Noncomputable Functions in the Blum-Shub-Smale Model

Wesley Calvert[1], Ken Kramer[2] and Russell Miller[2⋆]

[1] Murray State University
Murray, Kentucky 42071 USA
wesley.calvert@murraystate.edu
http://campus.murraystate.edu/academic/faculty/wesley.calvert
[2] Queens College of CUNY
65-30 Kissena Blvd., Flushing, NY 11367 USA
and the CUNY Graduate Center
365 Fifth Avenue, New York, NY 10016 USA
kkramer@qc.cuny.edu & Russell.Miller@qc.cuny.edu
http://qcpages.qc.cuny.edu/~rmiller

Abstract. We answer several questions of Meer and Ziegler about the Blum-Shub-Smale model of computation on $\mathbb{R}$: the set $\mathbb{A}_d$ of algebraic numbers of degree $\leq d$ is not decidable in $\mathbb{A}_{d-1}$, and the BSS halting problem is not decidable in any countable oracle.

Key words: Blum-Shub-Smale model, computability, real computation.

1 Introduction

Blum, Shub, and Smale introduced in [2] a notion of computation with full-precision real arithmetic, in which the ordered field operations are axiomatically computable, and the computable functions are closed under the usual operations. A more complete account of this model is given in [1].

The key question for this paper was posed by Meer and Ziegler in [5]. Section 2 gives the basic technical result, Lemma 1, applied in Section 3 to Question 1.

Question 1 (Meer-Ziegler). Let $\mathbb{A}_d$ be the set of algebraic numbers with degree (over $\mathbb{Q}$) at most d. Then is it true that

$$\mathbb{A}_0 \lneq_{BSS} \mathbb{A}_1 \lneq_{BSS} \cdots \mathbb{A}_d \lneq_{BSS} \cdots ?$$

$\mathbb{A}_{d-1} \leq_{BSS} \mathbb{A}_d$ is clear: if $x \in \mathbb{A}_d$, find its minimal polynomial in $\mathbb{Q}[X]$; while if $x \notin \mathbb{A}_d$ then $x \notin \mathbb{A}_{d-1}$. The question asks if $\mathbb{A}_d \leq_{BSS} \mathbb{A}_{d-1}$.

2 BSS-Computable Functions At Transcendentals

Here we introduce our basic method for showing that various functions on the real numbers fail to be BSS-computable. In many respects, it is equivalent to the method, used by many others (see for example [1]), of considering BSS computations as paths through a finite-branching tree of countable height, branching whenever there is a forking instruction in the program. However, we believe our method can be more readily understood by a mathematician unfamiliar with computability theory.

Lemma 1. *Let M be a BSS-machine, and $\boldsymbol{z}$ the finite tuple of real parameters mentioned in the program for M. Suppose that $\boldsymbol{y} \in \mathbb{R}^{m+1}$ is a tuple of real numbers algebraically independent over the field $Q = \mathbb{Q}(\boldsymbol{z})$, such that M converges on input $\boldsymbol{y}$. Then there exists $\epsilon > 0$ and rational functions $f_0, \ldots, f_n \in Q(\boldsymbol{Y})$, (that is, rational functions of the variables $\boldsymbol{Y}$ with coefficients from Q) such that for all $\boldsymbol{x} \in \mathbb{R}^{m+1}$ in the ϵ-ball $B_\epsilon(\boldsymbol{y})$, M converges on input $\boldsymbol{x}$ with output $\langle f_0(\boldsymbol{x}), \ldots, f_n(\boldsymbol{x})\rangle \in \mathbb{R}^{n+1}$.*

⋆ The corresponding author was supported by Grants # 90927-08 08 from the Queens College Research Enhancement Program, # 61467-00 39 and # 62632-00 40 from the PSC-CUNY Research Award Program, and (along with the first author) # 13397 from the Templeton Foundation.

