

Prof. Erney Plessmann de Camargo,
DD. Presidente, CNPq.
Brasília, DF.

Em 23 de Fevereiro de 2006.

Senhor Presidente,

Embora pela segunda vez consecutiva tenha deixado de receber qualquer resposta a meu pedido de bolsa de produtividade em pesquisa, venho por meio desta reiterá-lo, nos termos da documentação já existente neste CNPq. Permito-me usar de caminhos não ortodoxos para peticionar a esta entidade porque, afinal, em nada tem sido ortodoxo o CNPq face a meus pedidos.

Acrescento, em anexo, tudo o que já foi realizado do programa proposto de pesquisas. Ressalto, se me permite V. S., dois pontos: primeiro, a publicação, já disponível pela web no site da ScienceDirect, do número sobre hipercomputação, da revista *Applied Mathematics and Computation*, que co-editei. E, em segundo lugar, como que acatando a relevância filosófica de meus trabalhos, informo a V. S. que venho de ser eleito membro da Academia Brasileira de Filosofia.

Atenciosa e respeitosamente sempre,

Francisco Antonio Doria

Solicitação de Bolsa de Pesquisa — Addendum

Francisco Antonio Doria

Fevereiro de 2006

No pedido encaminhado há cerca de um ano, propunha-me a estudar três problemas, reunidos debaixo de uma questão unificadora, os *princípios de reflexão*. Eram os seguintes os problemas a serem desenvolvidos:

- A questão da hipercomputação.
- Progressões de funções recursivas totais e completude aritmética de teorias formais.
- Tópicos sobre o problema *P vs. NP*.

A unidade conceitual do projeto está discutida no texto encaminhado em resposta ao peculiar parecer que me foi enviado em fevereiro de 2005. Aqui me restrinjo a questões específicas e ao que foi feito e aprendido desde então.

1 Hipercomputação

Hipercomputação é uma aposta segura. Mais cedo ou mais tarde alguém vai conceber teoricamente um algoritmo que seja não-trivialmente realizável em termos concretos, e que decida instâncias interessantes do Problema da Parada. Que em certos casos isso pode sempre ser feito de modo simples, é óbvio pelo exemplo do algoritmo de Kunen, que prova diversas questões indecidíveis no âmbito da aritmética de Peano (PA) — usamos aqui a relação bem conhecida entre indecidibilidade e incompletude em teorias como PA.

Propus, em fins de 2004, aos editores de *Applied Mathematics and Computation*, revista da Elsevier, o preparo de um número especial, tendo a hipercomputação como tema. Fomos editores de tal número José Félix Costa, da Univ. Técnica de Lisboa, e eu. O trabalho — convites aos colaboradores, refereeing, correções eventuais — concluiu-se em inícios de setembro de 2005, já estando o número inteiro da revista disponível online, através do ScienceDirect. Noto que o primeiro texto da coletânea é de Martin Davis, um crítico acérrimo da possibilidade de desenvolvimento de hipercomputadores, mas que acedeu a nosso convite para apresentar, in loco, seu ponto de vista.

O texto de abertura do número, assinado por Félix e por mim, é de minha autoria. No artigo — expositivo — que contribuimos, Newton da Costa e eu, apresentamos uma idéia antiga nossa para um possível hipercomputador, o uso de máquinas analógicas servindo de oráculos para máquinas de Turing (e eventualmente, para computadores digitais), o que, teoricamente, faz o sistema funcionar como um hipercomputador. Também discutimos, brevemente embora, o

fenômeno ainda obscuro da completude aritmética de teorias às quais se acrescentam princípios de reflexão, as chamadas teorias de Turing–Fefermann.

2 Funções recursivas de crescimento rápido

Um dos objetos mais interessantes dentro da teoria da recursão é a função *Busy Beaver*, primeiro exemplo explícito de uma função de crescimento rápido (na verdade, monstruosamente rápido) e não computável. Na prova clássica de Radò, fica fácil ver que a Busy Beaver domina qualquer função recursiva total.

