

Matemática, “Inteligência” e Consciência da Computação

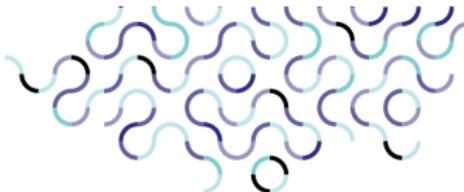
Mauricio Ayala-Rincón

Maria Eduarda Carvalho Santos (Bolsista IC),
Mehwish Arshid (Doutoranda)

Grupo de Teoria da Computação (GTC-UnB)
Departamentos de Matemática e Ciência da Computação



SEMANA
UNIVERSITÁRIA
UnB 27 set - 1º out
100 anos de Paulo Freire



28 de Setembro de 2021



- Atuação em Matemática e de Ciência da Computação



- Atuação em Matemática e de Ciência da Computação



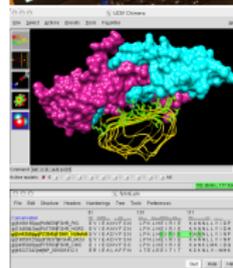
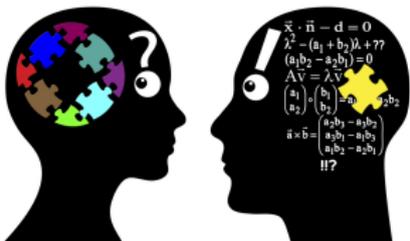
Alguns egressos e cooperações

- Luiz Gadelha Jr. - LNCC Petrópolis
- Ivan Eid Tavares Araújo - Yale University
- Daniele Nantes Sobrinho, Flávio L. C. de Moura, Andréia B. Avelar
- UnB
- Thaynara A. de Lima, Daniel L. Ventura, André L. Galdino - UFG
- Carlos Morra Scalglioti - Siemens Munique
- Washington L. R. de Carvalho - IBICT, etc.

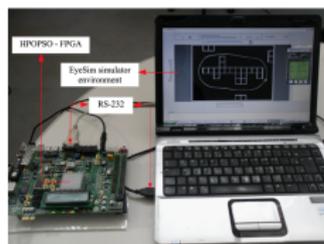
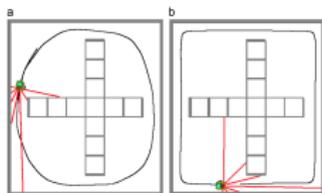
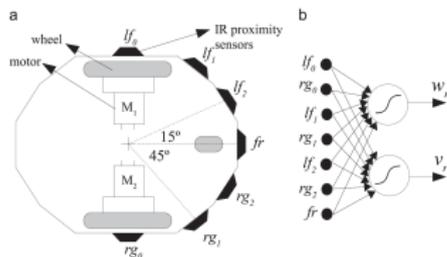
Cooperações

- NASA LaRC Formal Methods
- Heriot-Watt University
- Karlsruher Institute fuer Technologie
- King's College London
- University of Groningen

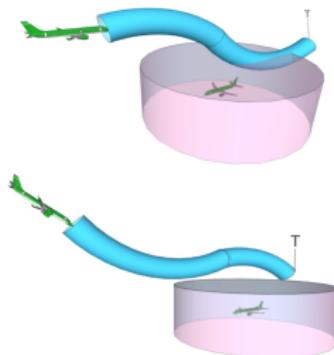
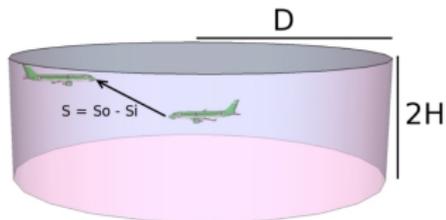
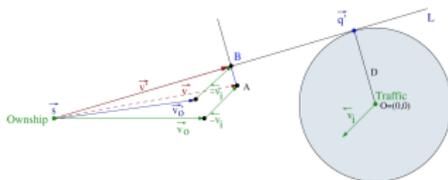
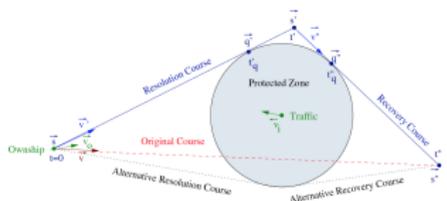
- Lógica e Semântica de Programas de Computadores (Cooperação Internacional)



