

# Lower Bounds for Solving Linear Diophantine Equations on Random Access Machines

FRIEDHELM MEYER AUF DER HEIDE

*Johann Wolfgang Goethe-Universität, Frankfurt, Federal Republic of Germany*

**Abstract.** The problem of recognizing the language  $L_n(L_{n,k})$  of solvable Diophantine linear equations with  $n$  variables (and solutions from  $\{0, \dots, k\}^n$ ) is considered. The languages  $\bigcup_{n \in \mathbb{N}} L_n$ ,  $\bigcup_{n \in \mathbb{N}} L_{n,1}$ , the knapsack problem, are NP-complete. The  $\Omega(n^2)$  lower bound for  $L_{n,1}$  on linear search algorithms due to Dobkin and Lipton is generalized to an  $\Omega(n^2 \log(k+1))$  lower bound for  $L_{n,k}$ . The method of Klein and Meyer auf der Heide is further improved to carry over the  $\Omega(n^2)$  lower bound for  $L_{n,1}$  to random access machines (RAMs) in such a way that it holds for a large class of problems and for very small input sets. By this method, lower bounds that depend on the input size, as is necessary for  $L_n$ , are proved. Thereby, an  $\Omega(n^2 \log(k+1))$  lower bound is obtained for RAMs recognizing  $L_n$  or  $L_{n,k}$ , for inputs from  $\{0, \dots, (nk)^{O(n^2)}\}^n$ .

Categories and Subject Descriptors: F.2.2. [Analysis of Algorithms and Problem Complexity]: Nonnumerical Algorithms and Problems—*geometrical problems and computations*

General Terms: Algorithms, Theory

Additional Key Words and Phrases: Integer programming, linear search algorithms, random access machines

## 1. Introduction

In this paper we prove lower bounds for the time complexity of deciding the solvability of Diophantine linear equations with  $n$  variables; that is, of deciding whether a given linear equation has a solution with nonnegative integer coefficients. Formally, we consider the problem of recognizing the language

$$L_n = \{(\bar{a}, b), \bar{a} \in R^n, b \in R \mid \exists \bar{\alpha} \in N^n: \bar{a} \cdot \bar{\alpha} = b\}$$

( $R \hat{=}$  set of real numbers). It is well known that recognizing  $\bigcup_{n \in \mathbb{N}} L_n$  is NP-complete [5] ( $N \hat{=}$  set of positive integers). Furthermore, we consider the similar languages

$$L_{n,k} = \{(\bar{a}, b), \bar{a} \in R^n, b \in R \mid \exists \bar{\alpha} \in \{0, \dots, k\}^n: \bar{a} \cdot \bar{\alpha} = b\}.$$

The problem of recognizing  $\bigcup_{n \in \mathbb{N}} L_{n,1}$  is the well-known knapsack problem and is NP-complete [5].

For proving lower bounds for these problems, we consider a very realistic computational model, namely, random access machines (RAMs) as defined in [1].

Such a RAM has the capability of executing a direct or indirect storage access, an arithmetic operation from  $\{+, -\}$ , or an if-question in one step. We assume that the input is given integer by integer, not bit by bit.

Part of this work was done while the author was visiting SFB 124 of the University of the Saarland.

Author's present address: Johann Wolfgang Goethe Universität, Fachbereich 20 (Informatik), Mertonstrasse 17-25, 6000 Frankfurt am Main, West Germany.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

© 1985 ACM 0004-5411/85/1000-0929 \$00.75

In [7], Klein and Meyer auf der Heide prove an  $\Omega(n^2)$  lower bound for  $L_{n,1}$  on RAMs. This proof is done by presenting a method of carrying over lower bounds from linear search algorithms (LSAs) to RAMs.

An LSA can be considered an abstraction of a RAM in which no indirect storage access is allowed and that can work on real inputs. The analogous model of computation, where the operations  $\{*, / \}$  are also allowed, is introduced by Ben Or [2] as *algebraic computation trees* (ACTs).

Dobkin and Lipton [4] prove an  $\Omega(\log(q))$  lower bound for recognizing a language  $L \subset R^n$  that consists of  $q$  connected components.

This result is generalized to ACTs by Ben Or [2]. Furthermore, in [4], it is shown that  $R^n \setminus L_{n,1}$  has at least  $2^{(1/2)n^2}$  connected components, which implies an  $\Omega(n^2)$  lower bound for  $L_{n,1}$  on LSAs and ACTs.