Em decorrência, embora possamos definir a função Busy Beaver em teorias como PA ou suas extensões, não é possível demonstrar que esta função é total em tais teorias — porque então mostraríamos serem total funções recursivas que não podem ter sua totalidade provada em tais teorias.

Mas, será que podemos construir nalgum contexto razoável uma sequência recursiva, ou ao menos recursivamente enumerável, de funções totais, tal que (num sentido que faríamos preciso), seu supremo seja a função Busy Beaver?

Tal sequência pode, aparentemente, ser construída no modelo standard (ou na teoria PA + regra ω), embora nenhuma teoria que possua um conjunto recursivamente enumerável de teoremas possa descrevê-la em todas as suas propriedades. Tal sequência, de certo modo, substitui a iteração de teorias que caracteriza o teorema de Turing–Fefermann e permite, penso, a prova algo mais intuitiva deste teorema de completude para a aritmética.

Tal sequência tem também importância para o problema *P vs. NP*, especificamente na construção de sequências de funções F_0, F_1, \dots , e G_0, G_1, \dots (ver abaixo).

3 O Problema *P vs. NP*

Como persistem incompreensões sobre nosso enfoque (de N. da Costa e meu) a respeito deste problema, faço um breve resumo da maneira como o abordamos.

- A sentença formal $P < NP$ ou $P \neq NP$ é uma sentença aritmética Π_2 , e como tal pode ser construída na aritmética de Peano (PA) — na verdade, podemos formulá-la mesmo na aritmética primitivo recursiva (PRA).
- Seja T uma teoria que inclui a aritmética, possui um modelo com a porção aritmética standard, possui um conjunto recursivamente enumerável de teoremas e baseia-se no cálculo clássico de predicados.
- T prova a sentença Π_2 ξ se e somente se certa função recursiva f_ξ , cujo número de Gödel depende recursivamente da matriz de ξ , for provada total por T .

Dito mais simplesmente: T prova ξ se e somente se provar que f_ξ é total. E construímos f_ξ , recursivamente, a partir de ξ .

O que fizemos foi examinar esta função f_ξ . Tentamos usar o resultado:

Se f_ξ for total, e dominar, no modelo standard, todas as funções recursivas provadamente totais na teoria T , então f_ξ não pode ser provada total em T . \square

Mas o problema é que f_ξ , por si só, é uma função difícil de lidar, no caso de $P < NP$. Nosso enfoque consistiu então em:

- Construímos explicitamente $[P < NP]$, a sentença Π_2 que traduz a correspondente hipótese, numa teoria T como a acima descrita.
- Tais teorias têm funções (notadas F_T) que são obtidas por meio de uma diagonalização sobre todas as funções recursivas que T prova totais. Tais funções (notadas F_T) são recursivas parciais com número de Gödel (programa) explícito, mas T não as prova totais ou estritamente parciais.
- Construímos outra sentença formal Π_2 , $[P < NP]^F$, que, no modelo standard, equivale a $[P < NP]$ mas tal que T não lhes prova a equivalência (na verdade, tal equivalência é indecidível em T).
- Para tal sentença, mostramos que T não prova $[P < NP]^F$.

Lembremos que esta nova sentença $[P < NP]^F$ é, intuitivamente, $[P < NP]$, embora não tenhamos para ambas uma equivalência formal em T . E sua negação, $[P = NP]^F$, é, intuitivamente, $[P = NP]$. Nossos resultados supra mostram:

- Se T é consistente, então $T + [P = NP]^F$ é consistente.
- Dada certa condição metamatemática complexa, $T + [P = NP]$ é consistente. (Tal condição é implicada por uma outra condição de significado intuitivo, mas difícil de se verificar: se a teoria $T + [P = NP]^F$ for ω -consistente, então $T + [P = NP]$ é consistente.)

Este, em resumo, o conteúdo de nosso artigo de 2003. Todas as críticas concentraram-se na condição metamatemática imposta para deduzir a consistência de $T + [P = NP]$. De fato, é condição formalmente não trivial, mas com uma interpretação simples: a teoria $T + [P = NP]^F$, que sabemos ser consistente, possuiria um modelo onde máquinas de Turing se comportam de acordo com nossas intuições a seu respeito (e, admitimos, sem prova pode-se objetar que tal modelo não existiria).

