Applied Mathematics and Computation 145 (2003) 655–665
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Consequences of an exotic definition for $P = NP$ ☆

N.C.A. da Costa, F.A. Doria *

Institute for Advanced Studies, University of São Paulo, Av. Prof. Luciano Gualberto, trav. J, 374, São Paulo, SP 05655-010, Brazil

Abstract

We introduce a formal sentence noted $[P = NP]^{\mathsf{F}}$ (the "exotic definition") that is intuitively equivalent to $P = NP$; however $P = NP$ and $[P = NP]^{\mathsf{F}}$ may not be equivalent in ZFC for some choices of F. Again for some F we show that $[P = NP]^{\mathsf{F}}$ is consistent with ZFC, and so is the equivalence $[P = NP]^{\mathsf{F}} \leftrightarrow [P = NP]$. We finally derive a consistency result for $P = NP$ itself.

1. Introduction

Suppose that we are given the following prescription for the computation of a function F^*:

> For each natural number n we are given a finite set of numbers S_n. Then the value $\mathsf{F}^*(n) = \max S_n + 1$. If there is also a recipe for the computation of the elements of S_n, for each n, then we can intuitively conclude that F^* is computable and total, that is, we have a program that computes F^* for each and every natural number n.

☆ Partially supported by CNPq, Philosophy Section, FAPESP, and by UNIP.
* Corresponding author.
E-mail addresses: ncacosta@usp.br (N.C.A. da Costa), fadoria2001@yahoo.com.br (F.A. Doria).

0096-3003/$ - see front matter
doi:10.1016/S0096-3003(03)00176-0

F^* is intuitively total and recursive, once each S_n is recursive, but (depending on the axiomatic framework and on the choice of S_n) we will not be able to prove that F^* is total; see Definition 3.1 in this paper.

Let us put that difficulty aside for a moment. Consider the following:

> A time-polynomial Turing machine (a poly-machine) is a Turing machine that on any binarily coded input x produces an output after less than t operation cycles, where t is bounded by a polynomial function of the length of x.

One should notice that here *any* positive-definite polynomial will do, beyond a fixed minimum degree and constant term for each poly-machine [10].

Now, let us combine both ideas: if $|x|$ is the length of the input x, then, if polynomial $p(|x|)$ bounds the operation time of machine M, for a strictly increasing function f so that $\mathsf{f}(n) > n$, $p(\mathsf{f}(|x|))$ will also bound it.

What will happen if we take $\mathsf{f} = \mathsf{F}$, for an F as a function like those F^* described in the quoted paragraph above and specified in Definition 3.1? The point is: formal systems like Peano Arithmetic (PA) or Zermelo–Fraenkel set theory (ZFC, as we add the Axiom of Choice) cannot "see" whether functions like F are total or not beyond a certain growth rate; F_{ϵ_0} marks the external boundary for PA, and F the same for ZFC [9,12].

There are several philosophical questions to be dealt with here, as functions like F_{ϵ_0} and F are intuitively total—after all, these functions arise as the function sketched at the beginning—but we will ignore them. We will only be interested in the behavior of a ZFC sentence abbreviated $[P = NP]^{\mathsf{F}}$ that—again—intuitively translates as $P = NP$, but that has a non-trivial behavior with respect to ZFC as we use that ZFC-boundary-function F to define the polynomial bound for poly-machines.

That sentence $[P = NP]^{\mathsf{F}}$, the "exotic" formulation, is easily seen to be consistent with ZFC, and from it we can derive a consistency result for $P = NP$ itself.

2. Preliminary concepts and definitions

For "intuitive", "informal mathematics" we mean mathematics as in the everyday practice of a professional mathematician, without any reference to some kind of axiomatic background; "formal mathematics", "formalization", refer to some axiomatic system, which is here taken to be Zermelo–Fraenkel set theory with the Axiom of Choice (ZFC), and some of its extensions which are specified *in loco*.

This introductory section goes from the intuitive to the formal, and compares our exotic formulation for $P = NP$, noted $[P = NP]^{\mathsf{F}}$, to the standard one.

Our blueprint is the Satisfiability Problem for Boolean expressions in conjunctive normal form (cnf); for a review of it see [10].

