International Journal of Theoretical Physics, Vol. 32, No. 11, 1993

Dynamical System Where Proving Chaos Is Equivalent to Proving Fermat's Conjecture

N. C. A. da Costa,[1] F. A. Doria,[2] and A. F. Furtado do Amaral[2,3]

Received July 14, 1992

We prove that we can explicitly construct the expression for a low-dimensional Hamiltonian system where proving the existence of a Smale horseshoe is equivalent to proving that Fermat's Conjecture is true. We then show that some sets of similar intractable problems are dense (in the usual topology) in the space of all dynamical systems over a finite-dimensional real manifold.

1. INTRODUCTION

We have recently started an exploration within physics and other axiomatized sciences of metamathematical phenomena such as undecidability and incompleteness (da Costa and Doria, 1991*a–e*, 1993; da Costa *et al.*, 1990, 1992*a,b*; Stewart, 1991*a,b*). The original motivation for our results was a question raised by Hirsch (1985) on the (apparently) enormous difficulty of deciding whether dynamical systems which represent actual physical systems are chaotic. Hirsch asked for a general criterion to settle that question: "A major challenge to mathematicians is to determine which dynamical systems are chaotic and which are not. Ideally one should be able to tell from the form of the differential equations."

We proved (da Costa and Doria, 1991*c–e*) that there is no such computable criterion; chaos is algorithmically undecidable in the general situation. Actually undecidability appears everywhere in mathematics, and is a quite commonplace phenomenon; a recent example concerns the

[1]Institute for Advanced Studies, University of São Paulo, 05508 São Paulo SP, Brazil.
[2]Research Center on Mathematical Theories of Communication, School of Communications, Federal University at Rio de Janeiro, 22290 Rio de Janeiro RJ, Brazil.
[3]Permanent address: Institute of Physics, Federal University at Rio de Janeiro, 21940 Rio de Janeiro RJ, Brazil.

0020-7748/93/1100-2187$07.00/0

nonrecursivity of certain functions in algebraic geometry (Nabutovsky, 1989). It was conjectured by Wolfram (1984) that undecidability and incompleteness were also to be expected everywhere in physics: "One may speculate that undecidability is common in all but the most trivial physical theories. Even simply-formulated problems in theoretical physics may be found to be provably insoluble."

We showed that such is the case. Moreover, the chief aspect of our results is their wide-ranging applicability, as they provide a blueprint for the construction of Gödel-like *incompleteness* theorems within any mathematized science that handles its objects through the language of classical analysis. We prove (da Costa and Doria, 1991*d*) that given any nontrivial property ϕ of a dynamical system within the language of classical elementary real analysis, we can explicitly obtain the formal expression for a countably infinite family of such systems where ϕ is algorithmically undecidable. Also there is another countably infinite family of systems of which it is true (in a "natural" interpretation) that they satisfy ϕ, but such that this fact cannot be proved from the usual axiomatizations for classical analysis.

We can immediately apply that to classical mechanics. Thus, there are infinitely many expressions for infinitely many different classical mechanical systems such that one cannot prove (within a "nice" axiomatization for our theory) that those systems have a nontrivial property ϕ, while it is true that they do have that property in all standard models, i.e., those where formalized arithmetic is interpreted as the intuitive theory of the natural numbers.

A consequence of our results is the existence of solvable but intractable problems within the realm of classical mechanics, that is to say, problems that can be stated in our formal language with the help of a small sequence of symbols, but such that their proofs are inordinately long and difficult (da Costa and Doria, 1991*d*; Ehrenfeucht and Mycielski, 1971; Gödel, 1986). Fermat's Conjecture that there are no positive integers x, y, z, m, where x, y, and $z > 1$, and $m > 2$, such that

$$x^m + y^m = z^m$$

seems to qualify (within number theory) as one of those problems with a simple statement and a very difficult proof. Well, nobody knows whether Fermat's Conjecture does, in fact, have a proof (or a counterexample), as it may also be undecidable within formalized arithmetic: if Fermat's Conjecture is false in the standard model for arithmetic, then its falsity can be proved within formalized arithmetic, but if it is true in the standard model, then it can either be provable or undecidable. If Fermat's Conjecture does have a proof, then the consensus is that it will be inordinately long and diffcult, even if we enrich number theory with several new concepts from other domains in mathematics. (Enriching a formal theory with what amounts to the addition of a consistent set of new axioms may shorten in a decisive way infinitely many difficult proofs while leaving untouched the difficulty of proving other results (da Costa and Doria, 1991*d*).) For a review of the main results about Fermat's Conjecture, including the Fåltings proof of Mordell's Conjecture, see Cornell and Silvermann (1986), Edwards (1977), and Ribenboim (1989). However, we will not need those results here and we quote the references for the sake of completeness.

We take Fermat's Conjecture simply as an example of a specific arithmetic problem with a short intuitive and elementary formulation and (if it is provable) what appears to be an extremely complicated proof. We notice that one of Gödel's last published remarks delves on that situation (Gödel, 1990): "another oddity..., namely the fact that such problems as Fermat's which can be written down in ten symbols of elementary arithmetic, are still unsolved 300 years after they have been posed."

As is well known, the fact that an axiomatic system which is consistent and sufficiently strong to include arithmetic has theorems with a very simple statement and inordinately long proofs is a result by Gödel himself (1986; Ehrenfeucht and Mycielski, 1971), which is related to the "speedup" theorems in computation theory, since some of those proofs can be arbitrarily shortened if we add to the original theory a new set of adequate (and consistent) axioms.

Our result shows that questions as difficult as Fermat's Conjecture appear everywhere in the sciences whose basic language is that of classical analysis. Checking for a simple property may lead to a problem equivalent to Fermat's. As far as we can tell, that seems to be a technically obvious but rather unexpected situation which we try to explore in the present note.

[We have also extended our results to show that there are problems in dynamical systems theory which lie beyond the pale of arithmetic—they cannot be made equivalent to any arithmetical problem. However, the general ground plan of that more general result is similar to the example in this paper; for details see da Costa and Doria (1993).]