Proof. The intuition is that by choosing $\boldsymbol{x}$ sufficiently close to $\boldsymbol{y}$, we can ensure that the computation on $\boldsymbol{x}$ branches in exactly the same way as the computation on $\boldsymbol{y}$, at each of the (finitely many) branch points in the computation on $\boldsymbol{y}$. Say that the run of M on input $\boldsymbol{y}$ halts at stage t, and that at each stage $s \leq t$, the non-blank cells contain the reals $\langle f_{0,s}(\boldsymbol{y}), \ldots, f_{n_s,s}(\boldsymbol{y})\rangle$. Each $f_{i,s}$ is a rational function in $Q(\boldsymbol{Y})$, uniquely determined, since $\boldsymbol{y}$ is algebraically independent over Q. Let $F = \{f_{i,s}(\boldsymbol{Y}) : s \leq t \;\&\; i \leq n_s \;\&\; f_{i,s} \notin Q\}$ be the finite set of nonconstant rational functions used in the computation. For each $f_{i,s} \in F$, the preimage $f_{i,s}^{-1}(0)$ is closed in $\mathbb{R}^{m+1}$, and therefore so is the finite union U of all these $f_{i,s}^{-1}(0)$. By algebraic independence, $\boldsymbol{y} \notin U$, so there exists an $\epsilon > 0$ with $B_\epsilon(\boldsymbol{y}) \cap U = \emptyset$. Indeed, for all $f_{i,s} \in F$ and all $\boldsymbol{x} \in B_\epsilon(\boldsymbol{y})$, $f_{i,s}(\boldsymbol{x})$ and $f_{i,s}(\boldsymbol{y})$ must have the same sign. Therefore, for any $\boldsymbol{x} \in B_\epsilon(\boldsymbol{y})$, it is clear that in the run of M on input $\boldsymbol{x}$, at each stage $s \leq t$, the cells will contain precisely $\langle f_{0,s}(\boldsymbol{x}), \ldots, f_{n_s,s}(\boldsymbol{x})\rangle$ and the machine will be in the same state in which it was at stage s on input $\boldsymbol{y}$. Therefore, at stage t, the run of M on input $\boldsymbol{x}$ must also have halted, with $\langle f_{0,t}(\boldsymbol{x}), \ldots, f_{n_t,t}(\boldsymbol{x})\rangle$ in its cells as the output. □

Lemma 1 provides quick proofs of several known results, including the undecidability of every proper subfield $F \subset \mathbb{R}$.

Corollary 1 *No BSS-decidable set $S \subseteq \mathbb{R}^n$ is both dense and co-dense in $\mathbb{R}^n$.*

Proof. If the characteristic function χ_S were computed by some BSS machine M with parameters $\boldsymbol{z}$, then by Lemma 1, it would be constant in some neighborhood of every $\boldsymbol{y} \in \mathbb{R}^n$ algebraically independent over $\boldsymbol{z}$. □

Corollary 2 *Define the boundary of a subset $S \subseteq \mathbb{R}^n$ to be the intersection of the closure of S with the closure of its complement. If S is BSS-decidable, then there is a finite tuple $\boldsymbol{z}$ such that every point on the boundary of S has coordinates algebraically dependent over $\boldsymbol{z}$.* □

Of course, Corollaries 1 and 2 follow from other results that have been established long since, in particular from the Path Decomposition Theorem described in [1]. We include them here because of the simplicity of these proofs, and because they introduce the method to be used in the following section.

3 Application to Algebraic Numbers

Here we modify the method of Lemma 1 to answer Question 1.