Neste ano findo de 2005, desde o encontro de Galway, em março, tentei, com N. da Costa, contornar tais dificuldades. Percebemos que as bases da solução do problema já estavam (ou estariam) dadas no artigo de 2003, com exceção de uma mudança na função F , que substituímos por outra, G , com propriedades similares às de F , mas com certos aspectos indecidíveis explicitados. Em resumo, se estivermos corretos, teremos o seguinte:

- Se T possuir um modelo com a aritmética standard, então $T + [P < NP] \leftrightarrow [P < NP]^F$ é consistente.

- Em consequência, $T + [P < NP] \leftrightarrow [P < NP]^F + [P = NP]^F$ é consistente.
- Daí segue a consistência desejada, de $T + [P = NP]$.

Tal trabalho está em fase final de elaboração.

Nota sobre problemas difíceis

N. da Costa e o signatário já tiveram sucesso na solução de dois problemas de interesse existentes na literatura, o problema de decisão para sistemas caóticos (Problema de Hirsch), e o problema de decisão para classes de equilíbrios em sistemas dinâmicos (Problema de Arnol'd). O problema P vs. NP certamente excede bastante aqueles em dificuldade, além de ter muito maior notoriedade. Nossos resultados a respeito, expostos no trabalho de 2003, estão corretos, embora se defrontem a um obstáculo que procuramos agora ultrapassar. Em 2003 prosseguimos, na verdade, uma abordagem para a questão que se inicia nos anos 1970 com artigos de Hartmanis e Hopcroft, DeMillo e Lipton, depois O'Donnell, Fortune et al., Kowalczyk, Maté, entre outros. Portanto, não é um caminho de aventuras, isolado: temos precedentes sabidos, com os seguintes resultados já conhecidos:

- Para vários fragmentos da aritmética F , sabe-se que $F + [P = NP]$ é consistente.
- Para teorias T , que incluem PA, sabe-se que $T + [P = NP]$ é consistente dada, sempre (até hoje), alguma condição metamatemática não trivial.

Portanto, estamos obtendo resultados que estendem, nessa linha, o que já se sabe a respeito da questão.

Linhas futuras de trabalho

Caso estejamos certos, e se tivermos obtido a consistência de $T + [P = NP]$, dada uma condição metamatemática razoável, teremos que nos voltar para o problema da consistência de $T + [P < NP]$.

Pouco se sabe sobre tal consistência, que não aparece na literatura. Mas conhecemos:

- Se $[P = NP]$ é verdadeiro no modelo standard (= no mundo real, digamos assim), então T prova $[P = NP]$.
- Se $T + [P < NP]$ é consistente, então $[P < NP]$ é verdadeiro no modelo standard. Se ocorrer independência, $T + [P = NP]$ terá apenas modelos não standard.

$T + [P < NP]$ é uma teoria muito forte, conjecturamos. De alguma forma ela implicaria a consistência de uma outra teoria que prova $\text{Consis}(T')$, para T' qualquer teoria com as características de T descritas acima. Na verdade — e isso ainda nos é pouco claro — é como se houvesse uma regra infinitária de dedução em jogo. Ainda não compreendemos isso bem.

4 Relevância filosófica deste projeto

Lidamos neste projeto com conceitos que perpassam toda a epistemologia e filosofia da matemática durante o século XX: completude e incompletude de teorias formais, o conceito de computabilidade, decidibilidade e indecidibilidade, entre outros. Se concebermos a filosofia como uma atividade que busca fazer o exame crítico de conceitos necessários ao pensamento, a relevância filosófica do que nos propomos a fazer é incontestável.

Mais explicitamente:

- A prova de Andrew Wiles para o Teorema de Fermat parece envolver, de modo essencial, o uso do Axioma da Escolha — a questão ainda é controversa. Ou seja, para demonstrarmos uma afirmação relativamente simples a respeito de potências de números inteiros, far-se-ia necessário o uso de um princípio matemático altamente não construtivo e contra-intuitivo.

