ALGORITHMIC PROCEDURES

HARVEY FRIEDMAN AND RICHARD MANSFIELD

ABSTRACT. We consider the state of elementary recursion theory when the familiar $0, 1, +, \times, =, <$ of ordinary arithmetic are replaced by constants, functions, and relations from an arbitrary model.

This paper should be viewed as a sequel to Friedman (1971). We sharpen and improve that paper as well as giving extensive coverage to various specific rings and fields. The impetus for reexamining this old paper comes from the work of Blum, Shub, and Smale (1989). One of the lessons to be drawn from their work is the importance and interest in applying the techniques of generalized recursion theory to various standard algebraic structures such as the real and complex numbers. It is only by taking this lesson to heart that we have been able to discover enough counterexamples to really extend the results in Friedman (1971).

Our first step, of course, is to define what we mean by "computable" in the general context. In this we follow Friedman closely, just rephrasing his definitions into more modern terminology. We then give the basic structure theorems for this definition, including an abstract analog for Church's thesis. Here again we closely, but not completely, follow Friedman. This section sets up the notation and the basic structure for what is to follow.

We then come to the main topic of this paper, charting the places of the elementary theorems about r.e. sets in the more general setting. This too was begun in Friedman (1971), but here we go far beyond what he did there. A characteristic result is Theorems 15 and 16, where we show that the reals with certain extra Borel relations added to the language, has a universal r.e. set but no universal computable functions.

1. INTRODUCTION

Let L be a language of finite type, i.e. using only finitely many constant, relation, and function symbols, and let M be an interpretation for L, i.e. a nonempty universe with actual constants, relations, and functions corresponding to the symbols in L. We first define the notion of a finite algorithmic procedure over M (fap for short). Take your favorite computer language and strip it to the bone and you will probably be left with simple variables (no arrays), assignment statements, conditionals, and goto's. Now consider the case where the assignments and conditionals use the symbols in L rather than the

usual stock of $+$, $\times$, $<$, $=$, etc. A fap is a program written in this stripped down language. We can give input to such a program by initializing some of its variables with values from M and receive output by examining the value of a variable (or variables if we want multidimensional output) on termination. A fap computable function is a function from M^n into M which can be programmed with a fap using finitely many extra constant symbols to stand for parameters in M. Here is a typical fap (over $\mathbb{R}$, the real numbers) with v both the input and output variable:

$$10 \text{ if } v < 1 \text{ then END},$$
$$20 \, v = v - 1,$$
$$30 \text{ goto } 10.$$

If this program starts with $v = x$, a real number ≥ 1, then it calculates the fractional part of x. Otherwise, it just returns x.

The reader may wish to substitute while statements for the conditionals and goto's, or evan abandon the programming analogy entirely and give a definition based on some sort of machine architecture. The essential features are:

1. Each program or machine must use only a fixed finite number of variables or locations, each of which may hold an arbitrary member of the universe of the structure.

2. The ability to evaluate terms of L and do conditional branches based on the atomic formulas of L.

Note that the above definition allows several features which most logicians think of as not computable, e.g. the ability to store an arbitrary irrational number in its entirety, not just a finite approximation to it, and the ability to equality test two arbitrary reals. Most numerical analysts, however, regard this as a realistic model of floating point arithmetic on a computer. Round-off error can be incorporated into this system by using a round-off algebra as the underlying structure rather than the reals. (See Knuth (1969) or Mansfield (1984).) This is a project which has not yet been carried out.

We can easily imagine many possible extensions of faps to seemingly more powerful languages. One in particular plays an important role in the theory, namely faps with stacks. A program in this language would use finitely many stacks, stack_1, stack_2, $\ldots$, stack_n. Each stack would be potentially infinite. The program would access these stacks with the commands $\text{push}_i(x)$ and the zero-place functions pop_i. The command $\text{push}_i(x)$ would push x onto stack_i and the function pop_i would return the value at the top of the stack_i.

With a little programming, the reader familiar with Blum et al. (1989) should be able to easily prove the following proposition:

Theorem 1. *When M is taken to be the real numbers with the language of ordered fields, the fap computable functions are exactly the functions definable by finite dimensional machines of Blum et al. (1989) and the fap with stacks functions are exactly the ones definable with infinite dimensional machines.*

The most general definition of computable is what Friedman (1971) calls effective definitional schemes or *eds* for short. A condition is called *basic semialgebraic* if it can be defined as a finite conjunction of atomic formulas and their negations. It is *semialgebraic* if it is a finite disjunction of basic semialgebraics. Such conditions can of course be identified with their Gödel numbers. A set of conditions is effective if its Gödel numbers is an ordinary recursively

enumerable set over the integers. A function $f(x)$ is eds definable if there is an effective set $\{\langle t_i(v, v_1, \ldots, v_n), \varphi_i(v, v_1, \ldots, v_n)\rangle : i \in \omega\}$ where v's are formal variables, each t_i is a formal term, and each φ_i is a basic semialgebraic condition and there are $a_1, \ldots, a_n$ from the universe of the model such that f is defined by the conjunction of all conditions of the form:

$$f(x) = t_i(x, a_1, \ldots, a_n) \quad \text{if } \varphi_i(x, a_1, \ldots, a_n).$$

The a's are called the parameters of the definition.

Theorem 2 (Friedman 1971). *Any fap with stacks computable function (and consequently any fap computable function) is eds definable.*

The reader may wish to consult Friedman's paper for a proof of this fundamental theorem, but I suggest a moment's reflection could be more effective. A more general philosophical argument can be given that for any reasonable definition, any computable function is eds definable. Hint: Consider computation trees and examine the following example.

