Análise de Computabilidade e Complexidade de Algoritmos

Docente: Diego Luiz e Cunha da Silva

Apresentação da Disciplina

- Noções e terminologias matemáticas
- A Máquina da Turing
- A Tese de Church-Turing
- Computabilidade
- Complexidade de Tempo e Espaço
- A classe NP
- NP-completude

Bibliografia

- Introdução a teoria da Computação
    - Michael Sipser

- Teoria da Computação: Máquinas Universais e Computabilidade
    - TiarajúAsmuzDiverioet.al.

- Complexidade de Algoritmos
    - Laira Vieira Toscaniet.al.

Noções e Terminologias Matemáticas

Conjunto

- Um conjunto é um grupo de objetos representados como uma unidade.
- Podem incluir qualquer tipo de objeto, incluindo números, símbolos e até mesmo outros conjuntos.
- O objetos de um conjunto são chamados de elementos ou membros.
- Uma forma de descrever os elementos de um conjunto:

  {7, 21, 57}

Conjunto

- Os símbolos de $\in$ e $\notin$ denotam pertinência e não-pertinência
- Baseado no conjunto {7, 21, 57}, temos:

$7 \in \{7, 21, 57\}$

$8 \notin \{7, 21, 57\}$

- Para dois conjuntos *A* e *B*, dizemos que *A* é um subconjunto de *B*, descrito pelo operador $A \subseteq B$, se todos os membros de A for também um membro de *B*.

Conjunto

- A ordem de descrição dos elementos de um conjunto não importa, nem a repetição de seus membros.
- Caso queiramos levar em consideração o número de ocorrências de um mesmo membro, chamamos o grupo de multiconjunto.

{7} e {7, 7} são diferentes como multiconjuntos, mas idênticos como conjunto.

- Conjunto com 0 membros é denominado como conjunto vazio e é descrito como Ø.

Conjunto

- Quando desejamos descrever um conjunto contendo elementos de acordo com algum regra, escrevemos {n | regra sobre n}.

{n|n=m^2 para algum m $\in \mathbb{N}$} – significa o conjunto de quadrados perfeitos.

- Tendo dois conjuntos *A* e *B*, a união entre eles pode ser descrita como $A \cup B$ que obtemos um conjunto combinando todos os elementos.
- A intersecção de *A* e *B*, pode ser descrita como $A \cap B$ que obtemos o conjunto de elementos que estão em ambos.

Conjunto

- O Complemento de $\overline{A}$, é o conjunto de todos os elementos sob consideração que não estão em *A*.
- Uma forma de representar os conjuntos usamos um tipo de desenho chamado de D**iagrama de Venn**. Ele representa os conjuntos como regiões delimitadas por linhas circulares.

Conjunto

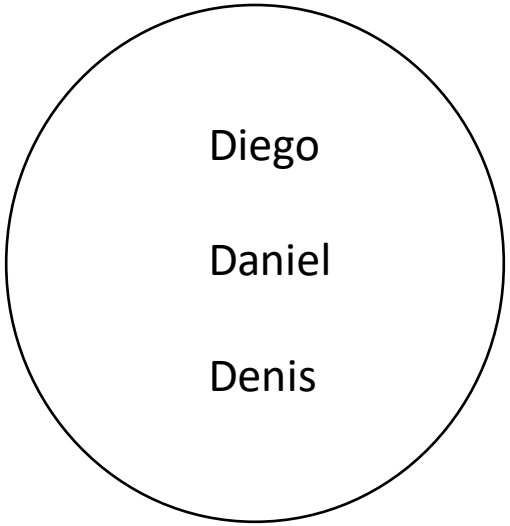


Diagrama de Venn para o conjunto de nomes próprios começando com a letra “D”

