On sparseness and Turing reducibility over the reals

Felipe Cucker [1,2]

Dept. of Mathematics
City University of Hong Kong
Hong Kong, Peoples Republic of China

Abstract

We prove some results about existence of NP-complete and NP-hard (for Turing reductions) sparse sets on different settings over the real numbers.

Key words: real computation, Turing reducibility, sparseness

1 Introduction

In recent years a number of papers were published dealing with extensions of Mahaney's Theorem to computations over the real numbers.

Mahaney's Theorem [13] states that, unless P = NP, there are no sparse NP-hard sets. A set $S \subseteq \{0,1\}^*$ 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 $p(n)$. Here $\{0,1\}^*$ denotes the set of all finite sequences of elements in $\{0,1\}$.

Mahaney's Theorem answers a question which originated with the Berman-Hartmanis conjecture [2]. The latter states that all NP-complete sets (over $\{0,1\}$) are polynomially isomorphic. That is, that for all NP-complete sets A and B, there exists a bijection $\varphi : \{0,1\}^* \to \{0,1\}^*$ 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. The Berman-Hartmanis conjecture is still unproved. Should it be proved, we would have as a consequence that no sparse NP-complete set exists. This is implied by Mahaney's theorem if we assume that P $\neq$ NP.

After 1982, a whole stream of research developed around the issue of reductions to "small" sets (see [1]).

[1] Partially supported by SRG grant 7001290.
[2] Email: macucker@math.cityu.edu.hk

The extension of Mahaney's Theorem to machines over the real numbers (as introduced in [4], see also [3]) was first raised in [7]. A first question was how to extend the notion of sparseness to subsets of $\mathbb{R}^\infty$ (the disjoint union of $\mathbb{R}^n$ for $n \in \mathbb{N}$). The notion suggested in [7] is the following. 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.

Using this notion of sparseness the main result of [7] proves that there are no sparse NP-hard sets in the context of machines over $(\mathbb{R}, +, =)$, i.e., machines 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. [14]). Also, we want to remark that the reducibility notion implicit in the consideration of NP-hardness in the result above is the so called "many-one."

A natural extension to the result in [7] would consider machines over $(\mathbb{R}, +, \leq)$. That is, machines which do not perform multiplications or divisions but are allowed to branch on inequality tests. While there is no proof that there are no sparse NP-hard sets (with respect to many-one reductions, assuming $\mathrm{P} \neq \mathrm{NP}$) in this setting, a result of Fournier and Koiran [11] shows that there exist NP-complete sparse sets with respect to Turing reductions. This follows from a surprising result (Lemma 3 in [11]) which, roughly speaking, states that any NP-complete set over $\{0, 1\}$ is NP-complete over $(\mathbb{R}, +, \leq)$ 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.

A natural question arises. Are there sparse NP-hard sets over $(\mathbb{R}, +, =)$ with respect to Turing reductions? A partial answer was given by Fournier in [10] where it is proved that there are no sparse *definable* NP-hard sets over $(\mathbb{R}, +, =)$ with respect to Turing reductions. Since any set in NP is definable, an immediate consequence (curiously not remarked in [10]) is the following.

Proposition 1.1 *There are no sparse* NP*-Turing-complete sets over* $(\mathbb{R}, +, =)$.

The definability condition is important. It is very easy to proof (see Section 2 below) the following.

Proposition 1.2 *There are sparse* NP*-Turing-hard sets over* $(\mathbb{R}, +, =)$.

A model of real machines, with multiplications and divisions allowed, attempting to get closer to the Turing machine (in the sense that iterated multiplication is somehow penalized) was introduced by Koiran in [12]. 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. For this model, it is also known that $\mathrm{P} \neq \mathrm{NP}$ [8].

In [6], it was shown that there are no sparse NP_W-hard sets (with respect to many-one reductions). Here NP_W denotes the class NP for the weak model. The second result in this paper extends Fournier's result to the weak context. It is actually stronger than Fournier's result in that we don't need to assume definability; instead, it holds for any family of sets satisfying a number of conditions.

Definition 1.3 Let $\mathscr{F}$ be a family of sets such that every $S \in \mathscr{F}$ is included in $\mathbb{R}^n$ for some $n \geq 1$. We say that $\mathscr{F}$ is *well-behaved* when

(i) $\mathscr{F}$ contains the semialgebraic sets.

(ii) $\mathscr{F}$ is closed under finite unions, intersections and complements.

(iii) $\mathscr{F}$ is closed under interior and closure for the Euclidean topology.

(iv) If $U \in \mathscr{F}$, $U \subset \mathbb{R}^n$ and $\varphi : U \to \mathbb{R}^m$ is a rational map then, for all $S \in \mathscr{F}$, $S \subset \mathbb{R}^m$, $\varphi^{-1}(S) \in \mathscr{F}$ and for all $S \in \mathscr{F}$, $S \subset U$, $\varphi(S) \in \mathscr{F}$.

