NONCOMPUTABLE FUNCTIONS IN THE BLUM-SHUB-SMALE MODEL

WESLEY CALVERT, KEN KRAMER, AND RUSSELL MILLER

Department of Mathematics, Mail Code 4408, Southern Illinois University, 1245 Lincoln Drive, Carbondale, Illinois 62901
e-mail address: wcalvert@siu.edu
URL: `http://www.math.siu.edu/calvert`

Department of Mathematics, Queens College – C.U.N.Y., 65-30 Kissena Blvd., Flushing, New York 11367 U.S.A.; Ph.D. Program in Mathematics, C.U.N.Y. Graduate Center, 365 Fifth Avenue, New York, New York 10016 U.S.A.
e-mail address: kkramer@qc.cuny.edu

Department of Mathematics, Queens College – C.U.N.Y., 65-30 Kissena Blvd., Flushing, New York 11367 U.S.A.; Ph.D. Programs in Mathematics & Computer Science, C.U.N.Y. Graduate Center, 365 Fifth Avenue, New York, New York 10016 U.S.A.
e-mail address: Russell.Miller@qc.cuny.edu
URL: `http://qc.edu/~rmiller`

Abstract. Working in the Blum-Shub-Smale model of computation on the real numbers, we answer several questions of Meer and Ziegler. First, we show that, for each natural number d, an oracle for the set of algebraic real numbers of degree at most d is insufficient to allow an oracle BSS-machine to decide membership in the set of algebraic numbers of degree $d+1$. We add a number of further results on relative computability of these sets and their unions. Then we show that the halting problem for BSS-computation is not decidable below any countable oracle set, and give a more specific condition, related to the cardinalities of the sets, necessary for relative BSS-computability. Most of our results involve the technique of using as input a tuple of real numbers which is algebraically independent over both the parameters and the oracle of the machine.

1998 ACM Subject Classification: F.1.1, F.1.3, I.1.2.

Key words and phrases: algebraic real numbers, Blum-Shub-Smale computation, BSS machine, oracle computation, relative computability.

Portions of this article describe results which appeared as [4] in the conference proceedings volume of the meeting *Computability and Complexity in Analysis* in Zhenjiang, China, 21-25 June 2010, and other results which were presented at the meeting *Logical Approaches to Barriers in Computing and Complexity* in Greifswald, Germany, 17-20 February 2010.

The first and third authors were partially supported by Grant #13397 from the Templeton Foundation. The seciond author was partially supported by NSF grant # DMS-0739346. The third author was partially supported by NSF grant # DMS-1001306, by grants numbered 61467-00 39, 62632-00 40, and 63286-00 41 from The City University of New York PSC-CUNY Research Award Program, and by Queens College Research Enhancement Program award # 90927-08 08.

DOI:10.2168/LMCS-???

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 complete account of this model is given in [1]. A program for such a machine consists of a finite set of instructions as described there, and the instructions are allowed to contain finitely many real parameters, since a single real number is viewed as a finite object. The program can add, multiply, subtract, or divide real numbers in its cells, can copy cell, can overwrite the contents of a cell with 0, and can use the relations $=$ and $<$ to compare the contents of two cells, forking according to whether the contents of those cells satisfy that relation. For our purposes, it will be convenient to assume that the forking instructions in the program compare the real number in a single given cell to 0, under either $=$ or $<$ or $>$. Such a machine has equivalent computing power to machines which can compare the contents of two different cells to each other.

Of course, the BSS model is not the only concept of computation on $\mathbb{R}$, nor should it be considered the dominant model. It corresponds to a view of the real numbers as a fixed structure, perhaps given axiomatically – defined, for instance, as the unique complete Archimedean ordered field, with field operations vouchsafed unto us mathematicians; as opposed to a view of real numbers as objects defined by Cauchy sequences or by Dedekind cuts in the rational numbers $\mathbb{Q}$, with operations derived from the analogous operations on $\mathbb{Q}$. There is no obvious method of implementing BSS machines by means of digital computers. More typically, as in [2, 1], one envisions BSS machines as a model for numerical computation in which features of approximation, rounding, and error analysis are treated as a separate posterior analysis. This failure invites a contrast with computable analysis, which treats real numbers as quantities approximated by rational numbers and is intended to reflect the capabilities of digital computers. However, the BSS model is of interest both for the analogy between it and the Turing model, which can be seen as BSS computation on the ring $\mathbb{Z}/(2)$, and because it reflects the intuitions of many mathematicians – dating back to the nineteenth century, and mostly outside of computer science – about the notion of algorithmic computation on $\mathbb{R}$

This paper will consider sets of algebraic real numbers, and other sets of tuples from $\mathbb{R}$, as oracles for BSS machines, and will examine the relative difficulty of deciding membership in such sets under the BSS model of computation. Several sections compare various sets of algebraic numbers under BSS-oracle computation, using these sets to demonstrate that there exists a rich structure of BSS-semidecidable degrees under BSS reducibility. Later sections consider questions about cardinality: to what extent the complexity of a subset of $\mathbb{R}$ (or $\mathbb{C}$) allows us to draw conclusions about its cardinality. The previous paper [11] by Meer and Ziegler focused attention on these issues, and here we answer several of the questions raised there. Our method adapts a known technique from BSS computability, and should be comprehensible to casual readers as well as to logicians and computer scientists. It requires significant use of algebraic properties of the real numbers, in addition to computability, reinforcing the general perception of the BSS model as an essentially algebraic approach to computation on $\mathbb{R}$, treating real numbers as indivisible finite items. In contrast, the use of computable analysis normally results in a more analytic approach to computation on $\mathbb{R}$. We the present authors comprise a number theorist and two computable model theorists with

experience in algorithms on (countable) Turing-computable fields, and thus we are more familiar with the algebraic side.

Our notation generally follows that of [11]. The set of all finite tuples of real numbers is denoted $\mathbb{R}^\infty$; the inputs and outputs of BSS machines on $\mathbb{R}$ all lie in this set, and the collective content of the cells of a BSS machine at a given stage in a computation may also be regarded as an element of $\mathbb{R}^\infty$. We use $\mathbb{A}$ to denote the set of all real numbers which are algebraic over the subfield $\mathbb{Q}$ of rational numbers. $\mathbb{A}$ is partitioned into subsets $\mathbb{A}_{=d}$, for each natural number d, so that $\mathbb{A}_{=d}$ contains those algebraic real numbers of degree exactly d over $\mathbb{Q}$. (Recall that the *degree* of x over $\mathbb{Q}$ is the vector space dimension over $\mathbb{Q}$ of the field $\mathbb{Q}(x)$ generated by x; equivalently, it is the degree of the minimal polynomial of x in $\mathbb{Q}[X]$.) We also write $\mathbb{A}_{\leq d} = \cup_{c \leq d} \mathbb{A}_{=c}$, the set of algebraic real numbers of degree $\leq d$. (In [11], this set was called $\mathbb{A}_d$; our notation is intended to distinguish $\mathbb{A}_{=d}$ from $\mathbb{A}_{\leq d}$.) By the definition of degree, $\mathbb{A}_{=0}$ is empty, and $\mathbb{A}_{=1}$ contains exactly the rational numbers themselves. We mention [13] as an excellent source for these and other algebraic preliminaries, and [5] for more advanced questions about algorithms on fields.

The following lemma is well known, and clear by induction on stages. It reflects the fact that the four field operations are the only operations which a BSS machine is able to perform.

Lemma 1.1. If M is a BSS machine using only the real parameters $\vec{z}$ in its program, then at every stage of the run of M on any input $\vec{x}$, the content of every cell lies in the field $\mathbb{Q}(\vec{z}, \vec{x})$. □

It is immediate from this lemma that the set $\mathbb{A}$ cannot be the image of $\mathbb{N}$ under any BSS-computable function, as it is not contained within any finitely generated field. (We will tend to use $\mathbb{N}$ to denote the subset of $\mathbb{R}$ consisting of the nonnegative integers, as here, whereas ω will denote the same set when not sitting inside of $\mathbb{R}$.) We say that $\mathbb{A}$ is not *BSS-countable*. On the other hand, $\mathbb{A}$ does satisfy the definition of *BSS semidecidability*, which is the best analogue of Turing-computable enumerability and has been studied more closely in the literature.

Definition 1.2. A set $S \subseteq \mathbb{R}^\infty$ is *BSS-semidecidable* if there exists a (partial) BSS-computable function with domain S, and *BSS-countable* if there exists a partial BSS-computable function mapping $\mathbb{N}$ onto S. A set S is *BSS-decidable* if its characteristic function χ_S is BSS-computable.

It is immediate that S is BSS-decidable if and only if both S and $(\mathbb{R}^\infty - S)$ are BSS-semidecidable. This justifies the analogy between BSS-semidecidability in $\mathbb{R}^\infty$ and computable enumerability in ω, and also dictates the use of the prefix "semi." The term *BSS-countable*, on the other hand, suggests that the set can be listed out, element by element, by a BSS machine, which is precisely the content of the definition above. (The related term *BSS-enumerable* has been used by other authors to denote the image of $\mathbb{R}^\infty$ under a BSS-computable partial function.) In the context of Turing computation, computable enumerability and semidecidability are equivalent, but in the BSS context, the set $\mathbb{A}$ distinguishes the two notions, being BSS-semidecidable but not BSS-countable. (On the other hand, every BSS-countable set is readily seen to be BSS-semidecidable.) The semidecision procedure for $\mathbb{A}$ is well-known: take any input x, and go through all nonzero polynomials $p(X) \in \mathbb{Q}[X]$, computing $p(x)$ for each. If ever $p(x) = 0$, the machine halts. The ability to go through the polynomials in $\mathbb{Q}[X]$ follows from the BSS-countability of $\mathbb{Q}[X]$, which

in turn follows from the BSS-countability of $\mathbb{Q}$. (A similar result applies to the set of algebraically dependent tuples in $\mathbb{R}^\infty$; see for instance [7].)

The two questions which gave rise to this paper were posed by Meer and Ziegler in [11]. Both use the notion of a *BSS reduction*, analogous to Turing reductions. An *oracle BSS machine* is essentially a BSS machine with the additional ability to take any finite tuple (which it has already assembled on the cells of its tape), ask an oracle set A whether that tuple lies in A, and fork according to whether the answer is positive or negative. The oracle A should be a subset of $\mathbb{R}^\infty$, of course, and we will write M^A to represent an oracle BSS program (or machine) equipped with an oracle set A. More precisely,

Definition 1.3. An oracle BSS machine using an oracle set $B \subseteq \mathbb{R}^\infty$ is a BSS machine with an additional type of node called an oracle node. This node branches according as $x \in B$, where x is some previously computed element.

