UFSC - CTC - INE
INE5403 - FUNDAMENTOS DE MATEMÁTICA DISCRETA PARA A COMPUTAÇÃO

NOTAS DE AULA COMPLETAS

NOTA: Este material foi elaborado com base, principalmente, nas seguintes referências:
* Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl,5ed, 2003.
* Rosen, "Discrete Mathematics and its Aplications", 6 ed., McGraw-Hill, 2007.
* Cormen, Leiserson, Rivest, Stein, "Introduction to Algorithms", 2 ed., MIT Press, 2001.

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

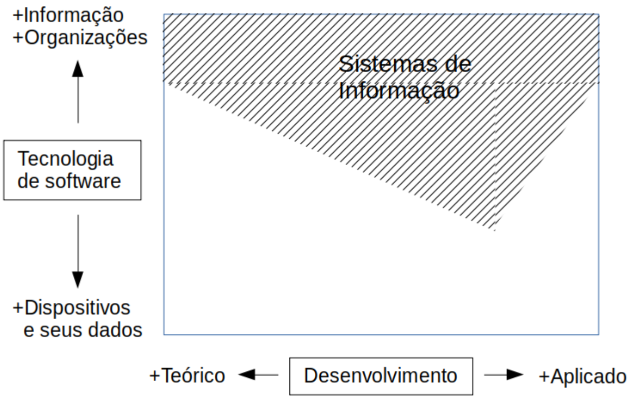
1) Introdução

ACM/IEEE definem 5 áreas na Computação:

- Tecnologia da informática
- Sistemas de Informação
- Engenharia de Software
- Engenharia de Computação
- *Ciência da Computação*

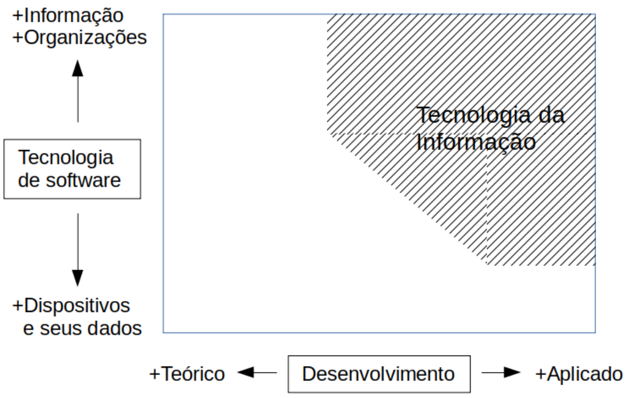
1) Sistemas de Informação:

- Ênfase em integrar soluções de TI com negócios
- Importam tanto fatores técnicos como organizacionais
- Tecnologia: instrumento para facilitar fluxo de informação
- Processamento tecnológico de informações como vantagem competitiva para as organizações
- Requisitos, especificação, projeto e implementação de um sistema de informação para uma empresa



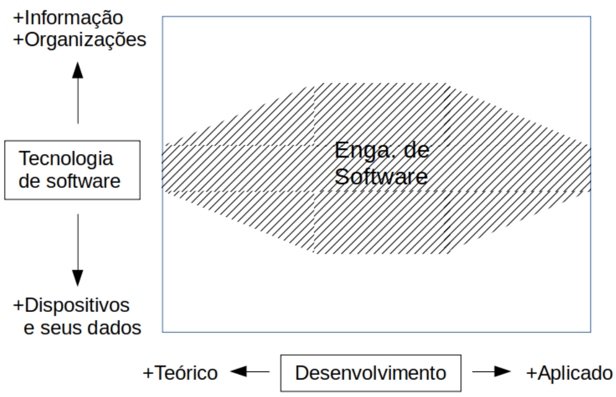
2) Tecnologia da Informática (TI):

- Foco mais na tecnologia em si do que na informação associada
- Conhecimento técnico e habilidades práticas:
  - suporte para qualquer problema relacionado a computadores
  - cuida tanto da infra-estrutura como das pessoas que a usam
- Lida com hardware e software:
  - seleciona, integra, instala, adapta, faz manutenção
  - funcionamento correto, segurança
  - upgrades, substituição, renovação



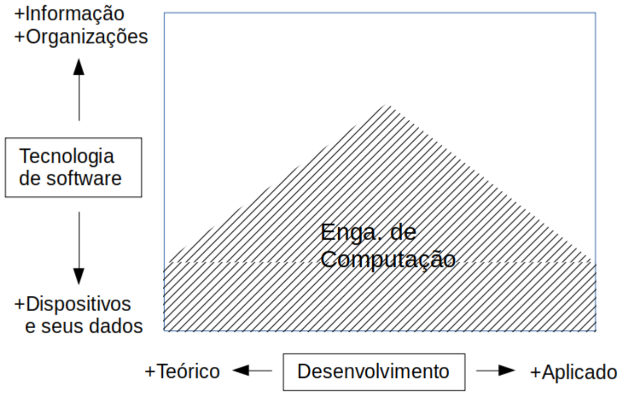
3) <u>Engenharia de software</u>:

- Preocupa-se com necessidades de clientes e desenvolve software para isto
- Lida com desenvolvimento de sistemas de software que:
  - se comportam de maneira confiável e eficiente
  - são fáceis de manter e de melhorar
  - satisfazem requisitos definidos pelos clientes
- Foco: técnicas para desenvolvimento de software que seja correto desde a sua concepção inicial



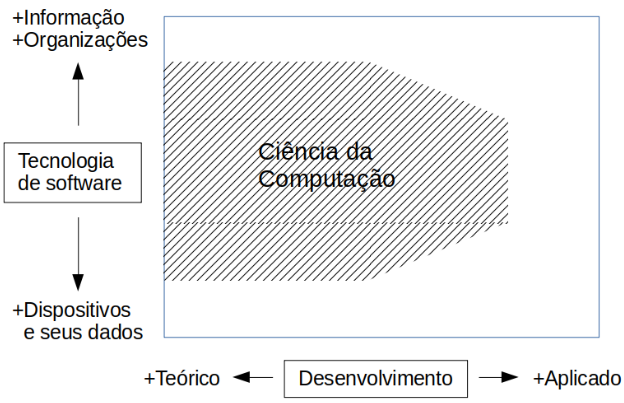
4) <u>Engenharia de Computação</u>:

- Projeto e construção de computadores e dispositivos que contêm computadores
- Projeta software para dispositivos digitais e suas interfaces
- Estuda HW, SW, sistemas de comunicação e suas interações
- Exemplos de aplicações: chips de computadores, celulares, reprodutores de áudio e gravadores de vídeos digitais, máquinas de raio-X, ferramentas cirúrgicas a laser, ...



5) Ciência da Computação:

- Vai desde a análise de um problema até a programação
- Estuda desde fundamentos teóricos até últimos avanços em robótica, visão computacional, sistemas inteligentes
  - sólida FUNDAMENTAÇÃO TEÓRICA facilita adaptação a novas ideias
- Foco: formas efetivas de resolver problemas computacionais
  - conhecimento de algoritmos usado para buscar desempenho ótimo
  - exs.: melhor forma de armazenar informação, enviar dados em redes, exibir imagens complexas
- Também lida com novas formas de usar computadores para:
  - tornar robôs mais inteligentes
  - transformar grandes volumes de dados em conhecimento novo
  - decifrar os segredos do nosso DNA
  - implementar criptografia forte



Ciência da Computação

- Problemas "pesados": trabalho nos limites da Computação

  Exemplo: fatorar $n = p \times q$ aonde p e q são primos com mais de 600 dígitos decimais...
- Palavras-chave: Abstração, eficiência, otimização, prova
- De uma lista de discussões do Massachusetts Institute of Technology (MIT):

  "Começa-se no MIT lidando com complexidade e abstração, e avança-se para o estudo de arquitetura de computadores (=como projetar computadores), IA, modelagem e teoria. (...)"

  "Tem uma boa quantidade de matemática avançada. (...)"

  "CC estuda como tornar os computadores mais rápidos, mais eficientes e mais inteligentes. (...)"
- Comentário atribuído a Edsger Dijkstra:

  "CC tem tanto a ver com computadores quanto a astronomia com telescópios"...

Matemática & CC

- Matemática: suporte para a modelagem de problemas
- Estruturas convenientes para resolver problemas
- "Linguagem" natural para expressar fatos científicos
- Dois "tipos" de Matemática relevantes para a CC: contínua e discreta

Matemática Contínua & CC

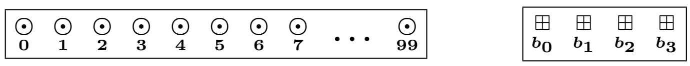
- Matemática Contínua: ligada ao Cálculo Infinitesimal
- Ligada à modelagem de fenômenos da Física
- Fundamentos: Análise Numérica

Matemática Discreta & CC

- Matemática Discreta: ligada a processos não contínuos (= "discretos")
  - realizados passo-a-passo
  - interessam apenas os "estados" de um sistema
  - e não os detalhes da "transição" entre eles
- Ferramentas típicas: indução e recursão
- Principal aplicação na CC: suporte teórico para algoritmos discretos

- **Ex.**: **Problema Combinatorial** *(adaptado de "Party Lamps", IOI-1998)*

  Você tem 100 lâmpadas acesas e 4 botões:



  b_0 muda o estado de todas as lâmpadas (acesa $\leftrightarrow$ apagada),

  b_1 muda só as lâmpadas pares,

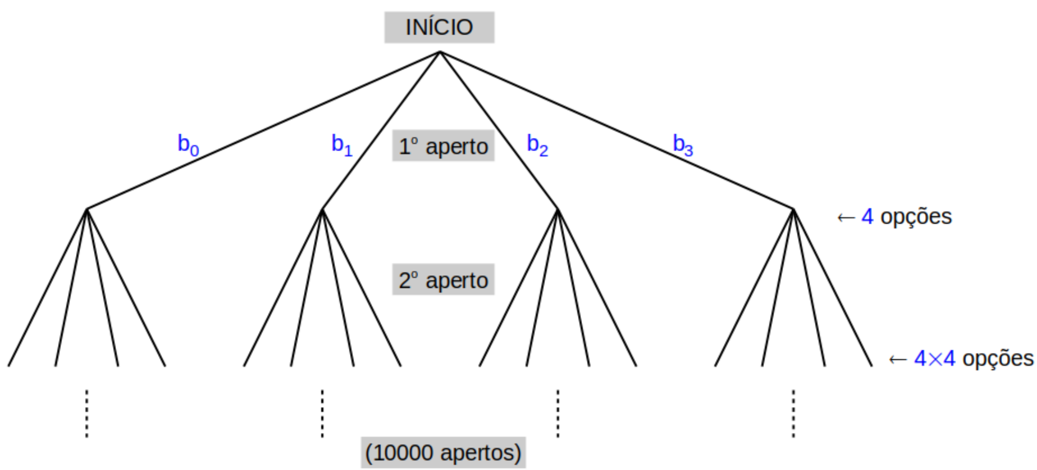
  b_2 muda só as lâmpadas ímpares e

  b_3 muda as lâmpadas $0, 3, 6, 9, \ldots$

  Problema: Dado o número n de apertos de botão ($n \leq 10000$) ,
  liste todos os possíveis estados finais das lâmpadas.

  - Possível sequência de apertos: $[b_2 b_3 b_0 b_2 b_3 b_1 b_2 b_2 \ldots b_1 b_1]$

  1) "**Ingenuamente**": para cada aperto de botão, 4 possibilidades:



  $*$ Lista final poderia chegar a: $4^{10000} \simeq 10^{6020}$ saídas (!!)

∗ MAS: estado final das lâmpadas não depende da ordem dos apertos

  · Efeito de um botão só depende da posição da lâmpada
  · Efeitos possíveis: "mudar de estado" ou "não mudar"

∗ Contribuição de cada aperto para o estado final de uma dada lâmpada independe do momento em que o aperto ocorreu

  · Ex.: $[b_2 b_1 b_0 b_3]$ e $[b_1 b_3 b_2 b_0]$ têm mesmo efeito sobre a #6 (vale para as outras lâmpadas)

∗ LOGO: pode ser visto como "combinações com repetição"...

2) **Usando MD**: problema de "combinações com repetição"

∗ Cada estado final corresponde a uma maneira de escolher (até) 10000 itens a partir de (apenas) 4 possibilidades

$$\overbrace{b_0 b_0 b_0 b_1 b_1 b_2 b_2 b_2 \ldots b_3 b_3}^{10000\ \textit{escolhas a partir de}\ \{b_0,b_1,b_2,b_3\}}$$

∗ O que pode ser feito de: *(ver cap. 8)*

$\binom{10000+3}{3} = \frac{10003 \times 10002 \times 10001}{3 \times 2 \times 1} \sim 10^{12}$ maneiras diferentes

∗ Redução por um fator $> 10^{6000}$ (!)

3) **Usando (mais) MD**:

∗ Note que, independente da posição da lâmpada, os efeitos de dois apertos do mesmo botão se anulam!

  · Ex.: $[b_0 b_0]$ faz todas as lâmpadas mudarem seu estado e logo depois faz todas elas voltarem atrás

∗ Dada uma sequência de apertos, *só precisamos saber se*:

  · o número de apertos de cada botão foi par ou ímpar
  · (lembre que a ordem dos apertos é irrelevante)

∗ Ou seja, na verdade, independente do tamanho da sequência de apertos, só existem $2^4 = 16$ saídas possíveis... $\square$

– EFEITO DA MD NESTE EXEMPLO: $\boxed{10^{6020} \longrightarrow 10^{12} \longrightarrow 16}$

Este curso

Um pouco sobre alguns elementos da Matemática Discreta relevantes para o estudo da CC:

- Provas (demonstrações) matemáticas
- Indução e Recursão
- Relações (entre conjuntos) e Funções
- Contagem de Conjuntos
- Noções elementares de Álgebra Abstrata
- Números Inteiros

Essencialmente: PROVAS, TEORIA, ABSTRAÇÃO

Regras deste curso (Administrivia)

- Metodologia: discussões em aula + **exercícios**

- Página da disciplina: `https://www.moodle.ufsc.br/`
  - cronograma estimado
  - notas de aula + listas de exercícios + videoaulas
  - avaliações e resultados

- Este curso foi elaborado com base, principalmente, nas seguintes referências:
  1. Kolman, Busby, Ross, Discrete Mathematical Structures, Prentice-Hall Intl. Eds, 5^{th} ed., 2003.
  2. Rosen, Discrete Mathematics and its Aplications, 6^{th} ed., McGraw-Hill, 2007.
  3. Cormen, Leiserson, Rivest, Stein, Introduction to Algorithms, 2^{nd} ed., MIT Press, 2001.

- Outras fontes ricas em ilustrações do uso da MD pela CC:
  - Olimpíada Brasileira de Informática (OBI):
    https://olimpiada.ic.unicamp.br/
  - Olimpíada Brasileira de Matemática (OBM):
    https://www.obm.org.br/
  - Olimpíada Brasileira de MTM para as Escolas Públicas (OBMEP):
    http://www.obmep.org.br/
  - Olimpíada Regional de Matemática (ORM) (mantida pela UFSC):
    http://orm.mtm.ufsc.br/

- Foco deste curso:
  - MD como suporte ao lado mais desafiador da CC:
    o lado relacionado a ALGORITMOS
  - Espera-se que este enfoque possa torná-lo interessante
    e divertido...

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

2) Métodos de Prova

2.1) Proposições

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Lógica Formal

Lógica: lida com métodos de raciocínio

- Regras e técnicas para determinar se argumento dado é válido

Aplicações diretas:

- Construção e verificação de programas
- Demonstração de correção de algoritmos
- Desenvolvimento de Inteligência Artificial
- Verificação de segurança de sistemas computacionais

Proposições Lógicas

Asserção: uma declaração (afirmação, sentença declarativa).
Proposição: uma asserção que é verdadeira (V) ou falsa (F), mas não ambos.
Valor verdade: resultado da avaliação de uma proposição (V ou F).

Exemplos:

$2+3=5$ $\rightarrow$ proposição (V)
3 não é um número par. $\rightarrow$ proposição (V)
A Terra é arredondada. $\rightarrow$ proposição (V)
$x > 5$ $\rightarrow$ asserção, mas não proposição
Esta declaração é falsa. $\rightarrow$ asserção, não proposição
Você fala francês? $\rightarrow$ nem asserção, nem proposição
Leia o livro texto. $\rightarrow$ nem asserção, nem proposição

Variáveis Proposicionais

Proposições podem ser denotadas por símbolos

- tais como $\boldsymbol{p, q, r, \ldots}$
- chamados de variáveis proposicionais

Assim, pode-se escrever:

$\boldsymbol{p}$: "O sol está brilhando hoje."

$\boldsymbol{q}$: "2 + 3 = 5"

Proposições Compostas

- Novas proposições podem ser construídas a partir de proposições existentes
  - com o auxílio de operadores lógicos
  - para obter proposições compostas
- A sentença: "Não é verdade que $\boldsymbol{p}$"
  - é uma outra proposição
  - chamada de "negação de $\boldsymbol{p}$"
  - notação: $\neg \boldsymbol{p}$, $\sim \boldsymbol{p}$, $\boldsymbol{not\ p}$

- **Exemplos**:

  $\boldsymbol{p}$ **:** "$\mathbf{2+3>1}$"

  $\neg\boldsymbol{p}$ **:** "$\mathbf{2+3}$ não é maior do que $\mathbf{1}$", (ou "$\mathbf{2+3\leq 1}$")

  $\boldsymbol{q}$ **:** "Hoje é quarta-feira"

  $\neg\boldsymbol{q}$ **:** "Não é verdade que hoje é quarta-feira", ou

  $\neg\boldsymbol{q}$ **:** "Hoje não é quarta-feira"

Tabelas Verdade

Da definição de negação segue que:

- se $\boldsymbol{p}$ é V, então $\neg\boldsymbol{p}$ é F
- se $\boldsymbol{p}$ é F, então $\neg\boldsymbol{p}$ é V

Logo, o valor verdade de $\neg\boldsymbol{p}$, relativo a $\boldsymbol{p}$, é dado por:

Tabela verdade da negação:

$\boldsymbol{p}$	$\neg\boldsymbol{p}$
V	F
F	V

Valores verdade de uma proposição composta em termos dos valores de suas partes componentes.

Conectivos Lógicos

- Operador negação: nova proposição a partir de uma única proposição existente.
- Conectivos: operadores para formar novas proposições a partir de duas ou mais proposições já existentes.

Conjunção (operação "e"):

- Notação: $\boldsymbol{p \wedge q}$, $\boldsymbol{p}$ e $\boldsymbol{q}$, $\boldsymbol{p}$ and $\boldsymbol{q}$
- Definição: (4 possibilidades)

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \wedge q}$
V	V	V
V	F	F
F	V	F
F	F	F

Exemplos de conjunção ($\boldsymbol{p \wedge q}$):

- $\boldsymbol{p}$: "Hoje é terça-feira."

  $\boldsymbol{q}$: "Está chovendo hoje."

  $\boldsymbol{p \wedge q}$: "Hoje é terça-feira **e** está chovendo hoje."

- $\boldsymbol{p}$: "$\mathbf{2 < 3}$"

  $\boldsymbol{q}$: "$\mathbf{-5 > -8}$"

  $\boldsymbol{p \wedge q}$: "$\mathbf{2 < 3}$ **e** $\mathbf{-5 > -8}$"

- $\boldsymbol{p}$: "Está chovendo hoje."

  $\boldsymbol{q}$: $\mathbf{3 < 5}$

  $\boldsymbol{p \wedge q}$: "Está chovendo hoje e $\mathbf{3 < 5}$."

Disjunção (operação "ou inclusivo"):

- Notação: $\boldsymbol{p \vee q}$, $\boldsymbol{p}$ ou $\boldsymbol{q}$, $\boldsymbol{p}$ or $\boldsymbol{q}$
- Definição:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \vee q}$
V	V	V
V	F	V
F	V	V
F	F	F

Exemplos de disjunção ($\boldsymbol{p \vee q}$):

* $\boldsymbol{p}$: "$\mathbf{2}$ é um inteiro positivo."

$\boldsymbol{q}$: "$\sqrt{\mathbf{2}}$ é um número racional."

$\boldsymbol{p \vee q}$: "$\mathbf{2}$ é um inteiro positivo **ou** $\sqrt{\mathbf{2}}$ é um número racional."

* $\boldsymbol{p}$: $\mathbf{2 + 3 \neq 5}$

$\boldsymbol{q}$: "Curitiba é a capital de Santa Catarina."

$\boldsymbol{p \vee q}$: "$\mathbf{2 + 3 \neq 5}$ **ou** Curitiba é a capital de Santa Catarina."

