Exmo. Sr. Presidente,
CNPq,
Brasília DF.

Senhor Presidente:

Encaminho a V. S. em anexo o pedido de reconsideração que ora faço, do indeferimento da bolsa em produtividade de pesquisa, no Proc. 30788520046 – CNPq.

Permita-me observar: o parecer do comitê assessor de filosofia, endossado pelo diretor de programas horizontais, José Roberto Drugowich, não fez justiça ao meu trabalho de pesquisa de mais de vinte anos, possivelmente por pouca familiaridade com o assunto de meu projeto de pesquisa. E talvez isso explique o tom adotado pelo resenhista, altamente adjetivado, mas pouco objetivo em apontar com precisão as possíveis falhas técnicas de minha proposta.

Decidi-me a contestá-lo em detalhe, num *review* técnico de meu trabalho, que ora encaminho a V. S.

E compete a V. S. ser o guardião e responsável pela preservação da ciência brasileira, infelizmente ainda tão frágil e incipiente.

Respeitosamente,

Francisco Antonio de Moraes Accioli Doria

Pedido de Reconsideração

Proc. 30788520046 - CNPq

Francisco Antonio de Moraes Accioli Doria

Resumo

O projeto divide-se em três tópicos: hipercomputação, o problema P vs. NP numa perspectiva metamatemática, e questões referentes à ontologia da matemática. O traço unificador entre estas questões é o conceito de Princípio de Reflexão, e de progressão iterada de teorias.

Tais conceitos levam ao teorema de completude de Turing-Feferman (TF), provado por Turing em 1939 e ampliado por Feferman em 1962. Historio as principais idéias a respeito desde 1939. Mostro sua relação à hipercomputação (ou computação super-Turing), já que o teorema TF "resolve" o Problema da Parada para máquinas de Turing. Passando às questões de complexidade computacional, examino a relevância dos princípios de reflexão para o problema P vs. NP, e discuto em detalhe os comentários críticos de Ralf Schindler a um trabalho recente (de 2003) de da Costa e do autor sobre tal problema. Concluo o tópico discutindo o comportamento dos princípios de reflexão para teorias com aritmética não-standard.

A parte final examina a relevância dos princípios de reflexão para algumas questões relacionadas à ontologia da matemática. Questões como: completude de teorias formais; teoremas de incompletude; a consistência das mesmas teorias; construções formais e informais; tudo isso é relacionado aos princípios de reflexão. Observa-se que: *não se pode fazer filosofia da matemática sem um bom conhecimento, um conhecimento que se pode dizer ativo, da prática matemática em determinadas questões de ponta.* Damos como exemplo a recente prova de K. Kunen para a consistência da aritmética, implementada através de um algoritmo de fácil exame.

Parecer do Comitê Assessor de Filosofia:

O projeto é extremamente ambicioso. O estilo jornalístico do proponente, juntando na íntegra referências a artigos que o mencionam, confunde os objetivos do projeto com a repercussão de seu trabalho. Por exemplo, o projeto não informa sobre a severa crítica a seus métodos e resultados publicadas no "Bulletin of Symbolic Logic." O resenhista mostra como a pretensão exagerada do proponente resulta em afirmações problemáticas e de fundamentação duvidosa.

A "Nota Final" do projeto sobre ontologia dos objetos matemáticos deveria merecer um grande destaque num projeto destinado à área de Filosofia e não a de Matemática. No entanto, essa parte do projeto é de uma enorme trivialidade que parece evidenciar que o solicitante não tem muita familiaridade com questões filosóficas.

Nota-se também a falta de envolvimento do proponente na formação de recursos humanos.

O comitê assessor de filosofia é constituído por Ricardo Terra, Ivan Domingues e Nelson Gomes. O parecer em causa foi endossado e encaminhado por José Roberto Drugowich.

Segue-se a contestação que faço.

Introdução

Solicitaria, se possível, que este pedido de reconsideração fosse analisado por alguém que conheça teoria da recursão na versão intuitiva como exposta, p.e., no clássico de Hartley Rogers Jr., *Theory of Recursive Functions and Effective Computability*, John Wiley (1967), devido ao caráter necessariamente técnico de minha argumentação. As referências que dou, em notas, complementam e estendem o que Rogers expõe.

Consta este projeto, originalmente, de três tópicos[1]

- Hipercomputação;
- Complexidade computacional e o problema P vs. NP, numa perspectiva metamatemática.
- Questões sobre a ontologia da matemática, a partir do contraste entre a matemática "informal" e a axiomatizada.

Hipercomputação é o estudo das máquinas de computar, ou dos (super)-algoritmos que resolvem o Problema da Parada, insolúvel para as máquinas de Turing. Complexidade computacional estuda a "economia" dos processos de computação, a quantidade de recursos, em termos de memória (espaço) e tempo necessários à solução de classes de problemas. O Problema P vs. NP é considerado o problema central em teoria da complexidade computacional: formulado de maneira intuitiva, a partir de um exemplo simples, é — será que existe um algoritmo "rápido" para a solução de instâncias arbitrárias do Problema do Caixeiro Viajante? As questões sobre a ontologia matemática a serem discutidas partem de um trabalho de Kenneth Kunen[2], de 1995[1], no qual este lógico explicitamente constroi um algoritmo que prova a consistência da aritmética[3]. Como é isto possível, face ao segundo teorema de incompletude de Gödel?

O traço unificador entre essas três questões é o conceito de *Princípio de Reflexão.* Tal conceito parte da tese de doutorado de Alan Turing, publicada em 1939[4]. Seja a aritmética de Peano, PA. Se PA é consistente, então a sentença que afirma sua consistência, Consis (PA), e sua negacão, ¬Consis (PA), são independentes de PA, pelo segundo teorema de incompletude de Gödel. Turing constroi a sucessão de teorias, PA, PA + Consis (PA), [PA + Consis (PA)] + Consis (PA + Consis(PA)), etc. ao longo da sucessão dos ordinais construtíveis. O resultado que obtem é: a iteração até um ordinal bem menor que Ω_1, o

[1] Aqui usamos o termo "modelo" no sentido tanto de semântica para sistemas formais quanto de esquema teórico para algum sistema (p.e., modelo para computação). O contexto esclarece.

[2] K. Kunen, "A Ramsey theorem in Boyer–Moore logic," *J. Automated Reasoning* **15**, 217 (1995).

[3] Na verdade o algoritmo de Kunen prova o teorema de Paris-Harrington, que implica a consistência da aritmética de Peano.

[4] A. M. Turing, "Systems of logics based on ordinals," *Proc. London Math. Soc.* ser. 2, **45,** 161 (1939).

primeiro ordinal não-construtivo, é suficiente para que a união das teorias até tal ordinal prove todas as sentenças $\prod_1$ verdadeiras no modelo standard para a aritmética. (Há uma série de detalhes técnicos que estou omitindo, e que podem ser vistos no resumo recente de Franzen[5].)