The theory can be illustrated with the above example of a fap. Here is the computation tree. Each node is labeled with the current value of the formal variable v as a polynomial in the input value x and with the condition on x necessary to reach the node. The end nodes of the tree give the eds.
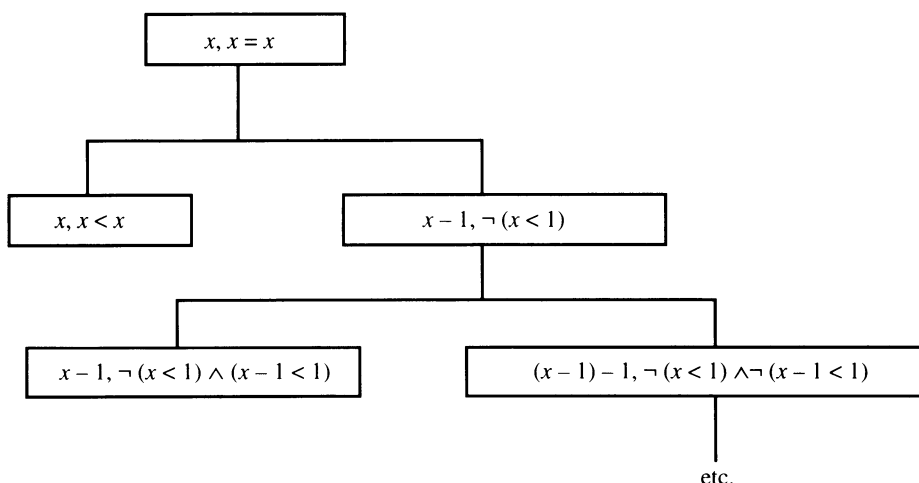
Let us call a set *generalized r.e.* if it is the domain of an eds definable function. Theorem 2 has the following corollary:

Theorem 3. *A set is r.e. iff it is an effective union of sets basic semialgebraic in the same finite set of parameters.*

Theorems 2 and 3 say in essence that computable functions are sort of generalized polynomials and r.e. sets are generalized semialgebraic sets. This means that the algebraic study of various specific rings and fields such as the algebraic number fields, the reals and complexes, etc. is incomplete without studying their computable functions. The purpose of this paper is to lay out the logical foundations of this essential branch of algebra.

Many of our theorems will have a hypothesis saying that M has a nontrivial relation, i.e. an atomic relation taking on both of the values true and false. The reason for this is given by the following easy fact:

Theorem 4. *If M has only trivial relations, then all r.e. relations are trivial and all computable functions are defined by formal terms. In other words, in order to have any recursion theory at all you must have a nontrivial relation.*

There are structures M for which fap definable is not as general as eds definable, i.e. there is a function f which is eds but not fap. However, for a wide class of models which includes all commutative rings and fields, these two classes do coincide. Here are the two definitions which allow us to state the relevant theorem.

A structure is *ω-rich* if there is an embedding of the natural numbers into the universe of the structure such that the predecessor and successor functions are the restriction to the range of this embedding of fap computable functions and the equal-zero relation is the restriction of an atomic relation applied to fap computable terms. It is easily seen that in an ω-rich structure all recursive functions are fap definable. (By which we mean, the restriction to the natural numbers of fap computable functions.)

A structure is *structural* if it is ω-rich and for each n there is a fap computable function $eval_n(x, x_1, \ldots, x_n)$ such that whenever x is the Gödel number of a formal term $t(v_1, \ldots, v_n)$ then $eval_n$ is the value of the term. Since we are assuming that the underlying language is finite, it is easily seen that the corresponding function $truth_n$ which gives the truth value of an atomic formula as a function of its Gödel number is also fap computable. Friedman (1971) Lemma 1.6.2 gives an elegant model theoretic property equivalent to structurality.

Theorem 5. *If the structure M is ω-rich and structural, then every eds definable function on M is fap computable.*

Proof. Suppose $f(x_1, \ldots, x_n)$ is eds definable. That means that there are integer recursive functions p and q which enumerate sets of Gödel numbers such that $f(x_1, \ldots, x_n)$ is defined by a conjunction of clauses of the form:

$$f(x_1, \ldots, x_n) = t_i(x_1, \ldots, x_n, a_1, \ldots, a_k) \quad \text{if } \varphi(x_1, \ldots, x_n, a_1, \ldots, a_k)$$

where t_i is the term with Gödel number $p(i)$ and φ_i is the formula with Gödel number $q(i)$. f is then defined by the fap which searches for an i with $truth_{n+k}(q(i), x_1, \ldots, x_n, a_1, \ldots, a_k) =$ true and then returns $eval_{n+k}(p(i), x_1, \ldots, x_n, a_1, \ldots, a_k)$.

Theorem 6. *Any field or commutative ring of characteristic* 0 *is structural and ω-rich.*

Proof. The ω-rich property is immediate. To prove structurality, first note that there is a recursive function $p(x)$ which associates to each Gödel number of a formal term another Gödel number, namely the Gödel number of the ratio of two polynomials provably equal to the original term. By ω-richness, this function is fap computable. Obviously, the function which evaluates the ratio of two polynomials in n variables is fap computable. Structurality follows since the composition of faps is a fap.

Theorem 7. *Over any field or ring of characteristic* 0 *, a function is fap computable iff it is fap with stacks computable.*

Theorem 8. *Any finite dimensional function computable with an infinite dimensional machine of Blum et al. is already computable with a finite dimensional machine. (This answers an open question stated in their paper.)*

Let us finish this section by stating some open problems. A function from $\mathbb{R}$ to $\mathbb{R}$ is a round-off function if it is idempotent, preserves $\leq$, and has a discrete range. If f is a round-off function, we can use it to define algebraic operations on the range of f, e.g. $x \oplus y = f(x + y)$. The IEEE standard for computer floating point operations demands that all computer arithmetic be defined in this way.

Problem. Which round-off functions lead to structural models?

2. UNIVERSAL AND PAIRING SYSTEMS

A pairing system consists of three functions, a total function P mapping M^2 one-to-one into M, and functions K and J mapping M into M whose domains both contain the range of P such that $K(P(x, y)) = x$ and $J(P(x, y)) = y$. The function P by itself is a pairing function, but in order to make much use of it we also need the decoders, K and J.