Notation and Preliminary Concepts

For the conventions and concepts we use here see da Costa and Doria (1991*b*–*e*).

We are going to specify some notation: logical connectives: $\wedge$, "and"; $\vee$, "or"; $\neg$, "not"; $\rightarrow$, "if ..., then ..."; $\leftrightarrow$, "if and only if." $\mathbf{N}$ is the standard model for arithmetic; ω_0 is the set of natural numbers (or positive integers). **Z** is the set of integers, **Q** is the set of rational numbers, and **R** is the set of reals.

When dealing with mathematical objects within a formalized theory T, one never handles those objects "in themselves," as they can only appear within T as strings of symbols which we call "expressions" for those objects. For example, a circle (with r as its radius) may be given within the language $\mathscr{L}_T$ of T as the formal description of a plane set of points that satisfies the usual algebraic relation $x^2 + y^2 = r^2$.

Let T be a consistent axiomatic theory that includes formalized arithmetic and which is sufficiently strong so that we may develop the whole theory of dynamical systems within T (from here on we suppose that $\mathrm{ZFC} \subseteq T$; that will be more than enough). Let $\mathscr{L}_T$ be its formalized language; we suppose that the *set of formal expressions* in T, which we represent by $\ulcorner \mathscr{L}_T \urcorner$, can be obtained within T. If ξ is a mathematical object dealt with in T, then the expression that represents it is $\ulcorner \xi \urcorner \in \ulcorner \mathscr{L}_T \urcorner$.

We define (da Costa and Doria, 1991*d*):

Definition 1.1. T is *arithmetically consistent* if and only if the standard model **N** for arithmetic is a model for the arithmetic sentences of T.

From here on we suppose that the theories T we deal with are arithmetically consistent; to avoid discussions about the specific proof strength of T, we also suppose that $\mathrm{ZFC} \subseteq T$.

We are going to deal here with sentences that are *T-demonstrably equivalent* to arithmetic sentences; for the definition of that concept see da Costa and Doria (1991*d*) and Rogers (1967).

2. THE MAIN RESULT

We are going to prove here the following theorem:

Theorem 2.1. If T is arithmetically consistent, then we can algorithmically construct within the formal language $\mathscr{L}_T$ of T the expression for a low-dimensional Hamiltonian system $\mathscr{H}$ such that the proof that $\mathscr{H}$ has a Smale horseshoe is equivalent to the proof of Fermat's Conjecture within T.

Remark 2.2. When we say that we can *algorithmically construct* an expression, we mean that we can explicitly give an algorithm (in the sense of recursion theory) that allows us to obtain that expression within $\ulcorner \mathscr{L}_T \urcorner$ out of the alphabet of $\mathscr{L}_T$. However, as is quite usual in recursion theory, we are going to give a clear albeit intuitive construction for the expression, and leave the toil and trouble of obtaining a rigorous algorithm to the archetypical "interested reader."

The proof will be given in a series of lemmata and propositions. Let $R \subset \omega_0^n$ be an n-place relation on the natural numbers, $n > 0$ an integer. Let $p(x_1, \ldots, x_n, y_1, \ldots, y_m)$ be a polynomial in the unknowns $x_1, \ldots, y_1 \ldots$ over the integers.

We can define (Davis, 1989):

Definition 2.3. $R(x_1, \ldots, x_n)$ is *Diophantine* if and only if there is a polynomial

$$p(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

as the one given above over the integers and

$$R(x_1, \ldots, x_n) \leftrightarrow \exists y_1, \ldots, y_m \in \omega_0 p(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

We then have the following well-known result that solved Hilbert's 10th Problem (Davis, 1982).

Lemma 2.4. $R(x_1, \ldots, x_n)$ is Diophantine if and only if it is recursively enumerable.

It is immediate that the set of solutions of any Diophantine equation is recursively enumerable; the hard part is the converse statement. Therefore, if Fermat's Conjecture is true, then the set of positive-integer solutions of all equations of the type $x^n + y^n = z^n$ (but for the trivial cases, and for exponents $n = 1, 2$) is trivially recursively enumerable. If Fermat's Conjecture is false, then the Fåltings–Mordell theorem (Cornell and Silvermann, 1986) ensures that, given any $n > 2$, there will only be a finite (and possibly zero) number of exceptions to the conjecture for every n. Thus we can devise a simple intuitive enumeration procedure to list those exceptions. Then, by Church's Thesis, there will be a Turing machine that does that enumeration, so that the set of positive-integer solutions for the Fermat equations is a recursively enumerable set. Call that set the Fermat set.

From Lemma 2.4, it follows that the Fermat set is Diophantine, and as a consequence there is a polynomial over the integers that represents it in the sense of Definition 2.3. Notice that such a polynomial will have no solution at all over ω_0 if Fermat's Conjecture is true.

We are now going to construct explicitly one such polynomial. In order to do so we will not require the full strength of the Matijasevič–Davis–Robinson theorem (Lemma 2.4); we only need the Diophantine characterization for the exponential relation $v = u^k$, where v, u, and k are natural numbers:

Proposition 2.5. $v = u^k$ if and only if there are natural numbers $x_1, \ldots, x_{20}$ such that $p(u, k, v, x_1, \ldots, x_{20}) = 0$, where the polynomial p

over the integers is given below:

$$\begin{aligned}
&p(u, k, v, x_1, \ldots, x_{20}) \\
&\quad = [x_1^2 - (x_2^2 - 1)x_3^2 - 1]^2 + [x_4^2 - (x_2^2 - 1)x_5^2 - 1]^2 \\
&\qquad + [x_6^2 - (x_7^2 - 1)x_8^2 - 1]^2 + (x_5 - x_9 x_3)^2 + [x_7 - (1 + 4x_{10}x_3)]^2 \\
&\qquad + [x_7 - (x_2 + x_{11}x_4)]^2 + [x_6 - (x_1 + x_{12}x_4]^2 \\
&\qquad + [x_8 - k + 4(x_{13} - 1)x_3]^2 + [x_3 - (k + x_{14}) + 1]^2 \\
&\qquad + \{[x_1 - x_3(x_2 - u) - v]^2 - (x_{15} - 1)^2(2x_2 u - u^2 - 1)^2\}^2 \\
&\qquad + [v + x_{16} - (2x_2 u - u^2 - 1)]^2 \\
&\qquad + [x_{17} - (u + x_{18})]^2 + [x_{17} - (k + x_{19})]^2 \\
&\qquad + [x_2^2 - (x_{17}^2 - 1)(x_{17} - 1)^2 x_{20}^2 - 1]^2
\end{aligned}$$