O conectivo “ou” pode ser interpretado de duas maneiras distintas:

- Ou inclusivo (e/ou):
  - “Eu passei em Cálculo **ou** eu rodei em Álgebra Linear.”
    - Pelo menos uma das possibilidades ocorre
    - Mas ambas podem ocorrer
- Ou exclusivo:
  - “Eu vim de carro para a UFSC ou eu vim a pé para a UFSC”
    - Somente uma das possibilidades pode ocorrer

Disjunção exclusiva (operação “xor”):

- Notação: $\boldsymbol{p} \oplus \boldsymbol{q}$, $\boldsymbol{p}$ xor $\boldsymbol{q}$, $\boldsymbol{p}$ ou $\boldsymbol{q}$ (mas não ambos)
- Definição:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p} \oplus \boldsymbol{q}$
V	V	F
V	F	V
F	V	V
F	F	F

(V quando exatamente um dos dois é V)

Condicional ou implicação (se $\boldsymbol{p}$, então $\boldsymbol{q}$):

- Notação: $\boldsymbol{p} \to \boldsymbol{q}$
- Definição:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p} \to \boldsymbol{q}$
V	V	V
V	F	F
F	V	V
F	F	V

Verdadeiro quando:

$\boldsymbol{p}$ e $\boldsymbol{q}$ são ambos V

$\boldsymbol{p}$ é F (não importando $\boldsymbol{q}$)

- Maneiras de expressar $\boldsymbol{p} \to \boldsymbol{q}$:

se $\boldsymbol{p}$, então $\boldsymbol{q}$

$\boldsymbol{p}$ é condição suficiente para $\boldsymbol{q}$

$\boldsymbol{q}$ é condição necessária para $\boldsymbol{p}$

$\boldsymbol{q}$, se $\boldsymbol{p}$

$\boldsymbol{p}$, somente se $\boldsymbol{q}$

$\boldsymbol{q}$ é consequência lógica de $\boldsymbol{p}$

Exemplo: se $\boldsymbol{n \geq 10}$, então $\boldsymbol{n^2 \geq 9}$

Na expressão $\boldsymbol{p \to q}$:

- $\boldsymbol{p}$ é chamado de hipótese ou antecedente
- $\boldsymbol{q}$ é chamado de conclusão ou consequente

Exemplo: "Fogo é uma condição necessária para fumaça":

- Esta sentença pode ser reformulada como: "Se há fumaça, então há fogo"
  - o antecedente (lógico) é: "Há fumaça"
  - o consequente (lógico) é: "Há fogo"

Exemplo: Indique o antecedente e o consequente em:

- "Se a chuva continuar, o rio vai transbordar"
- "Uma condição suficiente para a falha de uma rede é que a chave geral não funcione"
- "Os abacates só estão maduros quando estão escuros e macios"

Note que se p é F, então:

$\boldsymbol{p \to q}$ é V para qualquer $\boldsymbol{q}$

- Ou seja: uma falsa hipótese implica em qualquer conclusão...
- **Exemplo 1:** "Se 2+2=5, então no Brasil não há corrupção."
- **Exemplo 2:** Quando é que é Verdadeira a implicação: "Se hoje é terça-feira, então 2+3=6."?

Def.: Se $\boldsymbol{p \to q}$ é uma condicional. então:

- O <u>converso</u> de $\boldsymbol{p \to q}$ é: $\boldsymbol{q \to p}$
- O <u>inverso</u> de $\boldsymbol{p \to q}$ é: $\boldsymbol{\neg p \to \neg q}$
- A <u>contrapositiva</u> de $\boldsymbol{p \to q}$ é: $\boldsymbol{\neg q \to \neg p}$

Exemplo: "Se Rodolfo é catarinense, então Rodolfo é brasileiro".

$\boldsymbol{p \to q}$: $\boldsymbol{p}$: "Rodolfo é catarinense"
$\boldsymbol{q}$: "Rodolfo é brasileiro"

- $\boldsymbol{q \to p}$: "Se Rodolfo é brasileiro, então Rodolfo é catarinense" (??)
- $\boldsymbol{\neg p \to \neg q}$: "Se Rodolfo não é catarinense, Rodolfo não é brasileiro" (??)
- $\boldsymbol{\neg q \to \neg p}$: "Se Rodolfo não é brasileiro, Rodolfo não é catarinense" (OK)

Bicondicional ou equivalência ($p \to q \;\wedge\; q \to p$):

- Notação: $p \leftrightarrow q$

- Definição:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

V somente quando: p e q têm o mesmo valor verdade

Maneiras de representar $p \leftrightarrow q$:

- p se, e somente se, q
- p é necessário e suficiente para q

Exemplo: Seja $n \in \mathbb{N}$. Então: "$n \geq 3$ se, e somente se, $n^2 \geq 9$"

Proposições Compostas

- Podem ter muitas partes componentes, cada parte sendo uma sentença representada por alguma variável proposicional.
- Construídas com o auxílio dos conectivos lógicos.
- **Exemplos:**

  $s:\; p \to [q \wedge (p \to r)]$

  $s:\; \neg(p \leftrightarrow q) \leftrightarrow [(p \wedge \neg q) \vee (q \wedge \neg p)]$

  $r:\; [\neg p \wedge (p \vee q)] \to q$

Tabelas verdade de proposições compostas

- A sentença: $s:\; p \to [q \wedge (p \to r)]$
  - envolve 3 proposições independentes
  - logo, há $2^3 = 8$ situações possíveis:

p	q	r	$p \to [q \wedge (p \to r)]$
V	V	V	?
V	V	F	?
V	F	V	?
V	F	F	?
F	V	V	?
F	V	F	?
F	F	V	?
F	F	F	?

Construindo Tabelas verdade

Tabela verdade para uma proposição composta de $\boldsymbol{n}$ variáveis:

1) 1ras $\boldsymbol{n}$ colunas da tabela são rotuladas com as variáveis
   - outras colunas para combinações intermediárias
2) 1ras colunas listam os $\mathbf{2}^{\boldsymbol{n}}$ possíveis conjuntos de valores verdade das variáveis
3) para cada linha, computa-se os valores verdade restantes

Exemplo: Tabela verdade de $(p \vee q) \rightarrow (r \leftrightarrow p)$:

p	q	r	$p \vee q$	$r \leftrightarrow p$	$(p \vee q) \rightarrow (r \leftrightarrow p)$
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	V	V	V
V	F	F	V	F	F
F	V	V	V	F	F
F	V	F	V	V	V
F	F	V	F	F	V
F	F	F	F	V	V

□

Exemplo: Tabela verdade de $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$:

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$	$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
V	V	V	F	F	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

$\nwarrow$ equivalentes $\nearrow$

□

Classificação de Proposições Compostas

Tautologia: proposição sempre V (em todas as possíveis situações)

– Exemplo: $p \vee \neg p$

Contradição (ou absurdo): sempre F (todas as situações)

– Exemplo: $p \wedge \neg p$

Contingência: pode ser V ou F

– "nem tautologia nem contradição"

Equivalências Lógicas

- Se $\boldsymbol{p} \leftrightarrow \boldsymbol{q}$ é uma tautologia, $\boldsymbol{p}$ e $\boldsymbol{q}$ são logicamente equivalentes
  - Notação: $\boldsymbol{p} \Leftrightarrow \boldsymbol{q}$
- Se $\boldsymbol{p} \Leftrightarrow \boldsymbol{q}$, os dois lados são simplesmente diferentes modos de construir a mesma sentença
- Importante recurso da argumentação lógica:
  - substituição de uma proposição por outra equivalente
- Determinação da equivalência: Tabelas Verdade

Exemplo: Mostre que $\neg(\boldsymbol{p} \vee \boldsymbol{q})$ e $\neg \boldsymbol{p} \wedge \neg \boldsymbol{q}$ são equivalentes.

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

Algumas Equivalências importantes (outras nos livros-textos)

Equivalência	*Nome das leis*
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Idempotência
$\neg(\neg p) \Leftrightarrow p$	Dupla negação
$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Comutatividade
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Associatividade
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributividade
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	Leis de De Morgan

Uso das equivalências

Exemplo: $\boldsymbol{p} \vee \boldsymbol{q}$: "O rio é raso ou poluído". $\neg(\boldsymbol{p} \vee \boldsymbol{q})$: **?**

- pelas leis de De Morgan: $\neg(\boldsymbol{p} \vee \boldsymbol{q}) \Leftrightarrow \neg \boldsymbol{p} \wedge \neg \boldsymbol{q}$
- logo, $\neg(\boldsymbol{p} \vee \boldsymbol{q})$ é: "O rio não é raso E não é poluído."
- (Note que $\neg(\boldsymbol{p} \vee \boldsymbol{q})$ NÃO é equivalente a: "O rio não é raso OU não é poluído.")

Exemplo: Mostre que $\neg[(p \vee (\neg p \wedge q)]$ e $\neg p \wedge \neg q$ são logicamente equivalentes

$$
\begin{aligned}
\neg[(p \vee (\neg p \wedge q)] &\Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) && (2^a \text{ lei de De Morgan}) \\
&\Leftrightarrow \neg p \wedge [\neg(\neg p) \vee \neg q)] && (1^a \text{ lei de De Morgan}) \\
&\Leftrightarrow \neg p \wedge (p \vee \neg q) && (\text{Dupla negação}) \\
&\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) && (\text{Distributividade}) \\
&\Leftrightarrow F \vee (\neg p \wedge \neg q) && (\text{contradição}) \\
&\Leftrightarrow \neg p \wedge \neg q && p \vee F \Leftrightarrow p \qquad \square
\end{aligned}
$$

Provas Proposicionais

- Teorema: conjectura que se pode mostrar que é V
  - Também: “proposição”, “fato” ou “resultado”
- Prova: uma verificação de uma proposição por meio de uma cadeia de deduções lógicas (argumento), a partir de um conjunto base de axiomas
  - Estabelece a verdade de um teorema
- Construção de provas (argumentos):
  - novas declarações a partir das já conhecidas
- Questões importantes:
  - quando um argumento está correto?
  - quais os métodos para construir argumentos?

Teoremas na Lógica Proposicional

- Teoremas = tautologias
- Teorema mais comum: $p \to q$
  - p e q são proposições compostas
  - p é a hipótese
  - q é a conclusão
- Técnicas usuais de prova:
  - tabelas-verdade: inviáveis para muitas variáveis
  - dedução formal:
    - $p \to q$ só será teorema se for tautologia
      - daí: sempre que p for V, q também deverá ser
      - ou seja: é possível “deduzir q a partir de p”

Provas

Declarações em uma prova podem incluir:

- hipóteses do teorema a ser provado
- axiomas (ou postulados):
  - outras proposições que assume-se que são V
  - tautologias
  - “verdades evidentes”
- teoremas já provados previamente
- proposições derivadas através de regras de inferência

Regras de Inferência

Regras de inferência:
- “extraem conclusões” de afirmações prévias
- “amarram” os passos de uma prova

Inferências na Lógica Proposicional

- Regra fundamental: Modus Ponens

$$\begin{array}{ll} & \boldsymbol{p} \\ & \boldsymbol{p \to q} \\ \hline \therefore & \boldsymbol{q} \end{array}$$

  - “se tanto uma implicação quanto sua hipótese são V, a conclusão desta implicação é V”
  - baseada na tautologia: $\boldsymbol{(p \wedge (p \to q)) \to q}$

Exemplo: Suponha que sejam verdadeiras:

a implicação: “Se fizer sol hoje, eu irei à praia.”
e a hipótese: “Hoje o dia está ensolarado.”

- por modus ponens, segue que é V a conclusão da implicação:
  “Eu irei à praia.” $\square$

Exemplo: Assuma que é V a implicação: “Se $\boldsymbol{n > 3}$, então $\boldsymbol{n^2 > 9}$”.

- Agora assuma que sabemos que $\boldsymbol{n}$ é maior que 3
- Então, por modus ponens, segue que:
  “$\boldsymbol{n^2}$ é maior do que 9.” $\square$

Outras regras de inferência: (todas podem ser verificadas por tabelas-verdade)

Regra	Tautologia	Nome
$\begin{array}{l} p \\ \hline \therefore\ p \vee q \end{array}$	$p \to (p \vee q)$	**Adição**
$\begin{array}{l} p \wedge q \\ \hline \therefore\ p \end{array}$	$(p \wedge q) \to p$	**Simplificação**
$\begin{array}{l} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$	$((p) \wedge (q)) \to (p \wedge q)$	**Conjunção**
$\begin{array}{l} p \\ p \to q \\ \hline \therefore\ q \end{array}$	$[p \wedge (p \to q)] \to q$	**Modus Ponens**
$\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore\ \neg p \end{array}$	$[\neg q \wedge (p \to q)] \to \neg p$	**Modus Tollens**
$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore\ p \to r \end{array}$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	**Silogismo hipotético**
$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore\ q \end{array}$	$[(p \vee q) \wedge \neg p] \to q$	**Silogismo disjuntivo**
$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore\ q \vee r \end{array}$	$[(p \vee q) \wedge (\neg p \vee r)] \to (q \vee r)$	**Resolução**

- NOTA: Modus Tollens pode ser visto como um Modus Ponens "composto":

  Modus Tollens: $\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore\ \neg p \end{array}$

  Modus Tollens + Contrapositiva: $\begin{array}{l} \neg q \\ \neg q \to \neg p \\ \hline \therefore\ \neg p \end{array}$

- Silogismo disjuntivo também pode ser obtido a partir de Modus Ponens:

  Pois: $p \vee q \Leftrightarrow (\neg p) \to q$

- Interpretação útil do silogismo disjuntivo: "p corta com $\neg p$"

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore\ q \end{array}$$

- Interpretação útil também para a regra da Resolução:

$$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore\ q \vee r \end{array}$$

- **Exemplo 1(/3):** Determine qual regra de inferência é base para o argumento: "Está nublado agora. Portanto, ou está nublado ou está chovendo agora."
  - Sejam as proposições:

    p: "Está nublado agora."

    q: "Está chovendo agora."

– Então este argumento tem a forma:

$$\begin{array}{rl} & \boldsymbol{p} \\ \hline \therefore & \boldsymbol{p \vee q} \end{array}$$

∗ ou seja, usa a regra da adição. $\square$

- **Exemplo 2(/3):** "Está nublado e chovendo agora. Portanto, está nublado agora."

  – Proposições:

    $\boldsymbol{p}$: "Está nublado agora."
    $\boldsymbol{q}$: "Está chovendo agora."

  – Este argumento tem a forma:

$$\begin{array}{rl} & \boldsymbol{p \wedge q} \\ \hline \therefore & \boldsymbol{p} \end{array}$$

  – ou seja, usa a regra da simplificação. $\square$

- **Exemplo 3(/3):** "Se chover hoje, então hoje nós não teremos churrasco. Se não tivermos churrasco hoje, então teremos churrasco amanhã. Portanto, se chover hoje, teremos churrasco amanhã."

  $\boldsymbol{p}$: "Vai chover hoje."

  $\boldsymbol{q}$: "Não teremos churrasco hoje."

  $\boldsymbol{r}$: "Teremos churrasco amanhã."

  – Forma do argumento:

$$\begin{array}{rl} & \boldsymbol{p \rightarrow q} \\ & \boldsymbol{q \rightarrow r} \\ \hline \therefore & \boldsymbol{p \rightarrow r} \end{array}$$

  – ou seja, é um silogismo hipotético. $\square$

Argumentos válidos

- Um argumento tem forma válida se:
  – sempre que hipóteses são V, conclusão também é V
- Mostrar que $\boldsymbol{q}$ segue das hipóteses $\boldsymbol{p_1, p_2, \ldots, p_n}$:
- mesmo que mostrar que é V a implicação: $\boldsymbol{(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q}$
- Várias regras de inferência podem ser necessárias
  – argumento deve ser mostrado passo a passo
  – razão para cada passo deve ficar explícita

- **Exemplo 1:** Mostre que as hipóteses "Não está fazendo sol esta tarde e está mais frio do que ontem", "Nós iremos nadar somente se fizer sol", "Se nós não formos nadar, então nós vamos velejar", e "Se nós formos velejar, então estaremos em casa no final da tarde." levam à conclusão: "Estaremos em casa no final da tarde."

  $\boldsymbol{p}$: "Está fazendo sol esta tarde."

  $\boldsymbol{q}$: "Está mais frio do que ontem."

  $\boldsymbol{r}$: "Nós iremos nadar."

  $\boldsymbol{s}$: "Nós iremos velejar."

  $\boldsymbol{t}$: "Estaremos em casa no final da tarde."

  - Hipóteses: $\neg \boldsymbol{p} \wedge \boldsymbol{q}$, $\boldsymbol{r} \to \boldsymbol{p}$, $\neg \boldsymbol{r} \to \boldsymbol{s}$, $\boldsymbol{s} \to \boldsymbol{t}$
  - Conclusão: $\boldsymbol{t}$
  - Uma demonstração de que as hipóteses levam à conclusão:

Passo	**Justificativa**
1. $\neg \boldsymbol{p} \wedge \boldsymbol{q}$	Hipótese
2. $\neg \boldsymbol{p}$	1, Simplificação
3. $\boldsymbol{r} \to \boldsymbol{p}$	Hipótese
4. $\neg \boldsymbol{r}$	2, 3, Modus Tollens
5. $\neg \boldsymbol{r} \to \boldsymbol{s}$	Hipótese
6. $\boldsymbol{s}$	4, 5, Modus Ponens
7. $\boldsymbol{s} \to \boldsymbol{t}$	Hipótese
8. $\boldsymbol{t}$	6, 7, Modus Ponens $\square$

- NOTA: Pode-se inserir uma tautologia em qualquer passo de uma prova.

- **Exemplo 2(a):** A proposição "Meu cliente é canhoto. Mas, se o diário não desapareceu, então meu cliente não é canhoto. Logo, o diário desapareceu." é válida?

  $\boldsymbol{p}$: "Meu cliente é canhoto."

  $\boldsymbol{q}$: "O diário desapareceu."

  Argumento: $[\boldsymbol{p} \wedge (\neg \boldsymbol{q} \to \neg \boldsymbol{p})] \to \boldsymbol{q}$

  Prova:

Passo	**Justificativa**
1. $\boldsymbol{p}$	Hipótese
2. $\neg \boldsymbol{q} \to \neg \boldsymbol{p}$	Hipótese
3. $(\neg \boldsymbol{q} \to \neg \boldsymbol{p}) \to (\boldsymbol{p} \to \boldsymbol{q})$	Tautologia
4. $\boldsymbol{p} \to \boldsymbol{q}$	2, 3, Modus Ponens
5. $\boldsymbol{q}$	1, 4, Modus Ponens $\square$

- **Exemplo 2(b):** A prova do exemplo anterior pode ser simplificada para:

  Argumento: $[\boldsymbol{p} \wedge (\neg \boldsymbol{q} \rightarrow \neg \boldsymbol{p})] \rightarrow \boldsymbol{q}$

  Prova:

Passo	**Justificativa**
1. $\boldsymbol{p}$	Hipótese
2. $\neg \boldsymbol{q} \rightarrow \neg \boldsymbol{p}$	Hipótese
3. $\boldsymbol{q}$	1, 2, Modus Tollens $\square$

- NOTA: A validade da proposição depende apenas de sua forma lógica:
  - não tem a ver com o fato de seus componentes serem ou não realmente verdadeiros
  - no exemplo anterior, ainda não sabemos se o diário realmente desapareceu ou não...

- **Exemplo 3:** "Se a taxa para importação diminuir, o comércio interno aumentará. A taxa federal de desconto diminuirá ou o comércio interno não irá aumentar. A taxa para importação vai diminuir. Portanto, a taxa federal de desconto vai diminuir."

  $\boldsymbol{p}$: "A taxa para importação vai diminuir."

  $\boldsymbol{q}$: "O comércio interno vai aumentar."

  $\boldsymbol{r}$: "A taxa federal de desconto vai diminuir."

  Proposição: $[(\boldsymbol{p} \rightarrow \boldsymbol{q}) \wedge (\boldsymbol{r} \vee \neg \boldsymbol{q}) \wedge \boldsymbol{p}] \rightarrow \boldsymbol{r}$

  Prova:

Passo	**Justificativa**
1. $\boldsymbol{p} \rightarrow \boldsymbol{q}$	Hipótese
2. $\boldsymbol{r} \vee \neg \boldsymbol{q}$	Hipótese
3. $\boldsymbol{p}$	Hipótese
4. $\boldsymbol{q}$	1, 3, Modus Ponens

- **Exemplo 4(1/3):** "Você está a ponto de sair para o trabalho de manhã e descobre que está sem óculos. Você sabe os fatos a seguir. Onde estão os seus óculos?"

  1. Se meus óculos estão sobre a mesa da cozinha, então eu os vi no café da manhã.
  2. Eu estava lendo o jornal na sala ou na cozinha.
  3. Se eu estava lendo o jornal na sala, então meus óculos estão sobre a mesa de café.
  4. Eu não vi meus óculos no café da manhã.
  5. Se eu estava lendo meu livro na cama, então meus óculos estão sobre a mesinha de cabeceira.
  6. Se eu estava lendo o jornal na cozinha, então meus óculos estão sobre a mesa da cozinha.