(This is exactly the definition given in [11], and is equivalent to any reasonable formalization of the implicit definition given in Problem 10.2 of [2].) Oracle BSS programs can be enumerated (by tuples from $\mathbb{R}^\infty$) in much the same manner as regular BSS programs. If $B \subseteq \mathbb{R}^\infty$ and the characteristic function χ_B can be computed by an oracle BSS machine M^A with oracle A, then we write $B \leq_{BSS} A$, and say that B is *BSS-reducible* to A, calling M the *BSS reduction* of B to A. Should $B \leq_{BSS} A$ and also $A \leq_{BSS} B$, we write $A \equiv_{BSS} B$ and call the two sets *BSS-equivalent*. All this is exactly analogous to oracle Turing computation on subsets of ω. The first question regards the connection of this reducibility with algebra.

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

$$\mathbb{A}_{\leq 0} <_{BSS} \mathbb{A}_{\leq 1} <_{BSS} \cdots \mathbb{A}_{\leq n} <_{BSS} \cdots?$$

That $\mathbb{A}_{\leq d-1} \leq_{BSS} \mathbb{A}_{\leq d}$ is immediate for all d; see Lemma 5.2 below. The focus of the question is on the lack of any reduction in the opposite direction.

Meer and Ziegler credit the second question to an anonymous referee of [11].

Question 2. Let $\mathbb{A}$ be the set of algebraic numbers in $\mathbb{R}$, i.e. those which are roots of a nonzero polynomial in $\mathbb{Q}[X]$. Also, let $\mathbb{H}$ be the Halting Problem for BSS computation on $\mathbb{R}$, as described in [11] (Actually, a passing implicit reference is made to this set in [2, §8], in the guise of the halting set of a universal machine). Is it true that $\mathbb{H} \not\leq_{BSS} \mathbb{A}$? And more generally, could any countable subset of $\mathbb{R}^\infty$ contain enough information to decide $\mathbb{H}$?

That $\mathbb{A} \leq_{BSS} \mathbb{H}$ is immediate. Let P be the BSS program which, on input $x \in \mathbb{R}$, plugs x successively into each nonzero polynomial $p(X)$ in (the BSS-countable set) $\mathbb{Q}[X]$ and halts if ever $p(x) = 0$. Then $x \in \mathbb{A}$ iff the program P halts on input x. (Similarly, every BSS-semidecidable set is BSS-decidable in $\mathbb{H}$, and indeed 1-reducible to $\mathbb{H}$ in the BSS model.) Again, the question focusses on the lack of any reduction in the opposite direction.

Section 2 gives the basic technical lemma used in this paper to address such questions, and Section 4 applies it to give a positive answer to Question 1. To aid the reader's comprehension, Section 3 describes the solution to Question 1 in the specific case $\mathbb{A}_{\leq 2} <_{BSS} \mathbb{A}_{\leq 1}$. Section 5 considers other possible reductions among the sets $\mathbb{A}_{=d}$ for different values of d, and among unions of these sets. As a corollary, we define a new embedding of the partial order $(\mathcal{P}(\omega), \subseteq)$ into the partial order of the BSS-semidecidable degrees under BSS reducibility. Such embeddings, including the similar one already derived in [11], reveal a high level of complexity within the latter structure. In Section 6, we answer Question

2 by showing that no countable subset of $\mathbb{R}^\infty$ contains enough information to decide the halting problem in the BSS model. We also prove there a theorem relating BSS degrees to cardinality, showing that for infinite subsets $S \subseteq \mathbb{R}$ and $C \subseteq \mathbb{R}^\infty$, if $S \leq_{BSS} C$, then the local cardinality (in a technical sense defined in that section) of S cannot be greater than the (global, i.e. usual) cardinality of C. Finally, in Section 8, we offer analogies of these observations for BSS computation on the complex numbers, where the situation is far less messy.

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 Sections 3 and 4, this method will be extended to give answers about BSS-computability below certain oracles. However, even the non-relativized version yields straightforward proofs of several well-known results about BSS-decidable sets, as we will see shortly after describing the method.

In many respects, our method is equivalent to the method, used by many others, of considering BSS computations as paths through a finite-branching tree of height ω, branching whenever there is a forking instruction in the program. However, we think that the intuition for our method can be more readily explained to a mathematician unfamiliar with computability theory. Our main lemma says that near any transcendental input in its domain, the values in a BSS-machine computation must be defined by rational functions of the input. Where previous proofs usually made arguments about countable sets of terminal nodes in the tree of possible computations, we simply use the transcendence of this element.

Lemma 2.1. Let M be a BSS-machine, and $\vec{z}$ the finite tuple of real parameters mentioned in the program for M. Suppose that $\vec{y} \in \mathbb{R}^{m+1}$ is a tuple of real numbers algebraically independent over the field $Q = \mathbb{Q}(\vec{z})$, such that M converges on input $\vec{y}$. Then there exists $\epsilon > 0$ and rational functions $f_0, \ldots, f_n \in Q(\vec{Y})$, (that is, rational functions of the variables $\vec{Y}$ with coefficients from Q) such that for all $\vec{x} \in \mathbb{R}^{m+1}$ with $|\vec{x} - \vec{y}| < \epsilon$, M also converges on input $\vec{x}$ with output $\langle f_0(\vec{x}), \ldots, f_n(\vec{x})\rangle \in \mathbb{R}^{n+1}$.

Proof The intuition is that by choosing $\vec{x}$ sufficiently close to $\vec{y}$, we can ensure that the computation on $\vec{x}$ branches in exactly the same way as the computation on $\vec{y}$, at each of the (finitely many) branch points in the computation on $\vec{y}$. More formally, say that the run of M on input $\vec{y}$ halts at stage t, and that at each stage $s \leq t$, the non-zero cells contain the reals $\langle f_{0,s}(\vec{y}), \ldots, f_{n_s,s}(\vec{y})\rangle$. Lemma 1.1 shows that all $f_{i,s}(\vec{y})$ lie in the field $Q(\vec{y})$, so each $f_{i,s}$ may be viewed as a rational function of $\vec{y}$ with coefficients in Q. Indeed, each rational function $f_{i,s}$ is uniquely determined in $Q(\vec{Y})$, since $\vec{y}$ is algebraically independent over Q.

Let F be the finite set $\{f_{i,s}(\vec{Y}) : s \leq t \;\&\; i \leq n_s \;\&\; f_{i,s} \notin Q\}$ of nonconstant rational functions used in the computation. The union U of all preimages $f_{i,s}^{-1}(0)$ with $f_{i,s} \in F$ is closed in $\mathbb{R}^{m+1}$, and by algebraic independence, $\vec{y}$ does not lie in U, so there exists an $\epsilon > 0$ such that the ϵ-ball $B_\epsilon(\vec{y}) = \{\vec{x} \in \mathbb{R}^{m+1} : |\vec{x} - \vec{y}| < \epsilon\}$, does not intersect U, and is contained within the domain of each $f_{i,s} \in F$. Indeed, for all $f_{i,s} \in F$ and all $\vec{x} \in B_\epsilon(\vec{y})$, $f_{i,s}(\vec{x})$ and $f_{i,s}(\vec{y})$ must have the same sign, since $B_\epsilon(\vec{y})$ is a path-connected set.

Now fix any $\vec{x} \in B_\epsilon(\vec{y})$. We claim that in the run of M on input $\vec{x}$, at each stage $s \leq t$, the cells will contain precisely $\langle f_{0,s}(\vec{x}), \ldots, f_{n_s,s}(\vec{x})\rangle$ and the machine will be in the same state in which it was at stage s on input $\vec{y}$. This is clear for stage 0, and we continue by induction, going from each stage $s < t$ to stage $s + 1$. If the machine executed a copy

instruction or a field operation in this step, then the result is clear, by inductive hypothesis. Otherwise, the machine executed a fork instruction, comparing some $f_{i,s}(\vec{x})$ with 0. But we saw above that $f_{i,s}(\vec{x})$ and $f_{i,s}(\vec{y})$ have the same sign (or else $f_{i,s}(y) = 0$, in which case $f_{i,s}$ is the constant function 0), so in both runs the machine entered the same state at stage $s + 1$, leaving the contents of all cells intact. This completes the induction, and leaves us only to remark that therefore, at stage t, the run of M on input $\vec{x}$ must also have halted, with $\langle f_{0,t}(\vec{x}), \ldots, f_{n,s}(\vec{x})\rangle$ in its cells as the output. □

(If our BSS machines were allowed to compare the contents of two cells under $=$ or $<$, as is standard, then our set F would have to consist of all nonconstant differences $(f_{i,s} - f_{j,s})$. The proof would still work, but the method above is simpler.)

Lemma 2.1 provides quick proofs of several known results, including the undecidability of every proper subfield $F \subset \mathbb{R}$.

Corollary 2.2. *No BSS-decidable subset $S \subseteq \mathbb{R}^n$ can be both dense and co-dense in $\mathbb{R}^n$.*

Proof Since the characteristic function χ_S is BSS-computable, say by a machine with parameters $\vec{z}$, Lemma 2.1 shows that for every $\vec{y} \in \mathbb{R}^n$ with coordinates algebraically independent over $\vec{z}$, χ_S is constant in some neighborhood of $\vec{y}$. □

Indeed, the same proof shows that any BSS-computable total function with discrete image must be constant on each of the ϵ-balls given by Lemma 2.1.

Corollary 2.3. *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 $\vec{z}$ such that every point on the boundary of S has coordinates algebraically dependent over $\vec{z}$. In particular, if M computes χ_S, then its parameters may serve as $\vec{z}$.*

Proof This is immediate from Lemma 2.1. □

Of course, Corollaries 2.2 and 2.3 have been deduced long since from other known results, 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 methods to be used in the following sections.

3. Application to Algebraic Numbers of Degree 2

We know that $\mathbb{A}_{\leq 1} \not\leq_{BSS} \mathbb{A}_{\leq 0}$, since $\mathbb{A}_{\leq 0} = \emptyset$ and $\mathbb{A}_{\leq 1} = \mathbb{Q}$ and it is already known (and seen again in Corollary 2.2 above) that $\mathbb{Q}$ is BSS-undecidable. To introduce our main result, we prove the corresponding result one level further up. The proof constitutes a simple introduction to the method we used in the abstract [3] to prove the full Theorem 4.1. In the next section, we will give a separate new proof of Theorem 4.1, more elegant than the first one but less transparent, especially for readers not expert in field theory, who may prefer to look up the proof in [3].

