Logique & Analyse **153-154** (1996), 165-182

SOME NEW INCOMPLETENESS THEOREMS AND THEIR IMPORT TO THE FOUNDATIONS OF MATHEMATICS[1]

Francisco Antonio DORIA[2]

Abstract
We summarize our recent results on the incompleteness of classical first-order axiomatic theories and discuss their import to the foundations of mathematics.

1. *Motivation*

Current common wisdom on the foundations of mathematics can be summarized as follows:

> Axiomatic set theory, that is, Zermelo-Fraenkel set theory (ZF) with portions of the Axiom of Choice is enough for essentially all of classical analysis; if we conveniently extend that theory we can include all of our everyday mathematical fare together with some borderline results. That means: we can reproduce all standard mathematical results within axiomatic set theory; moreover, with the help of Bourbaki structures and Suppes predicates we can axiomatize large portions of physics and of the mathematically-based empirical sciences.
>
> Zermelo-Fraenkel theory is also intuitively sound. Its axioms more or less mirror our intuitions about sets in the "real world," that is, in our ordinary, everyday experience. We may argue that there are difficulties with axioms that generate large sets of mostly "undetermined" elements, such as the Power Set Axiom or strong forms of the Axiom of Infinity. But philosophical discussions can take care of those difficulties; on the practical side we can say that those "difficult" axioms are also intuitively valid, as reasonable extensions of our everyday experience.

[1] Partially supported by FAPESP and CNPq (Brazil).

[2] Permanent address: *Project Griffo*, School of Communications, Federal University at Rio de Janeiro, Av. Pasteur, 250, 22295-900 Rio RJ Brazil.

However axiomatic set theory is marred by the incompleteness (or Gödel) phenomenon, as any first-order theory that includes formal arithmetic. Incompleteness means that there are pairs of sentences ξ, and the negation of ξ, in one such theory T which turn out to be unprovable (granted that T be consistent), that is, $T \nvdash \xi$ and $T \nvdash \neg\xi$. Does that matter? According to several authors, that phenomenon is irrelevant: René Thom believes that those undecidable sentences are just "warning posts" which tell us that one shouldn't go further in directions that —as he asserts— do not matter for mathematics. Anyway, Thom believes, Gödel sentences lie far away from the actual heart of mathematical activity, which (again according to Thom's statement of faith) is perfectly decidable [44]. More recently, John Casti has also suggested that the Gödel incompleteness phenomenon is a "red herring," and that it has no import to mathematical practice [5, 6], if we take for granted the physicist's view that the universe is both finite and composed of discrete particles.

The point is: the Gödel phenomenon will matter for mathematics if there are *simple, easily understandable* questions which arise in our everyday experience and which (in a reasonable formalization) can be shown to give rise to an undecidable sentence in set theory. If not, the Gödel phenomenon is in fact irrelevant.

We are going to consider here two possibilities that may perhaps give rise to those *simple, easily understandable* questions related to Gödel-undecidable sentences in set theory. Recall that T, the main axiomatic theory we consider in this paper, includes (in a proper or improper way) Zermelo-Fraenkel theory with the full Axiom of Choice. Those possibilities are sketched below, together with a previous example dealt with by the author elsewhere [20].

The first example: Mrs. H.'s problem

Our prime candidate for one of those questions arises out of the following story:

> Mrs. H. is a gentle and able lady who has long been the secretary of a large university department. Every semester Mrs. H. is confronted with the following problem: there are courses to be taught, professors to be distributed among different classes of students, large and small classes, and a shortage of classrooms of varying sizes. She fixes a minimum acceptable level of overlap among classes and students and sets down (in a tentative way) to get the best possible schedule, given that minimum desired overlap. It's a tiresome task, and in most cases (when there are many new professors, or when the dean changes the classroom allocation system) Mrs. H. feels that she has to check every conceivable scheduling before she is able to reach a conclusion. In

despair she asks a professor whom she knows has a degree in math: *"tell me, can't you find in your math an easy way of scheduling our classes with a minimum level of overlap among them?"*

Mrs. H.'s question is our best candidate for a simple, intuitive, everyday question that gives rise to a set-theoretic undecidable sentence. We believe that if mathematics (seen as axiomatic set theory) cannot answer a simple, everyday query like that, it is definitely at fault, and one must rethink the whole foundational question.

For a more complete (and technical) discussion of Mrs. H.'s question see below Section 3.

The second example: a version of Rice's Theorem in analysis

Mrs. H.'s question is for sure our best bet in that direction, but there are other possibilities to be considered here that may also illuminate the relevance of Gödel's phenomenon. Rice's Theorem is a devastating result in theoretical computer science. It can be reasonably paraphased in an intuitive vein: there is no general decision procedure to test for properties of the output of arbitrary classes of programs.

Let's be a bit more technical. Notation, conceptual starting-points and proofs can be found in [19, 36, 38]. (But we'll try to make things as intuitive and self-contained as possible.) We say that $\mathcal{C}$ is an *index set of algorithms* (of *programs*, that is, partial recursive functions) if, given an algorithm $\phi \in \mathcal{C}$ and if, given another algorithm ψ, for all positive integers n in both domains, $\phi(n) = \psi(n)$, then $\psi \in \mathcal{C}$. An index set $\mathcal{C}$ is *trivial* if either $\mathcal{C} = \varnothing$ or $\mathcal{C}$ equals the set of all programs. Then:

Proposition 1.1 (Rice's Theorem.)