SAT is the set (adequately coded through binary words) of all satisfiable Boolean expressions in cnf. If ω is the set of all positive integers, SAT $\subset \omega$ is a primitive recursive subset. Thus we can code SAT by ω through a primitive recursive coding, which is supposed here.

2.1. $P = NP$, a first approach

We can informally state the $P = NP$ hypothesis as:

There is a time-polynomial Turing machine M_m that correctly "guesses" a satisfying line of truth-values for every input $x \in$ SAT.

The sketchy, preliminary formulation above can be made more rigorous in several ways. For example:

Definition 2.1 (*Standard formulation for $P = NP$, intuitive version*). There is a Turing machine M_m of Gödel number m, and there are positive integers a, b so that for every $x \in$ SAT, the output $\mathsf{M}_m(x)$ is a satisfying line for x, and the number of cycles of M_m over x, $t_m(x) \leqslant |x|^a + b$.

Within ZFC:

Definition 2.2 (*Standard formalization for $P = NP$*).

$$[P = NP] \leftrightarrow_{\mathrm{Def}} \exists m, a, b \in \omega \forall x \in \omega[(t_m(x) \leqslant |x|^a + b) \wedge R(x, m)].$$

($R(x, y)$ is a polynomial predicate; it subsumes a kind of "verifying machine" that checks whether or not x is satisfied by the output of Turing machine m.)

Definition 2.3. $[P < NP] \leftrightarrow_{\mathrm{Def}} \neg[P = NP]$.

2.2. Formulations for $P < NP$ through Π_2^0 sentences

Convention 2.4. $[P < NP]$ is a Π_2^0 sentence. We will only consider alternative formulations for $P < NP$ that are framed as Π_2^0 sentences.

2.3. An exotic formalization, I

We have dubbed "exotic" the formalization in Definition 2.6 as a reminder of Milnor's exotic spheres: they have the same topology, but exhibit non-equivalent differentiable structures. Here we have an *intuitive* equivalence between the exotic, or better, the infinitely many possible exotic formalizations, and the standard formalization that however does not hold in certain axiomatic systems.

Let f be a 1-variable, strictly increasing, total recursive function:

Definition 2.5 (*An exotic formulation*, *intuitive version*). There is a Turing machine M_m of Gödel number m, and there are positive integers a, b so that for every $x \in \mathrm{SAT}$, the output $\mathsf{M}_m(x)$ is a satisfying line for x, and the number of cycles of M_m over x, $t_m(x) \leqslant |x|^{\mathsf{f}(a)} + \mathsf{f}(b)$.

Follows, for ZFC:

Definition 2.6 (*An exotic formalization for $P = NP$*, *rigorous version*).

$$[P = NP]^{\mathsf{f}} \leftrightarrow_{\mathrm{Def}} \exists m, a, b \in \omega \forall x \in \omega[(t_m(x) \leqslant |x|^{\mathsf{f}(a)} + \mathsf{f}(b)) \wedge R(x, m)].$$

$R(x, y)$ is the polynomial predicate described above.

(However see subsection "An exotic formalization, II".) Informally one easily sees:

Proposition 2.7. *If* f *is total and strictly increasing*, $[P = NP]^{\mathsf{f}} \leftrightarrow [P = NP]$.

Proof (*informal*).

[$\Rightarrow$] It is enough to consider the bounding term: there are $a, b \in \omega$ so that $[t_m(x) \leqslant |x|^{\mathsf{f}(a)} + \mathsf{f}(b)]$. As f is total, we have that for any a, b, there are $\mathsf{f}(a) = a', \mathsf{f}(b) = b'$. Thus the bounding term becomes $[t_m(x) \leqslant |x|^{a'} + b']$.

[$\Leftarrow$] There are $a', b' \in \omega$ so that $[t_m(x) \leqslant |x|^{a'} + b']$. Since f is strictly increasing, there are $a, b \in \omega$ so that $a' \leqslant \mathsf{f}(a), b' \leqslant \mathsf{f}(b)$. Therefore there exist $a, b \in \omega$ such that $[t_m(x) \leqslant |x|^{\mathsf{f}(a)} + \mathsf{f}(b)]$. $\square$

Compare Proposition 2.7 to Propositions 4.7 and 4.9. For Definition 2.6: see below Definition 2.14.