Conjunto

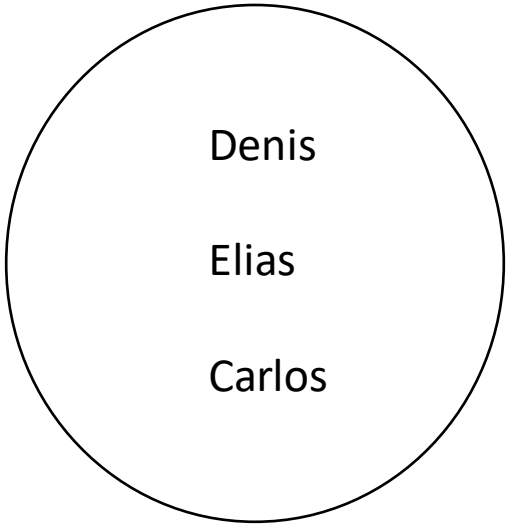
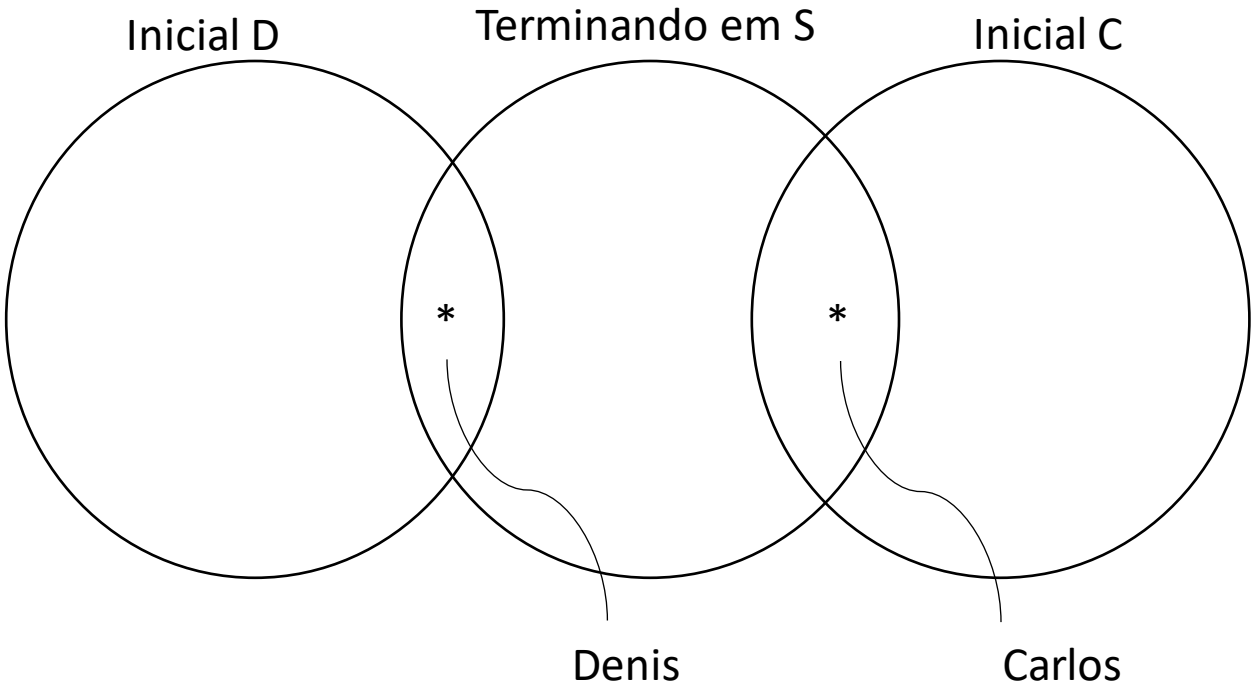
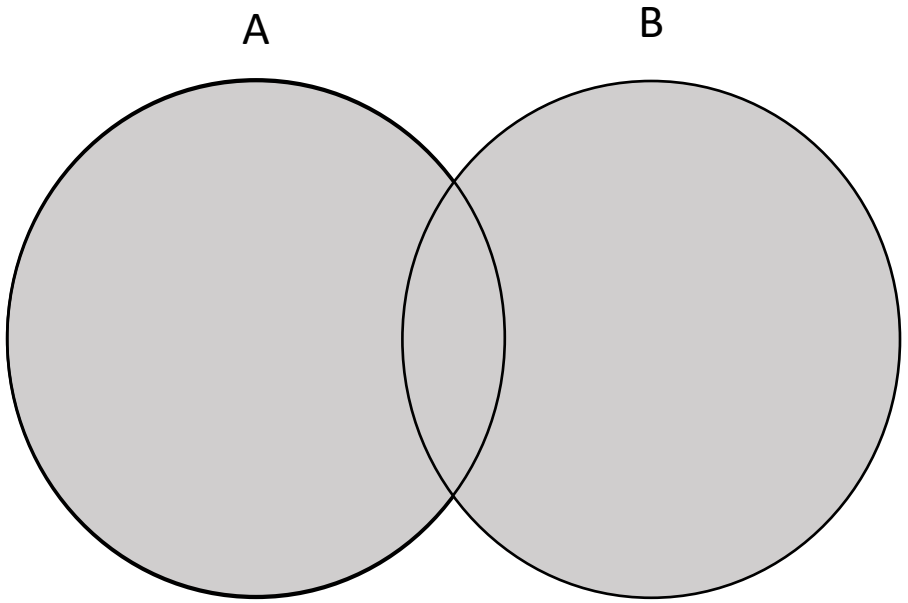