In Section 2 of this paper, we generalize this result to an  $\Omega(n^2 \log(k+1))$  lower bound for  $L_{n,k}$  on LSAs and ACTs.

This lower bound is tight within a factor  $O(n^2)$  (respectively,  $O(n^2 \log(n))$  if  $k = o(\log(n))$ ). This is shown for  $k = 1$  by Meyer auf der Heide [10] and can be generalized, in a straightforward manner, to  $L_{n,k}$  in order to obtain an  $O(n^4(\log(n) + \log(k)))$  upper bound for  $L_{n,k}$ .

We now want to prove lower bounds for  $L_n$ . But, in this case, we have to note that  $L_n$  cannot be recognized by an LSA or ACT of bounded complexity, because one can check that  $R^n \setminus L_n$  consists of infinitely many connected components.

This phenomenon is mirrored by the complexities of the best-known algorithms for  $L_n$ . If we apply Kannan's improvement to Lenstra's integer-programming algorithm [6, 9] to  $L_n$  (which is a special type of integer programming), we obtain an  $O(n^9 \log(p) \log \log(p))$  algorithm in which  $p$  denotes the maximum size of the inputs that are assumed to be integers.

This result shows that lower bounds for  $L_n$  should also be expressed in terms of the input size. Results of this type are proved by Lautemann and Meyer auf der Heide [8] for the integer programming problem with two variables.

The proof of the lower bound for  $L_{n,1}$  on RAMs from [7], mentioned above, is tailored to this problem and does not include bounds for the input size that one has to demand such that the lower bound holds.

In Section 3, we generalize this result to a large class of problems. In that section, we consider languages  $L \subset R^n$  that are unions of hyperplanes in  $R^n$ . If the hyperplanes that make up  $L$  are defined by linear equations with integer coefficients from  $\{-k, \dots, k\}$ , we say that  $L$  is defined by hyperplanes with description size  $k$ . For example,  $L_{n,k}$  is defined by hyperplanes with description size  $k$ .

For languages, like those mentioned previously, with  $q$ -connected components, we prove a  $\log(q) - n \log \log(q)$  lower bound on RAMs in Section 3. This bound is shown to hold already for a very small input set (dependent on  $k$ ).

In Section 4, we finally apply this result to  $L_{n,k}$  and  $L_n$  and obtain that each RAM recognizing  $L_{n,k}$  or  $L_n$  needs  $\Omega(n^2 \log(k+1))$  steps for some input from  $\{0, \dots, (kn)^{O(n^2)}\}^n$ .

We finish this section with some notations from linear algebra, and a combinatorial result that we shall use frequently.

A hyperplane (left, right halfspace) in  $R^n$  is a set  $\{\bar{x} \in R^n, \bar{a} \cdot \bar{x} = (<, >)b\}$  where  $\bar{a} \in R^n$ ,  $b \in R$  are fixed. The hyperplane is linear iff  $b = 0$ . A polytope is an intersection of (left or right) halfspaces of hyperplanes. Thus, polytopes are convex. In [7], the following lemma is shown. We use it frequently in this paper.

**LEMMA 1** [7]. *Let  $H_1, \dots, H_m$  be hyperplanes in  $R^n$ ,  $n, m \geq 2$ . Then  $R^n \setminus \bigcup_{i=1}^m H_i$  consists of at most  $m^n$ -connected components. They are polytopes.*

2. A Lower Bound for  $L_{n,k}$  on LSAs and ACTs

In this section, we prove lower bounds for  $L_{n,k}$  on two computational models that can be looked upon as abstractions of RAMs. An algebraic computation tree is a rooted tree with outdegree 0, 1, or 2. To each node  $v$  of the tree, a function  $f: R^n \rightarrow R$  is attached. If  $v$  has outdegree 1, then  $f = g_1 \circ g_2$ ,  $o \in \{+, -, *, /\}$ , where  $g_1$  and  $g_2$  are previously computed, that is, attached to some nodes on the path from the root to  $v$ . Furthermore,  $g_1$  or  $g_2$  may be a constant or one of the input variables  $x_1, \dots, x_n$ . If  $v$  has outdegree 2, then an instruction “if  $f(x_1, \dots, x_n) > 0$ , then choose the left branch, else the right branch” is attached to  $v$ , where  $f$  is attached to some node on the path from the root to  $v$ . If  $v$  has outdegree 0, that is, is a leaf, then “accept” or “reject” is attached to  $v$ . The complexity of an ACT is its depth; the recognized language is the set of inputs that choose a path in the tree arriving at an accepting leaf.