  - Proposições simples ("idéias atômicas"):

    $\boldsymbol{p}$: "Meus óculos estão sobre a mesa da cozinha"

    $\boldsymbol{q}$: "Eu vi meus óculos no café da manhã"

    $\boldsymbol{r}$: "Eu estava lendo o jornal na sala"

    $\boldsymbol{s}$: "Eu estava lendo o jornal na cozinha"

    $\boldsymbol{t}$: "Meus óculos estão sobre a mesa do café"

    $\boldsymbol{u}$: "Eu estava lendo meu livro na cama"

    $\boldsymbol{v}$: "Meus óculos estão sobre a mesinha de cabeceira"

– Hipóteses: (a) $\boldsymbol{p \to q}$

(b) $\boldsymbol{r \vee s}$

(c) $\boldsymbol{r \to t}$

(d) $\boldsymbol{\neg q}$

(e) $\boldsymbol{u \to v}$

(f) $\boldsymbol{s \to p}$

Prova:

Passo	**Justificativa**
1. $\boldsymbol{\neg q}$	Hipótese
2. $\boldsymbol{p \to q}$	Hipótese
3. $\boldsymbol{\neg p}$	1,3, Modus Tollens
4. $\boldsymbol{s \to p}$	Hipótese
5. $\boldsymbol{\neg s}$	3,4, Modus Tollens
6. $\boldsymbol{r \vee s}$	Hipótese
7. $\boldsymbol{r}$	5,6, Silogismo disjuntivo
8. $\boldsymbol{r \to t}$	Hipótese
9. $\boldsymbol{t}$	7,8, Modus Ponens $\square$

Nota 1: Uso de tabelas-verdade

Uma demonstração por tabela-verdade seria possível para o exemplo anterior

- mas exigiria a análise de $\boldsymbol{2^7 = 128}$ possibilidades (!!)
- é melhor aplicar as regras de inferência
- mesmo em um processo de *tentativa e erro*

Nota 2: Premissas falsas

Argumento correto pode levar a conclusão incorreta

- se uma ou mais premissas falsas forem usadas.

Exemplo: Argumento válido por Modus Ponens:

Se $\boldsymbol{\sqrt{2} > \frac{3}{2}}$, então: $\boldsymbol{(\sqrt{2})^2 > (\frac{3}{2})^2}$

– ora, "sabemos que": $\boldsymbol{\sqrt{2} > \frac{3}{2}}$

– consequentemente: $\boldsymbol{(\sqrt{2})^2 > (\frac{3}{2})^2}$ (!!?)

- Mas a conclusão deste argumento é falsa
  – ocorre que a premissa "$\boldsymbol{\sqrt{2} > \frac{3}{2}}$" é falsa
  – logo, a conclusão podia mesmo ser falsa.

Nota 3: Falácias

- Erro comum em demonstrações: utilização de falácias
  - Falácias parecem-se com regras de inferência
  - mas: são baseadas em contingências

- Exemplo de falácia 1: a proposição $[(\boldsymbol{p} \to \boldsymbol{q}) \land \boldsymbol{q}] \to \boldsymbol{p}$
  - é F quando $\boldsymbol{p}$ é F e $\boldsymbol{q}$ é V
  - Erro comum: tratá-la como tautologia
    - falácia de "afirmar a conclusão".

- **Exemplo:** "Se você resolver todos os problemas da lista de exercícios, então você vai aprender Matemática Discreta. Você aprendeu Matemática Discreta. Logo, você resolveu todos os problemas da lista de exercícios."
  - Proposições:

    $\boldsymbol{p}$: "Você resolveu todos os problemas da lista de exercícios."

    $\boldsymbol{q}$: "Você aprendeu Matemática Discreta."
  - Vemos que o argumento consiste em:

    se $\boldsymbol{p} \to \boldsymbol{q}$ e $\boldsymbol{q}$, então $\boldsymbol{p}$ ("falácia de afirmar a conclusão")
  - É plenamente possível aprender MD sem resolver toda a lista:
    - você pode, por ex., resolver alguns (mas não todos) os problemas da lista, resolver outros exercícios, etc.

- Exemplo de falácia 2: a proposição $[(\boldsymbol{p} \to \boldsymbol{q}) \land \neg \boldsymbol{p}] \to \neg \boldsymbol{q}$
  - é F quando $\boldsymbol{p}$ é F e $\boldsymbol{q}$ é V
  - Falácia de "negar a hipótese"
  - Muitos argumentos incorretos a usam como regra

- **Exemplo:** Assuma que é correto que: "Se você resolver todos os problemas da lista de exercícios, então você vai aprender Matemática Discreta."
  - Então, "Se você não resolveu todos os problemas da lista",
  - será que é correto concluir que: "você não aprendeu MD"??
  - "Falácia de negar a hipótese".
  - É possível que você tenha aprendido MD mesmo que você não tenha resolvido todos os problemas da lista...

Leituras sobre proposições

- Kolman5: itens 2.1 e 2.2
- Rosen6: itens 1.1 e 1.2

2) Métodos de Prova

2.2) Predicados e quantificadores

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Predicados e quantificadores

- Servem para declarações da forma:
  - "$x > 3$"
  - "$x = y + 3$"
  - "$x + y = z$"
- Nem V nem F enquanto valores das variáveis não são especificados.
- Como produzir proposições a partir destas declarações?

Predicados

- A declaração "x é maior do que 3" tem duas partes:
  - a variável x (= "sujeito")
  - "é maior do que 3" (= "predicado")
- Predicado: propriedade que o sujeito da declaração pode ter.
- Podemos denotar "x é maior do que 3" por $P(x)$:
  - P é o predicado
  - x é a variável
- Ou: $P(x)$ é o valor da função proposicional P em x.
  - Quando um valor é atribuído a x, $P(x)$ se torna uma proposição e tem valor verdade.

- **Exemplo:** seja $P(x)$ a declaração "$x > 3$". Quais são os valores verdade de $P(4)$ e $P(2)$?

  Resposta: $P(4)$ é V e $P(2)$ é F.

- Também podemos ter declarações com mais de uma variável.

- **Exemplo**: "$x = y + 3$".
  - Pode ser denotado por $Q(x, y)$
  - Quando se atribui valores para x e para y, $Q(x, y)$ passa a ter um valor verdade.
  - Quais são os valores verdade de $Q(1, 2)$ e $Q(3, 0)$?

  Resposta: $Q(1, 2)$ é F e $Q(3, 0)$ é V.

- **Exemplo**: Seja $R(x, y, z)$ daqdo por "$x + y = z$":
  - quais os valores verdade de $R(1, 2, 3)$ e $R(0, 0, 1)$?

  Resposta: $R(1, 2, 3)$ é V e $R(0, 0, 1)$ é F.

- Em geral, uma declaração envolvendo as n variáveis $x_1, x_2, \ldots, x_n$ pode ser denotada por: $P(x_1, x_2, \ldots, x_n)$
  - que é o valor da função proposicional P para a tupla: $(x_1, x_2, \ldots, x_n)$
  - P também é chamado de predicado

Quantificadores

- Atribuindo valores a todas as variáveis em uma função proposicional, o resultado é uma proposição com valor verdade determinado.
- Outra forma de criar uma proposição a partir de uma função proposicional: a quantificação
  - Discutiremos quantificação universal e quantificação existencial.

Quantificador Universal

- Muitas declarações afirmam que uma propriedade é V ou F para todos os valores de uma variável em um domínio em particular
  - ou seja, em um **universo de discurso**
- São expressas com um quantificador universal:
  - $P(x)$ é V para todos os valores de x
  - é o universo de discurso que especifica os possíveis valores da variável x.
- A **quantificação universal** de $P(x)$ é a proposição:
  - "$P(x)$ é V para todos os valores de x no universo de discurso."

- Denotada por: $\forall x\ P(x)$
  - $\forall$ é o quantificador universal
  - "para todo x, $P(x)$"
  - "para todos os x, $P(x)$"

- **Exemplo:** Seja $P(x)$ dado por "$x + 1 > x$".
  - Qual o valor verdade da quantificação $\forall x\ P(x)$, sendo que o universo de discurso consiste de todos os nros reais?

- **Exemplo:** Seja $Q(x)$ a declaração "$x < 2$".
  - Qual o valor verdade da quantificação $\forall x\ Q(x)$?
  - O universo de discurso consiste de todos os nros reais.

- Quando todos os elementos do universo de discurso podem ser listados:
  - por exemplo: $x_1, x_2, \ldots, x_n$

  a quantificação universal fica o mesmo que a conjunção:
  - $P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$
  - a qual é V sse: $P(x_1), P(x_2), \ldots, P(x_n)$ são todos V

- **Exemplo:** qual o valor verdade de $\forall x\ P(x)$, onde:
  - $P(x)$ é "$x^2 < 10$"
  - o universo de discurso são os inteiros positivos não maiores do que 4?

- Especificar bem o UD é importante quando se usa quantificadores.
- O valor verdade de uma declaração quantificada frequentemente depende de quais elementos estão neste universo...

- **Exemplo:** Qual é o valor verdade de $\forall x\ (x^2 \geq x)$ se:
  - o universo de discurso consiste de todos os nros reais?
  - o UD consiste de todos os nros inteiros?

  Resposta:
  - note que $x^2 \geq x$ sse $x.(x-1) \geq 0$
  - ou seja: sse $x \leq 0$ ou $x \geq 1$
  - logo:
    * $\forall x\ (x^2 \geq x)$ é F se o UD consiste dos reais
    * mas é V se o UD consiste dos inteiros $\square$

- Para mostrar que uma declaração da forma $\forall x\ P(x)$ é F:
  - só é preciso encontrar um valor de x no UD para o qual $P(x)$ é F
  - este valor é chamado de contra-exemplo da declaração $\forall x\ P(x)$

- **Exemplo:** Seja $P(x)$ dado por $x^2 > 0$.
  - Vemos que $x = 0$ é um contra-exemplo.

- Muitas declarações matemáticas estabelecem que existe um elemento com uma certa propriedade.
- São expressas usando quantificação existencial.
- Forma-se uma proposição que é V se e somente se $P(x)$ é V para pelo menos um valor de x no universo de discurso.
- A quantificação existencial de $P(x)$ é a proposição:
  - "existe um elemento x no universo de discurso tal que $P(x)$ é V"
  - usa-se a notação: $\exists x\ P(x)$
- $\exists$ é o quantificador existencial e significa:
  - "existe um x tal que $P(x)$"
  - "existe pelo menos um x tal que $P(x)$"
  - "para algum x, $P(x)$"

- **Exemplo:** Seja $P(x)$ a declaração "$x > 3$".
  - Qual é o valor verdade da quantificação $\exists x\ P(x)$?
  - O UD consiste de todos os números reais.

  Resposta: $\exists x\ P(x)$ é V

- **Exemplo:** Seja $Q(x)$ a declaração "$x = x + 1$".
  - Qual é o valor verdade da quantificação $\exists x\ Q(x)$?
  - O UD consiste de todos os números reais.

  Resposta: $\exists x\ Q(x)$ é F

- Se todos os elementos do universo de discurso podem ser listados: $x_1, x_2, \ldots, x_n$

  segue que a quantificação existencial é o mesmo que a disjunção:
  - $P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$
  - a qual é V sse pelo menos um entre $P(x_1), P(x_2), \ldots, P(x_n)$ for V

- **Exemplo:** Qual o valor verdade de $\exists x\ P(x)$, onde:
  - $P(x)$ é a declaração "$x^2 > 10$"
  - o UD consiste dos inteiros positivos não maiores do que 4?

  Resposta:
  - Como o UD é $\{1, 2, 3, 4\}$, $\exists x\ P(x)$ é o mesmo que a disjunção:
    $$P(1) \vee P(2) \vee P(3) \vee P(4)$$
  - Como $P(4)$ é V, segue que $\exists x\ P(x)$ é V $\square$

Quantificadores - Resumo

Declaração	Quando é V?	Quando é F?
$\forall x\ P(x)$	$P(x)$ é V para todo x	Existe um x para o qual $P(x)$ é F
$\exists x\ P(x)$	Existe um x para o qual $P(x)$ é V	$P(x)$ é F para todo x

"Ligando" variáveis

- Quando um quantificador é usado sobre a variável x ou quando atribuímos um valor a esta variável, dizemos que esta ocorrência da variável está ligada (ou "amarrada").
- Uma ocorrência de variável que não está ligada a um quantificador ou fixa em um valor particular é chamada de livre.
- Todas as variáveis que ocorrem em uma função proposicional devem estar ligadas, para que ela seja considerada uma proposição.
- Isto pode ser feito com uma combinação de:
  - quantificadores universais
  - quantificadores existenciais
  - atribuições de valores
- A parte de uma expressão lógica à qual um quantificador é aplicado é o seu escopo.
- Uma variável é livre se estiver fora do escopo de todos os quantificadores na fórmula que a especifica.

- **Exemplo:** na declaração $\exists x\ Q(x, y)$:
  - a variável x está ligada à quantificação $\exists x$
  - mas a variável y está livre:
    * não está ligada a nenhum quantificador
    * nenhum valor lhe está sendo atribuído.

- **Exemplo:** na declaração $\exists x\ (P(x) \wedge Q(x))\ \vee\ \forall x\ R(x)$:
  - Todas as variáveis estão ligadas.
  - O escopo de $\exists x$ é a expressão: $P(x) \wedge Q(x)$
  - O escopo do quantificador "$\forall x$" é $R(x)$
  - Note que esta expressão pode ser escrita como: $\exists x\ (P(x) \wedge Q(x))\ \vee\ \forall y\ R(y)$

Negações

- **Exemplo:** Considere a sentença: "Todo aluno nesta sala já fez um curso de Cálculo"
  - Quantificação universal: $\forall x\ P(x)$, onde $P(x)$ é "x já cursou Cálculo"
  - A negação desta sentença é: "Não é verdade que todo aluno nesta sala já tenha feito Cálculo"
  - Note que isto é equivalente a: "Existe algum estudante em sala que não cursou Cálculo"
  - ou seja: $\exists x\ \neg P(x)$
- Este exemplo ilustra a seguinte equivalência: $\neg\forall x\ P(x) \equiv \exists x\ \neg P(x)$
- Nota: isto pode ser provado generalizando (por indução) a lei de De Morgan:

$$\neg(P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n))) \Leftrightarrow (\neg P(x_1) \vee \neg P(x_2) \vee \cdots \vee \neg P(x_n)))$$

- **Exemplo:** Agora queremos negar: "Existe um estudante nesta sala que já cursou Cálculo"
  - Trata-se de uma quantificação existencial: $\exists x\ Q(x)$, onde $Q(x)$ é "x já cursou Cálculo"
  - A negação desta declaração é:
    * "Não é verdade que exista nesta sala um estudante que já tenha cursado Cálculo"
  - o que é equivalente a: "Todo estudante desta sala ainda não cursou Cálculo"
  - ou seja: $\forall x\ \neg Q(x)$
- Este exemplo ilustra a seguinte equivalência: $\neg\exists x\ Q(x) \equiv \forall x\ \neg Q(x)$
- Nota: Isto pode ser provado generalizando (por indução) a outra lei de De Morgan:

$$\neg(P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n))) \Leftrightarrow (\neg P(x_1) \wedge \neg P(x_2) \wedge \cdots \wedge \neg P(x_n)))$$

Negações - Resumo

Negação	Declaração Equivalente	Quando é V?	Quando é F?
$\neg\exists x\ P(x)$	$\forall x\ \neg P(x)$	Para todo x, $P(x)$ é F	Existe um x para o qual $P(x)$ é V
$\neg\forall x\ P(x)$	$\exists x\ \neg P(x)$	Existe um x para o qual $P(x)$ é F	Para todo x, $P(x)$ é V

- **Exemplo:** Qual é a negação de: "Existe um político honesto"?
  - Seja $H(x)$: "x é honesto"
  - Então a declaração acima é: $\exists x\ H(x)$
    * onde o UD consiste de todos os políticos
  - A negação disto é: $\neg\exists x\ H(x)$
  - a qual é equivalente a: $\forall x\ \neg H(x)$
  - a qual pode ser expressa como:
    * "Todos os políticos não são honestos"
    * ou: "Todos os políticos são desonestos" $\square$

- **Exemplo:** Qual é a negação de: "Todos os americanos comem hambúrgueres"?
  - Seja $C(x)$: "x come hambúrguer"
  - Então a declaração acima é: $\forall x\ C(x)$
    - onde o UD consiste de todos os americanos
  - A negação disto é: $\neg\forall x\ C(x)$
  - que é equivalente a: $\exists x\ \neg C(x)$
  - que pode ser expressa como:
    - "Alguns americanos não comem hambúrguer"
    - ou: "Existe pelo menos um americano que não come hambúrguer" $\square$

- **Exemplo:** A negação de "$\forall x\ (x^2 > x)$" é a declaração: $\neg\forall x\ (x^2 > x)$
  - que é equivalente a: $\exists x\ \neg(x^2 > x)$
  - a qual pode ser reescrita como: $\exists x\ (x^2 \leq x)$
  - *Note que o valor-verdade desta declaração depende do UD.*

- **Exemplo:** A negação de "$\exists x\ (x^2 = 2)$" é a declaração: $\neg\exists x\ (x^2 = 2)$
  - que é equivalente a: $\forall x\ \neg(x^2 = 2)$
  - a qual pode ser reescrita como: $\forall x\ (x^2 \neq 2)$
  - *Note que o valor-verdade desta declaração depende do UD.*

Inferências na Lógica de Predicados

Regra de Inferência	Nome	Observação
$\boldsymbol{\forall x P(x)}$ $\therefore\ \boldsymbol{P(c)}$	*Instanciação* Universal	$\boldsymbol{c}$ específico
$\boldsymbol{P(c)}$ para um $\boldsymbol{c}$ arbitrário $\therefore\ \boldsymbol{\forall x P(x)}$	Generalização Universal	$\boldsymbol{c}$ arbitrário
$\boldsymbol{\exists x P(x)}$ $\therefore\ \boldsymbol{P(c)}$ para algum elemento $\boldsymbol{c}$	*Instanciação* Existencial	$\boldsymbol{c}$ específico (não conhecido)
$\boldsymbol{P(c)}$ para algum elemento $\boldsymbol{c}$ $\therefore\ \boldsymbol{\exists x P(x)}$	Generalização Existencial	$\boldsymbol{c}$ específico e conhecido

- **Exemplo 1:** Mostre que as premissas "Todos nesta turma de Fundamentos já cursaram Cálculo" e "Manoel é um estudante nesta turma" implicam na conclusão "Manoel já cursou Cálculo".
  - Declarações básicas:

    $\boldsymbol{F(x)}$: "$\boldsymbol{x}$ está nesta turma de Fundamentos"

    $\boldsymbol{C(x)}$: "$\boldsymbol{x}$ já cursou Cálculo"

- Premissas:

  $\forall \boldsymbol{x}(\boldsymbol{F}(\boldsymbol{x}) \rightarrow \boldsymbol{C}(\boldsymbol{x}))$
  $\boldsymbol{F}(\text{Manoel})$

- Estabelecendo a conclusão a partir das premissas:

Passo	**Justificativa**
1. $\forall \boldsymbol{x}(\boldsymbol{F}(\boldsymbol{x}) \rightarrow \boldsymbol{C}(\boldsymbol{x}))$	Premissa
2. $\boldsymbol{F}(\text{Manoel}) \rightarrow \boldsymbol{C}(\text{Manoel})$	Instanciação universal de (1)
3. $\boldsymbol{F}(\text{Manoel})$	Premissa
4. $\boldsymbol{C}(\text{Manoel})$	(2), (3), Modus Ponens $\square$

- **Exemplo 2:** Mostre que as premissas "Tem um estudante nesta turma que não leu o livro-texto" e "Todos nesta turma se saíram bem na primeira prova" implicam na conclusão "Alguém que se saiu bem na primeira prova não leu o livro-texto".

