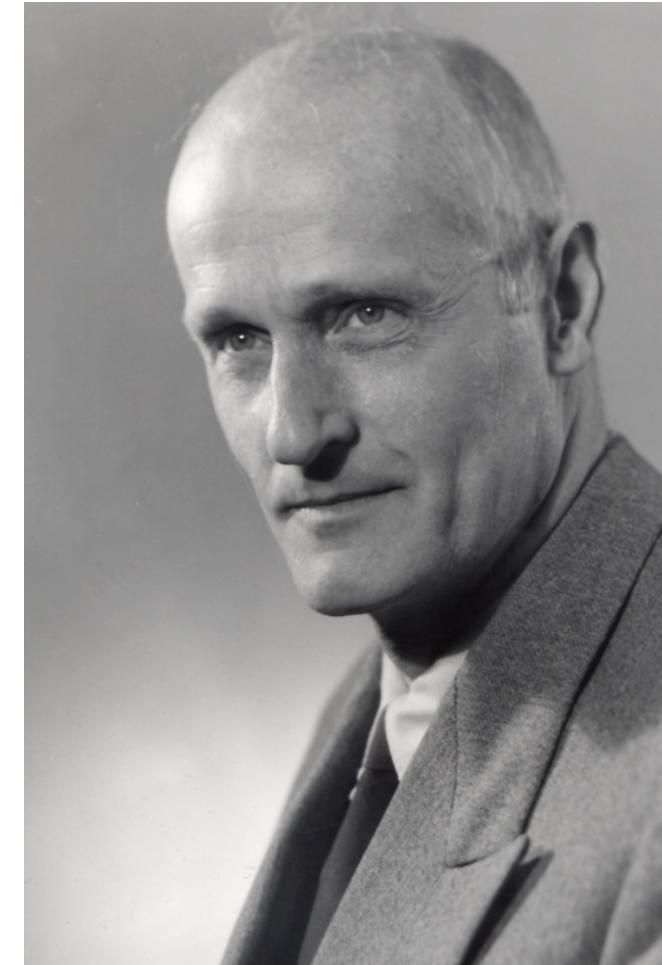


TEORIA DA COMPUTAÇÃO

0. Introdução



Alonzo Church



Stephen Kleene



Alan Turing

O que é Teoria da Computação? Quais seus objetivos?

Estudo das propriedades matemáticas fundamentais do hardware, do software e das aplicações de um computador.



Problema: aplicação prática difícil de enxergar e entender

Por ser uma disciplina essencialmente teórica, os alunos têm muita dificuldade de enxergar a aplicação imediata desse conhecimento. E com razão:

Gramáticas → **projetar uma linguagem de programação**

Autômatos Finitos → **buscas em strings e casamento de padrões**

Expressões regulares → **buscas em strings e casamento de padrões**

Problema difícil → **complexidade, NP-completo**

Provas matemáticas → **?**

Aplicação tardia:

Aumenta capacidade mental, melhora capacidade de se expressar de modo claro e preciso, de resolver problemas e saber quando um problema é insolúvel.

Qual a melhor maneira de aprender? Qual nossa abordagem?

**Fazer uma parte teórica pura com seminários
semanais de aplicação prática em situações de
programação e resolução de problemas.**

Vai dar certo? Só Jesus sabe...



Áreas fundamentais da Teoria da Computação



Quais são as capacidades fundamentais e limitações dos computadores?

Teoria da Complexidade

O que faz com que alguns problemas sejam computacionalmente difíceis e outros sejam computacionalmente fáceis? Exemplos:

→ Ordenação

→ Agendamento

Resposta:

Teoria da Complexidade

O que faz com que alguns problemas sejam computacionalmente difíceis e outros sejam computacionalmente fáceis? Exemplos:

- Ordenação
- Agendamento

Resposta:

NÃO SABEMOS. Em muitas situações não sabemos nem conseguimos demonstrar matematicamente que um problema é fácil ou difícil. Temos algumas evidências que indicam, mas uma prova definitiva ainda não.

Teoria da Complexidade

Uma conquista importante dessa área foi a criação de uma "tabela periódica" para a classificação dos problemas computacionais de acordo com seu grau de dificuldade.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18		
1 H Hydrogen 1.008	2 Be Beryllium 9.0122	3 Mg Magnesium 24.305	4 C Solid	5 Hg Liquid	6 Li Lithium 6.94	7 Na Sodium 22.990	8 Ti Alkali metals	9 V Alkaline earth metals	10 Cr Metals	11 Mn Lanthanoids	12 Fe Transition metals	13 Co Post-transition metals	14 Ni Nonmetals	15 B Metalloids	16 O Reactive nonmetals	17 He Noble gases	18 Ne Helium 4.0026		
2 He Helium 4.0026	3 Ne Neon 20.180	4 Ar Argon 39.948	5 Al Aluminium 26.982	6 Si Silicon 28.085	7 P Phosphorus 30.974	8 S Sulfur 32.06	9 Cl Chlorine 35.45	10 Br Bromine 83.798	11 Kr Krypton 83.798	12 Ga Gallium 69.723	13 Ge Germanium 72.630	14 As Arsenic 74.922	15 Se Selenium 78.971	16 In Indium 114.82	17 Sn Tin 118.71	18 Sb Antimony 121.76	19 Te Tellurium 127.60	20 I Iodine 126.90	21 Xe Xenon 131.29
3 Rb Rubidium 85.468	4 Ca Calcium 40.078	5 Sc Scandium 44.956	6 Ti Titanium 47.867	7 V Vanadium 50.942	8 Cr Chromium 51.996	9 Mn Manganese 54.938	10 Fe Iron 55.845	11 Co Cobalt 58.933	12 Ni Nickel 58.693	13 Cu Copper 63.546	14 Zn Zinc 65.38	15 Ga Gallium 69.723	16 Ge Germanium 72.630	17 As Arsenic 74.922	18 Se Selenium 78.971	19 Br Bromine 83.798	20 Kr Krypton 83.798	21 Rb Rubidium 85.468	
4 Sc Scandium 44.956	5 Ti Titanium 47.867	6 V Vanadium 50.942	7 Cr Chromium 51.996	8 Mn Manganese 54.938	9 Fe Iron 55.845	10 Co Cobalt 58.933	11 Ni Nickel 58.693	12 Cu Copper 63.546	13 Zn Zinc 65.38	14 Ga Gallium 69.723	15 Ge Germanium 72.630	16 As Arsenic 74.922	17 Se Selenium 78.971	18 Br Bromine 83.798	19 Kr Krypton 83.798	20 Rb Rubidium 85.468	21 Sc Scandium 44.956		
5 Rb Rubidium 85.468	6 Sr Strontium 87.62	7 Y Yttrium 88.906	8 Zr Zirconium 91.224	9 Nb Niobium 92.906	10 Mo Molybdenum 95.95	11 Tc Technetium (98)	12 Ru Ruthenium 101.07	13 Rh Rhodium 102.91	14 Pd Palladium 106.42	15 Ag Silver 107.87	16 Cd Cadmium 112.41	17 In Indium 114.82	18 Sn Tin 118.71	19 Sb Antimony 121.76	20 Te Tellurium 127.60	21 I Iodine 126.90	22 Xe Xenon 131.29	23 Rb Rubidium 85.468	
6 Cs Caesium 132.91	7 Ba Barium 137.33	8 Hf Hafnium 178.49	9 Ta Tantalum 180.95	10 W Tungsten 183.84	11 Re Rhenium 186.21	12 Os Osmium 190.23	13 Ir Iridium 192.22	14 Pt Platinum 195.08	15 Au Gold 196.97	16 Hg Mercury 200.59	17 Tl Thallium 204.38	18 Pb Lead 207.2	19 Bi Bismuth 208.98	20 Po Polonium (209)	21 At Astatine (210)	22 Rn Radon (222)	23 Cs Caesium 132.91		
7 Fr Francium (223)	8 Ra Radium (226)	9 Rf Rutherfordium (267)	10 Db Dubnium (268)	11 Sg Seaborgium (269)	12 Bh Bohrium (270)	13 Hs Hassium (277)	14 Mt Meitnerium (278)	15 Ds Darmstadtium (281)	16 Rg Roentgenium (282)	17 Cn Copernicium (285)	18 Nh Nihonium (286)	19 Fl Flerovium (289)	20 Mc Moscovium (290)	21 Lv Livermorium (293)	22 Ts Tennessine (294)	23 Og Oganesson (294)	24 Lu Lutetium 174.97		
8 Fr Francium (223)	9 Ra Radium (226)	10 Rf Rutherfordium (267)	11 Db Dubnium (268)	12 Sg Seaborgium (269)	13 Bh Bohrium (270)	14 Hs Hassium (277)	15 Mt Meitnerium (278)	16 Ds Darmstadtium (281)	17 Rg Roentgenium (282)	18 Cn Copernicium (285)	19 Nh Nihonium (286)	20 Fl Flerovium (289)	21 Mc Moscovium (290)	22 Lv Livermorium (293)	23 Ts Tennessine (294)	24 Og Oganesson (294)	25 Lu Lutetium 174.97		
9 Fr Francium (223)	10 Ra Radium (226)	11 Rf Rutherfordium (267)	12 Db Dubnium (268)	13 Sg Seaborgium (269)	14 Bh Bohrium (270)	15 Hs Hassium (277)	16 Mt Meitnerium (278)	17 Ds Darmstadtium (281)	18 Rg Roentgenium (282)	19 Cn Copernicium (285)	20 Nh Nihonium (286)	21 Fl Flerovium (289)	22 Mc Moscovium (290)	23 Lv Livermorium (293)	24 Ts Tennessine (294)	25 Og Oganesson (294)	26 Lu Lutetium 174.97		
10 Fr Francium (223)	11 Ra Radium (226)	12 Rf Rutherfordium (267)	13 Db Dubnium (268)	14 Sg Seaborgium (269)	15 Bh Bohrium (270)	16 Hs Hassium (277)	17 Mt Meitnerium (278)	18 Ds Darmstadtium (281)	19 Rg Roentgenium (282)	20 Cn Copernicium (285)	21 Nh Nihonium (286)	22 Fl Flerovium (289)	23 Mc Moscovium (290)	24 Lv Livermorium (293)	25 Ts Tennessine (294)	26 Og Oganesson (294)	27 Lu Lutetium 174.97		
11 Fr Francium (223)	12 Ra Radium (226)	13 Rf Rutherfordium (267)	14 Db Dubnium (268)	15 Sg Seaborgium (269)	16 Bh Bohrium (270)	17 Hs Hassium (277)	18 Mt Meitnerium (278)	19 Ds Darmstadtium (281)	20 Rg Roentgenium (282)	21 Cn Copernicium (285)	22 Nh Nihonium (286)	23 Fl Flerovium (289)	24 Mc Moscovium (290)	25 Lv Livermorium (293)	26 Ts Tennessine (294)	27 Og Oganesson (294)	28 Lu Lutetium 174.97		
12 Fr Francium (223)	13 Ra Radium (226)	14 Rf Rutherfordium (267)	15 Db Dubnium (268)	16 Sg Seaborgium (269)	17 Bh Bohrium (270)	18 Hs Hassium (277)	19 Mt Meitnerium (278)	20 Ds Darmstadtium (281)	21 Rg Roentgenium (282)	22 Cn Copernicium (285)	23 Nh Nihonium (286)	24 Fl Flerovium (289)	25 Mc Moscovium (290)	26 Lv Livermorium (293)	27 Ts Tennessine (294)	28 Og Oganesson (294)	29 Lu Lutetium 174.97		
13 Fr Francium (223)	14 Ra Radium (226)	15 Rf Rutherfordium (267)	16 Db Dubnium (268)	17 Sg Seaborgium (269)	18 Bh Bohrium (270)	19 Hs Hassium (277)	20 Mt Meitnerium (278)	21 Ds Darmstadtium (281)	22 Rg Roentgenium (282)	23 Cn Copernicium (285)	24 Nh Nihonium (286)	25 Fl Flerovium (289)	26 Mc Moscovium (290)	27 Lv Livermorium (293)	28 Ts Tennessine (294)	29 Og Oganesson (294)	30 Lu Lutetium 174.97		
14 Fr Francium (223)	15 Ra Radium (226)	16 Rf Rutherfordium (267)	17 Db Dubnium (268)	18 Sg Seaborgium (269)	19 Bh Bohrium (270)	20 Hs Hassium (277)	21 Mt Meitnerium (278)	22 Ds Darmstadtium (281)	23 Rg Roentgenium (282)	24 Cn Copernicium (285)	25 Nh Nihonium (286)	26 Fl Flerovium (289)	27 Mc Moscovium (290)	28 Lv Livermorium (293)	29 Ts Tennessine (294)	30 Og Oganesson (294)	31 Lu Lutetium 174.97		
15 Fr Francium (223)	16 Ra Radium (226)	17 Rf Rutherfordium (267)	18 Db Dubnium (268)	19 Sg Seaborgium (269)	20 Bh Bohrium (270)	21 Hs Hassium (277)	22 Mt Meitnerium (278)	23 Ds Darmstadtium (281)	24 Rg Roentgenium (282)	25 Cn Copernicium (285)	26 Nh Nihonium (286)	27 Fl Flerovium (289)	28 Mc Moscovium (290)	29 Lv Livermorium (293)	30 Ts Tennessine (294)	3			

