There are no sparse NP_W-hard Sets

Felipe Cucker*
Department of Mathematics
City University of Hong Kong
83 Tat Chee Avenue, Kowloon
HONG KONG
e-mail: macucker@math.cityu.edu.hk

Dima Grigoriev
IMR
Université de Rennes I
Campus de Beaulieu, Rennes 35042
FRANCE
e-mail: dima@maths.univ-rennes1.fr

Abstract. In this paper we prove that, in the context of weak machines over $\mathbb{R}$, there are no sparse NP-hard sets.

1 Introduction

In [1977] Berman and Hartmanis conjectured that all NP-complete sets are polynomially isomorphic. That is, that for all NP-complete sets A and B, there exists a bijection $\varphi : \Sigma^* \to \Sigma^*$ such that $x \in A$ if and only if $\varphi(x) \in B$. In addition both φ and its inverse are computable in polynomial time. Here Σ denotes the set $\{0, 1\}$ and Σ^* the set of all finite sequences of elements in Σ.

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". 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.

*Partially supported by CERG grant 9040393.

In 1982 Mahaney ([Mahaney 1982]) proved this weaker conjecture showing that there exist sparse NP-hard sets if and only if P = NP. After this, a whole stream of reserach developed around the issue of reductions to "small" sets (see [Arvind, Han, Hemachandra, Köbler, Lozano, Mundhenk, Ogiwara, Schöning, Silvestri, and Thierauf 1993]).

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

Clearly, the sparseness notion defined above for sets over $\{0,1\}$ will not define any meaningful class over $\mathbb{R}$ since now the set of inputs of size n is $\mathbb{R}^n$ and this is an infinite set. A notion of sparseness over $\mathbb{R}$ capturing the main features of the discrete one (independence of any kind of computability notion and capture of a notion of "smallness"), however, was proposed in [Cucker, Koiran, and Matamala 1997]. Let $S \subseteq \mathbb{R}^\infty$. We say that S is *sparse* if, for all $n \geq 1$, the set

$$S_n = \{x \in S \mid x \in \mathbb{R}^n\}$$

has dimension at most $\log^q n$ for some fixed q. Here dimension is the dimension, in the sense of algebraic geometry, of the Zariski closure of S_n. Note that this notion of sparseness parallels the discrete one in a very precise way. For a subset $S_n \subseteq \{0,1\}^n$ its cardinality gives a measure of its size and a sparse set is one for which, for all n, this cardinality is polylogarithmic in the largest possible (i.e. 2^n the cardinality of $\{0,1\}^n$). For a subset $S_n \subseteq \mathbb{R}^n$, we take the dimension to measure the size of S_n, and again define sparseness by the property of having this measure polylogarithmic in the largest possible (which is now n, the dimension of $\mathbb{R}^n$).

Using this definition of sparseness for subsets of $\mathbb{R}^\infty$ the main result of [Cucker, Koiran, and Matamala 1997] proves that there are no sparse NP-complete sets in the context of machines over $\mathbb{R}$ which do not perform multiplications or divisions and branch on equality tests only. Note that this result is not conditioned to the inequality $\mathrm{P} \neq \mathrm{NP}$ since this inequality is known to be true in this setting (cf. [Meer 1992]).

A variation on the BSS model attempting to get closer to the Turing machine (in the sense that iterated multiplication is somehow penalized) was introduced by Koiran in [1997]. This model, which Koiran called *weak*, takes inputs from $\mathbb{R}^\infty$ but no longer measures the cost of the computation as the number of arithmetic operations performed by the machine. Instead, the cost of each individual operation $x \circ y$ depends on the sequences of operations which lead to the terms x and y from the input data and the machine constants.

In this paper we extend Mahaney's theorem to machines over $\mathbb{R}$ endowed with the weak cost. Again, this is not a conditional result since it is known that $\mathrm{P} \neq \mathrm{NP}$ in this context too (cf. [Cucker, Shub, and Smale 1994]). If NP_W denotes the class of sets decided in non-deterministic polynomial cost, our main result is the following.