2.4. Notation convention

Convention 2.8. From here on we agree that all quantified variables range over the whole of ω unless specifically noted. Also $Qa, b, \ldots$ (for $Q = \forall$ or $Q = \exists$) means $Qa \in \omega Qb \in \omega \ldots$

2.5. An exotic formalization, II

Now let f be in general a (possibly partial) recursive function, and let e_{f} be the Gödel number of an algorithm that computes f.

Let $p(\langle e_{\mathsf{f}}, b, c\rangle, x_1, x_2, \ldots, x_k)$ be an universal Diophantine polynomial with parameters e_{f}, b, c; for convenience we may take p to be positive definite. Define the predicates:

Definition 2.9. $M_{\mathsf{f}}(x,y) \leftrightarrow_{\mathrm{Def}} \exists x_1, \ldots, x_k[p(\langle e_{\mathsf{f}}, x, y\rangle, x_1, \ldots, x_k) = 0]$.

Remark 2.10. Actually $M_{\mathsf{f}}(x,y)$ stands for $M_{e_{\mathsf{f}}}(x,y)$, or better, $M(e_{\mathsf{f}}, x, y)$; for dependence is on the Gödel number e_{f}. $M_{\mathsf{f}}(x,y)$ in Definition 2.9 means: x input to f produces an output y if and only if Diophantine equation

$$p(\langle e_{\mathsf{f}}, x, y\rangle, x_1, \ldots, x_k) = 0$$

has solutions. So the predicate is well-defined even if f is a partial function.

Definition 2.11. $\neg Q(m, \langle c, d\rangle, x) \leftrightarrow_{\mathrm{Def}} [(t_m(x) \leqslant |x|^c + d) \to \neg R(x,m)]$.

The primitive recursive predicate $\neg Q$ in Definition 2.11 is actually dependent on a and b. However to simplify things we may substitute the pair by a single variable a, that is, we may consider a bounding term of the form $|x|^a + a$. We can also handle the two-variable term through the usual 1–1 pairing function $\langle \ldots \rangle : \omega \times \omega \to \omega$.

Definition 2.12 (*Another version of the standard formalization*). $[P < NP] \leftrightarrow_{\mathrm{Def}} \forall m, a \in \omega \exists x \in \omega \neg Q(m, a, x)$.

Here a stands for $\langle b, c\rangle$. From Definition 2.12:

Definition 2.13. $[P = NP] \leftrightarrow_{\mathrm{Def}} \neg[P < NP]$.

From Definition 2.9:

Definition 2.14. $\neg Q_{\mathsf{f}}(m, a, x) \leftrightarrow_{\mathrm{Def}} \exists a'[M_{\mathsf{f}}(a, a') \wedge \neg Q(m, a', x)]$.

Definition 2.15 (*Another version of the exotic formalization*). $[P < NP]^{\mathsf{f}} \leftrightarrow_{\mathrm{Def}} \forall m, a \exists x \neg Q_{\mathsf{f}}(m, a, x)$.

Remark 2.16. Notice that this is still a Π^0_2 sentence:

$$\forall m, a \exists x, a', x_1, \ldots, x_k\{[p(\langle e_{\mathsf{f}}, a, a'\rangle, \ldots, x_1, \ldots, x_k) = 0] \wedge \neg Q(m, a', x)\}.$$

Since we decided to keep $[P < NP]^{\mathsf{f}}$ a Π^0_2 sentence, this requirement leads to Definition 2.14.

Definition 2.17. $[P = NP]^{\mathsf{f}} \leftrightarrow_{\mathrm{Def}} \neg[P < NP]^{\mathsf{f}}$.

Remark 2.18. For the universal polynomial $p(\langle e_{\mathsf{f}}, a, b\rangle, x_1, x_2, \ldots, x_k)$, if e_{f} is the Gödel number of a Turing machine that computes f:

1. [f is total] $\leftrightarrow_{\mathrm{Def}} \forall a \exists b, x_1, \ldots, x_k [p(\langle e_{\mathsf{f}}, a, b\rangle, x_1, \ldots, x_k) = 0]$.
2. [f is total] $\leftrightarrow \forall a \exists b M_{\mathsf{f}}(a, b)$.
3. If $\forall a \exists b M_{\mathsf{f}}(a, b)$ then:
   (a) $\mathsf{f}(a) =_{\mathrm{Def}} \mu_b M_{\mathsf{f}}(a, b)$.
   (b) $\forall a M_{\mathsf{f}}(a, \mathsf{f}(a))$.