Feferman revê em 1962[6] o trabalho de Turing, generalizando-o e generalizando as iterações feitas. Turing acrescenta a PA uma sentença obviamente verdadeira no modelo standard. Feferman acrescenta infinitas sentenças com a seguinte estrutura básica (em linguagem coloquial):

- Se existe uma prova de *P* em PA, então *P* é de fato provada em PA.
- Se existe uma prova de *P*(0), *P*(1), *P*(2), …, então prova-se "para todo x, *P*(x)."

São suposições razoáveis, e que valem no modelo standard, embora não construtivas. Logo, PA + Reflexão é uma teoria consistente, desde que PA o seja. Feferman itera as teorias com tais princípios, e mostra que o resultado de Turing pode ser estendido para se chegar a um teorema de completude muito amplo para uma iteração até um ordinal construtivo razoavelmente pequeno, embora transfinito.

O teorema de completude de Turing-Feferman, como é conhecido, é de difícil compreensão, em parte devido à dificuldade do trabalho de Feferman, e da construção elegantemente artificiosa que desenvolve. Ficou, portanto, no limbo, até que Lev Beklemishev[7] ofereceu-lhe uma prova elegante e sucinta.

Qual sua importância? Uma é imediata, a outra, bem mais, digamos, misteriosa:

- Se podemos provas todas as sentenças $\prod_1$ verdadeiras, podemos resolver todas as instâncias do Problema da Parada, já que cada uma sua instância é expressa em PA por uma sentença de tal classe.
- Toda teoria com alfabeto recursivo e conjunto recursivamente enumerável de teoremas é expresso por uma sentença $\sum_1$ particular (estas sentenças, recordo, são a negação das $\prod_1$). Daí resulta a importância do conceito de "$\sum_1$ soundness," um tipo de Princípio de Reflexão que engloba em PA e extensões codificações possíveis para esta teoria e para outras teorias com estrutura recursiva.

Como se sabe, $\sum_1$ soundness é equivalente à existência de uma certa função recursiva total, que no entanto não pode ser provada total, na teoria para a qual se afirma este particular princípio de reflexão. Tal função é conhecida desde a prova da incompletude de tais teorias proposta por Kleene em 1936.

---

[5] T. Franzen, "Transfinite progressions: a second look at completeness," *Bull. Symbol. Logic* **10**, 367 (2004).
[6] S. Feferman, "Transfinite recursive progressions of axiomatic theories," *J. Symbol. Logic* **27**, 259 (1962).
[7] L. Beklemishev, "Provability and reflection," Lecture notes for ESSLI' 97 (1997).

Esta a parte técnica. A parte epistemológica sintetiza-se na seguinte questão: *se o teorema de Turing-Feferman leva a uma teoria TF que prova todas as instâncias do Problema da Parada, teremos daí uma extensão que, quase algoritmicamente, prova todas as sentenças verdadeiras da aritmética.* Daí as perguntas: *onde está, exatamente, o "extra" da teoria TF que nos permiteviolar o teorema da parada? O que aprendemos, de fato, com a teoria TF e suas extensões?*

Vejam; o que Hilbert desejava era obter teorias completas: só se demonstra o que for verdadeiro, e vice-versa. Isto, aparentemente, é conseguido para a hierarquia aritmética, em construção que é, digamos, natural, com a teoria TF.

Voltaremos, ao fim, à questão dos Princípios de Reflexão.

Hipercomputação.

Rogers[8] faz, no seu capítulo sobre a hierarquia aritmética, o estudo de algumas teorias de computação que ultrapassam estritamente o modelo de Turing. Mas, com certeza, o primeiro trabalho a sugerir que há um aparato concreto, teoricamente passível de ser construído, e que decide questões computacionalmente indecidíveis, é o de Scarpellini[9] em 1963. Citando o que diz Scarpellini:

> In this connection one may ask whether it is possible to construct an analogue computer which is in a position to generate functions f(x) for which the predicate6 $\int f(x)\cos nx dx > 0$ is not decidable while the machine itself decides by direct measurement whether 6 $\int f(x)\cos nx dx$ is greater than zero or not. Such a machine is naturally only of theoretical interest, since faultless measuring is assumed, which requires the (absolute) validity of classical electrodynamics and probably such technical possibilities as the existence of infinitely thin perfectly conducting wires. All the same, the (theoretical) construction of such a machine would illustrate the possibility of non-recursive natural processes.

Tudo está dito aí: *existirão processos naturais que computam mais que uma máquina de Turing?*

A teoria da computação corrente baseia-se na Tese de Church: uma função é computável se e somente se existir uma máquina de Turing que calcule todos os seus valores. (Há nuances na formulação da tese, mas a que se oferece acima é satisfatória para nossos propósitos.) Há diferenças culturais, digamos assim, na percepção da Tese de Church. Assim sendo, teóricos da computação tem-na quase como um dogma; os lógicos dividem-se — a grande maioria aceita-a, mas para um pequeno grupo ela é vista apenas como a

---

[8] H. Rogers Jr., *Theory of Recursive Functions and Effective Computability*, ed. facsimiar, MIT Press (1991).

[9] B. Scarpellini, "Two undecidable problems of analysis," *Minds and Machines* **13**, 49 (2003); reedição traduzida para o inglês do original alemão de 1963.

caracterização de certo tipo de concepção para o que seja calcular. Existiriam outras possibilidades.

Em 1999 Copeland and Sylvan[10] publicam um artigo examinando a questão das máquinas super-Turing. A seção VIII deste trabalho é dedicada à exposição de idéias minhas e de Newton da Costa. E' precedida pelo comentário:

> However, in a recent article da Costa and Doria raise the possibility that processes of the sort described by Scarpellini might be 'usefully harnessable.'

Segue-se uma descrição exaustiva de trabalhos que Newton da Costa e eu publicamos em 1991[11]

Do caos à hipercomputação.

Fui em 1989 para Stanford, para o laboratório de Patrick Suppes, com uma bolsa Fulbright/CNPq, e levando comigo uma relação de problemas que pretendia atacar durante aquele período sabático. Um deles era o Problema de Hirsch, o problema de decisão para sistemas caóticos — dadas as equações de um sistema dinâmico, podemos dizer se tal sistema é caótico ou não? (Um dos outros era o problema P vs. NP, discutido abaixo.) O Problema de Hirsch, formulado por Morris Hirsch em 1983, foi resolvido por nós, numa colaboração mediada pela internet então nascendo, em julho/agosto de 1990. Mostramos que não há um algoritmo — uma máquina de Turing — capaz de separar sistemas caóticos de não-caóticos, qualquer que fosse o conceito para caos empregado. O centro da prova foi a construção explícita de uma função razoavelmente simples que resolvia (ou "resolvia") o Problema da Parada. Tal função não pode, obviamente, ser implementada através de uma máquina de Turing, mas pode facilmente ser simulada por um circuito elétrico de comportamento ideal. Uma máquina analógica sem falhas.

