The Gödel Incompleteness Theorem and Decidability over a Ring

Lenore Blum and Steve Smale
TR-90-036
August 1, 1990

Abstract

Gödel showed in 1931 that given any reasonable (consistent and effective) theory of arithmetic, there are true assertions about the natural numbers that are not theorems in that theory. This "incompleteness theorem" ended Hilbert's program of formalizing mathematics and is rightfully regarded as the most important result in the foundations of mathematics in this century. Now the concept of *undecidability* of a set plays an important role in understanding Gödel's work. On the other hand, the question of the undecidability of the Mandelbrot set has been raised by Roger Penrose. Penrose acknowledges the difficulty of formulating his question because "decidability" has customarily only dealt with countable sets, not sets of real or complex numbers.

Here we give an exposition of Gödel's result in an algebraic setting and also a formulation (and essentially an answer) to Penrose's problem. The notions of *computability* and *decidability over a ring R* underly our point of view. Gödel's Theorem follow from the Main Theorem: There is a definable undecidable set over **Z**. By way of contrast, Tarski's Theorem asserts that every definable set over the reals or any real closed field R is decidable over R. We show a converse to this result, namely: Any sufficiently infinite ordered field with this latter property is necessarily real closed.

The Gödel Incompleteness Theorem and Decidability over a Ring[1]

Lenore Blum and Steve Smale

Section 1 Introduction

Gödel showed [Gödel, 1931] that given any reasonable (consistent and effective) theory of arithmetic, there are true assertions about the natural numbers that are not theorems in that theory.[2] This "incompleteness theorem" ended Hilbert's program of formalizing mathematics and is rightfully regarded as the most important result in the foundations of mathematics in this century.

Now the concept of *undecidability* of a set plays an important role in understanding Gödel's work. On the other hand, the question of the undecidability of the Mandelbrot set has been raised by Roger Penrose [Penrose, 1989]. Penrose acknowledges the difficulty of formulating his question because "decidability" has customarily only dealt with countable sets, not sets of real or complex numbers.

Here we give an exposition of Gödel's result for mathematicians without background in logic and also a formulation (and essentially an answer) to Penrose's problem. The notions of *computability* and *decidability over a ring R* as developed in [BSS][3] underly our point of view.

A generalization of Gödel's theorem and various intermediate assertions may be formulated over an arbitrary ring or field R. If R=$\mathbf{Z}$, the integers, the specialization is essentially the original theorem. Our proof of it is valid in the case R is an algebraic number ring (i.e. a finite algebraic extension ring of $\mathbf{Z}$) or number field (a finite algebraic extension field of $\mathbf{Q}$). Using R=$\mathbf{R}$, the real numbers, the undecidability of the Mandelbrot set is dealt with.

Suppose that R is a commutative ring or field (perhaps ordered), which contains $\mathbf{Z}$, and R^k is the cartesian product, viewed as a k-dimensional vector space (or module) over R. A set $S \subset R^k$ is *decidable over R* if its *characteristic function*

$$\chi : R^k \to \{0,1\}, \quad \chi(\mathbf{x}) = 1 \; if \; and \; only \; if \; \mathbf{x} \in S,$$

is *computable over R* in the sense of [BSS].

A set $S \subset R^k$ is *definable over R* if it is of the form

$$S = \left\{(\mathbf{y_1}, \ldots, \mathbf{y_k}) \in R^k \mid \exists x_1 \forall x_2 \exists x_3 \cdots \forall x_n \; such \; that \; (\mathbf{y_1}, \ldots, \mathbf{y_k}, x_1, \ldots, x_n) \in Y\right\}$$

[1] Partially supported by NSF grants and (the first author) by the Letts-Villard Chair at Mills College.

[2] This formulation of Gödel's Theorem, with *consistency* in place of *ω-consistency*, is due to [Rosser, 1936].

[3] We use [BSS] to denote our Main Reference [Blum, Shub, Smale, 1989].

for some *constructible* (or *semi-algebraic*) set Y in R^{k+n}.[4]

A natural question is:

[D] Is a definable set over R necessarily decidable over R?

If R=**Z**, the answer is "No," and this is the backbone of the Gödel Incompleteness Theorem. This may be interpreted (Section 2) as asserting there is a "polynomially defined" set of assertions over **Z**,[5] and that there is no way of deciding which are the true ones. The proof is in Sections 3 and 4 below, the Gödel Theorem is proved in Section 5.

If R=**R**, the real numbers the answer is "Yes." Tarski's fundamental decidability result [Tarski, 1951] for the case of the reals may be interpreted as this assertion.

These results extend to certain other rings and fields as well.

Julia Robinson extended Gödel's result. Robinson did not have the notion of decidability over a ring and put her theorems in the context of "decidable rings" (or fields). A ring R is *decidable* if the set of "first order" sentences true in R is decidable in the traditional sense (of Turing, et. al., or decidable over **Z** in our sense). Her way of showing a certain ring R is undecidable is to reduce the problem to Gödel's Theorem by defining **Z** in R. We use her algebraic results [Robinson, 1959, 1962, 1965] on the definability of **Z** to answer **[D]** negatively for finite extensions of **Z** and **Q**.

On the positive side of **[D]**, Tarski's work was done in the generality of real closed fields. His work also implies that **[D]** has an affirmative answer for algebraically closed fields. Tarski's arguments are a developed form of elimination theory, which in a sharp complexity theoretic form can be seen in [Renegar, 1989].

What about the answer to **[D]** for the remaining rings and field? Let us say that R has *Property D*, just in case every definable set over R is decidable over R.

We give some results (Section 6) in the direction of showing Tarski's examples exhausts all fields (sufficiently infinite) satisfying Property D. Here we follow [MacIntyre, 1971], and [MacIntyre, McKenna, van den Dries, 1983]. Indeed, our results could be considered an infinitary version of theirs. Note that Property D, as stated, is a non-uniform property. That is, each decidable set might have a different decision procedure. However, an immediate corollary to these results (for sufficiently infinite fields), is the uniformity of Property D once it is satisfied.

We would like to acknowledge helpful insights gleamed from conversations with Michel Herman, Adrien Douady and others concerning the mathematics underlying the undecidability of the Mandelbrot set. The first author would like to acknowledge helpful discussions with George Bergman, Lou van den Dries, Leo Harrington and Simon Kochen; the personal influence of Julia Robinson is deeply felt.

[Friedman, Mansfield, 1988] and [Michaux, 1990] have results related to what we are doing here.

---

[4] That is, Y is a finite union of finite intersections of sets defined by polynomial equations and inequations (and inequalities, if R has an order) over R. (See Section 2.)

[5] By this we mean a set of sentences of the form $\{\exists x_1 \forall x_2 \exists x_3 \cdots \forall x_n P(\mathbf{z}, x_1, \cdots x_n) = 0\}_{\mathbf{z} \in \mathbf{Z}^k}$ where P is some polynomial over **Z**.