1. *$\mathcal{C}$ is recursive if and only if it is trivial.*
2. *$\mathcal{C}$ is nonrecursive if and only if it is nontrivial.* □

The practical consequence is: we are given a program and we wish it to have a specific behavior (say, to be fast and to give a desired output). Rice's Theorem asserts that there is no general recipe to test for the program's behavior. So, debugging of programs will always be a tentative, empirical procedure. No general procedure is available here.

Now suppose the following: let $P(x)$ be any set-theoretic predicate. Let a be a set. Given those general conditions, under which circumstances can we check whether $T \vdash P(a)$ or $T \vdash \neg P(a)$? The not so surprising answer to that question is given below in Section 2. It is due to da Costa and Doria, and assuredly shows that against Thom's hopeful thinking, the Gödel phenomenon lies at the very heart of everyday mathematics.

The third example: where does randomness come from?
One third example (not discussed in this paper) has to do with a much-debated philosophical question, the concept of randomness. Where does randomness stem from? Take a Bernouilli shift, the set of all (infinite) possible outcomes in a game of heads and tails. That set is isomorphic to the set of all two-sided infinite binary sequences over the alphabet $\{0,1\}$. Now eliminate from those sequences the ones with a prescribed (recursive) generating rule. We are left with the set of truly random sequences in our Bernouilli shift. Properties such as the shift's positive entropy and the like seem arise out of those irregular, nonrecursive sequences.

Now the trick. Formalize everything within Zermelo-Fraenkel set theory. Choose a particular model for our formal contruction. For example, a model which satisfies $\mathbf{V} = \mathbf{L}$, Gödel's Axiom of Constructibility. Random sequences in the shift within that model will be constructive in Gödel's sense. Expand the constructive model to a forcing extension that obeys (in an adequate way) Martin's Axiom. There will be a whole plethora of "new" random sequences in the expanded model, and *the constructive set of sequences will have zero measure* in the new model. So, properties that characterize randomness in the shift in the extended model, such as its entropy *will solely depend on the newly added sequences!* Where does randomness come from? Certainly not from a particular set of trajectories for the shift, as shown by the example. We can easily concoct here a set-theoretic formally undecidable sentence which relates to that situation [20].

There are simple noncomputable expressions for functions within mathematics; those expressions creep up even within languages close to arithmetic, and again lead to very simple questions such as, "does the integer-valued function $\theta(n)$ equal 0 or 1?" which turn out to be undecidable in the general case. Analogous naïve-looking but intractable expressions for functions can also be found within more elaborate languages, as classical elementary analysis. With their help we can generate infinitely many undecidable sentences with a trivial appearance from arithmetic on and all the way up to the whole of mathematics. Some of those intractable expressions represent the *halting function* $\theta(m, n)$, that tells us whether the Turing machine $M_m(n)$ stops over its input n. Once we have an expression for the halting function, we can obtain explicit expressions for all complete arithmetic degrees and even beyond. We can also concoct associated undecidable predicates which represent problems in all the corresponding degrees of unsolvability, both inside and outside the arithmetic hierarchy.

Previous work and an acknowledgment

Several of the results that are presented here are to be found in the papers [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 22, 23, 24, 25, 26]; other references are

[3, 31, 39, 40, 41]. More critical discussions and appraisals of some of those results are found in [29, 30, 34]. The author wishes to point out that the work discussed here arises out of a joint program carried out with N. C. A. da Costa since the late 80's; in particular, the results in Section 2 were first discussed in a joint informal seminar in December 1996 and appear here for the first time.

2. *Rice's Theorem in Classical Analysis*

We suppose that our discussion takes place within an axiomatic framework flexible enough to include arithmetic and elementary calculus; such is our T. For all practical purposes we deal here with a first-order classical axiomatic theory T which includes ZFC (or at least some portion of the Axiom of Choice). The language L_T of T can be extended with the use of descriptions; that use will be admitted throughout this paper. New symbols are introduced by contextual definition. A model $\mathbf{M}$ will be called *standard* if its arithmetic segment is standard; if not, the model is *nonstandard*.

The halting function

We can find some very simple expressions for the halting function in theoretical computer science within theories close to elementary arithmetic. Two of them are given here:

Lemma 2.1 The Turing machine $M_m(n)$ of index m halts over n if and only if $\theta(m, n) = 1$; $M_m(n)$ doesn't halt over n if and only if $\theta(m, n) = 0$, where θ is given by:

$$K(m, n) = \int_{\mathbf{R}_q} c(m, n, x_1, ..., x_q) \exp[-((x_1)^2 + ... + (x_q)^2)]\, d\Omega,$$

$$\theta(m, n) = \sigma K(m, n). \square$$

θ is the halting function of computer science [33, 36]. This Lemma shows that an expression for it exists within classical analysis. For the proof see [8]. c is obtained out of Richardson's transforms (see the reference); σ is the sign function: $\sigma(\pm|x|) = \pm 1$, $x \neq 0$, and $\sigma(0) = 0$.
Remark 2.2 A still nicer expression for the halting function is available within simple extensions of arithmetic [19]; one only has to be able to make infinite sums in order to obtain it. Let $p(n, \mathbf{x})$ be a 1-parameter universal polynomial; $\mathbf{x}$ abbreviates $x_1, ..., x_p$. Then either $p^2(n, \mathbf{x}) \geq 1$, for all $\mathbf{x} \in \omega^p$, or there are $\mathbf{x}$ in ω^p such that $p^2(n, \mathbf{x}) = 0$ sometimes. As $\sigma(x)$

when restricted to ω is primitive recursive, we may define a function $\psi(n, \mathbf{x}) = 1 - \sigma p^2(n, \mathbf{x})$ such that:

- Either for all $\mathbf{x} \in \omega^p$, $\psi(n, \mathbf{x}) = 0$;
- Or there are $\mathbf{x} \in \omega^p$ so that $\psi(n, \mathbf{x}) = 1$ sometimes.

Thus the halting function can be represented as:

$$\theta(n) = \sigma\,[\sum_{\tau^q(\mathbf{x})} \frac{\psi(n,\mathbf{x})}{\tau^q(\mathbf{x})!}],$$

where $\tau^q(\mathbf{x})$ denotes the positive integer given out of $\mathbf{x}$ by the pairing function τ: if τ^q maps q-tuples of positive integers onto single positive integers, $\tau^{q+1} = \tau(x, \tau^q(\mathbf{x}))$.

Moreover, given any family of Diophantine equations $p(n, \mathbf{x}) = 0$ parametrized by $n \in \omega$, we can obtain a halting-like function $\theta_p(n)$ such that it equals 1 whenever $p(n, \ldots) = 0$ has integer roots, and equals 0 if it has no such roots. The procedure for the construction of θ_p goes as in the construction of the halting function $\theta(m, n)$. □

The halting function leads to a general undecidability and incompleteness theorem

In 1990 (published 1991), da Costa and Doria proved a theorem with a formulation similar to Rice's Theorem within the language of classical analysis ([8], Prop. 3.28; [19]). Given a formal version of the language of beginning advanced calculus, where we only handle elementary functions and calculus operations (that is, polynomials, sines and cosines, exponentials, special constants such as π and e, the absolute value function $|x|$, derivatives and integrations over simple domains in $\mathbb{R}^n$) we obtain a result that immediately leads to a surprisingly user-friendly technique to prove undecidability and incompleteness theorems in the formal counterpart of classical mathematics.

We need a few definitions:

Definition 2.3

1. *Nontrivial P. P is nontrivial if and only if there is a closed term t such that P (t) is a theorem of T, and there is a closed* t' *such that ¬P (t') is a theorem of T.*
2. *Trivial P. P is trivial if and only if for every t P (t) isn't a theorem of T, or for every t, ¬P (t) isn't a theorem of T.*
3. *Incomplete P. P is incomplete if and only if there is a t such that: P (t) isn't a theorem of T and ¬P (t) isn't a theorem of T.*

4. *Complete P. P is complete if and only if: for every t either P (t) is a theorem of T, or ¬P (t) is a theorem of T.*
5. *Decidable P. P is decidable if and only if: either the set x_P of all closed terms t such that P (t) is provable, is a recursive set; or the set $x_{\neg P}$ of all t such that ¬P (t) is provable, is recursive.*
6. *Undecidable P. Both x_P and $x_{\neg P}$ aren't recursive.* □

Remark 2.4 Notice that if *P* is trivial, one may have to consider the possibility that it is also incomplete. □

In order to proceed we need a lemma which depends on the assumption that *T* be *arithmetically consistent*, that is, that one of its models has a standard arithmetic portion [8]:

Lemma 2.5 There is an explicit expression for a function β *such that* $T \vdash \beta = 0$ *or* $\beta = 1$*, while neither* $T \vdash \beta = 0$ *nor* $T \vdash \beta = 1$.

Proof: Follows from the fact that the θ function has a recursively enumerable set of nonzero values, with a nonrecursive complement, and from the existence of a Diophantine equation which has no roots in the standard model for arithmetic, while that fact can neither be proved nor disproved in *T*. □

Then:

Proposition 2.6 If P is nontrivial, then it is incomplete.

Proof: From Lemma 2.5, we form the term $\iota_x \{(x = t_0 \wedge \beta = 1) \vee (x = t_1 \wedge \beta = 0)\}$, where $T \vdash P(t_0)$ and $T \vdash \neg P(t_1)$. Clearly

$$T \nvdash P(\iota_x \{(x = t_0 \wedge \beta = 1) \vee (x = t_1 \wedge \beta = 0)\}),$$

and

$$T \nvdash \neg P(\iota_x \{(x = t_0 \wedge \beta = 1) \vee (x = t_1 \wedge \beta = 0)\}). \square$$

Then comes our version of Rice's Theorem:

Proposition 2.7 P is nontrivial if and only if P is undecidable.

