Complexity and Dimension

Felipe Cucker
City University of Hong Kong[1]
e-mail: macucker@sobolev.cityu.edu.hk

Pascal Koiran
LIP, École Normale Superieure[2]
e-mail: koiran@lip.ens-lyon.fr

Martín Matamala
Universidad de Chile[3]
mmatamal@dim.uchile.cl

NeuroCOLT Technical Report Series

NC-TR-96-051

October 1996[4]

Produced as part of the ESPRIT Working Group
in Neural and Computational Learning,
NeuroCOLT 8556

NeuroCOLT Coordinating Partner

Royal Holloway
University of London

Department of Computer Science
Egham, Surrey TW20 0EX, England

For more information contact John Shawe-Taylor at the above address
or email neurocolt@dcs.rhbnc.ac.uk

[1]Dept. of Mathematics, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon HONG KONG

[2]LIP, École Normale Superieure, 46, Allée d'Italie, Lyon 69364, FRANCE

[3]Depto. de Ingeniería Matemática, Universidad de Chile, Beaucheff 850, Casilla 170-3, Santiago, CHILE

[4]Received August 29, 1996

Keywords: algebraic decision trees – sparse sets – computational complexity.

1 Introduction

In 1977 Berman and Hartmanis ([1]) conjectured that all NP-complete sets are polynomially isomorphic. Should this conjecture be proved, we would have as a consequence that no "small" NP-complete set exists in a precise sense of the word "small".

Denote by Σ the set $\{0,1\}$ and by Σ^* the set of all finite sequences of elements in Σ. A set $S \subseteq \Sigma^*$ is said to be *sparse* when there is a polynomial p such that for all $n \in \mathbb{N}$ the subset S_n of all elements in S having size n has cardinality at most $p(n)$. If the Berman-Hartmanis conjecture is true, then there are no sparse NP-complete sets.

In 1982 Mahaney ([5]) proved this weaker conjecture showing that there exist sparse NP-hard sets if and only if $P = NP$.

In a different line of research, Blum, Shub and Smale introduced in 1989 a theory of computability and complexity over the reals [2] to describe the kind of computation done in numerical analysis. The computational model defined in [2] deals with real numbers as basic entities, and performs the arithmetic operations on them as well as sign tests at unit cost. Inputs and outputs are vectors of real numbers and decision problems are subsets of $\mathbb{R}^\infty$, the disjoint union of $\mathbb{R}^n$ for all $n \geq 1$. The classes $P_{\mathbb{R}}$ and $NP_{\mathbb{R}}$ —which are analogous to the well known classes P and NP— are defined in [2] and one of the main results there is the existence of natural $NP_{\mathbb{R}}$-complete problems.

In order to solve some problems such as the real valued generalizations of the Traveling Salesman or the Knapsack problems, it seems that multiplication and division are of little help. It makes sense then to consider machines similar to those defined in [2] which only make additions and subtractions. These machines, called *additive*, and some complexity classes defined by their means, where studied in [4, 3]. A similar model, in which multiplication by constants is also allowed, is studied in [6].

Mahaney's argument can be applied here to show that in the additive model, $P^{=}_{\mathrm{add}} = NP^{=}_{\mathrm{add}}$ if and only if there are $NP^{=}_{\mathrm{add}}$-hard sets which are sparse in the sense defined above. This remains true in more powerful models for *digital* non-determinism (this is a weak form of non-determinism where guesses are required to be boolean sequences [4, 3]). However, one can conjecture that a stronger result holds. All the examples of $NP^{=}_{\mathrm{add}}$-complete sets S we know are "large" in a stronger sense: their restriction to $\mathbb{R}^n$ has dimension "close" to n (this is also true in the original BSS model with multiplication).

In this note we define a notion of sparseness for subsets of $\mathbb{R}^\infty$ which relies on this observation and we prove that there are no sparse $NP^{=}_{\mathrm{add}}$-hard sets. Here we deal with additive machines which branch on equality tests of the form $x = y$ and $NP^{=}_{\mathrm{add}}$ denotes the corresponding class of sets decidable in nondeterministic polynomial time. Note that this result implies the separation $P^{=}_{\mathrm{add}} \neq NP^{=}_{\mathrm{add}}$ already known from [4, 6] (because $P^{=}_{\mathrm{add}}$ obviously contains sparse sets).

2 The main result

We denote by $\mathbb{R}^\infty$ the disjoint union $\bigsqcup_{n=1}^{\infty} \mathbb{R}^n$. If $x \in \mathbb{R}^n$ we define the *size* $|x|$ of x to be n. If S is any subset of $\mathbb{R}^\infty$ we denote by S_n the subset of S of points with size n.

