Matemática da Computação

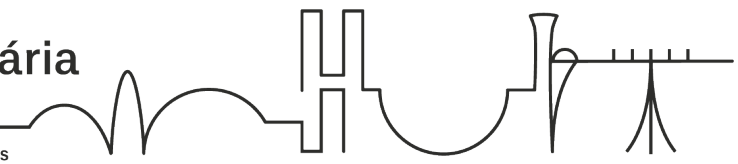
Mauricio Ayala-Rincón, Daniele Nantes, Flávio L. C. de Moura

Departamentos de Matemática e Ciência da Computação

21 a 25 de setembro de 2020 | Inscrições gratuitas

29ª Semana Universitária UnB

vinte anos de conexões



22 de Setembro de 2020

Grupo de Teoria da Computação - GTC/UnB

- Atuação em Matemática e de Ciência da Computação

Grupo de Teoria da Computação - GTC/UnB

- Atuação em Matemática e de Ciência da Computação

Alguns egressos e cooperações

-Luiz Gadelha Jr. - LNCC Petrôpolis

-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

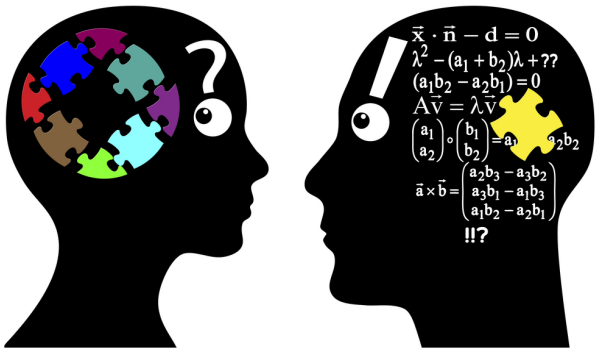
-Washington L. R. de Carvalho - IBICT, etc.

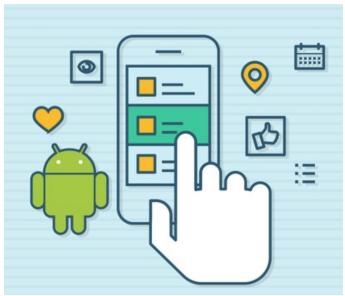
Cooperações

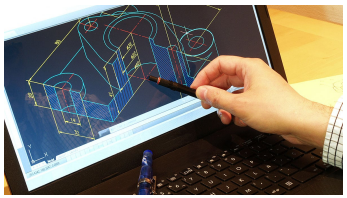
- NASA LaRC Formal Methods
- Heriot-Watt University
- Karlruher Institute fuer Technologie
- King's College London
- University of Groningen

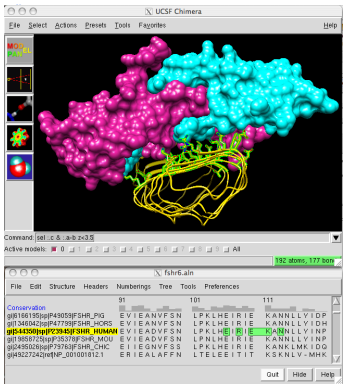
Projetos do GTC/UnB

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



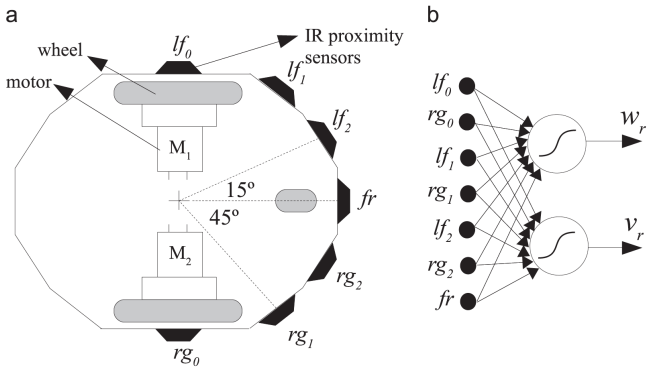


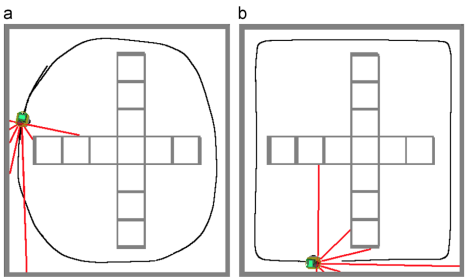


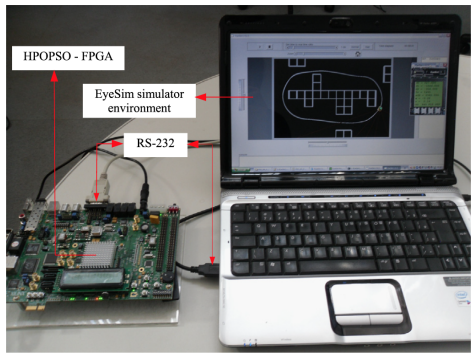


Projetos GTC/UnB

- Simulações em robôs (Cooperação Engenharia Mecatrônica)