Proof: Use the term $\iota_x \{(x = t_0 \wedge \theta(n) = 0) \vee (x = t_1 \wedge \theta(n) = 1)\}$. Then:

- *Nontrivial ⇒ Undecidable.* Immediate.
- *Undecidable ⇒ Nontrivial.* Take the negation, *trivial ⇒ decidable*, and the result follows from Definition 2.3. □

Proposition 2.8 If for every t, P (t) is provable, or if for every t, ¬P (t) is provable, then P is trivial. □

So, there are no decision procedures for nontrivial predicates. The limitation is a drastic one: we can't even decide whether an arbitrary expression in the language of analysis equals 0. Another example: if n is any integer, put $n + r\theta\ (q)$, where r is an irrational and $\theta\ (q)$ is the halting function; then we cannot in general decide whether an arbitrary member of that family of expressions is an integer or an irrational number.

More incompleteness results

We quote here a general undecidability and incompleteness result that originates in our ideas:

Proposition 2.9

1. *Given any nontrivial predicate P in T, there is an infinite denumerable family of expressions* ξ_m *such that for those m with* $T \vdash P\ (\xi_m)$, *for an arbitrary total recursive function* $g : \omega \rightarrow \omega$, *there is an infinite number of values for m such that the shortest length* $C_T\ (P\xi_m)$ *of a proof of* $P\xi_m$ *in T satisfies* $C_T\ (P\xi_m) > g\ (\|P\xi_m\|)$. *(*$\|...\|$ *denotes the length of the expression.).*
2. *Given any nontrivial predicate P in T, there is one of those expressions* ξ *such that* $T \vdash P\ (\xi)$ *if and only if* $T \vdash$ *Fermat's Conjecture.*
3. *There is an expression* ξ *such that for a nontrivial P, P* (ξ) *is T-arithmetically expressible as a* Π_{m+1} *problem, but not as any* Σ_k *problem,* $k \leq m$.
4. *There is an expression* ξ *so that P* (ξ) *isn't arithmetically expressible* [19]. □

Consequences

For a review of the main consequences of the preceding results see [10, 19, 39, 40, 41]. We would like to quote here just two of them:

- *Is there a decision procedure for chaos?* Chaos theory has been a fast-growing research area since the early 70's, a decade after the discovery of an apparently chaotic behavior in a deterministic nonlinear dynamical system by E. Lorenz (for references see [8, 41]). Chaos scientists usually proceed in one of two ways: whenever they wish to know if a given physical process is chaotic the usual starting point is to write down the equations that describe the process and out of them to check whether the process satisfies some of the established mathematical criteria for chaos and randomness.

However those equations are in most cases intractable nonlinear differential equations as they cannot in general be given explicit analytical solutions. Therefore, chaos theorists turn to computer simulations and for most nonlinear systems one sees a confusing, tangled pattern of trajectories on the screen. The system *looks* random, and there are statistical tests such as the Grassberger-Proccacia criterion that guarantee the existence of randomness in computer-simulated systems, modulo some error. Yet statistical tests furnish no *mathematical* proof of the existence of chaos in a dynamical system. There is always the chance that the system is undergoing a very long and complicated transient state, before it settles down to a nice and regular behavior. Therefore how can we prove that a dynamical system that *looks* chaotic is, in fact, chaotic?

This problem had been around since the discovery and early exploration of what is now called "deterministic chaos." In a 1983 conference (published in 1985) Morris Hirsch stated that time was ripe for a marriage between the "experimental" and "theoretical" sides of chaos research and posed the decision problem for chaotic systems [28].

da Costa and Doria showed [8] that no such a decision method exists. Moreover, for any nontrivial characterization of chaos in a dynamical system there will always be systems where proving the existence of chaos is unattainable within standard axiomatizations. Chaos theory and dynamical systems theory are both undecidable —there is no general algorithm to test for chaos in an arbitrary dynamical system— and incomplete —there are infinitely many dynamical systems that will look chaotic on a computer screen, for they are chaotic in an adequate class of standard models for axiomatized mathematics, but such that no proof of that fact will be found within the usual formalizations of dynamical systems theory.

So, Hirsch's query on the existence of an algorithmic criterion for chaos in dynamical systems has a negative answer.

- *The integrability problem in classical mechanics.* That's a question that goes back to the early age of classical mechanics. We quote a recent reference on it [32]:

> Are there any general methods to test for the integrability of a given Hamiltonian? The answer, for the moment, is no. We can turn the question around, however, and ask if methods can be found to construct potentials that give rise to integrable Hamiltonians. The answer here is that a method exists, at least for a restricted class of problems...

We can divide the integrability question into three problems:

- — Given any Hamiltonian h, is there an algorithm to decide whether the associated flow X_h can be integrated by quadratures?
- — Given an arbitrary Hamiltonian h such that X_h can be integrated by quadratures, can we algorithmically find a canonical transformation that will do the trick?
- — Can we algorithmically check whether an arbitrary set of functions is a set of first integrals for a Hamiltonian system?

No, in all three cases. There is no general algorithm to decide, for a given Hamiltonian, whether or not it is integrable. Also, for instance, there will be sentences such as ξ= "h is integrable by quadratures," where however $T \nvdash \xi$ and $T \nvdash \neg\xi$ [8].