(v) The notion of dimension is well-defined and it coincides with the usual one for semialgebraic sets. In particular, no set in $\mathscr{F}$ can contain a set of dimension greater than its own or be written as a finite union of sets of smaller dimension.

We say that sets $S \in \mathscr{F}$ or sets $S \subset \mathbb{R}^\infty$ such that $S \cap \mathbb{R}^n \in \mathscr{F}$ for all n are *well-behaved*.

Well-behaved families of sets do exist. The obvious example is the family of semialgebraic sets. But the definition above covers much more general families of sets. A main remark is that o-minimal structures are well-behaved families (for an overview of o-minimal structures and their geometry see [5] or [15]). Thus, in particular, the family of globally subanalityic sets [9] or that of sets defined by means of Pfaffian functions [16] are well-behaved.

Let us denote by NP_W the class of problems in NP for the weak model.

Proposition 1.4 *There are no sparse well-behaved* NP_W*-Turing-hard sets. In particular, there are no sparse* NP_W*-Turing-complete sets.*

2 Proofs of Propositions 1.2 and 1.4

Let us denote by $\mathrm{NP}^{=}_{\mathrm{add}}$ and $\mathrm{NP}^{\leq}_{\mathrm{add}}$ the classes of problems in NP over $(\mathbb{R}, +, =)$ and $(\mathbb{R}, +, \leq)$ respectively.

Proof of Proposition 1.2. Let $\mathscr{S} \subset \{0,1\}^*$ be any (classical) NP-complete set and consider

$$\mathscr{S}^* = \{(1, x) \mid x \in \mathscr{S}\} \cup \{(2, y) \mid y \in \mathbb{R}, y \geq 0\}.$$

Clearly $\mathscr{S}^*$ is sparse as a subset of $\mathbb{R}^\infty$. We now show that it is $\mathrm{NP}^{=}_{\mathrm{add}}$-Turing-hard. To do so, consider any set $A \in \mathrm{NP}^{=}_{\mathrm{add}}$. Clearly, $A \in \mathrm{NP}^{\leq}_{\mathrm{add}}$ as well. But then, Fournier and Koiran [11] show that there is an oracle machine M over $(\mathbb{R}, +, \leq)$ solving A with oracle $\mathscr{S}$ in polynomial time.

We modify M as follows. We replace branch nodes testing a value z for positivity by oracle nodes testing whether $(2, z) \in \mathscr{S}^*$. And we replace oracle nodes testing whether a vector $x \in \mathscr{S}$ by oracle nodes testing whether $(1, x) \in \mathscr{S}^*$. Clearly, the new machine is an oracle machine over $(\mathbb{R}, +, =)$ which, with oracle $\mathscr{S}^*$, decides A in polynomial time. □

We next proceed to the proof of Proposition 1.4.

Let $C_n = \{x \in \mathbb{R}^n \mid x_1^{2^n} + \cdots + x_n^{2^n} = 1\}$ and $\mathcal{C} \subset \mathbb{R}^\infty$ be the union of the sets C_n. We know that $\mathcal{C} \in \mathrm{NP}_W$.

Proposition 2.1 *Let $\mathscr{F}$ be a well-behaved family and $S \subset \mathbb{R}^\infty$ such that $S \cap \mathbb{R}^n \in \mathscr{F}$ for all n. Assume S is a NP_W-Turing-hard set. Then, for all $n \geq 1$, there exist sets $E, \Omega \in \mathscr{F}$, $E \subset \mathbb{R}^n$ and $\Omega \subset C_n$, a number $m \in \mathbb{N}$, $m = n^{\mathcal{O}(1)}$, and a rational map $h : \mathbb{R}^n \to \mathbb{R}^m$, well-defined on E and $\overline{E} \cap \Omega$, such that*

(i) $E \cap \Omega = \emptyset$,

(ii) $\dim(\overline{E} \cap \Omega) = n - 1$,

(iii) *the degrees of numerator and denominator of the components of h are bounded by a polynomial in n, and*

(iv) $h(\overline{E} \cap \Omega) \cap h(E) = \emptyset$.

Proof. Since $\mathcal{C} \in \mathrm{NP}_W$ there is an oracle machine M which, with oracle S, decides $\mathcal{C}$ in weak polynomial time. Let p be a polynomial time bound for M.

Consider $n \in \mathbb{N}$. The computation of M over inputs of size n induces a computation tree of depth at most $p(n)$ whose branching nodes are either a sign test or an oracle node.