  - Declarações básicas:

    $\boldsymbol{T}(\boldsymbol{x})$: "$\boldsymbol{x}$ está nesta turma"
    $\boldsymbol{L}(\boldsymbol{x})$: "$\boldsymbol{x}$ leu o livro-texto"
    $\boldsymbol{P}(\boldsymbol{x})$: "$\boldsymbol{x}$ se saiu bem na primeira prova"

  - Premissas: $\exists \boldsymbol{x}(\boldsymbol{T}(\boldsymbol{x}) \land \neg \boldsymbol{L}(\boldsymbol{x}))$
    $\forall \boldsymbol{x}(\boldsymbol{T}(\boldsymbol{x}) \rightarrow \boldsymbol{P}(\boldsymbol{x}))$

  - Conclusão: $\exists \boldsymbol{x}(\boldsymbol{P}(\boldsymbol{x}) \land \neg \boldsymbol{L}(\boldsymbol{x}))$

  - Estabelecendo a conclusão a partir das premissas:

Passo	**Justificativa**
1. $\exists \boldsymbol{x}(\boldsymbol{T}(\boldsymbol{x}) \land \neg \boldsymbol{L}(\boldsymbol{x}))$	Premissa
2. $\boldsymbol{T}(\boldsymbol{a}) \land \neg \boldsymbol{L}(\boldsymbol{a})$	Instanciação existencial de (1)
3. $\boldsymbol{T}(\boldsymbol{a})$	Simplificação de (2)
4. $\forall \boldsymbol{x}(\boldsymbol{T}(\boldsymbol{x}) \rightarrow \boldsymbol{P}(\boldsymbol{x}))$	Premissa
5. $\boldsymbol{T}(\boldsymbol{a}) \rightarrow \boldsymbol{P}(\boldsymbol{a})$	Instanciação Universal de (4)
6. $\boldsymbol{P}(\boldsymbol{a})$	(3), (5), Modus Ponens
7. $\neg \boldsymbol{L}(\boldsymbol{a})$	Simplificação de (2)
8. $\boldsymbol{P}(\boldsymbol{a}) \land \neg \boldsymbol{L}(\boldsymbol{a})$	Conjunção de (6) e (7)
9. $\exists \boldsymbol{x}(\boldsymbol{P}(\boldsymbol{x}) \land \neg \boldsymbol{L}(\boldsymbol{x}))$	Generalização Existencial de (8) $\square$

Inferências na Lógica de Predicados

- **Nota 1:** É comum que apareçam tanto uma regra de inferência proposicional quanto uma para quantificadores.

- Por exemplo, Instanciação Universal e Modus Ponens são frequentemente usadas juntas:

  - combinando $\forall \boldsymbol{x}(\boldsymbol{P}(\boldsymbol{x}) \rightarrow \boldsymbol{Q}(\boldsymbol{x}))$ e $\boldsymbol{P}(\boldsymbol{c})$,
  - onde $\boldsymbol{c}$ é um elemento do UD
  - obtemos que $\boldsymbol{Q}(\boldsymbol{c})$ é Verdadeiro.

- **Nota 2:** Muitos teoremas omitem o quantificador ao definir que uma propriedade vale para todos os elementos de um conjunto.
- Por exemplo, o real significado de:
  - "Se $x > y$, onde x e y são reais positivos, então $x^2 > y^2$"
  - é: "Para todos os reais positivos x e y, se $x > y$, então $x^2 > y^2$".

- **Nota 3:** É comum a lei de generalização universal ser usada implicitamente:
  - no início da prova, seleciona-se um elemento geral do UD
  - passos subseqüentes mostram que este elemento tem a propriedade em questão
  - conclui-se que o teorema vale para todos os elementos do UD.

Leituras sobre Predicados e Quantificadores

Rosen6: itens 1.3 e 1.5

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

2) Métodos de Prova

2.3) Provas matemáticas

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications"*, 6^{th} *ed., McGraw-Hill, 2007.*

Prova de Teoremas Matemáticos

- Tarefa difícil.
- Veremos diversos métodos diferentes.
- Relembrando: "$\boldsymbol{p \rightarrow q}$ só não é V quando $\boldsymbol{p}$ é V e $\boldsymbol{q}$ é F."
- Observações úteis:
  - o inteiro $\boldsymbol{n}$ é par se existe um inteiro $\boldsymbol{k}$ tal que $\boldsymbol{n = 2k}$
  - o inteiro $\boldsymbol{n}$ é ímpar se existe um inteiro $\boldsymbol{k}$ tal que $\boldsymbol{n = 2k + 1}$

Provas Diretas

- **Princípio**: para provar $\boldsymbol{p \rightarrow q}$:
  1. assumir que $\boldsymbol{p}$ é verdadeiro
  2. usar regras de inferência e teoremas já provados para mostrar que $\boldsymbol{q}$ também deve ser V.

- **Exemplo:** $\forall \boldsymbol{n} \in \mathbb{N}$, "se $\boldsymbol{n}$ é ímpar, então $\boldsymbol{n^2}$ é ímpar"
  - assuma a hipótese: $\boldsymbol{n}$ é ímpar
  - então: $\boldsymbol{n = 2k + 1}$, para algum inteiro $\boldsymbol{k}$
  - segue que:
    $\boldsymbol{n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1}$
  - portanto: $\boldsymbol{n^2}$ é ímpar $\square$

Provas Indiretas

- **Princípio**: mostrar que a contrapositiva de $\boldsymbol{p \to q}$ é V, usando outras técnicas de demonstração.

- **Exemplo:** $\forall \boldsymbol{n} \in \mathbb{N}$, "se $\boldsymbol{3n+2}$ é ímpar, então $\boldsymbol{n}$ é ímpar"
  - assuma que a conclusão desta implicação é F
  - então: $\boldsymbol{n = 2k}$, para algum $\boldsymbol{k}$ inteiro
  - daí: $\boldsymbol{3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)}$
  - de modo que: $\boldsymbol{3n+2}$ é par
  - logo, uma vez que a negação da conclusão implica que a hipótese é F, a implicação original é V. $\square$

Provas por Vácuo

- **Princípio**: $\boldsymbol{p \to q}$ é V se $\boldsymbol{p}$ é F, de modo que:
  - prova-se $\boldsymbol{p \Rightarrow q}$ estabelecendo que $\boldsymbol{p}$ é sempre F
- Provam casos especiais de teoremas do tipo $\forall \boldsymbol{nP(n)}$.

- **Exemplo:** mostre que a proposição $\boldsymbol{P(0)}$ é V, aonde $\boldsymbol{P(n)}$ é "se $\boldsymbol{n > 1}$, então $\boldsymbol{n^2 > n}$".
  - $\boldsymbol{P(0)}$ é a implicação: "se $\boldsymbol{0 > 1}$, então $\boldsymbol{0^2 > 0}$"
  - uma vez que a hipótese é F:
    * a implicação $\boldsymbol{P(0)}$ é automaticamente V. $\square$

Provas Triviais

- **Princípio**: $\boldsymbol{p \to q}$ é V se $\boldsymbol{q}$ é V, de modo que:
  - pode-se provar $\boldsymbol{p \Rightarrow q}$ apenas estabelecendo que $\boldsymbol{q}$ é sempre V
- Importantes quando casos especiais de teoremas precisam ser provados (por ex.: em provas por casos e na indução matemática).

- **Exemplo:** Mostre que a proposição $\boldsymbol{P(0)}$ é Verdadeira em:

  $\boldsymbol{P(n)}$ **:** "se $\boldsymbol{a}$ e $\boldsymbol{b}$ são inteiros positivos com $\boldsymbol{a \geq b}$, então $\boldsymbol{a^n \geq b^n}$"
  - $\boldsymbol{P(0)}$ é: "se $\boldsymbol{a \geq b}$, então $\boldsymbol{a^0 \geq b^0}$"
  - uma vez que $\boldsymbol{a^0 = b^0 = 1}$, a conclusão de $\boldsymbol{P(0)}$ é V $\square$
    * (a hipótese, "$\boldsymbol{a \geq b}$", não é necessária)

- Primeiro, tentamos uma prova direta.
- Quando não há modo óbvio de seguir, às vezes uma prova indireta funciona tranquilamente...

- **Nota**:
  - O número real $\boldsymbol{r}$ é racional se existem inteiros $\boldsymbol{p}$ e $\boldsymbol{q}$, com $\boldsymbol{q \neq 0}$, tais que $\boldsymbol{r = p/q}$.
  - Um real que não é racional é chamado de **irracional**.

- **Exemplo:** Prove que a soma de dois nros racionais é racional:
  - funciona uma prova direta...
  - sejam $\boldsymbol{r}$ e $\boldsymbol{t}$ números racionais
  - então, existem inteiros:

    $\boldsymbol{p}$ e $\boldsymbol{q}$, com $\boldsymbol{q \neq 0}$, tais que: $\boldsymbol{r = p/q}$
    $\boldsymbol{u}$ e $\boldsymbol{v}$, com $\boldsymbol{v \neq 0}$, tais que: $\boldsymbol{t = u/v}$
  - daí, adicionando $\boldsymbol{r}$ e $\boldsymbol{t}$:

    $\boldsymbol{r + t = \frac{p}{q} + \frac{u}{v} = \frac{p.v+q.u}{q.v}}$
  - como $\boldsymbol{q \neq 0}$ e $\boldsymbol{v \neq 0}$, segue que $\boldsymbol{q.v \neq 0}$
  - isto significa que $\boldsymbol{r + t}$ é racional $\square$

- **Ex.:** Prove que se $\boldsymbol{n}$ é um inteiro e $\boldsymbol{n^2}$ é ímpar, então $\boldsymbol{n}$ é ímpar:
  - tentando uma prova direta:
    * $\boldsymbol{n^2}$ é ímpar $\Rightarrow$ $\exists\boldsymbol{k}$ inteiro tal que $\boldsymbol{n^2 = 2k + 1}$
    * será que isto serve para mostrar que $\boldsymbol{n}$ é ímpar??
    * ora, resolvendo para $\boldsymbol{n}$, obtemos: $\pm\boldsymbol{\sqrt{2k+1}}$
    * o que não é muito útil...
  - prova indireta:
    * assumimos que $\boldsymbol{n}$ não é ímpar
    * então $\boldsymbol{n = 2k}$
    * elevando os dois lados ao quadrado: $\boldsymbol{n^2 = 4k^2 = 2(2k^2)}$
    * como $\boldsymbol{2k^2}$ é inteiro, temos que $\boldsymbol{n^2}$ é par. $\square$

- **Exemplo:** Prove que a média aritmética de um par de reais positivos distintos $\boldsymbol{x}$ e $\boldsymbol{y}$ é sempre maior do que a média geométrica (ex.:)

  Resposta: (raciocínio invertido) Note que:

  $$\begin{aligned}
  &\boldsymbol{(x+y)/2 > \sqrt{x.y}}\\
  &\Leftrightarrow \boldsymbol{(x+y)^2/4 > x.y}\\
  &\Leftrightarrow \boldsymbol{(x+y)^2 > 4.x.y}\\
  &\Leftrightarrow \boldsymbol{x^2 + 2.x.y + y^2 > 4.x.y}\\
  &\Leftrightarrow \boldsymbol{x^2 - 2.x.y + y^2 > 0}\\
  &\Leftrightarrow \boldsymbol{(x-y)^2 > 0}
  \end{aligned}$$
  - Prova: "Uma vez que $\boldsymbol{(x-y)^2 > 0}$ quando $\boldsymbol{x \neq y}$. Logo ..."

- **Exemplo:** Em um certo jogo, duas pessoas se revezam removendo um, dois ou três pedras de cada vez de uma pilha que começa com **15** pedras. Quem remover a última pedra ganha o jogo. Mostre que o primeiro jogador sempre pode ganhar este jogo.

  Resposta: (raciocínio invertido)

  - A pode ganhar se encontrar uma pilha com 1, 2 ou 3 pedras
  - o que ocorre se B tiver que remover pedras de pilha com 4
  - A pode deixar 4 pedras se receber 5, 6 ou 7
  - o que ocorre se B tiver que remover pedras de pilha com 8
  - ora, A pode deixar 8 pedras se receber 9, 10 ou 11
  - o que ocorre se B tiver que remover pedras de pilha com 12
  - logo: A ganha se deixar, sucessivamente, 12, 8 e 4 pedras $\square$

Outras técnicas: Provas por contradição

- Estratégia:
  - assuma que $\boldsymbol{p \rightarrow q}$ é F
    - isto é: que $\boldsymbol{p}$ é V e $\boldsymbol{q}$ é F
  - com regras de inferência, derive uma contradição desta hipótese.
    - $\boldsymbol{r \wedge \neg r}$, por exemplo

- **Exemplo 1:** Provar que: "Se $\boldsymbol{3n+2}$ é ímpar, então $\boldsymbol{n}$ é ímpar."
  - vamos assumir que $\boldsymbol{3n+2}$ é ímpar e que $\boldsymbol{n}$ não é ímpar
  - mas já vimos que, se $\boldsymbol{n}$ é par, então $\boldsymbol{3n+2}$ é par
  - isto contradiz a hipótese de que $\boldsymbol{3n+2}$ é ímpar, completando a prova $\square$

- **Exemplo 2:** Provar que $\boldsymbol{p}$: "$\boldsymbol{\sqrt{2}}$ é irracional" é V.
  - assuma que $\boldsymbol{\neg p}$ é V, ou seja: $\boldsymbol{\sqrt{2}}$ é racional
    - logo, existem inteiros $\boldsymbol{a}$ e $\boldsymbol{b}$ tais que $\boldsymbol{\sqrt{2} = a/b}$
    - onde $\boldsymbol{a}$ e $\boldsymbol{b}$ não têm fatores em comum
  - segue que $\boldsymbol{2 = a^2/b^2}$
    - de modo que: $\boldsymbol{2b^2 = a^2}$, ou seja, $\boldsymbol{a^2}$ é par
    - logo: $\boldsymbol{a}$ é par, ou seja, $\boldsymbol{a = 2c}$, para algum inteiro $\boldsymbol{c}$
  - então temos: $\boldsymbol{2b^2 = 4c^2}$, de modo que $\boldsymbol{b^2 = 2c^2}$
    - ou seja: $\boldsymbol{b^2}$ é par e $\boldsymbol{b}$ é par também
    - contradição: assumimos que $\boldsymbol{a}$ e $\boldsymbol{b}$ não tinham fatores em comum
  - portanto: $\boldsymbol{p}$ é que é V. $\square$

- **Princípio**: $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$ é equivalente a:

  $$(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$$

  – ou seja: provar cada um dos $p_i \to q$ individualmente

- **Exemplo:** Use a prova por casos para mostrar que $|xy| = |x||y|$, onde x e y são reais.

  Nota: $|x| = x$, se $x \geq 0$

  $|x| = -x$, se $x \leq 0$

  – Sejam:
    * p: "x e y são números reais"
    * q: "$|xy| = |x||y|$"

  – Note que p é equivalente a $p_1 \vee p_2 \vee p_3 \vee p_4$, onde:
    * p_1: "$x \geq 0 \ \wedge \ y \geq 0$"
    * p_2: "$x \geq 0 \ \wedge \ y < 0$"
    * p_3: "$x < 0 \ \wedge \ y \geq 0$"
    * p_4: "$x < 0 \ \wedge \ y < 0$"

  4 casos para provar:

  1. $p_1 \to q$ é V, pois:
     * $xy \geq 0$ quando $x \geq 0$ e $y \geq 0$
     * de modo que: $|xy| = xy = |x||y|$
  2. $p_2 \to q$ é V, pois:
     * se $x \geq 0$ e $y < 0$, então $xy \leq 0$
     * de modo que: $|xy| = -xy = x.(-y) = |x||y|$
  3. $p_3 \to q$ é V, pois:
     * se $x < 0$ e $y \geq 0$, então $xy \leq 0$
     * de modo que: $|xy| = -xy = (-x).y = |x||y|$
  4. $p_4 \to q$ é V, pois:
     * se $x < 0$ e $y < 0$, então $xy > 0$
     * de modo que: $|xy| = xy = (-x).(-y) = |x||y|$ $\square$

- **Exemplo:** "Não existem soluções em inteiros para $x^2 + 3y^2 = 8$"

  Prova:

  – Não existem soluções quando $|x| \geq 3$ ou quando $|y| \geq 2$

  – de modo que: $x \in \{-2, -1, 0, 1, 2\}$ e $y \in \{-1, 0, 1\}$

  – valores possíveis para x^2: $0, 1$ e 4

  – valores possíveis para $3y^2$: 0 e 3

  – logo, a máxima soma possível é 7 $\square$

- Provas de teoremas que são bicondicionais.
- Usar a tautologia: $(p \leftrightarrow q) \Leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$
- Ou seja, "p se e somente se q" pode ser provada ao serem provadas as implicações:
  - "se p, então q"
  - "se q, então p"

- **Exemplo:** Prove o teorema: "O inteiro n é ímpar sse n^2 é ímpar."
  - Teorema da forma: "p sse q", aonde p é dado por: "n é ímpar" e q é dado por: "n^2 é ímpar"
  - Temos que provar $p \rightarrow q$ e $q \rightarrow p$.
  - O que já foi feito:

    $\rightarrow$: provas diretas

    $\leftarrow$: estratégias de prova □

- Pode-se ter que mostrar que várias proposições são equivalentes:

  $$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n$$

  Prova-se que são mutuamente equivalentes usando a tautologia:

  $$[p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge \cdots \wedge (p_n \rightarrow p_1)]$$

  - Muito mais eficiente do que provar todos contra todos...
  - Qualquer encadeamento de declarações é igualmente válido.

- **Exemplo:** Mostre que as afirmações a seguir são equivalentes:

  p_1: n é um inteiro par

  p_2: $n - 1$ é um inteiro ímpar

  p_3: n^2 é um inteiro par

  Prova: Mostrar que são V as implicações: $p_1 \rightarrow p_2$ $p_2 \rightarrow p_3$ e $p_3 \rightarrow p_1$

  - Mostrando $p_1 \rightarrow p_2$ (prova direta):

    n é par $\Rightarrow$ $n = 2k$ $\Rightarrow$ $n - 1 = 2k - 1 = 2(k - 1) + 1$
  - Mostrando $p_2 \rightarrow p_3$ (prova direta):

    $n - 1$ é ímpar $\Rightarrow$ $n - 1 = 2k + 1$ $\Rightarrow$ $n = 2k + 2$

    logo: $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$ (par)
  - Mostrando $p_3 \rightarrow p_1$ (prova indireta):
    * ou seja, devemos provar que: "se n não é par, então n^2 não é par"
    * já provado (provas diretas) □

Teoremas com Quantificadores

- Muitos teoremas são propostos como proposições que envolvem quantificadores.
- Veremos alguns dos métodos mais importantes para provar teoremas deste tipo.

Provas de existência

- Muitos teoremas são asserções de que existem objetos de um tipo em particular:
  - ou seja, são proposições da forma: $\exists x P(x)$
- Modos de provar estes teoremas:
  - Provas **construtivas**: encontrar elemento a tal que $P(a)$ é V
  - Provas **não-construtivas**: mostrar que a negação da proposição implica em uma contradição.

- **Exemplo:** Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas formas diferentes.

  Solução: Após uma busca computacional, descobrimos que:

  $$1729 = 10^3 + 9^3 = 12^3 + 1^3 \qquad \square$$

- **Exemplo:** Mostre que existem números irracionais x e y tais que x^y é racional.
  - Sabemos que $\sqrt{2}$ é irracional.
  - Agora considere o número $\sqrt{2}^{\sqrt{2}}$
  - se ele for racional, já temos x e y irracionais com x^y racional
  - mas se ele for irracional, podemos re-escolher x e y como:

    $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$

    $\Rightarrow x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$
  - Um dos dois casos demonstra o que foi pedido. $\square$

- Note que esta foi uma prova *não-construtiva*: mostramos que existe um par de números com a propriedade, mas não sabemos qual dos dois é o certo. (!)

Provas de unicidade

- Alguns teoremas afirmam que um elemento com a propriedade especificada existe e é único.
  - Ou seja: existe exatamente um elemento com esta propriedade.

- Logo, uma prova de unicidade tem duas partes:

1. Existência: mostra-se que um elemento $\boldsymbol{x}$ com a propriedade desejada existe.
2. Unicidade: mostra-se que, se $\boldsymbol{y \neq x}$, então $\boldsymbol{y}$ não possui a propriedade desejada.
   - Nenhum outro elemento tem esta propriedade, ou seja:
     $\boldsymbol{\exists x(P(x) \land \forall y(y \neq x \to \neg P(y)))}$

- **Exemplo:** Mostre que todo inteiro tem uma única inversa aditiva.
  - Se $\boldsymbol{p}$ é um inteiro, $\boldsymbol{p+q=0}$ para o inteiro $\boldsymbol{q=-p}$.
  - Logo: existe um inteiro $\boldsymbol{q}$ tal que $\boldsymbol{p+q=0}$.
  - Agora, seja um inteiro $\boldsymbol{r \neq q}$ tal que $\boldsymbol{p+r=0}$.
  - Então: $\boldsymbol{p+q=p+r}$.
  - Só que, subtraindo $\boldsymbol{p}$ de ambos os lados, segue que: $\boldsymbol{q=r}$
  - o que contradiz a hipótese $\boldsymbol{q \neq r}$
  - Logo, só existe um único inteiro $\boldsymbol{q}$ tal que $\boldsymbol{p+q=0}$. $\square$

Contra-exemplos

- Podemos mostrar que uma declaração do tipo $\boldsymbol{\forall x P(x)}$ é falsa com um contra-exemplo.
  - Ou seja, um exemplo de $\boldsymbol{x}$ para o qual $\boldsymbol{P(x)}$ é falsa.
- Procuramos um contra-exemplo sempre que encontramos uma declaração do tipo $\boldsymbol{\forall x P(x)}$ que:
  - acreditamos ser falsa,
  - tenha resistido a muitas tentativas de prova...