A universal system consists of:

1. Computable functions $U_n(e, x_1, \ldots, x_n)$ such that for any computable function $f(x_1, \ldots, x_n)$ there is an e in M with $f = U_n(e, -)$.

2. Computable functions $S_{n,m}$ such that $U_{n+m}(e, x_1, \ldots, x_n, y_1, \ldots, y_n) = U_m(S_{n,m}(x_1, \ldots, x_n), y_1, \ldots, y_m)$ whenever either is defined.

A set is recursively enumerable iff it is the domain of a computable function.

Theorem 9. *If M has a universal system, then there is an r.e. set whose complement is not r.e. and there is an r.e. subset of M^2 universal for r.e. subsets of M.*

Proof. Our above definition contains all the parts necessary to carry out the normal proof. (See for instance Rogers (1967, §1.9).)

Most work in recursion theory has concentrated on finding r.e. sets whose complement is not r.e. Here we see that a universal system guarantees such a set, but it is not a necessary condition. We shall see shortly that $\mathbb{R}$ does not have a universal system, but it does have an r.e. not co-r.e. set. Blum et al. has pointed out that the eds definition of computable easily implies that any r.e. subset of $\mathbb{R}$ must have only countably many connected components. It is left as an exercise to show that the Cantor set is co-r.e. Similarly, over $\mathbb{C}$, the complex numbers, the set of integers is r.e. not co-r.e. In all the models that we have so far considered, there is some argument to show the existence of an r.e. not co-r.e. set. In Mansfield (1990), it is shown that all Archimedean ordered fields have an r.e. set whose complement is not r.e. We are far from characterizing those models which have this property.

We can prove two theorems concerning this problem.

Theorem 10. *If M is $\aleph_0$-categorical, then over M every r.e. set has an r.e. complement.*

Proof. By Ryll-Nardzewski's theorem (see Chang and Keisler, 1973, Theorem 2.13.3, p. 101), if M is $\aleph_0$-categorical, for each n it has only finitely many n-types. This means that every eds is equivalent to a finite eds.

Theorem 11. *There is an ω-rich model for which all r.e. sets have an r.e. complement.*

Proof. Let the universe of M consist of finite type theory, i.e. the disjoint union of ω and its power set and the power set of its power set etc. The language, L, has just two function symbols, succ and pred, and two relations, equal-zero, member. succ and pred are to be the ordinary successor and predecessor functions on ω and the identity elsewhere. While equal-zero(x) is true iff x is 0, and member(x, y) is true iff x is a member of y. Equality is not included.

Let us look at the sets which can be defined using atomic formulas and parameters from this model. In particular we are interested in examining how parameters can be used to single out sets of rank larger than the parameter. Whenever s and t are terms and x is of rank > 0, equal-zero$(t(x))$ is false, and member$(s(x), t(x))$ is false. Further, if a is a parameter and rank$(x) >$ rank(a), then member$(s(x), t(a))$ is false. This leaves us with the single case member$(s(a), t(x))$. When rank$(x) >$ rank$(a) + 1$, this too is false.

Thus we see that whenever $\varphi(x)$ is a basic semialgebraic condition in parameters $a_1, \ldots, a_n$, then $\varphi(x)$ is either always true or always false among the x's whose rank is greater than $1 +$ the maximum rank of the a_k. Consequently, any r.e. set also has this property. Suppose the r.e. set A has nontrivial intersection A_k with the sets of rank k for $k = 0$ to n and trivial intersection with all ranks larger than n. Also let B_k be the universe of all sets of rank k for $k = 0$ to n. Then the complement of A can easily be given with a finite eds using the A's and B's.

This model is still somewhat trivial in that, just like the categorical case, all eds definitions are equivalent to finite ones.

Problem. Is there a model M which has an eds not equivalent to a finite eds, but for which all r.e. sets have r.e. complements.

Theorem 12. *If M has a nontrivial relation and a pairing system, it is ω-rich and structural.*

Proof. To prove ω-richness, let $r(x_1, \ldots, x_n)$ be a nontrivial atomic relation. Let $a_1, \ldots, a_n$ satisfy r and $b_1, \ldots, b_n$ satisfy its negation. We may as well assume that $a_i = b_i$ for all but one i. Since otherwise we could change the a's to b's one at a time until we get the first true to false transition. So by using the other coordinates and parameters and supressing their mention, we may as well assume that r has one variable. We define the embedding, φ, of the natural numbers into M. $\varphi(0) = P(a, a)$ and $\varphi(n + 1) = P(\varphi(n), b)$. Then $P(x, b)$ is the successor, $K(x)$ is the predecessor, and $r(J(x))$ is the equal-zero test.

To prove structurality, we use the pairing function to simulate stacks. Assume that the recursive functions p and q are such that $p(i, x)$ gives the ith character in the reverse Polish representation of the term with Gödel number x, and $q(x)$ gives the length of this representation. By ω-richness, we know that p and q are fap computable. Using p and q as subroutines, it is straightforward to write down a fap for eval$_n$. (Use a variable s to represent a stack with $s = P(s, y)$ for push and $z = K(s)$; $s = J(s)$ for pop.)

Theorem 13. *If M has a nontrivial relation, it has a pairing system iff it has a universal system.*

Proof. Suppose M has a universal system. Let r, a, b be as in the proof of Theorem 12. Consider the eds,

$$f(c, d, x) = \begin{cases} c & \text{if } r(x), \\ d & \text{otherwise}. \end{cases}$$

It has a code e such that

$$U_2(e, c, d, x) = f(c, d, x).$$

Let

$$P(c, d) = S_{2,1}(e, c, d), \quad K(x) = U_1(x, a), \quad J(x) = U_1(x, b).$$

Thus M has a pairing system.