Section 2 Background

We give here some background on decidability and definability over a ring R. Then we state our Main Theorem.

Let R be a commutative ring or field, which contains $\mathbf{Z}$, and for the moment is ordered. Let R^k be the direct sum of R with itself k times. If $k = \infty$, then $\mathbf{x} \in R^k$ is a vector $(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}, ...)$ with $\mathbf{x_n} = 0$ for sufficiently large n. In this section, we may take k finite.

The notion of a *computable function over R*,

$$\varphi_M : \Omega_M \to R^l,$$

is taken from [BSS] where $\Omega_M \subset R^k$, the domain of φ_M, is the *halting set* of a machine M over R.

A set $S \subset R^k$, is called *decidable over R* if its characteristic function is computable over R. We note that a set is decidable over R if and only if both it and its complement are halting sets (over R). Halting sets may be naturally thought of as "semi-decidable" sets.

If $Y \subset R^k$ and $S \subset Y$, say that S is *decidable relative to Y over R* if the restriction of χ to Y, $\chi|_Y$, equals $\varphi|_Y$ for some φ computable over R. (We might say that the set of *admissible inputs* of the corresponding machine is Y.) In that case, if $Y' \subset Y$, then $S \cap Y'$ is decidable relative to Y' over R.

Next a very brief review of definability over R is given. First suppose $R = \mathbf{Z}$.

A subset S of $\mathbf{Z^k}$ is called *definable* over $\mathbf{Z}$ if there is a polynomial P in $n+k$ variables with integer coefficients such that

$$S = \left\{ \mathbf{y} = (\mathbf{y_1}, \ldots, \mathbf{y_k}) \in \mathbf{Z^k} | \exists x_1 \forall x_2 \exists x_3 ... \forall x_n P(\mathbf{y_1}, \ldots, \mathbf{y_k}, x_1, ..., x_n) = 0 \right\}.$$

The "defining" *formula* $\exists x_1 \forall x_2 \exists x_3 ... \forall x_n P(y_1, \ldots y_k, x_1, ..., x_n) = 0$ contains an alternating sequence of quantifiers which could begin or end with either $\exists$ or $\forall$. In this expression, $y_1, \ldots, y_k$ are called *free variables* (and $x_1, \ldots, x_n$ *bound variables*). If we replace each free variable y_i by an integer $\mathbf{y_i}$, the expression becomes a *sentence* perhaps true, perhaps false in $\mathbf{Z}$. (If there are no free variables, the formula is already a sentence.)

Note, we have been using bold letters to denote elements (constants) or vectors and non-bold letters to denote variables. Henceforth in the sequel we shall use non-bold letters for both; the intended meaning should be clear from context.

Quantifiers $\exists z$ or $\forall z$ with a new variable z may be added at any place in a formula without changing the set S. Thus the assumption of an alternating set of quantifiers places no restriction on the notion of definability. Moreover, "*not* $\forall$" is *logically equivalent* to " $\exists$ *not.*" Similarly, "*not* $\exists$" is equivalent to " $\forall$ *not.*" Thus negations of formulas could be incorporated using

$$P(y, x_1, ..., x_n) \neq 0.$$

But over $\mathbf{Z}$, we have $P \neq 0$ *if and only if*

$$\exists z_1 \exists z_2 \exists z_3 \exists z_4 \left(\left(P - \left(1 + z_1^2 + z_2^2 + z_3^2 + z_4^2 \right) \right) \left(P + \left(1 + z_1^2 + z_2^2 + z_3^2 + z_4^2 \right) \right) = 0 \right).$$

This assertion follows from the next Lemma. Suppose R is an ordered ring or field. Then,

Lemma. If $P(x)$ and $Q(x)$ are polynomials in n variables over R, and $x \in R^n$ then:

(a) $P(x) \neq 0$ *if and only if* $-P(x) > 0$ *or* $P(x) > 0$.

(b) *If* $R = \mathbf{Z}$:

$$P(x) > 0 \text{ if and only if } \exists z_1, \ldots, z_4 \in \mathbf{Z} \text{ such that } P(x) = \sum_{i=1}^{4} z_i^2 + 1 \quad (Lagrange).$$

(c) $P(x) = 0$ **or** $Q(x) = 0$ *if and only if* $P(x)Q(x) = 0$.

So over $\mathbf{Z}$, negations of formulas are equivalent to formulas of the specified type.[6] In the sequel, the following equivalences will also be useful:

(d) $P(x) = 0$ **and** $Q(x) = 0$ *if and only if* $P^2(x) + Q^2(x) = 0$,

(e) $Q(x) \not> 0$ *if and only if* $-Q(x) > 0$ *or* $Q(x) = 0$.

Now for definability over a general ordered ring or field R, we must modify our definition to incorporate semi-algebraic sets:

A *basic semi-algebraic* set $X \subset R^n$ *(over R)* is defined as the set of $x = (x_1, \ldots, x_n)$ satisfying *basic conditions* of the type

$$P(x_1, \ldots, x_n) = 0$$
$$Q_i(x_1, \ldots, x_n) > 0, \; i = 1, \ldots, m,$$

where P *and* Q_i are polynomials over R. A set $X \subset R^n$ is *semi-algebraic (over R)* if it is generated by basic semi-algebraic sets using a finite process taking unions (i.e. "*or*'s" of basic conditions), intersections ("*and*'s"), and complements ("*not*'s").

From the above Lemma, and by adding and substituting new variables, and by de Morgan's laws, it easily follows:

Proposition 1. Every semi-algebraic set $X \subset R^n$ can be expressed as a finite union of basic semi-algebraic sets (and conversely).

Intersections are eliminated using (d) and complements using (a) and (e).

Definition: A set $S \subset R^k$ is *definable over R* if there exists a semi-algebraic set $X \subset R^k \times R^n$ such that

$$S = \{(y_1, \ldots, y_k) \mid \exists x_1 \forall x_2 \exists x_3 \cdots \forall x_n \text{ such that } (y_1, \ldots, y_k, x_1, \ldots, x_n) \in X\}$$

Note that the image of a definable set in $R^k \times R^l$ under the projection $R^k \times R^l \to R^k$ is a definable set. Indeed, definable sets over R are precisely those sets that are "derivable" from semi-algebraic sets by means of a finite sequence of projections and complements.

