Available online at www.sciencedirect.com

SCIENCE DIRECT®

APPLIED MATHEMATICS AND COMPUTATION

ELSEVIER Applied Mathematics and Computation xxx (2005) xxx–xxx

www.elsevier.com/locate/amc

Addendum

Addendum to: "Consequences of an exotic formulation for $P = NP$" [Appl. Math. Comput. 145 (2–3) (2003) 655–665]

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

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

Abstract

We elaborate on the following result which appears in that paper: if ZFC + [ZFC is Σ_1-sound] + $[P = NP]^F$ is consistent, then so is ZFC + $[P = NP]$.

1. Introduction

We recently published a paper [2] whose main goal was to explore some consequences of a variant of the usual formalization for $P = NP$. We noted it $[P = NP]^F$ and called it the "exotic formulation" to emphasize that character. Our exotic formulation has the following peculiarity: while it—naïvely—translates our intuitions about the $P = NP$ hypothesis, it is not formally equivalent in ZFC to the standard formalization, noted $[P = NP]$.

DOI of original article: 10.1016/S0096-3003(03)00176-0.
* Corresponding author.
E-mail addresses: ncacosta@usp.br (N.C.A. da Costa), fadoria2001@yahoo.com.br, fdoria@eco.ufrj.br (F.A. Doria).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2005.03.002

Our paper received some attention and an immediate, quite unsympathetic, highly adjectival, review [3] by Schindler (''failed attempt'', ''crucial gap'', even a ''sic''!) Yet, despite all that *Schindler in fact sees no error in what we have done; he only finds what he calls a ''crucial gap'', which was however purposedly left open by us in the paper, as we explain in this note.*

2. The exotic formulation

The standard formalization for $P = NP$ can be given as

Definition 2.1

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

$R(x, y)$ is a polynomial predicate and $t_m(x)$ denotes the operation time of Turing machine of Gödel number m over x; x is coded as a binary string, and $|x|$ is its length. Then $[P < NP]$ is defined as $\neg[P = NP]$.

The exotic formalization requires some extra machinery. We now quote from our paper [2]. We write:

Definition 2.2

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

Let F be strictly increasing, intuitively total recursive, but such that ZFC cannot prove it to be total. Then:

Definition 2.3

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

$(a = \langle c, d \rangle)$ $M_{\mathsf{F}}(a, a')$ stands for $(\mathsf{F}(a) = a')$ and the exotic formalization is:

Definition 2.4

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

Again $[P = NP]^{\mathsf{F}}$ is defined as $\neg[P < NP]^{\mathsf{F}}$.

These definitions simply mean that instead of taking $|x|^a + b$ as polynomial bounds for the Turing machines, we use $|x|^{\mathsf{F}(a)} + \mathsf{F}(b)$. Anyway the bounds are still (always intuitively) polynomial.

Now, as F is naïvely, or intuitively, total, we have that the equivalence $[P < NP] \leftrightarrow [P < NP]^{\mathsf{F}}$ naïvely holds. So, we may say that the exotic formalization is, always naïvely, the same as the standard formalization.

Moreover, as Schindler duly points out:

- If we use function F as above—strictly increasing, intuitively total recursive, but such that ZFC cannot prove it to be total—then ZFC cannot prove that both formalizations, the standard and the exotic, are equivalent [2].
- Also, from the fact that ZFC proves $[P < NP]^{\mathsf{F}} \rightarrow [\mathsf{F} \text{ is total}]$, if consistent, ZFC cannot prove $[P < NP]^{\mathsf{F}}$ and therefore ZFC + $[P = NP]^{\mathsf{F}}$ is consistent.
- Finally, ZFC adequately strengthened proves the equivalence $[P < NP] \leftrightarrow [P < NP]^{\mathsf{F}}$. (This is discussed at length in Section 4 of [2].)

To sum it up: our exotic formalization is very close to the standard one, but is not the real thing.

3. The "gap"

So far so good. Yet we also derive the following result:

Proposition 3.1. *If* ZFC + [ZFC *is* Σ_1*-sound*] + $[P = NP]^{\mathsf{F}}$ *is consistent, then* [$P = NP$] *is consistent with* ZFC.