Now suppose M has a pairing system. Note that by the previous theorem, it is also ω-rich. Using the pairing function it is easy to code a finite parameter list by a single element. Obviously, the code e for an eds will consist of an integer e_0 coding the eds as an ordinary r.e. set over the integers, and the code for the parameter list, i.e. let $e = P(e_0, a)$ where a codes the parameter list. The function $U(e, x)$ will take such a pair, recover e_0 and the list a, then use Kleene's universal function of ordinary recursion theory with index e_0 to enumerate the eds until an element $\langle t(v, v_1, \dots, v_n), \varphi(v, v_1, \dots, v_n) \rangle$ is found such that $\varphi(x, a_1, \dots, a_n)$ is true, and then evaluate $t(x, a_1, \dots, a_n)$.

In order to carry out this process we need a strong eval function. This new function will take a Gödel number for a term (in an arbitrary number of variables) and an argument list coded by a single element and produce the value. The first step in the definition of this function is to take the Gödel number, however it was defined and convert it into the Gödel number of a term in reverse Polish. Since this translation is recursive in the ordinary sense, it can be defined via a fap due to the ω-richness of the model. It is then a simple matter to use the pairing function to simulate a stack and evaluate the term.

The function $S(e, x)$ will just add x to the parameter list in e.

By Theorems 9 and 13, in order to establish the nonexistence of a pairing system for $\mathbb{C}$ and for $\mathbb{R}$, it suffices to show that there is no universal r.e. set for either.

Theorem 14. *There is no r.e. subset of $\mathbb{R}^{n+1}$ universal for r.e. subsets of $\mathbb{R}$. Likewise for $\mathbb{C}$.*

Proof. Suppose that $A(x, y)$ is a counterexample. First note that if $\varphi(x, y)$ is a conjugation of equalities and inequalities and x is a real such that $\{y : \varphi(x, y)\}$ is finite, then all such y are algebraic in x. From the eds definition of A (Theorem 3), we see that this means that the same property holds with A in place of φ (at least if we allow a fixed finite set of parameters which we will proceed to ignore). Now define a function f from $\mathbb{R}$ onto $\mathbb{R}^2$. f is not meant to be computable.

$f(x) = \langle 0, 0 \rangle$ if $A(x, -)$ has more than three or less than
one element.

$f(x) = \langle y, y \rangle$ if y is the only element of $A(x, -)$.

$f(x) = \langle y, z \rangle$ if y and z are the only two elements of
$A(x, -)$ and $y < z$.

$f(x) = \langle z, y \rangle$ if $A(x, -)$ has exactly three elements and y, z
are the two smallest and $y < z$.

We now have a function f mapping $\mathbb{R}$ onto $\mathbb{R}^2$ such that for every x, both
coordinates of $f(x)$ are algebraic in x. This is impossible. In fact any such
function must have a range of the 1st Baire category. For each pair of rational
polynomials p, q and each pair of integers n, m, we can define the function
$f_{p,q,n,m}(x) = \langle$ the nth root of $p(x, -)$, the mth root of $q(x, -) \rangle$. All these
functions have a nowhere dense range, and there are only countably many of
them, but the range of f is contained in the union of their ranges. A similar
argument holds for $\mathbb{C}$.

We can actually prove a stronger theorem than this about the nonexistence
of pairing functions on $\mathbb{R}$ and $\mathbb{C}$.

Theorem 15. *Let M be $\mathbb{R}$ expanded by any finite number of Borel relations.
There is no one-to-one function computable over M mapping $\mathbb{R}^2$ into $\mathbb{R}$. Like-
wise for $\mathbb{C}$.*

Proof. Suppose f is a counterexample. Looking at the eds definition of f,
we see that there is a finite set of parameters $a_1, \ldots, a_n$ such that for every x
and y there is a rational function p and a Borel set B such that $\langle x, y \rangle \in B$
and $f(u, v) = p(a_1, \ldots, a_n, u, v)$ for all $\langle u, v \rangle \in B$. Since the eds only
gives countably many possibilities for p and B, this means that one of these
rational functions must be one-to-one on a 2nd category Borel set. This is
impossible. If $p(x, y)$ is one-to-one on the second category set A, consider
$B = \{x : \{y : \langle x, y \rangle \in A\}$ is 2nd category$\}$ by a theorem of Ulam, B is 2nd
category. But a nonconstant rational function of one variable plainly maps 2nd
category sets onto 2nd category sets. (It is piecewise continuous and strictly
monotone, and any such map really plainly preserves 2nd category.) Therefore,
for x in B, $\{p(x, y) : \langle x, y \rangle \in A\}$ is second category. Thus we have an
uncountable collection of pairwise disjoint 2nd category sets, a contradiction.

Theorem 16. *There is a model having a universal r.e. set but no pairing system.*

Proof. Let P be a one-to-one Borel function mapping $\mathbb{R}^2$ onto $\mathbb{R}$. Let K and
J be the Borel decoding functions. Then $M = \langle \mathbb{R}, P, K, J \rangle$ has a universal
computable function.

Let us recall how the function $U(e, x)$ was constructed in the proof of
Theorem 13. We start with a computable function, $\mathrm{eval}(g, a, x)$ whose three
arguments are as follows:

1. g is a Gödel number of a basic semialgebraic condition, $\varphi(v, v_1, \ldots, v_n)$.

2. a is a single point which encodes the parameter list, $a_1, \ldots, a_n$ to be
used in φ.

3. x is the argument of U.

eval(g, a, x) is then supposed to return the truth value of $\varphi(x, a_1, \ldots, a_n)$. $U(e, x)$ was then defined using Kleene's universal function for ordinary recursion theory with (e) and eval.