Let ν be a branching node in this tree. If ν is a sign test, then ν tests whether $\varphi_\nu(x) \geq 0$ where φ_ν is a rational function and $x \in \mathbb{R}^n$ is the input. In addition, since p is a bound for the weak running time of M, both the numerator and denominator of a relatively prime representation of φ_ν have degree bounded by $p(n)$.

If instead ν is an oracle node then it tests whether

$$\varphi_\nu(x) = (\varphi_1(x), \ldots, \varphi_m(x)) \in S_m$$

where $m \leq p(n)$ and, for $i = 1, \ldots, m$, φ_i is a rational function as above. Note that, since $\mathscr{F}$ is closed under complements and inverse images of rational maps, the sets $\{x \in \mathbb{R}^n \mid \varphi_\nu(x) \in S_m\}$ and $\{x \in \mathbb{R}^n \mid \varphi_\nu(x) \notin S_m\}$ are in $\mathscr{F}$. A similar remark holds if ν is a sign test.

For any leaf γ in the tree, we denote by Ω_γ the set of points in $\mathbb{R}^n$ whose computation ends in γ. This is a set in $\mathscr{F}$ since it is intersection of sets in $\mathscr{F}$. Now let $\mathcal{A}$ be the set of accepting leaves. Then,

$$C_n = \bigcup_{\gamma \in \mathcal{A}} \Omega_\gamma.$$

Since $\dim(C_n) = n-1$ and the union above is a finite union of sets in $\mathscr{F}$ there exists a leaf $\gamma^0 \in \mathcal{A}$ such that $\dim \Omega_{\gamma^0} = n-1$. So, Ω_{γ^0} is a subset of C_n, it belongs to $\mathscr{F}$, and it is of maximal dimension (among the Ω_γ for $\gamma \in \mathcal{A}$).

Let ν be a branching node in the path leading to γ^0. The *domain* of ν is

$$\Omega_\nu = \{x \in \mathbb{R}^n \mid x \text{ reaches the node } \nu\}$$

and its *excluded part*,

$$E_\nu = \{x \in \Omega_\nu \mid x \text{ deviates at } \nu \text{ from the path leading to } \gamma^0\}.$$

If $\nu_1, \ldots, \nu_\ell$ are the branching nodes in the path leading to γ^0 we then have the disjoint union

$$\mathbb{R}^n - \Omega_{\gamma^0} = E_{\nu_1} \cup \cdots \cup E_{\nu_\ell}.$$

Again, we remark that $E_{\nu_1}, \ldots, E_{\nu_\ell}$ are all sets in $\mathscr{F}$.

We next show that there exists $i \leq \ell$ such that $\dim(\overline{E_{\nu_i}} \cap \Omega_{\gamma^0}) = n-1$.

This follows from the fact that, since taking closures commutes with finite unions,

$$\mathbb{R}^n = \overline{E_{\nu_1}} \cup \cdots \cup \overline{E_{\nu_\ell}}.$$

Therefore,

$$\Omega_{\gamma^0} = (\Omega_{\gamma^0} \cap \overline{E_{\nu_1}}) \cup \cdots \cup (\Omega_{\gamma^0} \cap \overline{E_{\nu_\ell}})$$

and, since $\dim \Omega_{\gamma^0} = n-1$ it follows that there exists $i \leq \ell$ such that $\dim(\Omega_{\gamma^0} \cap \overline{E_{\nu_i}}) = n-1$.

Let $E = E_{\nu_i}$, $\Omega = \Omega_{\gamma^0}$, and $h = \varphi_{\nu_i}$, $h : \mathbb{R}^n \to \mathbb{R}^{m_i}$. We just proved that $\dim(\Omega \cap \overline{E}) = n-1$ and thus, (ii) holds. In addition, $\Omega_{\gamma^0} \subseteq \Omega_{\nu_i}$ from which $E \cap \Omega = \emptyset$ and (i) holds as well. Part (iii) follows, as we already remarked, from the weakness of M. Finally, for part (iv), consider first the case that ν_i is an oracle node. Then for $\mathcal{S}$ either S_{m_i} or its complement, we have $E_{\nu_i} = \varphi_{\nu_i}^{-1}(\mathcal{S})$ and $\Omega_{\gamma^0} \subseteq \varphi_{\nu_i}^{-1}(\mathcal{S}^{\mathsf{c}})$ where $^{\mathsf{c}}$ denotes complement, and therefore $h(\overline{E} \cap \Omega) \cap h(E) = \emptyset$. A similar reasoning holds if ν_i is a test node with $\mathcal{S}$ now either $\mathbb{R}^+$ or $\mathbb{R}^- - \{0\}$. □

The following result in real algebraic geometry will be used. Its proof can be found in Chapter 19 of [3].

Proposition 2.2 *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.* □

Proposition 2.3 *With the notations of Proposition 2.1, let* $k-1 = \dim h(\overline{E} \cap \Omega)$.

