}, h_{j,X_1}$ are in the variables $X_i \notin V$. Note that $P_{j,\gamma}, h_{j,X_1}$ depend on variables in I_0. Since V is a cover set, $\deg P_{j,\gamma} \le d - 1$ for each multi-index γ; obviously $\deg(h_{j,X_1}) \le d - 1$.

   Since $h_j^{(I)}$ vanishes identically, the polynomials $P_{j,\gamma}^{(I \setminus I_1)}$ also vanish identically, and furthermore, the polynomial $h_{j,X_1}^{(I \setminus I_1)}$ vanishes identically as well. Thus, $I \setminus I_1$ is a minimal set for which the polynomials $P_{j,\gamma}^{(I \setminus I_1)}, h_{j,X_1}^{(I \setminus I_1)}$, $1 \le j \le m$, vanish identically.

   By inductive hypothesis there are at most $2^{c(d-1)(n-|V|)}$ possible choices of $I \setminus I_1$. Since there are at most $2^{|V|}$ possibilities for the choice of I_1, we have in all at most

$$2^{c(d-1)(n-|V|)} 2^{|V|} \le 2^{c(d-1)n} 2^{(1-c(d-1))cn}. \tag{2}$$

   minimal sets I.

It is straightforward to verify from (1), (2) that the number of minimal sets are no greater than $2^{c(d)n}$ in both cases. This completes the inductive step. We have thus proved Proposition 3, and hence Theorem 1. □

4 Proof of Theorem 2

Let T be any degree-d algebraic decision tree for deciding whether $n-1$ input real numbers $x_2, x_3, \cdots, x_n$ are all less than or equal to 0. We show that the size of T is at least $2^{n-1}/m_{d,n-1}$. This implies Theorem 2, as any decision tree for MAX= with inputs $x_1, x_2, \cdots, x_n$ can be converted into a decision tree for the above problem by setting $x_1 = 0$.

The proof is analogous to the first half of the proof of Theorem 1. For each $I \subset \{2, 3, \ldots, n\}$, let $M_I = \{(x_2, x_3, \ldots, x_n) : x_i = 0 \text{ for } i \in I, x_j < 0 \text{ for } j \notin I\}$. Let B be any branch of T, with $f_1 = \cdots = f_k = 0, \quad g_1 > 0, \ldots, g_l > 0$ being the set of constraints along B; let $W_B \subset \mathbb{R}^n$ denote the set of inputs $(x_2, x_3, \ldots, x_n)$ satisfying these constraints. We say that W_B *touches* M_I if $\dim(W_B \bigcap M_I) = \dim M_I = n - 1 - |I|$.

For any $J \subseteq \{2, 3, \ldots, n\}$ and a polynomial $h \in \mathbb{R}[X_2, \ldots, X_n]$, define the polynomial $h^{(J)}(X_j, j \notin J) = h|_{X_j = 0, j \in J} \in \mathbb{R}[X_j, j \notin J]$.

Similar to Proposition 2, we have the following.

Proposition 2′ If W_B touches M_I, then I is a *minimal* subset among all subsets J satisfying $f_i^{(J)} \equiv 0$ for $1 \le i \le k$.

The proof of Proposition 2′ is virtually identical to that of Proposition 2. Note that if W_B touches M_I, then all the polynomials f_j have vanishing constant terms (i.e., $f_j(0) = 0$).

We want to rephrase Proposition 2′ in terms of hypergraphs. To do this, we first relate the "minimal subsets" to minimal cutsets for hypergraphs. For any $h \in \mathbb{R}[X_2, \ldots, X_n]$, let G_h denote the family of nonempty subsets $\{i_1, \ldots, i_q\}$ for which there exists a monomial of h with the set of variables $\{X_{i_1}, \ldots, X_{i_q}\}$. Given a family H of polynomials, let $G_H = \bigcup_{h \in H} G_h$. Note that G_h and G_H are hypergraphs.

Let $H = \{h_1, \ldots, h_m\}$ where $h_i \in \mathbb{R}[X_2, \ldots, X_n]$ are polynomials with no constant terms.

Proposition 4. For any $J \subset \{2, \ldots, n\}$, $h_1^{(J)} \equiv 0, \ldots, h_m^{(J)} \equiv 0$ if and only if J is a cutset of G_H.