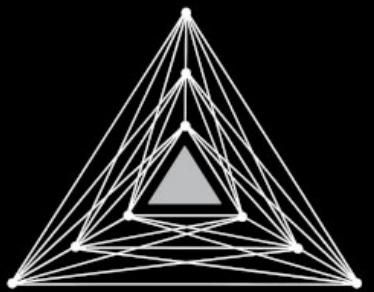
Teoria da Complexidade

194

NP-COMPLETE PROBLEMS

computers and intractability
A Guide to the Theory of NP-Completeness

Michael R. Garey / David S. Johnson



[GT16] PARTITION INTO PERFECT MATCHINGS

INSTANCE: Graph $G = (V, E)$, positive integer $K \leq |V|$.

QUESTION: Can the vertices of G be partitioned into $k \leq K$ disjoint sets V_1, V_2, \dots, V_k such that, for $1 \leq i \leq k$, the subgraph induced by V_i is a perfect matching (consists entirely of vertices with degree one)?

Reference: [Schaefer, 1978b]. Transformation from NOT-ALL-EQUAL 3SAT.

Comment: Remains NP-complete for $K = 2$ and for planar cubic graphs.

[GT17] COVERING BY CLIQUES

INSTANCE: Graph $G = (V, E)$, positive integer $K \leq |E|$.

QUESTION: Are there $k \leq K$ subsets V_1, V_2, \dots, V_k of V such that each V_i induces a complete subgraph of G and such that for each edge $\{u, v\} \in E$ there is some V_i that contains both u and v ?

Reference: [Kou, Stockmeyer, and Wong, 1978], [Orlin, 1976]. Transformation from PARTITION INTO CLIQUES.

[GT18] COVERING BY COMPLETE BIPARTITE SUBGRAPHS

INSTANCE: Bipartite graph $G = (V, E)$, positive integer $K \leq |E|$.

QUESTION: Are there $k \leq K$ subsets V_1, V_2, \dots, V_k of V such that each V_i induces a complete bipartite subgraph of G and such that for each edge $\{u, v\} \in E$ there is some V_i that contains both u and v ?

Reference: [Orlin, 1976]. Transformation from PARTITION INTO CLIQUES.

A1.2 SUBGRAPHS AND SUPERGRAPHS

[GT19] CLIQUE

INSTANCE: Graph $G = (V, E)$, positive integer $K \leq |V|$.

QUESTION: Does G contain a clique of size K or more, i.e., a subset $V' \subseteq V$ with $|V'| \geq K$ such that every two vertices in V' are joined by an edge in E ?

Reference: [Karp, 1972]. Transformation from VERTEX COVER (see Chapter 3).

Comment: Solvable in polynomial time for graphs obeying any fixed degree bound d , for planar graphs, for edge graphs, for chordal graphs [Gavril, 1972], for comparability graphs [Even, Pnueli, and Lempel, 1972], for circle graphs [Gavril, 1973], and for circular arc graphs (given their representation as families of arcs) [Gavril, 1974a]. The variant in which, for a given r , $0 < r < 1$, we are asked whether G contains a clique of size $r|V|$ or more is NP-complete for any fixed value of r .

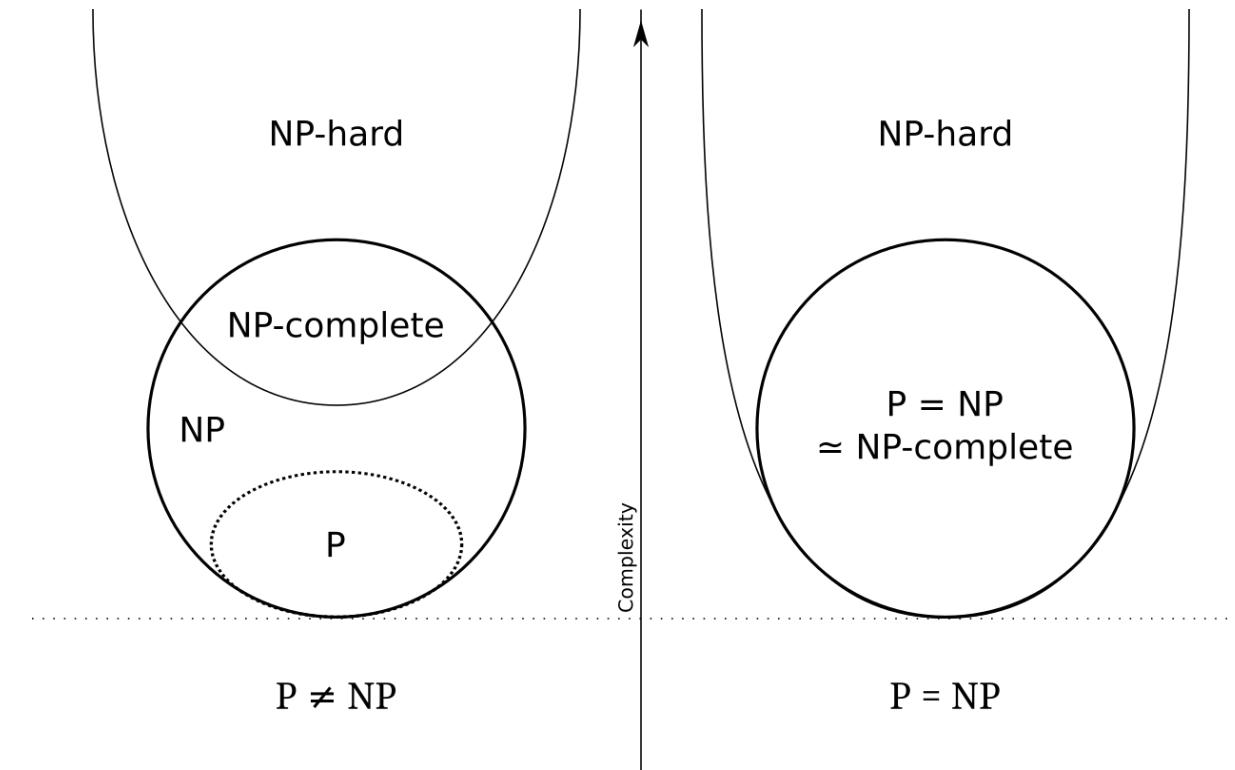
[GT20] INDEPENDENT SET

INSTANCE: Graph $G = (V, E)$, positive integer $K \leq |V|$.

QUESTION: Does G contain an independent set of size K or more, i.e., a subset

Com essas classificações conseguimos dar evidências de que um problema é difícil, mesmo que não seja possível provar.

Além disso, ainda há muita coisa que não sabemos: $P = NP$?



Teoria da Complexidade

Por que é importante classificar os problemas por grau de dificuldade?

- Alterar o problema para ficar mais fácil
- Buscar uma solução não ótima (heurística)
- Considerar tipos alternativos de computação
- Saber quando desistir

O objetivo é classificar os problemas em fáceis ou difíceis.