(O fato dessa função resolver o Problema da Parada só foi percebido por da Costa e por mim depois da sua construção, vale assinalar. Mas logo vimos sua importância para uma teoria de computação super-Turing, ou teoria da hipercomputação.)

Acoplando tal máquina analógica, enquanto oráculo, a uma máquina de Turing, podemos então decidir o que está no grau **0'**. Construindo uma nova função, semelhante à que fizemos originalmente, mas agora associada a tal máquina provida de oráculo, alcançamos o grau **0''**. E assim em diante, até decidirmos toda a hierarquia aritmética de acordo com o modelo standard.

Ou seja, nossa construção alcança o mesmo que o teorema de Turing-Feferman alcança.

---

[10] B. Jack Copeland, R. Sylvan, "Beyond the universal Turing machine," *Austral. J. of Philosophy* **77**, 46 (1999).

[11] Um bom resumo e discussão destas idéias de N. da Costa e minhas, está também no recente artigo de B. Scarpellini, "Comments on 'Two undecidable problems of analysis,'" *Minds and Machines* **13**, 79 (2003). Mais da metade do artigo de Scarpellini comenta e analisa nossos resultados.

A repercussão de nosso resultado foi imediata, mesmo antes dele sair publicado em meados de 1991. Como diz Ian Stewart em *Nature*[12] :

> A huge range of questions — mostly algebraic or combinatorial — has since been proved undecidable. da Costa and Doria show that undecidability extends to many basic questions in dynamical systems theory. These include whether the dynamic is chaotic, whether a trajectory starting from a given initial point eventually passes through some specific region of phase space, or whether the equations are integrable.

Mais recentemente, no livro sobre os Problemas Matemáticos para o Milênio, Steve Smale (que recebeu a Medalha Fields em 1966), vê nossos resultados de 1990/91 como sendo o principal obstáculo a ser vencido em seu Problema XIV:

> [Smale exibe certa função que é discutida em nossos trabalhos.] Observe that one cannot decide the following question: on input *u*, does this function have a zero in R^n. If one can't decide the existence of a zero, one can hardly expect to decide the existence of chaos. In fact Costa-Doria prove just that, chaos is undecidable.

E conclui, como esperaríamos:

> However we could well object in a number of ways: […] for one thing, *Turing machines would seem to be a poor idealization of algorithms used in this subject…*

(Minha ênfase.) Ou seja, Smale também levanta a questão da extensão do modelo Turing para a computação[13].

Mas a percepção de que nosso resultado levantava a possibilidade de construirmos uma máquina super-Turing havia já, como disse, sido percebida por Copeland e Sylvan. Desde então seguem-se diversas publicações a respeito da possibilidade de um modelo de computação super-Turing, ou hipercomputação, como passa a ser chamado. Citemos o verbete na *Stanford Encyclopedia of Philosophy*, de Copeland[14], onde somos referidos expressamente, da Costa e eu, ou o número especial em 2003 de *Minds and Machines*, revista dedicada à filosofia da cognição. Estamos preparando, José Félix Costa, da Univ. Técnica de Lisboa, e eu, um número especial da revista *Applied Mathematics and Computation*, tendo como tema a questão da hipercomputação. Tal número deverá ser fechado agora, em 25 de março de 2005, e terá colaboradores do nível de Martin Davis, Lenore Blum ou Vela Velupillai. Tomamos o cuidado especial de exibir argumentos pró- e contra, já que ciência e filosofia são áreas onde a controvérsia é parte essencial de seu movimento.

---

[12] I. Stewart, "Deciding the undecidable," *Nature* **352** 664 (1991).
[13] S. Smale, "Mathematical problems for the next century," in V. Arnol'd et al., *Mathematics: Frontiers and Perspectives*, AMS (2000).
[14] B. Jack Copeland, "The Church-Turing thesis," *Stanford Encyclopedia of Philosophy*, disponível online (2001).

Sobre hipercomputação, o projeto pretende abordar duas questões:

1. Aprofundar o exemplo das máquinas analógicas como oráculos de máquinas de Turing, podendo decidir sentenças aritméticas de acordo com sua verdade no modelo standard.
2. Estudar a possibilidade de relacionar ou fundar modelos de hipercomputação ao teorema da completude de Turing-Feferman.

(Sobre isso daremos mais detalhes ao final.)

Deixo bem claro o seguinte: tais propostas, embora com certeza numa área de fronteira em teoria da computação, nada têm de ousadas ou distantes da realidade. Correspondem apenas ao desenvolvimento natural de idéias que temos explorado, Newton da Costa e eu, desde cerca de quinze anos.

O problema P vs NP.

De início digo o que conjecturamos, Newton da Costa e eu: se ZFC possui um modelo com a parte aritmética standard, então P=NP e P<NP (representados por sentenças $\sum_2$ e $\prod_2$ na forma usual) são independentes daquela teoria. Mais: se T estende ZFC, com um vocabulário recursivo, um conjunto recursivamente enumerável de teoremas, e com um modelo com a aritmética standard, então P=NP e P<NP são independentes de T.

Mas PA + Regra Ω provam P<NP.

Esta não é, com certeza, a visão mais popular a respeito do problema. Para justificá-la, historio agora o que nos leva a acreditar que o problema vá se resolver assim, analisando *en passant* as duas resenhas de Ralf Schindler sobre nosso trabalho de 2003.

Conheci o problema P vs. NP em 1985, através de um artigo de John Hopcroft na revista *Scientific American* a respeito de máquinas de Turing. Este artigo me levou a outro, muito famoso, o chamado “artigo BGS,” onde estão os únicos resultados não-triviais conhecidos até hoje: relativizado para máquinas de Turing com oráculo, tanto pode valer $P=NP|^A$ quanto $P<NP|^B$, sendo A e B oráculos adequados[15]. Pensei de imediato, será uma questão indecidível?