Here we shall use these ingredients in a slightly different manner. Let $\{e\}\{n\}$ be Kleene's function. Then there is a primitive recursive predicate $T(e, x, y, z)$ such that $\{e\}\{n\} = y$ iff $\exists z T(e, n, y, z)$. Define $US = \{\langle e, n, m, g, a, x \rangle : T(e, n, g, m) \wedge \text{eval}(g, a, x) = \text{true}\}$. Note that US is plainly Borel. x is in the domain of $U(e, -)$ iff $\exists n \exists g \exists m US(K(e), n, g, J(e), x)$. Thus every generalized r.e. set over M is of the form $\exists n \exists g \exists m US(K(e), n, g, J(e), -)$. Call this new relation $US_1(e, x)$.

Now consider the model $N = \langle \mathbb{R}, US \rangle$. Claim: Any set r.e. over N is also r.e. over M. This follows easily since the complement of US is also r.e. over M. It is just $\neg T \cap (\text{eval} = \text{false})$. The first of which is primitive recursive and the second is r.e. over M.

From this claim, it follows that US_1 is universal for sets r.e. over N since we have already established that it is universal for M. We finish the theorem by noting that US_1 is itself r.e. over N.

Theorem 17. *If K is a real closed or algebraically closed field of infinite transcendence degree, there is no one-to-one computable function mapping K^2 into K.*

Proof. Again suppose otherwise. Let a and b be algebraically independent over the parameters used to define the pairing function f. The eds definition of f contain a clause of the form $f(x, y) = p(x, y)$ if $\varphi(x, y)$ where p is a polynomial in the parameters and φ is a conjunction of polynomial equalities and inequalities and $\varphi(a, b)$ is true. But a and b can satisfy no polynomial equalities, therefore φ consists solely of inequalities. Furthermore K must satisfy the first order sentence saying that p is one-to-one on φ and φ is nonempty. When we existentially quantify out the parameters in this statement we have a sentence in the language of ordered fields or just fields, depending on K. In any case the sentence must be true in either $\mathbb{R}$ or $\mathbb{C}$ since any real closed field is elementarily equivalent to $\mathbb{R}$ and any algebraically closed field is elementarily equivalent to $\mathbb{C}$. Therefore we have a polynomial which is one-to-one on a nonempty open set. In the previous theorem we established that this cannot happen, but of course here the situation is much simpler; the implicit function theorem also gives an immediate contradiction.

Theorem 18. *If K is any Archimedean ordered field of finite transcendence degree, then K does not have a pairing system.*

Proof. Let $a_1, \ldots, a_n$ be a transcendence basis for K over Q, the field of rational numbers. We first describe the pairing function $P(x, y)$. Enumerate all triples of polynomials with coefficients in $Q(a_1, \ldots, a_n)$ until three are found satisfying the identities, $p_1(p_3(x, y)) = x$ and $p_z(p_3(x, y)) = y$. The existence of such a triple follows from the theorem of the primitive element. (This is a basic theorem of algebra which for a field of characteristic 0 is exactly equivalent to the existence of these three polynomials. See any standard algebra text.) Let $z = p_3(x, y)$. Calculate the integer part and fractional part of z. (A modified version of the fap given at the beginning of this paper will do the trick.)

Let $P_0(x, y)$ be any standard recursive pairing function for the integers. By ω-richness, it is fap computable. Let $P(x, y) = P_0(\text{int}(z), P_0(p_1, p_2)) + \text{fract}(z)$. Decoding consists of finding the integer part of $P(x, y)$, recovering z and the polynomials, p_1 and p_2, using the decoders for P_0, and then calculating $p_1(z)$ or $p_2(z)$. By Theorem 6, this final calculation can be done as a computable function of the two Gödel numbers and the value z.

Theorem 19. *The field* $Q[2^{1/2}]$ *(without order) has a parameter free pairing system.*

Proof. Use the symbol $\times$ for multiplication. We show how to calculate the pair $\langle x, y \rangle$. Let $x = p + q \times 2^{1/2}$. We claim that p can be computably recovered from x. Let K_0 and J_0 be the decoders for the recursive pairing function P_0 used in Theorem 18. Using K_0 and J_0, we can easily write down a function mapping the natural numbers onto Q^2, e.g.

$$n \to \langle K_0(K_0(n))/(J_0(K_0(n)) + 1)), K_0(J_0(n))/(J_0(J_0(n)) + 1)) \rangle.$$

Starting with $n = 0$, keep incrementing n until the pair of rationals, $\langle a, b \rangle$, associated with n satisfies the condition, $(x - a)^2 = b$. Then $a = p$. We can also compute $q^2 = b/2$. Similarly, if $y = p' + q' \times 2^{1/2}$, we can calculate p' and q'^2. Applying the same algorithm to $x \times y$, we can calculate $p \times p' - 2 \times q \times q'$ and consequently, $q \times q'$. Next calculate the sign, s, of $q \times q'$. This is to be done by enumerating all positive rationals until one is found which is either $q \times q'$ or $-q \times q'$. Also extend P_0, J_0, and K_0 to the rationals by regarding each rational as a pair of integers. (Note that the above calculation of p and q^2 really produced pairs of integers.) Let $\langle x, y \rangle = \langle p, p', q^2, q'^2, s \rangle + q \times 2^{1/2}$ where the 4-tuple on the R.H.S. is built up using P_0. To decode, first calculate the 4-tuple by the above method for finding p. Subtracting this from $\langle x, y \rangle$ gives $q \times 2^{1/2}$. Then calculate p, p', q^2, q'^2 using J_0 and K_0. Then enumerate all positive rationals until one is found whose square is q'^2/q^2. Then multiply by s. In this way you have calculated q'/q. Multiplying by $q \times 2^{1/2}$ (which you already know) gives $q' \times 2^{1/2}$. Now calculate x and y.

Problem. Is there a one-to-one polynomial map from Q^2 into Q?

Problem. Is there a pairing function or a pairing system on the algebraic reals without the less than relation?

In many of the above uses of pairing functions, it did not really matter which pairing function was used, just as long as we chose one. The pairing function might be used for instance to simulate stacks for intermediate calculations, but the choice of which pairing function is used had no effect on the outcome. In these cases, the function can be computed without the use of any pairing function at all.