A *(defining) formula over R* for the above S is $\exists x_1 \forall x_2 \exists x_3 \ldots \forall x_k \Phi(y_1, \ldots, y_k, x_1, \ldots, x_n)$ where $\Phi(y_1, \ldots, y_k, x_1, \ldots, x_n)$ is a finite *disjunction* of *basic semi-algebraic formulas*, i.e. Φ is

$$\left(P^1 = 0 \& Q_1^1 > 0 \& \ldots \& Q_{m_1}^1 > 0\right) \text{ or} \cdots \text{or } \left(P^l = 0 \& Q_1^l > 0 \& \ldots \& Q_{m_l}^l > 0\right),$$

[6] Note here, and in the sequel, we are implicitly moving quantifiers to the front of formulas, changing variables as necessary to avoid clashes and to maintain logical equivalence.

the P's and Q's being polynomials over R (in the variables $y_1, \ldots, y_k, x_1, \ldots, x_n$) that describe the basic semi-algebraic pieces of X in a union as given by Proposition 1. Definitions for *free/bound variables* and *sentences over R* can be given as above for $\mathbf{Z}$.

We remark that for ordered rings, our notion of definability over R is *equivalent* to the classical notion of definability given in "first order" logic over the language containing the mathematical primitives $+, \times, =$ as well as $>$ *and* constants from R. That is, the sets defined are the same.

For consistency we need

Proposition 2. If $R = \mathbf{Z}$, our two notions of definable coincide.

But this follows from Proposition 1 and the Lemma since we can eliminate occurrences of > using (b), "and's" using (d), and "or's" using (c).

Both the concepts of decidability and definability over a ring can be developed without >, retaining $\neq 0$. For decidability one uses machines with branch nodes of which divide according to $h(x) = 0$ versus $h(x) \neq 0$. For definability, one omits all constructions requiring >. Semi-algebraic sets are replaced by what are usually called *constructible* sets, finite unions of sets satisfying *basic* conditions of the type

$$P_i(x_1, \ldots, x_n) = 0, \; i = 1, \ldots, k,$$
$$Q(x_1, \ldots, x_n) \neq 0.$$

Similarly, a *basic constructible formula* is of the type $P_1 = 0 \& \cdots \& P_k = 0 \& Q \neq 0$ and a formula over R is a finite disjunction of basic ones.

The following results apply to rings and field with an order, or without.

Main Theorem. Supposes R is a ring (of "algebraic integers") which is a finite extension of $\mathbf{Z}$, or a field which is a finite extension of the rationals $\mathbf{Q}$. Suppose $k < \infty$. Then there is a set $S \subset R^k$ which is definable over R, yet not decidable over R.

The Main Theorem may be interpreted as saying that there is a reasonable family of sentences over R, but there is no way of deciding which are true in R. It is an immediate consequence of Propositions A and B below.

Suppose R is as in the Main Theorem. Then:

Proposition A. For $k \leq \infty$, there is a halting set $S \subset R^k$ (of a machine) over R which is not decidable over R (i.e. S is a "semi-decidable" undecidable set over R).

Proposition A will be proved in Section 3.

Proposition B. For $k < \infty$, any halting set $S \subset R^k$ over R is definable over R.

Proposition B will be proved in Section 4.

Remark. We remark that over the reals **R**, Proposition A is true (see [BSS]). But by [Tarski, 1959], the Main Theorem must fail over **R** for each $k < \infty$, and thus so must Proposition B. See Section 6 for more discussion and results along these lines.

Section 3 Decidability: Proof of Proposition A

Proposition A is proved in part in [BSS] (see Proposition 2 below). Friedman and Mansfield have a complete proof [Friedman, Mansfield, 1988]. But to keep our paper accessible to non-logicians, we indicate in this section a proof of Proposition A.

Say that subsets $S_1 \subset R^k$, $S_2 \subset R^l$ are *computably isomorphic* over R if there is a bijection $f : S_1 \to S_2$ such that f, f^{-1} are computable over R.

Proposition 1. If R is as in the Main Theorem, there is a computable isomorphism

$$f : R \to \mathbf{Z^n} \subset R^n$$

over R where n is the degree of the extension.

Proof. Let $R = \mathbf{Z}[w_1, \ldots, w_n]$ and for $x = \sum_{i=1}^{n} x_i w_i$ let $f(x) = (x_1, \ldots, x_n)$. Clearly f^{-1} is computable over R. Now list the elements of $\mathbf{Z^n}$ with norm non-decreasing. A comparison machine using this list shows that f is computable.

Similarly, if R is a finite extension of $\mathbf{Q}$ of degree n, then R is computably isomorphic to $\mathbf{Q^n}$ over R. To finish the proof note that if R is any extension field of $\mathbf{Q}$, then there is a bijection $g : \mathbf{Z} \to \mathbf{Q}$ with g, g^{-1} computable over R.

The next step in our development (see [BSS]) is to associate to each machine M over a ring R, a point $\varphi(M) \in R^\infty$, its "code." This substitutes for the usual Gödel code which uses prime number factorization of positive integers. One can then construct a universal machine U which on input $(\varphi(M), x)$, $x \in U_M$, outputs $\varphi_M(x)$ and does not halt on other inputs. Then

Proposition 2. For any ring or field R, the halting set $\Omega_U \subset R^\infty$ is not decidable over R.

The proof is an adaptation of the Cantor diagonal argument.

Proposition 3. Suppose R is as in the Main Theorem. Then for any $k \leq \infty$, R and R^k are computably isomorphic over R.

Proof. The case R=**Z** is done using the Cantor pairing function. (See e.g. [Davis, 1982].) Next use Proposition 1 to obtain a computable isomorphism as the composition $R \to \mathbf{Z^n} \to (\mathbf{Z^n})^k \to R^k$.

Propositions 2 and 3 now combine to yield Proposition A.

As remarked earlier, it is shown in [BSS] that Proposition A holds for R=**R** (although Proposition 3 does not).

Problem. Find k, R such that Proposition A fails, i.e. such that every halting set $S \subset R^k$ is decidable over R. (See also [Friedman, Mansfield, 1988].)

Section 4 Definability: Proof of Proposition B

Suppose $S \subset R^k$ and $f : S \to R^l$, $k, l < \infty$. We say f is *definable over R* if the *graph of* $f = \{(x, f(x)) \mid x \in S\}$ is definable over R. Note that if f is definable over R then both S and $f(S)$ are definable over R, and if in addition f is a bijection then f^{-1} is definable over R.

Remark. For the proof of Proposition B it suffices to consider finite dimensional machines. (See footnote p. 28, [BSS].)

So suppose M is a finite dimensional machine with *input space* $\overline{I}$, *output space* $\overline{O}$, and *state space* $\overline{S}$, each of the form R^k, for some $k < \infty$ (although not necessarily the same k).

Recall [BSS] that the *computing endomorphism* of M is a map $H : \overline{N} \times \overline{S} \to \overline{N} \times \overline{S}$ defined by the pair (*next node, next state*). Here $\overline{N} = \{1, \ldots, N\}$ is the set of *node* labels (1 being the label of the *input node*, N of the *output node*), and M is assumed to be in *normal form*. From [BSS] it is clear that H is definable over R.

