

# PCC104 - Projeto e Análise de Algoritmos

Marco Antonio M. Carvalho

Departamento de Computação  
Instituto de Ciências Exatas e Biológicas  
Universidade Federal de Ouro Preto



- 1 Discussão P vs. NP
  - P =? NP Poll

## Fonte

Este material é baseado nos livros

- ▶ T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*. The MIT Press, 3rd edition, 2009.
- ▶ S. Halim. *Competitive Programming*. 3rd Edition, 2013.
- ▶ Ian Parberry and William Gasarch. *Problems on Algorithms*. Second Edition, 2002.
- ▶ Ian Parberry *Lecture Notes on Algorithm Analysis and Complexity Theory*. Fourth Edition, 2001.

## Licença

Este material está licenciado sob a Creative Commons BY-NC-SA 4.0. Isto significa que o material pode ser compartilhado e adaptado, desde que seja atribuído o devido crédito, que o material não seja utilizado de forma comercial e que o material resultante seja distribuído de acordo com a mesma licença.

## Aviso!

Conteúdo baseado nos artigos:

- ▶ Fortnow, L. 2009. The Status of the P Versus NP Problem. Communications of the ACM, Vol. 52 No. 9, Pages 78-86.
- ▶ Gasarch, W. I. 2012. Guest Column: The Second  $P = ?$  NP Poll. ACM SIGACT news, 43(2), 53-77.
- ▶ Gasarch, W. I. 2019. Guest Column: The Third  $P = ?$  NP Poll. SIGACT News 50(1), 38-59.

## NP-Completo

A maioria dos problemas de interesse pertencem comprovadamente à classe NP-Completo:

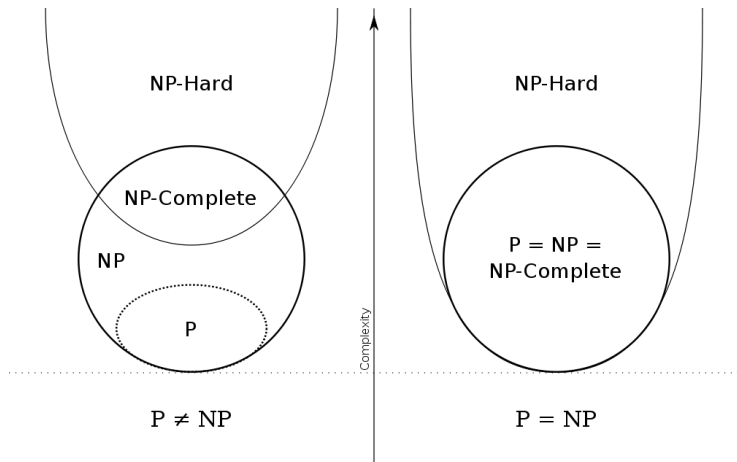
- ▶ Determinar a sequência de DNA que melhor se assemelha a um fragmento de DNA;
- ▶ Determinar procedimentos eficientes para predição de estrutura de proteínas;
- ▶ Determinar se uma afirmação matemática possui uma prova curta;
- ▶ Etc...

## P vs. NP

A partir das descobertas sobre os problemas da classe NP-Completo, grande parte dos cientistas da computação passou a acreditar que  $P \neq NP$ .

Provar isto se tornou a questão mais importante da ciência da computação e uma das mais importantes da matemática.

# Teoria da Complexidade Computacional



## P vs. NP – Um dos Problemas do Milênio

O *Clay Mathematics Institute* elencou 7 problemas matemáticos e oferece um prêmio de um milhão de dólares para quem resolver um deles.

Provar que  $P=NP$  ou  $P \neq NP$  é um dos 7 **Problemas do Milênio** desde o ano 2000:

- ▶ P vs. NP
- ▶ A conjectura de Poincaré (resolvido por Grigori Perelman em 2006);
- ▶ A conjectura de Hodge;
- ▶ A hipótese de Riemann;
- ▶ A existência de Yang-Mills e a falha na massa;
- ▶ A existência e suavidade de Navier-Stokes;
- ▶ A conjectura de Birch e Swinnerton-Dyer.