A linear search algorithm (LSA) is an ACT in which only the operations “+” and “−” are allowed. In this case the functions attached to the nodes of the tree are linear.

Dobkin and Lipton [4] and Ben Or [2] prove the following general lower bound for LSAs and ACTs.

**THEOREM 1** [2, 4]. *Let  $L \subset R^n$  consist of  $q$ -connected components. Then each LSA (ACT) recognizing  $L$  has complexity at least  $\log(q) (0.38 \log(q) - 0.61n)$ .*

In [4], this theorem is applied to prove an  $\Omega(n^2)$  lower bound for  $L_{n,1}$  by bounding the number of connected components of  $R^n \setminus L_{n,1}$ . Now, in order to obtain a lower bound for  $L_{n,k}$ , we bound the number of connected components of  $R_+^n \setminus L_{n,k}$ , where  $R_+$  denotes the set of nonnegative real numbers. We only consider components in  $R_+^n$  because later we want to prove lower bounds for RAMs that can only work with nonnegative inputs. For  $k = 1$ , a bound for the number of these components is proved in [7].

**LEMMA 2.**  $R_+^{n+1} \setminus L_{n,k}$  has at least

$$\frac{1}{2^n - 1} (k + 1)^{(1/2)n(n-1)}$$

connected components.

Applying this result to Theorem 1 yields the desired lower bounds for  $L_{n,k}$ .

**THEOREM 2.** *Each LSA (ACT) recognizing  $L_{n,k}$  has complexity at least*

$$\frac{1}{2}n(n - 1)\log(k + 1) - n \quad (0.19n(n - 1)\log(k + 1) - 1.61n).$$

It remains to prove Lemma 2.

For this purpose, we generalize the proof from [7] for the case  $k = 1$ .

We first introduce threshold functions. A function  $f: \{0, \dots, k\}^n \rightarrow \{0, 1\}$  is an  $(n, k)$  threshold function if there is  $\bar{a} \in R_+^n$ ,  $b \in R_+$  such that, for every  $\bar{\alpha} \in \{0, \dots, k\}^n$ , it holds that  $\bar{\alpha} \cdot \bar{a} < b$  if  $f(\bar{\alpha}) = 1$  and  $\bar{\alpha} \cdot \bar{a} > b$  if  $f(\bar{\alpha}) = 0$ , where  $\bar{a}$  is the weight vector and  $b$  is the threshold of  $f$ . Let  $N(n, k)$  denote the set of  $(n, k)$  threshold functions. The following two claims prove Lemma 2.

**CLAIM 1.**  $R_+^{n+1} \setminus L_{n,k}$  has  $\#N(n, k)$  connected components.

**CLAIM 2.**  $\#N(n, k) \geq 1/(2^n - 1)(k + 1)^{(1/2)n(n-1)}$ .

**PROOF OF CLAIM 1.** Let  $[k]^n := \{0, \dots, k\}^n \setminus \{\bar{0}\}$ . For  $\bar{\alpha} \in [k]^n$ , let  $H_{\bar{\alpha}}^+(H_{\bar{\alpha}}^{\pm}, H_{\bar{\alpha}}^-)$  denote the linear hyperplane (left, right halfspace)

$$\{(\bar{a}, b), \bar{a} \in R^n, b \in R, \bar{a} \cdot \bar{\alpha} - b = (<, >)0\}$$

in  $R^{n+1}$ . Then,  $L_{n,k} = \bigcup_{\bar{a} \in [k]^n} H_{\bar{a}}^+$  and each connected component of  $R_+^{n+1} \setminus L_{n,k}$  is defined by some  $I \subset [k]^n$  as

$$R_I := \bigcap_{\bar{a} \in I} H_{\bar{a}}^+ \cap \bigcap_{\bar{a} \in [k]^n \setminus I} H_{\bar{a}}^- \cap R_+^{n+1}.$$

Now let  $f$  be an  $(n, k)$  threshold function with weight vector  $\bar{a} \in R_+^n$ , threshold  $b \in R_+$ , and  $I = f^{-1}(\{1\})$ . Then, by the definitions of  $(n, k)$  threshold functions and the set  $R_I$ , we know that  $R_I \neq \emptyset$ , because  $(\bar{a}, b) \in R_I$ . Thus, exactly those  $R_I$  are nonempty, for which the function  $f$ , as above, is an  $(n, k)$  threshold function.  $\square$

PROOF OF CLAIM 2. We proceed by induction on  $n$ .

