

Matemática Discreta

Introdução

Antonio Alfredo Ferreira Loureiro

`loureiro@dcc.ufmg.br`

`http://www.dcc.ufmg.br/~loureiro`

DISCRETE Math *is*

Real $f(u)^n$

Introdução

- Por que estudar Matemática Discreta?
 - Provê um conjunto de técnicas para modelar problemas em Ciência da Computação.

Tópico de Matemática Discreta	Aplicação em Ciência da Computação
Lógica e Conjuntos	Sistemas Especialistas (IA)
Relações e funções	Bancos de dados relacionais, Algoritmos distribuídos
Análise combinatória	Análise de algoritmos (pior caso)
Grafos não-dirigidos	Linguagens e “parsing”
Grafos dirigidos	Algoritmos de roteamento em redes
Álgebra booleana	Projeto de circuitos digitais
Teoria de grupo	Teoria da informação
Autômato de estados finito	Modelo computacional para resolução de problemas em geral
Probabilidade	Análise de algoritmos (caso médio)

Definição dos termos discreto e contínuo

DISCRETO: feito de partes distintas.

CONTÍNUO: sem interrupção e sem mudança brusca.

Exemplos familiares de “matemática contínua”: cálculo e equações diferenciais.

- Muitos dos tópicos estudados e técnicas usadas em Ciência da Computação tanto de matemática discreta quanto de matemática contínua são os mesmos.
- Exemplos:
 - Em matemática (contínua e discreta) estamos interessados em conjuntos de objetos e suas estruturas.
 - Relações e funções.

Matemática discreta e contínua

- Matemática contínua: trata de conjuntos similares ao conjunto de números reais.
 - Conjuntos têm representações contínuas (do ponto de vista geométrico).
 - Conjuntos não podem ser enumerados.
Exemplo: intervalo de uma reta, região do plano.
- Matemática discreta: trata de objetos separados e desconectados (geometricamente) de cada um.
 - Conjuntos são, em geral, finitos e podem ser enumerados.

Os termos discreto e contínuo em Ciência da Computação

- Os computadores podem ser classificados em digitais e analógicos, do ponto de vista do dado processado.
- Dados obtidos através de algum processo de “contagem” (*counting*) são discretos.
 - Computadores que processam este tipo de dado são chamados de digitais.
- Dados obtidos através de algum processo de “medida” (*measuring*) são contínuos.
 - Computadores que processam este tipo de dado são chamados de analógicos.
- Exemplo de relógio: *Digital*



Analógico



Motivação para estudar Matemática Discreta do ponto de vista prático

- A influência e desenvolvimento de computadores digitais têm aumentado bastante nos últimos anos.
- Na verdade, deveríamos falar de elementos computacionais ao invés de “computador digital”.
- Um elemento computacional é basicamente um sistema discreto finito.
- Muitas de suas propriedades podem ser estudadas e ilustradas através de princípios da Matemática discreta, onde estudamos princípios e técnicas para projetar sistemas de computação (hardware e software).

Matemática Discreta vs. Ciência da Computação ou Entendendo a importância de Matemática Discreta para Ciência da Computação (1)

A seguir, são apresentados os tópicos que estudaremos nesta disciplina bem como exemplos de sua utilização em Ciência da Computação:

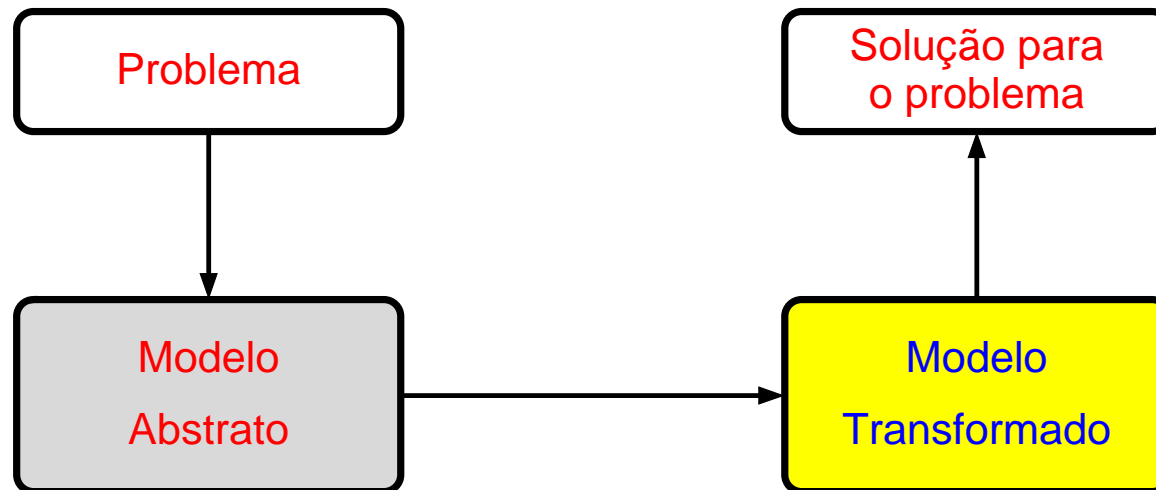
- Fundamentos da Lógica; Lógica Proposicional; Lógica de Proposições Quantificadas; e Cálculo de Predicados.
 - Banco de dados;
 - Circuitos integrados;
 - Inteligência artificial;
 - Sistemas computacionais (hardware e software);
 - Sistemas distribuídos.
- Métodos de Prova:
 - Circuitos integrados;
 - Projeto de algoritmos.
- Sequências e Indução Matemática:
 - Projeto de algoritmos.
- Teoria dos Conjuntos:
 - Banco de dados;
 - Circuitos integrados;
 - Inteligência artificial;
 - Sistemas distribuídos.

Matemática Discreta vs. Ciência da Computação ou Entendendo a importância de Matemática Discreta para Ciência da Computação (2)

- Funções:
 - Otimização;
 - Projeto de algoritmos.
- Recursão:
 - Projeto de algoritmos.
- Análise Combinatória:
 - Circuitos integrados;
 - Otimização;
 - Projeto de algoritmos;
 - Sistemas distribuídos.
- Relações:
 - Sistemas distribuídos.
- Grafos:
 - Banco de dados;
 - Circuitos integrados;
 - Compiladores e linguagens de programação;
 - Engenharia de software;
 - Inteligência artificial;
 - Otimização;
 - Projeto de algoritmos;
 - Redes de computadores;
 - Robótica;
 - Sistemas computacionais (hardware e software);
 - Sistemas distribuídos;
 - Sistemas operacionais.

Modelagem Matemática

- Metodologia: conjunto de conceitos que traz coesão a princípios e técnicas mostrando quando, como e porque usá-los em situações diferentes.
- A metodologia que usa matemática na resolução de problemas é conhecida como modelagem matemática.
- O processo de modelagem:



Exemplo de modelagem: Malha rodoviária (1)

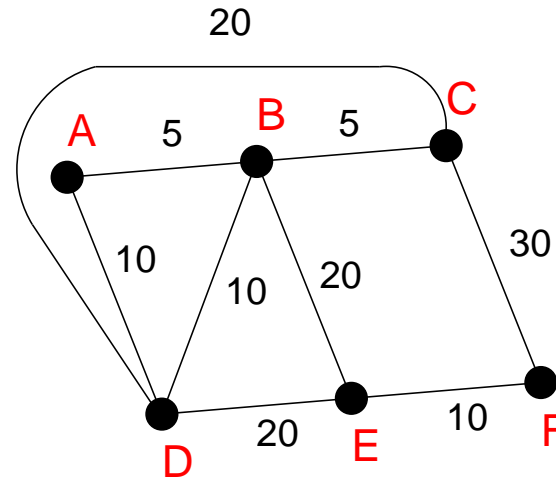
Suponha a malha rodoviária entre as seis cidades A, B, C, D, E, e F.

Problema: Achar um subconjunto da malha rodoviária representada pela tabela abaixo que ligue todas as cidades e tenha um comprimento total mínimo.

	B	C	D	E	F
A	5	–	10	–	–
B		5	10	20	–
C			20	–	30
D				20	–
E					10

Exemplo de modelagem: Malha rodoviária (2)

- Tabela já é um modelo da situação do mundo real.
- A tabela pode ser transformada numa representação gráfica chamada GRAFO, que será o modelo matemático.



Grafo G

- Grafo (definição informal): conjunto de “pontos” chamados de vértices ou nós, e um conjunto de linhas (normalmente não-vazio) conectando um vértice ao outro.
 - Neste caso, cidades são representadas por vértices e estradas por linhas (arestas).