Teoria da Computabilidade

Todos os problemas podem ser resolvidos através de computadores?
Infelizmente, não.

No começo do séc. XIX, matemáticos como Kurt Gödel, Alan Turing e Alonzo Church demonstraram que existem problemas para os quais nenhuma solução pode ser encontrada por um computador. Exemplo:

- Verificar se uma setença matemática é verdadeira.
- Como provar que $1 + 1 = 2$?

O objetivo é classificar os problemas em solucionáveis ou não.

Seja: $a = b = 1$.

Vamos provar que $2 = 1$:

$$a = b$$

$$a^2 = ab$$

$$a^2 - b^2 = ab - b^2$$

$$(a + b)(a - b) = b(a - b)$$

$$a + b = b$$

$$1 + 1 = 1$$

$$2 = 1$$

Teoria dos Autômatos

A Teoria dos Autômatos lida com as definições e propriedades matemáticas dos modelos de computação, ou seja, busca entender o modo como um computador essencialmente realiza uma computação.

Diversos modelos computacionais existem:

→ **Autômatos finitos**

Processamento de texto, compiladores, projeto de hardware

→ **Gramáticas livres de contexto**

Linguagens de programação, inteligência artificial

→ **Outros ...**

O objetivo é entender os modos de computar.

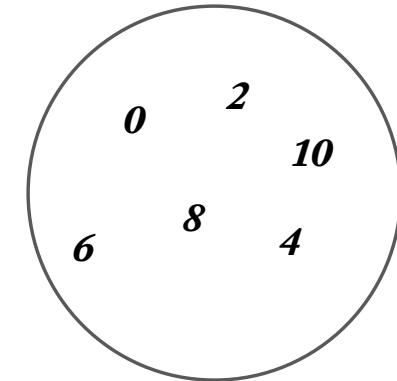
Revisão de matemática e terminologia

Conjunto:

- Coleção não ordenada de elementos com alguma característica em comum.
- Representados por enumeração, propriedade ou diagrama.

$$S = \{0, 2, 4, 6, 8, 10\}$$

$$S = \{x \mid (x \in \mathbb{Z}) \wedge (0 \leq x \leq 10)\}$$



- Se elementos repetidos importam, falamos de multiset:

$$\{10\} \quad \{10, 10\}$$

$$A \subset B$$

$$B \supset A$$

$$A \subseteq B$$

$$B \supseteq A$$

$$A \subsetneq B$$

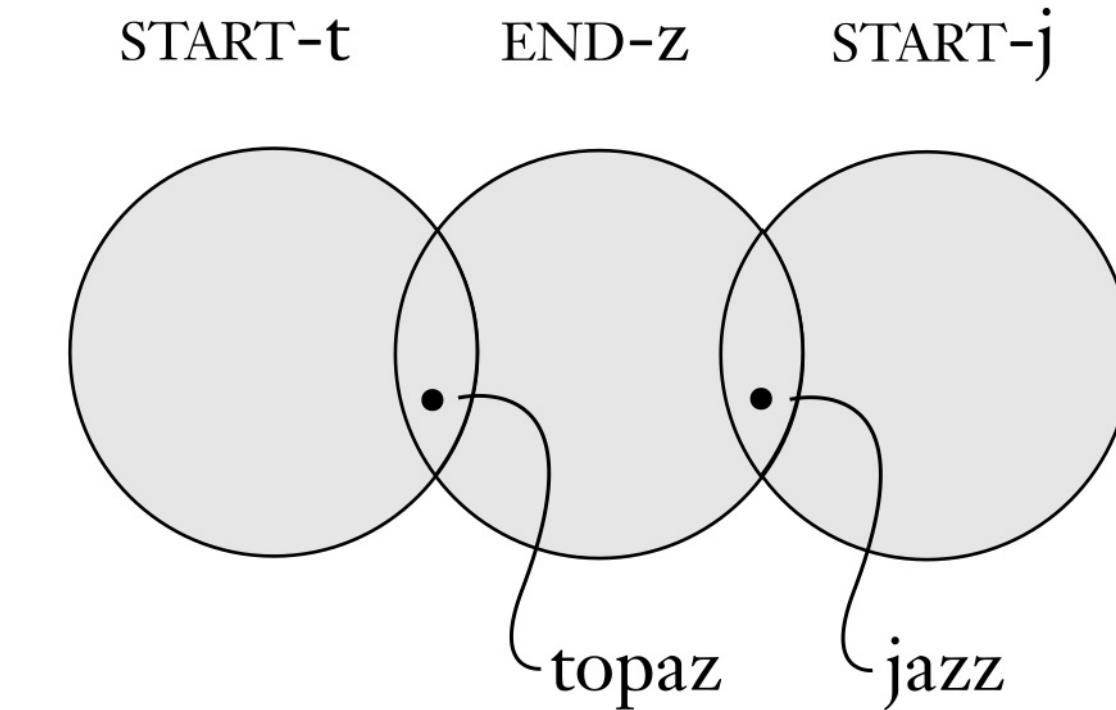
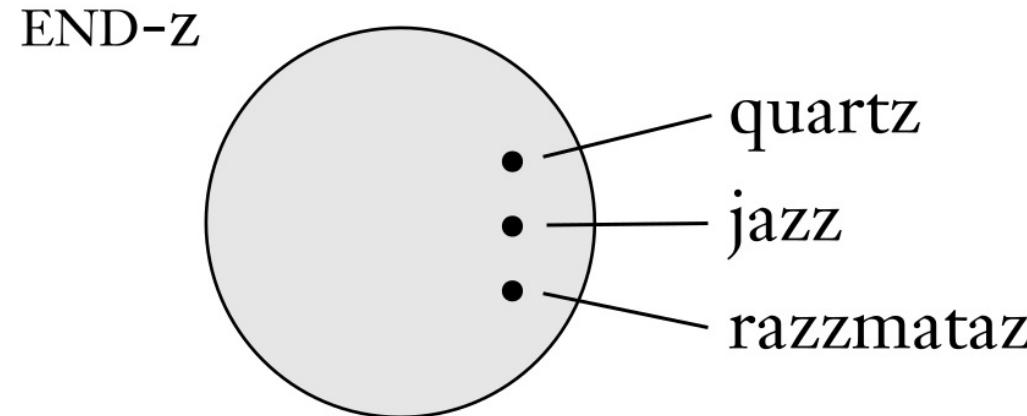
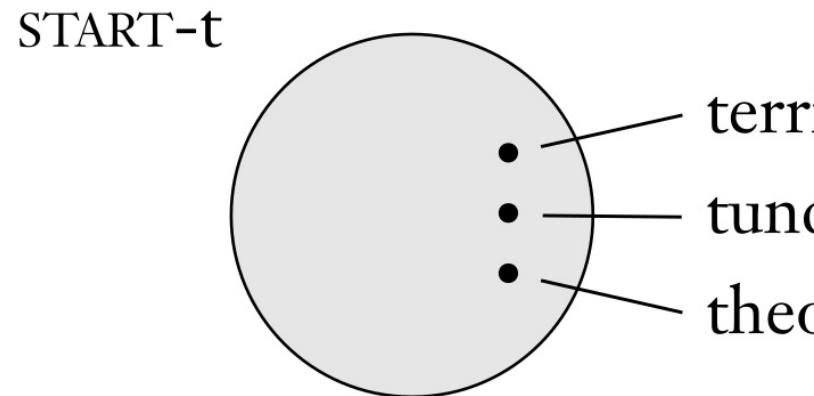
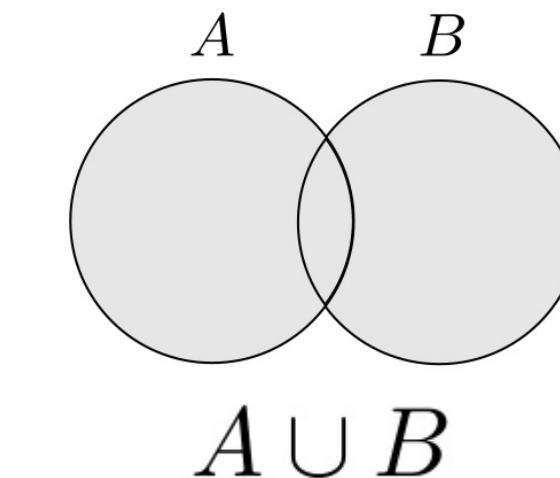
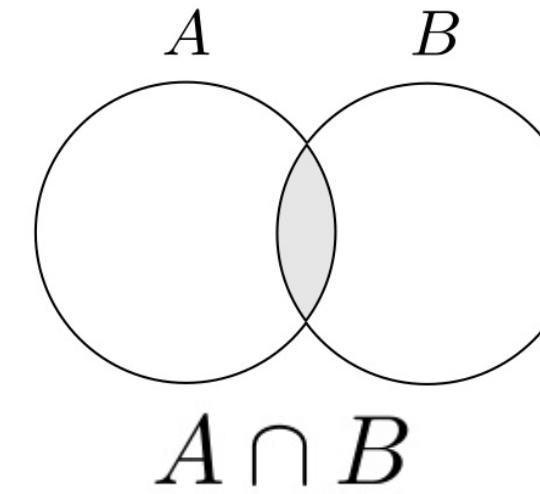
$$B \supsetneq A$$

- Complemento: \overline{A}

Revisão de matemática e terminologia

Conjunto:

→ União e intersecção



Revisão de matemática e terminologia

Conjunto:

→ **Produto cartesiano**

$$A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\}$$

$$\overbrace{A \times A \times \cdots \times A}^k = A^k$$

→ **Número de elementos, número de subconjuntos, power set**

$$n(A) \quad 2^{n(A)} \quad \wp(A)$$

→ **Conjunto vazio; conjunto unitário**

$$\emptyset \text{ ou } \{ \}$$

Revisão de matemática e terminologia

Seqüência:

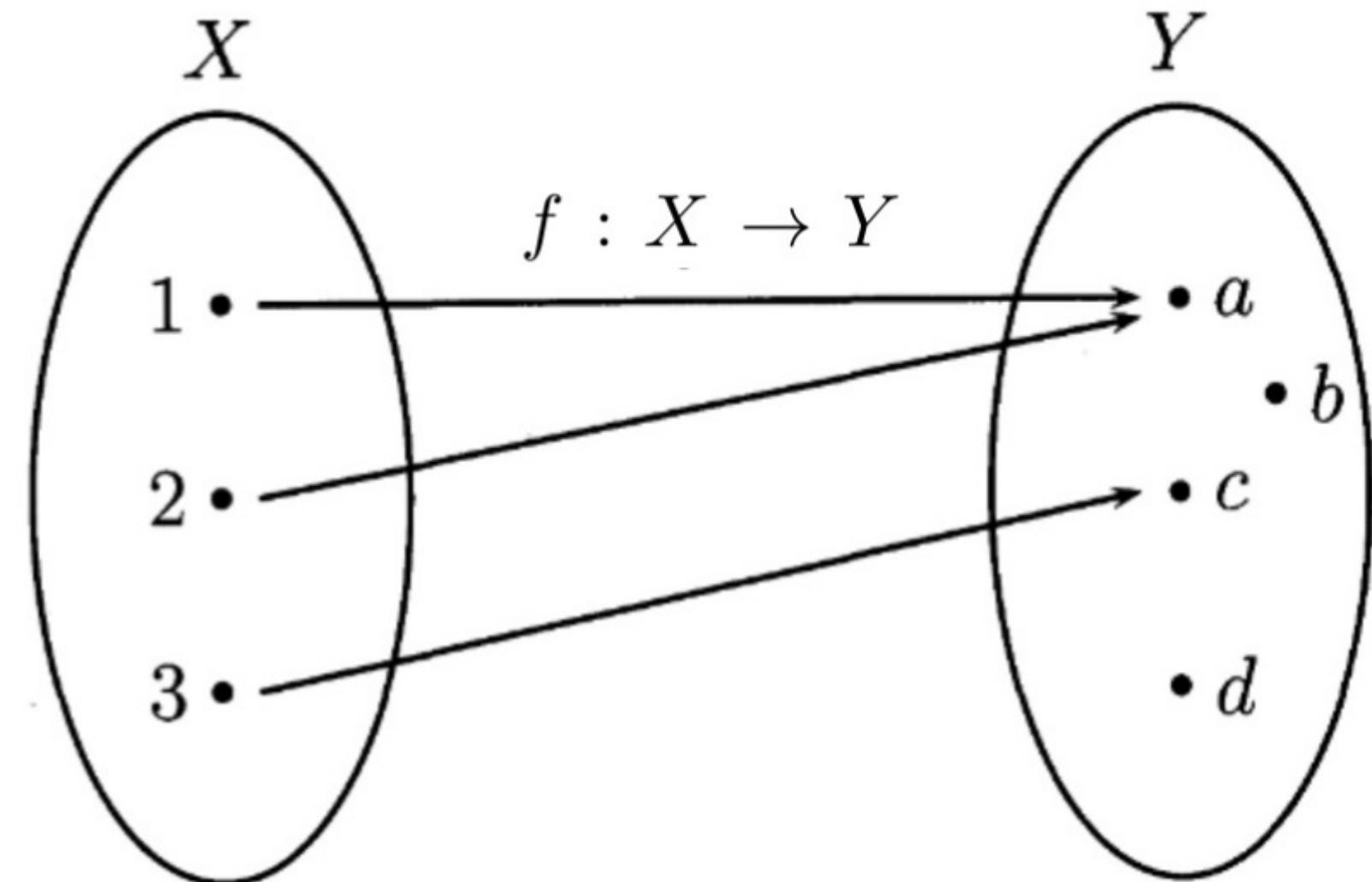
- Uma lista de objetos em uma ordem especificada.
- Seqüências finitas são chamadas de tuplas.
- Uma seqüencia com k elementos é uma k-tupla.
- Uma seqüência com 2 elementos é um par ordenado.

Revisão de matemática e terminologia

Função:

→ É uma **regra** que **associa** a cada elemento de um conjunto X um único elemento de um conjunto Y. Todos os elementos de X devem estar associados a um único elemento de Y

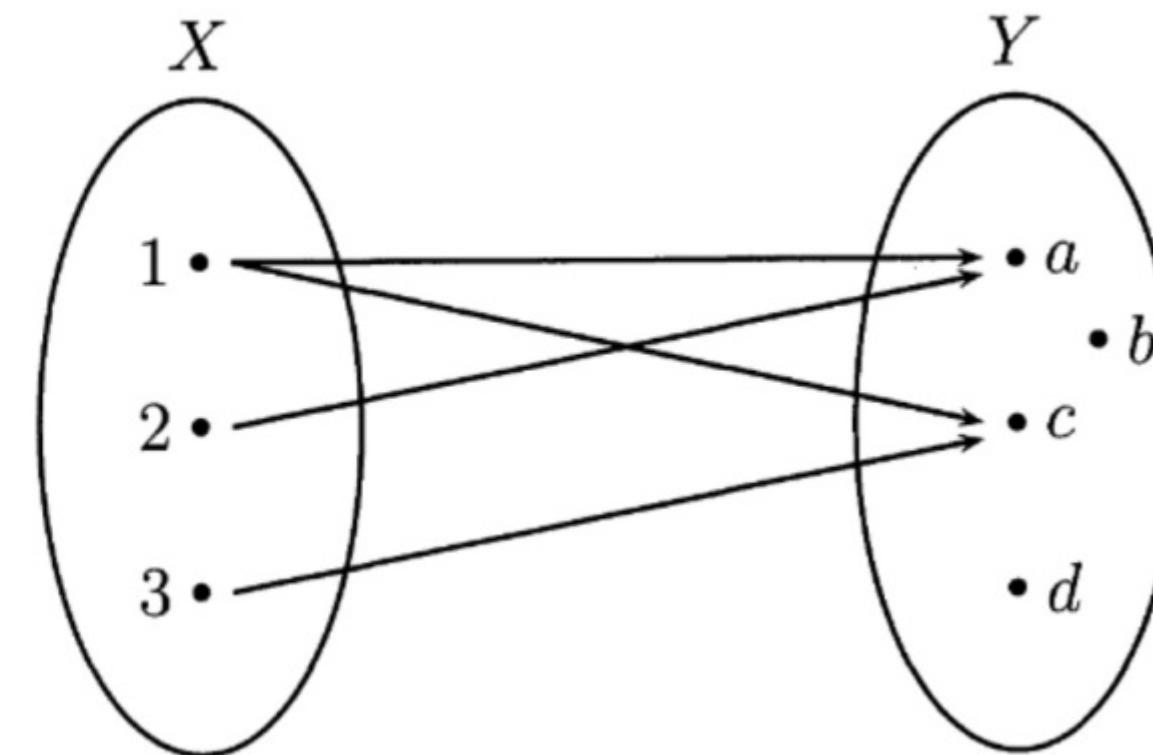
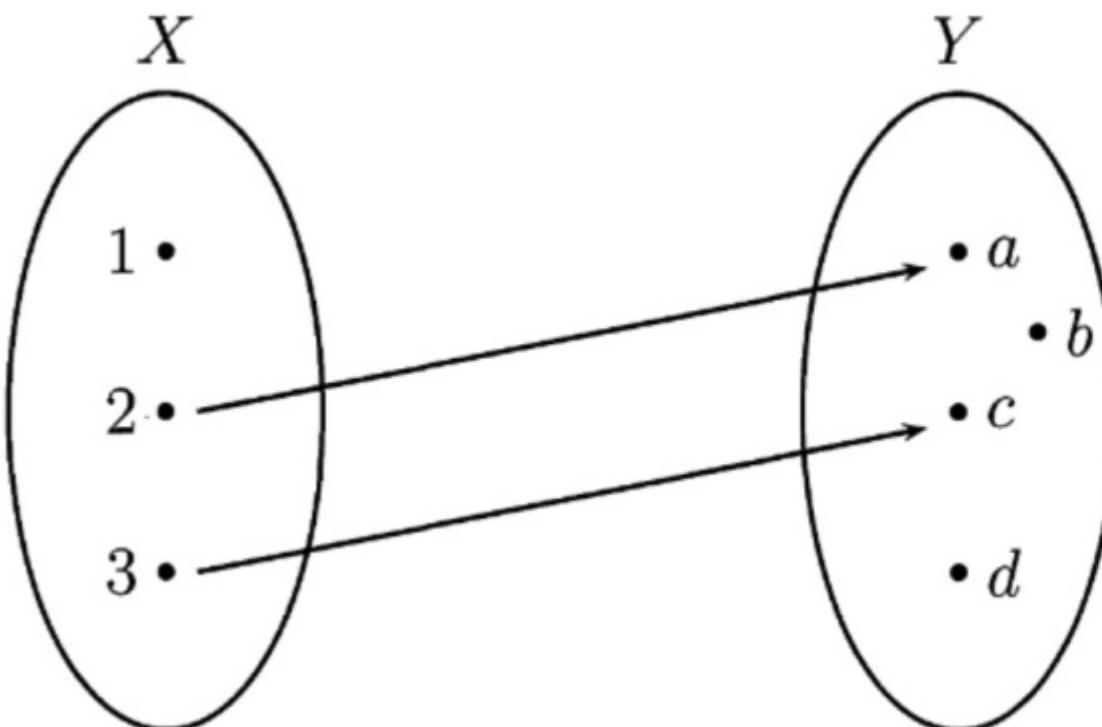
$$f : X \rightarrow Y$$



Revisão de matemática e terminologia

Função:

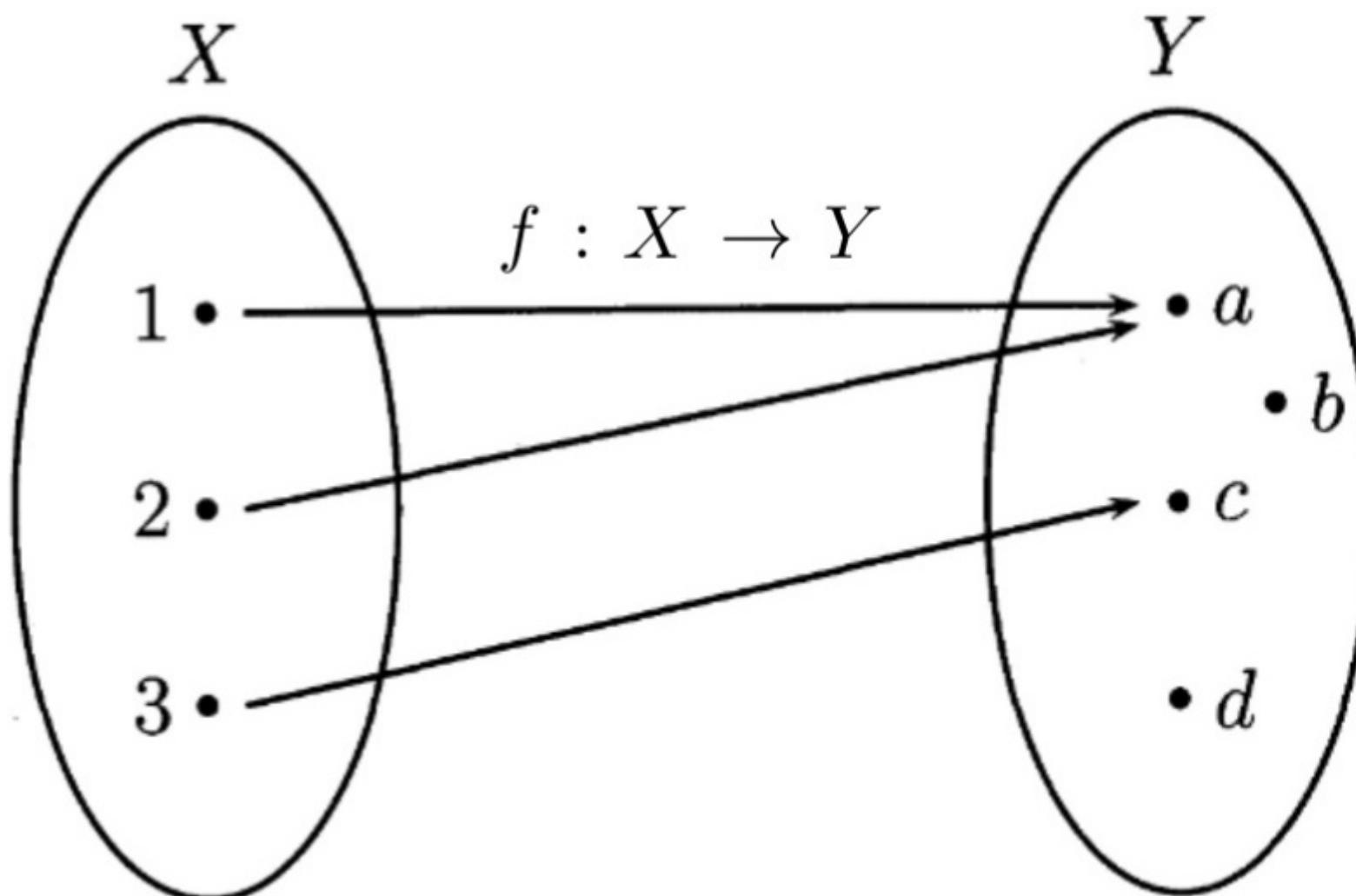
→ Se algum elemento de X não estiver associado a um elemento de Y, ou se um elemento de X estiver associado a mais de um elemento de Y, não temos uma função.



Revisão de matemática e terminologia

Função:

→ O domínio de uma função são os valores de X para os quais as operações indicadas pela regra da função são possíveis. O domínio não inclui os valores de X para os quais as operações indicadas pela regra da função não são possíveis.

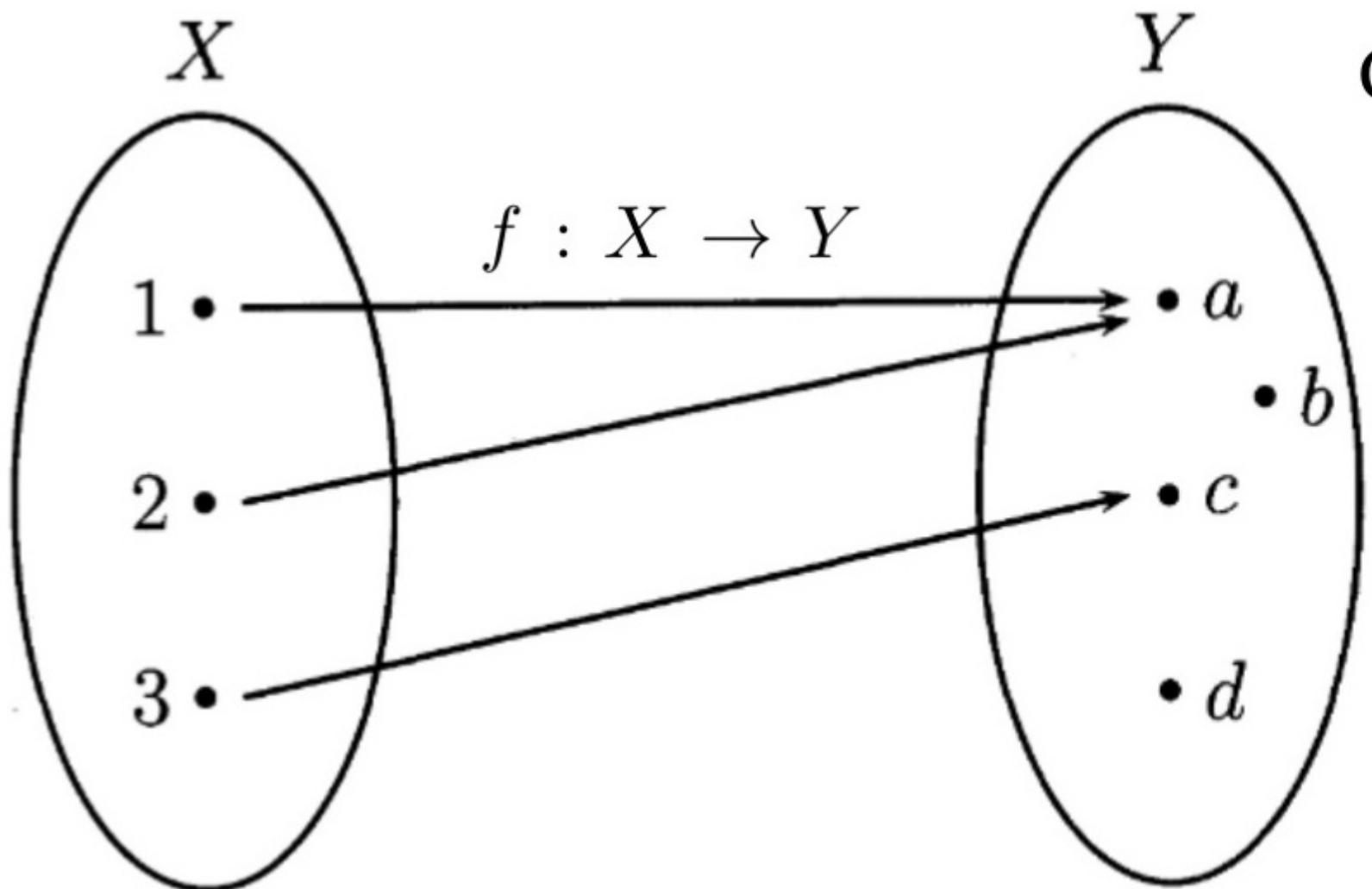


Domínio da função: $X = \{1, 2, 3\}$

Revisão de matemática e terminologia

Função:

→ O **contradomínio** de uma função são **todos os valores possíveis de Y**. O contradomínio corresponde a tudo o que a função pode produzir como saída.

