PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 112, Number 2, June 1991

ORDERED RINGS OVER WHICH OUTPUT SETS ARE RECURSIVELY ENUMERABLE SETS

CHRISTIAN MICHAUX

(Communicated by Andreas R. Blass)

ABSTRACT. In a recent paper [BSS], L. Blum, M. Shub, and S. Smale developed a theory of computation over the reals and over commutative ordered rings; in §9 of [BSS] they showed that over the reals (and over any real closed field) the class of recursively enumerable sets and the class of output sets are the same; it is a question (Problem 9.1 in [BSS]) to characterize ordered rings with this property (abbreviated by O = R.E. here). In this paper we prove essentially that in the class of (linearly) ordered rings of infinite transcendence degree over $\mathbb{Q}$, that are dense (for the order) in their real closures, only real closed fields have property O = R.E.

1. INTRODUCTION

In [BSS] L. Blum, M. Shub, and S. Smale developed a theory of computation for commutative ordered rings. In this framework they extended some classical results of the theory of recursive functions over $\mathbb{N}$. Here we deal with the classical result that the class of recursively enumerable sets (r.e. sets) over $\mathbb{N}$, and the class of ranges of recursive functions over $\mathbb{N}$, are the same. Both classes can be defined over any ordered ring. The class of r.e. sets can be described as the class of halting sets for some kind of machines—for example, Turing Machines over $\mathbb{N}$ or BSS machines over ordered rings. In the same way, the class of ranges of recursive functions can be viewed as the class of output sets for the same class of machines.

In the general case the class of halting sets and the class of output sets are not the same. However Blum, Shub, and Smale proved that this result holds over the reals using Tarski's theorem that the reals admit effective elimination of quantifiers (see, for example, [vdD]).

In this paper we assume that every ring is commutative and has a unit.

We prove the following results:

Theorem 1. *Let R be an ordered ring. Assume that R is finitely generated over $\mathbb{Z}$; then R satisfies the property $O = R.E.$*

Received by the editors January 29, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 03C10, 03D25, 68Q05.

Theorem 2. *Let R be an ordered ring which satisfies $O = R.E.$ Assume that R has infinite transcendence degree over $\mathbb{Q}$ and that R is dense (for the order) in its real closure; then R is a real closed field.*

Theorem 2 is related to a result by L. Blum and S. Smale (see §5 and [BS]).

2. Preliminaries

In this section, we give the basic degree of generality necessary for §§3, 4, and 5.

The following description of a machine over an ordered ring R (called here a BSS machine—see [BSS] for a complete definition) will be sufficient for our purpose. A BSS machine has infinitely many registers labelled $r_{-1}, r_0, r_1, \ldots, r_n, \ldots$. The registers $r_1, \ldots, r_n, \ldots$ at any moment of time contain an element of the ring R; r_{-1}, r_0 are two registers used for addressing. The contents of the registers may be altered by the machine in response to three kinds of instructions:

- computation instructions: the contents of the registers are altered by a polynomial map with coefficients in the ring R;
- transfer instructions (addressing);
- branch instructions (such an instruction has two successor instructions, one executed if the content of r_1 is negative, the other one if the content of r_1 is nonnegative).

A machine over R has a finite set of instructions with a "successor relation" that gives the order in which the instructions have to be obeyed by M. Often a machine over R is represented by a directed graph, the nodes of which are the instructions and the edges of which represent the successor relation between the instructions. The coefficients of the polynomial maps of the computation instructions of a machine M are called here the constants of M (there are finitely many such constants for a machine).

When we say that a function is computable over R, this means that there exists a BSS machine over R which computes f.