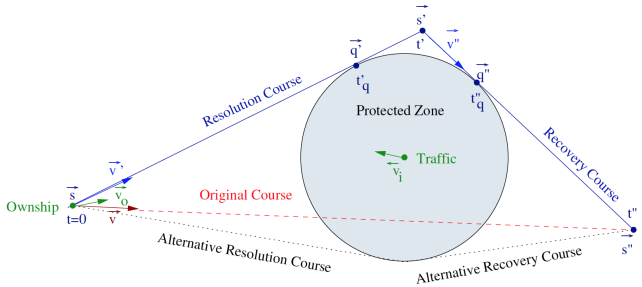


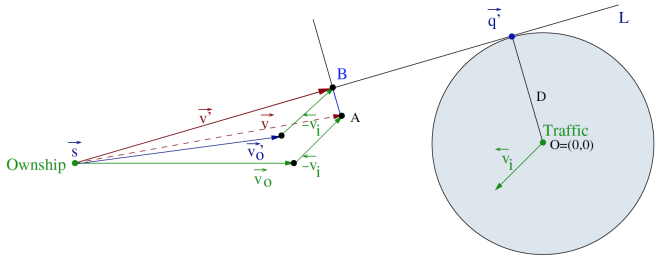


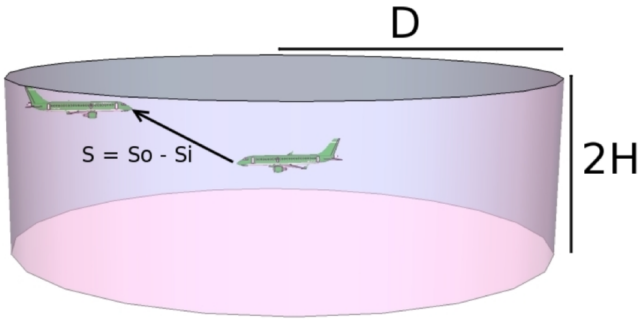


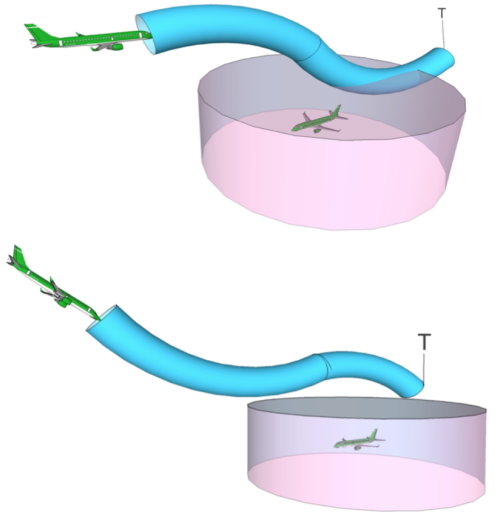
Projetos GTC/UnB

- Resolução de Conflitos em Tráfego Aéreo (cooperação NASA)









Problemas simples que têm aplicações em Matemática Aplicada à Computação:

- Cálculos com restrições
- Problema da Correspondência de Post
- Funções Recursivas e a Sequência de Fibonacci
- Verificação de Terminação de Programas
- Problemas do Milênio: $P =^{?} NP$