Exemplo de modelagem: Malha rodoviária (3)

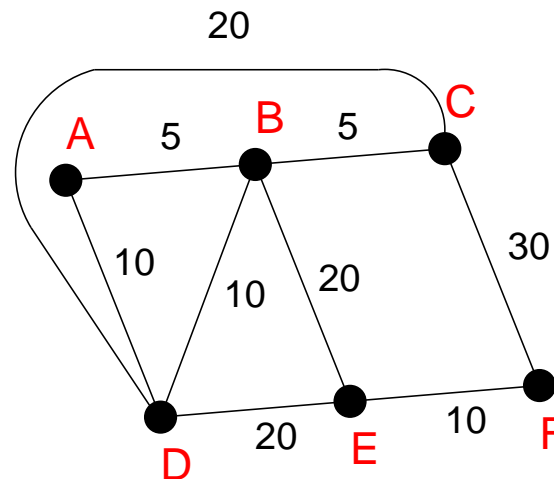
- Qual é o próximo passo?
 - Achar uma solução em termos desse modelo.
 - Nesse caso, achar um grafo G' com o mesmo número de vértices e um conjunto mínimo de arestas que conecte todas as cidades e satisfaça a condição do problema.
- Observação: o modelo matemático é escolhido, em geral, visando a solução.
- A solução será apresentada na forma de um algoritmo.

Exemplo de modelagem: Malha rodoviária (4)

Algoritmo:

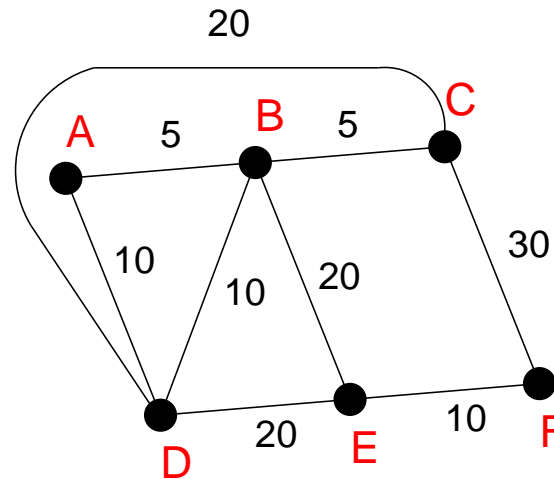
1. Selecione arbitrariamente qualquer vértice e o coloque no conjunto de vértices já conectados.
2. Escolha dentre os vértices não conectados aquele mais próximo de um vértice já conectado. Se existir mais de um vértice com essa característica escolha aleatoriamente qualquer um deles.
3. Repita o passo 2 até que todos os vértices já estejam conectados.

→ Este é um exemplo de um “algoritmo guloso” (*greedy algorithm*).



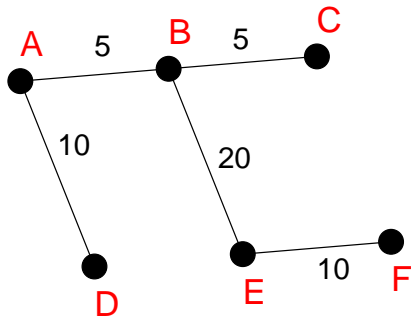
Grafo G

Exemplo de modelagem: Malha rodoviária – Soluções (5)

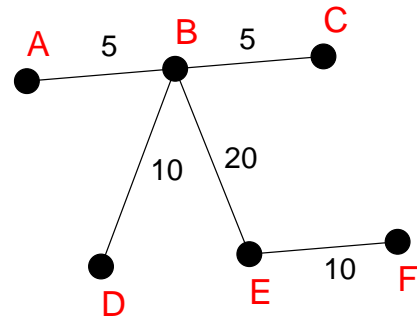


Grafo G

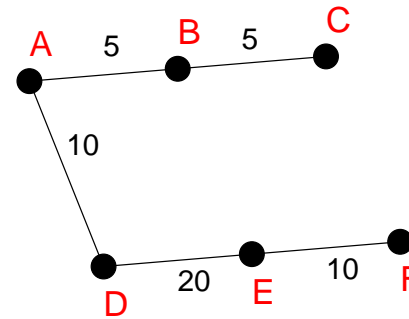
Soluções:



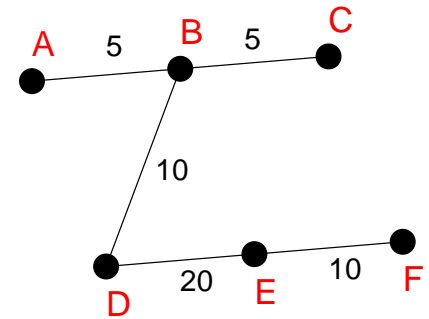
Grafo G_1



Grafo G_2



Grafo G_3



Grafo G_4

Exemplo de modelagem: Malha rodoviária (6)

- O que foi feito?
 1. Obtenção do modelo matemático para o problema.
 2. Formulação de um algoritmo em termos do modelo.