## A conjectura de Poincaré

“Todo o espaço tridimensional fechado, sem buracos, tem uma forma essencialmente esférica”.

- ▶ Conjectura elaborada em 1900 por Henri Poincaré;
- ▶ Refutada pelo próprio autor em 1904;
- ▶ Em 2003, anunciada a prova pelo russo Grigori Perelman, aos 47 anos;
- ▶ Tomasz Mrowka, do MIT, disse em 2006: “Estamos desesperadamente tentando entender o que ele fez”;
- ▶ Em 18 de março de 2010, o *Clay Mathematics Institute* anunciou que o Dr. Grigori Perelman era o vencedor de um dos sete Problemas do Milênio.

## A conjectura de Poincaré

*“Ninguém sabe onde está,” diz o matemático britânico Marcus du Sato sobre seu colega. “Me parece que não tem interesse nem em medalhas, nem em dinheiro”.*

*“I’m not interested in money or fame; I don’t want to be on display like an animal in a zoo.”*

## A hipótese de Riemann

Declara que os zeros não-triviais da função zeta de Riemann  $\zeta(s)$  pertencem todos à “linha crítica”:  $\sigma = \mathcal{R}[s]=1/2$ , em que  $\mathcal{R}[s]$  denota a parte real de  $s$ . Os zeros triviais da função zeta de Riemann são os inteiros negativos pares:  $\{-2,-4,-6,\dots\}$ .

- ▶ Publicada pela primeira vez em 1859 pelo matemático Bernhard Riemann;
- ▶ O professor nigeriano Dr. Opeyemi Enoch, que leciona na Universidade Federal de Oye-Ekiti, afirmou ter resolvido o problema em novembro de 2015. [Link](#).

## A hipótese de Riemann

*“Infelizmente, parece que neste caso não temos uma prova real da hipótese de Riemann... há um artigo no academia.edu sob o nome de Enoch, que na verdade é uma cópia de um artigo de outra pessoa chamada Werner Raab... Estranhamente, Enoch parece estar reunindo vários estudos sobre a Hipótese de Riemann no site academia.edu sob seu próprio nome.”*

## A hipótese de Riemann

Em 24 de setembro, o britânico Michael Atiyah, de 89 anos, afirmou que resolveu a hipótese de Riemann. [Link](#).

## E Se $P = NP$ ?

“O que ganharíamos com  $P=NP$  faria com que a Internet inteira parecesse apenas um rodapé na história”.

– Fortnow, L. 2009

## E Se $P = NP$ ?

Várias tarefas se tornariam triviais:

- ▶ Transporte de pessoas e produtos mais rápido e mais barato;
- ▶ Indústrias produzindo mais rápido e mais barato;
- ▶ Traduções automáticas;
- ▶ Reconhecimento de visão;
- ▶ Compreensão de linguagens;
- ▶ Previsão do tempo, terremotos e tsunamis;
- ▶ Provas curtas para teoremas matemáticos
  - ▶ 6 milhões de dólares ao invés de 1

## E Se $P = NP$ ?

Adeus criptografia!

A criptografia se baseia em problemas difíceis de serem resolvidos, como a fatoração de números muito grandes em números primos.

Portanto, é impossível de quebrar, a não ser que  $P=NP$  e fatoração seja um problema trivial...



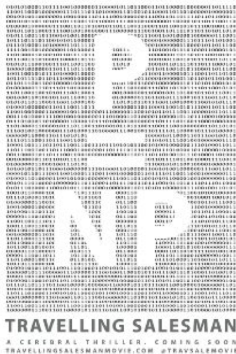
# Teoria da Complexidade Computacional

## O Filme

O filme “Travelling Salesman”, de 2012, conta a história de quatro matemáticos que descobrem um algoritmo eficiente para o Problema do Caixeiro Viajante, quando se deparam com as implicações globais da descoberta.

O departamento de defesa americano oferece US\$10 milhões para cada pelo algoritmo.

