PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 118, Number 2, June 1993

ORDERED SUBRINGS OF THE REALS IN WHICH OUTPUT SETS ARE RECURSIVELY ENUMERABLE

ROBERT E. BYERLY

(Communicated by Andreas R. Blass)

ABSTRACT. In *On a theory of computation and complexity over the real numbers ...*, Bull. Amer. Math. Soc. **21** (1989), 1–46, Blum, Shub, and Smale investigated computability over the reals and over ordered rings in general. They showed that over the reals, output sets of machines are recursively enumerable (i.e., halting sets of machines). It is asked in the aforementioned paper which ordered rings have this property (which we abbreviate $O = R.E.$). In *Ordered rings over which output sets are recursively enumerable*, Proc. Amer. Math. Soc. **112** (1991), 569–575, Michaux characterized the members of a certain class of ordered rings of infinite transcendence degree over $\mathbb{Q}$ satisfying $O = R.E.$ In this paper we characterize the subrings of $\mathbb{R}$ of finite transcendence degree over $\mathbb{Q}$ satisfying $O = R.E.$ as those rings recursive in the Dedekind cuts of members of a transcendence base. With Michaux's result, this answers the question for subrings of $\mathbb{R}$ (i.e., archimedean rings).

1. INTRODUCTION

In [BSS] Blum, Shub, and Smale investigated computability over commutative ordered rings and extended some classical results of ordinary recursive function theory over the natural numbers ω to this more general setting. A particularly useful result in classical recursive function theory is that the ranges of partial recursive functions in ω (output sets of ω-machines) coincide with the recursively enumerable sets (i.e., halting sets of machines over ω). Blum, Shub, and Smale showed that this result holds for the reals (and real closed fields in general) as well.

In any structure, the halting set of a machine M is also the output set of some machine, since one can modify M to output its inputs after the computation terminates. For an arbitrary structure, an output set need not be a halting set. In ω, output sets are also halting sets because for any machine M over ω, one can effectively generate all potential inputs and the corresponding outputs (cf. [Mi,§3]). This approach does not work for the reals, which are uncountable. Blum, Shub, and Smale used Tarski's theorem that the theory of real closed fields admits effective elimination of quantifiers (see [vdD]) to prove that every real closed field satisfies $O = R.E.$ Michaux showed that a ordered ring of infinite transcendence degree over the rationals whose field of fractions is dense

Received by the editors September 30, 1991.
1991 *Mathematics Subject Classification.* Primary 03D75.

in its real closure satisfies $O = R.E.$ if and only if it is a real closed field. As we shall see, the situation is quite different for rings of finite transcendence degree over $\mathbb{Q}$. (See also [Man].) For example, the ring of rationals $\mathbb{Q}$ and the constructible reals, neither of which form a real closed field, satisfy $O = R.E.$

Our main result is

Theorem 1. *Let R be an ordered subring of the reals having finite transcendence degree over $\mathbb{Q}$. R satisfies the property $O = R.E.$ if and only if R is a recursive ring relative to the Dedekind cuts of members of a transcendence base for R over $\mathbb{Q}$.*

An immediate corollary is

Corollary 1. *Let R be an ordered subring of the algebraic reals. R satisfies the property $O = R.E.$ if and only if R is a recursive ring.*

Actually, we shall prove only the corollary. The proof of Theorem 1 is a straightforward relativization of the proof we shall give of the corollary.

2. Preliminaries

In this paper, all rings will be assumed to be commutative, associative, and with a unit.

We shall denote the ordered ring of algebraic reals by $\mathbb{A}$. Note that $\mathbb{A}$ is a real closed field.