→ Ou seja, essa é a técnica de resolução de problemas em Ciência da Computação.
- Nem todos os problemas considerados terão como solução um algoritmo, mas muitos terão.

Exemplo de modelagem: Sudoku e Godoku (1)

		1	8			3		
	4	9	7	1	6		8	
	2			9				
		4					2	
	5	6			1	8		
	1					5		9
						4	3	
			1	6				8
7					2			1

Sudoku

A								
				C				
	B				F	I		D
		A					B	
E				G				
		F				H		
				D	E			
I				B				
							A	

Godoku

O objetivo do Sudoku (Godoku) é preencher todos os espaços em branco do quadrado maior, que está dividido em nove grids, com os números de 1 a 9 (letras). Os algarismos não podem se repetir na mesma coluna, linha ou grid.

Sudoku: A palavra Sudoku significa “número sozinho” em japonês, o que mostra exatamente o objetivo

do jogo. O Sudoku existe desde a década de 1970, mas começou a ganhar popularidade no final de 2004 quando começou a ser publicado diariamente na sessão de *puzzles* do jornal *The Times*. Entre abril e maio de 2005 o *puzzle* começou a ganhar um espaço na publicação de outros jornais britânicos e, poucos meses depois, ganhou popularidade mundial. Fonte: wikipedia.org

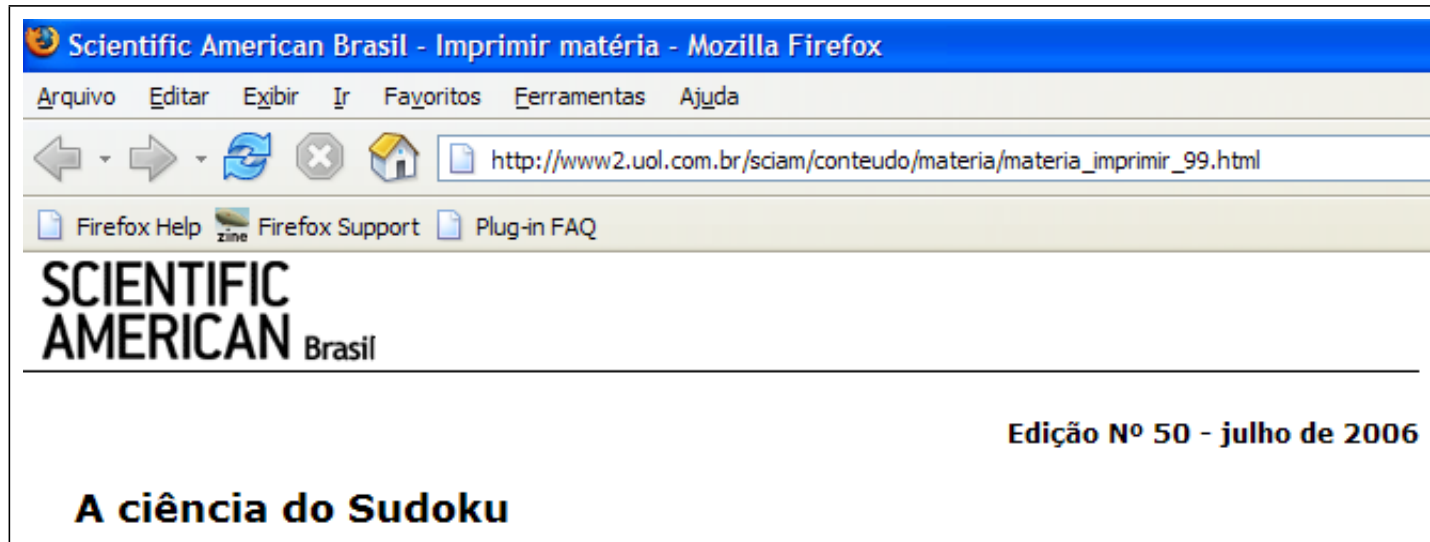
Godoku: O jogo Godoku é similar ao Sudoku mas formado apenas por letras.