Dito de outro modo: uma sentença matemática de sentido facilmente compreendido pelo não-especialista exigiria, na sua prova, um princípio de grande, digamos, complexidade conceitual. O que isso nos diz sobre a natureza do conhecimento matemático?

- Outro exemplo: se N. da Costa e eu estivermos corretos, a sentença $[P < NP]$ somente poderá ser demonstrada na aritmética acrescida de um princípio infinitário, como p.e. a regra ω recursiva de Shoenfield. Novamente temos aqui uma sentença matemática de fácil compreensão, em cuja prova se faria uso essencial de um princípio não construtivo. E podemos reiterar aqui a mesma pergunta feita acima sobre a natureza do conhecimento matemático: por que princípios complexos são necessários na prova de uma afirmativa simples, quase ingênua?

A relevância filosófica é ponto pacífico — a não ser que, no Brasil, tenha-se desenvolvido uma visão muito pessoal e idiosincrática para o que seja filosofia.

5 Artigos publicados ou em vias de publicação, 2005

1. N. C. A. da Costa and F. A. Doria, “Consequences of an exotic formulation for $P = NP$,” *Applied Mathematics and Computation* **145**, 655–665 (2003); also “Addendum,” *Applied Mathematics and Computation* **172**, 1364–1367 (2006).
2. N. C. A. da Costa and F. A. Doria, “Computing the future,” in K. Vela Velupillai, ed., *Computability, Complexity and Constructivity in Economic Analysis*, Blackwell (2005).

3. N. C. A. da Costa and F. A. Doria, “Some thoughts on hypercomputation,” to appear (2006).¹
4. F. A. Doria, “Informal vs. formal mathematics,” to appear in *Synthèse* (2006).
5. F. A. Doria and J. F. Costa, “Introduction to the special issue on hypercomputation,” *Applied Mathematics and Computation*, to appear (2006).²

6 Referências citadas

1. R. A. DeMillo and R. J. Lipton, “Some connections between computational complexity theory and mathematical logic,” in *Proc. 12th Ann. ACM Symp. on the Theory of Computing*, 153–159 (1979).
2. R. A. DeMillo and R. J. Lipton, “The consistency of $P = NP$ and related problems with fragments of number theory,” in *Proc. 12th Ann. ACM Symp. on the Theory of Computing*, 45–57 (1980).
3. S. Fortune, D. Leivant, M. O’Donnell, “The expressiveness of simple and second-order type structures,” *J. ACM* **38**, 151–185 (1983).
4. T. Franzen, “Transfinite progressions: a second look at completeness,” *Bull. Symbolic Logic* **10**, 367–389 (2004).
5. J. Hartmanis and J. Hopcroft, “Independence results in computer science,” *SIGACT News*, 13, Oct. Dec. (1976).
6. D. Joseph and P. Young, “Independence results in computer science?” *Proc. 12th Ann. ACM Symp. on the Theory of Computing*, 58–69 (1980).
7. Joseph D. Joseph and P. Young, “Fast programs for initial segments and polynomial time computation in weak models of arithmetic,” *STOC Milwaukee 1981*, 55–61 (1981).
8. W. Kowalczyk, “A sufficient condition for the consistency of $P = NP$ with Peano Arithmetic,” *Fund. Inform.* **5**, 233–245 (1982).
9. K. Kunen, “A Ramsey theorem in Boyer–Moore logic,” *J. Automated Reasoning* **15**, 217 (1995).
10. A. Maté, “Nondeterministic polynomial-time computations and models of arithmetic,” *J. ACM* **37**, 175–193 (1990).
11. M. O’Donnell, “A programming language theorem which is independent of Peano Arithmetic,” *Proc. 11th Ann. ACM Symp. on the Theory of Computation*, 176–188 (1979).

¹Disponível desde outubro/2005 no site ScienceDirect.

²Disponível desde outubro/2005 no site ScienceDirect.