Proof. See Davis (1982). Another Diophantine representation of the exponential function can be found in Matijasevič and Robinson (1975). ■

We now write down the Diophantine equation that represents Fermat's Conjecture:

Proposition 2.6. Given an arithmetically consistent theory T, Fermat's Conjecture is equivalent (within T) to the formal sentence below:

$$\begin{aligned}
&\forall x, y, z, m \in \omega_0 \neg \exists u, v, w, r_1, \ldots, s_1, \ldots, t_1, \ldots \in \omega_0 \\
&\quad \{x, y, z > 1 \wedge m > 2 \wedge [p^2(x, m, u, r_1, \ldots, r_{20}) \\
&\quad + p^2(y, m, v, s_1, \ldots, s_{20}) \\
&\quad + p^2(z, m, w, t_1, \ldots, t_{20}) + (u + v - w)^2 = 0]\}
\end{aligned}$$

or, equivalently,

$$\begin{aligned}
&\forall i, j, k, n \in \omega_0 \neg \exists x, y, z, m, u, v, w, r_1, \ldots, s_1, \ldots, t_1, \ldots \in \omega_0 \\
&\quad \{[p^2(x, m, u, r_1, \ldots, r_{20}) + p^2(y, m, v, s_1, \ldots, s_{20}) \\
&\quad + p^2(z, m, w, t_1, \ldots, t_{20}) + (u + v - w)^2 \\
&\quad + (i + 2 - x)^2 + (j + 2 - y)^2 + (k + 2 - z)^2 + (n + 3 - m)^2 = 0]\}
\end{aligned}$$

where p is given in Proposition 2.5.

Proof. Notice that $(x + 2)^{m+3} + (y + 2)^{m+3} = (z + 2)^{m+3}$ is equivalent to

$$\begin{aligned}
&\exists u, v, w \in \omega_0\, u = x^m \wedge v = y^m \wedge w = z^m \wedge u + v = w \\
&\quad \wedge x = i + 2 \wedge y = j + 2 \wedge z = k + 2 \wedge m = n + 3
\end{aligned}$$

We then obtain the Diophantine equation that represents the above sentence, and add the quantifiers (Davis, 1982); the conditions on x, y, z, m avoid both the trivial solutions and the Pythagorean equation. ∎

Richardson's Functor

Again we suppose that everything happens within our axiomatized theory T. Let $\mathscr{P}$ be the algebra of polynomials on a finite number of variables over the integers $\mathbf{Z}$; let $\mathscr{E}$ be the algebra of real-valued elementary functions in a finite number of variables over the rationals $\mathbf{Q}$, while $\mathscr{F}$ is the algebra of real-valued elementary functions in one variable, again over the rationals $\mathbf{Q}$; we finally add to both $\mathscr{P}$ and $\mathscr{F}$ an expression (a symbol) for the number π, and close everything under that new constant. Given a polynomial $p(x_1, \ldots, x_m, y_1, \ldots, y_n)$, let $\tau_m(x_1, \ldots, x_m)$ be the function that effectively codes m-tuples of natural numbers $\langle x_1, \ldots, x_m \rangle$ by a single natural number (Rogers, 1967, p. 63). Let $r = \tau_m(\langle \cdots \rangle)$. We abbreviate $p(x_1, \ldots, x_m, y_1, \ldots, y_n) = p_r(y_1, \ldots, y_n)$.

Then let us inductively construct out of a polynomial $q_m(x_1, \ldots, x_n)$ a real-defined and real-valued function ιq_m given through the following steps.

Initial Step. Suppose that we are given the expressions q_m as below:

- If $q_m(x_1, \ldots, x_n) = c$, where c is a constant, then we put $\iota q_m = |c| + 2$.
- If $q_m(x_1, \ldots, x_n) = x_i$, then $\iota q_m = x_i^2 + 2$.

Induction Step. We suppose that q_m is given as indicated. We then obtain as follows the corresponding ιq_m:

- If $q_m = s_m \pm t_m$, then $\iota q_m = \iota s_m + \iota t_m$.
- If $q_m = s_m t_m$, then $\iota q_m = \iota s_m \iota t_m$.

We then write $k_i(m, x_1, \ldots, x_n) = \iota\partial_i p_m(x_1, \ldots, x_n)$, where $\partial_i = \partial / \partial x_i$. Then:

Definition 2.7. The map $\rho: \mathscr{P} \to \mathscr{E}$, given by

$$p(x_1, \ldots, x_m, y_1, \ldots, y_n)$$
$$\mapsto \rho p(x_1, \ldots, x_m, y_1, \ldots, y_n) = (n+1)^4 p^2(x_1, \ldots, x_m, y_1, \ldots, y_n)$$
$$+ \sum_{i=1}^{n} (\sin^2 \pi x_i) k_i^4 (x_1, \ldots, x_m, y_1, \ldots, y_n)$$

is *Richardson's first map.*

Corollary 2.8. Given a polynomial expression $\ulcorner p_m \urcorner \in \ulcorner \mathscr{L}_T \urcorner$, there is an algorithm that allows us to obtain an expression $\ulcorner \rho p_m \urcorner \in \ulcorner \mathscr{L}_T \urcorner$ for the image of p_m under Richardson's first map.

Proof. Immediate, from the definition of ρ. ■

We can assert:

Proposition 2.9 (Richardson's First Lemma). Within the theory T there are natural numbers $x_1, \ldots, x_n$ such that $p_m(x_1, \ldots, x_n) = 0$ if and only if there are real numbers $x_1, \ldots, x_n$ such that $\rho p_m(x_1, \ldots, x_n) = 0$ if and only if there are real numbers $x_1, \ldots, x_n$ such that $\rho p_m(x_1, \ldots, x_n) \leq 1$.