Exemplo de modelagem: SuperSudoku (2)

6	1	B	2			5	3		A	D		8		C	F
		0	8		B	C			7	6	F				5
4	9		D	2			0	8			C	B		7	1
		F			D	8		3	B		1		A	0	E
3	4		5	A		1	7		F	2		C	0	9	
								6				A			B
0		E	B	D	6		9	1	4		A		5		
		6			4		5	9		8	7			E	3
				B				5	3			E	7		4
F		5				6		A		4	8			2	
	8		4				C	F	2			1	3		A
2		7				4		E			6			F	
		C	0	4			2			1	B			5	9
7	E			5		D		4	9		0	3		B	8
5		4		8		7	6		E	F	3		C		
8		1		3	0		B	C		5		7		4	D

O jogo SuperSudoku é similar ao Sudoku e Godoku formado por números e letras. Cada grid tem 16 entradas, sendo nove dos números (0 a 9) e seis letras (A a F).

Exemplo de modelagem: Mais informações sobre o Sudoku e jogos similares (3)



Para mais detalhes sobre o Sudoku e variantes desse jogo, veja o artigo “A ciência do Sudoku” por Jean-Paul Delahaye, na revista *Scientific American Brasil*, edição nº 50 de julho de 2006.

Exemplo de modelagem: Kasparov × Deep Blue



In the first ever traditional chess match between a man (world champion Garry Kasparov) and a computer (IBM's Deep Blue) in 1996, Deep Blue won one game, tied two and lost three. The next year, Deep Blue defeated Kasparov in a six-game match – the first time a reigning world champion lost a match to a computer opponent in tournament play. Deep Blue was a combination of special purpose hardware and software with an IBM RS/6000 SP2 (seen here) – a system capable of examining 200 million moves per second, or 50 billion positions, in the three minutes allocated for a single move in a chess game.

Referência: http://www-03.ibm.com/ibm/history/exhibits/vintage/vintage_4506VV1001.html



Questões sobre a modelagem (1)

- O objetivo é projetar um algoritmo para resolver o problema.
 - Veja que o Sudoku e o *Deep Blue* têm características bem diferentes!
- Esse projeto envolve dois aspectos:
 1. O algoritmo propriamente dito, e
 2. A estrutura de dados a ser usada nesse algoritmo.
- Em geral, a escolha do algoritmo influencia a estrutura de dados e vice-versa.
 - É necessário considerar diferentes fatores para escolher esse par (algoritmo e estrutura de dados).
 - Pontos a serem estudados ao longo do curso, começando pela sequência de disciplinas Algoritmos e Estruturas de Dados.
- Nesta disciplina, estudaremos vários tópicos relacionados tanto a algoritmos quanto estruturas de dados.

Questões sobre a modelagem (2)

O caso do jogo Sudoku

- Um possível algoritmo para resolver o jogo Sudoku é o Algoritmo de “Força Bruta”:
 - Tente todas as possibilidades até encontrar uma solução!
- Nessa estratégia, quantas possibilidades existem para a configuração abaixo?

		3	1					6
	7			3				2
6		9		8		7		
2					8			
	5	6		1		3	8	
			2					4
		8		6		5		1
	9			4			6	
1					3	2		

458	248		3	1	2579	24579	489	459	
3	3	3	1	4	4	3	3	6	
458		145	4569	3	4569	1489		589	
3	7	3	4	3	4	4	2	3	
6	124	9	45	8	245	7	1345	35	
3	3	9	2	8	3	7	4	2	
2	134	147	345679	579		8	189	1579	579
3	3	3	6	3		8	3	4	3
479			479	1	479	3	8	279	
3	5	6	3	1	3	3	8	3	
3789	138	17		579	5679	189	1579		
4	3	2	2	3	4	3	4	4	
347	234		79		279		3479		
3	3	8	2	6	3	5	4	1	
357		257	578		1257	8		378	
3	9	3	3	4	4	1	6	3	
1	46	457	5789	579		3	2	479	789
2	3	4	3	3		2	3	3	

Legenda: x n° de opções para a posição

→ Existem $1^1 \times 2^5 \times 3^{32} \times 4^{13} \times 6^1 =$
 $23\ 875\ 983\ 329\ 839\ 202\ 653\ 175\ 808 \approx 23,8 \times 10^{24}$ possibilidades!