Theorem 3.1. $\mathbb{A}_{\leq 2} \not\leq_{BSS} \mathbb{A}_{\leq 1}$.

Proof Suppose that M is an oracle BSS machine with real parameters $\vec{z}$, such that $\mathcal{M}^{\mathbb{Q}}$ computes the characteristic function of $\mathbb{A}_{\leq 2}$. (Of course $\mathbb{A}_{\leq 1}$ is just $\mathbb{Q}$ itself.) Fix any $y \in \mathbb{R}$ which is transcendental over the field $Q = \mathbb{Q}(\vec{z})$, and run $M^{\mathbb{Q}}$ on input y. Of course, this computation must halt after finitely many steps and output 0. As in the proof of Lemma 2.1, 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, it is no longer sufficient for us to run $M^{\mathbb{Q}}$ on an arbitrary $x \in B_\epsilon(y) \cap \mathbb{A}_{\leq 2}$, because such an x might lie in $\mathbb{Q}$, or might have $f(x) \in \mathbb{Q}$ for some $f \in F$, and in this case the computation on input x might ask its oracle whether $f(x) \in \mathbb{Q}$ and would then branch differently from the computation on input y. (Of course, for all $f \in F$, $f(y) \notin \mathbb{Q}$, since $f(y)$ must be transcendental over $\mathbb{Q}$ for nonconstant f.) So we must establish the existence of some $x \in B_\epsilon(y) \cap \mathbb{A}_{\leq 2}$ with $f(x) \notin \mathbb{Q}$ for all of the (finitely many) $f \in F$. Of course, we do not need to give any effective procedure which produces this x; its existence is sufficient.

For each $f \in F$, choose $g, h \in Q[Y]$ with $f = \frac{g}{h}$. Thus $f(x) = a$ iff $g(x) - ah(x) = 0$. In game-theoretic terms, the opponent first chooses the functions in F, after which we choose x, and then his functions pick out the value of a, based on our x. So we must ensure that our choice of x makes $0 \neq g(x) - ah(x)$ for every $a \in \mathbb{Q}$.

We need the following lemma from calculus.

Lemma 3.2. If $f \in \mathbb{R}(X)$ with $b \in \mathrm{dom}(f)$, and there are positive values of v arbitrarily close to 0 such that $f(b+v) = f(b-v)$, then $f'(b) = 0$. □

Given the collection F, we fix some $b \in \mathbb{Q}$ such that $|y - b| < \frac{\epsilon}{2}$ and such that b lies in the domain of every $f \in F$ and all $f'(b) \neq 0$. Since each $f \in F$ is differentiable and nonconstant, each f rules out only finitely many values, and F is finite, so such a b must exist. Now Lemma 3.2 makes it clear that for some sufficiently small $\delta > 0$, every $u \in \mathbb{Q}$ with $0 < \sqrt{u} < \delta$ satisfies $f(b + \sqrt{u}) \neq f(b - \sqrt{u})$ for every $f \in F$. So fix $x = b + \sqrt{u}$ for some $u \in \mathbb{Q}$ with $0 < \sqrt{u} < \min(\delta, \frac{\epsilon}{2})$, for which $\sqrt{u} \notin Q$. (The finitely generated field Q cannot contain every $\sqrt{u}$ in this interval, as every subfield of a finitely generated field is itself finitely generated. For a proof, see [12, Thm. 3.1.4, p. 82].) Thus $|x - y| < \epsilon$ and all $f \in F$ satisfy $f(b + \sqrt{u}) \neq f(b - \sqrt{u})$. We write $\overline{x} = b - \sqrt{u}$ for the conjugate of x over $\mathbb{Q}$.

Now let $p(X) = X^2 - 2bX + (b^2 - u)$, which is the minimal polynomial of x and of $\overline{x}$, over Q as well as over $\mathbb{Q}$. For each $f \in F$, we apply the division algorithm:

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

with $r_g(X)$ and $r_h(X)$ both linear polynomials. We write $r_g(X) = g_1 X + g_0$ and $r_h(X) = h_1 X + h_0$, with all coefficients in Q. Now $f(x) = \frac{q_g(x) \cdot 0 + r_g(x)}{q_h(x) \cdot 0 + r_h(x)} = \frac{r_g(x)}{r_h(x)}$, and likewise $f(\overline{x}) = \frac{r_g(\overline{x})}{r_h(\overline{x})}$. Since $f(x) \neq f(\overline{x})$, this shows that $\frac{r_g(X)}{r_h(X)}$ cannot be constant, so $r_g(X)$ is not a scalar multiple of $r_h(X)$.

Suppose that $a = f(x) = \frac{g(x)}{h(x)}$ lies in Q. Then

$$g_1 \cdot (b + \sqrt{u}) + g_0 = r_g(x) = g(x) = ah(x) = ar_h(x) = ah_1 \cdot (b + \sqrt{u}) + ah_0,$$

and this equation can be re-expressed as

$$(g_1 b + g_0 - ah_1 b - ah_0) + \sqrt{u}(g_1 - ah_1) = 0.$$

Here both expressions in parentheses lie in Q, but we chose u with $\sqrt{u} \notin Q$, and so

$$g_1 b + g_0 = a(h_1 b + h_0) \qquad \text{and} \qquad g_1 = ah_1.$$

But this immediately shows that $r_g(X) = g_1 X + g_0 = ah_1 X + ah_0 = ar_h(X)$, contradicting the statement above that $r_g(X)$ is not a scalar multiple of $r_h(X)$.

With this contradiction, we see that $f(x) \notin \mathbb{Q}$ (and indeed $f(x) \notin Q$). Since this holds for all $f \in F$, and since $|x - y| < \epsilon$, it is now clear (just as in Lemma 2.1) that the computation $M^{\mathbb{Q}}(x)$ follows the exact same path as $M^{\mathbb{Q}}(y)$, and outputs the same answer. However, $y \notin \mathbb{A}_{\leq 2}$ since y was transcendental over Q, whereas $x = b + \sqrt{u} \in \mathbb{A}_{\leq 2}$. Thus the machine M with oracle $\mathbb{Q}$ did not compute the characteristic function of $\mathbb{A}_{\leq 2}$. □

4. Application to Algebraic Numbers in General

Theorem 4.1. *For every $d > 0$, $\mathbb{A}_{\leq d} \not\leq_{BSS} \mathbb{A}_{\leq d-1}$. In particular, $\mathbb{A}_{=d} \not\leq_{BSS} \mathbb{A}_{\leq d-1}$.*

Proof The two statements in the theorem are equivalent, because $\mathbb{A}_{\leq d} \equiv_{BSS} \mathbb{A}_{\leq d-1} \oplus \mathbb{A}_{=d}$ (where $A \oplus B = \{\langle 0, \vec{a}\rangle : \vec{a} \in A\} \cup \{\langle 1, \vec{b}\rangle : \vec{b} \in B\}$). We prove the latter.

As usual, suppose that M is an oracle BSS machine which, given oracle $\mathbb{A}_{\leq d-1}$, computes $\mathbb{A}_{=d}$. Let $\vec{z}$ be the finite tuple of real parameters used by M, and set $Q = \mathbb{Q}(\vec{z})$, the field generated by these parameters. Then its algebraic portion $Q \cap \overline{\mathbb{Q}}$ is also finitely generated, since subfields of finitely generated fields are finitely generated, (see [12, Thm. 3.1.4, p. 82]). Being an algebraic extension, $Q \cap \overline{\mathbb{Q}}$ thus has finite dimension over $\mathbb{Q}$, so Q cannot contain d-th roots of all prime numbers. Theorem 9.1 from Chapter 6 of [9] shows that there exists a prime whose real d-th root α satisfies $[Q(\alpha) : Q] = d$. We also fix any real number y transcendental over Q, and let F be the set of all nonconstant rational functions $f \in Q(X)$ such that $f(y)$ appears in some cell during the run of M on input y with oracle $\mathbb{A}_{\leq d-1}$. By assumption this run halts and outputs 0, so F is a finite set. As before, we fix $\epsilon > 0$ such that $f(x) \cdot f(y) > 0$ for all $x \in B_\epsilon(y)$. Fix any $b \in \mathbb{Q}$ with $|b - y| < \frac{\epsilon}{2}$ and with $f'(b) \neq 0$ for all $f \in F$. (Each such f is a nonconstant rational function, and so $f'(X)$, being rational and nonzero, can only have finitely many roots.)

Now there exist d distinct embeddings $\sigma_j : \mathbb{Q}(\alpha) \to \overline{\mathbb{Q}}$, with $j = 1, \ldots, d$. With Q and $\mathbb{Q}(\alpha)$ linearly disjoint, each σ_j extends to an embedding $\overline{\sigma}_j : Q(\alpha) \to \overline{Q(\alpha)}$, with $\overline{\sigma}_j \restriction Q$ being the identity, and these are all the embeddings (over Q) of $Q(\alpha)$ into its algebraic closure.

Lemma 4.2. In this situation, let S be the set of rational numbers c such that $\beta_c = f(b + c\alpha)$ has degree $< d$ over Q. Then S is finite.

Proof For any $c \in S$, we have $Q(\beta_c) \subsetneq Q(\alpha)$, with inclusion because $\beta_c = f(b + c\alpha)$ and $f \in Q(X)$, and without equality because $[Q(\beta_c) : Q] < d = [Q(\alpha) : Q]$. Hence some $\overline{\sigma}_{j(c)}$ embeds $Q(\alpha)$ into its algebraic closure and equals the identity on $Q(\beta_c)$ but not on $Q(\alpha)$. But α has only d conjugates over Q, so if S were infinite, it would contain an infinite subset S' for which one particular embedding $\overline{\sigma} = \overline{\sigma}_j$ would have $\overline{\sigma}(\beta_c) = \beta_c$ for all $c \in S'$, but $\overline{\sigma}(\alpha) \neq \alpha$.