Theorem 20. *If M is ω-rich and structural, and there is a fap which computes f over any $\langle M, P, K, J \rangle$ where P, K, J is a pairing system, then f is computable over M.*

Proof. Let $\text{rat}(x_1, \ldots, x_n)$ be the set of all elements of M expressible as the values of formal terms with arguments $x_1, \ldots, x_n$. The function $k \to \text{eval}_n(k, x_1, \ldots, x_n)$ maps ω onto $\text{rat}(x_1, \ldots, x_n)$. Hence using a pairing

function for ω, we can define computable functions $P(x_1, \ldots, x_n, x, y)$ and $K(x_1, \ldots, x_n, x)$ and $J(x_1, \ldots, x_n)$ which uniformly serve as a pairing system on $\text{rat}(x_1, \ldots, x_n)$. The range of P will be entirely contained in ω. In the fap asserted to exist by the hypothesis of the theorem, replace the function symbols P, K, and J by subroutines to calculate these functions. We must now claim that the new fap computes exactly the same function as the old, but this is trivial. Imagine a given calculation of $f(x_1, \ldots, x_n)$ for some particular inputs. Extend the above computable P, K, and J defined on $\text{rat}(x_1, \ldots, x_n)$ to a total pairing system. Now in both the given fap and this derived one the only points that arise are in $\text{rat}(x_1, \ldots, x_n)$; therefore both faps give the same calculation.

3. RECURSIVELY ENUMERABLE SETS

Recall the definition immediately preceding Theorem 3; a set is recursively enumerable if it is the domain of a computable function. In this section, we study the elementary structure of r.e. sets. We have already discussed two questions about this structure, the existence of universal r.e. sets, and the question as to whether or not an r.e. set always has an r.e. complement. Our main concern is the theorems of ordinary recursion theory. What are the requirements on M necessary for each, and which ones imply or do not imply others? For these purposes, we are only willing to consider those M strong enough to have even a semblance of a recursion theory, namely those M with a nontrivial relation (see Theorem 4).

We begin with a slight reformulation of theorem 3 for the field $\mathbb{R}$.

Theorem 21. *Over $\mathbb{R}$, a relation is r.e. iff it is a countable union of sets basic semialgebraic with parameters all from the same field of finite transcendence degree.*

Proof. Given a real number, we can read off its binary digits recursively, i.e. there is a computable function $d(n, x)$ such that if n is an integer, d, is the nth digit of x. Therefore a single real may be used to encode an arbitrary set of integers.

Now suppose we have a relation in the variables $x_1, \ldots, x_n$ defined as a union of quantifier free formulas $\varphi(a_{i,1}, \ldots, a_{i,k(i)}, x_1, \ldots, x_n)$ where all the $a_{i,j}$ are in the algebraic closure of $b_1, \ldots, b_m$. For each $a_{i,j}$, we can find a quantifier free $\varphi_{i,j}$ with $a_{i,j}$ the unique real y satisfying $\varphi_{i,j}(b_1, \ldots, b_m, y)$. (Just say that y is the solution to a certain polynomial and that it lies in a certain rational interval.) Thus our original relation is the union of the relations defined by the formulas

$$\exists y_1, \ldots, y_{k(i)}(\varphi_i(y_1, \ldots, y_{k(i)}, x_1) \wedge \varphi_{i,1}(b_1, \ldots, b_m, y_1)$$
$$\wedge \varphi_{i,k(i)}(b_1, \ldots, b_m, y_{k(i)})).$$

However, by Tarski's quantifier elimination theorem for real closed fields, this is equivalent to a quantifier free formula with the same free variables. Let a be a single real whose nth binary digit is one iff n is the Gödel number of one of these quantifier free formulas. Now consider the fap with input $x_1, \ldots, x_n$ which searches for an n such that $d(n, a) = 1$ and the formula with Gödel number n is true of $x_1, \ldots, x_n$.

For the converse, Theorem 3 applied to the reals does the trick.

Theorem 22. *A countable subset of $\mathbb{R}$ is r.e. iff it is contained in the algebraic closure of a finite set.*

Proof. If X is contained in the algebraic closure of $Q(a_1, \ldots, a_n)$, consider the set of pairs $\langle p, \langle r, s \rangle \rangle$ such that p is a polynomial and there is a unique solution to $p(a_1, \ldots, a_n, x)$ in the rational interval (r, s) and that solution is in X. Then X is r.e. in any code for this set as defined in the first paragraph of the previous proof. To be more specific, let a be the real whose nth binary digit is 1 iff n is the Gödel number of one of the above pairs, $\langle p, \langle r, s \rangle \rangle$. Let $g(x, n)$ be a fap which gives the value 1 if x satisfies the condition with Gödel number n and 0 otherwise. Let $d(n, a)$ be the fap definable function which reads off the nth digit of a. Then the program $h(x)$ with parameter a which searches for an n with $d(n, a) = 1 \wedge g(x, n) = 1$ has domain X.

Conversely suppose X is an r.e. set containing an element not algebraic in its parameters. That element must satisfy a conjunction of equalities and inequalities which puts it into X. As above, since the element is not algebraic, there can be no equalities, therefore X has a nonempty interior.

Theorem 23. *Over $\mathbb{C}$, the set of integers does not have an r.e. complement.*

Proof. Over $\mathbb{C}$, one-variable basic semialgebraic sets are either finite or cofinite. Therefore any uncountable r.e. set is cofinite.

We have just seen that the recursion theory over $\mathbb{C}$ is very weak, we cannot define any nontrivial uncountable sets. The situation is even worse than this. Over $\mathbb{R}$ with $<$ any set of integers can be coded by a single real. For $\mathbb{C}$ nothing can be coded that is not already r.e. This is the content of the next theorem.