A useful tool will be Tarski's theorem on effective elimination of quantifiers for real closed fields. The language of ordered rings contains binary operators $+$, $-$, and $\cdot$, a relation $<$, and constants 0 and 1. Let RCF denote the theory of real closed fields formalized in the language of ordered rings. Tarski's theorem states that for every formula $A(\mathbf{x})$ of the language of ordered rings, there is a quantifier free formula $B(\mathbf{x})$ provably equivalent in RCF to $A(\mathbf{x})$. Furthermore, there is an algorithm for constructing such a $B(\mathbf{x})$ from $A(\mathbf{x})$. This will be useful because in any ordered ring R, if $B(\mathbf{x})$ is a quantifier free formula and $\mathbf{a}$ are members of R, an R-machine can effectively decide whether or not $B(\mathbf{a})$.

Since we will be discussing computability over various structures, we will often use the name of a structure as a prefix to such words as "recursive" in order to avoid ambiguity. In particular, when we mean that a set is recursive in the classical sense (over the nonnegative integers ω), we will use the expression "ω-recursive".

See [BSS] for a formal definition of a machine over an ordered ring R. Our descriptions of machines will be informal. Any machines capable of executing programs in a programming language with the features to be described will suffice. The programming language should contain variables ranging over the ring R, among which are designated input and output variables. The program can use any of a finite list of parameters from R. Expressions should use only the basic operations ($+$, $-$, and $\cdot$) of R. There should be test-and-branch instructions that should use only the $<$ relation from R. (Note, however, that $a = b$ if and only if $a \not< b$ and $b \not< a$, so equality can effectively be determined.)

Note that if R is an archimedean ring, an R-machine can effectively test for membership in $\mathbb{Z}$. (Given input r, set $x = |r|$. Repeatedly decrement x by

1 until $x < 0$. If $x = -1$ output TRUE; else output FALSE.) Consequently, in an archimedean ring R, partial $\mathbb{Z}$-recursive, and hence, partial ω-recursive, functions are partial R-recursive. The machines in the rings we are considering can therefore evaluate in an auxiliary computation the value of any ordinary recursive function.

Definition 1. We say that an ordered ring R is *recursive* if it is isomorphic to some $\langle D, +_D, -_D, \cdot_D, 0_D, 1_D, <_D\rangle$, where D is a ω-recursive subset of ω, $+_D$, $-_D$, and $\cdot_D$ are ω-recursive functions on D, and $<_D$ is an ω-recursive relation on D.

If $A_1, \ldots, A_n$ are subsets of ω, we can obtain the definition of a ring recursive relative to $A_1, \ldots, A_n$ by relativizing this definition. Theorem 1 speaks of rings recursive relative to the Dedekind cuts of a finite transcendence base. Since Dedekind cuts are sets of rationals, and rationals can be easily be coded (using a computable pairing mechanism) as integers, we can uniformly replace the Dedekind cuts by subsets of ω.

A particularly important example of a recursive ordered ring is $\mathbb{A}$. See [Ma] for a proof. We observe that this result easily relativizes: If F is the real closure of $\mathbb{Q}(c_1, \ldots, c_n)$, where $c_1, \ldots, c_n$ are algebraically independent reals, then F is recursive relative to Dedekind cuts of $c_1, \ldots, c_n$.

Definition 2. We fix a $\mathbb{B} = \langle B, +_B, \ldots\rangle$ witnessing that $\mathbb{A}$ is a recursive ordered ring, and an isomorphism $C : \mathbb{A} \to \mathbb{B}$. If r is an algebraic real, we call $C(r)$ the *canonical code* of r.

3. Proof of Corollary 1

We shall first show the harder direction of Corollary 1. Suppose R is an ordered subring of $\mathbb{A}$ satisfying $O = R.E.$ We shall prove that R is a recursive ring.