Let $\gamma = \frac{\overline{\sigma}(\alpha)}{\alpha} \neq 1$. Now for $c \in S'$,

$$f(b + c\alpha) = \beta_c = \overline{\sigma}(\beta_c) = \overline{\sigma}(f(b + c\alpha)) = f(b + c \cdot \overline{\sigma}(\alpha)).$$

So the equation $f(b + X) = f(b + \gamma X)$ holds whenever $X = c\alpha$ with $c \in S'$. Since S' is infinite, this must be an identity of rational functions, and by differentiating it (and recalling that $\gamma \neq 1$), we see that $f'(b) = 0$, contradicting our choice of b. □

So we may fix some positive rational $c < \frac{\epsilon}{|2\alpha|}$ such that for all $f \in F$, $f(b + c\alpha)$ has degree $\geq d$ over Q. (In fact, this degree must then equal d, since $f(b + c\alpha) \in Q(\alpha)$.) Let $x = b + c\alpha$. Then $|y - x| \leq |y - b| + |b - x| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$, so that for all $f \in F$, $f(x)$ and $f(y)$ have the same sign and both lie outside of the oracle set $\mathbb{A}_{\leq d-1}$. Therefore the computation of M on input x with oracle $\mathbb{A}_{\leq d-1}$ halts and outputs 0, yet $x \in \mathbb{A}_{=d}$, so this machine does not decide the set $\mathbb{A}_{=d}$. □

Thus we have a positive answer to Problem 1. Meer and Ziegler also posed a similar problem: whether $\mathbb{A}_{\leq d} \equiv_{BSS} \mathbb{A}_{=d}$ for every d. They had noted that this holds when $d \leq 2$, but in fact it holds for no other d than those. Since $\mathbb{A}_{\leq d} \equiv_{BSS} \mathbb{A}_{\leq d-1} \oplus \mathbb{A}_{=d}$, the problem essentially asks whether $\mathbb{A}_{\leq d-1} \leq_{BSS} \mathbb{A}_{=d}$. In the next section, Theorem 5.3 will use the same technique as Theorem 4.1 to show that for $d - 1 > 0$, $\mathbb{A}_{=d-1} \leq_{BSS} \mathbb{A}_{=d}$ iff $(d - 1)$ divides d.

5. Results on Sets of Degrees

Now we create more general versions, mostly along the same lines as Theorem 4.1. To make the notation as powerful as possible, we extend it: for any subset $S \subseteq \omega$, we will write $\mathbb{A}_S = \cup_{d \in S} \mathbb{A}_{=d}$, the set of all algebraic real numbers whose degrees over $\mathbb{Q}$ lie in S.

Lemma 5.1. For every $S \subseteq \omega$, $\mathbb{A}_S$ is a BSS-semidecidable set, and the semidecision procedure is uniform in one real parameter for S.

Proof The BSS machine M with range $\mathbb{A}_S$ has one real parameter $z_S = \sum_{n \in S} 2^{-n}$, whose binary representation forms a code for the set $S \subseteq \omega$. From this parameter, given any n, the machine can determine whether or not $n \in S$. On input x, the machine searches through all irreducible $h(X) \in \mathbb{Q}[x]$ until it finds one with $h(x) = 0$. Then it uses z_S to decide whether $\deg(h) \in S$, and halts only on a positive answer. (It was known as far back as 1882, in the work [8] of Kronecker, that there is a decision procedure for irreducibility of polynomials in $\mathbb{Q}[X]$.) □

Our first result on these BSS-semidecidable sets is immediate.

Lemma 5.2. If $S \subseteq T \subseteq \omega$, then $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$.

Proof With an $\mathbb{A}_T$ oracle, a BSS machine can decide whether an input x lies in $\mathbb{A}_T$. If it does not (and $S \subseteq T$), then $x \notin \mathbb{A}_S$; whereas if it does, then one merely searches for the minimal polynomial of x in $\mathbb{Q}$, and checks whether its degree lies in S. (For this purpose, the machine needs the parameter z_S from Lemma 5.1.) □

Theorem 5.3. *For every $d > 0$ in ω and every set $S \subset \omega$ with $S \cap d\mathbb{Z} = \emptyset$, $\mathbb{A}_{=d} \not\leq_{BSS} \mathbb{A}_S$.*

Proof Essentially the same construction as in Theorem 4.1 applies, and we use the same notation. In addition to the argument given there, we must show that for every $f \in F$, $f(x)$ cannot lie in the new oracle set $\mathbb{A}_S$, as opposed to $\mathbb{A}_{\leq d-1}$, which was the oracle used in Theorem 4.1. For this purpose, a few revisions are needed. First, with Q still denoting the field generated by the parameters of M, we let $K = Q \cap \overline{\mathbb{Q}}$, and let $F_K = F \cap K(X)$ be the set of nonconstant functions in $K(X)$ appearing in the computation by $M^{\mathbb{A}_S}$ on the transcendental input y. Now K is a finite algebraic extension of $\mathbb{Q}$ within $\mathbb{R}$, and we let L be the Galois extension of $\mathbb{Q}$ generated by K within the complex field $\mathbb{C}$. Moreover, we will

choose our x to have degree d not only over $\mathbb{Q}$, and not only over Q, but also over L. Since L and Q are both finitely generated, this can be done.

Now let $f \in F$ and consider $a = f(x)$. First, if $f \notin F_K$, then every expression of $f(X)$ involves transcendentals over $\mathbb{Q}$. Suppose that $f(X) = f^*(t_1, \ldots, t_m, X)$, where $f^* = \frac{g^*}{h^*} \in K(T_1 \ldots, T_m, X)$ and $\{t_1, \ldots, t_m\}$ (which we write as $\{\vec{t}\}$) is algebraically independent over $\mathbb{Q}$. If $a = f(x) = f^*(\vec{t}, x)$ lies in $\mathbb{A}$, then $g^*(\vec{t}, x) = ah^*(\vec{t}, x)$, so all coefficients in $g^*(\vec{T}, x) - ah^*(\vec{T}, x)$ are zero, which can happen for only finitely many values of x (since f is nonconstant). So, in the revised proof, we make sure to avoid those finitely many values of x (for each $f \in F - F_K$) when making our choice of x close to y.

Next we suppose that $a = f(x)$ for an $f \in F_K$. The same proof as in Theorem 4.1 shows that $L(a)$ cannot be a proper subfield of $L(x)$. (The argument there for Q goes through now with Q replaced by L.) Now, however, it is not guaranteed that a has degree $< d$ over L, and so it is possible that $L(a) = L(x)$. In this case, we know that $[L(a) : L] = [L(x) : L] = d$, and so a has minimal polynomial $q(X) \in L[X]$ of degree d. If a is transcendental over $\mathbb{Q}$, then of course $a \notin \mathbb{A}_S$; so assume a is algebraic, and let $p(X) \in \mathbb{Q}[X]$ be the minimal polynomial of a over $\mathbb{Q}$. Then $p(X)$ is just the product of $q(X)$ with several images of $q(X)$ under automorphisms of L. Specifically, if E is the subfield of L generated by the coefficients of $q(X)$, then

$$p(X) = \Pi_{\sigma \in G}\ q^\sigma(X),$$

where G is a set of representatives for the right cosets of $\mathrm{Gal}(L/E)$ in $\mathrm{Gal}(L/\mathbb{Q})$, and where $q^\sigma(X)$ is the image of $q(X)$ under the map σ on its coefficients. (This formula for the minimal polynomial $p(X)$ of the roots of q over the smaller subfield $\mathbb{Q}$ requires the extension $\mathbb{Q} \subseteq L$ to be Galois. This is why we used the Galois extension L, rather than just the fields K or Q.) It follows that $\deg(p(X)) = d \cdot [E : \mathbb{Q}]$. Since S contains no nonzero multiples of d, we see that $\deg(p(X)) \notin S$, and hence $a \notin \mathbb{A}_S$. The rest of the proof then proceeds exactly as in Theorem 4.1. □

For reference in Theorem 5.14, we note that in the above proof, when $L(a) = L(x)$, we showed that $[\mathbb{Q}(a) : \mathbb{Q}] = d \cdot [E : \mathbb{Q}]$ is a multiple of d by a factor $\leq [L : \mathbb{Q}]$. Here all that was needed was for $[\mathbb{Q}(a) : \mathbb{Q}]$ to be a multiple of d, but there we will need uniformity in the size of the multiple.

We will see below that the converse of Lemma 5.2 fails. However, we can prove a substitute for it, which yields the same principal results (Corollaries 5.5 and 5.7, below) that one would have derived from the converse.

Theorem 5.4. *Let P be the set of all prime numbers in ω. Then for all S and T in the power set $\mathcal{P}(P)$, $A_S \leq_{BSS} A_T$ if and only if $S \subseteq T$.*

Proof The backward direction follows from Lemma 5.2, and the forward from Theorem 5.3, since no element of P divides any other element of P. □

This allows us to show that the BSS-semidecidable degrees, which form the analogue for BSS computation of the computably enumerable Turing degrees, are a structure of significant complexity. In [11, Theorem 16], Meer and Ziegler showed that there exist uncountably many BSS-semidecidable degrees, pairwise incomparable with each other, and Corollary 5.5 (below) could also be proven using their sets $\mathbb{Q}_{\sqrt{p}}$, and unions of those sets, in place of the sets $\mathbb{A}_{=p}$ and their unions. In the case of additive BSS-machines, some related results appear in [6].

Corollary 5.5. *There exists a subset $\mathcal{L}$ of the BSS-semidecidable degrees such that as partial orders, $(\mathcal{L}, \leq_{BSS})$ is isomorphic to $(\mathcal{P}(\omega), \subseteq)$.*

Proof We have $(\mathcal{P}(\omega), \subseteq) \cong (\mathcal{P}(P), \subseteq)$, and Theorem 5.4 shows that the latter partial order embeds into the BSS-semidecidable degrees via the map $S \mapsto \mathbb{A}_S$. □

In Corollary 5.5, the isomorphism respects partial orders, but it is open whether it maps meets and joins within the lattice $(\mathcal{P}(\omega), \subseteq)$ to meets and joins within the upper semilattice of the BSS degrees, or within the sub-upper semilattice of the BSS-semidecidable degrees.

By adding the following elementary set-theoretic fact to Corollary 5.5 we create a different proof of [11, Thm. 16].