The *halting register equations* associated to M are given by (1), (2), and (3) as follows:

(1) $z_0 = (1, I(y))$, where $I : \overline{I} \to \overline{S}$ is the *input map*, a polynomial map.
(2) $H(z_{i-1}) = z_i$, $i = 1, 2, \ldots, T$, $z_i \in \overline{N} \times \overline{S}$.
(3) $z_T = (N, x)$, some $x \in \overline{S}$.

The *halting set* $\Omega_M \subset \overline{I}$ may be described by

$$\Omega_M = \left\{ y \in \overline{I} \mid \exists T \in \mathbf{Z}^+, z_0, \ldots, z_T \in R^{k+1},\ x \in R^k \ \textit{such that (1), (2), and (3) are satisfied} \right\}.$$

However, this expression for Ω_M does not make Ω_M definable over R because the number of equations and variables is not a fixed finite number. It depends on T. So we need more.

Generalized Gödel Sequencing Lemma. Let R be as in the Main Theorem and $k \leq \infty$. There is a map $\sigma : \mathrm{N} \times R^k \to R^k$ such that

(*a*) given $a_0, \ldots, a_m \in R^k$, $\exists u \in R^k$ such that $\sigma(i, u) = a_i$, $i = 0, \ldots, m$, and
(*b*) *if* $k < \infty$, σ is definable over R.

We now combine the register equations of a given finite dimensional machine M as above with the function σ of the Gödel lemma to show that Ω_M is definable over R.

Let F(y) denote the following "formula.":

$$\exists T \in \mathbf{Z}^+ \exists u \exists x \ \forall i \in \mathbf{Z} \ [\textbf{If } 0 < i \leq T \textbf{ then}$$
$$\sigma(0, u) = (1, I(y)),\ H(\sigma(i-1, u)) = \sigma(i, u),\ \textit{and}\ \sigma(T, u) = (N, x)].$$

Here R^k of the Gödel Sequencing Lemma is identified with $R \times \overline{S}$.

Now on the one hand, $\Omega_M = \{y \mid F(y)$ *is true in* $R\}$. This follows from the properties of the register equations and of $\sigma(i,u)$ of the Gödel lemma. On the other hand, the above expression for *F(y)*, and the definability of H and σ, and $\mathbf{Z}$ (also $\mathbf{Z}^+$and $\mathbf{N}$) in R [Robinson, 1959, 1961, 1965], gives us the definability required in Proposition B.[7]

It remains to consider the Gödel lemma.

First observe that if the Gödel lemma is true for k=1, then it is true for general k. This can be seen as follows. Suppose σ is the map of the Gödel lemma for k=1. Then let $\sigma_k : \mathbf{N} \times R^k \to R^k$ be defined by

$$\sigma_k(i,u) = (\sigma(i,u_1), \sigma(i,u_2), \ldots) \text{ where } \mathrm{u} = (\mathrm{u}_1, \mathrm{u}_2, \ldots).$$

Now let k=1. For R=**Z**, we have the original Gödel lemma [Gödel, 1931]] which is derived from the Chinese Remainder Theorem. The general case now follows by noting the isomorphisms given in the proofs of Proposition 1 and Proposition 3 in Section 3 with $k < \infty$ are definable over R.

Problem. For which commutative rings R is the following true? If **Z** is definable in R, then for each $k < \infty$, any halting set $S \subset R^k$ over R is definable over R (and conversely).

Section 5 Incompleteness

In this section, the Gödel Incompleteness Theorem is formulated and proved using the Main Theorem.

First fix a ring or field R, with or without order. Let Σ_R be the set of all *first order sentences over R*, i.e. the set of sentences in the first order language with mathematical primitives +, x , = (possibly >) and constants from R. (See for example [Cohen, 1966].)[8] The sentences over R described in Section 2 are first order sentences and can be considered in "normal form" since each first order sentence is equivalent to one of these.

One may consider Σ_R as a subset of R^∞ by an appropriate natural coding. For example, one can use pairs $(y_1, y_1'), (y_2, y_2'), \ldots$ where either y_i or y_i' is zero. If $y_i \neq 0$, then it stands for a logical symbol, not in R normally, but thus coded by an element of R. If $y_i = 0$, then $y_i' \in R$ plays its role as an element of R, as for example the coefficient of a polynomial used in the sentence.

One may use the codings of polynomials and rational functions of [BSS] for example.

---

[7] Here we are also using the logical equivalence of the expressions "*if P then Q*" and "*not P or Q*."

[8] One can think of a "first order sentence over R" as an ordinary mathematical sentence that is made up of variables (*x,y,z,...*), quantifiers ($\forall$ meaning "for all", $\exists$ "there exists"), connectives ($\neg$ meaning "not," & "and," $\vee$ "or," $\to$ "implies"), parentheses and mathematical symbols (=, +, x, perhaps > and constants from R). A sentence (as opposed to a "formula") has no free variables, i.e. all variables must be quantified. "First order" means that quantification is over elements (e.g. "there exists an element x in R such that for all elements y in R"), not over subsets.

It makes sense to talk about the subset of sentences $T_R \subset \Sigma_R$ that are *true* in R. For each sentence $\sigma \in \Sigma_R$, either $\sigma \in T_R$ or *not* σ (the negation of σ) $\in T_R$ (*completeness*), but not both *(consistency)*. A set of *axioms* Y over R is simply a subset $Y \subset T_R$. Of course Y could be empty.

Given a set of axioms Y, we will define the *derived set* Y_D, $Y \subset Y_D \subset T_R$, via (finite application of) a set of *rules of inference*. Then Y_D is the body of *theorems*, or *theory*, generated by the axioms in Y.

The rules of inference, which are convenient for our purposes are Rules A-G, pp. 9–11 of [Cohen, 1966].

As an example we state

Rule B. If A and $A \to B$ are sentences, then so is B.

Thus, if A and $A \to B$ both belong to Y, Y_D must include B. A similar situation prevails with the other rules.

Recall [BSS] that $S \subset R^k, k \leq \infty$, is an *output set over* R if there is a computable function $\varphi : \Omega_M \to R^k$ over R with $\varphi(\Omega_M) = S$.

We have the following:

Proposition 1. If $Y \subset \Sigma_R \subset R^\infty$ is an output set over R, then so is the derived set Y_D. For the proof we use the following Lemma.

Lemma. For each finite $Y' \subset \Sigma_R$, Y'_D is a halting set over R. Indeed, there is a machine M' such that $\Omega_{M'} = \bigcup_{Y'=\{y_1,\ldots,y_n\}\subset\Sigma_R} \{(y_1,\ldots,y_n)\} \times Y'_D$.

Now suppose $\varphi(\Omega_M) = Y$. Define $F : \Omega_M^\infty \times \Sigma_R \to \Sigma_R$ via

$$F((x_1,\ldots,x_n),\sigma) = \begin{cases} \sigma \text{ if } ((\varphi(x_1),\ldots,\varphi(x_n)),\sigma) \in \Omega_{M'} \\ \text{undefined otherwise.} \end{cases}$$

Any element in Y_D is in some Y'_D for some finite $Y' \subset Y$. So by the above Lemma, the range of F is Y_D and F is computable if φ is.