Proof. See Richardson (1968). ■

Now let

$$q(x, y, z, m, u, v, w, r_1, \ldots, r_{20}, s_1, \ldots, s_{20}, t_1, \ldots, t_{20})$$

[or, respectively, $q'(i, j, k, n, x, \ldots)$] denote each one of the polynomial expressions in the assertion within Proposition 2.6. We are going to rename the variables in that polynomial as follows:

$$\{u, v, w, r_1, \ldots, s_1, \ldots, t_1, \ldots\} \mapsto \{u_1, \ldots, u_\iota\}$$

where $\iota = 63$ or $\iota = 67$, depending on our choice of either q or q', so that the polynomial that represents Fermat's Conjecture becomes either

$$q(x, y, z, m, u_1, \ldots, u_{63})$$

or

$$q'(i, j, k, n, u_1, \ldots, u_{67})$$

Let ρ denote Richardson's first map as above. As always, we suppose that T is arithmetically consistent, and at least as strong as ZFC. Then:

Proposition 2.10. Within our T, Fermat's Conjecture is equivalent to each of the formal sentences below:

1.

$$\begin{aligned} &\forall x, y, z, m \in \omega_0 \ \neg \exists u_1, \ldots, u_{63} \in \mathbf{R} \\ &\quad [x, y, z > 1 \wedge m > 2 \\ &\quad \wedge \rho q(x, y, z, m, u_1, \ldots, u_{63}) = 0] \end{aligned}$$

2.

$$\begin{aligned} &\forall x, y, z, m \in \omega_0 \ \neg \exists u_1, \ldots, u_{63} \in \mathbf{R} \\ &\quad [x, y, z > 1 \wedge m > 2 \\ &\quad \wedge \rho q(x, y, z, m, u_1, \ldots, u_{63}) \leq 1] \end{aligned}$$

3.

$$\forall x, y, z, m \in \omega_0 \neg \exists u_1, \ldots, u_{67} \in \mathbf{R}$$
$$\rho q'(x, y, z, m, u_1, \ldots, u_{67}) = 0]$$

4.

$$\forall x, y, z, m \in \omega_0 \neg \exists u_1, \ldots, u_{67} \in \mathbf{R}$$
$$\rho q'(x, y, z, m, u_1, \ldots, u_{67}) \leq 1]$$

Proof. From Proposition 2.9. ■

Remark 2.11. We now define

$$h(x) = x \sin x$$
$$g(x) = x \sin x^3$$

Given a set of real variables $x_1, \ldots, x_n$, we define the following maps:

$$x_1 = h(x)$$
$$x_2 = h \circ g(x)$$
$$x_3 = h \circ g \circ g(x)$$
$$\ldots$$
$$x_{n-1} = h \circ g \circ \cdots \circ g(x)$$

(where g is composed $n-2$ times), and

$$x_n = g \circ g \circ \cdots \circ g(x)$$

where here g is composed n times.

Given a polynomial $p_m(x_1, \ldots, x_n) \in \mathscr{P}$, we define:

Definition 2.12. The maps $\rho': \mathscr{P} \to \mathscr{F}$ and $\rho'': \mathscr{P} \to \mathscr{F}$, given by (1)

$$p_m(x_1, \ldots, x_n)$$
$$\mapsto \rho'[p_m(x_1, \ldots, x_n)](x)$$
$$= \rho p_m(h(x), h \circ g(x), \ldots, g \circ g \circ \cdots \circ g(x))$$

where ρ is Richardson's first map; and (2)

$$p_m(x_1, \ldots, x_n)$$
$$\mapsto \rho''[p_m(x_1, \ldots, x_n)](x)$$
$$= \rho'[p_m(x_1, \ldots, x_n)](x) - 1/2$$

are *Richardson's second map* of the first (ρ') and second (ρ'') kinds.

Corollary 2.13. Given a polynomial expression $\ulcorner p_m \urcorner \in \ulcorner \mathscr{L}_T \urcorner$, there is an algorithm that allows us to obtain expressions $\ulcorner \rho' p_m \urcorner \in \ulcorner \mathscr{L}_T \urcorner$ and $\ulcorner \rho'' p_m \urcorner \in \ulcorner \mathscr{L}_T \urcorner$ for the images of p_m under Richardson's second map.

Proof. Immediate, from the definition of ρ' and ρ''. ■

ρ'' is due to Wang (1974), as well as the corresponding portion in the next result:

Proposition 2.14. Within T:

1. There are natural numbers $x_1, \ldots, x_n$ such that

$$p_m(x_1, \ldots, x_n) = 0$$

if and only if there is a real number x such that

$$\rho' p_m(x) \leq 1$$

2. There are natural numbers $x_1, \ldots, x_n$ such that

$$p_m(x_1, \ldots, x_n) = 0$$

if and only if there is a real number x such that

$$\rho'' p_m(x) = 0$$

Proof. See Richardson (1968) and Wang (1974). ■

We then apply Richardson's second map of the first and second kinds to the polynomials that represent Fermat's Conjecture in Proposition 2.6, so that we obtain (in an obvious notation)

$$(\rho' q)(x, y, z, m, u)$$

and

$$(\rho'' q)(x, y, z, m, u)$$

We can therefore assert:

Proposition 2.15. Given our arithmetically consistent theory T, then Fermat's Conjecture is equivalent (within T) to each of the formal statements below:

1.

$$\forall x, y, z, m \in \omega_0 \neg \exists u \in \mathbf{R}[x, y, z > 1 \wedge m > 2 \wedge (\rho' q)(x, y, z, m, u) \leq 1]$$

2.

$$\forall x, y, z, m \in \omega_0 \neg \exists u \in \mathbf{R}[x, y, z > 1 \wedge m > 2 \wedge (\rho'' q)(x, y, z, m, u) = 0]$$

3.

$$\forall x, y, z, m \in \omega_0 \neg \exists u \in \mathbf{R}[(\rho' q')(x, y, z, m, u) \leq 1]$$

4.

$$\forall x, y, z, m \in \omega_0 \neg \exists u \in \mathbf{R}[(\rho'' q'')(x, y, z, m, u) = 0]$$

Proof. From Proposition 2.14. ∎

A Two-State Function That "Solves" Fermat's Conjecture

In the next step we are going to obtain a two-state function $\beta(x, y, z, m)$ that will be expressed with the help of elementary functions plus a few commonplace operations in elementary real analysis such that, for $x, y, z, m \in \omega_0$, $x, y, z > 1$ and $m > 2$, then:

1. $\beta(x, y, z, m) = 1$ if and only if the 4-tuple x, y, z, m is a counterexample for Fermat's Conjecture.
2. $\beta(x, y, z, m) = 0$ if and only if the 4-tuple x, y, z, m does not contradict Fermat's Conjecture.