Em 1987, na lista de problemas que fiz com Newton da Costa, coloquei a questão, mas não lhe dei maior atenção, desde que procurava então resolver o problema de decisão para sistemas caóticos. Em 1991, resolvido aquele problema, nos voltamos para o P vs. NP. Tentamos, em primeiro lugar, ver se a questão relacionava-se à complexidade de Kolmogorov-Chaitin. Vem daí um primeiro resultado obtido, que nunca publicamos, e que, verifiquei, faz talvez parte do folclore da área: a “imensa maioria” (aspas necessárias, porque uso o termo de modo descritivo, num sentido informal) das instâncias de Sat, o

[15] T. Baker, J. Gill, R. Solovay, ``Relativizations of the P=?NP question,'' *SIAM Journal of Computing* **4**, 431 (1975).

problema da satisfação para expressões booleanas em forma normal conjuntiva (cnf), pode ser resolvida pelo método das tabelas-verdade em tempo polinomial. Tal fato verifica-se para as expressões em Sat que possuem tabelas-verdade — codificadas como uma sequência binária de comprimento 2^n, onde n é o número de variáveis booleanas — de máxima complexidade de Kolmogorov-Chaitin[16]. Estende-se este resultado para linguagens (subconjuntos de Sat) infinitas, formadas por tais expressões; no conjunto de todas as linguagens possíveis, estas associadas à máxima complexidade segundo KC possuem medida 1 (probabilidade de 100%). Ou seja, exceções a P=NP são, nesse sentido, e se houverem, muito raras, estando num conjunto de medida 0 (probabilidade nula).

Em 1995 recebemos de um amigo uma mensagem de e-mail que sintetizava resultados dados como folclóricos na área (nunca os vimos publicados). São, em resumo:

1. P<NP pode ser formalizado como uma sentença $\prod_2$.
2. Devemos olhar a função contraexemplo associada. (Intuitivamente: se P<NP, para cada máquina polinomial, na enumeração BGS — ver acima — para cada máquina haverá um momento em que esta dará uma resposta errada. Assim associamos a cada máquina um contraexemplo.) Esta função é a chamada função de Skolem para P<NP.
3. Com ajuda desta função, podemos fazer a sentença P<NP equivalente a uma sentença $\prod_1$.
4. Se P<NP e P=NP forem independentes de ZFC, e se este tiver um modelo com parte aritmética standard, então P<NP é válido para tal aritmética, porque é uma sentença $\prod_1$.
5. E, enfim, o ponto essencial, referido sem prova: *a função contraexemplo, se* P<NP, *cresce mais rápido que qualquer função provadamente total em* ZFC.

Levamos perto de três anos para conseguir uma prova para o último fato. Percebemos também que muito do que interessava à questão P vs. NP corria o mundo em comunicações privadas — tenho um arquivo com cerca de 2000 mensagens trocadas com especialistas que, generosamente, informam a da Costa e a mim sobre trabalhos em curso, idéias, conjecturas, fragmentos de folclore. Aliás, um dos artigos mais interessantes sobre a questão nunca foi publicado[17].

Demos duas provas para o crescimento rápido da função contraexemplo. Uma delas inédita em texto impresso mas publicada na internet como *work in progress*, o que provocou a primeira reação negativa de Schindler. A outra, em revista bem conhecida da Elsevier, *Applied Mathematics and Computation*. O primeiro artigo mereceu, em privado, um review em detalhe de um matemático de primeira linha, cujo nome omito devido ao caráter particular da correspondência, mas que tenho na íntegra em meus arquivos. E’ o seguinte o report:

---

[16] Daniele Mundici disse-me, após conferência que fiz em Milão em 1992, que tal fato seria conhecido. Mas, por exemplo, Joe Traub não sabia a respeito.

[17] S. Ben-David and S. Halevi, “On the independence of P vs. NP,” Technical Report no. 699, Technion (1991).

Chico,

Some day I am going to learn not to reply to math questions without allowing an hour for reflection. The following supersedes my previous four letters of this morning [as far as math points go].

1. Your paper makes a big deal about using an exotic Godel numbering for Turing machines so that Lemma 6 holds. But there is no need to do this.

a) One has the "usual" Godel numbering of TM's. This set of Godel numbers is primitive recursive, but not every number is the Godel number of a TM.

b) Next one squeezes out the gaps: That is TM M has new Godel number r, if in the old Godel numbering it had the {r+1}^th legitmate Godel number of a TM.

One proves easily that the map from old Godel numbers to new ones and its inverse are given by primitive recursive functions.

The usual S_m_n theorem is implemented by a primitive recursive function. Hence with respect to the new Godel numbering it is also true that the S_m_n function is primitive recursive.

But this is all one needs to make the proof in section 5 work.

N. B. I'm not saying there is anything wrong with your "new Godel numbering" approach: it's just unnecessary.

2. Since the notion of "Sigma_1 sound" is figuring prominently in the discussion, I should point out that the definition you give of this concept in your paper is not the standard one. [I am using the standard definition.].

Since your definition in remark 6.7 does not require that the predicate P is recursive, it amounts [in the case of PA] to asserting that every theorem of PA is true: that is PA holds in the standard model.

This is certainly provable in ZFC, but it can't even be formulated as a single sentence of PA.

The usual notion is obtained by requiring that the predicate P be "primitive recursive". What this means is a little dicy, but roughly it goes as follows:

Godel has shown how to associate to any primitive recursive definition of a primitive recursive predicate a formula [in the appropriate number of variables] that (a) numeralwise-expresses the prim. rec. predicate; (b) defines it in the standard model. It is the particular formulas yielded by Godel's construction that we refer to as "primitive recursive formulas of the language of PA".

We would get an equivalent concept if we required P to be a Delta_0 formula.

3. I want next to formulate precisely "Kreisel's Theorem on the provably recursive functions of PA". [Henceforth KT.] It is crucial for what follows that this can be formulated as an arithmetic sentence.

I am going to differ somewhat from the conventions of the anonymous referree:

By a PA-provably recursive function, I mean a *total* recursive function f such that for some Godel number e for a Turing machine that computes f, PA proves, e is the Godel number of a total function.

KT asserts the following:

The following are equivalent:

1) f is a PA-provably recursive function.

2) For some alpha < epsilon_0, f is primitive recursive in F_{alpha}.

End of statement.

I know two proofs of KT. Neither of them is trivial:

1) One can use Gentzen's ordinal analysis of PA.

2) One can use the Paris-Harrington techniques combined with the results of Solovay-Ketonen.

4. The following propositions are all provably equivalent in PA:

1) PA is Sigma_1-sound.

2) For all alpha < epsilon_0, F_alpha is total.

[Really, we are using an appropriate primitive recursive function which assigns to every [Godel number of an] alpha < epsilon_0 a Godel number of a TM that computes F_alpha.]

3) F_{epsilon_0} is total.

4) KT

5. You asked for references on all this. I don't know a concise treatment of just these facts. But here are some sources:

1) There is a paper of Tait in the J. S. L. called "The epsilon substitution method". It was written a long time ago and I don't have the precise cite. But if I recall correctly, this is where I learned about ordinal analysis.

2) There is Gentzen's collected works.