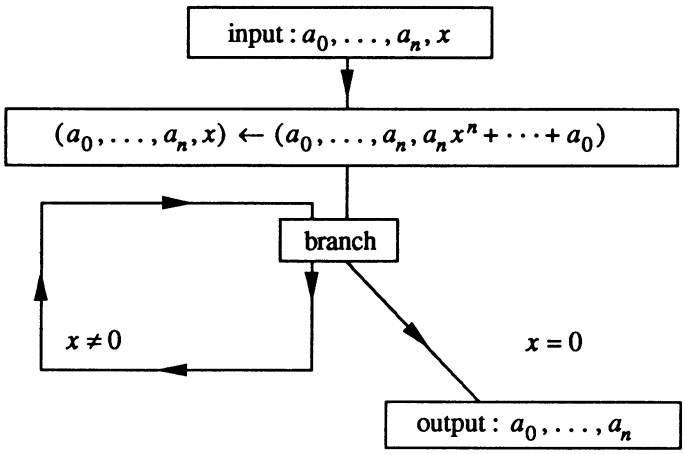
Now we give two results from [BSS] that we use repeatedly (sometimes without explicit mention) in the next sections.

(i) The functions that are computable by a BSS machine over $\mathbb{Z}$ are the classical recursive functions over $\mathbb{Z}$.

(ii) Let $A \subset R^n$ be an r.e. set over R, let $c_1, \ldots, c_t$ be the constants of a machine over R, the halting set of which is A. Then there exists a countable disjunction $\varphi(x_1, \ldots, x_n)$ of first-order formulas $\varphi_i(x_1, \ldots, x_n)$ of the form

$$p_{i1}(x_1, \ldots, x_n) \geq 0 \wedge \cdots \wedge p_{ik_i}(x_1, \ldots, x_n) \geq 0,$$
$$\wedge q_{i1}(x_1, \ldots, x_n) > 0 \wedge \cdots \wedge q_{ij_i}(x_1, \ldots, x_n) > 0,$$

where the p_{ij}'s and the q_{im}'s are polynomials over $\mathbb{Z}[c_1, \ldots, c_t]$ such that $\overline{x} = (x_1, \ldots, x_n) \in A$ if and only if $R \models \varphi(x_1, \ldots, x_n)$.



FLOWCHART 1

Now let us see how the property "O = R.E." is related to a weak notion of elimination of quantifiers. This relation is indirectly given by Lemma 1.

Lemma 1. *Assume R is a ring where the output set of any machine over R is r.e. over R (i.e., R has property "$O = R.E.$"). Then the set $A_n = \{(a_0, \ldots, a_n) \in R^{n+1} | \exists x \in R: a_n x^n + \cdots + a_0 = 0\}$ is an r.e. set over R.*

Proof. A_n is the output set of the machine with Flowchart 1. □

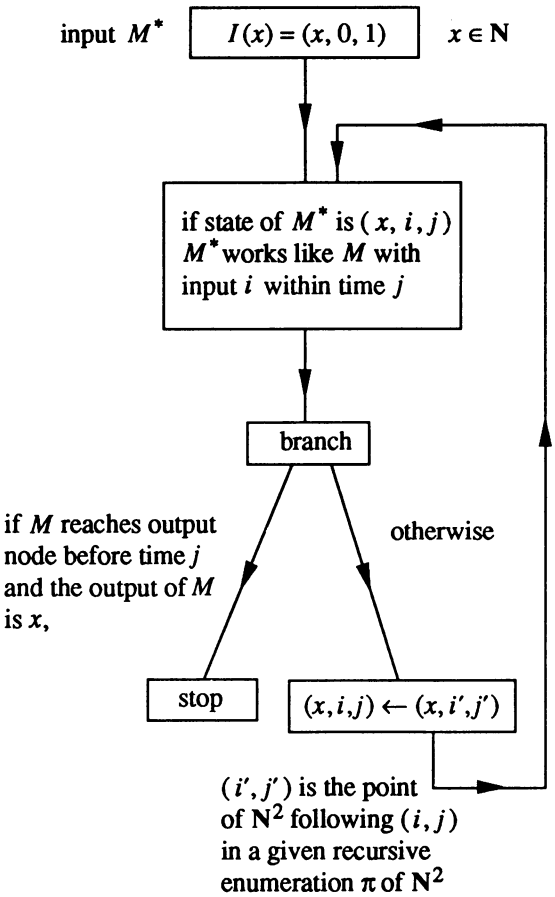
A consequence of this lemma is that the first-order formula $(\exists x)(a_n x^n + \cdots + a_0 = 0)$ is equivalent in R to a countable disjunction of quantifier-free formulas of the language $\mathscr{L} = \langle +, -, \cdot, 0, 1, <, c_{r_{(r \in R)}} \rangle$, but only finitely many additional constants c_r appear in this countable disjunction. So if R satisfies "O = R.E.," R has "weak elimination of quantifiers" for certain formulas. In fact a slight generalization of Lemma 1 shows that R has "weak elimination of quantifiers" for existential formulas of $\mathscr{L}$. We can also see that R satisfies "O = R.E." if and only if a projection of an r.e. set over R is still an r.e. set over R.