We need:

Definition 2.16. (1)

$$B(x, y, z, m, u) = |(\rho' q')(x, y, z, m, u) - 1| - [(\rho' q')(x, y, z, m, u) - 1]$$

and (2)

$$C(x, y, z, m, u) = [B(x, y, z, m, u)]^2$$

As a result, we have the following:

Proposition 2.17. Given our arithmetically consistent theory T, then:
1. Fermat's Conjecture is equivalent within T to the formal sentence below:

$$\forall x, y, z, m, u[x, y, z, m \in \omega_0 \wedge u \in \mathbf{R} \rightarrow C(x, y, z, m, u) = 0]$$

2. The negation of Fermat's Conjecture is equivalent within T to the formal sentence below:

$$\exists x, y, z, m, u[x, y, z, m \in \omega_0 \wedge u \in \mathbf{R} \wedge C(x, y, z, m, u) > 0]$$

Proof. From Definition 2.16 and from Proposition 2.14. ∎

We have:

Proposition 2.18. Given our arithmetically consistent theory T, we can explicitly and algorithmically construct within $\ulcorner \mathscr{L}_T \urcorner$ the formal expression for a function $\beta(x, y, z, m)$ with values in the set $\{0, 1\}$ such that:

1. $\forall x, y, z, m \in \omega_0 \beta(x, y, z, m) = 0$ if and only if Fermat's Conjecture is true.
2. $\exists x, y, z, m \in \omega_0 \beta(x, y, z, m) = 1$ if and only if x, y, z, m is a counterexample for Fermat's Conjecture.

Moreover, $\beta(x, y, z, m)$ can be constructed entirely within the language of elementary real analysis.

Proof. We write the expression

$$K(x, y, z, m) = \int_{-\infty}^{+\infty} \frac{C(x, y, z, m, u)e^{-u^2}}{1 + C(x, y, z, m, u)} du$$

and then put

$$\beta(x, y, z, m) = \sigma(K(x, y, z, m))$$

σ is the sign function; $\sigma(\pm x) = \pm 1$ and $\sigma(0) = 0$. ■

We can go beyond that and obtain a constant function θ such that $\theta = 0$ if and only if Fermat's Conjecture is true, and $\theta = 1$ if and only if Fermt's Conjecture is false, within an arithmetically consistent theory T; we will only need a slight extension of the algebra of functions (and of the corresponding set of expressions) we are dealing with:

Proposition 2.19. Given our arithmetically consistent theory T, we can explicitly and algorithmically construct within $\ulcorner \mathcal{L}_T \urcorner$ the formal expression for a constant function θ which is either equal to 0 or 1 such that:

1. $\theta = 0$ if and only if Fermat's Conjecture is true.
2. $\theta = 1$ if and only if Fermat's Conjecture is false.

Moreover, θ can be constructed entirely within the language of elementary real analysis.

Proof. Notice that, when extended to the reals in $\mathbf{R}^4$, $\beta(x, y, z, m) \geq 0$. We therefore write

$$L = \int_{\mathbf{R}^4} \frac{\beta(x, y, z, m) \exp[-(x^2 + y^2 + z^2 + m^2)]}{1 + \beta(x, y, z, m)} dx\, dy\, dz\, dm$$

Then $\theta = \sigma(L)$. ■

Remark 2.20. Notice that there are "innocent-looking" expressions in every day mathematical practice for both $|x|$ and $\sigma(x)$, namely we can write $|x| = +\sqrt{x^2}$ and $\sigma(x)$ can be algebraically obtained out of the absolute value function.

We also wish to point out that our previous results (da Costa and Doria, 1991*c*,*d*) imply the following: let $\mathscr{F}'$ denote the algebra $\mathscr{F}$ to which we have added the absolute value operation $|x|$ and closed everything under it. Therefore, if T is arithmetically consistent, then (i) there is no algorithm to decide, for each member $f_m(x)$ of a countable family of expressions that represent elements of $\mathscr{F}'$ whether one has $f_m(x) \neq 0$ somewhere or, for all reals, $f_m \equiv 0$. Moreover, (ii) there is an expression for a function $f(x)$ in $\mathscr{F}'$ such that it is true that, for all reals, $f(x) \equiv 0$ in a convenient "natural" model **M** that makes T an arithmetically consistent theory, but such that one cannot prove that fact from the axioms of T. [See on those results da Costa and Doria, 1991*c*,*d*].

Therefore we have in T:

1. Given a family $g_k(x, y, z, m, u)$ of expressions for functions in an adequate extension of $\mathscr{F}'$, parametrized by the natural numbers x, y, z, m, there is no algorithm to decide, for each k, whether one has $g_k = \beta$.

It suffices to take

$$g_k(x, y, z, m, u) = \beta(x, y, z, m) + f_k(u)$$

with $f_k(u)$ as above.

2. There is an expression for a function g, again in an adequate extension of $\mathscr{F}'$, such that it is true in **M** that $g = \beta$; however, that fact cannot be proved from the axioms of T.

Put

$$g(x, y, z, m, u) = \beta(x, y, z, m) + f(x)$$

where $f(x) \equiv 0$ in **M**, but such that one cannot prove this fact in T. The same is obviously true of the constant function θ in Proposition 2.19.