Theorem 24. *If K is any subfield of $\mathbb{C}$ and A is any relation r.e. over $\mathbb{C}$, the restriction of A to K is r.e. over K. In other words, complex parameters are not very useful.*

Proof. Let A be a relation on $\mathbb{C}^n$ which is r.e. over $\mathbb{C}$. We claim that there is an r.e. relation B using parameters only from K which has the same restriction to K as does A. This claim obviously implies the theorem . The proof of the claim is by induction on the number of parameters. If A has $k + 1$ parameters not in K, we show how to define a B with k such parameters and the same restriction to K.

From the eds definition of A we have an effective enumeration of formulas $\varphi(a_1, \ldots, a_{k+1}, x_1, \ldots, x_n)$ which define A. For notational simplicity, let us assume that $k = 0$ and $n = 1$. Each φ_i is a conjunction of equations and inequations. Suppose $x \in K$ and p is a polynomial and $p(a, x) = 0$ is true. Then a is algebraic over K and $p(b, x) = 0$ is also true whenever b is an algebraic conjugate of a. (Since $K[a]$ is isomorphic to $K[b]$.) Let q be the minimal polynomial of a over K. Then

$$p(a, x) = 0 \quad \text{iff} \quad \exists y (q(y) = 0 \wedge p(y, x) = 0).$$

Thus, for each i, there is polynomial q_i whose Gödel number can be calculated effectively from the Gödel number of φ_i such that $\varphi_i(a, x)$ is equivalent to $\exists y (q_i(y) = 0 \wedge \varphi_i(y, x))$ whenever x is in K. By the quantifier elimination

theorem for algebraically closed fields, there is a quantifier free $\gamma_i(x)$ equivalent to this existential statement. Make a new eds using the γ_i.

Many of the elementary theorems of recursion theory are just not true when applied to fields.

Theorem 25. *There is a real algebraic extension of Q having total computable function whose range is not r.e.*

Proof. Let X be an awful set of primes (i.e. not arithmetically definable). Let K be $Q[\{p^{1/2} : p \in X\}]$. Then a prime has a square root in K iff it is in X. This follows at once from an easy Galois argument applied to the finite degree approximations to K. In this model, the square function does not have an r.e. range. For if the set of squares of K were r.e., the set of primes with square roots would also be r.e. But any set of integers r.e. over this field is real live r.e. (over N) using an oracle for the field operations. However, the field $Q[p_1^{1/2}, \ldots, p_k^{1/2}]$ is obviously a recursive field for any finite sequence of primes.

Theorem 26. *If the equality relation is r.e., any computable function has a r.e. graph.*

Proof. Suppose the equality relation is the domain of the function $\text{equal}(x, y)$. Given the definition of $f(x)$, define a new function $F(x, y)$ as follows: proceed just as in f except when you are about to give an output, in that case proceed to calculate $\text{equal}(y, z)$ where z is the output variable for f.

Thus we see that Theorem 25 was actually a counterexample to another basic theorem of recursion theory, that the projection of an r.e. relation is r.e. We can formulate a condition on M equivalent to this basic fact.

Theorem 27. *If M is ω-rich, the projection of an r.e. set is always r.e. iff M satisfies generalized quantifier elimination; i.e. there is a parameter list $a_1, \ldots, a_n$ from M and a uniform procedure to associate with each quantifier free $\varphi(x, y)$ the Gödel number of an r.e. (over N) set of $\varphi_i(v_1, \ldots, v_n, x)$ with $\exists y \varphi(x, y)$ equivalent to the disjunction of the $\varphi(a_1, \ldots, a_n, x)$.*

Proof. This condition is obviously sufficient. To show that it is necessary, consider the r.e. relation given by $\langle n, x, y \rangle \in A$ iff there is a φ such that $\varphi(x, y)$ holds and n is the Gödel number of φ. If $\exists y A$ is r.e. there is an r.e. (over N) sequence φ defining it in the sense of Theorem 3. If N_φ is the Gödel number of φ, the formulas $\varphi_i(N_\varphi, x)$ satisfy the condition.

Theorem 28. *Over any real closed or algebraically closed field, every projection of an r.e. set is r.e.*

Proof. Both these classes have actual quantifier elimination.

Theorem 29. *Over any finitely generated field, every projection of an r.e. set is r.e.*

Proof. Replace $\varphi(x, y)$ by $\{\varphi(x, p(x)) : p \in Q[X]\}$.

Another theorem of an elementary recursion theory that does not generalize is that a function is computable iff it has an r.e. graph.

Theorem 30. *Over* $\mathbb{R}$, *the square root function is not computable.*

Proof. Suppose the function $x^{1/2}$ is definable by a countable set of clauses of the form, $x^{1/2} = t_i(x)$ if $\varphi_i(x)$, where each t_i is a rational function with real coefficients. Then at least one of the φ_i must be true on an uncountable set, and therefore there must be real polynomials, P_i and Q_i such that $P_i^2(x) = xQ_i^2(x)$ for uncountably many x's. This is impossible since the degree of the L.H.S. is even while the degree of the R.H.S. is odd.

Theorem 30 was also a counterexample to yet another basic theorem of recursion theory, that for any r.e. relation R there is a computable function f with the same domain such that $\exists y R(x, y)$ implies $R(x, f(x))$. This is not even true when R is the graph of a function. We can enquire, however, as to just when this property is true. As above (Theorem 20), let $\mathrm{rat}(x_1, \ldots, x_n)$ be the set of points expressible by a formal term in the variables $x_1, \ldots, x_n$.

Theorem 31. *If* M *is* ω-*rich and structural, every r.e. relation can be uniformized by a computable function iff there is a sequence* $a_1, \ldots, a_k$ *such that for every* $x_1, \ldots, x_n$ *and any quantifier free* φ, *we have*

$$\exists y \varphi(x_1, \ldots, x_n, y) \quad \textit{iff} \; \exists y \in \mathrm{rat}(x_1, \ldots, x_n, a_1, \ldots, a_k)\varphi(x_1, \ldots, x_n, y).$$

The proof of this is left to the reader. It is similar to our above proof of Theorem 27. We will content ourselves with three corollaries.