Diagrama de Venn para o conjunto de nomes próprios terminados com a letra “S”

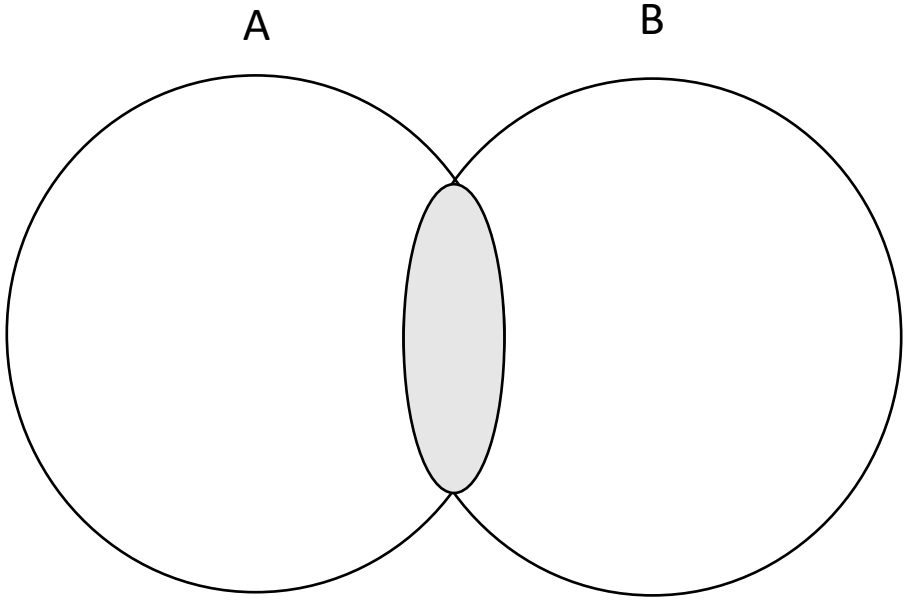
Conjunto



Conjunto



$A \cup B$



$A \cap B$

Sequência e Uplas

- Uma sequência de objetos é um lista desses objetos na mesma ordem. Geralmente designamos uma sequência escrevendo a lista entre parênteses.

(7, 21, 57)

- Em um conjunto a ordem não importa, mas em uma sequência sim. Daí (7, 21, 57) não o mesmo que (57, 7, 21).
- A repetição realmente importa em uma sequência.

Sequência e Uplas

- Como os conjuntos e sequências podem ser finitas ou infinitas. As sequências frequentemente são chamadas de uplas
- Uma sequência com *k* elementos é uma k-upla. Dessa forma (7, 21, 57) é uma 3-upla. Uma 2-upla é também chamado de par.
- Conjuntos e sequências podem aparecer como elementos de outros conjuntos e sequências. Por exemplo, o conjunto das partes de *A* é o conjunto de todos os subconjuntos de *A*.

Se *A* for o conjunto {0, 1}, o conjunto das partes de *A* é o conjunto {∅, {0}, {1}, {0, 1}}.

Sequência e Uplas

- O conjunto de todos os pares cujos elementos são 0s e 1s é {(0, 0), (0, 1), (1, 0), (1, 1)}.
- Se *A* e *B* são dois conjuntos, o produto cartesiano ou produto cruzado de A e B, pode ser descrito como *A* x *B*, é o conjunto de todos os pares nos quais o primeiro elemento é um membro de *A* e o segundo elemento é um membro de *B*.