Theorem 1 *There are no sparse* NP_W*-hard sets.*

2 The weak cost

Let M be a machine over $\mathbb{R}$, let $\alpha_1, \ldots, \alpha_s$ be its constants and $a = (\alpha_1, \ldots, \alpha_s) \in \mathbb{R}^s$. Let $x = (x_1, \ldots, x_n) \in \mathbb{R}^\infty$. At any step ν of the computation of M with input x, the intermediate value $z \in \mathbb{R}$ produced in this step can be written as a rational function of a and x, $z = \varphi(a, x)$. This rational function only depends on the computation path followed by M up to ν (i.e. on the sequence steps previously performed by M) and is actually a coordinate of the composition of the arithmetic operations performed along this path (see [Blum, Cucker, Shub, and Smale 1998] for details). Let $\varphi = \frac{g_\nu}{h_\nu}$ be the representation of φ obtained by retaining numerators and denominators in this composition. For example, the representation of the product $\frac{g}{h} \cdot \frac{r}{s}$ is always $\frac{gr}{hs}$ and the one of the addition $\frac{g}{h} + \frac{r}{s}$ always $\frac{gs+hr}{hs}$. We will now use g_ν and h_ν to define weak cost.

Definition 1 The *weak cost* of any step ν is defined to be the maximum of $\deg(g_\nu)$, $\deg(h_\nu)$, and the maximum bit size of the coefficients of g_ν and h_ν. For any $x \in \mathbb{R}^\infty$ the *weak cost of M on x* is defined to be the sum of the costs of the steps performed by M with input x.

The class $\mathrm{P_W}$ of sets decided within *weak polynomial cost* is now defined by requiring that for each input of size n the weak cost of its computation is bounded by a polynomial in n. A set S is decided in *weak nondeterministic polynomial cost* (we write $S \in \mathrm{NP}_W$) if there is a machine M working within weak polynomial cost satisfying the following: for each $x \in \mathbb{R}^\infty$, $x \in S$ if and only if there is $y \in \mathbb{R}^\infty$ with size polynomial in n such that M accepts the pair (x, y).

Remark 1 The definitions above do not fully coincide with those given in [Koiran 1997] since this reference requires the representation of the rational functions φ above to be relatively prime. The definitions we give here, which are taken from [Blum, Cucker, Shub, and Smale 1998], are essentially equivalent. For, if a set is in $\mathrm{P_W}$ with the definition above, it is clearly in $\mathrm{P_W}$ with Koiran's. The converse is more involved to prove. Roughly speaking, any machine can be simulated by another which keeps "programs" instead of performing the arithmetic operations at the computation nodes. When the computation reaches a branch node the program for the register whose value is tested for positivity is evaluated at the pair (a, x) to decide such positivity. Now note that one can use algorithms of symbolic computation to make the numerator and denominator of the rational function computed by the program relatively prime *before* evaluating.

3 Proof of the main result

Let $n \geq 1$. Consider the polynomial

$$f_n = x_1^{2^n} + \ldots + x_n^{2^n} - 1$$

and let $C_n = \{x \in \mathbb{R}^n \mid f_n(x) = 0\}$. The polynomial f_n is irreducible and the dimension of C_n is $n - 1$. Let $C \subset \mathbb{R}^\infty$ be given by $C = \cup C_n$. We know (cf. [Cucker, Shub, and Smale 1994]) that $C \in \mathrm{NP_W}$ but $C \notin \mathrm{P_W}$.

Let $S \subset \mathbb{R}^\infty$ be a NP_W-hard set. Then C reduces to S. That is, there exists a function $\varphi : \mathbb{R}^\infty \to \mathbb{R}^\infty$ computable with polynomial cost such that, for all $x \in \mathbb{R}^\infty$, $x \in C \iff \varphi(x) \in S$. For each $n \geq 1$, the restriction of φ to $\mathbb{R}^n$ is a piecewise rational function. Our first result, Proposition 2, gives some properties of this function. It uses the following simple fact in real algebraic geometry whose proof can be found in Chapter 19 of [Blum, Cucker, Shub, and Smale 1998].