- Simulações em robôs (Cooperação Engenharia Mecatrônica)



- Resolução de Conflitos em Tráfego Aéreo (cooperação NASA)



Matemática, “Inteligência” e Consciência da Computação

Capacidade de escolher as técnicas formais mais eficientes e eficazes para explorar convenientemente as restrições das ferramentas disponíveis.

Problemas simples que têm aplicações em Matemática Aplicada à Computação:

- ▶ Cálculos com restrições
- ▶ Verificação de Terminação de Programas

Cálculos com restrições - Aritmética Romana

Adicionar MCXLIV e CDXXIV

	+	-
M	1	
D		
C	1	
L	1	
X		1
V	1	
I		1

+

	+	-
M		
D	1	
C		1
L		
X	2	
V	1	
I		1

=

	+	-
M	1	
D	1	
C		
L	1	
X	1	
V	2	
I		2

MDLXVIII



Cálculos com restrições - Aritmética Romana

Sem “roubar” calcular em aritmética romana

$$\text{MDCXLIV} + \text{MCDXXIX}$$

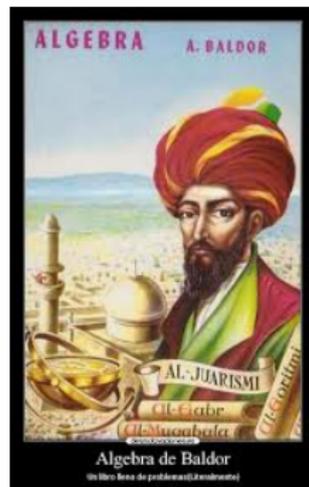
	+	-
M		
D		
C		
L		
X		
V		
I		

+

	+	-
M		
D		
C		
L		
X		
V		
I		

=

	+	-
M		
D		
C		
L		
X		
V		
I		



Cálculos com restrições - Aritmética Romana

MDCXLIV + MCDXXIX

	+	-
M	1	
D	1	
C	1	
L	1	
X		1
V	1	
I		1

+

	+	-
M	1	
D	1	
C		1
L		
X	3	
V		
I		1

=

	+	-
M	2	
D	2	
C		
L	1	
X	2	
V	1	
I		2

MMMLXXIII

Cálculos com restrições - Somadoras e subtração

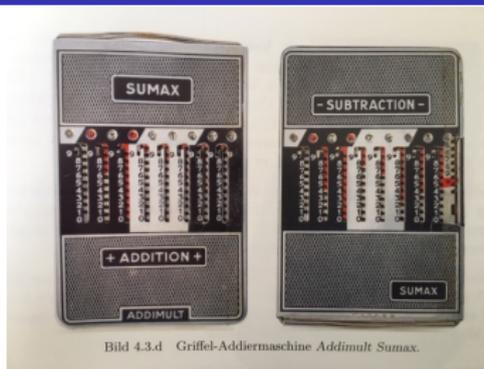


Bild 4.3.d Griffel-Addiermaschine Addimult Sumax.



Cálculos com restrições - Somadoras e subtração



Cálculos com restrições - Somadoras e subtração



“Acumular” 1423 e “descontar” 528

$$1423 - 528$$

$$1423 + 471 = 1894 \rightsquigarrow 895$$

471 é o complemento em algarismos de 528

Cálculos com restrições - Somadoras e subtração

Subtração: 1752 - 1334

$$1752 - 1334$$

$$1752 + 9665 = 11417 \rightsquigarrow 418$$



Verificação da terminação

A função de Fibonacci com qualquer entrada para!

$$\begin{cases} f(0) = f(1) = 1 \\ f(n) = f(n-1) + f(n-2), \text{ se } n > 1 \end{cases}$$

Mas terminação não é sempre uma questão fácil de responder.