Lemma 5.6 (Folklore)**.** There exists a collection $\mathcal{D} \subseteq \mathcal{P}(\omega)$ of cardinality 2^ω satisfying:

$$(\forall A \in \mathcal{D})(\forall B \in \mathcal{D})[A \subseteq B \implies A = B].$$

Proof Recall that for $A, B \subseteq \omega$, $A \oplus B = \{2n : n \in A\} \cup \{2n+1 : n \in B\}$. Let $\mathcal{D} = \{S \oplus S^C : S \in \mathcal{P}(\omega)\}$, where S^C is the complement of S. □

Corollary 5.7 (first shown in [11])**.** *There exists an antichain (under $\leq_{BSS}$) of cardinality 2^ω within the BSS-semidecidable degrees.* □

The remainder of this section is devoted to the question of when we can have $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$ without having $S \subseteq T$. The restriction on S in Theorem 5.3 is that it does not contain any multiples of d. This leaves open the full converse of Lemma 5.2, and it is natural to conjecture that $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$ if and only if $S \subseteq T$. The authors were surprised to find that this conjecture fails, and moreover, that it can fail even for finite sets S. To introduce this failure, we give a specific example, which builds on a technique introduced by Meer and Ziegler in [11, Lemma 17], in which they proved that $\mathbb{A}_{=1} \leq_{BSS} \mathbb{A}_{=2}$.

Proposition 5.8. $\mathbb{A}_{=2} \leq_{BSS} \mathbb{A}_{=6}$.

Proof The machine for this reduction, with oracle $\mathbb{A}_{=6}$, is simple. It has $\sqrt[3]{2}$ as a parameter, and on input x, it asks its oracle whether $x + \sqrt[3]{2} \in \mathbb{A}_{=6}$. If not, then it outputs "No" immediately; while if so, then it searches through the irreducible polynomials in $\mathbb{Q}[X]$ until it finds the minimal polynomial $h(X)$ of x, and then outputs "Yes" if h has degree 2 and "No" otherwise.

To see that this procedure computes $\mathbb{A}_{=2}$ correctly, we consider the algebraicity of the input x. If $x \notin \mathbb{A}$, then $x + \sqrt[3]{2}$ is certainly also transcendental, hence $\notin \mathbb{A}_{=6}$, and the machine outputs "No." If $x \in \mathbb{A}_{(\omega - \{2\})}$, then the machine must output "No": either immediately, if $x + \sqrt[3]{2} \notin \mathbb{A}_{=6}$, or else after finding the minimal polynomial of x. Finally, if $x \in \mathbb{A}_{=2}$, then we claim that $x + \sqrt[3]{2} \in \mathbb{A}_{=6}$, and so the machine goes into its search for the minimal polynomial of x, and finds that $x \in \mathbb{A}_{=2}$.

To see that $x + \sqrt[3]{2} \in \mathbb{A}_{=6}$ when $x \in \mathbb{A}_{=2}$, let F be the field $\mathbb{Q}(x + \sqrt[3]{2})$. Then $F \subseteq \mathbb{Q}(x, \sqrt[3]{2})$, and we show that indeed equality holds. First, $F(x) = \mathbb{Q}(x, \sqrt[3]{2})$, and so $\mathbb{Q}(x, \sqrt[3]{2})$ must have degree either 1 or 2 over F. But also $F(\sqrt[3]{2}) = \mathbb{Q}(x, \sqrt[3]{2})$, so $\mathbb{Q}(x, \sqrt[3]{2})$ must have degree either 1 or 3 over F. The only consistent solution is that $F = \mathbb{Q}(x, \sqrt[3]{2})$, so $[F : \mathbb{Q}] = 6$. Thus $x + \sqrt[3]{2} \in \mathbb{A}_{=6}$ as required. □

The only special aspect of the numbers 2 and 6 here was that $\frac{6}{2}$ is an integer relatively prime to 2.

Proposition 5.9. *Let p and q be any positive, relatively prime integers. Then $\mathbb{A}_{=p} \leq_{BSS} \mathbb{A}_{=pq}$.*

Proof The exact same proof as in Proposition 5.8, with 2 replaced by p, 6 by pq, and $\sqrt[3]{2}$ by any element of $\mathbb{A}_{=q}$ one may choose. □

The preceding argument can be uniformized, via a specific effective version of the Theorem of the Primitive Element. The basic result was proven by Kronecker; we suggest [5, Lemma 17.12] for a description. Here we simply adapt that proof to the BSS setting.

Theorem 5.10 (Effective Theorem of the Primitive Element, after Kronecker)**.** *There is a BSS-computable function which, given any two finite (possibly empty) tuples $\langle x_1, \ldots, x_n \rangle$ and $\langle y_1, \ldots, y_m \rangle$ of real numbers such that $\{x_1, \ldots, x_n\}$ is algebraically independent over $\mathbb{Q}$ and all y_i are algebraic over $\mathbb{Q}(x_1, \ldots, x_n)$, outputs a single real number z such that $\mathbb{Q}(\vec{x}, \vec{y}) = \mathbb{Q}(\vec{x}, z)$. (This z is called a* primitive element *for the field $\mathbb{Q}(\vec{x}, \vec{y})$ over $\mathbb{Q}(\vec{x})$.)*

Proof We use the procedure from [5, Lemma 17.12], with $K = \mathbb{Q}(\vec{x})$, noting that this K has a (Turing-computable) splitting algorithm, uniformly in n, so that our machine can begin by finding the minimal polynomial of each y_i over $K(y_1, \ldots, y_{i-1})$, for $i = 1, \ldots, m$. It can also find the minimal polynomial $f(Y)$ of the element $y = T_1 y_1 + \cdots + T_m y_m$ over the function field $K(T_1, \ldots, T_m)$, clearing denominators so that $f \in K[\vec{T}, Y]$. As argued in [5], for any $a_1, \ldots, a_m \in K$ such that $\frac{\partial f}{\partial Y}(a_1, \ldots, a_m, a_1 y_1 + \cdots + a_m y_m) \neq 0$, the element $z = a_1 y_1 + \cdots + a_m y_m$ generates $K(\vec{y}) = \mathbb{Q}(\vec{x}, \vec{y})$ over K, and our machine will output such a z.

For BSS machines, finding an appropriate tuple $\langle a_1, \ldots, a_m \rangle$ requires the machine to enumerate the elements of K, searching for such a tuple. Recall that a set $S \subseteq \mathbb{R}^\infty$ is *BSS-countable* if there exists a BSS machine M such that S is the image of the set $\mathbb{N}$ under M. Uniform BSS-countability in an input is then defined in the natural way: a collection $S_{\vec{x}}$ of sets, indexed by elements $\vec{x}$ of $\mathbb{R}^\infty$, is uniformly BSS-countable in these tuples if there is a BSS machine M' such that for all indices $\vec{x}$, $S_{\vec{x}} = \{\text{outputs } M'(\vec{x}, j) : j \in \mathbb{N}\}$. It is clear that the fields $K = \mathbb{Q}(\vec{x})$ above are BSS-countable uniformly in $\vec{x}$, and so our machine can search through elements of K^m to find the requisite tuple. □

Proposition 5.11. *Let S and T be subsets of the positive integers. Suppose that for some absolute constant N and each $d \in S$, there is a positive integer $n_d \leq N$ and prime to d such that $dn_d \in T$. Then $\mathbb{A}_S \leq_{\text{BSS}} \mathbb{A}_T$.*

Proof For $n = 1, \ldots, N$, fix parameters $z_n = \sqrt[n]{2} \in \mathbb{R}$, so each $\mathbb{Q}(z_n)$ is an extension of degree n over $\mathbb{Q}$. On input x, our machine computes a primitive element a_n for each of the fields $\mathbb{Q}(x, z_n)$, using Theorem 5.10, and checks whether any of the N elements a_n lies in the oracle set $\mathbb{A}_T$. If any one does, we know x is algebraic, so we search for the minimal polynomial of x over $\mathbb{Q}$ and output "yes" or "no" depending on whether or not its degree is in S.

Suppose that no a_n lies in $\mathbb{A}_T$. In this case the machine program outputs "no." Since this clearly is the correct answer when x is transcendental, we consider x algebraic of some degree d over $\mathbb{Q}$. If $d \in S$, let $m = n_d$. By assumption, $\gcd(m, d) = 1$, so $\mathbb{Q}(x) \cap \mathbb{Q}(z_m) = \mathbb{Q}$, forcing $[\mathbb{Q}(a_m) : \mathbb{Q}] = [\mathbb{Q}(x, z_m) : \mathbb{Q}] = dm \in T$, and therefore $a_m \in \mathbb{A}_T$. □

Next we show how to remove the assumption of relative primality for a finite set S.

Proposition 5.12. *Let p and r be any positive integers. Then $\mathbb{A}_{=p} \leq_{BSS} \mathbb{A}_{=r}$ if and only if p divides r.*

Proof The "only if" direction follows from Theorem 5.3. For the "if" direction, let $q = \frac{r}{p}$. We start with parameters $z_0, \ldots, z_n$, where $n = 2^p - 2$ and z_i is the positive real q-th root of the i-th prime number: $z_0 = \sqrt[q]{2}, z_1 = \sqrt[q]{3}, \ldots$. Notice that then $\mathbb{Q}(z_i) \cap \mathbb{Q}(z_j) = \mathbb{Q}$ for all $i \neq j$.

On input x, this machine asks its $\mathbb{A}_{=r}$-oracle whether any of the elements $a_{ij} = z_i + jx$ lies in $\mathbb{A}_{=r}$, where i and j are integers satisfying $0 \leq i \leq n$ and $1 \leq j \leq q(p-1)+1$. If not, it outputs "No," while if $(z_i + x) \in \mathbb{A}_{=r}$, it finds the minimal polynomial of x over $\mathbb{Q}$ and outputs "Yes" or "No" depending on whether that polynomial has degree p.

Once again, this machine clearly outputs "No" whenever x (and hence all a_{ij}) are transcendental, and clearly outputs the correct answer whenever it actually searches for the minimal polynomial of x (because it only does so when x is algebraic). The crucial situation is that in which x is algebraic and no a_{ij} lies in $\mathbb{A}_{=r}$, so that the output "No" comes immediately. We must show that no such x can lie in $\mathbb{A}_{=p}$.

So suppose $x \in \mathbb{A}_{=p}$. Then the minimal polynomial $h(X) \in \mathbb{Q}[X]$ of x has exactly $2^p - 2$ nontrivial factors in $\overline{\mathbb{Q}}[X]$, corresponding to the proper nonempty subsets of the set of all p roots of $h(X)$ in the algebraic closure $\overline{\mathbb{Q}}$. Now h has no proper factors in $\mathbb{Q}[X]$, hence any proper factor of h in one $\mathbb{Q}(z_i)[X]$ cannot lie in any other $\mathbb{Q}(z_j)[X]$, (since $\mathbb{Q}(z_i) \cap \mathbb{Q}(z_j) = \mathbb{Q}$), leaving at least one $i \leq n$ such that $\mathbb{Q}(z_i)[X]$ contains no proper factors of h at all. We fix this i, and note that then the field $\mathbb{Q}(x, z_i)$ has degree p over $\mathbb{Q}(z_i)$ (since $h(X)$ remains irreducible in $\mathbb{Q}(z_i)[X]$), hence has degree $pq = r$ over $\mathbb{Q}$.