3) For the Paris-Harrington approach, there is the book by Hajek and Pudlak:

Metamathematics of first-order arithmetic /
Petr Hajek, Pavel Pudlak
Publisher
Berlin ; New York : Springer-Verlag, v1993

6. I still agree that you have proved that the counterexample function overtakes all recursive functions. I stand by my comments in my prior letter concerning this point.

7. Again, I found your definition of G_{\epsilon_0} a bit vague. So I worked with F_{\epsilon_0} [as in my paper with Ketonen]. So in what follows, I will take the class C^{\epsilon_0} as defined using F_{\epsilon_0}.

With that proviso, I agree with my prior comment:

So it is indeed routine to prove in the theory "PA + 'PA is Sigma_1-sound' " that the machines in C^{\epsilon_0} are total.

8. I come to a crucial change from my prior letters:

You ask:

>
> 3) Do you think that we have proved that [P<NP]^B_{\epsilon_0} cannot be
> proved in PA from the viewpoint of the enlarged theory PA + "PA is
> Sigma_1 sound"?
>

I now think that you did not quite prove this. The trouble is that you only consider the case when C is a subset of {\cal P}. But for the particular C^{\epsilon_0} that you consider, it can well happen in some model of PA, that it is *not* a subset of {\cal P}.

9. Lets consider next what is actually happening.

The following equivalences are provable in PA:

A: The following are equivalent:

1) P < NP.

2) The proposition you call [P < NP]^B.

B: The following are equivalent:

1) (P < NP) and (P is Sigma_1-sound).

2) [P < NP]^B_{\epsilon_0}.

The proof of equivalence B is not difficult. The essential point is the following.

You introduce on page 10, the machine Q^{h(n)}. [The notation, by the way is abysmal. The machine depends *not* on h(n), but on n and a Godel number for h. Then if h(n) is undefined, then Q^{h(n)}is also totally undefined, and so the function f_{\neg A} is undefined on the Godel number of Q^{h(n)}.

From these equivalences, the following consequence is easy:

C: PA proves [P < NP]^B_{\epsilon_0} iff PA is inconsistent. [This is a theorem of PA.]

10. The following is a shade less trivial:

Theorem(PA):

The following are equivalent:

1) PA proves "If P < NP, then PA is Sigma_1-sound".

2) PA proves the equivalence of [P < NP]^B and [P < NP]^B_{\epsilon_0}.

Proof: In view of the equivalences A and B above, 2) is equivalent to:

2') PA proves the equivalence of (P < NP) and [(P < NP) and "PA is Sigma_1-sound"]

By propositional logic, 2') is equivalent to:

1) PA proves: If P < NP, then PA is Sigma_1-sound.

11. I certainly can't rule out 1). It would hold if PA proved P = NP. It would also hold in the [unlikely] case that "P < NP" is equivalent to "PA is Sigma_1-sound".

But 1) is certainly far from evident.

Este review, que nos foi enviado em 9 de dezembro de 2001, tem diversos pontos cruciais para nosso trabalho: confirma a relação que tínhamos obtido,

$$[P<NP]^F \text{ se e somente se } \{[P<NP] \text{ e } [PA \text{ é } \Sigma_1 \text{ sound}]\}.$$

(Isso mostra que a definição que tínhamos usado para a idéia informal P<NP, escrita $[P<NP]^F$, não era totalmente equivalente à definição standard, que chamáramos “definição no conjunto BGS.”) Mostra também que nossos resultados sobre a função contraexemplo eram corretos:

6. I still agree that you have proved that the counterexample function overtakes all recursive functions. I stand by my comments in my prior letter concerning this point.

E, ponto crucial, na referência que repito:

1. Your paper makes a big deal about using an exotic Godel numbering for Turing machines so that Lemma 6 holds. But there is no need to do this.

a) One has the "usual" Godel numbering of TM's. This set of Godel numbers is primitive recursive, but not every number is the Godel number of a TM.

b) Next one squeezes out the gaps: That is TM M has new Godel number r, if in the old Godel numbering it had the {r+1}^th legitmate

Godel number of a TM.

One proves easily that the map from old Godel numbers to new ones and its inverse are given by primitive recursive functions.

The usual S_m_n theorem is implemented by a primitive recursive function. Hence with respect to the new Godel numbering it is also true that the S_m_n function is primitive recursive.

But this is all one needs to make the proof in section 5 work.

N. B. I'm not saying there is anything wrong with your "new Godel numbering" approach: it's just unnecessary.

Esta observação sobre a numeração de Gödel que usamos no preprint de 2001 é decisiva, porque num preprint em que pretende nos contestar, Ralf Schindler comete um erro surpreendente: não percebe que bastava usarmos o teorema s-m-n para obter o sistema de números de Gödel necessário à prova do crescimento rápido da função contraexemplo. Aliás, noutra comunicação privada, Marcel Guillaume confirmou-nos que bastava usar o teorema s-m-n. Por que não o usáramos desde o início? Estávamos tentando manter tudo polinomial, e estendemos essa condição aos números de Gödel para as máquinas polinomiais, numa construção complicada mas correta, como se vê na referência acima. Depois vimos que bastava manter primitivo-recursivos os números de Gödel.

(Schindler comete outro erro incompreensível, ao menos: confunde funções recursivas totais com funções recursivas PA-provadamente totais. Isso lhe atrapalha boa parte da crítica.)

Nossos principais resultados do artigo de 2003, devo acrescentar, já estão todos citados no review supra para o caso de PA. No artigo de 2003 fizemos todas as provas explicita e computacionalmente, e estendemos tudo para ZFC. Uma questão levantada, se é que ocorre:

PA proves: If $P < NP$, then PA is Sigma_1-sound,

foi respondida em parte, pois é consistente a teoria:

ZFC + se $P<NP$ então ZFC is $\sum_1$– sound.

se ZFC for consistente, conforme o mostramos em nosso trabalho de 2003. Tal condição é demonstrada na teoria ZFC + ZFC é $\sum_1$–sound, que é o primeiro degrau numa hierarquia de iterações de ZFC com um princípio de reflexão. E, lembro enfim, a hierarquia de Turing-Feferman decide o problema P vs. NP — apenas, não sabemos ainda como…

O artigo de 2003.

Resolvemos, em meados de 2002, da Costa e eu, publicar um primeiro artigo com nossas idéias. Seria um artigo contra as tendências majoritárias na área: Razborov defendia, desde 1993, que eventualmente se demonstraria P<NP ao menos na teoria dos conjuntos, e usando alguma "técnica extraordinária," nova e muito forte; Freedman procurou-a em topologia. Para nós, o problema P vs. NP pode ser resolvido com técnicas simples, embora emanando de resultados muito profundos — em nosso trabalho de 2003, explicitamos todas as provas realizadas no âmbito de sistemas formais, mas partimos de resultados profundos, como a solução do Décimo Problema de Hilbert, ou a prova de Kleene, dada em 1936, para o teorema de Gödel, usando sentenças Π_2, além, com certeza, de propriedades de um tipo específico de princípio de reflexão, a Σ_1–soundness da teoria ZFC.