We conjecture that in order to obtain an expression for $\beta(x, y, z, m)$ and for θ out of elementary functions we will necessarily require an integration and something that might stand for σ; our conjecture about the integration operation is supported by a remark of M. S. Burgin (n.d.) on the computational power of the Riemann integration (which applies to the present case since we are dealing with continuous functions).

Also, simpler expressions for those objects will be obtained if we start from the *exponential* Diophantine version of Fermat's Conjecture; the whole construction is slightly more general (da Costa and Doria, 1991*d*; Richardson, 1968).

We can now conclude the proof of Theorem 2.1. Let h be the Hamiltonian for a free particle and let k be the Hamiltonian for the Holmes and Marsden (1982) example of a low-dimensional system with a horseshoe. Consider the countably infinite family $\mathscr{H}$ of expressions for

Hamiltonian systems given by

$$h_{(x,y,z,m)} = \beta(x, y, z, m)h + (1 - \beta(x, y, z, m))k$$

If we manage to show within T that such a family always coincides with k, we conclude that $\beta = 0$; therefore, we prove Fermat's Conjecture. Conversely, if we prove that Fermat's Conjecture holds within T, then we collapse the preceding family over k. We have proved:

Corollary 2.21. If our T is arithmetically consistent, then we can explicitly and algorithmically construct within $\ulcorner \mathscr{L}_T \urcorner$ a countably infinite family of expressions for Hamiltonian systems $\mathscr{H}$ such that all of them will provably have a Smale horseshoe if and only if Fermat's Conjecture can be proved within T.

The same construction, now with the help of the function θ in Proposition 2.19, allows us to state:

Corollary 2.22. If T is arithmetically consistent, then we can explicitly and algorithmically construct within $\ulcorner \mathscr{L}_T \urcorner$ the expression for a Hamiltonian h' such that h' will provably have a Smale horseshoe if and only if Fermat's Conjecture can be proved in T.

Proof. Put $h' = \theta h + (1 - \theta)k$. ■

Remark 2.23. The present example tries to suggest why it is so difficult to prove even the simplest property for innocent-looking systems, such as the Lorenz system (Afraimovich *et al.*, 1983). The fact that we can concoct a not-so-involved construction that leads to a dynamical system several of whose properties depend on the proof of Fermat's Conjecture suggests that very hard proofs are to be expected everywhere in the theory of dynamical systems.

Therefore we turn to the problem of the distribution of those "simple" questions with intractable proofs in the corresponding functional spaces.

Actually we have proved more than what was stated in Theorem 2.1. Let ϕ be a predicate defined for a domain that includes $\mathscr{F}'$ (and the corresponding expressions) plus the function (and the expression) for $\theta(x, y, z, m)$ given above. Suppose moreover, that there are ξ, ζ in T, $\xi \neq \zeta$, such that $T \vdash \phi(\xi)$ and $T \vdash \neg\phi(\zeta)$. Then:

Theorem 2.4. Within our T there is an object $\eta \in T$ such that $T \vdash \phi(\eta)$ if and only if $T \vdash$ "Fermat's Conjecture."

Proof. Write $\eta = (1 - \theta)\xi + \theta\zeta$. ■

Therefore, given *any* nontrivial predicate defined for an adequate extension of the algebra $\mathscr{F}'$ as above, we can explicitly and algorithmically obtain an object that will satisfy that predicate if and only if we can prove Fermat's Conjecture from our axiom system.

Remark 2.25. With the help of constructions developed in da Costa and Doria (1991*d,e*) (here quoted in Remark 2.20) we can show that (within a theory such as our T) there is no algorithm to decide whether a given problem in the theory of dynamical systems is T-equivalent to a solvable problem in the theory of Diophantine equations. Therefore, if we ask a question about a rather simple dynamical system, we have no algorithm to decide whether that question will turn out to be equivalent within T to an easy, hard, or impossible-to-check Diophantine problem.

Remark 2.26. Moreover, suppose that we have managed to reduce a Hamiltonian to an expression of the form $h = \eta h' + \lambda h''$. Can we check whether, say, η is the Richardson transform of a Diophantine polynomial—so that we can at least know when we are dealing with a number-theoretic problem under the guise of a problem in geometry? The results quoted in Remark 2.20 show that there will be infinitely many such η which are transforms of Diophantine polynomials, but such that we will never be able to prove that fact within T, since we have admitted that T is arithmetically consistent.

So, number-theoretic problems will appear within geometry, but in the general case we will never be able to prove that a problem we are dealing with is difficult because it is a number-theoretic problem embedded into a geometric question.

3. DENSITY THEOREMS

Again we suppose that T is arithmetically consistent, and that we can state facts about a topological space X (*specified below*) in $\mathscr{L}_T$.

We suppose that X is a function space which is a complete metric space and that a certain subset of the polynomials in a countable set of unknowns $x, y, z, \ldots$ over the rationals $\mathbf{Q}$ is dense in X. We then say that X is a Polish space. Let ϕ be a predicate in the language $\mathscr{L}_T$ which is defined for X.

Definition 3.1. ϕ is *open* in X if and only if $A_\phi = \{x \in X \colon \phi(x)\} \subset X$ is open in X.

ϕ is *open and dense* in X if and only if $A_\phi = \{x \in X \colon \phi(x)\} \subset X$ is open and dense in X.

Also, given an open and dense A_ϕ, let x_n, $n \in \omega_0$, be a countable family of polynomials over the rationals $\mathbf{Q}$ for whch we can prove (within T) that the family $\{x_n\}$ is dense in A_ϕ. Clearly, $T \vdash \phi(x_n)$, for each n. Let $y \in X$ be such that $T \vdash \neg\phi(y)$.

Remark 3.2. From here on we suppose that we have added to the language $\mathscr{L}_T$ the countably infinite set of expressions $\{\ulcorner x_n \urcorner\}$ that represent the x_n. Notice that we do not require that there is some procedure either to construct algorithmically the family x_n or to decide algorithmically whether, for a given y, there is an n such that $y = x_n$, or even to check, from a larger dense set $\{z_n\}$, whether one has, for an arbitrary n, $\phi(z_n)$. We only require that there are symbols within $\mathscr{L}_T$ that allow us to represent the elements of the set $\{x_n\}$, so that we can explicitly build an expression such as $\ulcorner \theta y + (1-\theta)x_n \urcorner$ which is used below.