Now we claim that for this i, there exists at least one $j \in \omega$ with $1 \leq j \leq q(p-1)+1$ such that $a_{ij} = z_i + jx$ is a primitive generator of $\mathbb{Q}(x, z_i)$. This a_{ij} must then lie in $\mathbb{A}_{=r}$, so this will complete the proof. The necessary result follows from the proof given in [13, §6.10] of the Theorem of the Primitive Element. Specifically, it is shown there (with $\Delta = \mathbb{Q}$ being separable) that $\mathbb{Q}(x, z_i)$ has a primitive generator of the form $z_i + cx$, with $c \in \mathbb{Q}$, and indeed that there are at most $q(p-1)$ values of c in $\mathbb{Q}$ for which $z_i + cx$ *fails* to be a primitive generator. Since we tested $q(p-1)+1$ different values of j, at least one a_{ij} does generate $\mathbb{Q}(x, z_i)$, hence has degree r over $\mathbb{Q}$ as required. □

We can generalize Proposition 5.12 to finitely many degrees.

Proposition 5.13. *For any subsets S and T of ω, if $(S-T)$ is finite and for every $p \in S-T$, there exists an integer $q > 0$ such that $pq \in T$, then $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$.*

Proof Let $S - T = \{p_1, \ldots, p_k\}$, so that

$$\mathbb{A}_S \equiv_{BSS} \mathbb{A}_{S\cap T} \oplus \mathbb{A}_{=p_1} \oplus \cdots \oplus \mathbb{A}_{=p_k} = \{\langle i, x\rangle : (i = 0 \ \&\ x \in \mathbb{A}_{S\cap T}) \text{ or } (x \in \mathbb{A}_{=p_i})\}.$$

(The set on the right is clearly the least upper bound under $\leq_{BSS}$ of $\mathbb{A}_{S\cap T}$ and the sets $\mathbb{A}_{=p_i}$.) Now $\mathbb{A}_{S\cap T} \leq_{BSS} \mathbb{A}_T$ by Lemma 5.2, and by assumption, for each p_i, there is some $q_i > 0$ with $p_i q_i \in T$, so that $\mathbb{A}_{=p_i} \leq_{BSS} \mathbb{A}_{=p_i q_i} \leq_{BSS} \mathbb{A}_T$, using Proposition 5.12 and Lemma 5.2. Hence $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$. □

In the preceding construction, each element of $(S - T)$ requires its own parameters in the given BSS reduction. However, Proposition 5.11 showed that in certain cases the reduction can be done uniformly, and so $(S-T)$ need not be finite. Next we show here that the uniformity in Proposition 5.11 was essential.

Theorem 5.14. *For sets $S, T \subseteq \omega$, if $\mathbb{A}_S \leq_{BSS} \mathbb{A}_T$, then there exists $N \in \omega$ such that all $p \in S$ satisfy $\{p, 2p, 3p, \ldots, Np\} \cap T \neq \emptyset$.*

Proof We prove the contrapositive, assuming that there is no such N. Suppose an oracle BSS machine M with parameters $\vec{z}$ computes $\chi_{\mathbb{A}_S}$ from oracle $\mathbb{A}_T$. Let $Q = \mathbb{Q}(\vec{z})$ as usual, and let L be the normal closure of $Q \cap \mathbb{A}$ within $\mathbb{C}$. Thus L is a Galois extension of $\mathbb{Q}$. By assumption we may fix some $d \in S$ such that $\{d, 2d, \ldots, [L : \mathbb{Q}] \cdot d\} \cap T = \emptyset$. Running our usual argument with any $y \in \mathbb{R}$ transcendental over Q, we get an ϵ and a finite set $F \subset Q(Y)$. Now suppose $x \in \mathbb{A}_{=d}$ lies in $B_\epsilon(y)$ and has degree d over L as well as over $\mathbb{Q}$. Then for every $f \in F$, either $f(x) \notin \mathbb{A}$ (so $f(x) \notin \mathbb{A}_T$), or $L(f(x)) = L(x)$, or $L(f(x))$ is a proper subfield of $L(x)$. But now, using the same argument as in Theorem 5.3 for the choice of x, and referring to the note at the end of the proof of that theorem, we see that the case of a proper subfield may be avoided, and that when $L(f(x)) = L(x)$, the degree of $f(x)$ over $\mathbb{Q}$ equals $d \cdot [E : \mathbb{Q}]$. Recall that E was the subfield of L generated by the coefficients of the minimal polynomial of $f(x)$ over L. Therefore $[E : \mathbb{Q}] \leq [L : \mathbb{Q}]$, and so $d \cdot [E : \mathbb{Q}]$, the degree of $f(x)$ over $\mathbb{Q}$, does not lie in T, by our choice of d. Hence $f(x) \notin \mathbb{A}_T$, and the usual argument then shows that the computation $M^{\mathbb{A}_T}(x)$ proceeds along the same path as for y, hence outputs 0, even though $x \in \mathbb{A}_{=d} \subseteq \mathbb{A}_S$. □

For the converse of Theorem 5.14, one would need to uniformize the construction in Proposition 5.12, along the lines of Proposition 5.11. We leave this question for another time.

6. Countable Oracle Sets

It is natural to think of countability of a subset $S \subseteq \mathbb{R}^\infty$ as a limit on the amount of information which can be encoded into S. This intuition requires significant restating before it can be made into a coherent (let alone true) statement, but we will give a reasonable version in this section. So far, all our oracle sets have been of the form $\mathbb{A}_S$, for various $S \subseteq \omega$, and so they have all been countable. In [11], it was asked whether there could exist a countable set $C \subseteq \mathbb{R}^\infty$ such that the halting problem $\mathbb{H}$ for BSS computation on $\mathbb{R}$ satisfies $\mathbb{H} \leq_{BSS} C$. We will show that the answer to this question is negative. For a definition of $\mathbb{H}$ in this context, we refer the reader to [11]. Since it is equiconsistent with **ZFC** for the Continuum Hypothesis to be false, we will make our arguments applicable to all infinite cardinals $\kappa < 2^\omega$, countable or otherwise. Many of the results of the present and subsequent sections were first announced in [4].

First, of course, every subset of $\mathbb{R}^\infty$ is BSS-equivalent to its complement, and so countability and co-countability impose the same restriction on information content. Of course, many sets of size continuum, with equally large complements, are quite simple: the set of positive real numbers, for example, is BSS-decidable, hence less complex than the countable set $\mathbb{A}$. So it is not possible to prove absolute results relating cardinality and co-cardinality (within $\mathbb{R}^\infty$) to BSS reducibility, but nevertheless, we can produce theorems expressing the intuition that countable sets are not highly complex in the BSS model. This process will culminate in Theorem 6.4 below, but first we show that with a countable oracle, one cannot decide the BSS halting problem $\mathbb{H}$. We conjecture that $\mathbb{H}$ is not an upper bound on the degree of a countable set, i.e. that such a set can still be BSS-incomparable with $\mathbb{H}$, but it certainly constitutes progress just to know that the upper cone of sets above $\mathbb{H}$ contains no countable sets.

Theorem 6.1. *If $C \subseteq \mathbb{R}^\infty$ is a set such that $\mathbb{H} \leq_{BSS} C$, then $|C| = 2^\omega$.*

We note that by BSS-equivalence, these conditions also ensure $|\mathbb{R}^\infty - C| = 2^\omega$, and ensure $|\mathbb{R}^m - C| = 2^\omega$ whenever $C \subseteq \mathbb{R}^m$.

Proof Let $C \subseteq \mathbb{R}^\infty$ have cardinality $< 2^\omega$, and suppose that M is an oracle BSS machine such that M^C computes the characteristic function of $\mathbb{H}$. We fix a program code number p for the program which takes inputs $\langle x_1, x_2\rangle \in \mathbb{R}^2$, searches through nonzero polynomials q in $\mathbb{Q}[Y_1, Y_2]$, and halts iff it finds one with $q(x_1, x_2) = 0$. Since the program coded by p uses no real parameters, p may be regarded as a natural number, but in our argument it can equally well be a tuple $\vec{p}$ from $\mathbb{R}^\infty$, with one or several real numbers coding program parameters. Then the elements of C, the finitely many parameters $\vec{z}$ of M, and the parameters, if any, in the program coded by $\vec{p}$ together generate a field $E \subseteq \mathbb{R}$ which also has cardinality $< 2^\omega$, and so $\mathbb{R}$ is an extension of infinite transcendence degree (indeed of degree 2^ω) over this E. (Since $C \subseteq \mathbb{R}^\infty$, we need to be precise: E is generated by the coordinates $p_1, \ldots, p_j$ and $z_1, \ldots, z_k$ of the tuples $\vec{p}$ and $\vec{z}$, and the coordinates of each tuple in C.)

Now fix a pair $\langle y_1, y_2\rangle$ of real numbers algebraically independent over E. Hence $\langle \vec{p}, y_1, y_2\rangle \notin \mathbb{H}$, so M^C on this input halts after finitely many steps and outputs 0. We fix the finitely many functions $f_{i,s}(\vec{Y}) \in E(Y_1, Y_2)$ such that $f_{i,s}(y_1, y_2)$ appears in the i-th cell at stage s during this computation. (The program code $\vec{p} \in E^\infty$ will stay fixed throughout this proof, so we may treat it as part of the function $f_{i,s}$, rather than as a variable.) As usual, F will be the set of those functions $f_{i,s}$ which are not constants in E, and we fix an $\epsilon > 0$ such that whenever $\langle x_1, x_2\rangle \in \mathbb{R}^2$ with $x_1 \in B_\epsilon(y_1)$ and $x_2 \in B_\epsilon(y_2)$, every $f \in F$ satisfies $f(x_1, x_2) \cdot f(y_1, y_2) > 0$. Write each $f \in F$ as a quotient $f = \frac{g}{h}$ with $g, h \in E[Y_1, Y_2]$, and let n be the greatest degree of Y_2 in all of these finitely many polynomials g and h.