Proposition 2. If R is as in the Main Theorem, a finite extension of $\mathbf{Z}$ or $\mathbf{Q}$, then the output sets and halting sets over R coincide.

One directly checks $\mathbf{Z}$ and $\mathbf{Q}$. (This is quite classic essentially). The general case follows from Proposition 1 of Section 3.

Gödel Incompleteness Theorem. Fix a ring R, a finite extension of $\mathbf{Z}$, or a finite field extension of $\mathbf{Q}$. Let $Y \subset T_R$ be any set of axioms which is a halting set over R (i.e. an "effective" set of axioms). Then Y_D, the body of theorems derived from Y, is not T_R, the true sentences of R.

If R=$\mathbf{Z}$, this is the usual Gödel Theorem.

The proof goes as follows. On the one hand, the Main Theorem asserts there is an undecidable definable set over R. This implies T_R is not *decidable* (i.e. not a decidable subset of Σ_R) over R. For if it were, then a decision procedure would restrict to decide *any* definable set $X \subset R^k$ since $x \in X$ if and only if the sentence $\varphi(x)$ is in T_R (where φ is a given defining formula for X).

On the other hand, by the above, Y_D is a halting set over R. But any complete and consistent theory T which is a halting set is necessarily decidable: Let T be the halting set of machine M. Given $\sigma \in \Sigma_R$, to decide whether or not $\sigma \in T$ input both σ and $not\,\sigma$ into M. Since one and only one of these inputs is in T, M will halt on one and only one of them, thus deciding whether or not $\sigma \in T$. Thus $Y_D \neq T_R$. Q.E.D.

Section 6 Decidability over R and Property D

In the following, R will denote $R_=$ (a commutative ring or field of characteristic 0) or $R_<$ (an ordered ring or field). L will denote the corresponding (first order) language $L_=$ with mathematical primitives $\{=, +, \times, 0, 1\}$ or $L_<$ with the additional primitive $<$. In case R is a field we will also assume the primitive $\div$ is included. Without loss of generality we may assume L has constants for each integer or each rational as appropriate. In general, if $C \subset R$, then L_C will denote the corresponding first order language allowing additional constants from C.

Now let Σ_C denote the set of *sentences* in L_C, and T_C the subset *true* in R.

Recall that in the classical setting, a ring or field R is said to be *decidable* iff $T_\emptyset$ (viewed as a subset of $\mathbf{Z}^\infty$, as in Section 5) is decidable relative to $\Sigma_\emptyset$ *over* $\mathbf{Z}$. This is what is meant for example when one says that the reals are decidable. But often one really has more. Thus, in the case of the reals, we see that $T_{\mathbf{R}_<}$ ($\subset \mathbf{R}^\infty$) is decidable over $\mathbf{R}_<$, by a machine with parameters from $\mathbf{Z}$. This follows immediately from Tarski's Theorem that $\mathbf{R}$ admits uniform elimination of quantifiers.[9]

Thus we are motivated to *extend* the notion of decidability over a ring.

Definition: R is *(strongly) decidable over* R iff T_R is decidable relative to Σ_R over R (by a machine with parameters from $\mathbf{Z}$).

If R is decidable over R, then clearly the Main Theorem fails for each $k < \infty$, i.e. R has *Property D*:

Definition: R has *Property D* iff for each $k < \infty$, any $S \subset R^k$ definable over R is also decidable over R.

Property D is a weak form of elimination of quantifiers:

---

[9] **Definition:** (Classical) R *admits elimination of quantifiers* iff for each L-formula $\varphi(x_1, \ldots, x_k)$ there is a *quantifier free* L-formula $\psi(x_1, \ldots, x_k)$ such that φ and ψ define the same subset of R^k. The elimination is *uniform* iff the map from φ to ψ is computable over $\mathbf{Z}$.

Proposition 1. If R has Property D then for each L_R-formula $\varphi_R(x_1,\ldots,x_k)$ there is a finite set $C \subset R$ and an (effectively) countable set of quantifier-free L_C-formulas $\psi_C^j(x_1,\ldots,x_k)$ such that $S = \cup S_j$, where S, S_j are the sets defined by φ_R, ψ_C^j respectively. Furthermore, we can assume without loss of generality the ψ_C^j to be basic semi-algebraic (or basic constructible) formulas.

Problem. Can we assume that C is just the set of constants occurring in φ_R? If so, we shall say R has *strong* Property D.

What is the relationship between the above notions of decidability?

Theorem. Suppose R is a field of infinite transcendence over the rationals. Then the following are equivalent:

1. R admits uniform elimination of quantifiers.
2. R is strongly decidable over R.
3. R has strong Property D.
4. a. R is an algebraically closed field in case $R = R_=$.
   b. R is a real closed field in case $R = R_<$.

And these imply:

5. R is decidable.

Furthermore, if we add the condition "R is dense in its real closure in case $R = R_<$,"[10] we can add to the above list of equivalences:

2.' R is decidable over R.

3.' R has Property D.

Remark 1. The stipulations of uniformity in 1 and effectiveness (of the countable decomposition of definable sets into semi-algebraic sets) as implied by 3 (or 3') are not necessary. These will follow from a simple analysis of the proof of the Theorem.

Remark 2. We note that in general, the notion of decidability is *weaker* than decidability over R (or Property D). For example, $\mathbf{R}_=$ is decidable, *but* since $\mathbf{R}_=$ is not algebraically closed, the Theorem implies it *cannot* be decidable over $\mathbf{R}_=$.

Proof of Theorem. It is easy to see that 1 implies 2 which implies 3; 4 implies 1 by Tarski's theorems [Tarski, 1951]. Clearly, 2 implies 5, and 2 implies 2' implies 3'. Thus we are left to show that under the appropriate hypotheses, strong Property D or Property D imply 4, i.e. the closedness conditions. Here we are inspired by, and indeed closely follow, the proof in [MacIntyre, McKenna, van den Dries, 1983] of the converse of Tarski's theorems.

---

[10] R is *dense in its real closure* $\widehat{R}$, means: For each r and $\epsilon > 0$ in $\widehat{R}$, there is an r' in R such that $|\, r - r' \,| < \epsilon$.

We start with some preliminaries. In the following, R will be a field (of characteristic 0).

