A note on an alleged proof of the relative consistency of $P = NP$ with PA

Ralf-Dieter Schindler

Institut für formale Logik, Universität Wien, 1090 Wien, Austria

rds@logic.univie.ac.at
http://www.logic.univie.ac.at/~rds/

N.C.A. da Costa and F.A. Doria claim to have shown in [1] that $P = NP$ is relatively consistent with PA. The purpose of the present note is to argue that there is a mistake in that paper. Specifically, we want to point out that Corollary 5.14 of [1] – which is used in the proof of their main result – seems to be wrong, or at least highly dubious.

We are first going to reconstruct their argument. According to that reconstruction, the argument of [1] would in fact show that PA proves $P = NP$. We'll then discuss Cor. 5.14 of [1]. However, rather than talking about provability in PA or stronger theories, we'll stick to a different attitude and argue internally: using Cor. 5.14 of [1] we'll derive a contradiction from the assumption that $P < NP$ (and we implicitly assume our argument goes thru in PA).

We'll follow the notation of [1] (with the exception of $f_{\neg A}$).

Some Turing machines. $\bigvee(z) = 1$ iff $\pi_1(z)$ codes a cnf-Boolean expression and $\pi_2(z)$ codes an assignment which satisfies it (o.w. $\bigvee(z) = 0$). E is a fixed exponential Turing machine that solves any instance of the satisfiability problem (in particular, $\bigvee(< z, E(z) >) = 1$ for any z coding a satisfiable cnf-Boolean expression). For $n < \omega$, Q^n will be that Turing machine s.t. $Q^n(z) = E(z)$ for $z \leq n$ and $Q^n(z) = 0$ for $z > n$ (cf. p. 10 of [1]). Notice $\bigvee$ and all Q^n (for $n < \omega$) are polynomial Turing machines. By the Baker-Gill-Solovay trick there is a recursive enumeration $(P_m \colon m < \omega)$ of all polynomial Turing machines.

Some recursive functions. We let $f(m)$ be the least z such that $\bigvee(z) = 1$, whereas $\bigvee(< \pi_1(z), P_m(\pi_1(z)) >) = 0$ (i.e., $f(m)$ witnesses that P_m doesn't prove $P = NP$). We have: f is total iff $P < NP$. (f is written $f_{\neg A}$ in [1]; cf. [1] p. 4.) Let $(\psi_i \colon i < \omega)$ be a rec. enumeration of all linear functions from ω to ω. We let $F(m) = max\{f \circ \psi_i(m) \colon m \leq i\} + 1$. Note that F dominates $f \circ \psi$ for any linear ψ.

Corollary 5.14 of [1] now reads as follows: **Main Lemma.** There is a *linear* $\psi \colon \omega \to \omega$ s.t. for all m and n do we have that $Q^{F(m)}(n) = P_{\psi(m)}(n)$.

Given this Main Lemma we may now prove $P = NP$ as follows. Suppose not. Then f is total. So F is total, too. If ψ is as in the Main Lemma then $F(m) > f \circ \psi(m)$ for all sufficiently large m. On the other hand, $f(\psi(m))$ is the least z such that $\bigvee(z) = 1$, whereas $\bigvee(< \pi_1(z), Q^{F(m)}(\pi_1(z)) >) = 0$. For $\pi_1(z) \leq F(m)$ we'll have $Q^{F(m)}(\pi_1(z)) = E(\pi_1(z))$, so that $f(\psi(m)) \geq < F(m) + 1, s >$ for all s, i.e., $f(\psi(m)) \geq F(m) + 1$. We'll thus have $F(m) > f \circ \psi(m) \geq F(m) + 1$ for all sufficiently large m. Contradiction! We have shown that $P < NP$.

Have we? Not so, I claim. Let's discuss the Main Lemma. We can't make the calculation of $F(m)$ part of the program of $Q^{F(m)}$, as we don't know how long that calculation might take. If we did make the calculation of $F(m)$ part of the program of $Q^{F(m)}$ then $Q^{F(m)}$'s clock might shut down $Q^{F(m)}$'s calculation even before $F(m)$ gets known. So it's not m, but rather $F(m)$, which will be part of the code $\psi(m)$ of $Q^{F(m)}$. But then the function ψ will be as complex as F is; which is, I think, as it should be. But this then poses a serious problem. Suppose a ψ as above can only be as complex as F. The above argument breaks down without an F s.t. F dominates $f \circ \psi$. (The argument on pp. 13 ff. of [1] appears somewhat dubious to me.)

This, I guess, indicates that it might be next to impossible to find a recursive enumeration $(P_m : m < \omega)$ of all polynomial Turing machines s.t. for any given total rec. function f there is another total function F s.t. F dominates $f \circ \psi$, where for all m and n we have that $Q^{F(m)}(n) = P_{\psi(m)}(n)$. (If so, we'd get a proof of $P = NP$ along the above lines.)

I cordially thank Chico Doria for his interest in my e-mail messages concerning [1]. I'd be more than happy to be taught that Cor. 5.14 of [1] does hold after all – at least in spirit.

References

[1] N.C.A. da Costa and F.A. Doria, *On the consistency of $P = NP$ with fragments of ZFC whose own consistency strength can be measured by an ordinal assignment*, http://arXiv.org/abs/math/0006079.