$n = 1$ :  $f: \{0, \dots, k\} \rightarrow \{0, 1\}$  is a  $(1, k)$  threshold function, iff it is monotonically decreasing and not constant 0. Thus,  $\#N(1, k) = k + 1$ .

$n > 1$ : Let  $g_0, \dots, g_k$  be  $(n - 1, k)$  threshold functions with the same weight vector  $\bar{a} \in R_+^{n-1}$  such that, for some  $b, \epsilon \in R_+$ ,  $g_i$  has threshold  $b + (k - i)\epsilon$ .

Then one easily checks

$$(*) \quad f: \{0, \dots, k\}^n \rightarrow \{0, 1\}$$

with

$$f(a_1, \dots, a_n) = g_{a_n}(a_1, \dots, a_{n-1})$$

is an  $(n, k)$  threshold function with weight vector  $(\bar{a}, \epsilon)$  and threshold  $b + k\epsilon$ .

Now let  $g$  be an  $(n - 1, k)$  threshold function with weight vector  $\bar{a}$  and threshold  $b$ . Then order  $\{0, \dots, k\}^{n-1}$  to a sequence

$$\bar{\alpha}_1, \dots, \bar{\alpha}_r, r = (k + 1)^{n-1},$$

such that

$$\bar{\alpha}_1 \cdot \bar{a} \leq \dots \leq \bar{\alpha}_r \cdot \bar{a}.$$

We may assume without loss of generality that the  $\bar{\alpha}_j \cdot \bar{a}$  are pairwise different. Let  $j_0$  be chosen such that

$$b \in (\bar{\alpha}_{j_0} \cdot \bar{a}, \bar{\alpha}_{j_0+1} \cdot \bar{a}).$$

Now we construct a set  $A_g$  of  $(n, k)$  threshold functions as follows. Let

$$j \in \{1, \dots, j_0\},$$

$$b_j \in (\bar{\alpha}_j \cdot \bar{a}, \bar{\alpha}_{j+1} \cdot \bar{a}), \quad b_{j_0} \leq b, \quad \epsilon = \frac{b - b_j}{k}.$$

For  $i \in \{0, \dots, k\}$ , we now define an  $(n - 1, k)$  threshold function  $g_i$  as follows:

Let  $p$  be chosen such that  $b_j + (k - i)\epsilon \in (\bar{\alpha}_p \cdot \bar{a}, \bar{\alpha}_{p+1} \cdot \bar{a})$ . Then  $g_i(\bar{\alpha}_l) = 1$  for  $l = 1, \dots, p$  and  $g_i(\bar{\alpha}_l) = 0$  for  $l = p + 1, \dots, r$ . Obviously,  $g_i$  is an  $(n - 1, k)$  threshold function with weight vector  $\bar{a}$  and threshold  $b_j + (k - i)\epsilon$ . By (\*), we can now define an  $(n, k)$  threshold function  $f_j$  from  $g_0, \dots, g_k$ . Let  $A_g = \{f_1, \dots, f_{j_0}\}$ . One easily verifies that the  $f_j$ 's are pairwise different, thus  $\#A_g = j_0 = \#g^{-1}(\{1\})$ , and that for different  $(n - 1, k)$  threshold functions  $g$  and  $g'$ ,  $A_g \cap A_{g'} = \emptyset$ . Thus, we have constructed  $A = \sum_{g \in N(n-1,k)} \#g^{-1}(\{1\})$  many  $(n, k)$  threshold functions.

In the same way, we can construct  $B = \sum_{g \in N(n-1,k)} \#g^{-1}(\{0\})$  many  $(n, k)$  threshold functions.

Since  $A + B = \#N(n - 1, k) \cdot (k + 1)^{n-1}$ , we may conclude

$$\begin{aligned} \#N(n, k) &\geq \max\{A, B\} \geq \frac{1}{2} \#N(n - 1, k) \cdot (k + 1)^{n-1} \\ &\geq \frac{1}{2^n - 1} (k + 1)^{(1/2)n(n-1)}. \end{aligned} \quad \square$$

### 3. A General Lower Bound for RAMs

In this section we generalize the proof from [7] for the  $\Omega(n^2)$  lower bound for  $L_{n,1}$  on RAMs. For this purpose we apply a theorem, proved in [7], that describes a method for applying a lower bound argument for LSAs to RAMs, as shown in the last section. The idea of this result is as follows:

A RAM without indirect storage access can almost be looked upon as an LSA that only has to work correctly for nonnegative integer inputs. If we also allow indirect storage access, the result from [7] says that we still can simulate a RAM by an LSA of the same complexity, but this simulation no longer works for all nonnegative integer inputs. For some inputs, namely, those belonging to so-called forbidden hyperplanes, the simulation may go wrong because we have incorrectly simulated an indirect storage access. In the sequel, we denote the set of inputs passing through a node  $v$  of an LSA by  $c(v)$ .