Ex. Se A={1, 2} e B={ x, y, z}

A x B = {(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)}

Sequência e Uplas

- Podemos também tomar o produto cartesiano de k conjuntos, A_1, A_2, A_3, ..., A_k, *descrito como* $A_1 \times A_2 \times A_3 \times \ldots \times A_k$
- Se temos o produto cartesiano de um conjunto com si próprio, usamos a abreviação:

$A_1 \times A_2 \times A_3 \times \ldots \times A_k = A^k$

Exercícios

1- Se *A*={1, 2} e *B*={x, y, z}, então qual o conjunto de: *A* x *B* x *A*

2- O conjunto $\mathbb{N}^2$ é igual a $\mathbb{N}\ x\ \mathbb{N}$. Ele consiste de todos os pares de números naturais. Dê a descrição forma para o conjunto.

Exercícios

1- Se A={1, 2} e B={x, y, z}, então qual o conjunto de: A x B x A

A x B x A ={(1, x, 1), (1, x, 2), (1, y, 1), (1, y, 2), (1, z, 1), (1, z, 2), (2, x, 1), (2, x, 2), (2, y, 1), (2, y, 2), (2, z, 1), (2, z, 2)}

2- O conjunto $\mathbb{N}^2$ é igual a $\mathbb{N}\, x\, \mathbb{N}$. Ele consiste de todos os pares de números naturais. Dê a descrição forma para o conjunto.

{(x, y) | x, y$\geq$1}

Funções e Relações

- As funções são centrais em matemática. Uma função é um objeto que estabelece um relacionamento de entrada-saída. Uma função toma uma entrada e produz uma saída. Em toda função, a mesma entrada produz a mesma saída.

  $f(a)=b$

- Por exemplo a função do valor absoluto *abs* toma o número x como entrada e retorna x se x for positivo e - x se x for negativo. Portanto, *abs(2) = abs(-2)=2*.

Funções e Relações

- O conjunto de entradas possíveis para um função é chamado seu domínio. As saídas de um função vêm de um conjunto denominado de contradomínio. A notação para dizer que *f* é uma função com domínio *D* e contradomínio *C* é:

  f: D -> C.

- Podemos descrever uma função específica de várias maneiras. Uma delas é por meio de um procedimento para computar uma saída a partir de uma entrada especificada. Outra através de uma tabela que listas todas as entradas possíveis e dá a saída para cada entrada.

Funções e Relações

n	*f(n)*
0	1
1	2
2	3
3	4
4	0

- Ex.

Considere a função *f:{0, 1, 2, 3, 4} -> {0, 1, 2, 3, 4}*

Essa função adiciona 1 à sua entrada e aí, dá como saída o resultado módulo 5.

Quando fazemos aritmética modular, definimos $\mathbb{Z}_m$={0, 1, 2, ..., m-1}.

Com essa notação, a função supramencionada *f* tem a forma:

$$f: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$$

Funções e Relações

- As vezes uma tabela bidimensional é usada se o domínio da função é o produto cartesiano de dois conjuntos

A função *g:* $\mathbb{Z}_4 \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$

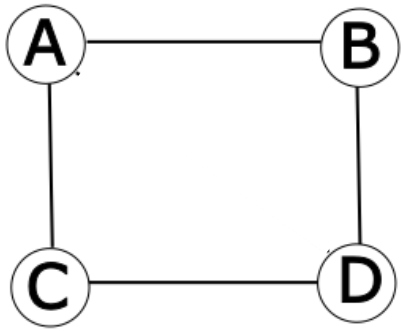
A entrada na linha rotulada *i* e na coluna *j* na tabela é o valor de *g(i, j)*

A função *g* é uma função de adição módulo 4

g	*0*	*1*	*2*	*3*
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Grafos

- Um grafo é um conjunto de pontos com linhas conectando alguns pontos.
- Os pontos são conhecidos como nós ou vértices, e as linhas são chamadas de arestas.