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

MDCXLIV + MCDXXIX

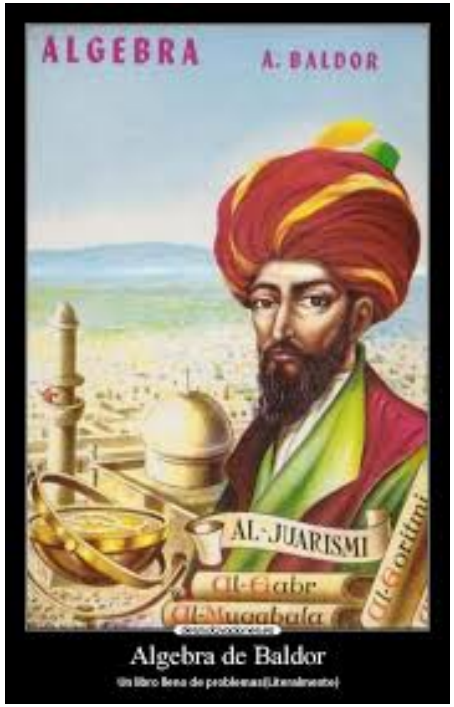
	+	−
M		
D		
C		
L		
X		
V		
I		

+

	+	−
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

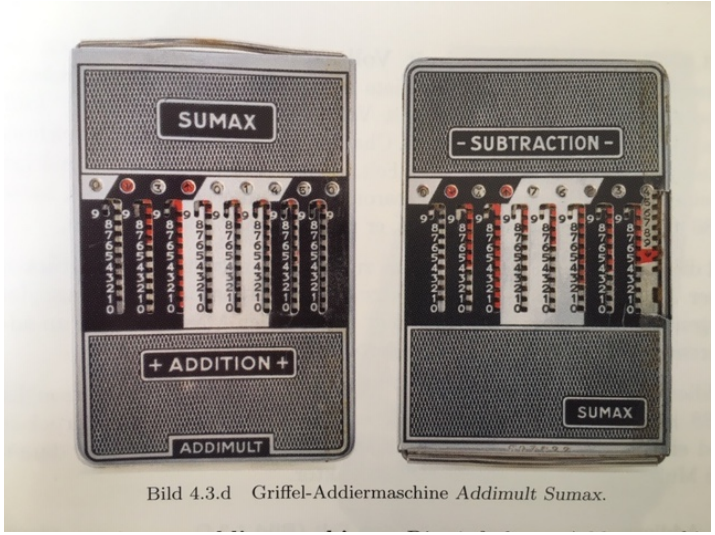
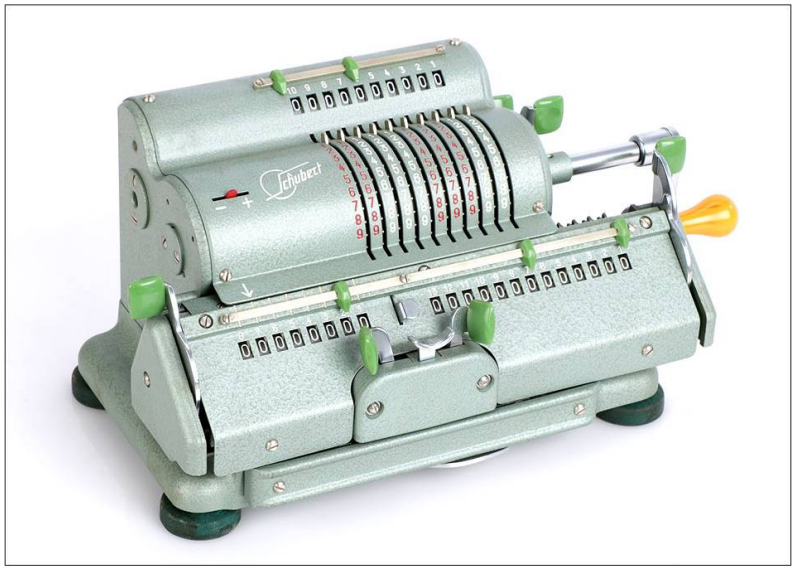


Bild 4.3.d Griffel-Addiermaschine *Addimult Sumax*.

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

Sua vez!

Substração: 1752 - 1334

$$1752 \quad - \quad 1334$$

$$1752 \quad + \quad ???? \quad = \quad ????? \rightsquigarrow ???$$

Cálculos com restrições - Somadoras e subtração

Substração: 1752 - 1334

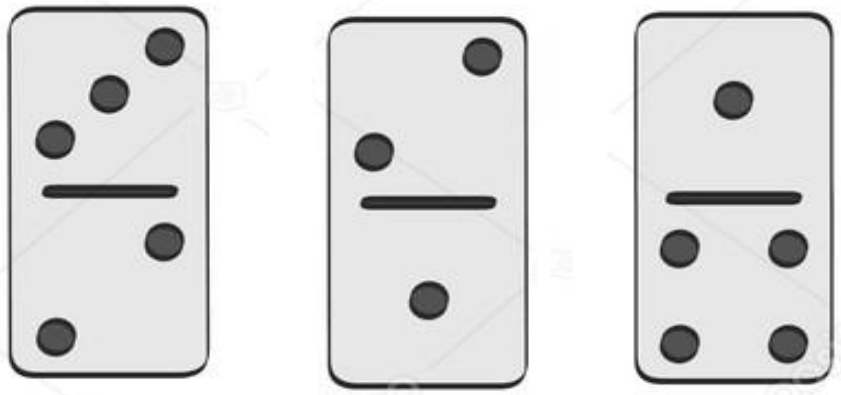
$$1752 \quad - \quad 1334$$

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

Problema de Correspondência de Post - PCP

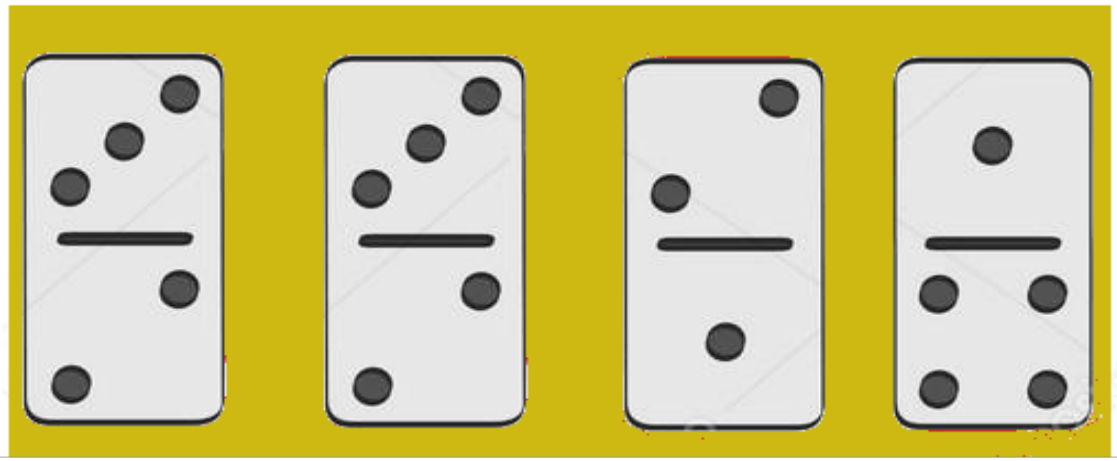
Pergunta:

Existe alguma combinação dos dominós abaixo de maneira que a quantidade de •'s da parte de cima seja igual à quantidade de •'s da parte de baixo?