Um dos matemáticos se recusa, sendo forçado a revelar um segredo importante sobre sua parte do algoritmo.



## E Se $P \neq NP$ ?

Se for provado que  $P \neq NP$ , não teremos os benefícios computacionais de  $P = NP$ .

Porém, ainda assim teríamos avanços na teoria da computação e uma direção para pesquisas futuras.

Se soubermos que um problema é intratável, não tentaremos resolvê-lo de maneira eficiente, ao invés disso, tentaremos soluções aproximadas ou parciais, com técnicas **apropriadas**.

Podemos utilizar a dificuldade em resolver problemas a nosso favor – como na criptografia.

## E Se $P \neq NP$ ?

Como dito anteriormente, os problemas de interesse são NP-Completo. Ainda precisamos tentar resolvê-los, mesmo sem os benefícios de  $P=NP$ . Mesmo não sendo totalmente eficientes, existem “bons” algoritmos para problemas industriais, matemáticos, computacionais, etc. Aparecem aí a **Otimização Combinatória** e a **Pesquisa Operacional**.

## P vs. NP Atualmente

Existem 116 provas sobre P vs. NP, registradas pelo P vs. NP Page.

Em 2016 tivemos seis tentativas (igual:4, diferente:2).

De 26 de setembro de 2016 em diante, nenhuma atualização. [Link](#).



## Prof. Sóstenes Luiz Soares Lins (UFPE)

“Este trabalho permanece não publicado: continuo pesquisando que problemas de decisão são a ele redutíveis. No período 2008-2010, provei que MAX-CUT era um tal problema. Isto implicaria  $P=NP$ . Escrevi 52 versões da prova do resultado até descobrir, um erro (até aqui intransponível) em 10/01/2010.”

“Numa época de ciência descartável (focada em número de publicações e estatísticas estranhas, dissociadas do conteúdo), orgulho-me de não transigir e ao menos tentar descobrir algo perene e importante.”

## P vs. NP Atualmente

Um artigo de 2002 realizou uma pesquisa/entrevista com 100 dos maiores teóricos da computação do mundo – a intenção era obter um registro objetivo de opiniões subjetivas.

Dez anos depois, a pesquisa/entrevista foi refeita, desta vez, com 200 participantes em potencial – 152 responderam.

Nove anos depois, a terceira edição contou com 124 teóricos da computação, e uma pesquisa via SurveyMonkey.

2019

P = NP?

- ▶ Sim (12%);
- ▶ Não (88%).

*“NO. People that think  $P=NP$  are like people who think Elvis is still alive. [Maybe Elvis will prove  $P=NP$ .]”*

*– Lance Fortnow, Georgia Tech*

## Quando solucionaremos P vs. NP?

- ▶ Antes de 2100 (66%);
- ▶ Depois de 2100 (34%).

*"I'd hope in the next 50 years. I'd really like to see it in my lifetime since it's going to be such a breakthrough whatever the answer is. And it will impact other big questions in computational complexity."*

*– Benoit Razet, Bucknell University*



## Quando solucionaremos P vs. NP?

*"I am sticking with my answer on the original poll (2036), so that I can be wrong only once. Who knows, maybe I will be right."*

—Clyde Kruskal, University of Maryland

*"The  $P=?NP$  problem will never be resolved. I'm pessimistic that anyone will ever prove  $P!=NP$ , but I'm optimistic that we will someday prove that there is no proof that  $P!=NP$ ."*

—William Hoza, The University of Texas at Austin

## Qual será o método utilizado na prova?

- ▶ Novas técnicas (65 pessoas);
- ▶ Técnicas conhecidas (5 pessoas);
- ▶ Um algoritmo (6 pessoas);
- ▶ Milagre (1 pessoa);
- ▶ “Não saberemos até que seja resolvido”;
- ▶ “Não vou te dizer”;
- ▶ “Os aliens nos dirão”;
- ▶ “Livros já amarelados, incluindo aqueles que sequer foram escritos ainda”.

# P =? NP Poll

Se alguém provar  $P=NP$ , haverá um grande efeito na computação prática?