3. *Mrs. H.'s Toils and Troubles*

Mrs. H.s's problem is a scheduling problem, which is known to be polynomially equivalent to the satisfiability question [33]. The satisfiability question can be informally stated as follows:

Is there a polynomial Turing machine P *that accepts every Boolean expression x in conjunctive normal form in time polynomial in the length* $|x|$*?*

That is, the machine P *should input a n-variable expression x, polynomially process it and output a binary line of length n which codes a satisfying line in x's truth-table.*

Consider the following facts about Boolean expressions in conjunctive normal form (cnf) and polynomial machines:

1. *There is a representation for polynomial machines which codes every polynomial machine with the help of two integers* $\langle m, n \rangle$. Such a representation is given by the pair $\mathsf{P}_{\langle m,n \rangle} = \langle \mathsf{M}_m(x), |x|^n \rangle$ [2], where m is the Turing machine's Gödel number and n is the exponent of a polynomial clock that terminates any computation of M_m whenever it has operated for $|x|^n$ machine cycles.

   Given an enumeration of the pairs $\langle m, n \rangle$ we can enumerate the set of all polynomial Turing machines in the above representation. Note that set $\mathcal{P}$.
2. *Finite sets of Boolean expressions in cnf and polynomial machines.* Another fact we will require goes as follows: if Sat is the set of all

Boolean expressions in cnf coded over a binary alphabet, let $\beta \subset$ Sat be finite. Then there is a polynomial machine P_k such that it accepts every expression in β and moreover accepts infinitely many expressions from Sat. There is an effective procedure for the construction of P_k.

3. *Machines that accept infinitely many instances of* Sat. Moreover, if P_k accepts infinitely many instances from Sat, and if $\beta \subset$ Sat is finite, then there is a machine P_l which accepts everything that P_k accepts together with the whole of β.

   Again there is an effective procedure to obtain P_l from P_k.

Let us now be given the following predicate:

$$P(k, s, x) \leftrightarrow \mathsf{P}_k(x) = s \wedge \mathsf{V}(s, x) = 1.$$

($\mathsf{V}(s, x)$ is the "verifying machine" that inputs the binary line s and checks whether it satisfies x or not —if it does, it prints 1; if not, 0; it is a time-polynomial machine.) Clearly $P(k, s, x)$ means, "the polynomial machine of index k inputs x, outputs s and the verifying machine checks that s satisfies x." Similarly,

$$A(k, x) \leftrightarrow \exists s\, P(k, s, x)$$

can be given the intuitive translation" P_k accepts x." The polynomial hypothesis for the satisfiability question can therefore be given the following reasonable formalization:

$$\exists k \in \omega, \forall x \in \text{Sat}\ A(k, x).$$

We call that *the Weak Polynomial Hypothesis* (WPH) for the satisfiability question. Granted (2) in the enumeration above, WPH is formally equivalent to:

Definition 3.1 Weak polynomial hypothesis in set theory (WPH).

$$\exists n \in \omega\ \exists k_0 \in \omega\ \forall x_k \in \text{Sat}\ (k > k_0 \rightarrow A(n, x_k)). \square$$

Definition 3.2 Negation of the weak polynomial hypothesis in set theory ($\neg$WPH).

$$\forall n \in \omega\ \forall k_0 \in \omega\ \exists x_k \in \text{Sat}\ (k > k_0 \wedge \neg A(n, x_k)). \square$$

Two conjectured consistency results

We conjecture:

Conjecture 3.3 Consis (ZFC) $\leftrightarrow$ Consis (ZFC + WPH).
We need:

Axiom System 3.4 Extend ZFC *as follows:*
1. *Add a new constant term* ν *to the language of the theory.*
2. *Impose that* P_ν *be a polynomial machine.*
3. *For* $x_i \in$ Sat, *impose:*
   (a) $A(\nu, x_0)$.
   (b) $A(\nu, x_1)$.
   (c) $A(\nu, x_2)$.
   (d) $A(\nu, x_3)$.
   (e) ... □

Call the extended theory ZFC** and recall that $\mathcal{P}$ is the set of all polynomial Turing machines, as characterized above. Then:

Proposition 3.5 ZFC *is consistent if and only if* ZFC** *is consistent.*
Proof: For any finite conjunction $\bigwedge_j A(\nu, x_j) \wedge \mathsf{P}_\nu \in \mathcal{P}$, we can find a model for ZFC**, since there will always be a polynomial machine P_n that accepts the finite set $\{\ldots x_j \ldots\}$. Consistency follows from compacity. Converse is immediate. □

Conjecture 3.6 ZFC** *proves the Weak Polynomial Hypothesis.*
"Proof": Define $a_\nu = \{x \in \text{Sat} : A(\nu, x)\}$.We need that $a_\nu = \text{Sat}$. So, $\mathsf{P}_\nu \in \mathcal{P}$ accepts the whole of Sat. □
Now:

Conjecture 3.7 Consis (ZFC) $\leftrightarrow$ Consis (ZFC + $\neg$WPH).
Again:

Axiom System 3.8 We will now extend ZFC *as follows:*
1. *Add denumerably many new constant terms* $\zeta_{i,j}$, $i, j \in \omega$, *to the language of the theory.*
2. *Recall that it is a theorem of our axiomatic theories that* Sat *is linearly ordered by* <, *with the order type of* ω *and some extra conditions.*
3. *Write the predicate* $P(k, s, x)$.
4. *Impose that the* $\zeta_{i,j} \in$ Sat.
5. *Impose moreover on the* $\zeta_{i,j}$ *the following denumerably infinite set of axioms:*

(a) $\neg P(k, 0, \zeta_{k,j}), \neg P(k, 1, \zeta_{k,j}), \neg P(k, 2, \zeta_{k,j}), \ldots,$ *for each* $j, k \in \omega$.