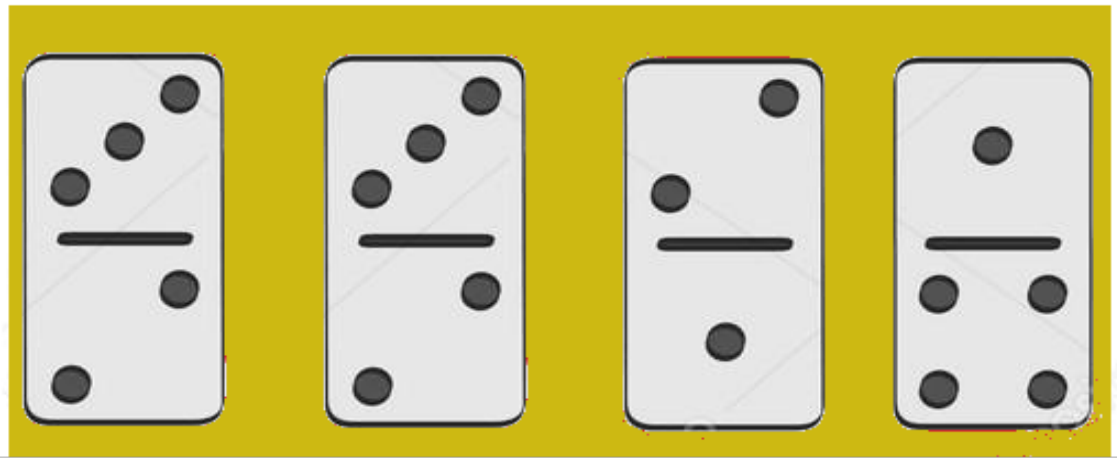


Problema de Correspondência de Post - PCP

Solução:



Problema de Correspondência de Post - PCP

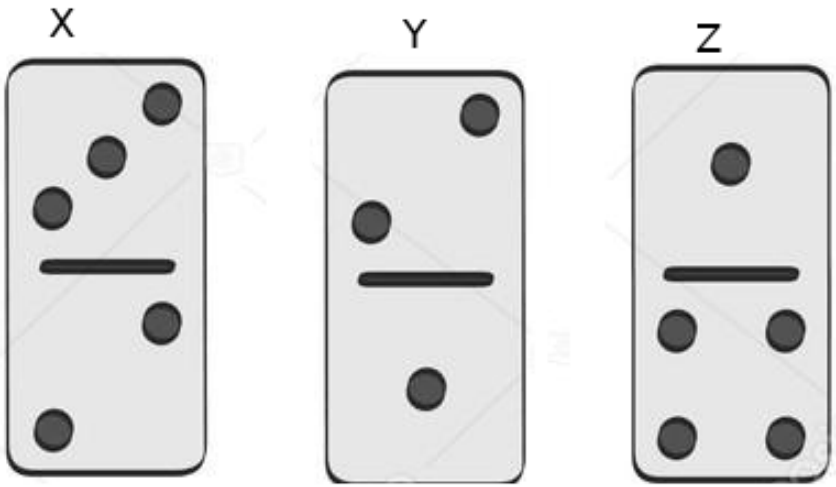


Solução:

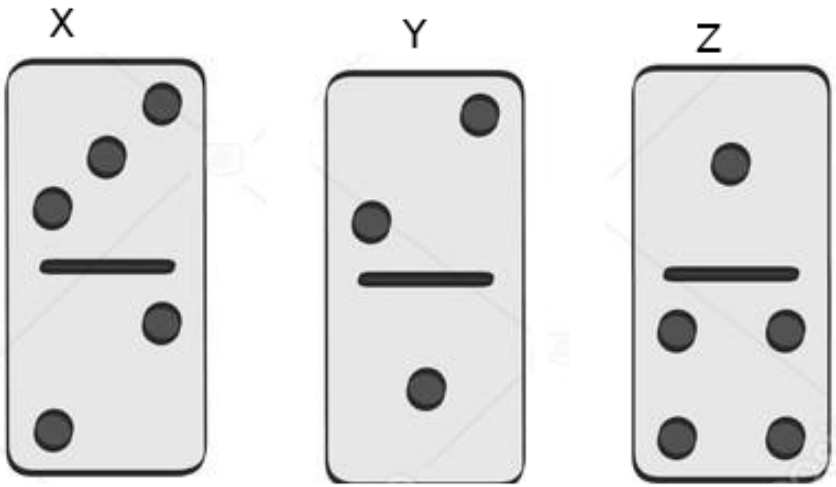
Existem outras soluções?