- ▶ Sim (58%);
- ▶ Não (42%).

*"While it is possible the solution will be ineffective, the consequences of a fully effective  $P=NP$  would be enormous. It can lead to human immortality in 5 years, or if held secret by a power-seeking group, world government in 2 years."*

*–Dmytro Taranovsky, MIT*

*"The practical impact would come not from the result itself, but from the new ideas needed to achieve it."*

*–Scott Aaronson, MIT*

Se alguém provar  $P \neq NP$ , haverá um grande efeito na computação prática?

- ▶ Sim (19%);
- ▶ Não (81%).

*"We already have put our faith in  $P \neq NP$ ."*

*–Hal Gabow, University of Colorado*

## Algum outro comentário?

*“Without proofs, the best we have are the opinions of experts, including differences of opinion.”*

*–Dmytro Taranovsky, MIT*

## Algun outro comentário?

*"I can't wait for people to realize that  $P=?NP$  is only a question about the existence of a poly- nomial time algorithm, not about the knowledge of one."*

*–Donald Knuth, Stanford*

*"I hope that all mathematicians enjoy the last decades in which mathematicians equipped with computer are significantly stronger in proving math theorems than computers alone. This will soon end. In 20 years, our role will be to press the button and either see the proof, or, if not, conclude that if a computer cannot prove the theorem then it is hopeless for humans to even start."*

*–Bogdan Grechuk, University of Leicester*

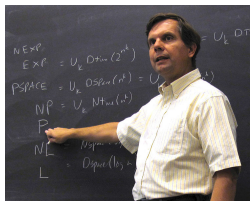
# P =? NP Poll



## Scott Aaronson, MIT

*"I believe  $P \neq NP$  on basically the same grounds that I think I won't be devoured tomorrow by a 500-foot-tall robotic marmoset from Venus, despite my lack of proof in both cases."*

# P =? NP Poll



## Eric Allender, Rutgers University

*" $P \neq NP$  will be resolved within 25 years, though this estimate is completely meaningless, of course.*

*Techniques: If I knew, then I wouldn't tell you."*



# $P = ?$ NP Poll



Stephen Cook, Universidade de Toronto

*" $P \neq NP$  will not be resolved in the next 20 years and will need new techniques".*



## Lance Fortnow, Georgia Tech

*" $P \neq NP$ . It will be resolved in an unpredictably long time. If I knew what kinds of techniques would be used I wouldn't tell."*



Richard Karp

*"I believe intuitively  $P \neq NP$  but it is only an intuition."*



## Michael Sipser, MIT

*"As far as I know, not much has changed mathematically relevant to  $P$  vs.  $NP$  since 2002 so I have nothing to add to my previous response to your questionnaire.*

*Use my prior response; however, update it so that I predict it will be solved 25 years from now, not from 2002.'*

*(...) And I'll stick with my earlier prediction that the resolution will be a proof that  $P \neq NP$ ."*

## Conclusão

*"(...) my first reaction was the article could be written in two words: Still open."*

– Fortnow, L. 2009

## Leitura Recomendada

Clay Mathematics Institute. The Millenium Problems. Disponível em:  
<http://www.claymath.org/millennium-problems>.

Fortnow, L. 2009. The Status of the P Versus NP Problem. Communications of the ACM, Vol. 52 No. 9, Pages 78-86.

Gasarch, W. I. 2002. The  $P=?$  NP Poll. Sigact News, 33(2), 34-47.

Gasarch, W. I. 2012. Guest Column: The Second  $P=?$  NP Poll. ACM SIGACT news, 43(2), 53-77.

Gasarch, W. I. 2019. Guest Column: The Third  $P=?$ NP Poll. SIGACT News 50(1), 38-59.

The P vs. NP Page. Disponível em:  
<http://www.win.tue.nl/~gwoegi/P-versus-NP.htm>. Acessado em 13 de novembro de 2018.

Turing, A. On computable numbers, with an application to the Etscheidungs problem. Proceedings of the London Mathematical Society 42 (1936), 230–265.

# Dúvidas?