Lemma 1. *Let R be an ordered subring of $\mathbb{A}$. Then $\hat{C} = C \restriction R$, the map that takes an element of R to its canonical code, is R-recursive.*

Proof. Suppose $f(x) \in \mathbb{Z}[x]$. If r is a real root of $f(x)$, it is the only real root in some interval with rational end points. The assertion $r > i/j$ can be expressed as a quantifier-free formula by

$$(j > 0 \implies r \cdot j > i) \wedge (j < 0 \implies r \cdot j < i) \wedge (j \neq 0).$$

Hence, the assertion "r is in the interval $(i/j, k/l)$" can be expressed by a quantifier-free formula. Let $\Phi_f(r, i, j, k, l)$ be the formula

$$r \in (i/j, k/l) \wedge f(r) = 0 \wedge \forall x(f(x) = 0 \wedge x \in (i/j, k/l) \implies x = r),$$

which asserts that r is the only root of $f(x)$ in $(i/j, k/l)$. By Tarski's effective elimination of quantifiers, we can effectively compute from Φ_f a quantifier-free formula Φ'_f such that $\Phi_f(r, i, j, k, l) \iff \Phi'_f(r, i, j, k, l)$ is provable in the theory of real closed fields. Quantifier-free formulas are absolute. In particular, if R is a subring of $\mathbb{A}$ and $r, i, j, k, l \in R$, then $\Phi'_f(r, i, j, k, l)$ is true in R if and only if it is true in $\mathbb{A}$ if and only if r truly is the only real root of $f(x)$ in the interval $(i/j, k/l)$.

Given $r \in R$, we informally describe an R-machine M for computing $C(r)$. M searches through $\mathbb{Z}[x]$ until it finds an $f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0$, such that $f(r) = 0$. M effectively enumerates all quadruples $i, j, k, l \in \mathbb{Z}$, stopping when it finds that $\Phi'_f(r, i, j, k, l)$ is true in R. (Since Φ'_f is quantifier free, M can determine when this happens. Note that by the preceding paragraph, r will be the only real root of $f(x)$ in $(i/j, k/l)$. The search will terminate at some finite stage.) Finally, M searches through B until it finds a b such that $\Phi'_f(b, C(i), C(j), C(k), C(l))$ is true in $\mathbb{B}$ and outputs b. ($C \restriction \mathbb{Z}$ is R-recursive, since $C(i)$ can be calculated by adding 1_B (or subtracting if $i < 0$) to 0_B $|i|$ times. Thus, M can R-effectively compute $C(i), C(j), C(k), C(l)$. Since $C(r)$ is the unique $b \in B$ such that $\Phi'(b, C(i), C(j), C(k), C(l))$ is true in $\mathbb{B}$, the computation will terminate with $C(r)$ as the output.) □

In the definition of recursive ring, if we relax the requirement that D be recursive by allowing D to be recursively enumerable, but requiring that $+_D$, $-_D$, and $\cdot_D$ (respectively, $<_D$) be restrictions of recursive functions (respectively, predicates) to D, we obtain the definition of a *recursively enumerable* ring.

Lemma 2. *Let R be an ordered ring. R is recursively enumerable if and only if it is recursive.*

Proof. Suppose R is recursively enumerable. (The other direction is trivial.) Let $\langle D, +_D, \ldots \rangle$ witness that R is recursively enumerable. Let $d_1, d_2, \ldots$ be an effective enumeration of D. Then the structure $\langle D', +_{D'}, \ldots \rangle$ witnesses that R is recursive, where $D' = \{1, 2, \ldots\}$, $i +_{D'} j = k$ if and only if $d_i +_D d_j = d_k$, etc. □

Lemma 3. *Let R be an ordered subring of $\mathbb{A}$ satisfying $O = R.E$. Then R is a recursively enumerable (hence recursive) ring.*

Proof. Since $\widehat{C} = C \restriction R$ is R-recursive, its range is, by hypothesis, R-recursively enumerable. We first show that it is, in fact, $\mathbb{A}$-recursively enumerable.

Let M be a machine over R the halting set of which is the range of $\widehat{C}$. Obtain a machine M' by modifying M as follows: when the computation begins, M' first tests its input to see if it is in ω. If it is not, M' goes into an infinite loop. Otherwise, M' proceeds to emulate M on the input. It is clear that M' and M have the same halting set over R. But, it is also easy to see that M' has the same halting set over R as it does regarded as a machine over $\mathbb{A}$. Hence the range of $\widehat{C}$ is $\mathbb{A}$-recursively enumerable. (The only reason to use M' instead of M is to avoid the possibility that M might halt on an algebraic real not in R. By taking an M' that is guaranteed not to halt on anything not in R, this possibility is avoided.)