**THEOREM 3 [7].** *Let  $M$  be a RAM accepting some language  $L \subset N^n$  in  $t$  steps. Then there is an LSA  $T_M$ , with complexity  $t$ , that has the following property: For each leaf  $v$  of  $T_M$ , there are hyperplanes  $H_1^v, \dots, H_{2^{t^2}}^v$  in  $R^n$ , the forbidden hyperplanes for  $v$ , such that  $T_M$  simulates  $M$  for all inputs from*

$$\left( c(v) \setminus \bigcup_{i=1}^{2^{t^2}} H_i^v \right) \cap N^n.$$

For each leaf  $v$  of  $T_M$ , each connected component  $c(v) \setminus \bigcup_{i=1}^{2^{t^2}} H_i^v$  is called a characteristic component of  $M$ . Since each such component is a subset of a set  $c(v)$  for some leaf  $v$  of  $T_M$ , it contains either only accepted or only rejected inputs. We now show that the number of characteristic components of  $M$  is not too large.

**LEMMA 3.**  *$M$  has at most  $2^{t+n} \cdot t^{2n}$  characteristic components. They are polytopes.*

**PROOF.** By Lemma 1, we know that for each leaf  $v$  of  $T_M$ ,  $c(v) \setminus \bigcup_{i=1}^{2^{t^2}} H_i^v$  consists of at most  $(2t^2)^n = 2^n t^{2n}$  characteristic components. Since  $T_M$  has at most  $2^t$  leaves,  $M$  has at most  $2^{t+n} t^{2n}$  characteristic components. The second proposition is clear.  $\square$

We now define a class of languages, for which we prove lower bounds.

Let  $H_1, \dots, H_m$  be linear hyperplanes in  $R^n$ , where  $H_j$  is defined by the linear equation

$$\sum_{i=1}^n c_i^j x_i = 0, \quad j = 1, \dots, m.$$

If  $c_i^j, i = 1, \dots, n, j = 1, \dots, m$  are integers from  $\{-k, \dots, k\}$  for some  $k \in N$ , we say that  $L = \bigcup_{i=1}^m H_i$  is defined by hyperplanes with description size  $k$ .

For such languages we show a lower bound similar to that for the LSAs in the last section. But, furthermore, we prove that such a bound already holds for a very restricted input set.

Let  $p, s \in N, \beta_1, \dots, \beta_n \in \{0, \dots, p-1\}$ . Then a set

$$\left( L \cup \prod_{i=1}^n (p \cdot N + \beta_i) \right) \cap \{0, \dots, s\}^n$$

is an  $(L, p, s)$ -set where

$$p \cdot N + \beta_i = \{\beta_i, \beta_i + p, \beta_i + 2p, \dots\}.$$

**THEOREM 4.** *Let  $L \subset R^n$  be defined by hyperplanes with description size  $k$ . Let  $R^n \setminus L$  have  $q$  connected components. Then, each RAM recognizing  $L$  for inputs from an  $(L, s, p)$ -set with  $s = (2k + 1)^{3n^2} \cdot n^{2n^2}$  and  $p \leq 2k$  needs at least  $\log(q) - 2n \log \log(q)$  steps.*

We prove Theorem 4 for input sets that are  $(L, p, s)$ -sets instead of the  $(L, 1, s)$ -set  $\{0, \dots, s\}^n$  only, because, in the next section, we apply it to  $p = 2$  when proving a lower bound for  $L_n$ .

We first prove a lower bound for languages that fulfill certain geometrical properties, as stated in the next lemma. Later, we show that these properties are fulfilled for languages as considered in the theorem.

A hyperplane  $H$  in  $R^n$  has permeability  $r > 0$  if each ball  $B$  on  $H$  with radius  $r$  contains an element from  $Z^n$  on  $H$  ( $Z \hat{=}$  set of integers).