(b) $K(\zeta_{i,j}) \neq K(\zeta_{i',j'})$, $i \neq i'$, $j \neq j'$ *or both. Here* K *is the Kolmogorov-Chaitin complexity.*

(c) For every $\zeta_{i,j}$ *there are* k_0, s_0, x_0 *such that*

$$(\zeta_{i,j} < x_0) \wedge P(k_0, s_0, x_0).$$

(That is, every $\zeta_{i,j}$ *is somewhere "in the middle of"* Sat.*)* □

Condition (5b) means that the ζ's cannot be recursively generated out of a finite set of expressions in cnf. So, we here deal with truly infinite set, modulo recursive operations. Call that extended theory ZFC*. Then:

Proposition 3.9 ZFC *is consistent if and only if* ZFC* *is consistent.*

Proof: The proposition follows from the compactness theorem and from the preceding results. If $\mathbf{p} \subset \omega$, ..., are finite subsets, and $\langle \ldots \rangle$ denotes the usual recursive 1-1 pairing function, form the conjunctions:

$$\bigwedge_{\langle k,s\rangle \in \mathbf{p}, \ \ldots, \langle k'',s''\rangle \in \mathbf{p}''} \neg P(k, s, \zeta_{k,j}) \wedge \ldots \wedge \neg P(k'', s'', \zeta_{k'',j''}).$$

Given that conjunction above, we can always simultaneously choose a finite set of Boolean expressions in cnf $\{\zeta_{k,j}, \ldots\}$ so that:

- Let $l = \max\{|s|, |s'|, |s''|, \ldots\}$.
- We can choose $z_{k,j}$ such that their satisfying lines $t, t'', \ldots$ obey $l < |t| < |t'| < \ldots$.

  Therefore the $z_{k,j}$ satisfy the conjunction above.
- Their corresponding Kolmogorov-Chaitin complexities are larger than the largest complexity of the satisfiability lines in the conjunction, which are given by the codings $s, s'', \ldots$.
- For axiom (5c), take the truth-table generating machine T and form the polynomial machine $\mathsf{P}_{k_0} = \langle \mathsf{T}, |\ldots|^{n_0} \rangle$, $n_0 > 2$. Then that machine will accept most expressions in Sat [16], and we will easily find one x_0 accepted by P_{k_0} with the desired properties, that is, $z_1 < z_2 < \ldots < z_k < x_0$ in the ordering induced on Sat. Out of that fact we can easily obtain another machine $\mathsf{P}_{k'_0}$ which accepts all those elements accepted by P_{k_0} plus the $z_1, \ldots, z_k$. Since that is a general construction, by compactness we have our result. □

Remark 3.10

- We just ask of the exceptional language for P_i, $\tilde{\zeta}_i = \{\zeta_{i,j}\}$, all j, that it be rejected by that algorithm P_i. Finite subsets of them will necessarily be accepted by different algorithms, since that's a theorem of ZFC. (See above.)
- Now write $\tilde{\zeta} = \{\tilde{\zeta}_i\}$. We can state it more precisely: every $\zeta_{i,j}$ will be accepted by some $\mathsf{P}_{n'}$, that is, there are infinitely many nonempty $\alpha_{n'}$ (the language accepted by $\mathsf{P}_{n'}$) such that $\tilde{\zeta} \cap \alpha_n \neq \emptyset$, and that intersection is at least finite. Yet every polynomial machine P_n admits a P_n-exceptional language which is rejected by it, and that language is an infinite subset $\tilde{\zeta}_n \subset \tilde{\zeta}$.
- Moreover, due to its unbounded KC-complexity, such a sequence cannot be recursively generated out of any finite string.
- Also the choice of the $\zeta_{k,j}$ determines those $\zeta^g_{k,j}$ which cannot be accepted by the algorithm $g\mathsf{P}_i$ where g is a recursive permutation.
- Finally notice that no exceptional language $\{\zeta_{i,j}\} \subset \mathrm{Sat}$, $j \in \omega$, can be accepted *in totum* by some polynomial algorithm $\mathsf{P}_{i'}$. For if it were so, due to the completeness of the set of polynomial languages, that language would be polynomial [33]. □

Conjecture 3.11 ZFC* *disproves the Weak Polynomial hypothesis, that is:*

$$\mathrm{ZFC}^* \vdash \neg\,(\exists n \in \omega\ \exists k_0 \in \omega\ \forall x_k \in \mathrm{Sat}\ (k > k_0 \rightarrow \exists s\,(P\,(n, s, x_k)))).$$

"Proof": Suppose that ZFC* proves WPH. Then there is an n_0 such that, for every $x \in \mathrm{Sat}$, there will be an s such that $P\,(n_0, s, x)$. However, given one such algorithm P_{n_0} the axioms of ZFC* should allow us to find an exceptional language for it, namely the set of constants $\{\zeta_{n_0,j}\} \subset \mathrm{Sat}$, for all $j \in \omega$. This would contradict our hypothesis, and our result would follow by *modus tollendo tollens*. □

So, it would turn out that WPG is independent of the axioms of ZFC, supposed consistent.