Fix n. Let $Poly_R(n)$ denote the *space of* ***monic degree n polynomials in one variable*** *over* R. There is a natural *identification*, $Poly_R(n) \simeq R^n$ where

$$r_0 + \cdots + r_{n-1}z^{n-1} + z^n \leftrightarrow r = (r_0, \ldots, r_{n-1}) \in R^n.$$

Let $\mathbf{S} \subset R^n$ correspond to the set of polynomials in $Poly_R(n)$ *not solvable* in R. Note that

$$\mathbf{S} = \{r \in R^n \mid \mathbf{f}(r, z) \text{ has no root in } R\}$$

where $\mathbf{f}(r,z) = r_0 + \cdots + r_{n-1}z^{n-1} + z^n$. Thus $\mathbf{S}$ is *defined* by the L-formula $\forall z \mathbf{f}(x_0, \ldots, x_{n-1}, z) \neq 0$. So if R has Property D, then by the Proposition 1, $\mathbf{S} = \bigcup_{j \in J} S_j$ where J is countable and

$$S_j = \left\{r \in R^n \mid P_i^j(r) = 0, i = 1, \ldots, m_j,\ Q^j(r) \neq 0\right\} \text{ in case } \mathrm{R} = \mathrm{R}_{=},$$

or

$$S_j = \left\{r \in R^n \mid P^j(r) = 0, Q_i^j(r) > 0, i = 1, \ldots, m_j\right\} \text{ in case } R = R_{<}.$$

Here the P's and Q's are polynomials over $\mathbf{Q}(C)$, where C is a finite subset of R.

Proposition 2 Suppose R is of infinite transcendence. If R has an algebraic extension of degree n, then for each finitely generated subfield $K \subset R$, $\mathbf{S}$ cannot be covered by a countable union of proper algebraic varieties V_j in R^n defined over K (i.e. with $V_j = \left\{r \in R^n \mid P_i^j(r) = 0, i = 1, \ldots, k_j\right\}$, the P's being non-zero polynomials with coefficients from K).

Modulo Proposition 2, we proceed with our proof.

We first consider the case $R = R_{=}$ and suppose R has property D. Suppose R is not algebraically closed, i.e. for some n, R has an algebraic extension of degree n. So by Proposition 2 (and noting $\mathbf{S} \neq R^n$) we may assume for at least one j, $S_j = \{r \in R^n \mid Q^j(r) \neq 0\} \neq \emptyset$, and so $Q^j \not\equiv 0$. Also $S_j \subset S$. So for $r \in R^n$, *whenever* $Q^j(r) \neq 0$ *then* $\mathbf{f}(r,z) = 0$ *has no solution in* R. This contradicts

Lemma 1. For each non-zero polynomial $Q : R^n \to R$, there is an $r \in R^n$ such that $Q(r) \neq 0$ *and* $\mathbf{f}(r,z)$ has *all* its solutions in R.

To see this let $\sigma : R^n \to R^n$ be the polynomial map given by the elementary symmetric functions $\sigma_1, \sigma_2, \ldots, \sigma_n$. σ is and algebraically independent map. So for $Q \not\equiv 0$, and since R is infinite, there is $\alpha = (\alpha_1, \ldots, \alpha_n) \in R^n$ such that $Q(\sigma(\alpha)) \neq 0$. Letting $r = \sigma(\alpha)$ we have $Q(r) \neq 0$ and $\mathbf{f}(r,z) = \sigma_1(\alpha) + \sigma_2 z \cdots + \sigma_n(\alpha) z^{n-1} + z^n = \prod_{i=1}^{n} (z - \alpha_i)$. Thus, r has the required properties.

Now we consider the case $R = R_<$ and suppose R has Property D.

Suppose first that some odd degree polynomial has no solution in R. This implies, as above, that for some odd $n > 1$ and j in J, we may assume

$$S_j = \left\{ r \in R^n \mid Q_i^j(r) > 0, i = 1, \ldots, m_j \right\} \neq \emptyset.$$

Let $\psi(c, x)$ be the formula $Q_1^j(x) > 0 \,\&\, \ldots \,\&\, Q_{m_j}^j(x) > 0$ where $x = (x_0, \ldots, x_{n-1})$ and $c \in R^m$ is a vector of all the coefficients occurring in the Q's. So, there is an $r \in R^n$ such that $\psi(c, r)$ is true in R *and* for all $r \in R^n$, *whenever* $\psi(c, r)$ *is true in* R, *then* $\mathbf{f}(r,z)=0$ *has no solution in* R. Note if R has strong Property D, then without loss of generality we may assume $c \in \mathbf{Q}^{\mathbf{m}}$. Then, given the hypotheses of our Theorem, the following Lemma will yield a contradiction.

Lemma 2. Suppose R is dense in $\widehat{R}$, its real closure, or that $c \in \mathbf{Q}^{\mathbf{m}}$. Suppose $\psi(c, r)$ is true in R for some $r \in R^n$. Then there is an $r' \in R^n$ such that $\psi(c, r')$ is true in R *and* $\mathbf{f}(r', z) = 0$ is solvable in R.

Proof. Let

$$F = \begin{cases} R, if\ R\ is\ dense\ in\ \widehat{R} \\ \mathbf{Q},\ in\ case\ \ c \in \mathbf{Q}^{\mathbf{m}}. \end{cases}$$

If $\psi(c, r)$ is true in R, then $\psi(c, r)$ is true in $\widehat{R}$, and so either trivially in the first case, or by the transfer property for real closed fields in the second case, $\psi(c, r^*)$ is true in $\widehat{F}$, some $r^* \in \widehat{F}^n$. Now, $\mathbf{f}(r^*, z) = (z - \xi)\left(a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}\right)$, some $\xi, a_0, \ldots, a_{n-1} \in \widehat{F}$. For $\xi', a_0', \ldots, a_{n-1}' \in F$, define $r' \in F^n$ by $\mathbf{f}(r', z) = (z - \xi')\left(a_0' + a_1' z + \cdots + a_{n-1}' z^{n-1}\right)$. Since F is dense in $\widehat{F}$, we can choose $\xi', a_0', \ldots, a_{n-1}'$ close enough to $\xi, a_0, \ldots, a_{n-1}$ to guarantee $\psi\left(c, r'\right)$ is true in F, and hence in R.

Now suppose some positive element in R has no square root in R i.e. $T = \left\{ t \in R \mid t > 0 \, and \, \sqrt{t} \notin R \right\} \neq \emptyset$. But then, $\left\{ tr^2 \mid t \in T, r \in R, r \neq 0 \right\} \subset T$, and so if $T \neq \emptyset$ then T must have an infinite number of algebraically independent elements. (Recall the degree of transcendence of R over $\mathbf{Q}$ is infinite.) Now T is definable and hence decidable over R. Thus, T can be decomposed as in the Proposition, and so there is a $c \in R^m$ such that either all element of T are algebraic over $\mathbf{Q}(c)$, or else T contains a non-empty interval $T' = (t_1, t_2) \cap R$, *some* $t_1, t_2 \in \widehat{\mathbf{Q}(c)}$. The former is not possible as we have just seen, but neither is the latter:

For let F be as in Lemma 2, Then, $T'' = (t_1, t_2) \cap F \neq \emptyset$. But since F is dense in $\widehat{F}$, for each $t \in T''$, we can choose $s \in F$ close enough to $\sqrt{t}$ so that s^2 will be close enough to t to be in the interval (t_1, t_2), a contradiction to the definition of T.