Theorem 1 *For all $d > 0$, $\mathbb{A}_d \not\leq_{BSS} \mathbb{A}_{d-1}$.*

Proof. Suppose that M is an oracle BSS machine with real parameters $\boldsymbol{z}$, such that $M^{\mathbb{A}_{d-1}}$ computes the characteristic function of $\mathbb{A}_d$. Fix any $y \in \mathbb{R}$ which is transcendental over the field $Q = \mathbb{Q}(\boldsymbol{z})$, and run $M^{\mathbb{A}_{d-1}}$ on input y. As in the proof of Lemma 1, we set F to be the finite set of all nonconstant rational functions $f \in Q(Y)$ such that $f(y)$ appears in some cell during this computation. Again, there is an $\epsilon > 0$ such that all x within ϵ of y satisfy $f(x) \cdot f(y) > 0$ for all $f \in F$. However, when $M^{\mathbb{A}_{d-1}}$ runs on an arbitrary input $x \in B_\epsilon(y) \cap \mathbb{A}_d$, it may have a different computation path, because such an x might lie in $\mathbb{A}_{d-1}$, or might have $f(x) \in \mathbb{A}_{d-1}$ for some $f \in F$, and in this case the computation on input x might ask its oracle whether $f(x) \in \mathbb{A}_{d-1}$ and would then branch differently from the computation on input y. (Of course, for all $f \in F$, $f(y) \notin \mathbb{A}_{d-1}$, since $f(y)$ must be transcendental over $\mathbb{Q}$ for nonconstant f.) So we must establish the existence of some $x \in B_\epsilon(y) \cap \mathbb{A}_d$ with $f(x) \notin \mathbb{A}_{d-1}$ for all $f \in F$. Of course, we do not need to give any effective procedure which produces this x; its existence is sufficient.

We will need the following lemma from calculus. The lemma uses complex numbers, but only for mathematical results about $\mathbb{R}$; no complex number is ever an input to M.

Lemma 2. *If ζ is a primitive k-th root of unity and $f \in \mathbb{R}(Y)$ and there are positive real values of v arbitrarily close to 0 for which at least one of $f(b + \zeta v), f(b + \zeta^2 v), \ldots, f(b + \zeta^{k-1} v)$ has the same value as $f(b + v)$, then $f'(b) = 0$.* □

Fix ζ to be a primitive d-th root of unity. We choose $b \in \mathbb{Q}$ such that $|y-b| < \frac{\epsilon}{2}$ and such that b lies in the domain of every $f \in F$, with all $f'(b) \neq 0$. Such a b must exist, since all $f \in F$ are differentiable and nonconstant. Now Lemma 2 yields a $\delta > 0$, such that every $v \in \mathbb{R}$ with $0 < v < \delta$ satisfies $f(b+v) \neq f(b+\zeta^m v)$ for every $f \in F$ and every m with $0 < m < d$. So fix $x = b + \sqrt[d]{u}$ for some $u \in \mathbb{Q}$ with $0 < \sqrt[d]{u} < \min(\delta, \frac{\epsilon}{2})$, for which $(X^d - u)$ is irreducible in $Q[X]$. (This ensures $\sqrt[d]{u} \notin Q$, of course. If there were no such u, then Q could not be finitely generated over $\mathbb{Q}$; this follows from the criterion for irreducibility of $(X^d - u)$ in [4, Thm. 9.1, p. 331], along with [6, Thm. 3.1.4, p. 82].) Thus $|x-y| < \epsilon$ and all $f \in F$ satisfy $f(b+\sqrt[d]{u}) \neq f(b+\zeta^m \sqrt[d]{u})$ for all $0 < m < d$.

Suppose that $f(x) = a \in \mathbb{A}_{d-1}$. Then $Q \subseteq Q(a) \subseteq Q(x)$, and a has degree $< d$ over Q (since $\mathbb{Q} \subseteq Q$), while $[Q(x) : Q] = d$, so $Q(a)$ is a proper subfield of $Q(x)$. Indeed $[Q(x) : Q(a)] \cdot [Q(a) : Q] = [Q(x) : Q] = d$, so the degree of a over Q is some proper divisor of d. Now let $p(X)$ be the minimal polynomial of x over the field $Q(a)$. Of course $p(X)$ may fail to lie in $\mathbb{Q}[X]$, but $p(X)$ must divide the minimal polynomial of x in $\mathbb{Q}[X]$, and so the roots of $p(X)$ are x and some of the $\mathbb{Q}$-conjugates $(b + \zeta^m \sqrt[d]{u})$ of x. At least one $(b + \zeta^m \sqrt[d]{u})$ with $0 < m < d$ must be a root of $p(X)$, since $\deg(p(X)) = [Q(x) : Q(a)] > 1$. We fix this m and let $\overline{x} = b + \zeta^m \sqrt[d]{u}$, and also fix $k = \deg(p(X))$.