Função 91 de McCarthy:
$$\begin{cases} M(n) = n - 10, & \text{se } n > 100 \\ M(n) = M(M(n + 11)), & \text{se } n \leq 100 \end{cases}$$

PERGUNTA: M termina?

Verificação da terminação

Variações da função 91 de McCarthy - $n \in \mathbb{Z}$

$$\begin{cases} M(n) = n - 10, & \text{se } n > 100 \\ M(n) = M(M(n + 11)), & \text{se } n \leq 100 \end{cases}$$

$$\begin{cases} M_1(n) = n - 10, & \text{se } n > 100 \\ M_1(n) = M_1(M_1(n + 10)), & \text{se } n \leq 100 \end{cases}$$

$$\begin{cases} M_2(n) = n - 3, & \text{se } n > 100 \\ M_2(n) = M_2(M_2(M_2(n + 7))), & \text{se } n \leq 100 \end{cases}$$

Chamadas para M , $n \leq 100$:

$$k + [((101 - (n + k * 11)) * 2 + 1)] + k * 21, \text{ where } k = \lfloor \frac{(100-n)}{11} \rfloor.$$

Generalização de D. Knuth

Para $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $a \in \mathbb{R}$, and $b, c \in \mathbb{R}^+$

$$\begin{cases} K(n) = n - b, & \text{se } n > a \\ K(n) = K^m(n + c), & \text{se } n \leq a \end{cases}$$

Exemplo: $M = K$, quando $a = 100$, $b = 10$, $c = 11$ e $m = 2$.

Verificação da terminação

Teorema de Knuth - $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $a \in \mathbb{R}$, e $b, c \in \mathbb{R}^+$

Para parâmetros (a, b, c, m) , K define uma **função total** sobre \mathbb{Z} se e somente se $(m - 1)b < c$.

Exemplos:

- ▶ Para M , K tem parâmetros $(100, 10, 11, 2)$, e $(2 - 1)10 < 11$;
- ▶ Para M_1 , K tem parâmetros $(100, 10, 10, 2)$, mas $(2 - 1)10 = 10$;
- ▶ Para M_2 , K tem parâmetros $(100, 3, 7, 3)$, e $(3 - 1)3 < 7$.

Verificação da terminação

Teorema de Knuth - $n \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, $a \in \mathbb{R}$, e $b, c \in \mathbb{R}^+$

Para parâmetros (a, b, c, m) , K dado por

$$\begin{cases} K(n) = n - b, & \text{se } n > a \\ K(n) = K^m(n + c), & \text{se } n \leq a \end{cases}$$

define uma **função total** sobre \mathbb{Z} se e somente se $(m - 1)b < c$.

Nesse caso:

$$\begin{cases} K(n) = n - b, & \text{se } n > a \\ K(n) = K(n + c - (m - 1)b), & \text{se } n \leq a \end{cases}$$

Verificação da terminação

Em geral, a questão de se um programa termina é fundamental para responder se sistemas computacionais são ou não corretos.

Novamente a questão é indecidível, mas fundamental em matemática e computação.

Problemas simples que têm aplicações em Matemática Aplicada à Computação:

- ▶ Cálculos com restrições:

FPGA based floating-point library for CORDIC algorithms

DM Muñoz, DF Sanchez, CH Llanos, M Ayala-Rincón, SPL 2010.

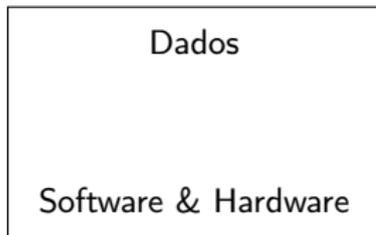
- ▶ Verificação de Terminação de Programas:

Formal Verification of Termination Criteria for First-Order Recursive Functions

CA Muñoz, M Ayala-Rincón, MM Moscato, AM Dutle, AJ Narkawicz, AA Almeida, AB Avelar, TMF Ramos, ITP 2021.