4. *Comments*

Back to the question we asked at the beginning of this paper: is set theory enough for mathematics? We pointed out [20] that there are problems with important concepts such as randomness when they are framed within axiomatic set theory. Well, but here the trouble may perhaps arise out of an inadequate construction of the concept of randomness. Let us elaborate a bit on this point: we can show that satisfiability problems of maximum Kolmogorov-Chaitin complexity have low computational complexity. (They are actually are low-degree polynomial problems.) So the two formal concepts, computational complexity and Kolmogorov-Chaitin complexity, do not match [24], even if their intuitive starting points are similar.

Our results as presented in Section 2 seem to tip a bit more the scales against axiomatic set theory, as they show that Gödel incompleteness affects *every interesting predicate we can think about*. Think for instance that given a complicated expression which represents a real number, there is no algorithm to check whether it is algebraic or transcendental, and that there will be some expressions (in ZFC) for real numbers whose transcendentality is formally undecidable!

Mrs. H.'s problem perhaps tells us the source of those troubles.[3] Given the much required *caveat*, that the WPH adequately translates Mrs. H.'s question, then we will have here an example of a very simple, easily understood mathematical question *which cannot be decided by mathematical tools as found in axiomatic set theory*. The point is: while the satisfiability question is more easily framed within arithmetic, the independence result we presented shows that it gains nothing from the (supposedly stronger) set-theoretic axioms.

We cautiously suggest that this might indicate an essential cleavage between set theory and arithmetic; as if they belonged to different conceptual domains, with however a few points of intersection. Set theory was born within classical analysis, and that is the area where we can best formalize ordinary intuitive mathematics with set-theoretic concepts. Perhaps our troubles with large cardinals and the like arise from the fact that classical analysis has very little or nothing in fact to (intuitively) say about them. And, also, set theory has very little to tell us about arithmetic, which is sort of clumsily integrated into the set-theoretical universe.

Whereas Mrs. H.'s troubles.

ACKNOWLEDGMENTS

The author acknowledges a suggestion by John Casti that they should synthetize and summarize their main argument on the satisfiability problem; a clarification of his remarks on the Gödel phenomenon is also acknowledged. Comments by Jean-Yves Béziau and Maurício Kritz have also

[3]While still unpublished, our paper [21] with the complete discussion of the independence of the Weak Polynomial Hypothesis for the satisfiability problem underwent an informal refereeing process with at least nonnegative results, that is, so far no mistakes have been found in our arguments.

helped in clarifying our discussion. Support is acknowledged from a number of agencies: CNPq (Philosophy program), FAPESP, FAPERJ (who gave the author a grant that supported Casti's July 1996 visit to Rio) and the PREVI Program at the UFJF, where earlier versions of this paper have been discussed.

Help and encouragement from Emmanuel Carneiro Leão and Muniz Sodré are also gratefully acknowledged, as well as full support from Marcus Palatnik, Dean for Graduate Studies at Rio's Federal University and from its Rector Magnificus Paulo Gomes.

Formatting of this text is due to *Project Griffo* at the School of Communications, Federal University at Rio de Janeiro.

Department of Physics, Institute for the Exact Sciences (ICE),
Federal University at Juiz de Fora. Campus de Martellos.
36036-330 Juiz de Fora MG Brazil.
doria@omega.lncc.br
doria@fisica.ufjf.br

REFERENCES

[1] S. Albeverio, J. E. Fenstad, R. Hoegh-Krohn, T. Lindstrom, *Nonstandard Methods in Stochastic Analysis and Mathematical Physics*, Academic Press (1986).
[2] T. Baker, J. Gill, R. Solovay, *SIAM J. Comput. 4*, 431 (1975).
[3] J. Casti, *Reality Rules II*, John Wiley (1992), pp. 350-351.
[4] J. Casti, message to the 'Limits' BBS (1994).
[5] J. Casti and J. Traub, editors, *On Limits*, Santa Fe institute (1994).
[6] J. Casti and A. Karlqvist, *Boundaries and Barriers*, Addison-Wesley (1996).
[7] N. C. A. da Costa and R. Chuaqui, *Erkenntnis 29*, 95 (1988).
[8] N. C. A. da Costa and F. A. Doria, *Int. J. Theor. Phys. 30*, 1041 (1991).
[9] N. C. A. da Costa and F. A. Doria, *Found. Phys. Letters 4*, 363 (1991).
[10] N. C. A. da Costa and F. A. Doria, *Philosophica 50*, 901 (1992).
[11] N. C. A. da Costa and F. A. Doria, "Suppes Predicates for Classical Physics," in J. Echeverría et al., eds., *The Space of Mathematics*, Walter de Gruyter, Berlin-New York (1992).
[12] N. C. A. da Costa and F. A. Doria, "On the Existence of Very Difficult Satisfiability Problems," *Bulletin of the Section of Logic*, (University of Ł odz) *21* # 4, 122 (1992).
[13] N. C. A. da Costa and F. A. Doria, *Metamathematics of Physics*, to appear.