Pedimos a ajuda de Marcel Guillaume, de Clermont-Ferrand, lógico internacionalmente famoso, que concordou em fazer um review em privado de nosso trabalho. A colaboração de Guillaume foi essencial para o resultado obtido, que consideramos muito bom. Corrigidos todas as dificuldades, contactamos a editoria de *Applied Mathematics and Computation*, que concordou em examinar o artigo. Devo enfatizar que os referees de AMC nada exigiram, embora o artigo tenha estado sob avaliação durante um tempo longo, nove meses. Foi aceito em junho de 2003, e saiu no final do ano[18]. A idéia central é "clonar" a função F, descrita pela primeira vez no artigo de Kleene de 1936, tal que ZFC não pode prová-la recursiva total, embora ela seja intuitivamente total. Com isto obtemos resultados de incompletude que levam à consistência da teoria ZFC + $[P=NP]^F$, se ZFC for consistente. Noto que *nada disso é contestado por Schindler, inclusive em contradição a seu review anterior, publicado apenas como preprint na net.* A discussão central está na condição:

ZFC + $[P=NP]^F$ + [ZFC é Σ_1–sound] é uma teoria consistente.

Tal condição é altamente não trivial do ponto de vista técnico, mas possui uma interpretacão simples: sabe-se que a teoria ZFC + $[P=NP]^F$ é uma teoria consistente, se ZFC o for. No entanto pode-se mostrar que tal teoria terá um modelo com aritmética standard se e somente se ZFC provar P=NP. Nesse caso específico, as três condições supra são imediatamente consistentes. Mas se ZFC + $[P=NP]^F$ for apenas consistente, porque ZFC + $[P<NP]^F$ também o é, ZFC + $[P=NP]^F$ terá apenas modelos com aritmética não standard. Então a tripla condição supra significará, intuitivamente, que nalgum modelo não-standard para ZFC + $[P=NP]^F$ teremos que máquinas intuitivamente polinomiais têm, de fato, uma interpretação polinomial. Ou seja, o sistema formal, de algum modo, traduz conceitos intuitivos; e isso é o que esperamos de um sistema formal.

Schindler afirma, sem provas, que a condição supra é inconsistente. Por que não nos aprofundamos a respeito no artigo? Condições fortes como a exposta supra são correntes em matemática: por exemplo, todos os axiomas de grandes cardinais, que beiram a inconsistência. A condição supra é muito forte porque implica a sentença formal Consis (ZFC), que afirma a consistência de ZFC. Isso pode ser visto num cálculo direto, ou por exemplo nos trabalhos de Beklemishev e Franzen citados acima. Também sabemos que:

ZFC prova {[ZFC é Σ_1–sound] se e somente se [F é total]}.

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

Há uma prova direta desse fato, longa mas elucidativa, feita pelos autores e examinada por Guillaume, ainda inédita, e provas mais simples, menos esclarecedoras do que acontece, também vistas nos trabalhos citados, provas que resultam da equivalência de princípios de reflexão $\sum_1$ e $\prod_2$, equivalência demonstrável em fragmentos da aritmética.

E' plausível que condições como estas que discutimos inclusive impliqume na existência de um grande cardinal; há evidências que sugerem tal fato, e que merecem um esclarecimento.

A leitura da resenha de Schindler mostra que ele, um matemático em cujo currículo nada de especialmente notável existe, ignora todos esses fatos, resultados ou mesmo conjecturas. Já enviamos à revista AMC um "Addendum,"[19] onde notamos que toda a adjetivação de Schindler em sua resenha resulta em dois fatos: o nosso trabalho está correto, e a condição:

$$\text{ZFC} + [\text{P=NP}]^F + [\text{ZFC é } \textstyle\sum_1\text{–sound}] \text{ é uma teoria consistente}$$

merece uma fundamentação técnica, que ofereceremos.

Note-se que se tal condição não for consistente, então resultará direto que ZFC prova P<NP. Isto, no entanto, não parece plausível, face ao que sabemos sobre a função contraexemplo e seu comportamento no modelo standard — que é onde teremos P<NP, se demonstrado em ZFC (com aritmética standard) ou ao menos se consistente com ZFC, e que é onde vemos o "mundo real," se é que se pode usar tal termo sem maiores cautelas, para a teoria da computação.

Quero deixar claro que logo após a aceitação do artigo pela revista AMC, enviei dele cópias a vários colegas, como Greg Chaitin (que o mencionou, sem julgamentos, num artigo na página da MAS, depois publicado no *Mathematical Intelligencer*) e a Alasdair Urquhart, editor de reviews do *Bulletin of Symbolic Logic*. Não sou ingênuo a ponto de achar que um artigo lidando com uma questão em aberto de tal tamanho vai ter um julgamento sem esquadrinhamento minucioso, o que serve como refereeing extra, pós-publicação. Sabemos agora que precisamos de fato, como pressentíamos, esclarecer o status da tripla condição acima.

Em várias trocas de mensagens com Guillaume, sugeriu-nos este outra versão, enfraquecida, da nossa definição exótica. Tal versão, para reproduzirmos os resultados mencionados, exige uma condição de consistência bem mais fraca,

$$\text{ZFC} + [\text{F tem um domínio infinito}] + \neg[\text{F é total}] \text{ é consistente.}$$

Se tal condição se verificar, temos que ZFC + [F tem um domínio infinito] não prova nem

[19] Alasdair Urquhart enviou-me uma mensagem dizendo que não é política da seção de Reviews do *Bulletin* publicar contestações às suas resenhas. O *addendum* sairá como: N. C. A. da Costa and F. A. Doria, "Addendum to: Consequences of an exotic definition for P=NP," *Applied Mathematics and Computation* (a sair, 2o. semestre de 2005).

desprova [F é total], e vale no modelo standard. Logo, a teoria ZFC + [F tem um domínio infinito] possui as mesmas funções provadamente totais que ZFC.

Tal condição possui outra vantagem: envolve apenas ZFC e um princípio de reflexão, parcialmente negado. Precisamos de um modelo onde um princípio de reflexão tenha falhas (será necessariamente um modelo com aritmética não standard) mas ainda assim funcione individualmente infinitas vezes. Que tal um modelo de ZFC onde valham sentenças do tipo "existe um c, e c é o número de Gödel de uma prova de ¬ (0 = 0)," "existe um c', e c' é o número de Gödel de uma prova de ¬ (1 = 1)," "existe um c'', e c'' é o número de Gödel de uma prova de ¬ (2 = 2),", … "existe um $c^{[k]}$, e $c^{[k]}$ é o número de Gödel de uma prova de ¬ (k = k)," …

Estamos, no momento, examinando tal sistema formal e seus modelos, obrigatoriamente não-standard.