- **Exemplo:** Mostre que é falsa a declaração:

  "Todo inteiro positivo é igual à soma dos quadrados de três inteiros".
  - Possível com os 6 primeiros inteiros positivos:
    $\boldsymbol{1=0^2+0^2+1^2} \quad \boldsymbol{2=0^2+1^2+1^2} \quad \boldsymbol{3=1^2+1^2+1^2}$
    $\boldsymbol{4=0^2+0^2+2^2} \quad \boldsymbol{5=0^2+1^2+2^2} \quad \boldsymbol{6=1^2+1^2+2^2}$
  - Porém, não conseguimos fazer o mesmo com 7:
  - os únicos quadrados que poderíamos usar são: 0, 1 e 4 (aqueles que não excedem 7)
  - e não há maneira de combinar estes 3 números para somar 7
  - Logo, a declaração acima é falsa. $\square$

- Um erro comum é achar que (apenas) um ou mais exemplos são suficientes para concluir que uma declaração é verdadeira...

- Não importa quantos exemplos indiquem que $\boldsymbol{P(x)}$ é V:
  - a quantificação $\forall \boldsymbol{x}\boldsymbol{P(x)}$ ainda pode ser falsa...

- **Exemplo:** Será que é verdade que todo inteiro positivo é a soma de 18 inteiros elevados à quarta potência??
  - Observa-se que todos os inteiros até 78 podem mesmo ser escritos desta maneira (!!).
  - Daí, se decidíssemos que já havíamos verificado o suficiente, chegaríamos a uma conclusão errada, pois:
  - 79 não é a soma de 18 quartas potências. □

Erros comuns em provas (1)

- Mais comuns: erros em aritmética ou álgebra básica.

- **Exemplo 1:** O que está errado com a "prova" abaixo para 1=2?

  "Prova:" ($\boldsymbol{a}$ e $\boldsymbol{b}$ são dois inteiros positivos iguais)

Passo	**Justificativa**
1. $\boldsymbol{a = b}$	Dado
2. $\boldsymbol{a^2 = ab}$	Multiplicando os 2 lados de (1) por $\boldsymbol{a}$
3. $\boldsymbol{a^2 - b^2 = ab - b^2}$	Subtraindo $\boldsymbol{b^2}$ dos 2 lados de (2)
4. $\boldsymbol{(a - b)(a + b) = b(a - b)}$	Fatorando ambos os lados de (3)
5. $\boldsymbol{a + b = b}$	Dividindo ambos os lados de (4) por $\boldsymbol{a - b}$
6. $\boldsymbol{2b = b}$	Substituindo $\boldsymbol{a}$ por $\boldsymbol{b}$ em (5) (pois $\boldsymbol{a = b}$)
7. $\boldsymbol{2 = 1}$	Dividindo ambos os lados de (6) por $\boldsymbol{b}$

  Problema: Todos os passos são válidos, com exceção do passo 5, em que houve divisão por zero

Erros comuns em provas (2)

- Um erro comum ocorre em provas por casos, aonde nem todos os casos são considerados...

- **Exemplo:** O que está errado com esta "prova"?

  "Teorema:" Se $\boldsymbol{x}$ é um número real, então $\boldsymbol{x^2}$ é um real positivo.

  "Prova:" *Sejam:*

  $\boldsymbol{p_1}$: "$\boldsymbol{x}$ é positivo"
  $\boldsymbol{p_2}$: "$\boldsymbol{x}$ é negativo"
  $\boldsymbol{q}$: "$\boldsymbol{x^2}$ é positivo"

  - *provando* $\boldsymbol{p_1 \to q}$:
    - *quando* $\boldsymbol{x}$ *é positivo,* $\boldsymbol{x^2}$ *é positivo, pois é o produto de dois positivos*
  - *provando* $\boldsymbol{p_2 \to q}$:
    - *quando* $\boldsymbol{x}$ *é negativo,* $\boldsymbol{x^2}$ *é positivo, pois é o produto de dois negativos*

- Mas o suposto "teorema" é falso, pois está faltando o caso: $\boldsymbol{p_3}$: "$\boldsymbol{x = 0}$"

Erros comuns em provas (3)

- Erro particularmente desagradável: falácia chamada de "usar a questão".
- Consiste em basear um ou mais passos de uma prova na verdade daquilo que está sendo provado.
  - Ou seja: provar uma declaração usando ela mesma (ou uma outra equivalente a ela).
  - Também chamada de **raciocínio circular**.

- **Exemplo:** O argumento a seguir supostamente mostra que $\boldsymbol{n}$ é um inteiro par sempre que $\boldsymbol{n^2}$ é um inteiro par. Será que está correto??
  - Suponha que $\boldsymbol{n^2}$ é par.
  - Então $\boldsymbol{n^2 = 2k}$ para algum inteiro $\boldsymbol{k}$.
  - Seja $\boldsymbol{n = 2l}$ para algum inteiro $\boldsymbol{l}$.
  - Isto mostra que $\boldsymbol{n}$ é par.

  Análise:

  - Nada na prova permite concluir que $\boldsymbol{n}$ possa ser escrito como $\boldsymbol{2l}$.
  - Isto é equivalente ao que está sendo provado ("$\boldsymbol{n}$ é par").
  - *Note que o resultado em si é correto: apenas o método de prova está errado.*

Erros comuns: comentários finais

- Cometer erros em provas é parte do processo de aprendizagem.
- Quando cometer um erro que seja encontrado por outros, certifique-se de não cometê-lo de novo.
- Mesmo matemáticos profissionais cometem erros em provas.
- Diversas provas incorretas enganaram muitas pessoas durante anos antes que erros sutis fossem encontrados nelas...
- Note que não existe um algoritmo para provar teoremas.
- A construção de provas deve ser aprendida através da experiência.
- Ainda veremos muitas provas ao longo deste curso...

Nota: Tipos de teoremas

- Lema: teorema simples usado na prova de outros teoremas.
  - Teoremas complicados são mais fáceis de provar quando sub-divididos em uma série de lemas.
- Corolário: proposição que é consequência imediata de um teorema recém provado.
- Conjectura: declaração cujo valor-verdade não é conhecido.
  - Se for encontrada uma prova para a conjectura, ela se torna um teorema.

Leituras sobre Métodos de Prova:

- Rosen6: itens 1.6 e 1.7

3) Coleções

3.1) Conjuntos

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Conjuntos e subconjuntos

- Conjunto: "coleção" "bem definida" de objetos
  - Objetos: membros ou elementos do conjunto.
  - "Bem definida": possível decidir se um dado objeto pertence ou não à coleção
- Ou: "coleção não-ordenada de objetos".
- Normalmente, os objetos em um conjunto possuem uma mesma propriedade.
- **Exemplo:** o conjunto dos "inteiros menores do que 4": $A = \{1, 2, 3\}$

Exemplos de Conjuntos

- Conjunto dos livros da livraria da biblioteca (finito)
- Conjunto dos números naturais (infinito)
- Conjunto dos dinossauros vivos (Vazio, { }, $\emptyset$)
- Conjunto $\boldsymbol{S}$ de 2 elementos, um dos quais é o conjunto das letras minúsculas do alfabeto e o outro é o conjunto dos dígitos decimais:

$$\boldsymbol{X = \{a, b, c, d, \ldots, y, z\}}$$

$$\boldsymbol{Y = \{0, 1, 2, \ldots, 9\}}$$

$$\boldsymbol{S = \{X, Y\} = \{\{a, b, c, \ldots, y, z\}, \{0, 1, 2, \ldots, 9\}\}}$$

- Usualmente:
  - letras maiúsculas denotam conjuntos
  - letras minúsculas denotam elementos de um conjunto
- (Pertinência) O símbolo $\in$ denota que um elemento pertence ao conjunto ($\boldsymbol{a \in A}$).
- **Exemplo:** Se $\boldsymbol{A = \{violeta, amarelo, vermelho\}}$, então:
  - $\boldsymbol{amarelo \in A}$
  - $\boldsymbol{azul \notin A}$

Características dos Conjuntos

- A ordem em que os elementos são listados é irrelevante:

  $\{3, 2, 1\}$ e $\{1, 3, 2\}$ representam o mesmo conjunto

- A repetição dos elementos em um conjunto é irrelevante:

  $\{1, 1, 1, 3, 2\}$ é uma outra representação de $\{1, 2, 3\}$

Conjuntos definidos por propriedades

- Conjuntos infinitos podem ser definidos indicando-se um padrão

  Exemplo: conjunto S de todos os inteiros pares: $\{2, 4, 6, \ldots\}$

- S também pode ser definido por recursão:

  1) $2 \in S$
  2) Se $n \in S$, então $(n + 2) \in S$

- Outra forma de descrever este conjunto S:

  $S = \{x \mid x \text{ é inteiro positivo par}\}$

  ou: "o conjunto de todos os x tal que x é inteiro positivo e par"

- Definir um conjunto: especificar uma propriedade que seus elementos têm em comum

- Usa-se um predicado $P(x)$ para denotar uma propriedade P referente a uma variável objeto x.

- Notação para um conjunto S cujos elementos têm a propriedade P:

  $S = \{x \mid P(x)\}$

  o que significa também:

  $\{x \mid x \in S \wedge P(x)\}$

  $\{x \in S \mid P(x)\}$

- **Exemplos:**

  1. $\{x \mid x \text{ é um inteiro e } 3 < x \leq 7\}$
  2. $\{x \mid x \text{ é um mês com exatamente 30 dias}\}$
  3. $\{x \mid x \text{ é a capital do Brasil}\}$

Conjuntos especiais

$\mathbb{N}$: conjunto dos números naturais: $\{0, 1, 2, 3, \ldots\}$

$\mathbb{Z}$: conjunto dos nros inteiros: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Z}^+$: conjunto dos nros inteiros positivos: $\{1, 2, 3, \ldots\}$

$\mathbb{Q}$: conjunto dos nros racionais: $\{x \mid x = \frac{n}{m},\ m, n \in Z \text{ e } m \neq 0\}$

$\mathbb{R}$: conjunto dos nros reais: $\{x \mid x \text{ é um número real}\}$

Conjunto universo

- Para cada discussão existe um "conjunto universal" $\boldsymbol{U}$ contendo todos os objetos para os quais a discussão faz sentido

NOTA: O Paradoxo de Russell

- O conjunto "todos os conjuntos" não pode ser definido
- Uma "Teoria dos Conjuntos" que permitisse isto seria inconsistente:
  - considere o conjunto: $\boldsymbol{S = \{x \mid x}$ é um conjunto$\boldsymbol{\}}$ ($\boldsymbol{S \in S}$?!)
  - agora seja: $\boldsymbol{Q = \{x \in S \mid x}$ é um conjunto e $\boldsymbol{x \notin x\}}$
    - ∗ se $\boldsymbol{S}$ é um conjunto, então $\boldsymbol{Q}$ também o é ($\boldsymbol{Q \subseteq S}$)
    - ∗ note que alguns conjuntos estão em $\boldsymbol{Q}$ e outros não:
      - · $\boldsymbol{A = \{1, 2, 3\}}$ não é elemento de si mesmo e $\boldsymbol{A \in Q}$ (ok)
      - · mas: $\boldsymbol{P = \{}$todos os conjs infinitos$\boldsymbol{\} \Rightarrow P \in P \Rightarrow P \notin Q}$
    - ∗ questão: será que $\boldsymbol{Q \in Q}$??
      - · $\boldsymbol{Q \in Q \quad \Rightarrow \quad Q \notin Q \quad \Rightarrow}$ contradição!
      - · $\boldsymbol{Q \notin Q \quad \Rightarrow \quad Q \in Q \quad \Rightarrow}$ contradição!

- Solução: "Teoria dos Conjuntos Axiomática"
  - regras para quais conjuntos podem ser formados
  - as quais não permitem que o conjunto Q seja especificado
  - apenas interesse teórico neste curso

Subconjuntos

- O conjunto $\boldsymbol{A}$ é um subconjunto de $\boldsymbol{B}$ se e somente se:
  - todo elemento de $\boldsymbol{A}$ é também um elemento de $\boldsymbol{B}$
  - isto é: $\forall \boldsymbol{x} \ (\boldsymbol{x \in A \rightarrow x \in B})$
- Neste caso, diz-se que "$\boldsymbol{A}$ está contido em $\boldsymbol{B}$" e escreve-se $\boldsymbol{A \subseteq B}$
- Se $\boldsymbol{A}$ não é um subconjunto de $\boldsymbol{B}$, escreve-se $\boldsymbol{A \nsubseteq B}$
- Se $\boldsymbol{A}$ é um subconjunto de $\boldsymbol{B}$, mas $\boldsymbol{A \neq B}$, escrevemos $\boldsymbol{A \subset B}$
  - neste caso, $\boldsymbol{A}$ é um subconjunto próprio de $\boldsymbol{B}$

- **Exemplo:** Para os conjuntos:

  $$\boldsymbol{A = \{1, 7, 9, 15\} \qquad B = \{7, 9\} \qquad C = \{7, 9, 15, 20\}}$$

  - as seguintes sentenças são verdadeiras:

  $$\begin{array}{ll} \boldsymbol{B \subseteq C} & \boldsymbol{15 \in C} \\ \boldsymbol{B \subseteq A} & \boldsymbol{\{7, 9\} \subseteq B} \\ \boldsymbol{B \subset A} & \boldsymbol{\{7\} \subset A} \\ \boldsymbol{A \not\subset C} & \boldsymbol{\emptyset \subseteq C} \end{array}$$

- Nota: O conjunto Vazio é um subconjunto de todo conjunto, pois:
  - "Se $\boldsymbol{x \in \emptyset}$, então $\boldsymbol{x \in S}$" é sempre V (pois o antecedente é sempre F)

- Conjuntos podem ter outros conjuntos como membros.

- **Exemplo:** $A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

  Ou: $A = \{x \mid x \text{ é um subconjunto do conjunto } \{a, b\}\}$

- **Exemplo:** Seja A um conjunto e seja $B = \{A, \{A\}\}$.
  - Como A e $\{A\}$ são elementos de B, tem-se que:
    $A \in B$ e $\{A\} \in B$
  - Segue então que $\{A\} \subseteq B$ e que $\{\{A\}\} \subseteq B$
  - Mas não é verdade que $A \subseteq B$ (Por quê?)

Provando que $A \subseteq B$

- Suponha que $\boldsymbol{B = \{x \mid P(x)\}}$

- Para provar que $\boldsymbol{A \subseteq B}$:
  - toma-se um $\boldsymbol{x \in A}$ arbitrário (IU)
  - mostra-se que $\boldsymbol{P(x)}$ é verdadeira
    - (os elementos de $\boldsymbol{A}$ "herdam" a propriedade de $\boldsymbol{B}$)
  - generaliza-se (GU)

- **Exemplo:** seja $\boldsymbol{B = \{x \mid x}$ é múltiplo de $4\boldsymbol{\}}$ e $\boldsymbol{A = \{x \mid x}$ é múltiplo de $8\boldsymbol{\}}$
  - tome um $\boldsymbol{x \in A}$ (IU)
  - então: $\boldsymbol{x = m.8}$ para algum inteiro $\boldsymbol{m}$
  - daí: $\boldsymbol{x = m.2.4 = k.4}$, onde $\boldsymbol{k = 2m}$ também é um inteiro
  - isto mostra que $\boldsymbol{x}$ é múltiplo de 4 e que, portanto, $\boldsymbol{x \in B}$
  - logo: $\boldsymbol{A \subseteq B}$ (GU) $\square$

Igualdade de conjuntos

- Dois conjuntos $\boldsymbol{A}$ e $\boldsymbol{B}$ são ditos <u>iguais</u> se e somente se contêm os mesmos elementos:

  $$(\forall \boldsymbol{x}) \; [\, (\boldsymbol{x \in A \to x \in B}) \;\wedge\; (\boldsymbol{x \in B \to x \in A}) \,]$$

- Logo, podemos provar que $\boldsymbol{A = B}$ provando que: $\boldsymbol{A \subseteq B}$ e $\boldsymbol{B \subseteq A}$

- **Exemplo:** Provar que: $\boldsymbol{\{x \mid x \in \mathbb{N}}$ e $\boldsymbol{x^2 < 15\} = \{x \mid x \in \mathbb{N}}$ e $\boldsymbol{2x < 7\}}$
  - Elementos de $\boldsymbol{A}$: $\boldsymbol{\{0, 1, 2, 3\}}$ (todos com dobro $\boldsymbol{< 7}$)
  - Elementos de $\boldsymbol{B}$: $\boldsymbol{\{0, 1, 2, 3\}}$ (todos com quadrado $\boldsymbol{< 15}$)

Conjunto potência

- Muitos problemas envolvem testar todas as combinações dos elementos de um conjunto
- Conjunto potência de um conjunto $\boldsymbol{A}$: formado por todos os subconjuntos de $\boldsymbol{A}$
  - denotado por $\boldsymbol{P(A)}$ ou $\boldsymbol{2^A}$
  - também chamado de conjunto de "todas as partes" de $\boldsymbol{A}$
- **Exemplo:** $\boldsymbol{A = \{1, 2, 3\}}$
  - $\boldsymbol{P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}}$
- **Nota:** se $\boldsymbol{A}$ tem $\boldsymbol{n}$ elementos, então $\boldsymbol{P(A)}$ tem $\boldsymbol{2^n}$ elementos

Produto cartesiano

- O produto cartesiano de dois conjuntos $\boldsymbol{A}$ e $\boldsymbol{B}$, é o conjunto de todos os pares ordenados $\boldsymbol{(a, b)}$, onde $\boldsymbol{a \in A}$ e $\boldsymbol{b \in B}$, ou seja:

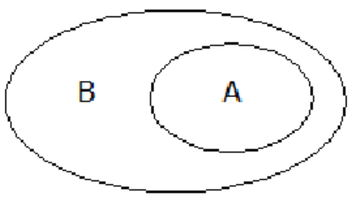
$$\boldsymbol{A \times B = \{(a, b) \mid a \in A \land b \in B\}}$$

- Exemplo: $\boldsymbol{A = \{1, 2\}}$ e $\boldsymbol{B = \{a, b, c\}}$

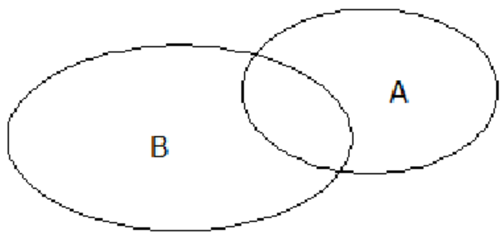
$$\boldsymbol{A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}}$$

- Note que: $\boldsymbol{B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\} \neq A \times B}$

Diagramas de Venn

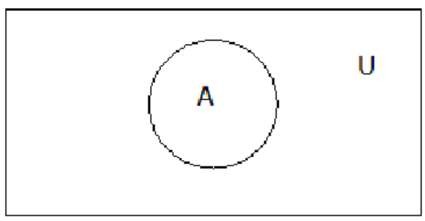


$A \subseteq B$



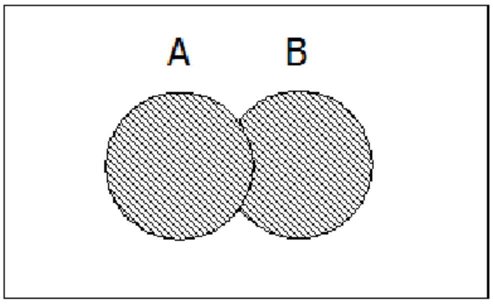
$A \not\subseteq B$

- O conjunto universo U contém todos os objetos em consideração:



- A <u>união</u> de dois conjuntos $\boldsymbol{A}$ e $\boldsymbol{B}$ é o conjunto que contém os elementos que estão em $\boldsymbol{A}$ ou em $\boldsymbol{B}$, ou em ambos:

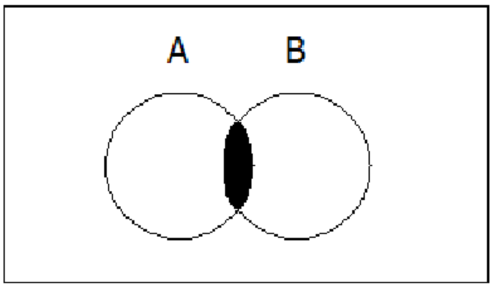
$$\boldsymbol{A} \cup \boldsymbol{B} = \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A} \vee \boldsymbol{x} \in \boldsymbol{B}\}$$



Exemplo: $\mathbf{\{1,3,5\} \cup \{1,2,3\} \ = \ \{1,2,3,5\}}$

- A <u>intersecção</u> de dois conjuntos $\boldsymbol{A}$ e $\boldsymbol{B}$ é o conjunto que contém elementos que estão tanto em $\boldsymbol{A}$ como em $\boldsymbol{B}$:

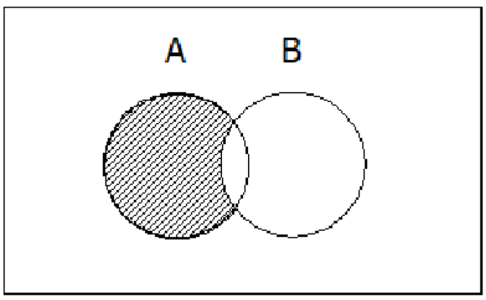
$$\boldsymbol{A} \cap \boldsymbol{B} = \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{x} \in \boldsymbol{B}\}$$



Exemplo: $\mathbf{\{1,3,5\} \cap \{1,2,3\} \ = \ \{1,3\}}$

- A <u>diferença</u> de dois conjuntos $\boldsymbol{A}$ e $\boldsymbol{B}$ é o conjunto de todos os elementos que estão em $\boldsymbol{A}$ mas não em $\boldsymbol{B}$:

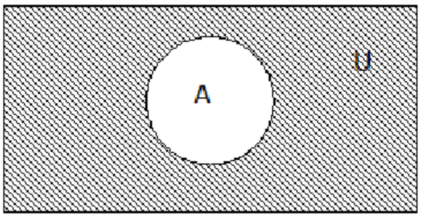
$$\boldsymbol{A} - \boldsymbol{B} = \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{A} \ \wedge \ \boldsymbol{x} \notin \boldsymbol{B}\}$$



Exemplo: $\mathbf{\{1,3,5\} \ - \ \{1,2,3\} \ = \ \{5\}}$

- Se U é o conjunto universo, $U - A$ é o complemento de A:

$$\overline{A} = \{x \mid x \notin A\}$$



Exemplo: Seja A o conjunto dos inteiros positivos maiores do que 10 e seja U o conjunto de todos os inteiros positivos).