Problema de Correspondência de Post - PCP

Onde está a matemática no Problema da Correspondência de Post?

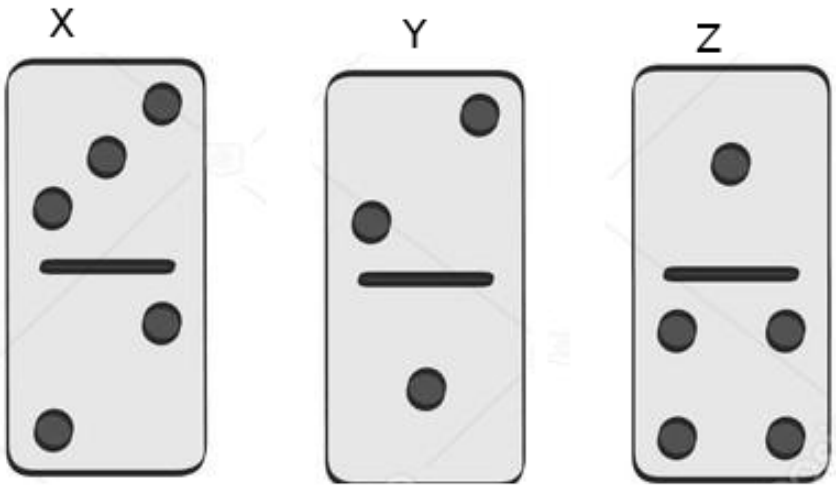


$$3x + 2y + 1z = 2x + 1y + 4z$$



$$3x + 2y + 1z = 2x + 1y + 4z$$

$$(3x - 2x) + (2y - y) + (z - 4z) = 0$$



$$3x + 2y + 1z = 2x + 1y + 4z$$

$$(3x - 2x) + (2y - y) + (z - 4z) = 0$$

$$x + y - 3z = 0$$

$$\left\{ \begin{array}{l} x = 2 \\ y = 1 \\ z = 1 \end{array} \right\}$$ é uma solução.

Problema de Correspondência de Post - PCP

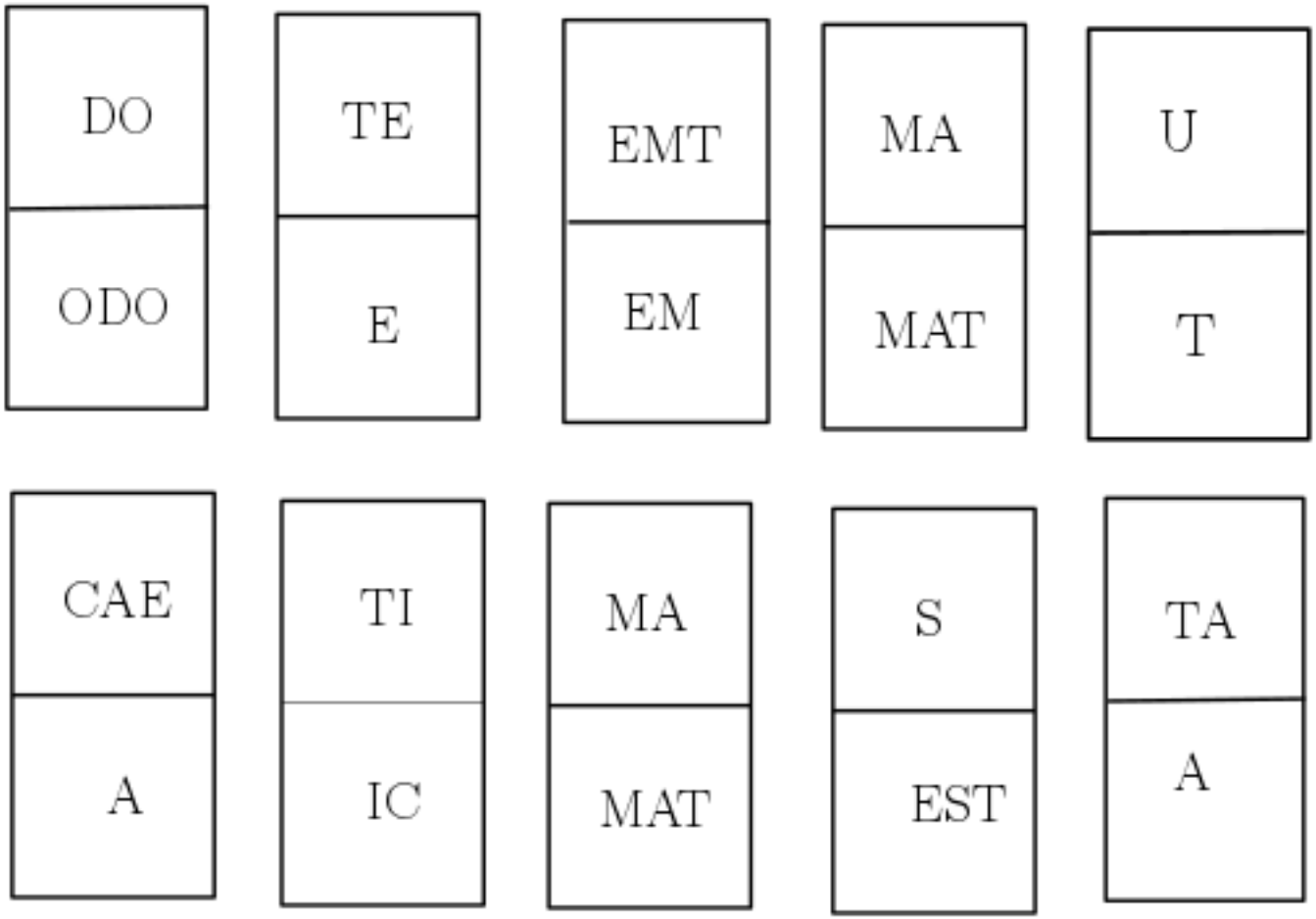
O alfabeto do dominó clássico é apenas: $\Sigma = \{\bullet\}$.