Aplicação essencial:

- ▶ Detecção de erros, **produção verificada** de *software* e *hardware* competitivo.
- ▶ **Certificação matemática** de objetos computacionais.
- ▶ **Valorização** da industria e aplicações de IT.



Matemática, “Inteligência” e Consciência da Computação

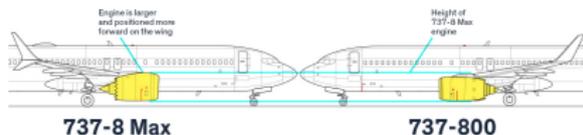
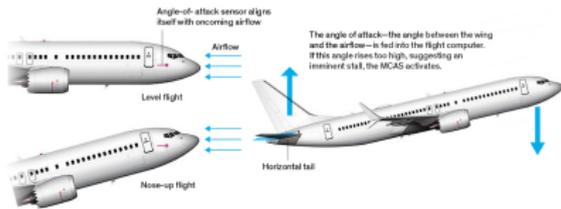
Capacidade de implementar eficiente e eficazmente o raciocínio lógico formal humano para explorar convenientemente as restrições das ferramentas disponíveis.

“Boeing’s out-of-control autopilot

O primeiro avião 737 Max Boeing novinho em folha, Lion Air Flight 510, caiu logo após a decolagem. Depois outro fez o mesmo. Todos a bordo morreram. Em cada caso, os pilotos tinham lutado contra um sistema de piloto automático que tomou o controle e mergulhou os aviões em sua desgraça.

Os pilotos tiveram pouco tempo para reagir a um controle de vôo, chamado MCAS, do qual pouco ou nada sabiam.”

How the new Max flight-control system (MCAS) operates to prevent a stall



A. Regalado, *The biggest technology failures of 2019*, MIT Tech. Review, Oct. 2019

“Viés de gênero no cartão de crédito da Apple

Por que um empresário rico em tecnologia obteria um limite de crédito 10 vezes maior que o de sua esposa no novo Cartão Apple, mesmo que seus bens sejam mantidos em comum? Quando alguém reclamou, um representante lhe disse: 'é apenas o algoritmo'. Um algoritmo sexista! Steve Wozniak, cofundador da Apple, disse que isso também aconteceu com sua esposa. Mas o que é o programa, e o que ele faz? A Apple e Goldman Sachs, o banco que apoia o cartão, não disseram. E esse é o problema. Existe um **viés computadorizado**, mas é difícil responsabilizar alguém, ou qualquer coisa.



A. Regalado, *The biggest technology failures of 2019*, MIT Tech. Review, Oct. 2019

“Missed Breast Cancer Screenings Due to ‘Algorithm Failure’

Quase meio milhão de mulheres idosas no Reino Unido perderam os exames de mamografia por causa de um erro de programação causado por um **algoritmo de computador incorreto**, e várias centenas dessas mulheres podem ter morrido precocemente como resultado.

O algoritmo errante estava no software de programação de exames de câncer de mama do Sistema Nacional de Saúde (NHS), e permaneceu sem ser descoberto por nove anos.