Let us be given:

Definition 3.3. $Y = \{z_n : z_n = \theta_y + (1-\theta)x_n\}$ (θ as in Proposition 2.19).

We assert:

Proposition 3.4. Within our T, let A_ϕ be open and dense. Then:

1. If $T \vdash$ "Fermat's Conjecture," then $T \vdash$ "$Y \subset X$ is dense in X."
2. If $T \vdash$ "$\neg$(Fermat's Conjecture)," then $T \vdash$ "$Y \subset X$ is a singleton."

Proof. Suppose that there is a formal proof of Fermat's Conjecture within the theory T. We write ξ for that proof so that ξ proves (within T) "Fermat's Conjecture." Then (from Proposition 2.19) we can construct within T a formal proof ξ, ζ for $\theta = 0$ by adding an adequate set ζ of sentences in $\mathscr{L}_T$ to the formal proof ξ of Fermat's Conjecture, and from that second proof we obtain a proof $\xi, \zeta, \theta = 0$ for $z_n = x_n$, for each n, so that by construction we conclude that $\{z_n\} \subset A_\phi$ is dense in Y.

The second statement has a similar proof. ∎

Remark 3.5. Informally speaking, Y is the set of those objects in X that provably have property ϕ if and only if we can prove Fermat's Conjecture in T.

Let us now specify our X and write $X = C^r(m, \mathbf{R}^s)$, where $0 \leq r < +\infty$, $1 \leq s < +\infty$, and M is a real, compact, finite-dimensional Hausdorff differentiable manifold. Suppose that we have defined an atlas for M; therefore M becomes a specification of k domains in $\mathbf{R}^m$ together with the corresponding transition functions, where $m = \dim(M)$.

We wish to obtain explicitly the expressions for a countably infinite dense subset in our function space $C^r(M, \mathbf{R}^s)$. We will then patch up over

M ordered sets of s polynomials each. In order to obtain those objects in $C^r(M, \mathbf{R}^s)$, we define for each domain k an ordered set of s polynomials in m variables $\langle p_1, p_2, \ldots, p_s \rangle$ with coefficients in $\mathbf{Q}$. Since the number of transition functions is finite, we can explicitly and algorithmically characterize one such object by a finite string of symbols. Therefore we can obtain a procedure to enumerate all elements of that dense subset in $C^r(M, \mathbf{R}^s)$; we call that set of expressions $\mathscr{K} \in \mathscr{L}_T$; it is a decidable set within the set of all formulas in our formal language. Given each rational diameter $q \in \mathbf{Q}$ together with our enumeration of the expressions for $\mathscr{K}$, we can also explicitly and algorithmically define an enumeration for a basis of the C^r topology of our space of sections over M which is centered around the elements of $\mathscr{K}$. Finally, given an ordered set of polynomials $p = \langle p_1, \ldots, p_s \rangle$, there is a decision procedure (Tarski, 1948) that allows us to answer the question, "is p within an open ball of diameter q centered at the polynomial $s \in \mathscr{K}$?"

If we are given an open set $C \in C^k(M, \mathbf{R}^s)$ such that, let us say, the boundaries of its closure are polynomially defined, or such that one can algorithmically decide ϕ at least for polynomials, again there is an algorithm that allows us to enumerate explicitly a dense subset of C. Suppose that ϕ is open over C. Then we can state:

Corollary 3.6. Given the preceding conditions, we can explicitly construct the expressions for the elements of a dense countable family $\{z_n\} \subset C^r(M, \mathbf{R}^s)$ such that for each n, $T \vdash \phi(z_n)$ if $T \vdash$ "Fermat's Conjecture."

Remark 3.7. We have in mind as examples of ϕ assertions such as "z_n is Morse–Smale" or similar stuff. Over some trivial low-dimensional M (and if there is a proof of Fermat's Conjecture) there is a dense set of Morse–Smale vectorfields that can be explicitly and constructively expressed with the help of elementary functions plus some operations in real analysis, but such that the proof that they really are Morse–Smale fields is as hard as the proof of Fermat's Conjecture.

Moreover, as a consequence of a previous result (da Costa and Doria, 1991*d*) there will be families of dynamical systems X_n parametrized by $n \in \omega_0$ such that we can always check a given property ϕ for every element in the family, that is, $T \vdash \phi(X_n)$, but such that, for infinitely many values of n, the complexity of the proof [see da Costa and Doria (1991*d*) on that concept] will be larger than any recursive function of the length (in characters) of the statement $\ulcorner \phi(X_n) \urcorner$. That is to say, the proof of the property ϕ for X_k may have nothing to do with the proof of the same property for X_{k+1}; the first one may be easy, while the next one may be exceedingly hard.

Finally, the same arguments that we have used here allow us to show that, if the property ϕ is open, then the set of systems X such that it is true that $\phi(X)$ (in a model where T is arithmetically consistent), but such that $T \nvdash \phi(X)$, is dense in the set A where ϕ is open.

4. CONCLUSIONS

We had a few goals in mind when we started to write the present paper. First of all, we wanted to show that most concepts and ideas that arise in mathematical logic have something like an "everyday meaning" for the working mathematician and mathematical physicist. Nonrecursivity is already accepted as a natural, even if weird, situation in today's mathematical practice (Nabutovsky, 1989); the related phenomenon of the nonexistence of algorithms in order to solve specific mathematical problems is again well known and much explored (Davis, 1989). Forcing techniques have allowed the proof of many specific independence results in set theory, set-theoretic topology, analysis, and even in algebra (Juhász, 1989); they are examples of the Gödel incompleteness phenomenon within "standard" mathematics.