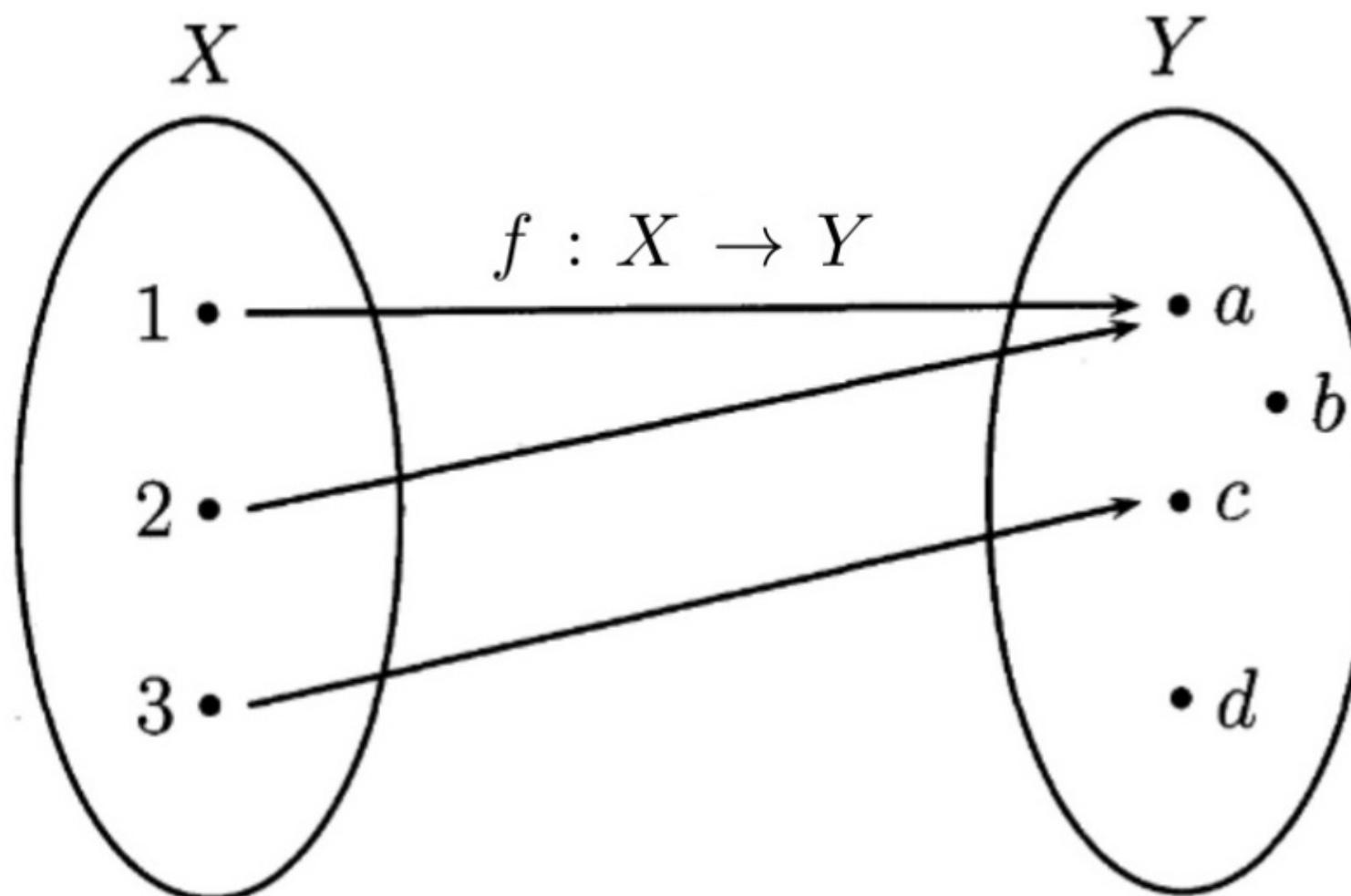


Contradomínio da função: $Y = \{a, b, c, d\}$

Revisão de matemática e terminologia

Função:

→ Uma **imagem** corresponde a um **valor específico de y** que está **associado a um valor de x** pela regra da função. Se x é um elemento de X, o único y de Y associado à x é denominado de **imagem de x pela função f**.



$$y = f(x)$$

Imagen de 1: $y = f(1) = a$

Imagen de 2: $y = f(2) = b$

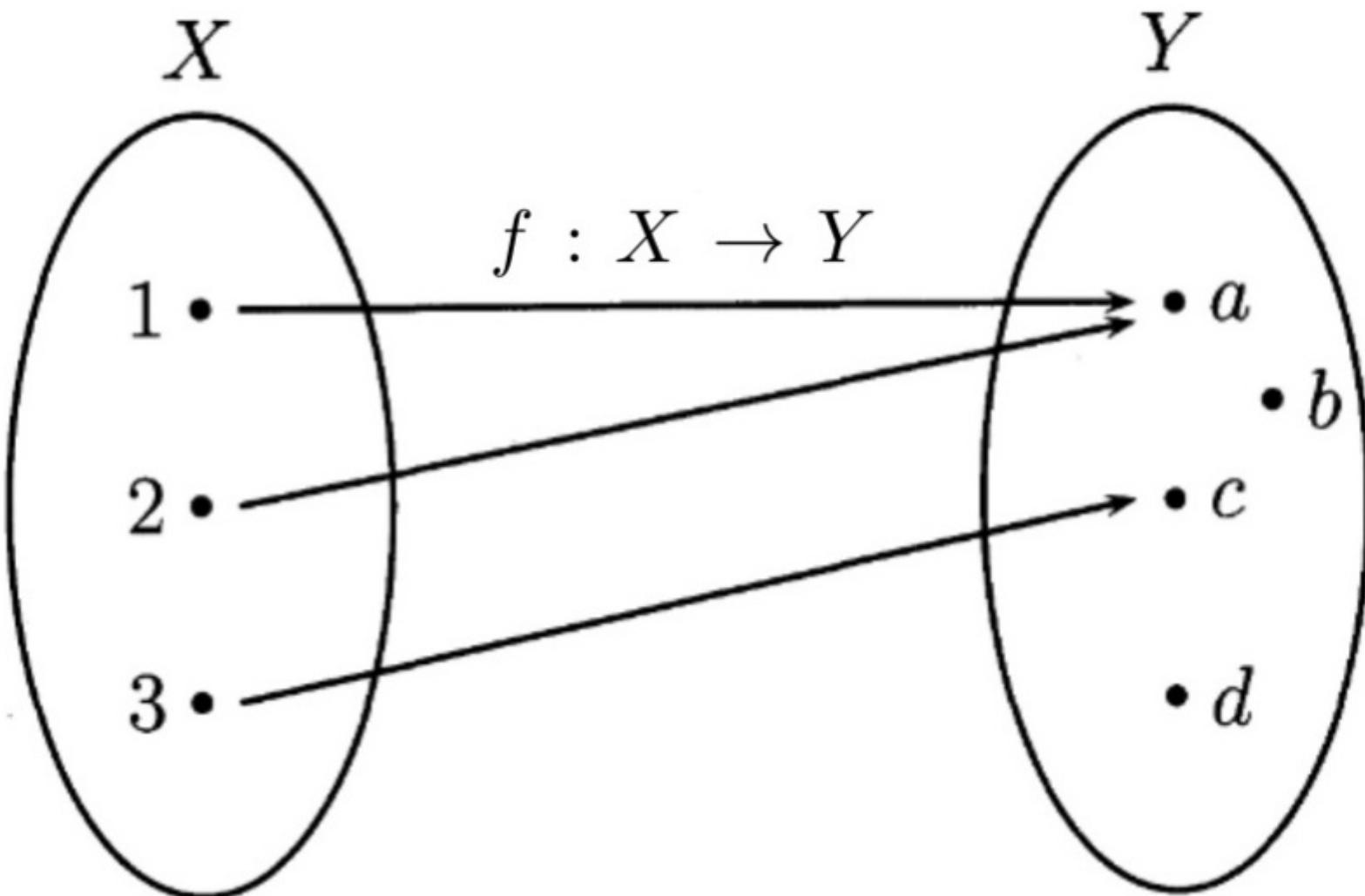
Imagen de 3: $y = f(3) = c$

Revisão de matemática e terminologia

Função:

→ O **conjunto imagem** corresponde ao **conjunto de todas as imagens** obtidas pela função.

$$y = f(x)$$



Conjunto imagem da função: $\{a, c\}$

$$\text{Im}(f) \subseteq Y$$

Revisão de matemática e terminologia

Função:

→ Maneiras de descrever um função:

- fórmula
- tabela de mapeamento
- gráfico
- verbalmente

→ Quando o domínio de uma função f é dado por $A_1 \times A_2 \times \dots \times A_k$ para alguns conjuntos A_1, A_2, \dots, A_k , o input da função é a k-tupla (a_1, a_2, \dots, a_k) e nós chamamos os a_i de argumentos da função.

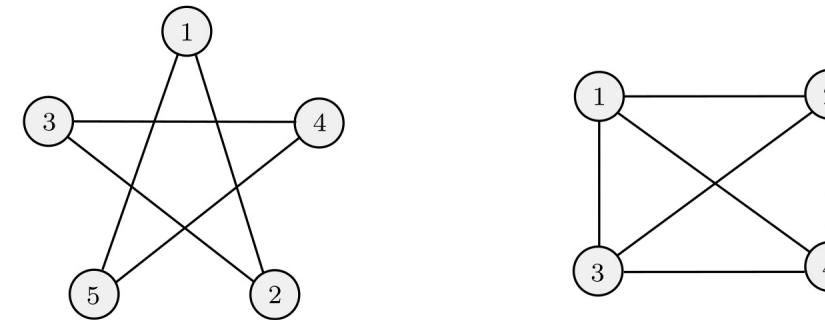
→ Uma função com k argumentos é chamada de **k-ária**, e k é a **aridade** da função.
Se k = 1 a função é unária; se k = 2 a função é binária.

→ Um **predicado** é uma função cujo contradomínio é TRUE ou FALSE.

Revisão de matemática e terminologia

Grafos:

→ Um **grafo não dirigido** (ou simplesmente **grafo**) é um conjunto de pontos (chamados de **nós** ou **vértices**) com linhas (**arestas**) que conectam alguns desses pontos.



→ O número de arestas em um nó é chamado de **grau** desse nó. Não pode existir mais do que uma aresta entre dois nós (mas pode existir uma aresta que liga o nó nele mesmo).

→ Em um grafo **G** que contém os nós **i** e **j**, o par **(i, j)** representa a aresta que conecta esses nós. A ordem não importa em um grafo não dirigido.

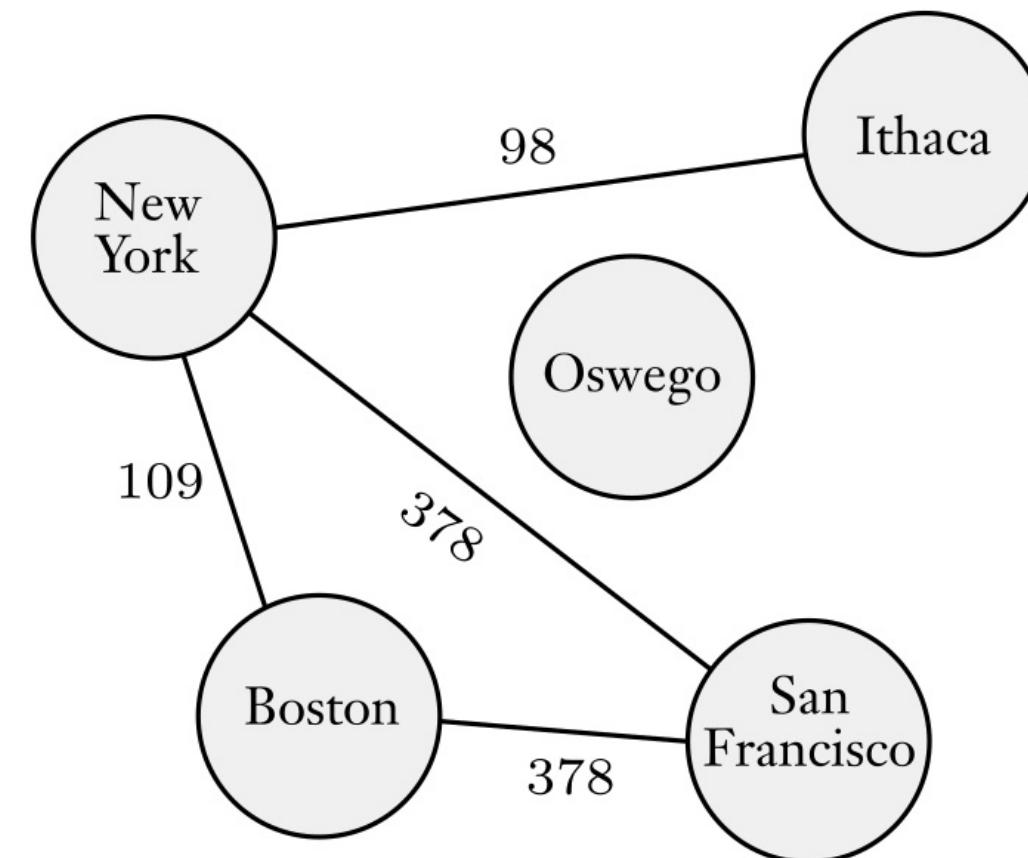
→ Se **V** é o conjunto de nós de **G**, e **E** é o conjunto de arestas, dizemos que **G = (V, E)**. Um grafo é descrito por um diagrama ou pela especificação de **V** e **E**:

$$(\{1, 2, 3, 4, 5\}, \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 1)\})$$

Revisão de matemática e terminologia

Grafos:

- São usados para representar dados.
- Se tiverem nomes associados são chamados de grafos nomeados, etiquetados, identificados ou **rotulados**.

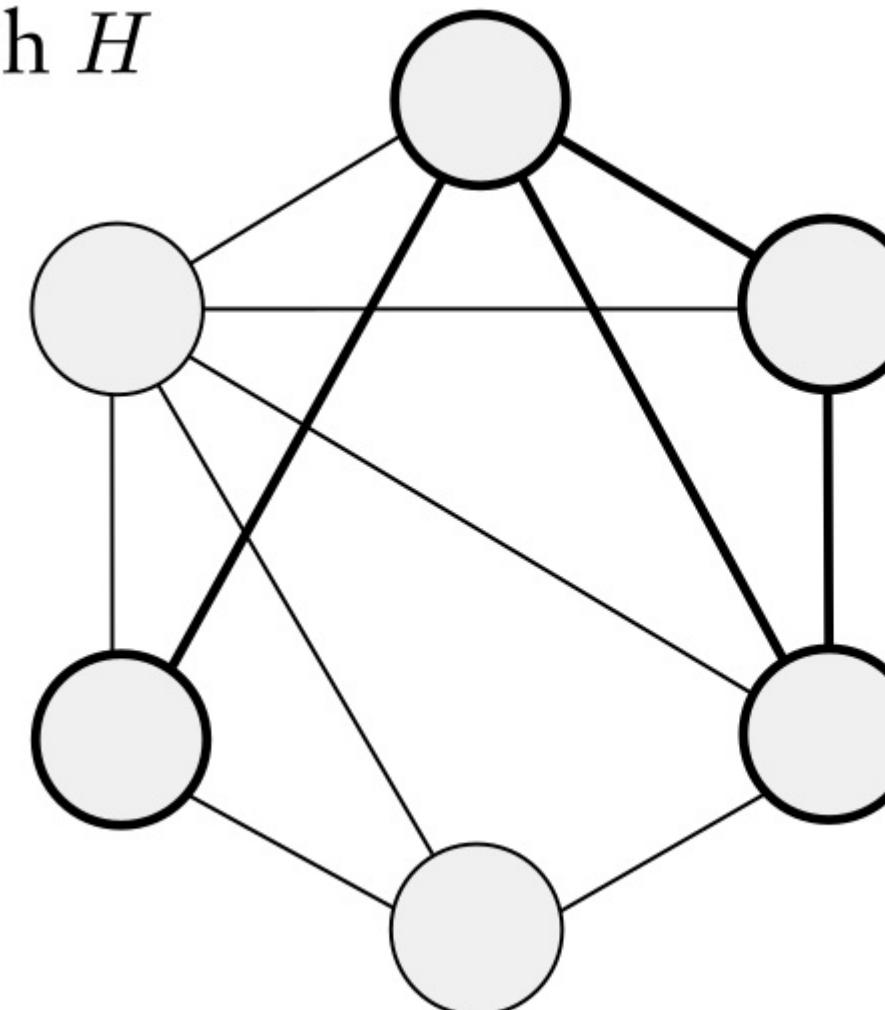


Revisão de matemática e terminologia

Grafos:

→ Um grafo G é um **subgrafo** de um grafo H se os nós de G forem um subconjunto dos nós de H , e as arestas de G são as arestas de H nos nós correspondentes.

Graph H

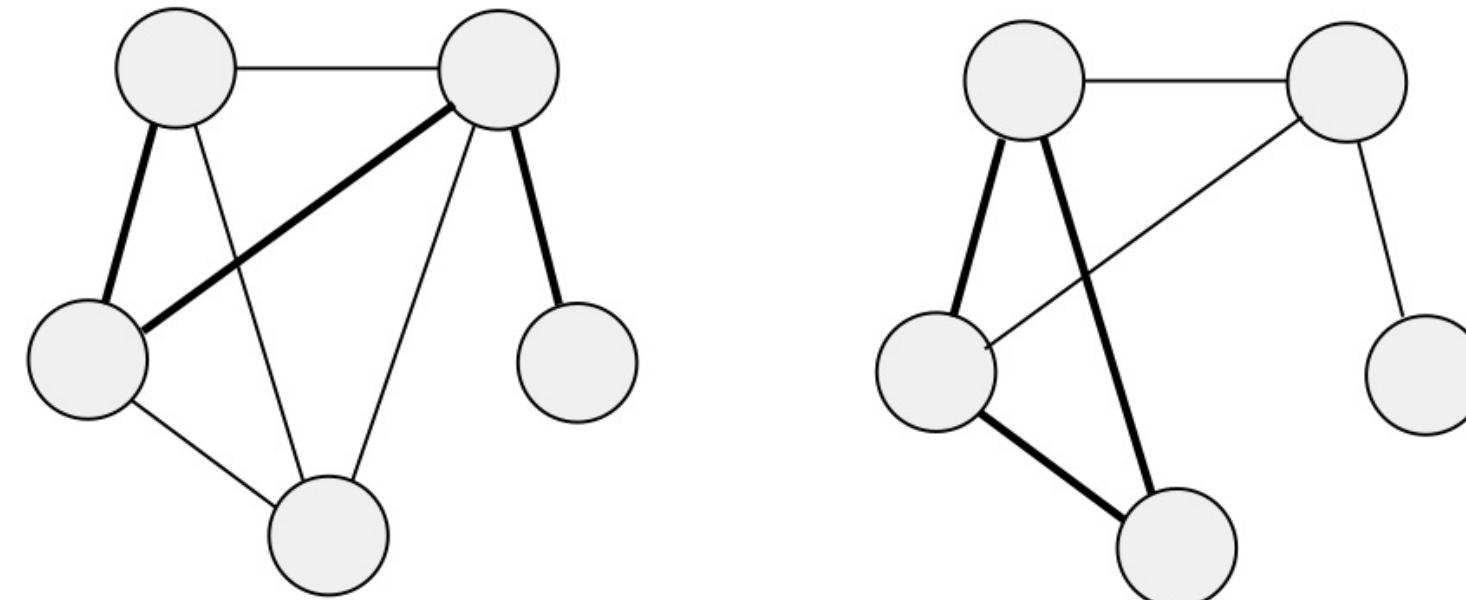


Subgraph G
shown darker

Revisão de matemática e terminologia

Grafos:

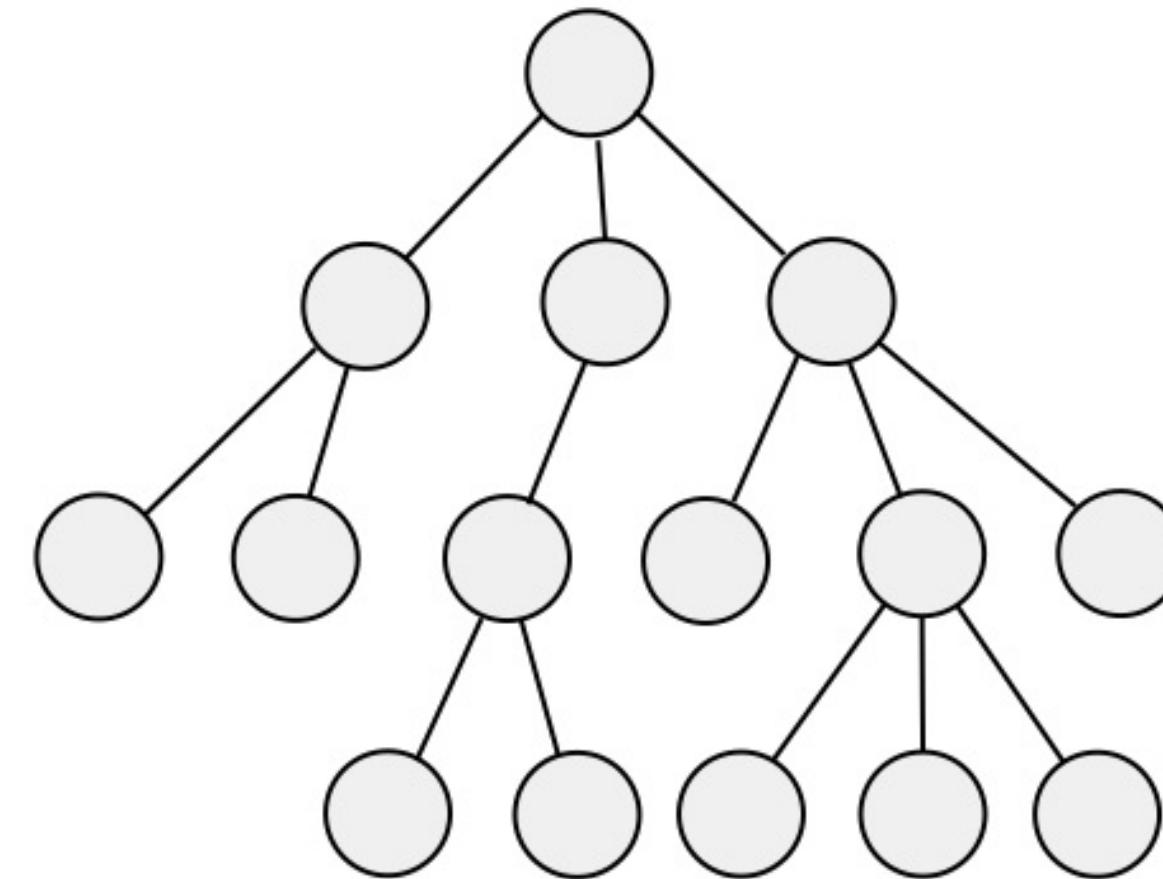
- Um **caminho** em um grafo é uma **seqüência de nós conectados por arestas**. Se não houver nós repetidos, o caminho é dito **simples**.
- Um grafo é **conexo** se existir um caminho entre todos os pares de vértices. Obs.: não é necessário que um vértice seja conectado a todos os outros!
- Um caminho é **cíclico** se começar e terminar no mesmo nó. Um **ciclo simples** é aquele que contém pelo menos três nós e repete apenas o primeiro e o último.