Então: $\overline{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Identidades de conjuntos

- As operações sobre conjuntos satisfazem às propriedades:
  - Comutatividade:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

  - Associatividade:

$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$

  - Distributividade:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

  - Idempotência:

$$A \cup A = A$$
$$A \cap A = A$$

  - Propriedades do complemento:

$$\overline{\overline{A}} = A$$
$$A \cup \overline{A} = U$$
$$A \cap \overline{A} = \emptyset$$
$$\overline{\emptyset} = U \quad \text{e também:} \quad \overline{U} = \emptyset$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B} \qquad \text{(1a. Lei de De Morgan)}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B} \qquad \text{(2a. Lei de De Morgan)}$$

  - Outras propriedades:

$$A - (B \cap C) = (A - B) \cup (A - C)$$
$$A - (B \cup C) = (A - B) \cap (A - C)$$

- Propriedades do conjunto Universo:

$$\boldsymbol{A} \cup \boldsymbol{U} = \boldsymbol{U}$$
$$\boldsymbol{A} \cap \boldsymbol{U} = \boldsymbol{A}$$

- Propriedades do conjunto Vazio:

$$\boldsymbol{A} \cup \emptyset = \boldsymbol{A}$$
$$\boldsymbol{A} \cap \emptyset = \emptyset$$

- Nota: cada identidade acima tem o seu dual:
  - Troca-se $\cup$ por $\cap$
  - Troca-se $\boldsymbol{U}$ por $\emptyset$

Utilização das identidades

Exemplo: Sejam $\boldsymbol{A}$, $\boldsymbol{B}$ e $\boldsymbol{C}$ conjuntos. Mostre que: $\overline{\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})} = (\overline{\boldsymbol{C}} \cup \overline{\boldsymbol{B}}) \cap \overline{\boldsymbol{A}}$

Solução:

$$\begin{aligned}
\overline{\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})} &= \overline{\boldsymbol{A}} \cap \overline{(\boldsymbol{B} \cap \boldsymbol{C})} && \text{(1}^{a}\text{ lei de De Morgan)}\\
&= \overline{\boldsymbol{A}} \cap (\overline{\boldsymbol{B}} \cup \overline{\boldsymbol{C}}) && \text{(2}^{a}\text{ lei de De Morgan)}\\
&= (\overline{\boldsymbol{B}} \cup \overline{\boldsymbol{C}}) \cap \overline{\boldsymbol{A}} && \text{(comutatividade de } \cap\text{)}\\
&= (\overline{\boldsymbol{C}} \cup \overline{\boldsymbol{B}}) \cap \overline{\boldsymbol{A}} && \text{(comutatividade de } \cup\text{)}
\end{aligned}$$

Provando identidades de conjuntos

Exemplo: provar a lei de De Morgan: $\forall \boldsymbol{A}, \boldsymbol{B} (\overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}} = \overline{\boldsymbol{A} \cup \boldsymbol{B}})$

1) Fixe $\boldsymbol{A}$ e $\boldsymbol{B}$ (IU)
2) $\forall \boldsymbol{x}\ (\boldsymbol{x} \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}} \Leftrightarrow \boldsymbol{x} \in \overline{\boldsymbol{A} \cup \boldsymbol{B}})$:
   - 2.1) Fixe $\boldsymbol{x}$ (IU)
   - 2.2) $\boldsymbol{x} \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}} \Rightarrow \boldsymbol{x} \in \overline{\boldsymbol{A} \cup \boldsymbol{B}}$:
     - i. assuma que $\boldsymbol{x} \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$
     - ii. $\boldsymbol{x} \in \overline{\boldsymbol{A}}$ e $\boldsymbol{x} \in \overline{\boldsymbol{B}}$ (definição de intersecção)
     - iii. $\boldsymbol{x} \notin \boldsymbol{A}$ e $\boldsymbol{x} \notin \boldsymbol{B}$ (definição de complemento)
     - iv. $\boldsymbol{x} \notin \boldsymbol{A} \cup \boldsymbol{B}$ (definição de união)
     - v. $\boldsymbol{x} \in \overline{\boldsymbol{A} \cup \boldsymbol{B}}$ (definição de complemento)
   - 2.3) $\boldsymbol{x} \in \overline{\boldsymbol{A} \cup \boldsymbol{B}} \Rightarrow \boldsymbol{x} \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$
     - i. assuma que $\boldsymbol{x} \in \overline{\boldsymbol{A} \cup \boldsymbol{B}}$
     - ii. $\boldsymbol{x} \notin \boldsymbol{A} \cup \boldsymbol{B}$ (complemento)
     - iii. $\boldsymbol{x} \notin \boldsymbol{A}$ e $\boldsymbol{x} \notin \boldsymbol{B}$ (união)
     - iv. $\boldsymbol{x} \in \overline{\boldsymbol{A}}$ e $\boldsymbol{x} \in \overline{\boldsymbol{B}}$ (complemento)
     - v. $\boldsymbol{x} \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$ (intersecção)
   - 2.4) Generalize para todo $\boldsymbol{x}$ (GU)
3) Generalize para todo $\boldsymbol{A}, \boldsymbol{B}$ (GU) $\square$

- Conjuntos são muito usados em problemas de contagem, o que leva a uma discussão sobre o seu tamanho.
- Um conjunto $\boldsymbol{A}$ é dito finito se ele tem $\boldsymbol{n}$ elementos distintos ($\boldsymbol{n} \in \mathbb{N}$)
  - Neste caso, $\boldsymbol{n} = |\boldsymbol{A}|$ é chamado de cardinalidade de A
  - Um conjunto que não é finito é chamado de infinito
  - Exemplo: $|\{\mathbf{2}, \mathbf{5}, \mathbf{7}\}| = \mathbf{3}$

- Conjunto contável:
  - seus elementos podem ser arranjados em uma <u>lista ordenada</u>
  - a qual pode, portanto, ser contada
- Todos os conjuntos finitos são contáveis.
- Alguns conjuntos infinitos também:
  - por definição, o conjunto $\mathbb{Z}^+ = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \ldots\}$ é contável
- Um conjunto que não é contável é dito incontável

- Importante: saber se dois conjuntos possuem mesma cardinalidade
  - se ambos forem finitos, é só contar os elementos de cada um
  - porém: será que $\mathbb{Z}$, $\mathbb{Q}$, e $\mathbb{R}$ possuem a mesma cardinalidade??
- Ainda: será que $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são contáveis???

- Para nos convencermos de que dois conjuntos $\boldsymbol{X}$ e $\boldsymbol{Y}$ possuem a mesma cardinalidade:
  - tentamos produzir um "emparelhamento" de cada $\boldsymbol{x}$ em $\boldsymbol{X}$ com apenas um $\boldsymbol{y}$ em $\boldsymbol{Y}$
  - de maneira que cada elemento de $\boldsymbol{Y}$ seja usado apenas uma vez neste emparelhamento

- **Exemplo:** para os conjuntos $\boldsymbol{X} = \{\mathbf{2}, \mathbf{5}, \mathbf{7}\}$ e $\boldsymbol{Y} = \{?, !, \#\}$, o emparelhamento:

  $\mathbf{2} \leftrightarrow ?, \qquad \mathbf{5} \leftrightarrow \#, \qquad \mathbf{7} \leftrightarrow !$

  mostra que ambos possuem a mesma cardinalidade. $\square$

- **Exemplo:** O emparelhamento:

  $$\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & -4 & 4 & -5 & \cdots \end{array}$$

  - mostra que os conjuntos $\mathbb{Z}$ e $\mathbb{Z}^+$ possuem mesma cardinalidade
  - logo, o conjunto $\mathbb{Z}$ é contável. $\square$

- **Exemplo:** O conjunto dos racionais, $\mathbb{Q}$, é contável.
  - Emparelhamento com $\mathbb{Z}^+$???

- **Exemplo:** o conjunto de todos os reais entre $\mathbf{0}$ e 1 é incontável
  - Nota: um nro real entre 0 e 1 é o decimal infinito $\boldsymbol{.a_1 a_2 a_3 \ldots}$
  - onde $\boldsymbol{a_i}$ é um inteiro tal que $\mathbf{0} \leq \boldsymbol{a_i} \leq \mathbf{9}$.

Prova:

- assuma que o conjunto dos decimais ($\boldsymbol{0.a_1 a_2 a_3 \ldots}$) entre 0 e 1 é contável (!)
- então deve ser possível formar uma sequência contendo todos estes decimais:

$$\begin{aligned} \boldsymbol{n_1} &= \boldsymbol{.a_1 a_2 a_3 \ldots} \\ \boldsymbol{n_2} &= \boldsymbol{.b_1 b_2 b_3 \ldots} \\ \boldsymbol{n_3} &= \boldsymbol{.c_1 c_2 c_3 \ldots} \\ &\vdots \end{aligned}$$

- todo decimal infinito deve aparecer em algum lugar desta lista
- vamos estabelecer uma contradição construindo um decimal infinito $\boldsymbol{x}$ que não está na lista
- construindo o decimal $\boldsymbol{x = .x_1 x_2 x_3 \ldots}$:
  - valor de $\boldsymbol{x_1}$: qualquer dígito diferente de $\boldsymbol{a_1}$
  - valor de $\boldsymbol{x_2}$: qualquer dígito diferente de $\boldsymbol{b_2}$
  - valor de $\boldsymbol{x_3}$: qualquer dígito diferente de $\boldsymbol{c_3}$
  - e assim por diante...
- por exemplo, se tivéssemos:

$$\begin{aligned} \boldsymbol{n_1} &= \mathbf{0.3659663426\ldots} \\ \boldsymbol{n_2} &= \mathbf{0.7103958453\ldots} \\ \boldsymbol{n_3} &= \mathbf{0.0358493553\ldots} \\ \boldsymbol{n_4} &= \mathbf{0.9968452214\ldots} \\ &\vdots \end{aligned}$$

  - o número $\boldsymbol{x}$ poderia ser dado por: $\mathbf{0.5637\ldots}$
- o número $\boldsymbol{x}$ que resulta é um decimal infinito
  - certamente está entre 0 e 1
  - mas: difere de todos os números da lista em algum dígito
  - logo, $\boldsymbol{x}$ não está na lista
- resumindo: não importa como a lista é construída
  - sempre é possível construir um número real entre 0 e 1 que não está nela
- Contradição!
  - (a lista deveria conter todos os reais entre 0 e 1) $\square$

Leituras sobre Conjuntos

- Koman5: itens 1.1 e 1.2
- Rosen6: itens 2.1 e 2.2

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPTO DE INFORMÁTICA E ESTATÍSTICA
INE5403-FUNDAMENTOS DE MATEMÁTICA DISCRETA PARA A COMPUTAÇÃO

3) COLEÇÕES

3.2) SEQUÊNCIAS E SOMAS

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

SEQUÊNCIAS

- Como os conjuntos não são ordenados, uma estrutura diferente é necessária para representar coleções ordenadas.
- Uma sequência é uma lista de objetos em ordem
  - um "primeiro elemento", um "segundo elemento",...
  - pode ser finita ou não
- Uma sequência é uma função de um subconjunto dos inteiros, $\boldsymbol{0, 1, 2, \ldots}$ para um conjunto $\boldsymbol{S}$
  * denotada por $\boldsymbol{\{a_n\}}$
  * $\boldsymbol{a_n}$ representa um termo da sequência $\boldsymbol{\{a_n\}}$
  * $\boldsymbol{a_n}$ é a imagem do inteiro $\boldsymbol{n}$
- Descrevemos sequências listando os seus termos em ordem crescente do índice
- **Exemplo:** considere a sequência $\boldsymbol{\{a_n\}}$, onde: $\boldsymbol{a_n = \frac{1}{n+1}}$
  * a lista dos termos desta sequência, ou seja: $\boldsymbol{a_0, a_1, a_2, a_3, \ldots}$
  * começa com: $\boldsymbol{1,\ 1/2,\ 1/3,\ 1/4}$

EXEMPLOS DE SEQUÊNCIAS

- $\boldsymbol{1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1}$
- $\boldsymbol{1, 4, 9, 16, 25, \ldots =}$ "quadrados dos n^{os} positivos" (infinita)
  - também pode ser denotada por $\boldsymbol{(n^2)_{1\leq n\leq\infty}}$
- A sequência finita $\boldsymbol{1, 2, 4, \ldots, 256}$ pode ser denotada por $\boldsymbol{(2^n)_{0\leq n\leq 8}}$
- A notação $\boldsymbol{(1/n)_{2\leq n\leq\infty}}$ representa a sequência: 1/2, 1/3, 1/4,...
- A palavra "pesquisa" pode ser vista como a sequência finita: p,e,s,q,u,i,s,a
  - é costume omitir-se as vírgulas e escrever a palavra no modo usual
  - a palavra "abacabcd" pode ser vista como uma sequência de tamanho 8
  - sequências de letras ou outros símbolos, sem vírgulas, são chamadas de "strings"
- Progressões aritméticas: $\boldsymbol{a,\ a+d,\ a+2.d,\ \ldots,\ a+n.d}$

- Progressões geométricas: $\boldsymbol{a,\ a.r,\ a.r^2,\ \ldots,\ a.r^n}$

Formas Fechadas

- Problema: encontrar uma fórmula (regra geral) para a construção dos termos de uma sequência
  - às vezes, apenas alguns termos são conhecidos
  - então como identificar a sequência?
- 1ros termos não definem a sequência:
  - infinitas sequências começam com os mesmos termos iniciais
  - mas ajudam a montar uma conjectura
- Busca-se um padrão nos primeiros termos
- Pode-se também tentar determinar como um termo é produzido a partir dos que o precedem:
  - O mesmo valor reaparece?
  - Há termos obtidos a partir dos anteriores pela adição de uma qtde fixa?
    - Ou de uma qtde que dependa da posição?
  - Há termos obtidos a partir dos anteriores pela multiplicação por um valor fixo?
  - Há termos obtidos a partir de uma combinação dos anteriores?
  - Algum termo se repete?

- **Exemplo:** encontre uma fórmula para a sequência cujos 1ros termos são dados por: $\mathbf{1,\ 3,\ 5,\ 7,\ 9}$
  - cada termo obtido pela adição de 2 ao anterior
  - opção possível: $\boldsymbol{a_n = 2.n + 1}$ (“explícita”)
  - ou: PA com $\boldsymbol{a_0 = 1}$ e $\boldsymbol{d = 2}$
  - ou: $\boldsymbol{a_0 = 1}$ e $\boldsymbol{a_n = a_{n-1} + 2 \quad (\forall n \geq 1)}$ (“recursiva”)

- **Exemplo:** encontre uma fórmula para a sequência cujos 1ros termos são dados por:

  $\mathbf{1,\ 1/2,\ 1/4,\ 1/8,\ 1/16}$
  - os denominadores são potências de 2
  - opção possível: $\boldsymbol{a_n = 1/2^n}$ (“explícita”)
  - ou: PG com $\boldsymbol{a_0 = 1}$ e $\boldsymbol{r = 1/2}$
  - ou: $\boldsymbol{a_0 = 1}$ e $\boldsymbol{a_n = a_{n-1}/2 \quad (\forall n \geq 1)}$ (“recursiva”)

- **Exemplo:** como se pode produzir uma sequência cujos 1ros termos são dados por $\mathbf{1, -1, 1, -1, 1}$?
  - os termos alternam entre $\mathbf{1}$ e $\mathbf{-1}$
  - opção possível: $\boldsymbol{a_n = (-1)^n}$ (“explícita”)
  - ou: PG com $\boldsymbol{a = 1}$ e $\boldsymbol{r = -1}$
  - ou: $\boldsymbol{a_0 = 1}$ e $\boldsymbol{a_n = -a_{n-1} \quad (\forall n \geq 1)}$ (“recursiva”)

- **Exemplo:** como se pode produzir uma sequência cujos 1ros termos são dados por $\mathbf{1, 2, 2, 3, 3, 3, 4, 4, 4, 4}$?
  - possível regra de formação: "o inteiro n aparece exatamente n vezes"

- **Exemplo:** como se pode produzir uma sequência que começa com: $\mathbf{5, 11, 17, 23, 29, 35, 41, 47, 53, 59}$?
  - cada um destes termos é obtido pela adição de **6** ao anterior
  - possível regra: "n-ésimo termo produzido começando-se com 5 e adicionando-se 6 por $\boldsymbol{n}$ vezes"
  - ou seja: $\boldsymbol{a_n = 5 + 6.n}$

Formas de Construção

- Outra técnica: <u>comparar</u> com sequência bem conhecida, como:
  - termos de uma PA, PG
  - quadrados perfeitos
  - cubos perfeitos, ...

Sequências úteis

n-ésimo termo	primeiros 10 termos
n^2	$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, ...$
n^3	$0, 1, 8, 27, 64, 125, 216, 343, 512, 729, ...$
n^4	$0, 1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, ...$
2^n	$1, 2, 4, 8, 16, 32, 64, 128, 256, 512, ...$
3^n	$1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, ...$
$n!$	$1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880...$

- **Exemplo:** Deduza uma fórmula para a sequência $\boldsymbol{\{a_n\}}$ cujos 1ros termos são: $\mathbf{1, 7, 25, 79, 241, 727, 2185, 6559, 19681, 59047}$
  - diferenças entre termos consecutivos não indicam um padrão...
  - razão entre termos consecutivos, embora variável, fica próxima de **3**
    * suspeita: fórmula envolvendo $\boldsymbol{3^n}$
    * comparando com a sequência $\boldsymbol{\{3^n\}}$: $\boldsymbol{a_n = 3^{n+1} - 2}$

- Neil Sloane: Enciclopédia da sequências de inteiros
  - Coleção de milhares de sequências na Internet
  - Também busca sequências que combinam com termos iniciais fornecidos

- **Exemplo (Google):** encontre uma possibilidade para a próxima linha da sequência abaixo:

1
1 1
2 1
1 2 1 1

Conjunto correspondente a uma sequência

- Conjunto de todos os elementos distintos na sequência.
- **Exemplo**: o conjunto correspondente à sequência: $\boldsymbol{a, b, a, b, a, b, ...}$

  é, simplesmente: $\boldsymbol{\{a, b\}}$

Sequências e alfabetos

- $\boldsymbol{A^*}$: conjunto de todas as sequências finitas de elementos de $\boldsymbol{A}$
  - quando $\boldsymbol{A}$ é um conjunto de símbolos (e não de números), é chamado de alfabeto
- Sequências em $\boldsymbol{A^*}$: palavras ou strings de $\boldsymbol{A}$
  - sequências em $\boldsymbol{A^*}$ não são escritas com vírgulas entre os elementos
- Assume-se que $\boldsymbol{A}$ contém a sequência vazia ($\boldsymbol{\Lambda}$)
- **Exemplo:** seja $\boldsymbol{A = \{a, b, c, \dots, x, y, z\}}$

  $\boldsymbol{A^*}$ = todas as palavras comuns
  - ∗ tais como: macaco, universidade, desburocratizar,...
  - ∗ mas também: ixalovel, zigadongdong, cccaaa, pqrst, ...
  - Todas as sequências finitas de $\boldsymbol{A}$ estão em $\boldsymbol{A^*}$, tenham elas significado ou não...