Now choose $x_1 \in \mathbb{R}$ to be transcendental over E and within ϵ of y_1, and pick x_2 within ϵ of y_2 such that x_2 is algebraic over $\mathbb{Q}(x_1)$ but has degree $> n$ over $E(x_1)$. For instance, let $x_1 = y_1$ and $x_2 = \sqrt[m]{x_1} + b$, where $m > n$ is prime and $b \in \mathbb{Q}$ is selected to place $x_2 \in B_\epsilon(y_2)$. The subfield $E(x_1)$ of $\mathbb{R}$ contains no nontrivial m-th roots of unity, nor any m-th roots of x_1 (by our choices), so the Galois group of the splitting field of $(Y^m - x_1)$ over $E(x_1)$ is just the Galois group of its splitting field over $\mathbb{Q}(x_1)$, which acts transitively on the roots. Thus this polynomial is irreducible over $E(x_1)$, and so x_2 has degree m over $E(x_1)$.

Thus, for any $f \in F$, if $a = f(x_1, x_2) \in E$, then $0 = g(x_1, x_2) - ah(x_1, x_2)$. Since f is nonconstant, g is not a scalar multiple of h, and so $(g - ah)$ would then be a nonzero polynomial in $E[Y_1, Y_2]$ of degree $\leq n$, contradicting our choice of x_2. Hence $f(x_1, x_2) \notin E$ for every $f \in F$. But then the oracle computation $M^C(\vec{p}, x_1, x_2)$ must follow the same path as $M^C(\vec{p}, y_1, y_2)$ and give the same output, namely 0. Since $\langle \vec{p}, x_1, x_2\rangle \in \mathbb{H}$, this proves that M^C does not compute the characteristic function of $\mathbb{H}$. □

Indeed the preceding proof shows slightly more than was stated.

Corollary 6.2. *If $C \subseteq \mathbb{R}^\infty$ is a set such that $\mathbb{H} \leq_{BSS} C$, then $\mathbb{R}$ has finite transcendence degree over the field K generated by (the coordinates of the tuples in) C, and also has finite transcendence degree over the field generated by the complement of C.*

Proof Given an oracle BSS machine M which computes $\mathbb{H}$ from oracle C, let E be the extension field $K(\vec{z}, \vec{p})$, with K as defined in the corollary. If $\mathbb{R}$ had transcendence degree ≥ 2 over this E, then the proof of Theorem 6.1 would go through: we could choose $y_1, y_2 \in \mathbb{R}$ algebraically independent over E, say with $y_1 > 0$, and then let $x_1 = y_1$ and $x_2 = b + \sqrt[m]{x_1}$, with $m > n$ prime, as in the proof, and with $b \in \mathbb{Q}$ selected to put $x_2 \in B_\epsilon(y_2)$. But this

would show that M^C does not compute $\mathbb{H}$. So $\mathbb{R}$ has transcendence degree ≤ 1 over this E, and therefore is algebraic over $E(t) = K(t, \vec{z}, \vec{p})$ for some $t \in \mathbb{R}$.

Since C is BSS-equivalent to its complement, the same proof applies to $(\mathbb{R}^\infty - C)$, and also to $(\mathbb{R}^m - C)$ if $C \subseteq \mathbb{R}^m$. □

As we consider the general case of a BSS computation of the characteristic function χ_S of a set $S \subseteq \mathbb{R}$ using an oracle C of infinite cardinality $\kappa < 2^\omega$, the following definition will be useful.

Definition 6.3. 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 $|U \cap S| \leq \kappa$ and $|V \cap S^C| \leq \kappa$.

If $\kappa < 2^\omega$, then such U and V must be disjoint, since $(U \cap V)$ is open with $|U \cap V| \leq |U \cap S| + |V \cap \overline{S}| \leq \kappa$. So the definition roughly says that up to sets of size κ, each of S and $\overline{S}$ is equal to an open subset of $\mathbb{R}$. It is not equivalent to weaken the requirement $|\mathbb{R} - (U \cup V)| \leq \kappa$ in Definition 6.3, for instance by requiring that $|U \cap V| < 2^\omega$. For a counterexample, let $V = \emptyset$ and let U be the complement S^C of the Cantor middle-thirds set S, which contains all real numbers x whose non-integer part $x - \lfloor x \rfloor$ has a ternary expansion in only 0's and 2's. Thus $U \cap S = V \cap \S^C = U \cap V = \emptyset$, yet this S is not locally of bicardinality $\leq \omega$ (nor $\leq$ any other $\kappa < 2^\omega$), as shown in full in Lemma 7.3 below.

The *local bicardinality of* S is the least cardinal κ such that S is locally of bicardinality $\leq \kappa$.

The property of having local bicardinality $\leq \kappa$ does not appear to us to be equivalent to any more easily stated property, and we are not aware of it having been used (or even stated) elsewhere in the literature. The same definition in higher dimensions completely loses its power: any connected component U_0 of U must have boundary ∂U_0 with $U_0 \cap \partial U = V \cap \partial U_0 = \emptyset$, since U and V are open and disjoint. But then $|\partial U_0| \leq |\mathbb{R}^n - (U \cup V)| \leq \kappa$, which is feasible in $\mathbb{R}^1$ but not in higher dimensions, unless U or V were empty or $\kappa = 2^\omega$. Thus, in $\mathbb{R}^n$ with $n > 1$, every set of local bicardinality $< 2^\omega$ has either cardinality $< 2^\omega$ or co-cardinality $< 2^\omega$. Nevertheless, within $\mathbb{R}^1$, this is exactly the condition needed in our general theorem on cardinalities.

Theorem 6.4. *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 $\kappa < 2^\omega$.*

Proof Again let $\vec{z}$ be the parameters used by the oracle BSS machine M which, given oracle C, computes χ_S. Then for any input $y \in \mathbb{R}$ transcendental over the subfield E of cardinality κ generated by $\vec{z}$ and the individual coordinates of all elements of C, there will again exist a finite set $F_y \subseteq E(X)$ as above, and an $\epsilon > 0$ such that $f(x) \cdot f(y) > 0$ for all $x \in B_\epsilon(y)$ and $f \in F_y$. For each such y, let $B(y)$ be an open interval of length less than the corresponding ϵ, such that $B(y)$ contains y and has rational end points. Now if $x \in B(y)$ is also transcendental over E, then the computation of $\chi_S(x)$ using this machine and the C-oracle proceeds along the same path as the computation for y, since $f(x) \notin E$ for all $f \in F_y$. (Indeed, this would hold whenever $x \in B(y)$ has degree $> n$ over E, where n is the maximum degree of all numerators and denominators of elements of F_y.) This shows that $\chi_S(x) = \chi_S(y)$ for all such x. Since only κ-many elements of $B(y)$ can be algebraic over the size-κ field E, it follows that either $S \cap B(y)$ or $S^C \cap B(y)$ has size $\leq \kappa$.

Now if $t \in B(y_0) \cap B(y_1)$ is transcendental over E, then t follows the same computation path as both y_0 and y_1, implying that $\chi_S(y_0) = \chi_S(y_1)$ whenever $B(y_0) \cap B(y_1) \neq \emptyset$, and

therefore that either $B(y_0) \cap S$ and $B(y_1) \cap S$ both have size $\leq \kappa$, or else $B(y_0) \cap \S^C$ and $B(y_1) \cap \S^C$ both have size $\leq \kappa$. So when we set

$$U = \bigcup\{B(y) : |S \cap B(y)| \leq \kappa\} \text{ and } V = \bigcup\{B(y) : B(y) \not\subseteq U\},$$

we will have $U \cap V = \emptyset$. Here the unions are over those $y \in \mathbb{R}$ transcendental over E (as $B(y)$ is not defined for any other y), and so the complement $\mathbb{R} - (U \cup V)$ is a subset of the algebraic closure of E, which has size κ. Moreover, being a union of open intervals $B(y)$ with rational end points, U in fact equals the union of countably many such intervals, say $U = \cup_{i\in\omega} B(y_i)$ for some sequence $y_0, y_1, \ldots$. Since each $B(y_i)$ has intersection of size $\leq \kappa$ with S (and since $\kappa \geq \omega$), so does the entire union U. Likewise $|\S^C \cap V| \leq \kappa$, proving the theorem.

The claim about oracles of co-cardinality κ follows from applying the same argument to the oracle $(\mathbb{R}^\infty - C)$, which is BSS-equivalent to C. If $C \subseteq \mathbb{R}^m$ for some m, then the same holds of $(\mathbb{R}^m - C)$. □

Notice that the set S of smaller complexity must be a subset of $\mathbb{R}$, whereas C is allowed to contain tuples from $\mathbb{R}^\infty$. We conjecture that to extend the theorem to sets $S \subseteq \mathbb{R}^\infty$, we would need to allow $\mathbb{R}^\infty - (U \cup V)$ to be a size-κ union of proper algebraic varieties defined over the field generated by C. It is an open question (of interest only under $\neg$**CH**) whether it is equivalent, for the purposes of this conjecture and Theorem 6.4, to replace $|\mathbb{R}^\infty - (U \cup V)| \leq \kappa$ by $|\mathbb{R}^\infty - (U \cup V)| \leq \omega$ here or in Definition 6.3.

To understand that this theorem cannot readily be stated using a simpler property than Definition 6.3, consider the BSS-computable set

$$S = \{x \in (0,1) : (\exists m \in \omega)\ 2^{-(2m+1)} \leq x - \lfloor x \rfloor \leq 2^{-(2m)}\},$$

containing those $x \in (0,1)$ which have a binary expansion with an even number of zeroes following the decimal point, along with all translations of this set by integers. The closure of S is just $S \cup \mathbb{Z}$, but any open set containing any integer z would intersect each of S and $\S^C$ in 2^ω-many points. So the theorem cannot require the complement $\mathbb{R}^\infty - (U \cup V)$ to be finite, let alone empty. With such tricks one can create examples defying most conceivable simplifications of Theorem 6.4.

In the next section we discuss the Cantor set, which is often another useful counterexample in this vein.

7. The Cantor Set

As an example of a set of local bicardinality 2^ω, we consider the Cantor set $\mathfrak{C}$, well known as a set of measure 0 within $\mathbb{R}$ which nevertheless has cardinality 2^ω. By definition, $\mathfrak{C}$ contains all real numbers $x \in [0,1]$ having ternary expansions in only 0's and 2's. One usually views $\mathfrak{C}$ as the set of numbers in the unit interval $[0,1]$ which remain after ω-many iterations of deleting the open "middle third" of each interval (starting with the middle third $(\frac{1}{3}, \frac{2}{3})$ of $[0,1]$). It is clear from this description that $\mathfrak{C}$ is co-semidecidable in the BSS model: even a Turing machine could enumerate the end points of all those middle-third intervals to be deleted. Hence fC is 1-reducible to the complement $\mathbb{H}^C$, forcing $\mathfrak{C} \leq_{BSS} \mathbb{H}$. The natural next question, whether $\mathbb{H} \leq_{BSS} \mathfrak{C}$, was settled by Yonezawa in [15], and we thank the anonymous referee of [4] who pointed out the necessary result there.