O papel de algoritmos em computação

- Definição: um **algoritmo** é um conjunto finito de instruções precisas para executar uma computação.
 - Um algoritmo pode ser visto como uma ferramenta para resolver um problema computacional bem especificado.
 - O vocábulo algoritmo origina do nome *al-Khowarizmi*.
- Um algoritmo pode receber como entrada um conjunto de valores e pode produzir como saída um outro conjunto de valores.
 - Um algoritmo descreve uma sequência de passos computacionais que transforma a entrada em uma saída, ou seja, uma relação entrada/saída.

Origem do vocábulo algoritmo



Abu Ja'Far Mohammed Ibn Musa al-Khwarizmi (780–850), astrônomo e matemático árabe. Era membro da “Casa da Sabedoria”, uma academia de cientistas em Bagdá. O nome al-Khwarizmi significa da cidade de Khwarizmi, que agora é chamada Khiva e é parte do Uzbequistão. al-Khwarizmi escreveu livros de matemática, astronomia e geografia. A álgebra foi introduzida na Europa ocidental através de seus trabalhos. A palavra álgebra vem do árabe al-jabr, parte do título de seu livro *Kitab*

al-jabr w'al muquabala. Esse livro foi traduzido para o latim e foi usado extensivamente. Seu livro sobre o uso dos numerais hindu descreve procedimentos para operações aritméticas usando esses numerais. Autores europeus usaram uma adaptação latina de seu nome, até finalmente chegar na palavra **algoritmo** para descrever a área da aritmética com numerais hindu.

Algoritmo e modelo computacional (1)

- **Modelo:**
 - Esquema que possibilita a representação de uma entidade (Houaiss).
 - No modelo, só se deve incluir o que for relevante para a modelagem do objeto em questão.
- **Computacional:**
 - Relativo ao processamento (Houaiss).
- **Definição (nosso contexto):**
 - Esquema que descreve como é o modelo abstrato do processamento de algoritmos.
- **Importância:**
 - Um algoritmo não existe, ou seja, não é possível escrevê-lo, se antes não for definido o modelo computacional associado (onde será executado).
 - Conceito básico no projeto de qualquer algoritmo.

Algoritmo e modelo computacional (2)

- Que modelos existem?
 - Literalmente dezenas deles.
 - Se não estiver satisfeito, invente o seu!
- O mais popular (usado) de todos:
 - RAM – Random Access Machine.
 - Modela o computador tradicional e outros elementos computacionais.



Computador pessoal



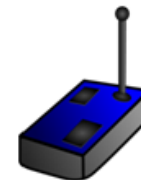
Laptop



Tablet



Telefone celular



Sensor

Algoritmo e modelo computacional: Modelo RAM (3)

- Elementos do modelo:
 - um único processador;
 - memória.
- Observações:
 - Podemos ignorar os dispositivos de entrada e saída (teclado, monitor, etc) assumindo que a codificação do algoritmo e os dados já estão armazenados na memória.
 - Em geral, não é relevante para a modelagem do problema saber como o algoritmo e os dados foram armazenados na memória.

Algoritmo e modelo computacional: Modelo RAM (4)

- Computação nesse modelo:
 - Processador busca instrução/dado da memória.
 - Uma única instrução é executada de cada vez.
 - Cada instrução é executada sequencialmente.
- Cada operação executada pelo processador, incluindo cálculos aritméticos, lógicos e acesso à memória, implica em um **custo de tempo**:
 - Função de complexidade de tempo.
- Cada operação e dado armazenado na memória, implica em um **custo de espaço**:
 - Função de complexidade de espaço.

Complexidade de tempo e espaço

- A complexidade de tempo não representa tempo diretamente, mas o número de vezes que determinada operação considerada relevante é executada.
- A complexidade de espaço representa a quantidade de memória (em uma unidade qualquer) que é necessário para armazenar as estruturas de dados associadas ao algoritmo.
- Usa-se a notação assintótica para representar essas complexidades:
 - O (O grande);
 - Ω (Ômega grande);
 - Θ (Teta);
 - o (o pequeno);
 - ω (ômega pequeno).

Modelo computacional para sistemas distribuídos

- Mundo distribuído:
 - Normalmente os elementos computacionais seguem o modelo RAM que são interconectados através de algum meio e só comunicam entre si através de troca de mensagens.
 - Não existe compartilhamento de memória.
- Elementos desse modelo:
 - Elemento computacional representado pelo modelo RAM.
 - Canal normalmente representado pelo modelo FIFO (first-in, first-out).