3. PROOF OF THEOREM 1

It is well known that $\mathbb{N}$ satisfies the property O = R.E. Let us recall briefly the proof:

If A is the output set of a machine M over $\mathbb{N}$ (for example a Turing machine), then A is the halting set of the machine M^* described by Flowchart 2.

Let us turn now to the proof of Theorem 1. If R is an ordered ring, finitely generated over $\mathbb{Z}$, then $R = \mathbb{Z}[c_1, \ldots, c_\ell]$ and there exists a computable function σ over R from $\mathbb{N}$ *onto* R (σ is obtained by the composition of a computable (over $\mathbb{N}$) bijection from $\mathbb{N}$ to $\mathbb{Z}[X_1, \ldots, X_\ell]$ (the ring of polynomials in ℓ indeterminates) with the function that computes the value $p(c_1, \ldots, c_\ell)$ for any $p \in \mathbb{Z}[X_1, \ldots, X_\ell]$). If A is the output set of a BSS-machine M



FLOWCHART 2

over R, then A is the halting set of the machine $M^\star$ described by Flowchart 2 where we have replaced "$M^\star$ works like M on input i within time j" by "$M^\star$ works like M on input $\sigma(i)$ within time j." □

4. PROOF OF THEOREM 2

Let us recall that we assume in this section that R is an ordered commutative ring with unit (and thus R has no zero divisors).

Lemma 2. *Let $X \subset R^n$ be an r.e. set over R. Assume $t_1, \ldots, t_n$ are algebraically independent over $\mathbb{Q}(c_1, \ldots, c_\ell)$ where $c_1, \ldots, c_\ell$ are the constants of a machine the halting set of which is X. If $(t_1, \ldots, t_n)$ belongs to X, then there exists an open set O (we considered $(R^n, <)$ as a topological subspace of $(\widehat{R}^n, <)$ where $\widehat{R}$ is the real closure of R) such that $(t_1, \ldots, t_n) \in O \subset X$.*

The proof is straightforward using (ii) of §2. □

Lemma 3. *Assume R has infinite transcendence degree over $\mathbb{Q}$ and R is dense in its field of fractions $\overline{R}$. If R satisfies the property "$O = R.E.$," then R is a field.*

Proof. Take the set $E = \{(a, b) \in R^2 | \exists x \in R: ax = b\}$. Since R has property "O = R.E.", E is an r.e. set over R (Lemma 1). Let $c_1, \ldots, c_\ell$ be the coefficients of a machine M over R, the halting set of which is E. Take t_1, t_2 in R with t_1, t_2 algebraically independent over $\mathbb{Q}(c_1, \ldots, c_\ell)$. Then $(t_1, t_1 t_2)$ belongs to E and $t_1, t_1 t_2$ are algebraically independent over $\mathbb{Q}(c_1, \ldots, c_\ell)$. Lemma 2 implies that there exists an open set O in R such that $(t_1, t_1 t_2) \in O \subset E$. Since R is dense in its field of fractions $\overline{R}$, $O \neq \{(t_1, t_1 t_2)\}$. Thus for every ε, $\varepsilon' \in R$ sufficiently near zero, $R \models (\exists x)((t_1 + \varepsilon)x = t_1 t_2 + \varepsilon')$, in particular $R \models (\exists x)(t_1 x = t_1 t_2 + \varepsilon')$. Thus there exists an open interval I (in R) around 0 such that if $\varepsilon \in I$ then $R \models (\exists x)(t_1 x = \varepsilon)$. We claim that t_1 is invertible in R. Otherwise for every $r \in R$, $R \models (\forall x)(t_1 x \neq 1 + r t_1)$. But the set $1 + R t_1$ is dense in R (since R is dense in $\overline{R}$) and thus it intersects with I; this furnishes the contradiction. It is clear that the argument above can be repeated for every t transcendental over $\mathbb{Q}(c_1, \ldots, c_\ell)$.