O que aconteçe se o alfabeto é maior? Por exemplo:

$\Sigma = \{a, b, c, d, \ldots, z, A, B, C, D, \ldots, Z\}$.

Problema de Correspondência de Post - PCP

Você consegue resolver o PCP para estes dominós?



Este problema pode não ter solução : o Problema da Correspondência de Post é indecidível!

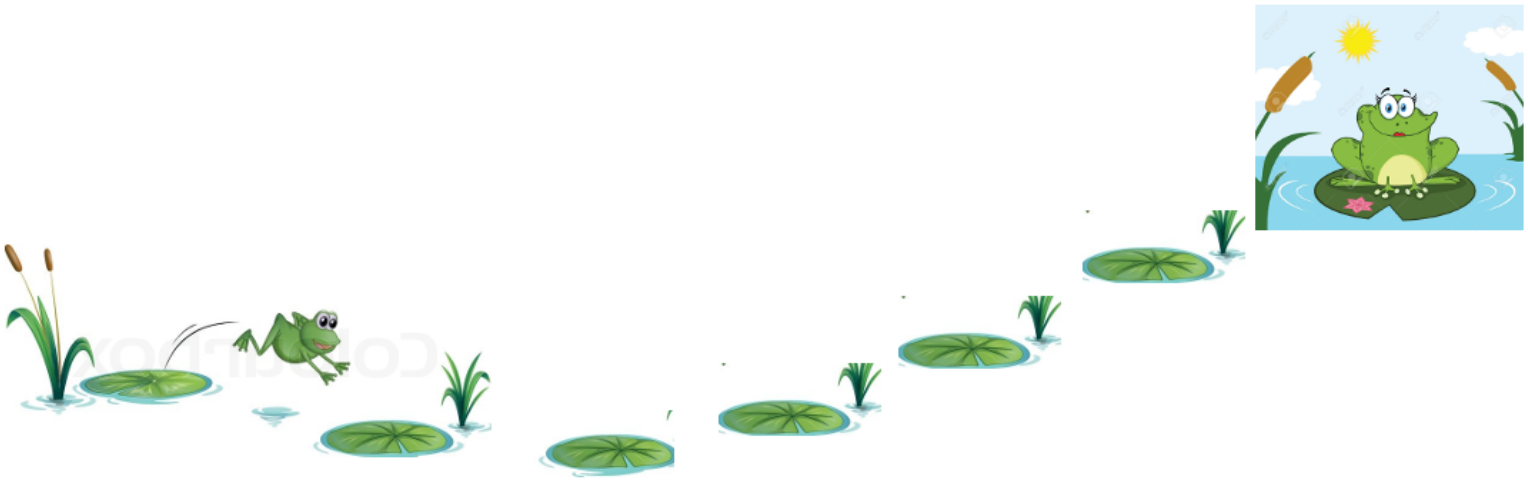
- Indecidibilidade do problema de terminação para Máquinas de Turing!

Um outro problema interessante

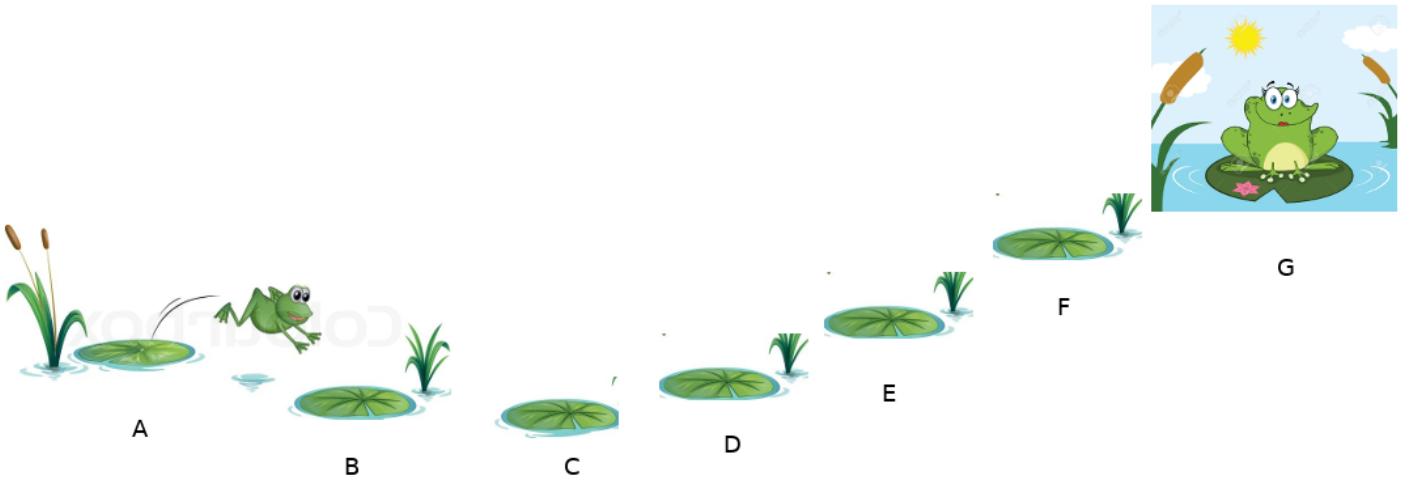
O sapo da esquerda quer chegar ao outro lado, e precisa respeitar as seguintes regras:

- Só pode andar para direita.
- Só pode pular 1 ou 2 folhas de cada vez.

PERGUNTA: De quantas maneiras diferentes o sapo da esquerda pode chegar ao seu destino?



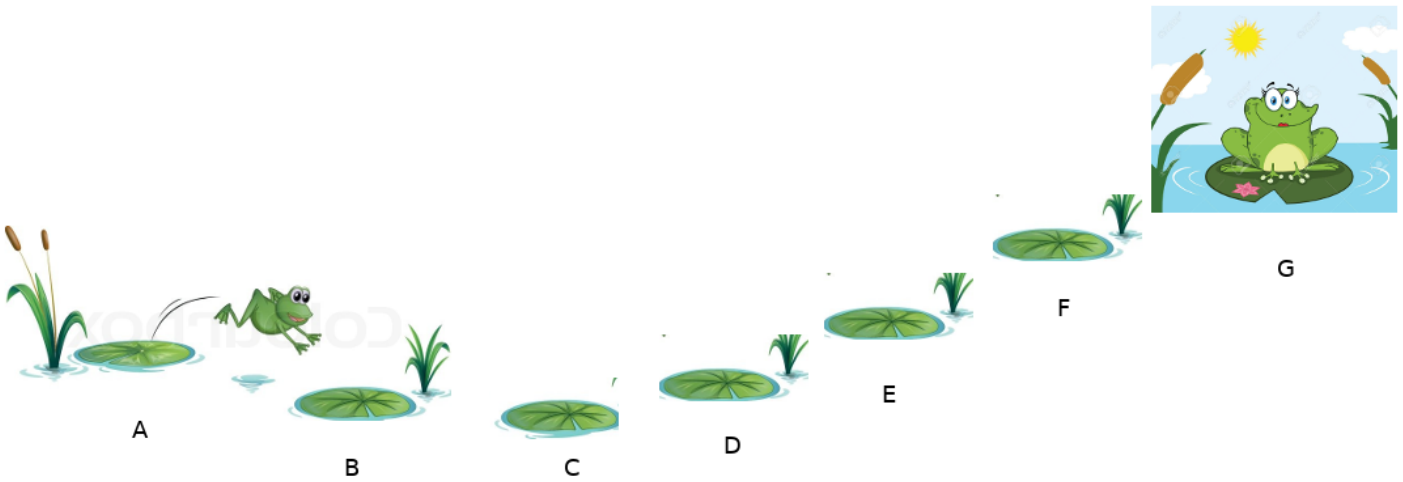
Solução



- A,B,C,D,E,F,G
- B,C,D,E,F,G
- B,D,F,G
- C,E,G
- ...

Folha	nºde possibilidades
A	1
B	1
C	2
D	3
⋮	

Solução



$\text{caminhos}(A) = \text{caminhos}(B) = 1$

$\text{caminhos}(G) = \text{caminhos}(F) + \text{caminhos}(E)$

Em geral:

$\text{caminhos(folha 0)} = \text{caminhos(folha 1)} = 1,$ e

$\text{caminhos(folha } n) = \text{caminhos(folha } n-1) + \text{caminhos(folha } n-2)$

Sequência de Fibonacci e funções recursivas: linguagem de programação funcional.

$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots,$

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

Outro problema em computação: terminação

A função de Fibonacci com qualquer entrada para!

$f(0) = f(1) = 1$

$f(n) = f(n-1) + f(n-2),$ se $n > 1$

Mas terminação não é sempre uma questão fácil de responder.

Função 91 de McCarthy:

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

Verificação da terminação

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

Exemplos:

$$M(101) = 91$$

$$M(100) = M(M(111)) = M(101) = 91$$

$$\begin{aligned} M(0) &= M(M(11)) = M(M(M(22))) = M^4(33) = \cdots \\ &= M^{11}(110) = M^{10}(100) = \cdots = M^9(91) = \cdots ? \end{aligned}$$

$$M(91) = M^2(102) = M(92) = M^2(103) = \cdots = M(100) = \cdots = 91$$

PERGUNTA: M termina?