**LEMMA 4.** *Let  $d, r, s \in R_+, p \in N \setminus \{0\}$ . Let  $L = \bigcup_{i=1}^m H_i$ , where  $H_1, \dots, H_m$  are hyperplanes in  $R^n$  with permeability  $r$ . Suppose that  $[0, s]^n \setminus L$  has  $q$  connected components each containing a ball with radius  $d$ . If  $r \geq p \cdot \sqrt{n}$  and  $d \geq q \cdot \log(q)^{2n} \cdot 2^{2n} \cdot (r + 1) \cdot p$ , then each RAM recognizing  $L$  for inputs from an  $(L, p, s)$ -set has complexity of at least  $\log(q) - n \log \log(q)$ .*

**PROOF.** Let  $M$  be a RAM recognizing  $L$  in  $t$  steps. We first assume that the following property holds:

(\*) For each connected component  $P$  of  $[0, s]^n \setminus L$ , there is a characteristic component  $Q(P)$  of  $M$  such that  $P \cap Q(P)$  contains a ball with radius  $r$ .

In this case we show that the  $Q(P)$ 's are pairwise different. Let  $I$  be an  $(L, p, s)$ -set. Suppose that for two different connected components  $P_1$  and  $P_2$ ,  $Q(P_1) = Q(P_2) = Q$ . Then  $Q \cap P_1$  and  $Q \cap P_2$  contain balls  $B_1$  and  $B_2$  with radius  $r$ . Since  $r \geq p \cdot \sqrt{n}$ ,  $Q$  contains elements from  $I \setminus L$  and thus  $Q$  is rejecting.

Now, let  $H_i$  be a hyperplane from  $H_1, \dots, H_m$  that separates  $P_1$  from  $P_2$ . Since  $Q$  is convex and contains a ball with radius  $r$  on both sides of  $H_i$ , it also contains an  $((n - 1)$ -dimensional) ball with radius  $r$  on  $H$ . But, by the definition of permeability, this ball contains an element from  $Z^n$  and, thus, from  $I \cap L$ . This contradicts the fact, shown above, that  $Q$  is rejecting.

Thus, we have proved that  $M$  has at least  $q$  characteristic components. By Lemma 3, we may conclude  $2^{t+n} \cdot t^{2n} \geq q$ , which proves the lemma for the case that (\*) holds.

Now we suppose that (\*) does not hold. Let  $P$  be a connected component of  $[0, s]^n \setminus L$  such that for each characteristic component  $Q$  of  $M$ ,  $Q \cap P$  has an inner radius smaller than  $r$ . Let  $B$  be a ball of radius  $d$  contained in  $P$ . Then, the following three properties hold:

- (i)  $\#(I \cap B) \geq (d/(\sqrt{n} \cdot p))^n$ .
- (ii)  $\#(I \cap B \cap Q) \leq r \cdot (n + 1) \cdot (d/p)^{n-1}$ .
- (iii)  $\#(I \cap B \cap H) \leq (d/p)^{n-1}$  for every hyperplane  $H$  in  $R^n$ .

(i) and (iii) follow by elementary geometrical considerations. In order to prove (ii), we apply a theorem from Blaschke [3] that says that the thickness of a convex polytope  $S$  in  $R^n$ , that is, the minimum distance of two parallel hyperplanes between which  $S$  lies, is at most  $(n + 1) \cdot (\text{inner radius of } S)$ . Thus,  $Q$  has thickness at most  $r \cdot (n + 1)$ , which implies (ii).

We now assume that  $t \leq \log(q)$ . Then, the whole number of forbidden hyperplanes in  $T_M$  is at most  $2^t \cdot 2t^2 \leq q \cdot 2 \log(q)^2$ . Thus, by (iii), they together contain

at most  $X_1 = q \cdot 2 \log(q)^2 \cdot (d/p)^{n-1}$  elements from  $I \cap B$ . Furthermore, we know by Lemma 3, that  $M$  has at most  $2^{t+n} \cdot t^{2n} \leq q \cdot 2^n \cdot \log(q)^{2n}$  characteristic sets.