Somas

- Notação usada para expressar a soma dos termos $\boldsymbol{a_m, a_{m+1}, \dots, a_n}$, a partir da sequência $\boldsymbol{\{a_n\}}$:

$$\sum_{j=m}^{n} a_j$$

  - a escolha da letra "$\boldsymbol{j}$" como índice é arbitrária

- **Exemplo:** A soma dos **100** primeiros termos da sequência $\boldsymbol{\{a_n\}}$, onde $\boldsymbol{a_n = \frac{1}{n+1}}$, é representada por:

$$\sum_{j=0}^{99} \left(\frac{1}{j+1}\right)$$

- **Exemplo:** Qual o valor de $\sum_{j=0}^{4} j^2$?

$$\sum_{j=0}^{4} j^2 = 0^2 + 1^2 + 2^2 + 3^2 + 4^2 = 30$$

Deslocamento do índice

- Útil quando duas somas precisam ser adicionadas, mas os seus índices não combinam
- Importante fazer as mudanças apropriadas no somando
- **Exemplo:** Suponha que tenhamos a soma: $\sum_{j=0}^{4} j^2$
  - mas precisamos que o índice vá de **1** a **5**, em vez de **0** a **4**
  - para isto, fazemos $k = j + 1$
  - e o termo j^2 se torna $(k-1)^2$:

$$\sum_{j=0}^{4} j^2 = \sum_{k=1}^{5} (k-1)^2 = 30$$

Somas Duplas

- Aparecem, por exemplo, na análise de loops "aninhados" em algoritmos
- **Exemplo:** $\sum_{i=1}^{4} \sum_{j=1}^{3} i.j$
  - avaliação: expanda a soma interna e então compute a externa

$$\sum_{i=1}^{4} \sum_{j=1}^{3} i.j = \sum_{i=1}^{4} (i + 2i + 3i) = \sum_{i=1}^{4} 6i = 60$$

Outras Somas

- Pode-se adicionar os valores de uma função ou termos de um conjunto indexado
- Escreve-se: $\sum_{s \in S} f(s)$ para representar a soma dos valores $f(s)$ para todos os membros s de S
- **Exemplo:** Qual o valor de $\sum_{s \in \{0,2,4\}} s$?

$$\sum_{s \in \{0,2,4\}} s = 0 + 2 + 4 = 6$$

Somas Úteis

- Certas somas aparecem repetidamente ao longo da Matemática Discreta
- Útil ter coleção de fórmulas para estas somas
- Há muitas maneiras de se provar/obter estas somas (todas podem ser provadas por indução)

.

soma	forma fechada
$\sum_{k=0}^{n-1} ar^k, \ (r > 1)$	$\frac{ar^n - a}{r-1}$
$\sum_{k=1}^{n} k$	$\frac{n.(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n.(n+1).(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2.(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \ \|x\| < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} k.x^{k-1}, \ \|x\| < 1$	$\frac{1}{(1-x)^2}$

- **Exemplo:** Encontre $\sum_{k=50}^{100} \boldsymbol{k^2}$?
  - Primeiro, note que: $$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2$$
  - Então use a fórmula para $\sum \boldsymbol{k^2}$ da tabela:

$$\sum_{k=50}^{100} k^2 = \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6} = 297925$$

- **Exemplo: (usa Cálculo)** Seja $\boldsymbol{x}$ um real com $|x| < 1$. Ache $\sum_{n=0}^{\infty} x^n$
  - pela 1ra fórmula da tabela, com $a = 1$ e $r = x$:

$$\sum_{n=0}^{k} x^n = \frac{x^{k+1} - 1}{x - 1}$$

  - então, já que $|x| < 1$: $x^{k+1} \to 0$ quando $k \to \infty$
  - portanto: $$\sum_{n=0}^{\infty} x^n = \lim_{k \to \infty} \frac{x^{k+1} - 1}{x - 1} = \frac{-1}{x - 1}$$

Leituras sobre Sequências e Somas

- Kolman5: item 1.3
- Rosen6: item 2.4

4) Indução Matemática

4.1) Princípio da indução

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Indução Matemática

- **Exemplo:** Provar que $\boldsymbol{n! \geq 2^{n-1}}$ para $\boldsymbol{n \in \{1, 2, 3, 4, 5\}}$

  Prova: usar a técnica de prova por casos:

  $\boldsymbol{n=1}$: $\boldsymbol{1! = 1 \geq 2^{1-1} = 1}$
  $\boldsymbol{n=2}$: $\boldsymbol{2! = 2 \geq 2^{2-1} = 2}$
  $\boldsymbol{n=3}$: $\boldsymbol{3! = 6 \geq 2^{3-1} = 4}$
  $\boldsymbol{n=4}$: $\boldsymbol{4! = 24 \geq 2^{4-1} = 8}$
  $\boldsymbol{n=5}$: $\boldsymbol{5! = 120 \geq 2^{5-1} = 16}$

  – Assim, como $\boldsymbol{n! \geq 2^{n-1}}$ para todo $\boldsymbol{n \in \{1, 2, 3, 4, 5\}}$, concluímos que esta proposição é V

- **Questão**: provar que $\boldsymbol{n! \geq 2^{n-1}}$ para todo $\boldsymbol{n \geq 1}$ $(\boldsymbol{n} \in \mathbb{Z}^+)$?

- **Exemplo:** Qual é a fórmula para a soma dos primeiros $\boldsymbol{n}$ inteiros positivos ímpares?

  – Note que:

  $\boldsymbol{1 = 1}$
  $\boldsymbol{1 + 3 = 4}$
  $\boldsymbol{1 + 3 + 5 = 9}$
  $\boldsymbol{1 + 3 + 5 + 7 = 16}$
  $\boldsymbol{1 + 3 + 5 + 7 + 9 = 25}$

  – Aparentemente a soma dos $\boldsymbol{n}$ primeiros inteiros positivos ímpares é dada por $\boldsymbol{n^2}$
  – Como ter certeza de que isto vale para qualquer $\boldsymbol{n}$?
  – Como provar esta suposição?

Método da Indução Matemática

- Técnica de demonstração de conjecturas.
- **Ilustração:** imagine que você deseja subir em uma escada sem fim.
  – Como saber se você será capaz de alcançar um degrau arbitrariamente alto?

- Agora suponha que sejam verdadeiras as seguintes afirmações sobre as suas habilidades de subir escadas:

  1. você pode alcançar o primeiro degrau
  2. ao chegar a um degrau qualquer, você sempre sempre pode passar ao degrau seguinte (uma implicação).

- Pela sentença 1, você tem garantia de chegar ao primeiro degrau

  – pela 2, você garante que chega ao segundo
  – novamente pela 2, você garante que chega ao segundo
  – novamente pela 2, você garante que chega ao terceiro
  – assim por diante

Princípio da Indução Matemática

- Técnica de prova de teoremas que estabelece que uma propriedade $\boldsymbol{P(n)}$ é V para todo $\boldsymbol{n}$ inteiro e positivo.

- A prova por indução matemática consiste de 2 passos:

  1. Passo básico: $\boldsymbol{P(1)}$ é V
  2. Passo indutivo: para um $\boldsymbol{k}$ genérico fixo é V o condicional:

     $$\boldsymbol{P(k) \to P(k+1)}$$

- Observações:

  1. Assumir que $\boldsymbol{P(k)}$ é V não é o mesmo que assumir o que queremos provar.

     ($\boldsymbol{k}$ se refere a apenas um caso em particular)
  2. Esta é uma técnica de raciocínio dedutivo, usada para provar alguma idéia obtida com um raciocínio indutivo.

- **Exemplo 1:** Mostre que, se $\boldsymbol{n}$ é um inteiro positivo:

  $$\boldsymbol{1+2+\cdots+n = n.(n+1)/2}$$

  Solução:

  – Passo básico: $\boldsymbol{P(1)}$ é V, pois $\boldsymbol{1 = 1.(1+1)/2}$
  – Passo indutivo: vamos assumir que $\boldsymbol{P(k)}$ vale, de modo que:

    $$\boldsymbol{1+2+\cdots+k = k.(k+1)/2}$$

    ∗ Com base nisto, queremos mostrar que vale:

    $$\boldsymbol{1+2+\cdots+k+(k+1) = (k+1).[(k+1)+1]/2}$$

    ∗ Ora, adicionando-se $\boldsymbol{(k+1)}$ a ambos os lados de $\boldsymbol{P(k)}$:

    $$\begin{aligned}\boldsymbol{1+2+\cdots+k+(k+1)} &= \boldsymbol{k.(k+1)/2+(k+1)}\\ &= \boldsymbol{(k+1).(k+2)/2} \qquad \square\end{aligned}$$

- **Exemplo 2:** Use a indução matemática para provar que a soma dos primeiros inteiros positivos ímpares é $\boldsymbol{n^2}$
  - Seja $\boldsymbol{P(n)}$ **:** "A soma dos primeiros ímpares é $\boldsymbol{n^2}$"
    - ou: "$\mathbf{1 + 3 + 5 + \cdots + (2}\boldsymbol{n}\mathbf{ - 1) =} \boldsymbol{n^2}$"
  - Passo básico: comprovar $\boldsymbol{P(1)}$
    - $\boldsymbol{P(1)}$ estabelece que $\mathbf{1 = 1^2}$, o que é V
  - Passo indutivo: mostrar que $\boldsymbol{P(k) \to P(k+1)}$ é V
    - Suponha que $\boldsymbol{P(k)}$ é V para um $\boldsymbol{k}$ fixo, ou seja:
      $\boldsymbol{1 + 3 + 5 + \cdots + (2k - 1) = k^2}$
    - A partir disto, queremos provar que $\boldsymbol{P(k+1)}$ é V, ou seja:
      $\boldsymbol{1 + 3 + 5 + \cdots + (2k - 1) + [2(k+1) - 1] = (k+1)^2}$ (será ??)
    - Uma vez que $\boldsymbol{P(k)}$ é V, o lado esquerdo acima fica:
      $$\begin{aligned} \boldsymbol{k^2 + [2(k+1) - 1]} &= \boldsymbol{k^2 + (2k + 2 - 1)} \\ &= \boldsymbol{k^2 + 2k + 1} \\ &= \boldsymbol{(k+1)^2} \end{aligned}$$
    - Isto mostra que, efetivamente, $\boldsymbol{P(k+1)}$ segue de $\boldsymbol{P(k)}$.
  - Assim, uma vez que $\boldsymbol{P(1)}$ e $\boldsymbol{P(k) \to P(k+1)}$ são V, independente da escolha de $\boldsymbol{k}$, concluímos que é V a proposição $\boldsymbol{\forall n\, P(n)}$

- **Exemplo 3:** Prove que, para qualquer inteiro positivo $\boldsymbol{n}$, $\boldsymbol{2^n > n}$

  Solução:
  - Passo básico: comprovar $\boldsymbol{P(1)}$
    - $\boldsymbol{P(1)}$ estabelece que $\mathbf{2^1 > 1}$, o que é V
  - Passo indutivo: mostrar que $\boldsymbol{P(k) \to P(k+1)}$ é V
    - Suponha que $\boldsymbol{P(k)}$ é V para um $\boldsymbol{k}$ fixo, ou seja: $\boldsymbol{2^k > k}$
    - Multiplicando os dois lados por 2, temos:
      $\boldsymbol{2.2^k > 2.k}$
      $\boldsymbol{2^{k+1} > k + k \geq k + 1}$
      $\boldsymbol{2^{k+1} > k + 1}$
    - $\boldsymbol{P(k+1)}$ é V $\square$

- **Exemplo 4:** Prove que $\boldsymbol{n^2 > 3.n}$, para $\boldsymbol{n \geq 4}$.
  - Passo básico: neste caso,o passo inicial é $\boldsymbol{P(4)}$:
    - $\mathbf{4^2 > 3.4}$, é, efetivamente, V
  - Passo indutivo:
    - Hipótese de indução: $\boldsymbol{k^2 > 3.k}$, para $\boldsymbol{k \geq 4}$
    - Queremos mostrar que $\boldsymbol{(k+1)^2 > 3.(k+1)}$ (??)
      $$\begin{aligned} \boldsymbol{(k+1)^2} &= \boldsymbol{k^2 + 2.k + 1} \\ &> \boldsymbol{3.k + 2.k + 1} && \text{(pela hipótese de indução)} \\ &\geq \boldsymbol{3.k + 8 + 1} && \text{(já que } \boldsymbol{k \geq 4}\text{)} \\ &> \boldsymbol{3.k + 3 = 3(k+1)} && \text{(já que } \boldsymbol{k \geq 4}\text{)} \end{aligned}$$
    - Isto mostra que $\boldsymbol{P(k+1)}$ é V sempre que $\boldsymbol{P(k)}$ é V. $\square$

- **Exemplo 5:** Sejam $A_1, A_2, A_3, \ldots, A_n$ conjuntos quaisquer. Prove por indução que:

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}$$

Solução:

- Seja $P(n)$: "vale a igualdade para quaisquer n conjuntos"
- Passo básico: $P(1)$ é $\overline{A_1} = \overline{A_1}$, o que é V
- Passo indutivo: usar $P(k)$ para provar $P(k+1)$:

$$\begin{aligned}
\overline{(\bigcup_{i=1}^{k+1} A_i)} &= \overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}} \\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}} \quad \text{(associatividade de } \cup\text{)} \\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k)} \cap \overline{A_{k+1}} \quad \text{(De Morgan para 2 conjs)} \\
&= (\bigcap_{i=1}^{k} \overline{A_i}) \cap \overline{A_{k+1}} \quad \text{(usando } P(k)\text{)} \\
&= (\bigcap_{i=1}^{k+1} \overline{A_i})
\end{aligned}$$

- Portanto, a implicação $P(k) \to P(k+1)$ é uma tautologia.
  - Logo, pelo princípio da indução, $P(n)$ é V, $\forall n \geq 1$. □

- Ao utilizar a indução para provar resultados, tome cuidado para não assumir que "$P(k)$ é V" para forçar o resultado esperado.
- Esta aplicação incorreta do princípio da indução matemática é um erro bastante comum.

Por que a Indução é válida?

- Por que o método da indução matemática é uma técnica de prova válida?
- Consequência do "Axioma do bom ordenamento" para os inteiros positivos:

  "Todo sub-conjunto não-vazio do conjunto dos inteiros positivos tem um elemento mínimo."

- Argumento:
  - Suponha que sabemos que $P(1)$ é V e que a proposição $P(k) \to P(k+1)$ é V, independente do k escolhido.
  - Agora assuma que existe pelo menos um inteiro positivo para o qual $P(n)$ é F
    - então o conjunto S dos "inteiros positivos para os quais $P(n)$ é F" é não-vazio.
  - Logo, pelo bom ordenamento, S tem um elemento mínimo (m):
    - sabemos que $m \neq 1$, pois assumimos que $P(1)$ é V
  - uma vez que m é positivo e > 1, temos que: $m-1$ é um inteiro positivo
  - mas $m-1$ não pode estar em S, já que $m-1 < m$
  - então: $P(m-1)$ deve ser V
  - Daí, uma vez que $P(k) \to P(k+1)$ também é V, devemos ter:

    $P(m)$ é V (contradição!)
  - Portanto, $P(n)$ deve ser V para todo inteiro positivo n. □

- Em toda prova usando indução matemática, devemos executar de forma correta e completa tanto o passo básico como o passo indutivo.

- **Erro #1**: Passo indutivo correto, mas passo básico não verificado.

  Exemplo: Seja $P(n)$ a afirmação "$\forall n \in \mathbb{Z}^+, \ \ n^2 + n$ é um número ímpar".

  - Passo indutivo: podemos provar que $P(k) \Rightarrow P(k+1)$:
    - Hipótese: $k^2 + k = 2m + 1$ (é ímpar)
    - Mas: $(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = 2m + 1 + 2k + 2 = 2(m + k + 1) + 1$
    - Portanto, $(k+1)^2 + (k+1)$ é ímpar também
    - Logo: $P(k) \Rightarrow P(k+1)$
  - Mas isto não permite concluir que $P(n)$ é verdadeiro "para todo n":
    - pois $P(1)$ é F.

- **Erro #2**: Passos básico e indutivo corretos, mas passo indutivo não inclui o passo básico.

  Exemplo: Encontre o erro na falsa prova abaixo de que todo conjunto de linhas no plano não-paralelas aos pares se encontra em um ponto comum.

  "Prova": Seja $\boldsymbol{P(n)}$: "Todo conjunto de $\boldsymbol{n}$ linhas não-paralelas aos pares no plano se encontra em um ponto comum".

  - Vamos "provar" que $\boldsymbol{P(n)}$ é V para todo inteiro positivo $\boldsymbol{n \geq 2}$.
  - Passo básico: $\boldsymbol{P(2)}$ é V, pois quaisquer duas linhas não-paralelas no plano se encontram em um ponto comum.
  - Passo indutivo:
    - Hipótese: assuma que $\boldsymbol{P(k)}$ é V (ou seja, assuma que "$\boldsymbol{k}$ linhas não-paralelas aos pares no plano efetivamente se encontram em um ponto")
    - Agora considere $\boldsymbol{k+1}$ linhas distintas no plano:
      - Pela hipótese: as primeiras $\boldsymbol{k}$ se encotram em um ponto $\boldsymbol{p_1}$
      - Também: as últimas $\boldsymbol{k}$ se encontram em um ponto $\boldsymbol{p_2}$
      - Agora se fosse $\boldsymbol{p_1 \neq p_2}$, todas as linhas que os contêm deveriam ser uma só (2 pontos determinam uma reta)
      - Portanto: $\boldsymbol{p_1}$ e $\boldsymbol{p_2}$ são o mesmo ponto
      - E o ponto $\boldsymbol{p_1 = p_2}$ está em todas as $\boldsymbol{k+1}$ linhas
    - Mostramos que, se assumirmos que todo conjunto de $\boldsymbol{k}$ ($\boldsymbol{k \geq 2}$) linhas distintas não-paralelas se encontram em um ponto, isto valerá também para $\boldsymbol{k+1}$ linhas.
  - Completamos o passo básico e o passo indutivo de uma prova por indução que parece correta...

  Problema com esta prova: Note que o passo indutivo requer que $\boldsymbol{k \geq 3}$ (!!)

  - Pois não podemos mostrar que $\boldsymbol{P(2)}$ implica em $\boldsymbol{P(3)}$!
  - Quando $\boldsymbol{k = 2}$, o nosso objetivo é mostrar que "quaisquer 3 linhas distintas não-paralelas aos pares se encontram em um ponto".

- As 2 primeiras linhas se encontram mesmo em um ponto $\boldsymbol{p_1}$ e as 2 últimas em um ponto $\boldsymbol{p_2}$.
- Mas, neste caso, $\boldsymbol{p_1}$ e $\boldsymbol{p_2}$ não precisam ser o mesmo ponto
  * pois apenas a 2a linha é comum a ambos os conjuntos... $\square$

Leituras sobre Indução matemática

- Kolman5: item 2.4
- Rosen6: item 4.1

4) Indução Matemática

4.2) Indução forte

Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.*

Indução Forte

- Outra forma para o princípio da indução matemática.

- Também consiste de 2 passos:
  1. Passo básico: provar que $\boldsymbol{P(1), P(2), \ldots, P(m)}$ é V
  2. Passo indutivo: provar que, para $\boldsymbol{k \geq m}$:

     $\boldsymbol{P(1) \wedge P(2) \wedge \ldots \wedge P(k) \;\Rightarrow\; P(k+1)}$

- Interpretação: "Posso me apoiar em $\boldsymbol{k}$ *ou qualquer degrau antes dele* para tentar chegar a $\boldsymbol{k+1}$."

- Forma equivalente à primeira: escolha depende da conveniência.

- A validade de ambos os princípios de indução segue do princípio do bom ordenamento.
  - De fato, os 3 princípios são equivalentes.
  - Ou seja, qualquer prova que utilize um destes princípios pode ser reescrita utilizando qualquer um dos outros dois.
  - Dependendo do caso a ser provado, pode ser mais conveniente usar um ou outro princípio...
  - Pode-se mostrar que qualquer uma das técnicas é válida assumindo que a outra é válida.

- Note que toda prova que usa indução simples pode ser considerada uma prova por indução forte, pois:
  - a hipótese indutiva de uma prova por indução simples é parte da hipótese indutiva de uma prova por indução forte
  - ou seja, se podemos completar o passo indutivo de uma indução simples mostrando que $\boldsymbol{P(k+1)}$ decorre de $\boldsymbol{P(k)}$:
  - $\boldsymbol{P(k+1)}$ também decorre de todos os $\boldsymbol{P(1), P(2), \ldots, P(k)}$
  - neste caso, temos garantia de que "mais do que" $\boldsymbol{P(k)}$ é V

- Também é possível converter uma prova por indução forte em uma prova por indução simples.

- A indução forte também permite uma analogia com a escada infinita.
- Ela diz que podemos alcançar todos os degraus se:
  - pudermos alcançar os primeiros m degraus
  - para todo inteiro $\boldsymbol{k}$, se pudermos alcançar todos os primeiros $\boldsymbol{k}$ degraus ($\boldsymbol{k} \geq \boldsymbol{m}$), então poderemos alcançar o $\boldsymbol{(k+1)}$-ésimo degrau
- O exemplo a seguir ilustra o uso da indução forte em um caso que não pode ser provado facilmente utilizando indução fraca.