Revisão de matemática e terminologia

Grafos:

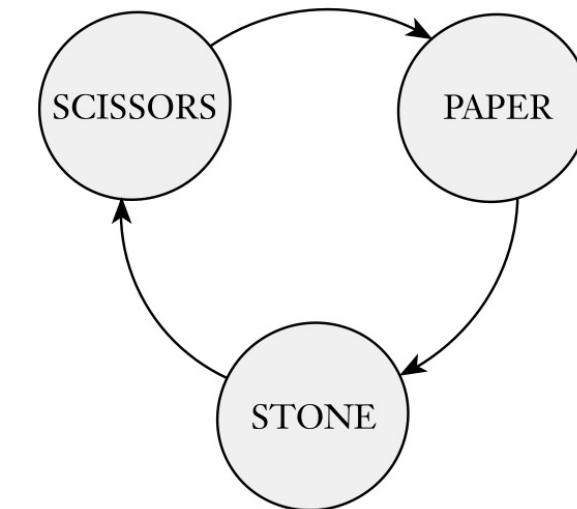
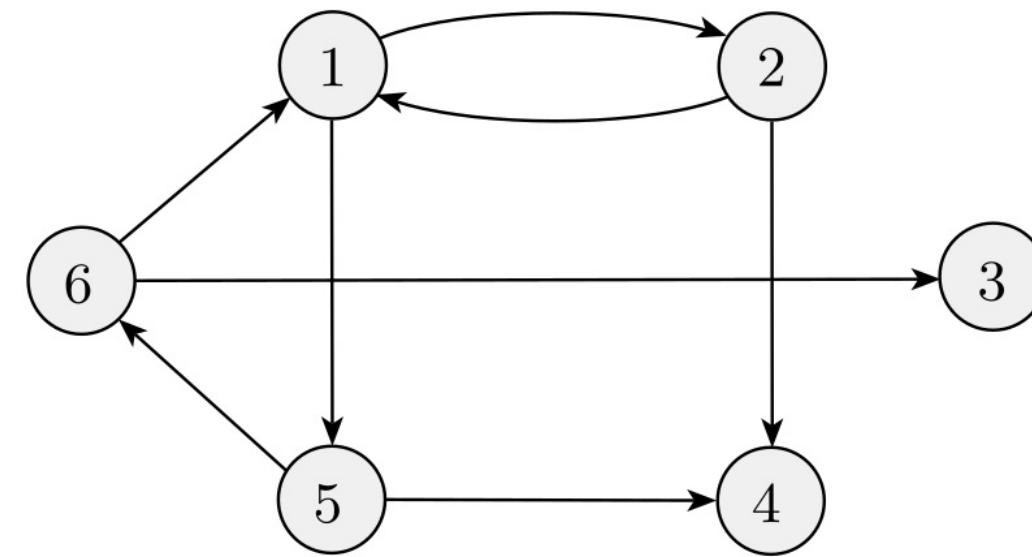
→ Um grafo é uma **árvore** se for **conexo** e **não tiver ciclos simples**. Um nó especial, de grau 1, pode existir e ser chamado de **raiz** da árvore. Os outros nós da árvore que tiverem grau 1, exceto a raiz, são chamados de **folhas**.



Revisão de matemática e terminologia

Grafos:

→ Um grafo é dito **dirigido** se arestas diverem uma direção.



→ O número de arestas que saem de um nó é o **grau de saída** desse nó.

→ O número de arestas que chegam em um nó é o **grau de entrada** desse nó.

→ Um grafo dirigido é **fortemente conexo** se existir um caminho entre qualquer par de nós em ambas as direções, tal que cada nó é alcançável a partir de qualquer outro.

Revisão de matemática e terminologia

Strings e linguagens:

→ Um **alfabeto** é qualquer conjunto finito não vazio. Geralmente usamos as letras gregas maiúsculas Sigma (Σ) e Gamma (Γ) para representar um alfabeto.

$$\Sigma_1 = \{0,1\}$$

$$\Sigma_2 = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$$

$$\Gamma = \{0, 1, x, y, z\}$$

→ Os membros que pertencem a um alfabeto são seus **símbolos**.

→ Uma **string sobre um alfabeto** é uma seqüência de símbolos desse alfabeto, escritos um após o outro, não separados por vírgulas.

01001

abracadabra

Revisão de matemática e terminologia

Strings e linguagens:

- Se W é uma string sobre Σ , o **comprimento** de W é escrito $|w|$ e corresponde ao número de símbolos que essa string contém.
- A string de comprimento zero é chamada de **string vazia** e representada por \mathcal{E} .
- Se W tem comprimento n , então $w = w_1 w_2 \cdots w_n$ para cada $w_i \in \Sigma$.
- O **reverso** de W , representado por w^R , é $w_n w_{n-1} \cdots w_1$.
- A string Z é **substring** de W se aparecer consecutivamente dentro de W .
- Se uma string X de comprimento m e uma string Y de comprimento n forem concatenadas, a **concatenação** de X e Y é escrita como XY e é obtida colocando a string Y ao final de X :

$$x_1 \cdots x_m y_1 \cdots y_n$$

Revisão de matemática e terminologia

Strings e linguagens:

→ Para concatenar uma string com ela mesma muitas vezes, usamos a notação x^k :

$$\overbrace{xx \cdots x}^k$$

→ A ordem **lexicográfica** de uma string é a mesma ordem do dicionário. Usaremos também a **shortlex order** (ordenação radix, lexicográfica por comprimento, militar, genealógica), que é idêntica à lexicográfica mas com strings menores em primeiro lugar:

$$\Sigma_1 = \{0, 1\} \quad (\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots)$$

→ Uma **linguagem** é um conjunto de strings de um alfabeto.

Revisão de matemática e terminologia

Lógica Booleana:

→ AND, OR, NOT:

$$0 \wedge 0 = 0$$

$$0 \wedge 1 = 0$$

$$1 \wedge 0 = 0$$

$$1 \wedge 1 = 1$$

$$0 \vee 0 = 0$$

$$0 \vee 1 = 1$$

$$1 \vee 0 = 1$$

$$1 \vee 1 = 1$$

$$\neg 0 = 1$$

$$\neg 1 = 0$$

→ XOR, equivalência, implicação:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

$$0 \leftrightarrow 0 = 1$$

$$0 \leftrightarrow 1 = 0$$

$$1 \leftrightarrow 0 = 0$$

$$1 \leftrightarrow 1 = 1$$

$$0 \rightarrow 0 = 1$$

$$0 \rightarrow 1 = 1$$

$$1 \rightarrow 0 = 0$$

$$1 \rightarrow 1 = 1$$

→ Relacionamentos:

$$P \vee Q$$

$$\neg(\neg P \wedge \neg Q)$$

$$P \rightarrow Q$$

$$\neg P \vee Q$$

$$P \leftrightarrow Q$$

$$(P \rightarrow Q) \wedge (Q \rightarrow P)$$

$$P \oplus Q$$

$$\neg(P \leftrightarrow Q)$$

→ Distributividade: $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$

$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

Definições, teoremas e provas

Definições:

→ Descrevem os objetos e notações que usamos. Deve ser matematicamente precisa.

Sentenças matemáticas:

→ Sentenças matemáticas sobre um objeto expressam que algum objeto tem alguma propriedade. A sentença pode ou não ser verdadeira, mas deve ser precisa.

Prova:

→ É um argumento lógico-matemático de que uma sentença matemática é verdadeira, sem qualquer dúvida ou possibilidade de dúvida.

Teorema:

→ É uma sentença matemática importante e significativa que foi provada ser verdadeira.

Lema:

→ É uma sentença menos importante que foi provada apenas como auxílio na prova de uma outra sentença mais importante e significativa.

Corolário:

→ Sentença facilmente deduzida como verdadeira a partir de um teorema.

Definições, teoremas e provas

Encontrar provas:

→ É difícil

→ Seja paciente

→ Volte ao problema várias vezes

→ Seja simples

→ Seja conciso

Definições, teoremas e provas

Tipos de provas:

- **Construção:** muitos teoremas afirmam que um tipo particular de objeto existe. Uma maneira de provar isso é demonstrar como construir um objeto.
- **Contradição:** assumimos que um teorema é falso e, então, tentamos demonstrar que esse pressuposto é falso, ou seja, achamos uma contradição ao nosso pressuposto inicial de que o teorema é falso e, portanto, o teorema é verdadeiro.
- **Indução:** demonstramos que todos os elementos de um conjunto infinito tem uma propriedade específica.

Seminários de hoje!

Chega de teoria por hoje. Vamos aos seminários preparados pelos grupos!