In what follows we shall deal in with additive machines, i.e. machines which do not multiply or divide. Moreover, we shall only consider machines which branch on equality tests. Then $P^{=}_{\text{add}}$ and $NP^{=}_{\text{add}}$ are defined to be the classes of sets decided by these machines in deterministic and nondeterministic polynomial time respectively. The main properties of these machines and complexity classes can be found in [4].

In the proof of our main result, we find it convenient to deal with linear decision trees rather than additive machines (hence we actually prove a slightly stronger result than stated since the former model is non-uniform). We recall that a *linear decision tree* is a binary tree whose internal nodes are labeled by non-constant affine function $l : \mathbb{R}^n \to \mathbb{R}$, where n is the dimension of the input space. At a given node, an input $x \in \mathbb{R}^n$ goes to the left child if $l(x) = 0$ and to the right child if $l(x) \neq 0$. Since our machines compute reductions, we assume that each leaf is labeled by an affine function $l : \mathbb{R}^n \to \mathbb{R}^s$, where s is the dimension of the output space. Let γ be a path from the root to a leaf. The affine function labeling that leaf will be called the *function computed along* γ.

Linear decision trees are closely related with additive machines in the following sense. For any additive machine M with running time bounded by a function t, and any positive integer n, there is a linear decision tree T_n of depth at most $t(n)$ which computes the same function as M for inputs in $\mathbb{R}^n$.

Definition 1 Let $S \subseteq \mathbb{R}^\infty$. We will say that S is *sparse* if there are positive integers c, d such that for all $n \geq 2$ the set S_n has topological dimension bounded by $c(\log n)^d$.

We recall that the *Knapsack Problem* over the reals is the set

$$\text{KP} = \{x \in \mathbb{R}^\infty \mid \exists b_1, \ldots, b_n \in \{0,1\}\ b_1x_1 + \ldots + b_nx_n = 1 \ \textit{where}\ n = |x|\}.$$

It is proved in [4] that KP does not belong to $P^{=}_{\text{add}}$. Since KP belongs to $NP^{=}_{\text{add}}$ it follows that $P^{=}_{\text{add}} \neq NP^{=}_{\text{add}}$.

For each $n \in \mathbb{N}$, the set KP_n is the union of $2^n - 1$ hyperplanes in $\mathbb{R}^n$. We shall denote this set of hyperplanes by $\mathcal{H}(\text{KP}_n)$. Given an hyperplane $h \subseteq \mathbb{R}^n$, $\widehat{h}$ denotes the linear variety associated to h (i.e., $\widehat{h}$ is parallel to h and contains the origin). Denote also by $\mathcal{L}(\text{KP}_n)$ the set $\{\widehat{h};\ h \in \mathcal{H}(\text{KP}_n)\}$.

Lemma 1 *Let $v \in \mathbb{R}^n$, $v \neq 0$. Then there are at least 2^{n-1} hyperplanes H in $\mathcal{L}(KP_n)$ such that $v \notin H$.*

Proof. Let $v = (v_1, \ldots, v_n)$ and assume for instance that $v_n \neq 0$. Consider now a point $(b_1, \ldots, b_{n-1}) \in \{0,1\}^{n-1}$. If $b_1v_1 + \ldots + b_{n-1}v_{n-1} = 0$ then the hyperplane given by the equation

$$b_1X_1 + \ldots + b_{n-1}X_{n-1} + X_n = 0$$

does not contain v. Else, if $b_1v_1 + \ldots + b_{n-1}v_{n-1} \neq 0$ then the hyperplane

$$b_1X_1 + \ldots + b_{n-1}X_{n-1} = 0$$

does not contain v. We thus see that each one of the 2^{n-1} points in $\{0,1\}^{n-1}$ gives rise to a hyperplane in $\mathcal{L}(\mathrm{KP}_n)$ not containing v. □

Proposition 1 *Let $S \subseteq \mathbb{R}^\infty$ and $\varphi : \mathbb{R}^\infty \to \mathbb{R}^\infty$ be a polynomial time reduction from* KP *to S. Then there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$*

(1) $\dim \varphi(KP_n) = n - 1$

(2) $\dim \varphi(\mathbb{R}^n - KP_n) = n$.

Proof. Let p be a polynomial which bounds the time needed to compute φ and consider $n_0 \in \mathbb{N}$ such that $2^n > 2p(n)$ for all $n \geq n_0$.

Consider an integer $n \geq n_0$. The computation of φ over inputs of size n can be done by a linear decision tree T of depth at most $p(n)$. Let γ be the canonical path of T, that is, the path having all tests answered with $\neq$.

The set X_γ of points in $\mathbb{R}^n$ which follow γ is an open set in $\mathbb{R}^n$. Its complement A is the union of at most $p(n)$ hyperplanes. Denote by l the affine function computed along the path γ, $l : \mathbb{R}^n \to \mathbb{R}^m$ for some $m \leq p(n)$. We then have that $l_{|X_\gamma} = \varphi_{|X_\gamma}$. In the sequel L denotes the linear part of l.