We will also eventually write $\neg Q(m, \mathsf{f}(a), x)$ for $\neg Q_{\mathsf{f}}(m, a, x)$, whenever assumption 3. in Remark 2.18 holds. One should always keep in mind that actual dependence is on e_{f}, and not on f; see Remark 2.10.

3. Function F, $[P < NP]^F$ and $[P < NP]$

See Section 1 for comments on the following:

Definition 3.1. For each n, $\mathsf{F}(n)$ is the sup of those $\{e\}(k)$ such that:

1. $k \leqslant n$.
2. $\ulcorner \mathrm{Pr}_{\mathrm{ZFC}}(\ulcorner \forall x \exists z T(e, x, z)\urcorner)\urcorner \leqslant n$. That is, there is a proof of [$\{e\}$ is total] in ZFC whose Gödel number is $\leqslant n$. (For sentence ϕ, $\ulcorner \phi \urcorner$ is its Gödel number; T is Kleene's predicate [8].)

Proposition 3.2. *We can explicitly compute a Gödel number e_{F} so that $\{e_{\mathsf{F}}\} = \mathsf{F}$.*

Given Remark 2.18 (formalization of [f is total]) and Definition 3.1 (for F):

Proposition 3.3. [F *is total*] *is not proved by* ZFC, *supposed consistent*.

Definition 3.4. $[P < NP]^{\mathsf{F}} \leftrightarrow_{\mathrm{Def}} \forall m,\ a \exists x \neg Q_{\mathsf{F}}(m, a, x)$.

3.1. Main theorems

Lemma 3.5. *If $I \subseteq \omega$ is infinite and $0 \in I$, then*:

$$\mathrm{ZFC} \vdash \{[\forall m\ \forall a \in I \exists x \neg Q(m, a, x)] \rightarrow [\forall m\ \forall a \in \omega \exists x \neg Q(m, a, x)]\}.$$

Proof. We can prove the following:

$$\mathrm{ZFC} \vdash \{[\forall m\ \forall a \in I \exists x \neg Q(m, a, x)] \rightarrow [\forall m\ \forall a \in I \forall a' \geqslant a \exists x \neg Q(m, a', x)]\}.$$

The two conditions "for all $a \in I$" and "for all $a' \geqslant a$" can be substituted for "for all $a \in \omega$". $\square$

This is the "size of bounds does not matter" result.

Proposition 3.6. ZFC $\vdash [P < NP]^{\mathsf{F}} \leftrightarrow \{[\mathsf{F}\ \mathit{is\ total}] \wedge [P < NP]\}$.

Proof

[$\Leftarrow$]. Suppose that $[P < NP] \wedge [\mathsf{F}$ is total$]$ holds.

1. $\forall a \exists a' M_{\mathsf{F}}(a, a')$.
2. $\forall m\ \forall b \exists x \neg Q(m, b, x)$.
3. By restriction to $\mathrm{Im}(\mathsf{F})$ in 2.,

   $$\forall m\ \forall b \in \mathrm{Im}(\mathsf{F}) \exists x \neg Q(m, b, x).$$

4. For $b = \mathsf{F}(a)$ due to step 1 above and Remark 2.18:

   $$\forall m\ \forall a \in \mathrm{Dom}(\mathsf{F}) \exists x \neg Q(m, \mathsf{F}(a), x).$$

5. Then, $\forall m\ \forall a \exists x \neg Q_{\mathsf{F}}(m, a, x)$.
6. That is, $[P < NP]^{\mathsf{F}}$.

[$\Rightarrow$]. Now suppose that $[P < NP]^{\mathsf{F}}$ holds:

1. That is, $\forall m\ \forall a \exists x \neg Q_{\mathsf{F}}(m, a, x)$.
2. We get that $\forall a \exists a', M_{\mathsf{F}}(a, a')$. (See below Scholium 3.7.)
3. Then for $b = \mathsf{F}(a)$, into 1, we get: $\forall m\ \forall b \in \mathrm{Im}(\mathsf{F}) \exists x \neg Q(m, b, x)$.
4. This is equivalent to $[P < NP]$.
   (See Lemma 3.5. This has an intuitive meaning: the size of the gaps in the polynomial bounds is irrelevant; the only point is that all possible polynomial bounds fit into the prescribed bounds.)
5. From 2 and 4 we finally get: $[P < NP] \wedge [\mathsf{F}$ is total$]$. $\square$

Scholium 3.7. ZFC $\vdash [P < NP]^{\mathsf{F}} \rightarrow [\mathsf{F}\ \mathit{is\ total}]$.

Remark 3.8. The following informal argument clarifies the scholium. Let:

$$\mathsf{f}_{\mathsf{F}}(\langle m, a \rangle) = \mu_x[\neg Q(m, \mathsf{F}(a), x)],$$

where we can here look at F as a (partial) recursive function. (The brackets $\langle \ldots, \ldots \rangle$ note the usual 1–1 pairing function.) Now if f_{F} is total, then $\mathsf{F}(a)$ has to be defined for all values of the argument a, that is, F must be total; the function f_{F} is the so-called counterexample function to $[P = NP]^{\mathsf{F}}$.

Proof of the scholium. Immediate, from $\exists b[M_{\mathsf{F}}(a, b) \wedge \neg Q(m, b, x)]$. $\square$

Remark 3.9. Proposition 3.6 was originally stated for PA and for F_{ϵ_0}; it also dealt with a very different, restricted $[P < NP]^{\mathsf{F}_{\epsilon_0}}$. For comments about it in its original form see [3].

Corollary 3.10. $\mathrm{ZFC} \vdash [P = NP]^{\mathsf{F}} \leftrightarrow \{[\mathsf{F} \textit{ is total}] \rightarrow [P = NP]\}$.

Proof. From Proposition 3.6. □

4. Main results

The next result was stated and given a very different, direct and constructive proof in a May, 2000 talk [2]; the earlier proof will appear in [1]. For the present proof see [4].

Proposition 4.1. *If* ZFC *is consistent*, *then* ZFC *does not prove* $[P < NP]^{\mathsf{F}}$.

Proof

1. Suppose $\mathrm{ZFC} \vdash [P < NP]^{\mathsf{F}}$.
2. We have that $\mathrm{ZFC} \vdash [(P < NP)^{\mathsf{F}} \rightarrow (\mathsf{F} \text{ is total})]$. (Scholium 3.7.)
3. Follows that $\mathrm{ZFC} \vdash (\mathsf{F} \text{ is total})$, which is impossible. (From Proposition 3.3.) □

Corollary 4.2. $[P = NP]^{\mathsf{F}}$ *is consistent with* ZFC.

Lemma 4.3. $\mathrm{ZFC} \vdash [\mathsf{F} \textit{ is total}] \leftrightarrow [\mathrm{ZFC} \textit{ is } \Sigma_1 - \textit{sound}]$.

Proof. Follows from the formal definition of Σ_1-soundness and the construction of F; see [5,6,11]. □

Proposition 4.4. *If* ZFC *is consistent then*:

$$\mathrm{ZFC} + [P = NP]^{\mathsf{F}} + [\mathrm{ZFC} \textit{ is } \Sigma_1 - \textit{sound}]$$

is consistent.

Proof (*informal*). If ZFC and therefore $\mathrm{ZFC} + [P = NP]^{\mathsf{F}}$, are consistent, then so is $\mathrm{ZFC} + [P = NP]^{\mathsf{f}} + [\mathrm{ZFC} \textit{ is } \Sigma_1\text{-sound}]$, as we can add a reflection principle to $\mathrm{ZFC} + [P = NP]^{\mathsf{F}}$; see [6,13]. □

Proposition 4.5. *If* $\mathrm{ZFC} + [\mathrm{ZFC} \textit{ is } \Sigma_1 - \textit{sound}] + [P = NP]^{\mathsf{F}}$ *is consistent*, *then* $[P = NP]$ *is consistent with* ZFC.