Now we apply the division algorithm to write

$$f(X) = \frac{g(X)}{h(X)} = \frac{q_g(X) \cdot p(X) + r_g(X)}{q_h(X) \cdot p(X) + r_h(X)}$$

with $r_g(X)$ and $r_h(X)$ both in $Q(a)[X]$ of degree $< k$. We write $r_g(X) = g_{k-1}X^{k-1} + \cdots + g_1 X + g_0$ and $r_h(X) = h_{k-1}X^{k-1} + \cdots + h_1 X + h_0$, with all coefficients in $Q(a)$. Then $r_g(x) = g(x) = ah(x) = ar_h(x)$, since $p(x) = p(\overline{x}) = 0$. The equation $0 = r_g(x) - ar_h(x)$ can then be expanded in powers of $\sqrt[d]{u}$:

$$\begin{aligned}
0 = & \sum_{j<k} \left(g_j \cdot (b + \sqrt[d]{u})^j - ah_j \cdot (b + \sqrt[d]{u})^j \right) \\
= & \Big[(g_{k-1}b^{k-1} + g_{k-2}b^{k-2} + \cdots + g_1 b + g_0) \\
& \quad - a(h_{k-1}b^{k-1} + h_{k-2}b^{k-1} + \cdots + h_1 b + h_0) \Big] \\
& + \sqrt[d]{u} \cdot \Bigg[\left(\binom{k-1}{1} g_{k-1}b^{k-2} + \binom{k-2}{1} g_{k-2}b^{k-3} + \cdots + \binom{1}{1} g_1 b^0 \right) \\
& \qquad - a \left(\binom{k-1}{1} h_{k-1}b^{k-2} + \binom{k-2}{1} h_{k-2}b^{k-3} + \cdots + \binom{1}{1} h_1 b^0 \right) \Bigg] \\
& \qquad \vdots \\
& + (\sqrt[d]{u})^{k-2} \left[\left(\binom{k-1}{k-2} g_{k-1}b + g_{k-2} \right) - a \left(\binom{k-1}{k-2} h_{k-1}b + h_{k-2} \right) \right] \\
& + (\sqrt[d]{u})^{k-1} \Big[g_{k-1} - ah_{k-1} \Big]
\end{aligned}$$

Here all bracketed expressions lie in $Q(a)$. However, $x = b + \sqrt[d]{u}$ has degree k over $Q(a)$, and therefore so does $\sqrt[d]{u}$. It follows that $\{1, \sqrt[d]{u}, (\sqrt[d]{u})^2, \ldots, (\sqrt[d]{u})^{k-1}\}$ forms a basis for $Q(x)$ as a vector space over $Q(a)$, and hence, in the equation above, all bracketed expressions must equal 0. One then proceeds inductively: the final bracket shows that $g_{k-1} = ah_{k-1}$, and plugging this into the second-to-last bracket shows that $g_{k-2} = ah_{k-2}$, and so on up. Thus $r_g(X) = ar_h(X)$, and so

$$f(x) = \frac{r_g(x)}{r_h(x)} = a = \frac{r_g(\overline{x})}{r_h(\overline{x})} = f(\overline{x}),$$

contradicting the choice of δ above. This contradiction shows that $f(x) \notin \mathbb{A}_{d-1}$, for every $f \in F$, and as in Lemma 1, it follows immediately that the computations by the machine M with oracle $\mathbb{A}_{d-1}$ on inputs x and y proceed along the same path and result in the same output. Since $x \in \mathbb{A}_d$ and $y \notin \mathbb{A}_d$, this proves the theorem. □

4 Further Results

We state here a few further results we have recently proven. For these we extend the notation: given any subset $S \subseteq \mathbb{N}$, write $\mathbb{A}_S = \cup_{d \in S} \mathbb{A}_{=d}$.