Now if a is an element in R and t is an element in R, transcendental over $\mathbb{Q}(a, c_1, \ldots, c_\ell)$, then at is transcendental over $\mathbb{Q}(c_1, \ldots, c_\ell)$. Thus at is invertible in R so a is invertible in R. □

Lemma 3 explains why Theorem 1 is limited to the "finitely generated case". If $\{r_i, i \in \omega\}$ is a countable set of algebraically independent reals, the subring $\mathbb{Z}[r_i, i \in \omega]$ of the reals does not satisfy the property O = R.E. although it is countable and even recursive in the sense of Rabin [Ra].

Lemma 4. *Assume R is an ordered field that is dense in $\hat{R}$, its real closure. Let $X_n = \{(a_0, \ldots, a_{n-1}) \in [R(i)]^n | \exists x \in R(i), a_0 + \cdots + a_{n-1} x^{n-1} + x^n = 0\}$ (where $i^2 = -1$). If $R \neq \hat{R}$, there exists an integer n such that X_n^c is dense in $[R(i)]^n$. ($R(i)$ is identified with R^2 and dense is defined w.r.t. the product topology on R^2.)*

Proof. We use a refinement of a standard trick (see [MMV]). If $R \neq \hat{R}$, take the least n such that $X_n^c \neq \varnothing$. Let $(b_0, \ldots, b_{n-1})$ be in X_n^c. Then for every x in $R(i)$, $b_0 + \cdots + b_{n-1} x^{n-1} + x^n \neq 0$. By the choice of n, $b_0 + \cdots + b_{n-1} X^{n-1} + X^n$ is irreducible over $R(i)$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $b_0 + \cdots + b_{n-1} X^{n-1} + X^n$ in $\hat{R}(i)$. Since the characteristic of R is zero, the α_i's are distinct, so the following matrix M is invertible:

$$M = \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix}.$$

Set $\bar{r} = M\bar{t}$ with $\bar{t} \in [R(i)]^n$, and set $(X - r_1) \cdots (X - r_n) = X^n + g_{n-1} X^{n-1} + \cdots + g_0$. It is easy to see that the g_i's are invariant under permutations of

the α_i's; it follows from a standard result in Galois theory that the g_i's are in $R(i)$. Note that φ, defined by $\varphi(\bar{t}) = M\bar{t}$, is a bijective mapping from $[\hat{R}(i)]^n$ to $[\hat{R}(i)]^n$. Thus the mapping $\mathscr{G}: [\hat{R}(i)]^n \to [\hat{R}(i)]^n: \bar{t} \to g(\varphi(\bar{t}))$ (where $g(\bar{r}) = (g_0, \ldots, g_{n-1})$, with the g_i's defined as above) is onto. It follows that $\mathscr{G}([R(i)]^n)$ is dense in $[\hat{R}(i)]^n$ since $\mathscr{G}$ is a continuous mapping. We also have $\mathscr{G}([R(i)]^n) \subset X_n^c$, as otherwise there would exist $\bar{t}$ in $[R(i)]^n$ such that $(X - r_1)\cdots(X - r_n)$ (where $\bar{r} = M\bar{t}$) has a root in $R(i)$, i.e., one of the r_i's would belong to $R(i)$. Then one of the α_i's satisfies a polynomial equation of degree $< n$, a contradiction since $b_0 + \cdots + b_{n-1}X^{n-1} + X^n$ is irreducible over $R(i)$, and thus it is the minimal polynomial of the α_i's. □

We can now finish the proof of Theorem 2.

Lemma 3 says that R is a field. Let X_n be as in Lemma 4; a slight improvement of Lemma 1 shows that X_n is an r.e. set over R (when we considered $X_n \subset R^{2n}$). We claim that X_n contains a nonempty open set of R^{2n}. By Lemma 4 we can conclude that $X_n = R^{2n}$; therefore $R(i)$ is algebraically closed, so R is real closed.