We had proved that if ZFC is consistent, then so is ZFC + $[P = NP]^{\mathsf{F}}$. Then we added a reflection principle to it, as it seems reasonable to believe that consistent theory ZFC + $[P = NP]^{\mathsf{F}}$ remains consistent when we add to it the set of conditions that assert the Σ_1–soundness of ZFC. We are going to elaborate on that now.

Theory ZFC + [ZFC is Σ_1-sound] + $[P = NP]^{\mathsf{F}}$ is exceedingly strong, as it proves Consis(ZFC) (the usual formalization for the consistency of ZFC). Here is the so–called "gap". *Due to the strength of the hypothesis, we presented no proof for its consistency and decided just to make a brief remark about it.* (We were perhaps too succinct at this point.)

Recall that ZFC proves [F is total] $\leftrightarrow$ [ZFC is Σ_1-sound].

Let us ponder the hypothesis of the consistency of ZFC + [F is total] + $[P = NP]^{\mathsf{F}}$. It simply means that there is a model for it where all polynomial Turing machines do converge over all its inputs. *It is a naïvely reasonable assumption, even if formally very strong.* Let us stress the point: we never tried to pass some plausibility argument for mathematical proof. This is the reason for the label "Proof (informal)" at this point in our paper [2]. Anyway theorems that result from strong unproved but reasonable hypotheses are quite common in mathematics; in the present case some kind of strong principle will be required to prove the desired consistency.

Let us take a look at the alternatives we have at this juncture

- If ZFC proves $[P = NP]^{\mathsf{F}}$ and has a model with standard arithmetic, then the consistency of ZFC + [ZFC is Σ_1-sound] + $[P = NP]^{\mathsf{F}}$ is trivial. This fact shows that there is no a priori reason to say that theory ZFC + [ZFC is Σ_1-sound] + $[P = NP]^{\mathsf{F}}$ is inconsistent.
- If ZFC proves $[P < NP]$, then ZFC + [ZFC is Σ_1-sound] + $[P = NP]^{\mathsf{F}}$ is of course inconsistent.To put it differently: if ZFC proves [$P<NP$], then all models for consistent theory ZFC + $[P = NP]^{\mathsf{F}}$ will have a highly counterintuitive behavior, namely F will have a finite domain, and sentence $[P = NP]^{\mathsf{F}}$ will have no easy informal interpretation.
- However, if $[P = NP]^{\mathsf{F}}$ is independent of ZFC, then the models for ZFC + [ZFC is Σ_1-sound] + $[P = NP]^{\mathsf{F}}$ may be highly nontrivial.

Proposition 3.1 *is therefore to be seen as depending on a strong supposition that nevertheless translates as a naïvely plausible fact*. Just that. Again we stress: we never intended to substitute naïve arguments for formal rigor.

Two final remarks: Schindler refers to an unpublished paper of us and to his own refutation of (actually, just a plausibility argument against) one of its lemmas [3]. That contested lemma—where we go from a single poly Turing machine $\mathsf{Q}_z(m, x)$ to the family $\mathsf{Q}_{\mathsf{g}(z,m)}(x)$ indexed by g, g primitive recursive—results from an application of the $s - m - n$ theorem (we gave a direct construction in that preprint); this is enough to lead to the result we were looking for.

Also, as noted by Schindler, we use pretty elementary techniques in our published paper [2]. We did so precisely in order to avoid techniques that would be of uncertain justification. Moreover several interesting papers on the P vs. NP question do use elementary techniques, for example the Ben David and Halevi paper [1]; those simple techniques again lead to nontrivial conclusions.

We must thank R. D. Schindler for a recent exchange and clarification on his review of our work.

Note: E. Bir pointed out to the authors that the following paper:

R.A. DeMillo, R.J. Lipton, The consistency of "$P = NP$" and related problems with fragments of number theory, Proc. 12th Ann. ACM Symp. on Theory of Computing, 1980, pp. 45–57

obtains similar results as [2] and with similar techniques.

References

[1] S. Ben–David, S. Halevi, On the independence of P vs. NP, Technical Report #, 699, Technion, 1991.

[2] N.C.A. da Costa, F.A. Doria, Consequences of an exotic definition for $P = NP$, Applied Mathematics and Computation 145 (2003) 655.

[3] R.D. Schindler, Bulletin of Symbolic Logic 10 (2004) 118, review of [2].