Proof
1. Suppose that ZFC is consistent.
2. From Corollary 4.2, theory $\{\mathrm{ZFC} + [P = NP]^{\mathsf{F}}\}$ is consistent.
3. ZFC, $[P = NP]^{\mathsf{F}} \vdash [P = NP]^{\mathsf{F}}$.
4. ZFC, $[P = NP]^{\mathsf{F}} \vdash [\mathsf{F}$ is total $\to [P = NP]$. (Corollary 3.10.)
5. ZFC, $[P = NP]^{\mathsf{F}}, [\mathsf{F}$ is total$] \vdash [P - NP]$.

That is, $[P = NP]$ is derived from theory ZFC + [F is total] + $[P = NP]^{\mathsf{F}}$. Or, ZFC + [ZFC *is* Σ_1-sound] together with hypothesis $[P = NP]^{\mathsf{F}}$ implies $[P = NP]$. So, $[P = NP]$ is consistent with ZFC, supposed consistent. □

Corollary 4.6. *If* ZFC *is consistent*, *then so is* ZFC + $[P = NP]$.

4.1. More consequences

Proposition 4.7
1. ZFC + [ZFC *is* Σ_1-*sound*] $\vdash [P < NP] \leftrightarrow [P < NP]^{\mathsf{F}}$.
2. ZFC + [ZFC *is* Σ_1-*sound*] $\vdash [P = NP] \leftrightarrow [P = NP]^{\mathsf{F}}$.

Proof. First, one has that ZFC $\vdash [P < NP]^{\mathsf{F}} \to [P < NP]$. (From Proposition 3.6; see Scholium 3.7.)

For the other implication:

1. ZFC $\vdash ([\mathsf{F}$ is total$] \wedge [P < NP]) \to [P < NP]^{\mathsf{F}}$. (From Proposition 3.6.)
2. ZFC $\vdash [\mathsf{F}$ is total$] \to ([P < NP] \to [P < NP]^{\mathsf{F}})$.
3. ZFC, [F is total $\vdash [P < NP] \to [P < NP]^{\mathsf{F}}$. □

Corollary 4.8. $[P < NP] \leftrightarrow [P < NP]^{\mathsf{F}}$ *is consistent with* ZFC, *supposed consistent*.

We can improve on Proposition 4.7 and Corollary 4.8; we give the argument in detail since it is of interest—how much do we actually need to establish the equivalence? The present proof is straightforward. However notice that it is not required for Corollary 4.6 although it provides an alternative route to it; Proposition 4.9 only tells us how much we have to add to ZFC in order to establish an equivalence between $[P = NP]^{\mathsf{F}}$ and $[P = NP]$.

Proposition 4.9. *For some* $a_0, b_0 \in \omega$ *so that* $M_{\mathsf{F}}(a_0, b_0)$ *holds*, *then*:

$$[\mathrm{ZFC} + M_{\mathsf{F}}(a_0, b_0)] \vdash [P < NP]^{\mathsf{F}} \leftrightarrow [P < NP].$$

Proof. From Proposition 3.6 we have that: $[P < NP]^{\mathsf{F}} \to [P < NP]$. For the converse, we will prove $[P = NP]^{\mathsf{F}} \to [P = NP]$. As before the argument has the form $\mathrm{ZFC}, A \vdash B$ if and only if $\mathrm{ZFC} \vdash A \to B$.

1. $[P = NP]^{\mathsf{F}}$.
2. That is, $\exists m, a \forall x, c[M_{\mathsf{F}}(a, c) \to Q(m, c, x)]$.
3. Add m_0, a_0 so that: $\forall x, c[M_{\mathsf{F}}(a_0, c) \to Q(m_0, c, x)]$.
4. Particularized: $\forall x[M_{\mathsf{F}}(a_0, b) \to Q(m_0, b, x)]$.
5. From step 4 we get $[(\forall x M_{\mathsf{F}}(a_0, b)) \to \forall x Q(m_0, b, x)]$.
6. That is, $[M_{\mathsf{F}}(a_0, b) \to \forall x Q(m_0, b, x)]$, or $[M_{\mathsf{F}}(a_0, b_0) \to \forall x Q(m_0, b_0, x)]$, for notational convenience.
7. Leads to $\mathrm{ZFC}, M_{\mathsf{F}}(a_0, b_0) \vdash \forall x Q(m_0, b_0, x)$.
8. Now impose that $M_{\mathsf{F}}(a_0, b_0)$ holds. From theory $\mathrm{ZFC} + M_{\mathsf{F}}(a_0, b_0)$ we deduce $\forall x Q(m_0, b_0, x)$.
9. We then derive $\exists m, b \forall x Q(m, b, x)$.
10. This is $[P = NP]$.
11. That is, we have proved within $\mathrm{ZFC} + M_{\mathsf{F}}(a_0, b_0)$ that $[P = NP]^{\mathsf{F}} \to [P = NP]$. □