By (ii), together they contain at most

$$X_2 = q \cdot 2^n \cdot \log(q)^{2n} \cdot r \cdot (n + 1) \cdot \left(\frac{d}{p}\right)^{n-1}$$

elements from  $I \cap B$ . Since the characteristic sets of  $M$  and the forbidden hyperplanes must contain  $I \cap B$ , we obtain

$$X_1 + X_2 \geq \#(I \cap B).$$

Applying (i) and a rough estimation yields

$$q \cdot 2^n \cdot \log(q)^{2n} \cdot (r + 1) \cdot (n + 1) \cdot \left(\frac{d}{p}\right)^{n-1} > X_1 + X_2 \geq \left(\frac{d}{\sqrt{n} \cdot p}\right)^n.$$

Solving this inequality shows

$$d < q \cdot 2^{2n} \cdot \log(q)^{2n} \cdot (r + 1) \cdot p,$$

which contradicts the bound for  $d$  from the lemma. Thus  $t > \log(q)$ , and the lemma follows.  $\square$

In order to conclude Theorem 4 from Lemma 4, we have to bound the parameters  $d, r, s$  in terms of the description size of the linear hyperplanes defining  $L$ .

LEMMA 5. *Let  $L = \bigcup_{i=1}^m H_i$  be defined by linear hyperplanes in  $R^n$  with description size  $k$ . Then the following holds:*

- (i) *Let  $s \in R_+$ . Then each connected component of  $[0, s]^n \setminus L$  has inner radius at least  $(k^{2n^2} \cdot n^{n^2})^{-1} \cdot s$ .*
- (ii) *Each  $H_i$  has permeability  $2k\sqrt{n}$ .*

PROOF. It suffices to prove (i) for  $s = 1$ , because the inner radius of a component of  $[0, s]^n \setminus L$  grows linearly with  $s$ . For  $s = 1$ , each component is a convex polytope defined by a system of linear inequalities with integer coefficients from  $\{-k, \dots, k\}$ . For such polytopes, the desired bound for the inner radius is proved in [10].

In order to prove (ii), let  $H_i$  be defined by the equation

$$\sum_{j=1}^n c_j x_j = 0, \quad c_1, \dots, c_n \in \{-k, \dots, k\}.$$

Then the  $(n - 1)$  vectors

$$\begin{aligned} \bar{y}_1 &= (c_2, -c_1, 0, \dots, 0), \\ \bar{y}_2 &= (0, c_3, -c_2, 0, \dots, 0), \\ &\vdots \\ \bar{y}_{n-1} &= (0, \dots, 0, c_n, -c_{n-1}) \end{aligned}$$

form a basis of  $H_i$ .

Let  $S$  be the set  $\{\sum_{i=1}^{n-1} \alpha_i \bar{y}_i, \alpha_1, \dots, \alpha_{n-1} \in Z\}$ . Then,  $S \subset Z^n$ , because the  $\bar{y}_i$ 's have integer coefficients. Now let  $B$  be a ball on  $H_i$  with radius  $2k\sqrt{n}$  and center  $\bar{x} \in H$ . Then, there is a (unique)  $\bar{y} \in S$  such that  $\bar{x}$  belongs to the convex hull of

the set

$$\left\{ \bar{y} + \sum_{i=1}^{n-1} \alpha_i \bar{y}_i, \alpha_1, \dots, \alpha_{n-1} \in \{0, 1\} \right\}.$$

For some  $\bar{z} \in R^n$  let  $|\bar{z}|$  denote its Euclidean length. Then, for each

$$(\alpha_1, \dots, \alpha_{n-1}) \in \{0, 1\}^{n-1}, \quad \left| \sum_{i=1}^{n-1} \alpha_i \bar{y}_i \right| \leq \sqrt{n} \cdot 2k,$$

because the  $i$ th coefficient of  $\sum_{i=1}^{n-1} \alpha_i \bar{y}_i$  is either  $(-c_{i-1})$  or  $(c_{i+1})$  or  $(-c_{i-1} + c_{i+1})$  or 0; thus, its absolute value is at most  $2k$ , which implies the above bound for the length of  $\sum_{i=1}^{n-1} \alpha_i \bar{y}_i$ .

Now we may conclude that  $|\bar{x} - \bar{y}| \leq \sqrt{n}2k$  and therefore  $\bar{y} \in B$ , which proves (ii).  $\square$

Now we can prove Theorem 4. Since there are only  $(2k + 1)^n - 1$  linear hyperplanes with description size  $k$ , the set  $R^n \setminus L$  from Theorem 4 has at most  $(2k + 1)^{n^2}$  connected components by Lemma 1. Inserting this bound for  $q$ , the bound for  $s$  from Theorem 4 and the bounds for  $d$  and  $r$  from Lemma 5 in the bounds for  $r$  and  $d$  in Lemma 3 yield Theorem 4.

#### 4. Lower Bounds for $L_{n,k}$ and $L_n$ on RAMs.

In this section, we apply Theorem 4 to  $L_{n,k}$  and  $L_n$ .