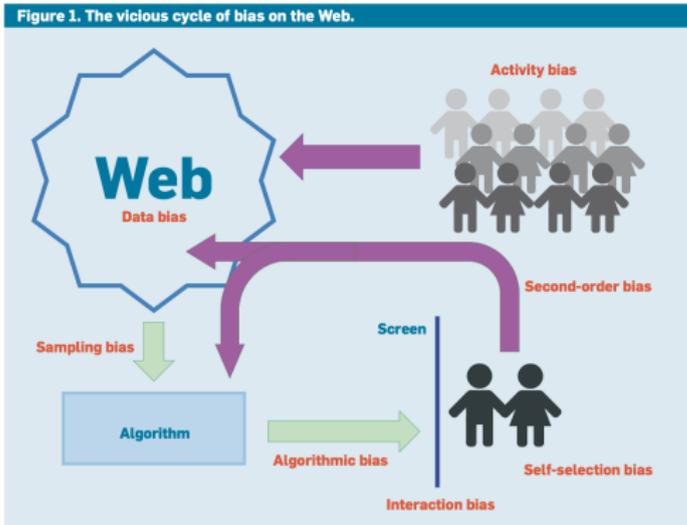


R. N. Charette, *450,000 Women Missed Breast Cancer Screenings Due to “Algorithm Failure”*, IEEE Spectrum, May 2018.

Matemática, “Inteligência” e **Consciência** da Computação

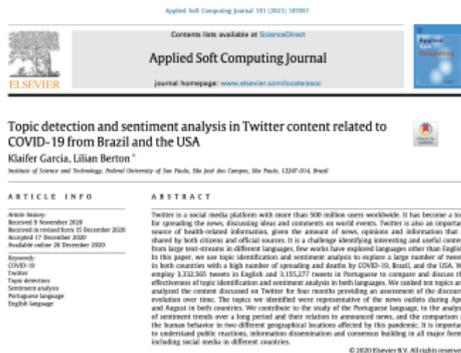
Capacidade de compreender e aceitar o mundo e a própria mente de forma tolerante e sensível, com valores morais e retidão.

R. Baeza-Yates, *Bias on the Web* Comm. of the ACM 61(8), 2018



Discussão inicial com
Maria Eduarda e Mehwish:

- ▶ Viés de dados
- ▶ Viés de algoritmos



Discussão inicial com Maria Eduarda e Mehwish:

- ▶ Usuários de Twitter é restrito
- ▶ Análise sobre mostra elitista
- ▶ Resultados *honestos*, mas uso como recomendação para tomada de decisões ineficazes.
- ▶ Necessidade de inclusão de especialistas.



ARTICLE

<https://doi.org/10.1038/s41567-020-01723-8> OPEN

The association between early career informal mentorship in academic collaborations and junior author performance

Bedoor AShebi^{1,2*}, Kings Makoi³ & Talal Rahwan³

We study mentorship in scientific collaborations, where a junior scientist is encouraged by potentially multiple senior collaborators, without them necessarily having formal supervisory roles. We identify 3 million mentor-protégé pairs and survey a random sample, verifying that their relationship involved some form of mentorship. We find that mentorship predicts the scientific impact of the papers written by protégés just as effectively without their mentors. We also find that increasing the proportion of female mentors is associated not only with a reduction in post-mentorship impact of female protégés, but also a reduction in the gain of female mentees. While current diversity policies encourage some gender mentorships to retain women in academia, our findings suggest the possibility that opposite gender mentorship may actually increase the impact of women who pursue a scientific career. These findings add a new perspective to the policy debate on how to best elevate the status of women in science.

Discussão inicial com Maria Eduarda e Mehwish:

- ▶ Dados precisos, mas
- ▶ Análise preconceituosa e
- ▶ imprecisa.
- ▶ Necessidade de inclusão de especialistas.

Grandes Institutos Modelo em IA - DFKI

“O *Deutsches Forschungszentrum für Künstliche Intelligenz* - DFKI), fundado em 1988, com 650 pesquisadores e 440 estudantes graduados de 65 países, está comprometido com a **promoção de IA segura e confiável**. As estratégias gerais do DFKI para seu programa de pesquisa e atividades aderem aos princípios e valores éticos baseados nos direitos humanos fundamentais. Como parte importante dessas estratégias, o DFKI encoraja a **avaliação objetiva** dos sistemas de IA visando a atestação de conformidade com os princípios e valores éticos. O programa de avaliação de IA do DFKI está concentrado em seu novo Laboratório de Certificação e Soberania Digital (CertLab). CertLab esforça-se para estabelecer um centro de excelência para a **certificação de sistemas de IA** alinhado com padrões técnicos e sociais de diferentes contextos e estruturas. A avaliação da **segurança, privacidade e autonomia** abre caminho para sistemas de IA confiáveis e seguros e promove a **soberania digital de todas as pessoas** afetadas pelo uso dos sistemas de