Proposition 1 *Let $f \in \mathbb{R}[x_1, \ldots, x_n]$ be an irreducible polynomial such that the dimension of its zero set $\mathcal{Z}(f) \subseteq \mathbb{R}^n$ is $n - 1$. Then, for any polynomial $g \in \mathbb{R}[x_1, \ldots, x_n]$, g vanishes on $\mathcal{Z}(f)$ if and only if g is a multiple of f.* $\square$

Proposition 2 *Let n be sufficiently large. There exist $x \in C_n$ and $U \subset \mathbb{R}^n$ an open ball centered at x such that the restriction of φ to U is a rational map $h : U \to \mathbb{R}^m$ for some m bounded by a polynomial in n. In addition, if $h_1, \ldots, h_m$ are the coordinates of h, then the degrees of the numerator and denominator of h_i are also bounded by a polynomial in n for $i = 1, \ldots, m$.*

PROOF. Let M be a machine computing φ within weak polynomial cost. By unwinding the computation of M in a standard manner we obtain an algebraic computation tree of depth polynomial in n. To each branch η in this tree one associates a set $D_\eta \subseteq \mathbb{R}^n$ such that the D_η partition $\mathbb{R}^n$ (i.e. $\cup D_\eta = \mathbb{R}^n$ and $D_\eta \cap D_\gamma = \emptyset$ for $\eta \neq \gamma$). In addition, each branch η computes a rational map h_η and $\varphi_{|D_\eta} = h_\eta$. The set D_η is the set of points in $\mathbb{R}^n$ satisfying a system

$$\bigwedge_{i=1}^{s_\eta} q_i(x_1, \ldots, x_n) \geq 0 \wedge \bigwedge_{i=s_\eta+1}^{t_\eta} q_i(x_1, \ldots, x_n) < 0 \tag{1}$$

where the $q_i(X_1, \ldots, X_n)$ are the rational functions tested along the branch. Since M works within weak cost, the numerators and denominators of the q_i as well as those of h_η have degrees bounded by a polynomial in n.

Everything we need now to see is that for some branch η, D_η contains an open neighbourhood of a point $x \in C_n$.

To do so first notice that, by replacing each q_i by the product of its numerator and denominator, we can assume that the q_i are polynomials. Also, by writing $q_i \geq 0$ as $q_i = 0 \vee q_i > 0$ and distributing the disjunctions in (1) we can express D_η as a finite union of sets satisfying a system

$$\bigwedge_{i=1}^{s} q_i(x_1, \ldots, x_n) = 0 \wedge \bigwedge_{i=s+1}^{t} q_i(x_1, \ldots, x_n) < 0. \tag{2}$$

We have thus described $\mathbb{R}^n$ as a union of sets which are solutions of systems like (2). Since this union is finite there exists one such set D containing a subset H of C_n of dimension $n-1$. Let D be the solution of a system like (2). We claim that there are no equalities in such system. Assume the contrary. Then there is a polynomial q such that $H \subset \mathcal{Z}(q)$. Since $\dim H = n-1$ and C_n is irreducible this implies that $q(C_n) = 0$ and, by Proposition 1, that q is a multiple of f_n. Since $\deg f_n = 2^n$ this is not possible for sufficiently large n.

The above implies that D is an open set from which the statement follows. $\square$

For the next result we keep the notation of the statement of Proposition 2.

Proposition 3 *Let $k = \dim h(U)$.*

(i) *There exist indices $i_1, \ldots, i_k \in \{1, \ldots, m\}$, a polynomial $g \in \mathbb{R}[y_1, \ldots, y_k]$ and a rational function $q \in \mathbb{R}(x_1, \ldots, x_n)$ with both numerator and denominator relatively prime with f_n such that*

$$g(h_{i_1}, \ldots, h_{i_k}) = f_n^\ell q$$

for some $\ell > 0$.