Proof. If J is a cutset of G_H, then setting X_j to 0 for all $j \in J$ kills all the monomials in h_i. Hence $h_i^{(J)} \equiv 0$ for all i. If, on the other hand, $h_i^{(J)} \equiv 0$ for all i, then for each i no monomials in h_i can be free from all $X_j, j \in J$, since otherwise $h_i^{(J)}$ is not identically equal to 0. Thus, J is a cutset of G_{h_i}, and since G_H is a union of all G_{h_i}, J is a cutset of G_H. $\square$

Proposition 4 implies that the sets minimal among I such that the polynomials $h_1^{(I)}, h_2^{(I)}, \ldots, h_m^{(I)}$ vanish identically are exactly the minimal cutsets of G_H.

Using Proposition 4, we can rephrase Propositions 2′ as follows: If W_B touches M_I, then I is a minimal cutset of G_F where $F = \{f_1, \ldots, f_k\}$. Since G_F is of rank d or less, there are at most $m_{d,n-1}$ such cutsets. This proves that W_B can touch at most $m_{d,n-1}$ M_I's. To touch all 2^{n-1} M_I's, at least $2^{n-1}/m_{d,n-1}$ branches B are needed. Thus, T must have size at least $2^{n-1}/m_{d,n-1}$. This completes the proof of Theorem 2.

References

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

[BFMUW87] A. Borodin, F. Fich, F. Meyer auf der Heide, E. Upfal, and A. Wigderson, A Time-Space Tradeoff for Element Distinctness, SIAM J. on Computing **16** (1987), pp. 97-99.

[BFKLT81] A. Borodin, M. Fischer, D. Kirkpatrick, N. Lynch, and M. Tompa, A Time-Space Tradeoff for Sorting on Oblivious Machines, J. of Computer and System Sciences **22** (1981), pp. 351-364.

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

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

[DL75] D. Dobkin and R.J. Lipton, On the complexity of computations under varying sets of primitives, in *Automata Theory and Formal Languages* (edited by H. Bradhage), Lecture Notes in Computer Science, Volume 33, Springer-Verlag, 1975, pp. 110-117.

[F93] R. Fleischer, Decision Trees: Old and New Results, Proc. 25th ACM STOC (1993), pp. 468–477.

[FG79] F. Fussenegger, H.N. Gabow, A Counting Approach to Lower Bounds for Selection Problems, J. Assoc. Comput. Mach. 25 (1979), pp.227-238.

[GS79] C. Gane and T. Sarson, Structured Systems Analysis: Tools and Techniques, Prentice Hall, Englewood Cliffs, NJ, 1979.

[GK93] D. Grigoriev, M. Karpinski, Lower Bounds on Complexity of Testing Membership to a Polygon for Algebraic and Randomized Computation Trees, Technical Report TR-93-042, International Computer Science Institute, Berkeley, 1993.

[GKV95] D. Grigoriev, M. Karpinski, N. Vorobjov, Improved Lower Bound on Testing Membership to a Polyhedron by Algebraic Decision Trees, Proc. 36th IEEE FOCS (1995), pp. 258-265.

[K73] D. E. Knuth, The Art of Computer Programming, Vol. 3, Addison-Wesley, 1973.

[MM65] J. W. Moon, L. Moser, On Cliques in Graphs, Israel J. Math. 3(1965), pp. 23-28.

[MPR94] L. J. Montana, L. M. Pardo, T. Recio, A Note on Rabin's Width of a Complete Proof, Computational Complexity, 4(1994), pp. 12-36.

[R72] M. O. Rabin, Proving Simultaneous Positivity of Linear Forms, J. Comput. Sci. **6** (1972), pp. 639–650.

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

[TY94] H. F. Ting and A. C. Yao, A Randomized Algorithm for Finding Maximum with $O((\log n)^2)$ Polynomial Tests, Information Processing Letters **49** (1994), pp. 39-43.

[Y75] A. C. Yao, On the Complexity of Comparison Problems Using Linear Functions, Proc. 16th IEEE FOCS (1975), pp. 85–89.

[Y82] A. C. Yao, On the Time-Space Tradeoff for Sorting with Linear Queries, Theoretical Computer Science **19** (1982), pp. 203-218.

[Y89] A. C. Yao, On Selecting the k Largest with Median Tests, Algorithmica **4** (1989), pp. 293–300.