- O número de arestas em um nó específico é o grau do nó, na figura acima todos os nós possuem grau 2

Grafos

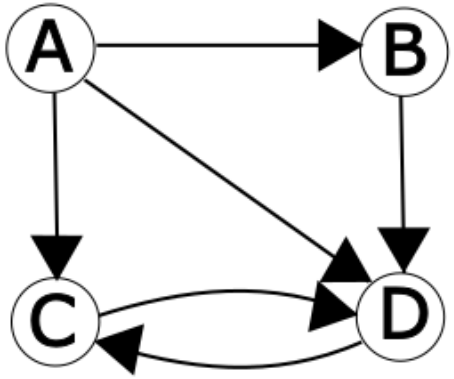
- Em um grafo G que contém nós i e j, o par (i, j) representa a aresta que conecta i e j. A ordem de i e j não importam em um grafo não-direcionado.
- As vezes descrevemos arestas com conjunto em vez de pares, como em {i, j}, porque a ordem dos nós não é importante.
- Se V é o conjunto de nós de G e E, os de arreatas, dizemos que G = (V, E).

No caso do modelo anterior, podemos fazer a descrição formal

G= ({A, B, C, D}, {(A,B), (A, C), (B, D), (C,D)}

Grafos

- Os grafos frequentemente são usados para representar dados. Os nós podem ser cidades e as arestas, as estradas que as conectam.
- Se um grafo possui setas em vez de linhas, o grafo é um grafo direcionado.



- A descrição do forma do grafo acime é:

G=({A,B, C, D},{(A,B),(A,C),(A,D),(B,D),(C,D),(D,C)}

Cadeias e Linguagens

- Cadeias de caracteres são blocos básicos fundamentais em ciência da computação. O alfabeto sobre o qual as cadeias são definidas pode variar com a aplicação.
- O alfabeto é definido como um conjunto finito não vazio.
- Os membros do alfabeto são os símbolos do alfabeto
- Geralmente utilizamos letras gregas maiúsculas Σ ou Γ(sigma ou gama) para designar alfabetos.

Σ = {0, 1}

Σ = {a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z}

Cadeias e Linguagens

- Uma cadeia sobre um alfabeto é uma sequência finita de símbolos daquele alfabeto.

Σ= {0,1}, então 01001 é uma cadeia sobre Σ

Γ ={a, b, c, ..., z}, então abracadabra é uma cadeia de Γ

- Se *w* é uma cadeia sobre Σ o comprimento de *w*, é escrito $|w|$, ou seja é o número de símbolos que a cadeia contém.
- A cadeia de comprimento zero é chamada de cadeia vazia e é escrita por ε (epsílon)

Cadeias e Linguagens

- Concatenação de cadeias $w^0 = \varepsilon$, $w^3 =$ www
- Prefixo de uma palavra é qualquer sequência inicial de símbolos da palavra
- Sufixo de uma palavra é qualquer sequência final de símbolos de uma palavra

Ex. relativamente a palavra abcb, tem-se:

Prefixos: ε, a, ab, abc, abcb

Sufixos: ε, b, cb, bcb, abcb

Cadeias e Linguagens

- Se Σ representa um alfabeto, então:

Σ^* denota o conjunto de todas as palavras sobre Σ

Σ^+ denota Σ^* -{ε}

Lógica Booleana

- Sistema matemático construído em torno de “VERDADEIRO” e “FALSO”
- Operações com booleanos:
  - Negação “NÃO”. Símbolo ~ ou ¬
  - Conjunção “E”. Símbolo ^
  - Disjunção “OU”. Símbolo v
  - Ou Exclusivo, ou XOR $\oplus$

Definições, Teoremas e Provas

- O teorema e as provas são o coração e a alma da matemática
- As definições são o espírito

- Definição: descrevem os objetos e noções que usamos. Pode ser simples como conjunto ou complexa como a definição de segurança em um sistema criptográfico

Definições, Teoremas e Provas

- Prova: é o argumento lógico convincente de que um enunciado é verdadeiro. Em matemática um argumento tem de ser um enunciado inatacável, isto é, convincente em um sentido absoluto.

- Teorema: é um enunciado matemático demonstrado como verdadeiro

Encontrando provas

- Determinar a veracidade ou falsidade de um enunciado matemático é com uma prova matemática.

- Exemplo
  - Suponha que você deseje provar o enunciado: para todo grafo G a soma dos graus de todos os nós em G é um número par.

  Primeiro, pegue uns poucos grafos e observe esse enunciado em ação.

  A seguir tente encontrar um contra-exemplo.

- Para praticar Lei de Morgan

Tipos de prova

- Determinar a veracidade ou falsidade de um enunciado matemático é com uma prova matemática.

- Para praticar Lei de Morgan