(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) *For* n *sufficiently large,* $k \geq n$.

Proof. Let $K = \dim h(\overline{E})$. Since $\dim h(E) = K$, 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 next want to show that $k \leq K$. To do so let $X = h(\overline{E} \cap \mathrm{dom}(h)), Y = h(E)$ and $Z = h(\overline{E} \cap \Omega)$. Here $\mathrm{dom}(h)$ denotes the set of points in $\mathbb{R}^n$ where h is well-defined. We have that all X, Y and Z are sets of $\mathscr{F}$ in $\mathbb{R}^m$. In addition, Z is contained in the closure of Y with respect to the Euclidean topology relative to X since h is continuous and $Y \cap Z = \emptyset$ by Proposition 2.1 (iv). From here it follows that Z is included in the boundary of Y relative to X. Hence, $\dim Z < \dim Y = \dim X$.

The above shows that $\dim h(\overline{E} \cap \Omega) < K$, i.e. $k \leq K$. Therefore, there exist a set of k elements in $\{i_1, \ldots, i_K\}$, which we may assume are $i_1, \ldots, i_k$, and a polynomial $g \in \mathbb{R}[y_1, \ldots, y_k]$ such that, for all $x \in \overline{E} \cap \Omega$, $g(h_{i_1}(x), \ldots, h_{i_k}(x)) = 0$. Write this as a rational function $g(h) = a/b$ with $a, b \in \mathbb{R}[x_1, \ldots, x_n]$ relatively prime. Then, since $\dim(\overline{E} \cap \Omega) = n - 1$, $\overline{E} \cap \Omega \subset C_n$, C_n is irreducible and $h_{i_1}, \ldots, h_{i_k}$ are algebraically independent, $a(C_n) = 0$ and $a \neq 0$. By Proposition 2.2 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 part (i) follows by taking $q = \frac{r'}{b}$ where r' is the quotient of r divided by $f_n^{\ell-1}$.

Part (ii) is proved as in Proposition 3.3 of [6]. □

Proof of Proposition 1.4. Assume the set S in Proposition 2.1 is sparse and let q be a polynomial such that $\dim(S_n) \leq q(\log n)$. Let $n \in \mathbb{N}$, $n \geq 3$, be sufficiently large such that $q(\log p(n)) < n - 1$ and part (ii) of Proposition 2.3 holds. Recall, p is a polynomial bounding the running time of the reduction in Proposition 2.1.

Recall from the proof of Proposition 2.1 that $h = \varphi_\nu$ for some branching node ν in the tree associated to M and n. First assume that ν is a sign test. Then since $\dim(h(\Omega)), \dim(h(E)) \leq 1$ since both sets are included in $\mathbb{R}$. But

$$\dim h(\Omega) \geq \dim h(\overline{E} \cap \Omega) = k - 1 \geq n - 1 > 1$$

and

$$\dim h(E) = K \geq k \geq n > 1.$$

Therefore, ν can not be a sign test and is an oracle node instead. Let m be such that $h : \mathbb{R}^n \to \mathbb{R}^m$. Then $m \leq p(n)$ and

$$\dim h(\Omega) \geq \dim h(\overline{E} \cap \Omega) = k - 1 \geq n - 1 > q(\log p(n)) \geq \dim S_m$$

and

$$\dim h(E) = K \geq k \geq n > q(\log p(n)) \geq \dim S_m.$$

This is a contradiction since either $h(E)$ or $h(\Omega)$ is included in S_m. □

References

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

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

[3] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer-Verlag, 1998.

[4] 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. *Bulletin of the Amer. Math. Soc.*, 21:1–46, 1989.

[5] M. Coste. *An Introduction to o-minimal Geometry.* Istituti Editoriali e Poligrafici Internazionali, 2000.

[6] F. Cucker and D.Yu. Grigoriev. There are no sparse NP_W-hard sets. *SIAM Journal on Computing*, 31:193–198, 2001.

[7] F. Cucker, P. Koiran, and M. Matamala. Complexity and dimension. *Information Processing Letters*, 62:209–212, 1997.

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

[9] J. Denef and L. van den Dries. p-adic and real subanalytic sets. *Ann. of Math.*, 128:80–138, 1998.

[10] H. Fournier. Sparse NP-complete problems over the reals with addition. *Theoretical Computer Science*, 255:607–610, 2001.

[11] H. Fournier and P. Koiran. 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.*, pages 832–843. Springer-Verlag, 2000.

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

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

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

[15] L. van den Dries and C. Miller. Geometric categories and o-minimal structures. *Duke Math. J.*, 84:497–540, 1996.

[16] A.J. Wilkie. A theorem of the complement and some new o-minimal structures. *Selecta Math. (N.S.)*, 5:397–421, 1999.