We have thus shown modulo Proposition 2 that R is real closed.

We now proceed as follows. Let $X \subset R^n$.

Definition: We shall say X has *property A* iff for each finitely generated subfield $K \subset R$, X cannot be covered by a countable union of proper algebraic varieties V_j in R^n defined over K.

Lemma 3. Suppose R is of infinite transcendence. Then R^n has property A.

The proof is by induction on n and is similar to the proof of a related result of [Amitsur, 1956]:[11] Suppose R is an uncountable field. Then R^n cannot be covered by a countable union of proper algebraic varieties defined over R.

Remark 3. Here we cannot weaken the hypothesis of infinite transcendence. For example, let $R = \widetilde{Q(c)}$, where $c = (c_1, \ldots, c_m)$ and let $\{P_j(x)\}_{j \in \mathbf{Z}^+}$ be a listing of all non-zero polynomials in one variable over $\mathbf{Q}(\mathbf{c})$. Then, $R = \cup_{j \in \mathbf{Z}^+} V_j$, where $V_j = \{r \in R \mid P_j(r) = 0\}$.

Remark 4. If R^n has property A, then $\mathbf{X} = \{r = (r_0, \ldots, r_{n-1}) \in R^n \mid r_i \neq 0 \; some \; i > 0\}$ has property A since $R^n = \mathbf{X} \cup \left\{ r \in R^n \mid \prod_{i=1}^{n-1} r_i = 0 \right\}$. More generally, if $X \subset R^n$ has property A, then so does $\{x \in X \mid x_i \neq 0 \; some \; i \in I\}$ where $I \subset \{0, \ldots, n-1\}$.

Remark 5. If X has property A, and $X \subset S \subset R^n$, then S has property A.

Lemma 4. Suppose $F : R^n \to R^n$ is an algebraically independent polynomial map (i.e. for all polynomials $g : R^n \to R$, *if* $g \cdot F \equiv 0$ *then* $g \equiv 0$). Then if $X \subset R^n$ has property A, then so does *F(X)*.

Proof. Let *Y=F(X)* and consider the following diagram:

$$\begin{array}{ccc} X \subset R^n & & \\ & \overset{g \cdot F}{\searrow} & \\ F \downarrow & & \\ Y = F(X) \subset R^n & \underset{g}{\to} & R \end{array}$$

First suppose $\{Y_j\}_{j \in J}$ covers Y. Let $X_j = F^{-1}(Y_j)$. Then $\{X_j\}_{j \in J}$ covers X. Now suppose Y_j is a variety in R^n defined by a (finite) set G_j of polynomials over $K \subset R$. Then

$$X_j = \{r \in R^n \mid F(r) \in Y_j\} = \{r \in R^n \mid g \cdot F(r) = 0, all \; g \in G_j\}$$

is a variety in R^n defined by the (finite) set of polynomials $\{g \cdot F \mid g \in G_j\}$ over $K(a_1, \ldots, a_m)$. Here $a_1, \ldots, a_m$ are the constants occurring in F.

So if $\{Y_j\}_{j \in J}$ is a countable cover of Y by varieties over a finitely generated subfield K, then $\{X_j\}_{j \in J}$ is a countable cover of X by varieties over $K(a_1, \ldots, a_m)$.

If X has property A, then $X_j = R^n$, some $j \in J$. So for all $r \in R^n$, $g \cdot F(r) = 0$, all $g \in G_j$. Thus, since R is infinite, $g \cdot F \equiv 0$ all $g \in G_j$. But F is algebraically independent. Therefore $g \equiv 0$, all $g \in G_j$. Therefore, $Y_j = R^n$ and so Y has property A.

---

11 We are grateful to George Bergman for pointing us to this paper.

Now let $\widetilde{R}$ be the algebraic closure of R, and so $\widetilde{R}^n$ can be considered the *space of (sequences of all) roots* of elements of $Poly_{\widetilde{R}}(n)$.

The *Viete map* $\pi : \widetilde{R}^n\,(roots) \to \widetilde{R}^n \left(\simeq Poly_{\widetilde{R}}(n)\right)$ is given by

$$\pi(\xi) \leftrightarrow \prod_i (z - \xi_i) \quad for\ \xi = (\xi_1, \ldots, \xi_n) \in \widetilde{R}^n.$$

We consider the following diagram:

$$\begin{array}{ccccc}
\widehat{Poly_R}(n-1) \times \widetilde{R}^n \simeq R^n \times \widetilde{R}^n & \longrightarrow^{Eval} & \longrightarrow \widetilde{R}^n & \textbf{(Space of roots)} \\
Proj \downarrow & \searrow F & \downarrow \pi & \textbf{(Viete map)} \\
\widehat{Poly_R}(n-1) \simeq R^n & \longrightarrow^{F_\alpha} & \longrightarrow \widetilde{R}^n \simeq Poly_{\widetilde{R}}(n) & \\
\textbf{(Space of degree n-1 polys/R)} & & \textbf{(Space of monic degree n polys/}\widetilde{\mathbf{R}}\textbf{)} &
\end{array}$$

Here $\widehat{Poly_R}(n-1)$ is the *space of univariate degree (n-1) polynomials over R* which is naturally associated with R^n via

$$r_0 + \cdots + r_{n-1}y^{n-1} \leftrightarrow r = (r_0, \ldots, r_{n-1}) \in R^n.$$

And for $r \in R^n$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \widetilde{R}^n$, $Eval$ is given by $Eval(r,\alpha)_i = r_0 + \cdots + r_{n-1}\alpha_i^{n-1}$, $F = \pi \cdot Eval$ and $F_\alpha(r) = F(r,\alpha)$. Thus,

Remark 6. $\left\{Eval(r,\alpha)_{i=1,\ldots,n}\right\}$ is the set of all roots of the monic polynomial associated with $F_\alpha(r)$.

Let $R_*^n = \left\{\alpha \in \widetilde{R}^n \mid \{\alpha_i\}_{i=1,\ldots,n}\ are\ distinct\ conjugates\ of\ degree\ n\ over\ R\right\}$.

So, $R_*^n \neq \emptyset$ just in case R has an algebraic extension of degree n. If $\xi \in R_*^n$, then $\pi(\xi)$ is the *minimal polynomial* of ξ_i over R.

Lemma 5. Suppose $\alpha \in R_*^n$. Then

(a) $F_\alpha : R^n \to R^n$ and
(b) F_α is algebraically independent.

Proof. See [MacIntyre, McKenna, van den Dries, 1983].

Recall $\mathbf{X} = \{r \in R^n \mid r_i \neq 0, some\ i > 0\}$ and $\mathbf{S} = \{r \in R^n \mid \mathbf{f}(r,z)$ has no roots in $R\}$.