[14] N. C. A. da Costa and F. A. Doria, "On Arnol'd's Hilbert Symposium Problems," in G. Gottlob, A. Leitsch, D. Mundici, eds., *Proceedings of the 1993 Kurt Gödel Colloquium: Computational Logic and Proof Theory*, Lecture Notes in Computer Science *713*, Springer (1993).
[15] N. C. A. da Costa and F. A. Doria, "Suppes Predicates and the Construction of Unsolvable Problems in the Axiomatized Sciences," in P. Humphreys, ed., *Patrick Suppes, Mathematician, Philosopher II*, Kluwer (1994).
[16] N. C. A. da Costa and F. A. Doria, *Philosophia Naturalis 31*, 1 (1994).
[17] N. C. A. da Costa and F. A. Doria, *Int. J. Theor. Phys. 33*, 1913 (1994).
[18] N. C. A. da Costa and F. A. Doria, *Studia Logica 55*, 23 (1995).
[19] N. C. A. da Costa and F. A. Doria, *Complexity 1* # 3, 40 (1995).
[20] N. C. A. da Costa and F. A. Doria, "Structures, Suppes Predicates and Boolean-Valued Models in Physics," in J. Hintikka and P. Bystrov, eds., *Festschrift in Honor of Prof. V. Smirnov on his 60th Birthday*, Kluwer (1996).
[21] N. C. A. da Costa and F. A. Doria, "Independence of WPH for the Satisfiability Problem from the Axioms of Set Theory," 11th Brazilian Symposium on Artificial Intelligence, Curitiba (PR, Brazil, 1996).
[22] N. C. A. da Costa, F. A. Doria and A. F. Furtado do Amaral, *Int. J. Theor. Phys. 32*, 2187 (1993).
[23] N. C. A. da Costa, F. A. Doria and J. A. de Barros, *Int. J. Theor. Phys. 29*, 935 (1990).
[24] N. C. A. da Costa, F. A. Doria and D. Krause, "Metamathematical Results on the Satisfiability Problem, I" preprint CETMC-30 (1994).
[25] N. C. A. da Costa, F. A. Doria and M. Tsuji, "The Incompleteness of Finite Games with Nash Equilibria," preprint CETMC-17 (1997).
[26] N. C. A. da Costa, F. A. Doria, A. F. Furtado do Amaral, J. A. de Barros, *Found. Phys. 24*, 783 (1994).
[27] A. Ehrenfeucht and J. Mycielski, *Bull. AMS 77*, 366 (1971).
[28] M. Hirsch, "The Chaos of Dynamical Systems," in P. Fischer and W. R. Smith, *Chaos, Fractals and Dynamics*, M. Dekker (1985).
[29] J. Horgan, "Anti-Omniscience: An Eclectic Gang of Thinkers Pushes at Knowledge's Limits," *Scientific American 271*, 12 (August 1994).
[30] J. Horgan, *The End of Science*, 231 ff., Addison-Wesley (1996).
[31] A. A. Lewis and Y. Inagaki, "On the Effective Content of Theories," preprint, U. of California at Irvine, School of Social Sciences (1991).
[32] A. J. Lichtenberg and M. A. Lieberman, *Regular and Stochastic Motion*, Springer (1983).

[33] M. Machtey and P. Young, *An Introduction to the General Theory of Algorithms*, North-Holland (1979).
[34] D. Miller, *Critical Rationalism: a Restatement and Defence*, pp. 166 and 236, Open Court, Chicago (1994).
[35] D. Richardson, *J. Symbol. Logic 33*, 514 (1968).
[36] H. Rogers Jr., *Theory of Recursive Functions and Effective Computability*, MacGraw-Hill (1967).
[37] B. Scarpellini, *Z. Math. Logik & Grundlagen d. Math. 9*, 265 (1963).
[38] R. I. Soare, *Recursively Enumerable Sets and Degrees*, Springer (1987).
[39] I. Stewart, *Nature 352*, 664 (1991).
[40] I. Stewart, "Deciding the Undecidable," in *The Problems of Mathematics*, 2nd. ed., Oxford (1992), pp. 308-311.
[41] I. Stewart, "Deciding the Undecidable," in *From Here to Infinity*, Oxford (1996), pp. 270-273.
[42] P. Suppes, *Set-Theoretical Structures in Science*, mimeo., Stanford University (1967).
[43] P. Suppes, *Scientific Structures and their Representation*, preliminary version, Stanford University (1988).
[44] R. Thom, *Parabole e Catastrofi*, Il Saggiatore, Milan (1980).
[45] S. Wolfram, *Commun. Math. Phys. 96*, 15 (1984).