Problema dos dois exércitos (1)

Na Grécia antiga, lugares maravilhosos como este ...



Vale perto de Almfiklia, Grécia

...podiam se transformar em cenários de guerra.



→ É quando algum filósofo propõe o “Problema dos dois exércitos”.

Problema dos dois exércitos (2)

Cenário inicial



- Exército **Alfa** está em maior número que o exército **Gama** mas está dividido em duas metades, cada uma em uma lateral do vale.
- Cada metade do exército **Alfa** está em menor número que o exército **Gama**.
- Objetivo do exército **Alfa**: coordenar um ataque ao exército **Gama** para ganhar a guerra.

Problema dos dois exércitos (3)

O problema da coordenação

Exército Alfa
Lateral do vale



Exército Gama
Centro do vale



Exército Alfa
Lateral do vale



Vale perto de Almfiklia, Grécia



1. General do exército **Alfa**, do lado esquerdo do vale, chama o seu melhor soldado para levar uma mensagem para o general do exército **Alfa** do lado direito:



Vamos atacar conjuntamente o exército **Gama** amanhã às 6:00h?

- Observações:
- A **única** possibilidade de comunicação entre os dois generais é através de um mensageiro.
 - Os dois generais têm um “relógio perfeitamente sincronizado”, ou seja, eles sabem quando será 6:00h.

Problema dos dois exércitos (4)

O problema da coordenação

Exército Alfa
Lateral do vale



Exército Gama
Centro do vale



Exército Alfa
Lateral do vale



Vale perto de Almfiklia, Grécia



2. O soldado do exército **Alfa** atravessa as linhas inimigas e leva a mensagem até o general do outro lado.

Problema dos dois exércitos (5)

O problema da coordenação

Exército Alfa
Lateral do vale



Exército Gama
Centro do vale



Exército Alfa
Lateral do vale



Vale perto de Almfiklia, Grécia



- O general do exército **Alfa** do lado direito concorda em atacar o exército **Gama** no dia seguinte às 6:00h.

Problema dos dois exércitos (6)

O problema da coordenação

Exército Alfa
Lateral do vale



Exército Gama
Centro do vale



Exército Alfa
Lateral do vale



④
←



Vale perto de Almfiklia, Grécia



- O soldado do exército **Alfa** atravessa novamente as linhas inimigas e confirma com seu general o ataque para o dia seguinte.

Problema dos dois exércitos (7)

O problema da coordenação

Exército Alfa
Lateral do vale



Exército Gama
Centro do vale



Exército Alfa
Lateral do vale



Vale perto de Almfiklia, Grécia

→ Após esses quatro passos terem sido realizados com sucesso no mesmo dia, haverá ataque no dia seguinte às 6:00h?

O problema dos dois robôs (1)

- Imagine dois ou mais robôs que vão carregar uma mesa de tal forma que um ficará de frente para outro.
- Problema:
 - Projete um algoritmo para coordenar a velocidade e direção do movimento de cada robô para que a mesa não caia.
 - Os robôs só podem comunicar entre si através de um canal de comunicação sem fio.
- Esse problema tem solução?
 - Variante do problema anterior!



O problema dos dois robôs (2)

- É possível projetar um algoritmo distribuído para esse problema?
NÃO! Não existe um algoritmo distribuído para o problema de coordenação considerando o modelo computacional proposto!
- E se o canal de comunicação usado para troca de mensagens for “perfeito”, ou seja, toda mensagem enviada chegará garantidamente ao seu destino em um tempo finito?
Sim! Supõe-se que cada elemento computacional participante desse processo também não falha.

Alguns comentários sobre algoritmos distribuídos

- São a base do mundo distribuído, ou seja, de sistemas distribuídos.
- Sistemas distribuídos podem ser:
 - Tempo real ou não;
 - Reativos ou não.
- Sistemas distribuídos podem ser especificados tomando-se como base:
 - tempo;
 - eventos.

Considerações finais

- Até agora falamos sobre Matemática Discreta como um conjunto de princípios, técnicas e metodologias para resolução de problemas.
- Essa é exatamente a abordagem que desenvolveremos neste disciplina.
- Matemática Discreta inclui um número muito grande de assuntos e só discutiremos alguns deles.
- Os tópicos que estudaremos não são novos. A maior parte deles são mais antigos que Ciência da Computação.