(ii) *Let n be sufficiently large. Then $k \geq n$.*

PROOF. For part (i), first, notice that, since $\dim(h(U)) = k$, there exist $i_1, \ldots, i_k \in \{1, \ldots, m\}$ such that the functions $h_{i_1}, \ldots, h_{i_k}$ are algebraically independent. We want to show that $\dim(U \cap C_n) < k$. To do so let $X = h(U), Y = h(U - C_n)$ and $Z = h(U \cap C_n)$. We have that all X, Y and Z are semialgebraic subsets of $\mathbb{R}^m$. In addition, Z is contained in the closure of Y with respect to the Euclidean topology relative to X since h is continuous and $Y \cap Z = \emptyset$ since h is the restriction of φ to U and φ is a reduction.

From here it follows that Z is included in the boundary of Y relative to X. Hence, $\dim Z < \dim Y = \dim X$ (see e.g. Proposition 2.8.12 of [Bochnak, Coste, and Roy 1987]).

The above shows that $\dim h(U \cap C_n) < k$. Therefore, there exists $g \in \mathbb{R}[y_1, \ldots, y_k]$ such that, for all $x \in U \cap C_n$, $g(h_{i_1}(x), \ldots, h_{i_k}(x)) = 0$. Write this as a rational function $g(h) = a/b$ with $a, b \in \mathbb{R}[x_1, \ldots, x_n]$ relatively prime. Then $a(C_n) = 0$ and $a \neq 0$ (since $h_{i_1}, \ldots, h_{i_k}$ are algebraically independent). By Proposition 1 this implies that there exists $r \in \mathbb{R}[x_1, \ldots, x_n]$ such that $a = r f_n$. If ℓ is the largest power of f_n dividing a then the result follows by taking $q = \frac{r'}{b}$ where r' is the quotient of r divided by $f_n^{\ell-1}$.

We now proceed to part (ii). To simplify notation, assume that $i_j = j$ for $j = 1, \ldots, k$. Also, let d be a bound for the degrees of the numerators and denominators of the h_j. Recall from Proposition 2 that d is bounded by a polynomial in n.

By part (i) there exists $q \in \mathbb{R}(x_1, \ldots, x_n)$ relatively prime with f_n such that

$$f_n^\ell q = g(h_1, \ldots, h_k)$$

for a certain $\ell \geq 1$. Taking derivatives on both sides we obtain that, for all $x \in \mathbb{R}^n$,

$$\nabla(f_n^\ell q)(x) = \nabla(g)(h(x)) \circ Dh(x) \tag{3}$$

where ∇ denotes the gradient and $Dh(x)$ is the Jacobian matrix of h at x.

Assume that $k < n$. Transposing (3) one sees that $\nabla(f^\ell q)(x)$ is the image of a vector of dimension k. Thus, there exists a linear dependency among the first $k+1$ coordinates of $\nabla(f^\ell q)(x)$

$$\sum_{i=1}^{k+1} \lambda_i \frac{\partial f_n^\ell q}{\partial x_i} = 0 \tag{4}$$

and the coefficients λ_i of this linear dependency are the determinants of some minors of $Dh(x)$. Thus, for $i = 1, \ldots, k+1$, λ_i is a rational function of x whose numerator and denominator have degrees bounded by kd. Since the submatrix of $Dh(x)$ obtained by keeping its first $k+1$ rows contains at most $k(k+1)$ different denominators, multiplying equation (4) by the product of all of all of them allows one to assume that the λ_i are polynomials with degree at most $kd(k+1)$.

By the product rule we get

$$\sum_{i=1}^{k+1} \lambda_i \left(\ell f_n^{\ell-1} q \frac{\partial f_n}{\partial x_i} + f_n^\ell \frac{\partial q}{\partial x_i} \right) = 0$$

i.e.

$$\ell f_n^{\ell-1} q \sum_{i=1}^{k+1} \lambda_i \frac{\partial f_n}{\partial x_i} + f_n^\ell \sum_{i=1}^{k+1} \lambda_i \frac{\partial q}{\partial x_i} = 0.$$

Since f_n^ℓ divides the second term above it must also divide the first from which, using that f_n and q are relatively prime, it follows that f_n divides $\sum_{i=1}^{k+1} \lambda_i \frac{\partial f_n}{\partial x_i}$. That is, there exists a polynomial p such that

$$f_n p = \sum_{i=1}^{k+1} \lambda_i \frac{\partial f_n}{\partial x_i}$$

i.e.