Gödel incompleteness was first discovered within formalized arithmetic, and formal arithmetic turned out to be essentially the theory of Diophantine equations. When we embed the theory of Diophantine equations within, say, analysis, we import the whole conceptual structure of mathematical logic into the language of analysis. We can therefore obtain sentences within an extended axiomatic framework T (such as Zermelo–Fraenkel set theory) that are T-equivalent to arithmetical sentences. As a result, the translation of logical questions into commonplace mathematical problems becomes an essentially mechanical procedure. Diophantine questions are "hard"; they deal with discrete, denumerable objects related through algebraic equations. Differential geometric questions handle continuous, nondenumerable objects with the help of differential equations. Yet we have shown that some intractable problems in geometry are difficult because they are equivalent to Diophantine problems. Actually we went beyond that; we have shown that, given any Diophantine problem, we can obtain a whole family of equivalent problems within geometry. Therefore we will find within dynamical systems theory infinitely many problems which are equivalent not only to Fermat's Conjecture, but also to Goldbach's Conjecture or to Riemann's Hypothesis.

Fermat's Conjecture is thus a symbol. We have shown that it does not stand isolated within the theory of Diophantine equations; equivalently difficult questions with a naive presentation may pop up anywhere within mathematics and even within any applied mathematical domain.

ACKNOWLEDGMENTS

The main ideas for the present paper were developed while F.A.D. was a Senior Fulbright Scholar at the Institute for Mathematical Studies in the Social Sciences, Stanford University, and have been announced without proofs elsewhere (da Costa and Doria, 1991*a*). F.A.D. wishes to thank Prof. Patrick Suppes for his hospitality at the IMSSS and for many enlightening discussions on the meaning of the present results and related phenomena, as well as for pointing out the relevance of Richardson's paper (1968) to our work. N.C.A.dC and F.A.D. also wish to thank Prof. Morris Hirsch for a detailed criticism of related results.

We acknowledge support from the Fulbright Commission, CNPq (Brazil), Fapesp, and CEPG-UFRJ.

NOTE ADDED IN PROOF

Recently A. Wiles announced during a series of conferences at Cambridge University a proof of Fermat's Conjecture, which is still being evaluated but which is generally believed to be correct.

REFERENCES

Afraimovich, V. S., Bykov, V., and Shil'nikov, P. (1983). *Transactions of the Moscow Mathematical Society*, **44**(2), 153.

Burgin, M. S. (n.d.). Personal communication to F. A. Doria.

Cornell, G., and Silvermann, J., eds. (1986). *Arithmetic Geometry*, Springer, Berlin.

Da Costa, N. C. A., and Doria, F. A. (1991*a*). Structures, Suppes predicates, and Boolean-valued models in physics, in *Essays in Honor of V. Smirnov on his 60th Birthday*, J. Hintikka and P. Bystrov, eds., Kluwer, Dordrecht.

Da Costa, N. C. A., and Doria, F. A. (1991*b*). Suppes predicates for classical physics, *Proceedings of the San Sebastián Congress on Scientific Structures*, A. Ibarra, ed.

Da Costa, N. C. A., and Doria, F. A. (1991*c*). *Foundations of Physics Letters*, **4**, 363.

Da Costa, N. C. A., and Doria, F. A. (1991*d*). *International Journal of Theoretical Physics*, **30**, 1041.

Da Costa, N. C. A., and Doria, F. A. (1991*e*). Sur l'incomplétude formelle de la mécanique classique, preprint.

Da Costa, N. C. A., and Doria, F. A. (1993). Suppes predicates and the construction of unsolvable problems in the axiomatized sciences, in *Patrick Suppes, Mathematician, Philosopher*, P. Humphreys, ed., Kluwer, Dordrecht.

Da Costa, N. C. A., Doria, F. A., and de Barros, J. A. (1990). *International Journal of Theoretical Physics*, **29**, 935.

Da Costa, N. C. A., Doria, F. A., and Tsuji, M. (1992*a*). The incompleteness of the theory of finite noncooperative games with Nash equilibria, preprint CETMC-17.

Da Costa, N. C. A., Doria, F. A., Furtado do Amaral, A. F., and de Barros, J. A. (1992*b*). Two questions on the geometry of gauge fields, *Foundations of Physics*, to appear.

Davis, M. (1982). *Computability & Unsolvability*, 2nd ed., Dover, New York.

Davis, M. (1989). Unsolvable problems, in *Handbook of Mathematical Logic*, J. Barwise, ed., North-Holland, Amsterdam.

Edwards, H. M. (1977). *Fermat's Last Theorem*, Springer, Berlin.

Ehrenfeucht, A., and Mycielski, J. (1971). *Bulletin of the AMS*, **77**, 366.

Gödel, K. (1986). On the length of proofs, in *Kurt Gödel: Collected Works* I, S. Feferman *et al.*, eds., Oxford University Press, Oxford.

Gödel, K. (1990). Remark on non-standard analysis, in *Kurt Gödel: Collected Works* II, S. Feferman *et al.*, eds., Oxford University Press, Oxford.

Hirsch, M. (1985). The chaos of dynamical systems, in *Chaos, Fractals and Dynamics*, P. Fischer and W. R. Smith, eds., Dekker, New York.

Holmes, P. J., and Marsden, J. (1982). *Communications in Mathematical Physics*, **82**, 523.

Juhász, I. (1989). Consistency results in topology, in *Handbook of Mathematical Logic*, J. Barwise, ed., North-Holland, Amsterdam.

Matijasevič, Y., and Robinson, J. (1975). *Acta Arithmetica*, **27**, 521.

Nabutovsky, A. (1989). *Bulletin of the AMS* (New Series), **20**, 61.

Ribenboim, P. (1989). *The Book of Prime Number Records*, Springer, Berlin.

Richardson, D. (1968). *Journal of Symbolic Logic*, **33**, 514.

Rogers, H., Jr. (1967). *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York.

Stewart, I. (1991*a*). *Nature*, **352**, 664–665.

Stewart, I. (1991*b*). *Nonlinear Science Today*, **1**(4), 8.

Tarski, A. (1948). A Decision Method for Elementary Algebra and Geometry, The Rand Corporation.

Wang, P. (1974). *Journal of the ACM*, **21**, 586.

Wolfram, S. (1984). *Communications in Mathematical Physics*, **96**, 15.