Grandes Institutos Modelo em IA - **CLAIRE**

A *Confederation of Laboratories for Artificial Intelligence Research in Europe* **CLAIRE**, fundada em 2018, com 385 instituições e labs de 36 países, busca **fortalecer a excelência europeia em pesquisa e inovação AI**. "Acreditamos que a IA mudará fundamentalmente a nossa maneira de viver e trabalhar. Também é provável que se torne crucial para enfrentar os grandes desafios da sociedade, tais como clima, energia e mobilidade; alimentos e recursos naturais; saúde; e sociedades inclusivas e seguras. Além disso, a IA é uma 'mudança de jogo' global que se tornou um importante motor de inovação, crescimento futuro e competitividade. Se a Europa ficasse para trás na tecnologia da IA, provavelmente enfrentaríamos consequências econômicas desafiadoras, fuga de cérebros, menor transparência e crescente dependência de tecnologias, produtos e valores estrangeiros. **CLAIRE** apresenta uma proposta para evitar isso."



DFKI News 01-2020

EU-Kommission: 50 Millionen Startförderung fürs KI-Bündnis Claire

Die EU-Kommission unterstützt Forschungsprojekte rund um Künstliche Intelligenz, mit denen die Technik auch das menschliche Denken verbessern helfen soll.

Lesezeit: 1 Min.  In Pocket speichern

   2



1. **Enriquecimento com avaliação humana** - Avaliação do impacto de previsões incorretas e, quando razoável, projeção de sistemas com processos de revisão "human-in-the-loop".

2. **Avaliação do viés de data e computacional** - Elaboração de processos que permitam compreender, documentar e monitorar preconceitos.

Ao construir sistemas que têm que tomar decisões não triviais, sempre enfrentaremos o viés computacional e social que é inerente aos dados, o que é impossível de evitar, mas é possível documentar e/ou mitigar.

3. **Explicabilidade e transparência** - Desenvolvimento de ferramentas e processos para melhorar continuamente a transparência e a explicabilidade dos modelos de aprendizagem de máquinas onde for razoável. Mesmo que em certas situações a precisão possa diminuir, os ganhos em transparência e explicabilidade podem ser significativos.

4. **Operações reproduzíveis** - Desenvolvimento da infra-estrutura necessária para permitir um nível razoável de reprodutibilidade. Nos sistemas de produção, é importante realizar procedimentos padrão, como reverter um modelo para uma versão anterior, ou reproduzir um input para depurar uma funcionalidade específica, o que introduz complexidade na infra-estrutura.

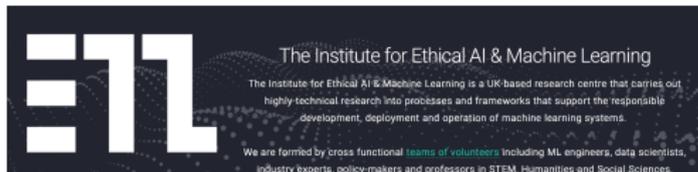
5. **Estratégia de deslocamento** - Identificação e documentação de informações para que os processos de mudança comercial possam ser desenvolvidos para mitigar o impacto para os trabalhadores que estão sendo automatizados.

6. **Precisão** - Desenvolvimento de processos para garantir precisão e funções métricas de custo alinhadas às aplicações específicas do domínio.

7. **Confiança e privacidade** - Construção e comunicação de processos que protejam e tratem os dados com as partes interessadas que possam interagir com o sistema direta e/ou indiretamente.

8. **Conscientização do risco dos dados** - Desenvolvimento e melhoria de processos e infra-estrutura razoáveis para garantir que os dados e modelos de segurança estejam sendo levados em consideração.

Sistemas autônomos de tomada de decisão abrem as portas para novas brechas potenciais de segurança.