$$p \left(\sum_{i=1}^{n} x_i^{2^n} - 1 \right) = 2^n \sum_{i=1}^{k+1} \lambda_i x_i^{2^n - 1}.$$

Now, for n large enough, the degrees of the λ_i are smaller than $2^n - 1$ since $kd(k+1)$ is polynomial in n. This implies that the degree of p must also be bounded by $kd(k+1)$. But then, for each $i \leq k+1$, $px_i^{2^n} = \lambda_i x_i^{2^n-1}$, i.e., $px_i = \lambda_i$. And from here it follows that $-p = 0$, a contradiction. $\square$

Theorem 1 now readily follows. For all $n \in \mathbb{N}$, Proposition 2 ensures the existence of an open ball $U \subset \mathbb{R}^n$ whose image by the reduction φ is included in $\mathbb{R}^m$ with m polynomially bounded on n. But for all n sufficiently large this image, by Proposition 3 (ii), has dimension at least n and therefore it can not be polylogarithmic on m.

Remark 2 The result of Theorem 1, together with that in [Cucker, Koiran, and Matamala 1997], supports the conjecture that there are no sparse NP-hard sets over the reals unless P = NP. There are two main settings where this remains to be proved. On the one hand, machines which do not multiply nor divide but which branch over sign tests. On the other hand, the unrestricted case in which the machine can multiply or divide (and branch over sign tests) with unit cost. In these two cases, the result seems harder since there is no proof that P $\neq$ NP. In the first case, we would like to remark that, if many-one reductions are replaced by Turing reductions and we assume that P $\neq$ NP then Mahaney's conjecture is false. This is due to a result of Fournier and Koiran [Fournier and Koiran 2000] proving that any NP-complete set in the Boolean setting (i.e. over $\{0,1\}$) is NP-complete over the reals with addition and order for Turing reductions. Since the subsets of elements of size n of any such set S have dimension 0 the sparseness of S is immediate. For more on this see [Fournier 2000].

References

Arvind, V., Y. Han, L. Hemachandra, J. Köbler, A. Lozano, M. Mundhenk, M. Ogiwara, U. Schöning, R. Silvestri, and T. Thierauf (1993). Reductions to sets of low information content. In K. Ambos-Spies, S. Homer, and U. Schöning (Eds.), *Complexity Theory: current research*, pp. 1–45. Cambridge University Press.

Berman, L. and J. Hartmanis (1977). On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing 6*, 305–322.

Blum, L., F. Cucker, M. Shub, and S. Smale (1998). *Complexity and Real Computation*. Springer-Verlag.

Blum, L., M. Shub, and S. Smale (1989). On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the Amer. Math. Soc. 21*, 1–46.

Bochnak, J., M. Coste, and M.-F. Roy (1987). *Géométrie algébrique réelle.* Springer-Verlag.

Cucker, F., P. Koiran, and M. Matamala (1997). Complexity and dimension. *Information Processing Letters 62*, 209–212.

Cucker, F., M. Shub, and S. Smale (1994). Complexity separations in Koiran's weak model. *Theoretical Computer Science 133*, 3–14.

Fournier, H. (2000). Sparse NP-complete problems over the reals with addition. Technical Report 2000-12, LIP.

Fournier, H. and P. Koiran (2000). Lower bounds are not easier over the reals: Inside PH. In *28th International Colloquium on Automata, Languages and Programming*, Volume 1853 of *Lect. Notes in Comp. Sci.*, pp. 832–843. Springer-Verlag.

Koiran, P. (1997). A weak version of the Blum, Shub & Smale model. *J. Comput. System Sci. 54*, 177–189. A preliminary version appeared in *34th annual IEEE Symp. on Foundations of Computer Science*, pp. 486–495, 1993.

Mahaney, S. (1982). Sparse complete sets for NP: Solution of a conjecture by Berman and Hartmanis. *J. Comput. System Sci. 25*, 130–143.

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