



Bruno Loff

Title: *The Hardness of Finding Good Algorithms*

Abstract:

One of the main tasks of a computer scientist is to find algorithms for solving various computational problems. We are interested in the question of whether this task, itself, can be automated. I.e., does there exist a "master algorithm" which, when given as input the specification of a computational problem, outputs a good algorithm for solving it?

There are many different specific instantiations of the above question, depending on what one means by "algorithm", "computational problem", and what one means by "good" algorithm.

This question belongs to the field of Computational Complexity. The main unsolved riddle in this field is: how does one prove impossibility results? How does one prove that a given computational problem is difficult to solve? Our question, it turns out, is deeply connected with the problem of proving such impossibility results, and several variants of this same question are equivalent to fundamental open questions in cryptography, pseudorandomness, and learning theory.

In this presentation, we will briefly overview the history of this question, and outline its manifold connections with various other important problems in Computer Science. The presentation will be in English, and is intended for a general scientific audience.

Título: *A dureza de encontrar bons algoritmos*

Resumo:

Uma das principais tarefas de um cientista da computação é inventar novos algoritmos para resolver problemas computacionais. Coloca-se a questão de saber se esta tarefa pode ela mesma ser automatizada. Ou seja, existirá um "algoritmo mestre" que, ao receber como input a especificação de um problema computacional, produz como output um bom algoritmo para resolvê-lo?

Existem muitas formas diferentes de instanciar esta pergunta, dependendo do tipo de "algoritmo" que nos interessa, do tipo de "problema computacional" e de qual é o nosso critério que faz um algoritmo ser "bom".

Esta pergunta pertence a uma área do conhecimento chamada "Complexidade Computacional", que estuda a dificuldade inerente em resolver problemas computacionais. O maior problema em aberto nesta área é: como podemos demonstrar que um dado problema computacional não pode ser resolvido eficientemente? Acontece que a pergunta acima, aparentemente inocente, tem ligações profundas com o problema de provar tais resultados, e várias variantes da questão acima são equivalentes a questões abertas fundamentais em criptografia, pseudo-aleatoriedade e teoria da aprendizagem.

Nesta apresentação, faremos uma breve visão geral da história dessa pergunta e delinearemos suas múltiplas conexões com vários outros problemas importantes na Ciência da Computação. A apresentação será em inglês, e destina-se a um público de cientistas de várias áreas.

Academia das Ciências de Lisboa, 2 de março de 2023