Theorem 32. *If* M *is finitely generated, every r.e. relation is uniformizable.*

Theorem 33. *There is an* M *which is not finitely generated but none the less all r.e. relations are uniformizable.*

Proof. Let M be an uncountable ω-rich model with a pairing system. Add Skolem functions to M, and then Skolem functions for the expanded language etc. Continue this procedure to infinity so that we have a model whose basic functions include Skolem functions for all formulas of the language. Many of these functions, of course, have more than one variable, replace them by functions of one variable which use the decoders to construct a finite sequence e.g. replace $f(x, y)$ by $g(x) = f(K(x), J(x))$ etc. We now have an infinite sequence $f_0(x), f_1(x), \ldots$. Make a new function $f(n, x)$ coding the whole sequence. (Let $f(y, x)$ have some conventional value when $y \notin \omega$.) Add this function to M.

We must show that $\mathrm{rat}(x_1, \ldots, x_n)$ is always a Σ_1-elementary submodel of $\langle M, f \rangle$. If we look at just those formulas in which the first argument to f is always an integer constant this is clear. However, any quantifier free formula is equivalent to an infinite disjunction of these. $\varphi(\cdots f(t, x) \cdots)$ is equivalent to the disjunction of the $t = n \wedge \varphi(\cdots f(n, x) \cdots)$ along with $t \notin \omega \wedge \varphi(\ldots a, \ldots)$ where a is the conventional value of f. Thus if $\exists y \varphi$ is true, there will be a y of the form $f(n, x)$ making it true where x is a finite sequence built up with pairing function P from the parameters of φ.

Theorem 34. *There is an* ω-*rich, structural model with equality and a pairing function which has a nonuniformizable r.e. set.*

In this model, the projection of every r.e. relation is r.e.

Proof. Let K be the algebraic reals with $<$. Every finitely generated subfield has an unsolvable polynomial with rational coefficients. Yet the field does have a pairing function. See Theorem 18. Note that this counterexample is a real closed field, therefore it has the property that the projection of any r.e. set is r.e. See Theorem 28.

Theorem 35. *Over* $\mathbb{R}$, *if a function* f *has an r.e. graph, there is a computable function* $F(x, \varepsilon)$ *such that for all positive* ε, $|f(x) - F(x, \varepsilon)| < \varepsilon$.

Proof. Let the graph of f be defined by the disjunction of the quantifier free, $\varphi_i(x, y)$. To calculate $F(x, e)$, enumerate all paris i, $\langle a, b \rangle$ such that i is an integer and a, b are rationals with $a < b$ and $b - a < e$. Carry out this enumeration until a pair is found such that $\mathbb{R} \vDash \exists y (\varphi_i(x, y) \land a < y < b)$. Recall Tarski's quantifier elimination argument for real closed fields which says that this is indeed a recursive condition. Return a as the value of F.

Theorem 36. *The intersection and union of two r.e. sets is r.e.*

Proof. For intersection, consider an eds $\{\varphi_i : i \in \omega\}$ for A and an eds $\{\gamma_j : j \in w\}$ for B, consider the $\varphi_i \land \gamma_j$. For unions just take the union of the two eds.

Theorem 37. *If the equality relation is r.e., the class of ranges of computable functions is closed under intersection. If* M *has a nontrivial relation, it is closed under unions.*

Proof. For intersections, given functions $f(x)$ and $g(x)$, define a new function $\text{int}(x, y)$ as follows:

calculate $f(x)$, then calculate $g(y)$, then $\text{equal}(f(x), g(y))$. For unions take $\text{union}(x, y) = $ if $r(x)$ then $f(y)$ else $g(y)$.

Theorem 38. *If* M *is* ω-*rich and structural, then every nonempty r.e. set is the image of* ω *under a computable function defined on all of* ω *iff* M *is finitely generated.*

Proof. Left to reader.

Theorem 39. *If* M *is finitely generated,* ω-*rich, and structural, every function with an r.e. graph is computable.*

Proof. Left to reader.

Problem. Does the converse to Theorem 38 hold?

REFERENCES

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

C. C. Chang and H. J. Keisler, *Model theory*, North-Holland, Amsterdam,

Harvey Friedman, *Algorithmic procedures, generalized Turing algorithms and elementary recursion theories*, Logic Colloquium '69, (R. O. Gandy and C. E. M. Yates, eds.), North-Holland, 1971, pp. 361–390.

A. I. Kfoury, *The pebble game and logics of programs*, Harvey Friedman's Research on the Foundations of Mathematics, (L. Harrington et al., eds.), Elsevier Science Publishers, 1985, pp. 317–329.

Donald E. Knuth, *The art of computer programming*, vol. 2, Addison-Wesley, Menlo Park, Calif., 1969.

R. Mansfield, *A complete axiomatization of computer arithmetic*, Math. Comp. **42** (1984), pp, 623–635.

＿＿＿, *The irrationals are not recursively enumerable*, Proc. Amer. Math. Soc. **110** (1990), 495–497.

Hartley Rogers, Jr., *The theory of recursive functions and effective computability*, Mc-Graw Hill, New York, 1967.

J. C. Sheperdson, *Algorithmic procedures, generalized Turing algorithms, and elementary recursion theory*, Harvey Friedman's Research on the Foundations of Mathematics, (L. Harrington et al., eds.), Elsevier Science Publishers, 1985, pp. 285–308.

A. Tarski and J. C. C. McKinsey, *A decision procedure for elementary algebra and geometry*, (2nd ed.), Univ. of California Press, Berkeley, Calif., 1948.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, STATE COLLEGE, PENN-SYLVANIA 16802
   E-mail address: melvin@euler.psu.edu