Lembro, concluindo esta seção, que controvérsia é parte do desenvolvimento da ciência. O relatório do resenhista do CNPq faz uma afirmativa genérica,

> [Schindler] mostra como a pretensão exagerada do proponente resulta em afirmações problemáticas e de fundamentação duvidosa.

Do jeito que está, é como se Schindler, de um golpe, demolisse meus vinte anos de trabalho com Newton da Costa. O resenhista do CNPq parece, com isso, querer desvalorizar e desmerecer todo o meu trabalho, desde fins dos anos 80. Como mostrei, no entanto, pesquisadores do nível de Smale, Kreisel, Stewart e outros já o esquadrinharam sem lhe encontrarem falhas. Penso, se me permitem, que o resenhista do CNPq, talvez assoberbado com outras responsabilidades, não examinou e não conhece meu trabalho, simplesmente.

Ou, quem sabe, desejou esquecer as controvérsias da história da matemática: Weierstrass contra Kronecker, Kronecker contra Cantor, as discussões sobre o Axioma da Escolha, o recente debate sobre o axioma do "dardo no alvo," que decide a hipótese do continuum, ou a muito recente controvérsia entre Stephen Simpson e Harvey Friedmann, ocorrendo justo agora, neste momento, em começos de 2005, sobre graus incompletos recursivamente enumeráveis e "naturais" (aspeio porque é o ponto em debate). No nosso caso, temos uma condição metamatemática forte, de interpretação intuitiva, que está sendo debatida.

Ciência vive de controvérsia, precisa de controvérsia[20]

---

[20] Noto que os resultados do trabalho de 2003 sobre o P vs. NP estão sendo reiterados e republicados, com nova discussão agora, em V. Velupillai, ed., *Computability, Complexity and Constructivity in Economic Analysis,* Blackwell (2005), no capítulo, de minha autoria com Newton da Costa, "Computing the future." Cito o comentário do editor no prefácio:

> In the late 1980s the issue of undecidability in dynamics was beginning to be given serious attention. Two of the absolute pioneers in this pioneering attempt were Newton da Costa and Francisco Doria (cf. Costa & Doria, 1991, Stewart, 1991). Almost simultaneously with this pioneering work, da Costa and Doria, together

Princípios de Reflexão, novamente.

Voltamos ao ponto de partida. As questões sobre a ontologia da matemática que me interessam dizem respeito aos princípios de reflexão.

Conto a idéia motivadora. Há cerca de dez anos, como já o referi, Kenneth Kunen publicou um artigo no qual exibe um algoritmo (programa de computador) que prova a consistência da aritmética de Peano, PA — o algoritmo de Kunen prova o teorema de Paris-Harrington, que implica a consistência de PA. Como é isso possível? Algoritmos são, digamos, objetos aritméticos. Não temos aqui uma violação do segundo teorema de incompletude de Goedel? Não, na verdade: pois vê-se intuitivamente que o algoritmo leva ao resultado pretendido, embora tal fato não possa ser provado em PA, devido a um segmento indutivo no algoritmo que corresponde à indução transfinita da prova de Gentzen.

De imediato vi, nesse resultado de Kunen, o contraste entre a matemática intuitiva, em cujo âmbito podemos dizer que se dá a prova de consistência de Kunen, e a matemática formal, na qual temos o fenômeno da incompletude. A consistência, no argumento de Kunen, é, podemos dizer, óbvia; resulta da convergência, percebida intuitivamente, do algoritmo que exibe. Algo como o que justifica, no entender de Feferman, seus Princípios de Reflexão. Como diz Feferman, os princípios de reflexão simplesmente afirmam a sensatez (soundness) da teoria. E iterados até um ordinal transfinito construtivo mas relativamente pequeno, permitem tornarmos completa, ao longo da hierarquia aritmética, a teoria. Franzen, no artigo também acima referido, ao examinar a completude de Turing-Feferman, acha que nada ganhamos quanto a informações novas. Devo dizer que não

---

with Marcelo Tsuji, began investigating undecidability issues in finite structures and applications in economics, particularly in game theory. Contrary to popular misconceptions about the feasibility of applying 'simple' counting arguments to determine equilibria in finite games, da Costa and Doria were able to show how slippery such illusions can be. Economists interested in questions of dynamics and formulations of all kinds of economic problems in game theoretic frameworks have not had access to this collection of impressive work by what I have come to call the 'Brazilian School'. In their contribution to this volume, with the alluring title '*Computing the Future*', da Costa and Doria give a towering survey of a decade and a half of foundational work on the mathematical foundations of the philosophy, epistemology and methodology of modelling with serious computational foundations and their implications. The crowing achievement of their contribution, in this writer's opinion, is the development of a version of Rice's Theorem in the context of analysis. Economists who might be led to believe that recasting general equilibrium theory in terms of recursive analysis would do well to pay heed to this new theorem. The da Costa-Doria contribution is entirely self contained in terms of the mathematics, except for standard notions of recursion theory.

concordo. E adianto que o cerne do meu argumento será buscar a construção de uma sequência enumerável de funções recursivas monotonamente crescentes, intuitivamente totais, com a propriedade de que, dada uma função recursiva total qualquer, existe uma função na sequência que a domina.

Tal sequência apresenta uma propriedade peculiaríssima: ela pode ser caracterizada intuitivamente, mas nenhuma extensão "aritmeticamente sensata" (*arithmetically sound*) de ZFC, com um conjunto recursivamente enumerável de teoremas, pode caracterizá-la formalmente. A sequência descrita, se existir, será, como se vê, dominada pela função Busy Beaver. E, como se sabe, há equivalência provada, em ZFC e em PA ou extensões, entre cada função na sequência em causa, ou entre funções recursivas totais dominadas por alguma similar na sequência construída, e um princípio particular de reflexão.

Ou seja: tal sequência levará diretamente à hierarquia de teorias necessária ao teorema de Turing-Feferman.

O objetivo é fazer a construção da sequência, ou ver que obstáculos metamatemáticos existem a quando buscamos realizar tal construção. Se assim feito com sucesso, daí seguirá a completude de Turing-Feferman.

Por trás uma questão que considero básica sobre a ontologia da matemática*: o que melhor a descreve, a matemática formal ou a informal? Se a informal, como caracterizá-la?*

Aqui tudo se fecha: dos princípios de reflexão (nosso ponto de entrada para questões referentes à ontologia da matemática) chegamos à prova das sentenças verdadeiras na hierarquia aritmética, implicada também pelo modelo que propusemos para a hipercomputação. E um princípio de reflexão está no cerne da condição metamatemática em nosso trabalho de 2003, condição que Ralf Schindler não quis aceitar.