Notice that theory $\mathrm{ZFC} + M_{\mathsf{F}}(a_0, b_0)$ is consistent once $\mathrm{ZFC} + [\mathsf{F}$ is total$]$ is consistent. However, if ZFC is consistent, then $\mathrm{ZFC} + \neg(\mathsf{F}$ is total$) + M_{\mathsf{F}}(a_0, b_0)$ is also consistent. That is to say, our requirement to establish Proposition 4.9 is a very weak one, since the condition we have to add to ZFC in order to derive it is consistent with either [F is total] or with ¬[F is total]. (Cf. Proposition 4.9 to Proposition 2.7.)

Acknowledgements

An early, constructive proof of the results is Section 3 about the non-provability of $[P < NP]^{\mathsf{F}}$ and the consistency of $[P = NP]^{\mathsf{F}}$ was announced by the authors in late 1999 and presented at the Brazilian Logic Symposium, May 2000. It was later corrected in several details and improved by M. Guillaume; it bypassed the formal equivalence in Proposition 3.6 with the help of a long, direct proof [1,7].

This paper is part of the Research Project on Complexity and the Foundations of Computation at the Institute for Advanced Studies, University of São Paulo (IEA-USP). We thank them for support, as well as CNPq (Philosophy Section), UNIP, and the Graduate Studies Program at the School of Communications, Federal University of Rio de Janeiro.

The authors thank the Institute for Advanced Studies, University of São Paulo, for support, especially its former Director Prof. A. Bosi and its current

Director, Prof. G. Malnic, as well as F. Katumi, S. Sedini, M. Alves and I. Iwashita. The second author also wishes to thank Professors S. Amoedo de Barros, A. Cintra, J. Argolo and M. Sodré at the Federal University of Rio de Janeiro (University of Brazil) as well as its Rector Prof. J. Vilhena.

References

[1] N.C.A. da Costa, F.A. Doria, M. Guillaume, On a total function which overtakes all total recursive functions, preprint 01-RGC-IEA, 200X.
[2] F.A. Doria, Talk at the Brazilian Logic Symposium on his joint work with N.C.A. da Costa on computational complexity, May 2000.
[3] F.A. Doria, Messages to the newsgroup theory-edge, November 2000–October 2001.
[4] F.A. Doria, Metamathematics of $P = ?NP$, informal presentation at the meeting *Two Days with Patrick Suppes*, Federal University at Santa Catarina, Brazil, 22–23 April 2002.
[5] S. Feferman, Arithmetization of metamathematics in a general setting, Fund. Math. 49 (1960) 35.
[6] S. Feferman, Transfinite recursive progressions of axiomatic theories, J. Symbolic Logic 27 (1962) 259.
[7] M. Guillaume, E-mail messages to N.C.A. da Costa and F.A. Doria, September 2000–January 2002.
[8] S.C. Kleene, Mathematical Logic, Wiley, 1967.
[9] G. Kreisel, On the interpretation of non-finitist proofs, I and II, J. Symbolic Logic 16 (1951) 241, and 17 (1952) 43.
[10] M. Machtey, P. Young, An Introduction to the General Theory of Algorithms, North-Holland, 1979.
[11] J. Paris, L. Harrington, A mathematical incompleteness in Peano arithmetic, in: J. Barwise (Ed.), Handbook of Mathematical Logic, North-Holland, 1977.
[12] H. Schwichtenberg, Proof theory: some applications of cut-elimination, in: J. Barwise (Ed.), Handbook of Mathematical Logic, North-Holland, 1989.
[13] C. Smoryński, The incompleteness theorems, in: J. Barwise (Ed.), Handbook of Mathematical Logic, North-Holland, 1989.