Finally, we observe that the range of $\widehat{C}$ is ω-recursively enumerable. Actually, we show that if S is *any* $\mathbb{A}$-recursively enumerable subset of ω, S is ω-recursively enumerable. Let M be an $\mathbb{A}$-machine whose halting set is S. Change M into a $\mathbb{B}$-machine M' by replacing the machine parameters $c_1, \ldots, c_n$ by $C(c_1), \ldots, C(c_n)$ and $+, -, \cdot, <$ by $+_B, -_B, \cdot_B$, and $<_B$, respectively. M' can be emulated by an ω-machine since $+_B$, etc., are ω-recursive functions. Construct a machine M_S over ω that does the following.

Given $n \in \omega$, M_S computes $C(n)$. (This can be done by iterating $+_B$ on 1 as in the proof of Lemma 1.) Then M_S emulates M' on input $C(n)$. □

This completes the proof of the harder half of Corollary 1. We now prove the other half by showing that a recursive subring of $\mathbb{A}$ satisfies $O = R.E.$

If R is a recursive ordered subring of $\mathbb{A}$, let $\pi : R \to \langle D, +_D, \ldots \rangle$, where $D \subseteq \omega$, witness that R is recursive. Note that the method of proof of Lemma 1 can be used to show that π is R-recursive. Suppose B is an output set of an R-machine. Then $\pi(B)$ is an output set of an ω-machine, and therefore, since ω satisfies $O = R.E.$, is the halting set of an ω-machine M. We construct an R-machine M' whose halting set is B as follows. Given $b \in R$, M' computes $\pi(b)$ and sees if the ω-machine M halts on $\pi(b)$.

4. Concluding remarks

It would be nice to have a purely "algebraic" characterization of those subrings of the reals of finite transcendence degree satisfying $O = R.E.$ In view of the fact that this would amount to an algebraic characterization of the recursive subrings, it seems unlikely there is a decent such characterization.

If we turn our attention to computability over arbitrary unordered subfields of the complex numbers (we need to add division as a primitive operation and equality as a basic test), the situation is much more complicated. The constructible reals are an example of an (unordered) recursive field of finite transcendence degree over $\mathbb{Q}$ not satisfying $O = R.E.$ Every recursive normal extension of $\mathbb{Q}$ (or of a finitely generated extension of $\mathbb{Q}$) satisfies $O = R.E.$, but there are recursive nonnormal extensions that do so as well. However, any subfield of $\mathbb{C}$ of finite transcendence degree over $\mathbb{Q}$ that satisfies $O = R.E.$ is recursive (see [B]). This area would seem to be worth studying in order to gain insight into computability over more general classes of structures.

References

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

[B] R. Byerly, *Computability over subfields of* $\mathbb{C}$, in preparation.

[F] H. Friedman, *Algorithmic procedures, generalized Turing algorithms, and elementary recursion theory*, Logic Colloquium 1969 (R. O. Gandy and C. M. E. Yates, eds.), North-Holland, Amsterdam, 1971, pp. 361–390.

[Ma] E. W. Madison, *A note on computable real fields*, J. Symbolic Logic **35** (1970), 239–241.

[Man] R. Mansfield, *The irrationals are not recursively enumerable*, Proc. Amer. Math. Soc. **110** (1990), 495–498.

[Mi] C. Michaux, *Ordered rings over which output sets are recursively enumerable*, Proc. Amer. Math. Soc. **112** (1991), 569–575.

[vdD] L. van den Dries, *Alfred Tarski's elimination theory for real closed fields*, J. Symbolic Logic **53** (1988), 7–19.

Department of Mathematics, Texas Tech University, Lubbock, Texas 79409–1042
E-mail address: byerly@ttmath.ttu.edu