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.

Desafios Lógicos - Problema 1

Considere uma ilha que possui dois tipos de habitantes: os honestos, que sempre falam a verdade; e os desonestos, que sempre mentem. Considere dois habitantes A e B da ilha. Determine o que são A e B, supondo que A diz **"Eu sou desonesto ou B é honesto"**.

Desafios Lógicos - Problema 1

Considere uma ilha que possui dois tipos de habitantes: os honestos, que sempre falam a verdade; e os desonestos, que sempre mentem. Considere dois habitantes A e B da ilha. Determine o que são A e B, supondo que A diz **"Eu sou desonesto ou B é honesto"**.

Sejam p e q duas proposições com a seguinte semântica:

- p: A é honesto.
- q: B é honesto.

Desafios Lógicos - Problema 1

Sejam p e q duas proposições com a seguinte semântica:

- p: A é honesto.
- q: B é honesto.

O desafio pode ser codificado pela fórmula: $p \leftrightarrow ((\neg p) \vee q)$

Desafios Lógicos - Problema 1

Sejam p e q duas proposições com a seguinte semântica:

- p: A é honesto.
- q: B é honesto.

O desafio pode ser codificado pela fórmula: $p \leftrightarrow ((\neg p) \vee q)$

p	q	$(\neg p) \vee q$
V	V	V
V	F	F
F	V	V
F	F	V

Como a única maneira de satisfazer a fórmula $p \leftrightarrow ((\neg p) \vee q)$ é fazendo com que tanto p quanto q sejam verdadeiros, concluímos que A e B são honestos!

Desafios Lógicos - Problema 2

Você está andando por um labirinto quando se depara com três possíveis caminhos: um de ouro, um de mármore e outro de pedras. Cada caminho é protegido por um guardião mentiroso.

1. **Guardião do caminho de ouro**: Este caminho o levará diretamente para o centro. Mais ainda, se o caminho de pedras te levar ao centro, então o caminho de mármore também te levará ao centro;
2. **Guardião do caminho de mármore**: Nem o caminho de ouro, nem o caminho de pedras te levará ao centro;
3. **Guardião do caminho de pedras**: Siga o caminho de ouro e você chegará ao centro, siga o caminho de mármore e você se perderá.

Qual caminho leva **com certeza** ao centro?

Desafios Lógicos - Problema 2

Sejam G, M e S proposições com a seguinte semântica:

- G: o caminho de ouro leva ao centro;
- M: o caminho de mármore leva ao centro;
- S: o caminho de pedra leva ao centro.

Desafios Lógicos - Problema 2

Sejam G, M e S proposições com a seguinte semântica:

- G: o caminho de ouro leva ao centro;
- M: o caminho de mármore leva ao centro;
- S: o caminho de pedra leva ao centro.

1. $\neg(G \wedge (S \rightarrow M))$
2. $\neg(\neg G \wedge \neg S)$
3. $\neg(G \wedge (\neg M))$

Desafios Lógicos - Problema 2

1. $\neg(G \wedge (S \rightarrow M)) \equiv \neg G \vee (S \wedge \neg M)$
2. $\neg(\neg G \wedge \neg S) \equiv G \vee S$
3. $\neg(G \wedge (\neg M)) \equiv \neg G \vee M$

G	M	S	$\neg G \vee (S \wedge \neg M)$	$G \vee S$	$\neg G \vee M$	$1 \wedge 2 \wedge 3$
V	V	V	F	V	V	F
V	V	F	F	V	V	F
V	F	V	V	V	F	F
V	F	F	F	V	F	F
F	V	V	V	V	V	V
F	V	F	V	F	V	F
F	**F**	**V**	**V**	**V**	**V**	**V**
F	F	F	V	F	V	F

Problemas do milênio: $P =^{?} NP$

- Estes desafios lógicos estão relacionados a uma classe de problemas para os quais não se conhecem soluções eficientes, como por exemplo, o problema SAT.
- Encontrar uma solução eficiente para algum problema desta classe, ou mostrar que estas não existem, consiste em resolver o importante problema $P =^{?} NP$.
- O CMI (*The Clay Mathematics Institute*) oferece 1 milhão de dólares para quem resolver o problema $P =^{?} NP$!

A Matemática e Computação nos acompanham por toda a vida!

Bem-vindos ao Instituto de Ciências Exatas!

https://www.mat.unb.br/pg/45/Teoria-da-Computacao

Universidade de Brasília
Instituto de Ciências Exatas

Departamento de Matemática

Português

Buscar

Home Institucional Graduação Pós Graduação Pesquisa Extensão Pessoas Contato

- 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 includem 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 Rincon
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

Mauricio 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 Brasilia D. F., Brasil
Tels. +55-61-3307 2441|2442| +55- 61-3107 6453 | 3676 Fax +55-61-3273 2737
e-mail: *ayala[at]unb.br*

Publicações · Cursos <<<== Inicio 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

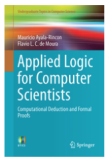
---

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 Portugês.



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

---

ayala[at]unb.br