Proof of the claim. Let $c_1, \ldots, c_\ell$ be the coefficients of a machine over R, the halting set of which is X_n. Take $t_{11}, t_{12}, \ldots, t_{n1}, t_{n2}$ in R, $2n$ algebraically independent elements over $\mathbb{Q}(c_1, \ldots, c_\ell)$. Consider the polynomial $(X-(t_{11}+it_{12})\cdots(X-(t_{n1}+it_{n2}))$; then its coefficients $s_j = s_{j1}+is_{j2}$ belong to X_n. Since $\mathbb{Q}(c_1, \ldots, c_\ell)(i, t_{11}, t_{12}, \ldots, t_{n1}, t_{n2})$ is the splitting field of

$$(X - (t_{11} + it_{12}))\cdots(X - (t_{n1} + it_{n2}))(X - (t_{11} - it_{12}))\cdots(X - (t_{n1} - it_{n2}))$$

over $\mathbb{Q}(c_1, \ldots, c_\ell)(i, s_{11}, s_{12}, \ldots, s_{n1}, s_{n2})$, it follows that $s_{11}, s_{12}, \ldots, s_{n1}, s_{n2}$ are algebraically independent over $\mathbb{Q}(c_1, \ldots, c_\ell)$. We conclude using Lemma 2. □

5. Remarks

From Theorem 1 and Theorem 2, $\mathbb{Q}$ does not satisfy property O = R.E. However, if we allow rational maps instead of polynomial maps in the computation instructions, it is not too difficult to see that the following is true.

Theorem 1′. *Let R be an ordered commutative field. Assume R is finitely generated over $\mathbb{Q}$; then R satisfies the property O = R.E.*

In the same way (by modifying the primitives used in the instructions) we can develop a theory of computation over rings or over fields (we have to replace the test "$r_1 < 0$" in branch instructions by "$r_1 \neq 0$").

In this case *a commutative ring R without zero divisors of infinite transcendence degree over $\mathbb{Q}$, satisfies the property O = R.E. if and only if R is an algebraically closed field.* It suffices to modify Lemma 1 slightly and to follow closely the proof of Theorem 1 in [MMV] (that proves the converse of Tarski's theorem for fields). Curiously, in the proof of our Theorem 2 we cannot closely

follow the proof of Theorem 2 in [MMV] (that proves the converse of Tarski's theorem for ordered fields) because the proof of [MMV] works on A_n^c (where A_n is defined as in Lemma 1) which is not a priori an r.e. set over R under our assumptions.

L. Blum and S. Smale have proved a result related to Theorem 2; in particular they show Theorem 2 under the stronger assumption that every definable set over R is decidable over R ($X \subset R^n$ is decidable over R if X and X^c are r.e. sets over R); A_n and X_n are clearly decidable sets over R under this assumption. (For a discussion and a proof of this result, see [BS], §6.)

Finally let us recall the folk result that in a sufficiently saturated first-order structure (see [CK] or [Sa] for a definition) weak elimination of quantifiers is equivalent to elimination of quantifiers (and thus in the case of ordered rings it is equivalent to be a real closed field). This shows, for example, that any sufficiently saturated elementary extension $\langle Z^*, +, \cdot, <, 0, 1\rangle$ of $\langle \mathbb{Z}, +, \cdot, <, 0, 1\rangle$ does not satisfy the property O = R.E.

Acknowledgment

I wish to thank Angus Macintyre and Françoise Point for stimulating conversations.

References

[BS] L. Blum and S. Smale, *The Gödel incompleteness theorem and decidability over a ring*, 1989.

[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. **21** (1989), 1–46.

[CK] C. C. Chang and H. J. Keisler, *Model theory*, North-Holland, Amsterdam, 1973.

[MMV] A. Macintyre, K. McKenna and L. van den Dries, *Elimination of quantifiers in algebraic structures*, Adv. in Math. **47** (1983), 74–87.

[Ra] M. O. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

[Sa] G. E. Sacks, *Saturated model theory*, W. A. Benjamin, 1972.

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

UNIVERSITE DE MONS, FACULTE DES SCIENCES, AVENUE MAISTRIAU 15, B 7000 MONS, BELGIQUE