Let $\mathcal{H}(A)$ be the set of hyperplanes of $\mathcal{H}(\mathrm{KP}_n)$ not included in A. Since A contains at most $p(n)$ hyperplanes and $2^n > 2p(n)$ it follows that $\mathcal{H}(A)$ contains more than 2^{n-1} hyperplanes.

We will now show that L is injective. Denote by q the dimension of $\ker L$ and suppose that $q \geq 1$.

Consider H a hyperplane through the origin not containing $\ker L$. Then $\dim(H \cap \ker L) = q - 1$ and thus $\dim \ker L_{|H} = q - 1$. This implies

$$\dim L(H) = n - 1 - (q - 1) = n - q = \dim L(\mathbb{R}^n).$$

Therefore, $L(H) = L(\mathbb{R}^n)$. Since $\mathcal{H}(A)$ contains more than 2^{n-1} hyperplanes by Lemma 1 there exists $h \in \mathcal{H}(A)$ such that $\widehat{h}$ does not contain $\ker L$. We conclude that $L(h) = L(\widehat{h}) = L(\mathbb{R}^n)$.

Now, since $\mathbb{R}^n - \{A \cup \mathrm{KP}_n\}$ is an open set in $\mathbb{R}^n$ and L is open in its image, we deduce that $L(\mathbb{R}^n - \{A \cup \mathrm{KP}_n\})$ is open in $L(\mathbb{R}^n)$. Moreover, by continuity

$$L(\overline{h - A}) \subseteq \overline{L(h - A)}$$

where the bar denote topological closure. But $\overline{h - A} = h$ and $L(h) = L(\mathbb{R}^n)$ from which we deduce that $L(h - A)$ is dense in $L(\mathbb{R}^n)$. This implies that

$$L(\mathbb{R}^n - \{A \cup \mathrm{KP}_n\}) \cap L(h - A) \neq \emptyset.$$

Let a be a point in this intersection and $x \in \mathbb{R}^n - \{A \cup \mathrm{KP}_n\}$, $y \in h - A$ such that $L(x) = L(y) = a$. Since x and y are both in X_γ it follows that $\varphi(x) = \varphi(y)$ but this is in contradiction with the fact that $x \notin \mathrm{KP}_n$ and $y \in \mathrm{KP}_n$. This proves that $\dim \ker L = 0$ that is, that L is injective. Both (1) and (2) trivially follows. □

Corollary 1 *There are no $NP^{=}_{\text{add}}$-hard nor co$NP^{=}_{\text{add}}$-hard sparse sets.*

PROOF. Suppose S is $NP^{=}_{\text{add}}$-hard. Then KP reduces in polynomial time to S. By (1) of the preceding proposition we know that there is an $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$, the set $S_{p(n)}$ has dimension $n-1$ where p is a polynomial which bounds the running time of the reduction. Therefore, S can not be sparse.

Using (2) of the proposition above instead of (1) we prove in the same way that S can not be sparse if it is co$NP^{=}_{\text{add}}$-hard. $\square$

3 Final Remarks

The result of Corollary 1 still holds in some related settings. This is the case for instance if we consider linear machines instead of additive, that is, machines which can also multiply by constants. This is also the case for machines over the complex numbers $\mathbb{C}$.

A question left open in this note is whether a similar result holds in the case in which branching over inequalities is also allowed. Denote by $P^{<}_{\text{add}}$ and $NP^{<}_{\text{add}}$ the corresponding classes for deterministic and nondeterministic polynomial time respectively. Then it is unlikely to easily get a version of Corollary 1 for $NP^{<}_{\text{add}}$ since this would imply as a consequence the inequality $P^{<}_{\text{add}} \neq NP^{<}_{\text{add}}$. The question we leave open has rather the form of Mahaney's theorem: is it true that there are no sparse $NP^{<}_{\text{add}}$-hard sets, assuming that $P^{<}_{\text{add}} \neq NP^{<}_{\text{add}}$?

This question also remains open in the general case in which multiplications and divisions are also allowed.

References

[1] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM J. on Computing*, 6:305–322, 1977.

[2] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. American Mathematical Society*, 21:1–46, 1989.

[3] F. Cucker and P. Koiran. Computing over the reals with addition and order: higher complexity classes. *Journal of Complexity*, 11:358–376, 1995.

[4] P. Koiran. Computing over the reals with addition and order. *Theoretical Computer Science*, 133:35–47, 1994.

[5] S.R. Mahaney. Sparse complete sets for NP: solution of a conjecture by Berman and Hartmanis. *J. of Computer and System Sciences*, 25:130–143, 1982.

[6] K. Meer. A note on a $P \neq NP$ result for a restricted class of real machines. *Journal of Complexity*, 8:451–453, 1992.