**THEOREM 5.** *Each RAM recognizing  $L_{n,k}$  needs at least  $\frac{1}{2}n(n - 1)\log(k + 1) - n$  steps for inputs from*

$$\{0, \dots, (2k + 1)^{3(n+1)^2} \cdot (n + 1)^{2(n+1)^2}\}^n.$$

**PROOF.**  $L_{n,k}$  is defined by hyperplanes with description size  $k$ , and  $R^{n+1} \setminus L_{n,k}$  has at least  $1/(2^n - 1) \cdot (k + 1)^{(1/2)n(n-1)}$  connected components by Lemma 2. Thus, we obtain Theorem 5 from Theorem 4 with the  $(L, 1, s)$ -set  $\{0, \dots, s\}^n$ .  $\square$

**THEOREM 6.** *Each RAM recognizing  $L_n$  needs at least  $\frac{1}{2}n(n - 1)\log(k + 1) - n$  steps for inputs from*

$$\{0, \dots, 2 \cdot (2k + 1)^{3(n+1)^2} \cdot (n + 1)^{2(n+1)^2}\}^n.$$

**PROOF.** We define an  $(L, 2, s)$ -set  $I$ , such that, for each  $\bar{x} \in I$ , it holds that  $\bar{x} \in L_n$  iff  $\bar{x} \in L_{n,k}$ . If we can find such an  $I$ , we obtain Theorem 6 from Theorem 4 and Lemma 2.

Let

$$I = \left\{ L_{n,k} \cup \left( \prod_{x=1}^n 2N \right) \times (2N + 1) \right\} \cap \{0, \dots, s\}^n.$$

This set contains all the inputs  $\{a_1, \dots, a_n, b\} \in \{0, \dots, s\}^n$  for which the equation  $\sum_{i=1}^n a_i x_i = b$  either has a solution in  $\{0, \dots, k\}^n$  or consists of even numbers  $a_1, \dots, a_n$  and an odd number  $b$ . Thus, in this case, there is no solution in  $N^n$ , because for each  $(x_1, \dots, x_n) \in N^n$ ,  $\sum_{i=1}^n a_i x_i$  is even, whereas  $b$  is odd.

Thus, we may conclude: Each RAM recognizing  $L_n$  for inputs from  $I$  recognizes  $L_{n,k}$  for inputs from  $I$ , and therefore we may apply Theorem 4 as in the proof of Theorem 5 and obtain Theorem 6.  $\square$

## REFERENCES

1. AHO, A., HOPCROFT, J. E., AND ULLMANN, J. D. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Mass., 1974.
2. BEN OR, M. Lower bounds for algebraic computation trees. In *Proceedings of the 15th Annual ACM Symposium on the Theory of Computing*. (Boston, Mass., Apr. 25–27). ACM, New York, 1983, pp. 80–86.
3. BLASCHKE, W. Über den größten Kreis in einer konvexen Punktmenge. *Jahresbericht der Deutschen Mathematiker Vereinigung* 23 (1914), 369–374.
4. DOBKIN, D., AND LIPTON, R. A lower bound of  $\frac{1}{2}n^2$  on linear search programs for the knapsack problem. *J. Comput. Syst. Sci.* 16 (1975), 417–421.
5. GARY, M. R., AND JOHNSON, D. S. *Computers and Intractability. A Guide to the Theory of NP-Completeness*. Freeman and Company, San Francisco, Calif., 1979.
6. KANNAN, R. Improved algorithms for integer programming and related problems. In *Proceedings of the 15th Annual ACM Symposium on the Theory of Computing*. (Boston, Mass., Apr. 25–27). ACM, New York, 1983, pp. 193–206.
7. KLEIN, P., AND MEYER AUF DER HEIDE, F. A lower time bound for the knapsack problem on random access machines. *Acta Inf.* 19 (1983), 385–395.
8. LAUTEMANN, C., AND MEYER AUF DER HEIDE, F. Lower time bounds for integer programming with two variables. *Inf. Proc. Lett.*, to appear.
9. LENSTRA, H. W. Integer programming with a fixed number of variables. Rep. 81-03, Mathematisch Instituut, Universiteit Amsterdam, Amsterdam, The Netherlands, 1981.
10. MEYER AUF DER HEIDE, F. A polynomial linear search algorithm for the  $n$ -dimensional knapsack problem. *J. ACM* 31, 3 (July 1984), 668–676.

RECEIVED JUNE 1984; REVISED MARCH 1985; ACCEPTED APRIL 1985