Corollary 1. If $\alpha \in R_*^n$, then $F_\alpha(\mathbf{X}) \subset \mathbf{S}$.

Proof. Suppose $\alpha \in R_*^n$ and $r \in R^n$. Then by Lemma 5(a), $F_\alpha(r) \in R^n$. If in addition $r \in \mathbf{X}$, then $Eval(r,\alpha)_i \notin R$, $i = 1, \ldots, n$. So by Remark 6, $F_\alpha(r) \in \mathbf{S}$.

Corollary 2. Suppose the degree of transcendence of R is infinite. If $R_*^n \neq \emptyset$, then $\mathbf{S}$ has property A.

Proof. By Lemma 3 and Remark 4, $\mathbf{X}$ has property A. Let $\alpha \in R_*^n$. Then, by Lemmas 5(b) and 4, $F_\alpha(\mathbf{X})$ has property A. So by Corollary 1 and Remark 5, $\mathbf{S}$ has property A.

Thus we have proved Proposition 2.

Remark 7. Using a lemma of [Michaux, 1990], we need only assume as hypothesis in the Theorem, in case $R = R_=$ (likewise, in case $R = R_<$), that R be a commutative ring without zero divisors (an ordered commutative ring) of infinite transcendence over $\mathbf{Q}$.

Section 7 On the Undecidability of the Mandelbrot set over R

For a heuristic discussion of the problem of the decidability of the Mandelbrot set M one can see [Penrose, 1989]. For the mathematics of M see [Douady, Hubbard 1984–5].

A well known and presumably difficult conjecture is: The boundary of M has Hausdorff dimension 2. On the other hand, it seems much easier from the work of Douady, Hubbard, Misiurewicz, Tan Lei and others that the following holds.

Weak Conjecture. The boundary of M has Hausdorff dimension greater than 1.

Proposition. If the Weak Conjecture is true, then the Mandelbrot set is undecidable over $\mathbf{R}$.

Proof. Suppose the contrary. Then M is the halting set of some machine over $\mathbf{R}$ and hence is the countable union of basic semi-algebraic sets (see [BSS]). M is closed, and the closure of a basic semi-algebraic set is a semi-algebraic set. Thus we may suppose,

$$M = \cup_{i=1}^{\infty} S_i$$

where each $S_i \subset \mathbf{C} = \mathbf{R^2}$ is a closed semi-algebraic set. For each i, we claim: $dim(\partial M \cap S_i) \leq 1$ where ∂M is the boundary of M and *dim* is the Hausdorff dimension.

If $dim S_i \leq 1$ this is immediate. However if $dim S_i > 1$, then $dim S_i = 2$ since S_i is a closed semi-algebraic set. So $dim \partial S_i \leq 1$. Next note that the interior of S_i must be contained in the interior of M. Therefore,

$$\partial M \cap S_i \text{ is contained in } \partial M \cap \partial S_i \text{ and has dimension } \leq 1.$$

So now we have,

$$\partial M = \cup_{i=1}^{\infty} (\partial M \cap S_i) \text{ has dimension } \leq 1$$

contradicting the Weak Conjecture.

Remark. It is easy to show that the complement of M is a halting set, so once more we have (provisionally) an example of an undecidable "semi-decidable" set.

Added in proof. At the Smalefest in Berkeley (August 1990), Dennis Sullivan has shown us what appears to be a direct proof that the Mandelbrot set is not the countable union of semi-algebraic sets.

References

Amitsur, S.A., "Algebras over Infinite Fields," *Proceedings of the American Mathematical Society*, **7** (1956), 35–48.

Blum, L., Shub, M., and S. Smale, "On a Theory of Computation and Complexity over the Real Numbers: NP-Completeless, Recursive Functions and Universal Machines," *Bulletin of the American Mathematical Society*, **21** (1989), 1-46.

Cohen, P., *Set Theory and the Continuum Hypothesis*, Benjamin, N.Y. 1960.

Davis, M., *Computability and Unsolvability*, Dover, N.Y., 1982.

Douady, A. and J. Hubbard, "Etude Dynamique des Polynomes Complex, I, 84–20, 1984 and II, 85–40. 1985, Publ. Math. d'Orsay, Univ. de Paris-Sud, Dept. de Math. Orsay, France.

Friedman, H., and R. Mansfield, "Algorithmic Procedures," preprint, Penn State, 1988.

Gödel, K., "Uber formal Unentscheidbare Satze der Principia Mathematica und Verwandter Systeme, I," *Monatsh. Math. u. Phys.*, **38** (1931), 173-198.

Grigoriev, D.Yu., and N. N. Vorobojov, "Solving Systems of Polynomial Inequalities in Subexponential Time," *Journal of Symbolic Computation* **5**, (1988), 37–74.

Ierardi, D., "Quantifier Elimination in the First-Order Theory of Algebraically Closed Fields," *Proceedings of the 21st Annual ACM Symposium on the Theory of Computing* (1989) and Ph.D. Thesis, Cornell University (Computer Science).

MacIntyre, A., "On ω_1- Categorical Fields," *Fund. Math.* **7** (1971), 1-25.

MacIntyre, A., McKenna, K. and L. van den Dries, "Elimination of Quantifiers in Algebraic Structures," *Advances in Math.*, Vol. **47**, (1983), 74-87.

Michaux, C., "Ordered Rings over which Output Sets are Recursively Enumerable Sets," preprint, Universite de Mons, Belgium, 1990.

Penrose, R., *The Emperor's New Mind*, Oxford University Press, Oxford, 1989.

Renegar, J., "On the Computational Complexity and Geometry of the First-Order Theory of the Reals," Part I, II, III, Cornell University, preprint, 1989.

Robinson, J. "Definability and Decision Problems in Arithmetic," *Journal of Symbolic Logic*, **14**, No. 2 (1949), 98–114.

Robinson, J., "The Undecidability of Algebraic Rings and Fields," *Proceedings of the American Mathematical Society*, **10** (1959), 950-957.

Robinson, J., "On the Decision Problem for Algebraic Rings," in *Studies in Mathematical Analysis and Related Topics*, (Ed.), Gilberson, et al., Stanford., University Press, 1962, 297-304.

Robinson, J., "The Decision Problem for Fields," in *Symposium on the Theory of Models*, North Holland, 1965, 299-311.

Robinson, R.M., "Undecidable Rings," *Transactions of the American Math. Society*, **70**, No.1 (1951), 137–159.

Rosser, B. "Extensions of Some Theorems of Gödel and Church," *Journal of Symbolic Logic* **1** (1936), 87–91.

Tarski, A., *A Decision Method for Elementary Algebra and Geometry*, University of California, Press, 1951.

INTERNATIONAL COMPUTER SCIENCE INSTITUTE, 1947 CENTER STREET, BERKELEY, CALIFORNIA 94704 (lblum@icsi.berkeley.edu)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720 (smale@cartan.berkeley.edu)