Theorem 2 *For sets $S, T \subseteq \mathbb{N}$, if $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$, then there exists $M \in \mathbb{N}$ such that all $p \in S$ satisfy $\{p, 2p, 3p, \ldots, Mp\} \cap T \neq \emptyset$. As a near-converse, if $(S - T)$ is finite and $(\forall p \in S - T)(\exists q > 0)[pq \in T]$, then $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$.*

Corollary 3 *There exists a subset $\mathcal{L}$ of the BSS-semidecidable degrees such that $(\mathcal{L}, \leq_{BSS}) \cong (\mathcal{P}(\mathbb{N}), \subseteq)$.*

Proof. We may replace the power set $\mathcal{P}(\mathbb{N})$ by the power set $\mathcal{P}(\{\text{primes}\})$. The latter maps into the BSS-semidecidable degrees via $S \mapsto \mathbb{A}_S$, and Theorem 2 shows this to be an embedding of partial orders. (The same map on all of $\mathcal{P}(\mathbb{N})$ is not an embedding.) In particular, if S and T are sets of primes and $n \in S - T$, then no multiple of n can lie in T; thus, by the theorem, $S \not\subseteq T$ implies $\mathbb{A}_S \not\leq_{BSS} \mathbb{A}_T$. The converse is immediate (for subsets of $\mathbb{N}$ in general, not just for prime numbers): if $S \subseteq T$, then ask whether an input x lies in the oracle set $\mathbb{A}_T$. If not, then $x \notin \mathbb{A}_S$; if so, find the minimal polynomial of x over $\mathbb{Q}$ and check whether its degree lies in S. (This program requires one parameter, to code the set S.) □

Theorem 3 *If $C \subseteq \mathbb{R}^\infty$ is a set to which the Halting Problem for BSS machines is BSS-reducible, then $|C| = 2^\omega$. Indeed, $\mathbb{R}$ has finite transcendence degree over the field K generated by (the coordinates of the tuples in) C.*

For the definition of the Halting Problem, see [1, pp. 79-81]. Since a program is allowed finitely many real parameters, it must be coded by a tuple of real numbers, not merely by a natural number. Theorem 3 is a specific case of a larger result on cardinalities, which is a rigorous version of the vague intuition that a set of small cardinality cannot contain enough information to compute a set of larger cardinality.

Definition 4 A set $S \subseteq \mathbb{R}$ is *locally of bicardinality* $\leq \kappa$ if there exist two open subsets U and V of $\mathbb{R}$ with $|\mathbb{R} - (U \cup V)| \leq \kappa$ and and $|U \cap S| \leq \kappa$ and $|V \cap \overline{S}| \leq \kappa$. (Here $\overline{S} = \mathbb{R} - S$.)

This definition roughly says that up to sets of size κ, each of S and $\overline{S}$ is equal to an open subset of $\mathbb{R}$. For example, the BSS-computable set $S = \{x \in \mathbb{R} : (\exists m \in \mathbb{N})\ 2^{-(2m+1)} \leq x \leq 2^{-(2m)}\}$, containing those x which have a binary expansion beginning with an even number of zeroes, is locally of bicardinality ω. The property of local bicardinality $\leq \kappa$ does not appear to us to be equivalent to any more easily stated property, but it is exactly the condition needed in our general theorem on cardinalities.

Theorem 5 *If $C \subseteq \mathbb{R}^\infty$ is an oracle set of infinite cardinality $\kappa < 2^\omega$, and $S \subseteq \mathbb{R}$ is a set with $S \leq_{BSS} C$, then S must be locally of bicardinality $\leq \kappa$. The same holds for oracles C of infinite co-cardinality $\kappa < 2^\omega$.*

References

1. L. Blum, F. Cucker, M. Shub, and S. Smale; *Complexity and real computation* (Berlin: Springer-Verlag, 1997).
2. L. Blum, M. Shub, and S. Smale; On a theory of computation and complexity over the real numbers, *Bulletin of the A.M.S. (New Series)* **21** (1989), 1–46.
3. C. Gassner; A hierarchy below the halting problem for additive machines, *Theory of Computing Systems* **43** (2008) 3–4, 464–470.
4. S. Lang; *Algebra* (second edition) (Menlo Park, CA: Addison-wesley Publishing Co., Inc., 1984).
5. K. Meer & M. Ziegler; An explicit solution to Post's Problem over the reals, *Journal of Complexity* **24** (2008) 3–15.
6. M. Nagata; *Theory of Commutative Fields*, English trans. (American Mathematical Society, 1993).
7. Y. Yonezawa; The Turing degrees for some computation model with the real parameter, *J. Math. Soc. Japan* **60** 2 (2008), 311-324.