Todas as questões aqui levantadas baseiam-se em tópicos fartamente discutidos pela filosofia da matemática ao longo do século XX:

- completude de sistemas formais,
- o fenômeno da incompletude de Gödel,
- o problema da consistência da aritmética e de um sistema tão poderoso quanto ZFC,
- a relação entre sistemas formais e construções intuitivas.

O conceito de estrutura matemática, o que é formalização, a idéia de Bourbaki de caracterizar objetos matemáticos através de "espécies de estruturas," tudo isso acaba sendo considerado, ponderado e empregado nas nossas discussões.

Enfatizo um ponto: *não se pode fazer filosofia da matemática sem um bom conhecimento, um conhecimento que se pode dizer ativo, da prática matemática em determinadas questões de ponta.* Um exemplo é a própria prova de Kunen, acima referida: como pode um algoritmo, objeto aritmético, demonstrar a consistência da aritmética? Porque tal algoritmo não pode ser internalizado mesmo em teorias aritméticas fortes, como a aritmética de

Peano. Tal explicação é imediata a quem trabalha no assunto, mas confunde com frequência quem não está habituado ao dia-a-dia de tais questões. Os Princípios de Reflexão têm uma história já de quase sete décadas: e sua natureza é ainda mal percebida; veja-se por exemplo, o próprio artigo de Feferman de 1962, quando este os justifica. De fato, há sistemas formais aos quais não podem ser aplicados — vários sistemas que não têm porção aritmética standard.

Com o que passamos a outra questão essencialmente filosófica: o que é mais "natural," o modelo standard para a aritmética ou os modelos não-standard? Os modelos não-standard têm raízes nos infinitésimos, *ghosts of departed quantities*, conceito que surge no fim do século XVII, e que só é formalizado em meados do século XX, com a construção dos ultrafiltros. Compreendemos hoje que uma teoria como PA + ¬Consis PA só possa ter modelos não-standard, porque o número de Gödel não-standard da prova de ¬(0=0) não pode ser efetivamente decodificado numa prova de tal fato. Mas falta, como disse, estender tais idéias para os Princípios de Reflexão mais complexos, além do nível $\sum_0$. E permanece a questão básica: será que teremos ganho alguma coisa se provarmos que há modelos não-standard nos quais vale P=NP, como parece ser o caso?

Ou seja: a observação, feita pelo resenhista do CNPq, na qual diz que isto é "de uma enorme trivialidade," mostra que tal resenhista tem uma visão altamente não-trivial do que sejam trivialidades…

Formação de pessoal.

Lembro que, no ítem formação de pessoal, devem ser considerados dois aspectos, o quantitativo e o qualitativo. Entre meus alunos de pós-graduação conto Marcelo Gleiser, de Dartmouth, que me fez calorosas referências em recente entrevista na televisão, concedida a Roberto D'Avila, e José Acácio de Barros, que há dez anos trabalha com Pat Suppes em Stanford. Por outro lado, tenho dúvidas se destas questões poderia tirar temas de teses de doutorado (mestrado nem se fala). São, de fato, questões na fronteira do conhecimento. São temas de pesquisa, e não temas que sirvam de exemplos didáticos, já que uma tese de doutorado é apenas a última etapa na formação de um pesquisador. Se me permitem, estas idéias que expus e que tenho desenvolvido são, em parte, um salto no escuro: posso encontrar, aqui, muita coisa interessante, no meu trabalho, mas muita surpresa e coisa nova pode também me confrontar neste caminho.

A questão da repercussão de meus resultados.

Como já falei, controvérsia faz parte da ciência, às vezes de modo trágico, como no caso que levou ao suicídio de Boltzmann, cujas idéias e resultados foram violentamente criticados por Ernst Mach. A parte nova que deveremos utilizar para completarmos, da Costa e eu, nosso trabalho sobre o P vs. NP, exige a compreensão da natureza de modelos para teorias como:

ZFC + [F tem um domínio infinito] + ¬[F é total].

Serão modelos nao-standard, como disse. E' possível que nos seja necessário usar algum princípio forte, heuristicamente justificável mas de prova em aberto ou impossível. De modo que o *affair* Schindler é apenas o começo da discussão…

De 2l de março vindouro a 25 realiza-se em Galway, na Irlanda, um simpósio sobre fundamentos computacionais das teorias econômicas; nele farei duas conferências sobre meus trabalhos nestes últimos quinze anos, uma delas sobre P vs. NP. Prepara-se outra conferência similar para Trento, em setembro do corrente, onde de novo devo falar sobre complexidade computacional e P vs. NP. Logo, meu espaço está garantido no caso, internacionalmente. Que defendo no tema uma tese controversa, sei-o bem, mas — controvérsia é parte do jogo a ser jogado.

Faço, enfim, uma observação final: o parecer do CNPq a respeito do meu trabalho é fortemente adjetivado de modo a me depreciar, o que considero um tratamento altamente injusto. Ao fazer isso, com diria meu mestre Prof. Leopoldo Nachbin, o resenhista não atinge somente a minha pessoa, mas um grande número de professores, alunos e pesquisadores, brasileiros e estrangeiros, com que colaborei em toda a minha vida, e que de uma forma ou outra deram a sua aprovação ao meu trabalho acadêmico.

Rio, 5 de março de 2005

Francisco Antonio de Moraes Accioli Doria

Como exemplo, junto o parecer com o qual o livro *Metamathematics of Science* (título provisório) foi aceito pela Kluwer, hoje Springer Verlag. (Tal parecer me foi comunicado, sem sua autoria, pela Kluwer.)

Dear Inge Hardon

Thank you very much for sending me all the detailed supporting material
for the Doria/da Costa "Metamathematics of Science" book proposal!
To summarize, I feel that this is a work of historic importance and
significance, and that publishing it will considerably contribute to
Kluwer Academic's prestige.

da Costa and Doria have been pursuing, almost single handedly,
this very fundamental and important research program for many years.
Their work is scattered in many papers in many different journals,
and it is important to gather all this work in one volume and to
explain
it in a more leisurely fashion than is possible in journal papers,
because Metamathematics of Science, combining as it does, ideas
from physics, logic, theory of computation, and philosophy, is a work
that will be of tremendous interdisciplinary interest and significance.

I feel it is impossible to overstate the significance and importance
of this book, and that it certainly deserves the most prestigious
academic publisher that is possible. I very much hope that you
will be that publisher.

Best wishes, and thanks very much for asking me for my opinion;
it has been a privilege and a pleasure for me to review the da Costa/

Doria book proposal for "Metamathematics of Science".