Theorem 7.1 (Corollary 2.5 in [15])**.** *The sets $\mathbb{Q}$ and $\mathfrak{C}$ are BSS-incomparable.* □

Since the BSS-semidecidable set $\mathbb{Q}$ must be $\leq_{BSS} \mathbb{H}$, this immediately answers the question: $\mathbb{H} \leq_{BSS} \mathfrak{C}$ would imply $\mathbb{Q} \leq_{BSS} \mathfrak{C}$, contradicting Theorem 7.1.

Corollary 7.2. $\mathbb{H} \not\leq_{BSS} \mathfrak{C}$. □

Now we consider the local bicardinality of $\mathfrak{C}$. The next lemma, combined with Theorem 6.4, immediately proves that $\mathfrak{C}$ is not BSS-decidable, nor even BSS-semidecidable, in any oracle of size $< 2^\omega$.

Lemma 7.3. The Cantor set $\mathfrak{C}$ has local bicardinality 2^ω.

Proof Suppose $\mathfrak{C}$ were locally of bicardinality $\leq \kappa < 2^\omega$. Then we would have open disjoint sets U and V satisfying Definition 6.3, and $\mathfrak{C}$, having size 2^ω, would have to intersect V in some point x, since

$$\mathfrak{C} - V \subseteq (U \cap \mathfrak{C}) \cup (U \cup V)^C$$

and the right-hand side has size $\leq \kappa$. The open set V would then contain an ϵ-ball around x. However, every open interval around x intersects each of $\mathfrak{C}$ and $\mathfrak{C}^C$ in 2^ω-many points. (To see this, just consider all y whose ternary expansions match that of x for sufficiently many places to lie within that interval.) Therefore $|V \cap \mathfrak{C}^C| = 2^\omega$, yielding a contradiction. □

Corollary 7.4. *The Cantor set $\mathfrak{C}$ is not BSS-semidecidable below $\mathbb{A}$, or below any other oracle of cardinality $< 2^\omega$.*

Proof This simply means that no function which is BSS-computable in the oracle $\mathbb{A}$ can have $\mathfrak{C}$ as its domain. Indeed, if it did, then $\mathfrak{C} \leq_{BSS} \mathbb{A}$, since $\mathfrak{C}$ and $\mathfrak{C}^C$ would both be $\mathbb{A}$-semidecidable. By Lemma 7.3, we know that $\mathfrak{C}$ has local bicardinality 2^ω, so that by Theorem 6.4 we have $|\mathbb{A}| \geq 2^\omega$, contrary to the assumption. The same holds for any other oracle of size $< 2^\omega$. □

Corollary 6.2, our natural hope for reproving Yonezawa's result that $\mathbb{H} \not\leq_{BSS} \mathfrak{C}$ by the methods of this paper, fails to do so, for the field generated by $\mathfrak{C}$ does not satisfy the hypothesis there. It seems counterintuitive that a set of measure 0 could generate such a large field, so we prove it here. (The authors assume that this fact has been proven long since, and would appreciate a reference for it.)

Lemma 7.5 (Folklore)**.** The Cantor set $\mathfrak{C}$ generates the entire field $\mathbb{R}$. Indeed, it generates $\mathbb{R}$ as a ring.

Proof The argument is best understood by seeing an example. Here we begin with an element of $[0, 1]$, chosen arbitrarily, in ternary form:

$$\begin{aligned} & 0.2201020001211\ldots \\ = {} & 0.2200020000200\ldots \\ & +0.0001000001011\ldots \\ = {} & 0.2200020000200\ldots \\ & +(0.0002000002022\ldots) \cdot \frac{1}{2} \end{aligned}$$

Since $\frac{1}{2}$ lies in every subfield of $\mathbb{R}$, this shows that this number is generated from $\mathfrak{C}$ by field operations. Indeed, since $\frac{1}{2} = 2 \cdot \frac{1}{4} = 2 \cdot (0.020202\ldots)$, the number is generated from elements of $\mathfrak{C}$ by ring operations. The same process can be applied to any element of $[0, 1]$, so $\mathfrak{C}$ generates the entire unit interval, and hence all of $\mathbb{R}$. (In particular, let $x \in [0, 1]$, and

write x as $x_1 + x_2$, where each non-zero ternary digit of x_i is equal to i. Now $x_1' = 2x_1$ is in $\mathfrak{C}$, and $\frac{1}{4}$ is in $\mathfrak{C}$. Thus, $x = x_2 + (\frac{1}{4} + \frac{1}{4})x_1'$ is in the subring generated by $\mathfrak{C}$.) □

8. A Nicer Situation: the Complex Numbers

BSS computation has also been widely considered on the field $\mathbb{C}$ of complex numbers. The principal differences are the algebraic closure of $\mathbb{C}$ and the consequent impossibility of any order on $\mathbb{C}$ compatible with the field operations. Of these, the second is probably the more significant difference. With no order available, BSS machines on $\mathbb{C}$ can only make comparisons of cell contents under $=$ (and can compute the four field operations, of course). To help show the importance of this difference, we demonstrate here how much easier the questions of Section 6 become when considered on $\mathbb{C}$. The following is the analogue in $\mathbb{C}$ of Theorem 6.4.

Theorem 8.1. *If $C \subseteq \mathbb{C}^\infty$ is an oracle set of infinite cardinality $\kappa < 2^\omega$, and $S \subseteq \mathbb{R}$ is a set with $S \leq_{BSS} C$, then either S or its complement must have cardinality $\leq \kappa$. The same holds for oracles C of infinite co-cardinality $\kappa < 2^\omega$.*

Proof If the machine M with parameters $\vec{z}$ computes χ_S from oracle C, consider any two inputs $x, y \in \mathbb{C}$ which are both transcendental over the field F generated by $\vec{z}$ and all components of tuples in C. One immediately sees that the computations of M^C on each of these inputs follow the same path, with the cell contents at each stage given by rational functions f with coefficients in $\mathbb{Q}(\vec{z})$. With x transcendental over F, the only way for $f(x)$ to lie in F is for f to be constant, in which case $f(y)$ is the same constant. Thus the oracle questions in the two computations always yield the same answers, and so $\chi_S(x) = M^C(x) = M^C(y) = \chi_S(y)$, since the possible output values for M^C are just 0 and 1, which are both in the field F. So S contains either all such transcendentals, or else none of them. Since there are only κ-many elements of $\mathbb{C}$ algebraic over the size-κ field F, the theorem follows. □

So, without the order $<$ requiring inputs to be chosen within ϵ of other inputs, the result involves no local bicardinality whatsoever. We consider this theorem on $\mathbb{C}$ to be the best starting point for a generalization to sets $S \subseteq \mathbb{C}^\infty$ BSS-decidable below oracles of cardinalities $< 2^\omega$. As stated above, the theorem is false for such S; indeed, in $\mathbb{C}^2$, the zero set of any finite collection of polynomials in $\mathbb{C}[X, Y]$ is decidable, and even when the collection contains just a single nontrivial polynomial, this set has both cardinality and co-cardinality 2^ω. The correct analogy should be that points in $\mathbb{C}$ should be considered as varieties there (after all, the singletons are exactly the irreducible affine varieties in $\mathbb{C}^1$), and that the generalization of Theorem 8.1 to $\mathbb{C}^n$ should not concern the cardinality of S, but rather the least possible cardinality of a set of irreducible varieties such that S is a Boolean combination of those varieties.

References

[1] L. Blum, F. Cucker, M. Shub, and S. Smale; *Complexity and real computation* (Berlin: Springer-Verlag, 1998).

[2] L. Blum, M. Shub, and S. Smale; On a theory of computation and complexity over the real numbers, *Bulletin of the American Mathematical Society (New Series)* **21** (1989), 1–46.

[3] W. Calvert, K. Kramer, & R. Miller; Noncomputable functions in the Blum-Shub-Smale model, in the abstract booklet for the conference *Logical Approaches to Barriers in Computing and Complexity* (17-20 February 2010, Greifswald, Germany). Available at `qcpages.qc.cuny.edu/~rmiller/BSSabstract.pdf`.

[4] W. Calvert, K. Kramer, & R. Miller; The Cardinality of an Oracle in Blum-Shub-Smale Computation, Computability and Complexity in Analysis (CCA 2010) *Electronic Proceedings in Theoretical Computer Science* **24** (2010), 56–66.

[5] M.D. Fried & M. Jarden; *Field Arithmetic* (Berlin: Springer-Verlag, 1986).

[6] C. Gassner; A hierarchy below the halting problem for additive machines, *Theory of Computing Systems* **43** (2008) 3–4, 464–470.

[7] W. Koolen & M. Ziegler; Kolmogorov complexity theory over the reals, in *Proceedings of the Fifth International Conference on Computability and Complexity in Analysis, CCA '08*, *Electronic Notes in Theoretical Computer Science* **221** (Elsevier, 2008), 153-169.

[8] L. Kronecker; Grundzüge einer arithmetischen Theorie der algebraischen Größen, *J. f. Math.* **92** (1882), 1-122.

[9] S. Lang; *Algebra*, third edition (Addison-Wesley Publishing Co., Inc., 1993).

[10] S. Lang; *Algebraic Number Theory*, second edition (Springer, 2000).

[11] K. Meer and M. Ziegler; An explicit solution to Post's Problem over the reals, *Journal of Complexity* **24** (2008) 3–15.

[12] M. Nagata; *Theory of Commutative Fields*, English trans. (American Mathematical Society, 1993).

[13] B.L. van der Waerden; *Algebra*, volume I, trans. F. Blum & J.R. Schulenberger (New York: Springer-Verlag, 1970 hardcover, 2003 softcover).

[14] H. Wozniakowski; Why does information-based complexity Use the real number model? *Theoretical Computer Science* **219** 1-2 (1999), 451–465.

[15] Y. Yonezawa; The Turing degrees for some computation model with the real parameter, *J. Math. Soc. Japan* **60** 2 (2008), 311–324.