A Matemática e Computação nos acompanham por toda a vida!





- Notícias
- Seminários
- Concursos
- Eventos
- Links e Formulários
- Mídia MAT
- Galeria
- Comissões

Teoria da Computação

A pesquisa está focada no desenvolvimento de estruturas matemáticas e formais para dedução e computação. Especificamente, arcabouços lógicos como os sistemas de reescrita, o cálculo Lambda, as substituições explícitas, e os sistemas nominais são estudados e suas aplicações em computação e dedução investigadas.

Colaboradores do grupo incluem coautores brasileiros e estrangeiros: César Muñoz, Maribel Fernández, Fairouz Kamareddine, Flávio L.C. de Moura, Daniel Ventura, entre outros.

Linhas de Pesquisa

- Teoria da reescrita
- Teoria de tipos
- Lógica formal e computacional
- Teoria de prova
- Dedução formal e equacional

Atividades

[Página do seminário de Teoria da Computação](#) | [Eventos](#) | [Publicações](#)

Quem Somos



[Daniele Nantes Sobrinho](#)

Aplicações de Estruturas Formais em Dedução Equacional e Modelos Computacionais.

Orientadora de mestrado



[Maurício Ayala Rincón](#)

Aplicações das Teorias de Reescrita, Tipos e Prova em Formalização e Dedução.

Orientador de mestrado e doutorado

Bem-vindos ao Instituto de Ciências Exatas!

<https://www.mat.unb.br/~ayala>



Maurício Ayala Rincón, Dr. rer. nat.

Professor Titular

[Teoria da Computação](#)

Departamentos de [Ciência da Computação](#) e [Matemática](#)
Universidade de Brasília

Endereço:

Departamento de Matemática, [Universidade de Brasília](#)

Campus Universitário Darcy Ribeiro, Asa Norte

70910-900 Brasília D. F., Brasil

Tels. +55-61-3307 2441|2442| +55- 61-3107 6453 | 3676 Fax +55-61-3273 2737

e-mail: ayala@unb.br

-
- [Publicações](#) ● [Cursos <=> Início 17 Agosto - atividades remotas 2020-1](#)
 - [PVS Class 2017](#) (associado a ITP 2017) ● [PVS Tutorial for Mathematicians](#) (associado a SW in Math 2020)
 - [Atividades profissionais](#) ● [CV Lattes](#)
 - [Grupo de Teoria da Computação](#)
-

Tópicos de pesquisa:

Propriedades e aplicações dos sistemas de reescrita de termos e suas extensões. [Links relacionados](#)

- [TRS PVS teoria de reescrita](#) ● [Alg. evolut. para ordenação de permutações](#)
-

[English](#) [Español](#)

Oportunidades

- [Bolsas de doutorado Edital de Seleção](#) com inscrição até 18 de Agosto -[estendido para 1ro de Setembro, 2020](#). Interessados no tema 2: *Algorítmica e Teoria de Sequenciamento de Informação Genômica*, entrar em contato.
- RTA (1983 ... 2015) and TLCA (1993 ... 2015) evolved to Int. Conf. on Formal Structures for Computation and Deduction [FSCD](#) (2016 ... 2019, 2020), [FSCD 2021 em Buenos Aires](#) (a 12/2/2021, p 15/2/2021) [cfp](#).
- 30th Int. Symp. on Logic-based Program Synthesis and Transformation [LOPSTR 2020](#), Bologna, 7-9 Setembro, 2020.
- 15th Int. Logical and Semantic Frameworks, with Applications [LSFA 2020](#), 26-28 Agosto, 2020.
- [Conferencias em curso no GTC/UnB](#)



M. Ayala-Rincón & Flávio L.C. de Moura, *Fundamentos da Programação Lógica e Funcional - O Princípio de Resolução e a Teoria de Reescrita* -, Course Notes, Ed. UnB, December 2014. Em Português.



M. Ayala-Rincón & Flávio L.C. de Moura, *Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs*, Springer, 2017.

ayala@unb.br