- **Exemplo:** Suponha que:
  - podemos alcançar o 1^o e o 2^o degraus de uma escada infinita
  - sabemos que, uma vez estando em um degrau, podemos alcançar dois degraus acima

  Prove que podemos alcançar qualquer degrau da escada usando:

  (a) o princípio da indução matemática

  (b) indução forte

  Solução (a): usando indução fraca:
  - Passo básico: vale, pois podemos alcançar o primeiro degrau
  - Passo indutivo (tentativa):
    * Hipótese: podemos alcançar o $\boldsymbol{k}$-ésimo degrau da escada
    * Precisamos mostrar que, se assumirmos esta hipótese, então poderemos alcançar o $\boldsymbol{(k+1)}$-ésimo degrau
    * Mas não existe modo evidente de completar este passo, pois não sabemos, a partir da informação dada, que podemos alcançar o degrau $\boldsymbol{(k+1)}$ a partir do $\boldsymbol{k}$-ésimo
    * Só o que sabemos é: se podemos alcançar um degrau, então poderemos alcançar o degrau dois níveis acima...

  Solução (b): usando indução forte:
  - Passo básico: vale (com $\boldsymbol{m = 2}$), pois podemos alcançar os $\boldsymbol{2}$ primeiros degraus
  - Passo indutivo:
    * Hipótese: podemos alcançar cada um dos $\boldsymbol{1^{os}}$ $\boldsymbol{k}$ degraus
    * Precisamos mostrar que, assumindo esta hipótese, poderemos alcançar o $\boldsymbol{(k+1)}$-ésimo degrau
    * Já sabemos que podemos alcançar o segundo degrau:
      · Então, a partir de $\boldsymbol{k = 2}$, sempre poderemos alcançar o degrau $\boldsymbol{(k+1)}$ a partir do degrau $\boldsymbol{(k-1)}$
      · Pois sabemos que podemos escalar 2 degraus a partir de um degrau que já tenhamos atingido
  - Isto completa a prova por indução forte. $\square$

- **Exemplo:** Mostre que se $\boldsymbol{n}$ é um inteiro $> \mathbf{1}$, ele pode ser escrito como o produto de números primos.

  Solução: Seja $\boldsymbol{P(n)}$: "$\boldsymbol{n}$ pode ser escrito como o produto de números primos"

  <u>Passo básico</u>: $\boldsymbol{P(2)}$ é verdade, pois 2 pode ser escrito como um primo (ele mesmo).

  <u>Passo Indutivo</u>:

  - Vamos assumir que $\boldsymbol{P(r)}$ é verdade para todo $\boldsymbol{r \leq k}$
  - Devemos mostrar que, com esta hipótese, $\boldsymbol{P(k+1)}$ é V
  - Há dois casos a considerar:

    1) $\boldsymbol{k+1}$ é primo: neste caso, $\boldsymbol{P(k+1)}$ é imediatamente V
    2) $\boldsymbol{k+1}$ é composto: então ele pode ser escrito como:

       $\boldsymbol{k+1 = a.b}$, onde $\boldsymbol{2 \leq a \leq b \leq k}$
  - Daí, pela hipótese de indução, tanto $\boldsymbol{a}$ como $\boldsymbol{b}$ podem ser escritos como o produto de primos
  - Portanto, se $\boldsymbol{k+1}$ é composto, ele pode ser escrito como o produto de alguns primos.
    - (Aqueles da fatoração de $\boldsymbol{a}$ e de $\boldsymbol{b}$) $\square$

- **Exemplo:** Prove que todo inteiro positivo $\boldsymbol{n > 1}$ pode ser escrito unicamente como $\boldsymbol{p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}}$, onde os $\boldsymbol{p_i}$ são primos e $\boldsymbol{p_1 < p_2 < \cdots < p_s}$ (mais detalhado que o exemplo anterior).

  Solução:

  - Passo básico: $\boldsymbol{P(2)}$ é V, uma vez que 2 é primo
  - Passo indutivo: vamos usar $\boldsymbol{P(2)}$,$\boldsymbol{P(3)}$,...,$\boldsymbol{P(k)}$ para mostrar $\boldsymbol{P(k+1)}$:

    "$\boldsymbol{k+1}$ pode ser escrito unicamente como $\boldsymbol{p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}}$"
  - Aqui há dois casos a considerar:
    - $\boldsymbol{k+1}$ é primo: então $\boldsymbol{P(k+1)}$ é V
    - $\boldsymbol{k+1}$ não é primo:
      - · então $\boldsymbol{k+1 = l.m}$, aonde: $\boldsymbol{2 \leq l \leq k}$ e $\boldsymbol{2 \leq m \leq k}$
      - · daí, usando $\boldsymbol{P(l)}$ e $\boldsymbol{P(m)}$, temos:
      - · $\boldsymbol{k+1 \;=\; l.m \;=\; (q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}).(r_1^{c_1} r_2^{c_2} \cdots r_v^{c_v}) \;=\; p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}}$
      - · onde cada $\boldsymbol{p_i = (q_j}$ ou $\boldsymbol{r_k)}$ e $\boldsymbol{p_1 < p_2 < \cdots < p_s}$
      - · além disto, se $\boldsymbol{q_j = r_k = p_i}$, então $\boldsymbol{a_i = b_j + c_k}$
      - · caso contrário: ($\boldsymbol{p_i = q_j}$ e $\boldsymbol{a_i = b_j}$) ou ($\boldsymbol{p_i = r_k}$ e $\boldsymbol{a_i = c_k}$)
    - já que a fatoração de $\boldsymbol{l}$ e $\boldsymbol{m}$ são únicas, a de $\boldsymbol{k+1}$ também o é $\square$

- **Exemplo:** Considere um jogo em que dois jogadores se revezam removendo um nro qualquer que desejem de palitos de uma de duas pilhas. O jogador que remover o último palito ganha o jogo. Mostre que, se as duas pilhas contiverem o mesmo número de palitos inicialmente, o segundo jogador sempre pode garantir uma vitória.

  Solução:

  – Seja $\boldsymbol{n}$ o número de palitos em cada pilha.
  – Usaremos indução forte para provar $\boldsymbol{P(n)}$: "o $\mathbf{2^o}$ pode ganhar quando houver, inicialmente, $\boldsymbol{n}$ palitos em cada pilha"
  – Passo básico:
    * quando $\boldsymbol{n = 1}$, o $\mathbf{1^o}$ jogador só pode remover um palito de uma das pilhas
    * e sobra uma única pilha com um único palito
  – Passo indutivo:
    * Hipótese: $\boldsymbol{P(j)}$ é V, $\forall \boldsymbol{j}$, com $\boldsymbol{1 \leq j \leq k}$
      ("o $\mathbf{2^o}$ jogador pode ganhar se há inicialmente $\boldsymbol{j}$ palitos em cada pilha")
    * Precisamos provar que $\boldsymbol{P(k+1)}$ ("o $\mathbf{2^o}$ jogador pode ganhar se o jogo começar com $\boldsymbol{k+1}$ palitos em cada pilha") é V
    * Suponha que há $\boldsymbol{(k+1)}$ palitos em cada uma das pilhas e que o $\mathbf{1^o}$ jogador remove $\boldsymbol{r}$ palitos ($\boldsymbol{1 \leq r \leq k}$) de uma das pilhas
      · deixando $\boldsymbol{(k+1-r)}$ palitos nesta pilha
    * Se remover o mesmo nro da outra pilha, o $\mathbf{2^o}$ jogador cria a situação onde há duas pilhas com $\boldsymbol{(k+1-r)}$ palitos
    * Uma vez que $\boldsymbol{1 \leq (k+1-r) \leq k}$, o $\mathbf{2^o}$ jogador pode ganhar pela hipótese indutiva.
  – Note que o $\mathbf{1^o}$ jogador perde se remover todos os $\boldsymbol{(k+1)}$ palitos de uma das pilhas

Indução Forte X Fraca

- O exemplo a seguir mostra que alguns resultados podem ser prontamente provados utilizando-se tanto indução simples como indução forte.

- **Exemplo:** Prove que todo valor de postagem de 12 centavos ou mais pode ser formado usando-se somente selos de 4 e de 5 centavos.

  Solução usando indução fraca:

  – Passo básico: 12 centavos = 3 X 4 centavos
  – Passo indutivo:
    * Hipótese: $\boldsymbol{P(k)}$ é V ("valores de $\boldsymbol{k}$ centavos podem ser formados com selos de 4 e 5")
    * A partir disto, como obter valores de $\boldsymbol{k+1}$ centavos?
    * Suponha que pelo menos um selo=4 foi usado para formar $\boldsymbol{k}$:
      · basta substituir este selo por um de 5 para obter $\boldsymbol{k+1}$ centavos
    * Agora, se nenhum selo de 4 foi usado, $\boldsymbol{k}$ é formado só de 5s:
      · foram necessários pelo menos 3 selos de 5 para formar $\boldsymbol{k}$ (pois $\boldsymbol{k \geq 12}$)
      · daí, substituindo-se 3 selos de 5 centavos por 4 selos de 4 centavos, pode-se formar $\boldsymbol{(k+1)}$. $\square$

Solução usando indução forte:

- Passo básico: $P(12),\ P(13),\ P(14)\ e\ P(15)$ são V
- Passo indutivo:
  * Hipótese: $P(j)$ é V para $12 \leq j \leq k$
  * Por esta hipótese, podemos assumir que $P(k-3)$ é V, pois $k-3 \geq 12$
    · ou seja, podemos formar valores de $(k-3)$ centavos utilizando apenas selos de 4 e de 5
  * Para formar $(k+1)$, só precisamos adicionar um selo de 4 aos selos usados para formar $(k-3)$ centavos. $\square$

Leituras sobre Indução forte

- Rosen6: item 4.2

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

5) Recursão

5.1) Definições Recursivas

Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.*

Definições recursivas

- Algumas vezes pode ser difícil definir um objeto explicitamente, mas pode ser fácil defini-lo recursivamente
  - incluindo o item que está sendo definido como parte da definição
- A recursão pode ser usada para definir sequências, funções e conjuntos.
- Exemplo: uma sequência de potências de 2 é dada por:

  $\boldsymbol{a_n = 2^n}$, para $\boldsymbol{n = 0, 1, 2, \ldots}$

  - mas ela também pode ser definida a partir do 1o termo e de uma regra para encontrar um termo da sequência a partir do anterior:

    $\boldsymbol{a_0 = 1}$

    $\boldsymbol{a_{n+1} = 2.a_n}$, para $\boldsymbol{n = 0, 1, 2, ...}$

Definições recursivas de funções

- Quando definimos uma sequência recursivamente, podemos usar indução para provar resultados sobre a sequência.
- Quando definimos um conjunto recursivamente:
  - especificamos alguns elementos iniciais em um passo básico e
  - fornecemos uma regra para construir novos elementos a partir que já temos no passo recursivo.
- A definição recursiva de uma função cujo domínio é o conjunto dos inteiros não-negativos consiste em duas etapas:
  - Passo básico: especificar o valor da função em zero.
  - Passo recursivo: fornecer regra para encontrar o valor da função em um inteiro a partir dos seus valores em inteiros menores.

- Esta definição é chamada de **recursiva** ou de **indutiva**.

- **Exemplo**: Uma f é definida recursivamente por:

$$f(0) = 3$$

$$f(n+1) = 2.f(n) + 3$$

encontre $f(1)$, $f(2)$, $f(3)$ e $f(4)$.

Solução:

$$f(1) = 2.f(0) + 3 = 2.3 + 3 = 9$$
$$f(2) = 2.f(1) + 3 = 2.9 + 3 = 21$$
$$f(3) = 2.f(2) + 3 = 2.21 + 3 = 45$$
$$f(4) = 2.f(3) + 3 = 2.45 + 3 = 93$$

- Muitas funções podem ser estudadas recursivamente.
  - Um bom exemplo é a função fatorial.

- **Exemplo**: Forneça uma definição recursiva para a função fatorial $F(n) = n!$ e use-a para avaliar $5!$

Solução:
$$F(0) = 1$$
$$F(n+1) = (n+1)F(n)$$

Avaliando $F(5)$:

$$F(5) = 5.F(4) = 5.4.F(3) = 5.4.3.F(2) =$$
$$= 5.4.3.2.F(1) = 5.4.3.2.1.F(0) = 5.4.3.2.1.1 = 120$$

Indução & Recursão

- O Princípio da indução matemática garante que funções definidas recursivamente ficam bem definidas:
  - para todo inteiro positivo, o valor da função neste inteiro é determinado de forma não ambígua
  - ou seja, obtemos o mesmo valor qualquer que seja o modo de aplicar as duas partes da definição

- Em algumas definições de funções, os valores da função nos primeiros k inteiros positivos são especificados
  - então é fornecida uma regra para determinar o valor da função em inteiros maiores a partir dos seus valores em alguns ou todos os inteiros que o precedem
  - o princípio da indução forte garante que tais definições produzem funções bem definidas.

- Os Números de Fibonacci, $f_0, f_1, f_2, \ldots$, são definidos por:

$$f_0 = 0, \quad f_1 = 1$$
$$f_n = f_{n-1} + f_{n-2}, \quad \text{para } n = 2, 3, 4, \ldots$$

- **Exemplo:** encontre os números de Fibonacci f_2, f_3, f_4, f_5 e f_6.

$$\begin{aligned}
f_2 &= f_1 + f_0 = 1 + 0 = 1 \\
f_3 &= f_2 + f_1 = 1 + 1 = 2 \\
f_4 &= f_3 + f_2 = 2 + 1 = 3 \\
f_5 &= f_4 + f_3 = 3 + 2 = 5 \\
f_6 &= f_5 + f_4 = 5 + 3 = 8
\end{aligned}$$

- Existe uma conexão natural entre recursão e indução:
  - É comum ser usada uma sequência natural em definições recursivas de objetos.
  - É comum a indução ser o melhor (talvez o único) modo de provar resultados sobre objetos definidos recursivamente.

- Algumas vezes é útil conhecer algumas propriedades de uma relação de recorrência com a qual estamos trabalhando.

- Pode-se usar a definição recursiva dos números de Fibonacci para provar muitas propriedades destes números.

- **Exemplo:** Mostre que, sempre que $n \geq 3$, temos que $f_n > \phi^{n-2}$, onde $\phi = (1 + \sqrt{5})/2$

  Solução: podemos provar esta desigualdade usando indução forte:
  - Seja $P(n)$: "$f_n > \phi^{n-2}$"
  - Queremos provar que $P(n)$ é V sempre que $n \geq 3$.
  - Passo básico:

    $2 = f_3 > \phi$

    $3 = f_4 > \phi^2 = (3 + \sqrt{5})/2$
    - de modo que $P(3)$ e $P(4)$ são ambas V.
  - Passo indutivo:
    - vamos assumir que $P(j)$ é V, ou seja:
      $f_j > \phi^{j-2}$, $\forall j$, com $3 \leq j \leq k$, onde $k \geq 4$
    - (Temos que mostrar que $P(k+1)$ é V, ou seja: $f_{k+1} > \phi^{k-1}$)
    - Como ϕ é solução de $x^2 - x - 1 = 0$, temos: $\phi^2 = \phi + 1$
    - Portanto:

$$\begin{aligned}
\phi^{k-1} &= \phi^2 . \phi^{k-3} \\
&= (\phi + 1)\phi^{k-3} \\
&= \phi \cdot \phi^{k-3} + 1 \cdot \phi^{k-3} \\
&= \phi^{k-2} + \phi^{k-3}
\end{aligned}$$

    - Pela hipótese indutiva, se $k \geq 4$, segue que:
      $f_{k+1} = f_k + f_{k-1} > \phi^{k-2} + \phi^{k-3} = \phi^{k-1}$ $\square$

- **Exemplo:** Outra propriedade dos nros de Fibonacci: $f_n \leq (\frac{5}{3})^n$
  - (um limite superior para a rapidez de crescimento dos nros)

  Prova (por indução forte):

  - Passo básico: $P(1)$ é $1 \leq \frac{5}{3}$, o que, evidentemente, é V.
  - Passo indutivo:
    * usar $P(j)$, $j \leq k$, para $P(k+1)$: "$f_{k+1} \leq (\frac{5}{3})^{k+1}$"
    * $$\begin{aligned} f_{k+1} = f_k + f_{k-1} &\leq (\tfrac{5}{3})^k + (\tfrac{5}{3})^{k-1} \\ &= (\tfrac{5}{3})^{k-1}(\tfrac{5}{3} + 1) \\ &= (\tfrac{5}{3})^{k-1}(\tfrac{8}{3}) \\ &< (\tfrac{5}{3})^{k-1}(\tfrac{5}{3})^2 \\ &= (\tfrac{5}{3})^{k+1} \qquad \square \end{aligned}$$

Definições recursivas de funções

- **Exemplo:** Considere uma definição recursiva da função fatorial:

  $$1! = 1$$

  $$n! = n(n-1)!, \quad n > 1$$

  Queremos provar que: $\forall n \geq 1, \ n! \geq 2^{n-1}$

  Solução: podemos provar esta desigualdade usando indução forte.

  - Seja $P(n)$: "$n! \geq 2^{n-1}$"
  - Passo básico: $P(1)$ é a proposição $1! \geq 2^0$
    * o que é V, já que $1! = 1$
  - Passo indutivo:
    * Queremos provar que $P(k) \Rightarrow P(k+1)$ é uma tautologia.
    * Suponha que $k! \geq 2^{k-1}$, para algum $k \geq 1$
    * Daí, pela definição recursiva, o lado esquerdo de $P(k+1)$ é:
      $$\begin{aligned} (k+1)! &= (k+1)k! \\ &\geq (k+1)2^{k-1} && \text{usando } P(k) \\ &\geq 2 \times 2^{k-1} && k+1 \geq 2, \text{ pois } k \geq 1 \\ &= 2^k && \text{lado direito de } P(k+1) \end{aligned}$$
    * Portanto, $P(k+1)$ é V $\square$

- Definições recursivas de conjuntos também têm duas partes:
  - **Passo básico**: uma coleção inicial de elementos é especificada.
  - **Passo recursivo**: regras para formar novos elementos a partir daqueles que já se sabe que estão no conjunto.

- **Exemplo:** Considere o subconjunto $\boldsymbol{S}$ dos inteiros definido por:
  - Passo básico: $\mathbf{3} \in \boldsymbol{S}$
  - Passo indutivo: se $\boldsymbol{x} \in \boldsymbol{S}$ e $\boldsymbol{y} \in \boldsymbol{S}$, então $\boldsymbol{x} + \boldsymbol{y} \in \boldsymbol{S}$
- Elementos que estão em $\boldsymbol{S}$:
  - 3 (passo básico)
  - aplicando o passo indutivo:
    * $\mathbf{3+3=6}$ (1ra aplicação)
    * $\mathbf{3+6=6+3=9}$ e $\mathbf{6+6=12}$ (2da aplicação)
    * etc...
  - Note que $\boldsymbol{S}$ é o conjunto de todos os múltiplos positivos de 3.

Strings

- Definições recursivas são muito importantes no estudo de strings.

- **String** sobre um alfabeto $\boldsymbol{\Sigma}$: sequência finita de símbolos de $\boldsymbol{\Sigma}$.
- O conjunto $\boldsymbol{\Sigma^*}$, de **strings sobre o alfabeto $\boldsymbol{\Sigma}$** pode ser definido por:
  - **Passo básico**: $\boldsymbol{\lambda} \in \boldsymbol{\Sigma^*}$ (contém a string vazia)
  - **Passo recursivo**: se $\boldsymbol{w} \in \boldsymbol{\Sigma^*}$ e $\boldsymbol{x} \in \boldsymbol{\Sigma}$, então $\boldsymbol{wx} \in \boldsymbol{\Sigma^*}$

- O passo recursivo estabelece que:
  - novas strings são produzidas pela adição de um símbolo de $\boldsymbol{\Sigma}$ ao final das strings já em $\boldsymbol{\Sigma^*}$
  - a cada aplicação do passo recursivo, são geradas strings contendo um símbolo a mais.

- **Exemplo:** se $\boldsymbol{\Sigma = \{0, 1\}}$:
  - $\boldsymbol{\Sigma^*}$ é o conjunto de todas as strings de bits
  - Strings que estão em $\boldsymbol{\Sigma^*}$:
    * $\boldsymbol{\lambda}$
    * 0 e 1 ($\mathbf{1}^{\boldsymbol{a}}$ aplicação do passo recursivo)
    * 00, 01, 10, 11 (após $\mathbf{2}^{\boldsymbol{a}}$ aplicação do passo recursivo)
    * etc...

- Definições recursivas podem ser usadas para definir operações ou funções sobre os elementos de conjuntos definidos recursivamente.
  - Exemplificado na combinação de duas strings mostrada a seguir.

- Sejam:
  - $\boldsymbol{\Sigma}$ um conjunto de símbolos
  - $\boldsymbol{\Sigma^*}$ o conjunto das strings formadas com símbolos de $\boldsymbol{\Sigma}$.
  - A **concatenação** de duas strings $(\cdot)$ é definida como:
    * passo básico: se $\boldsymbol{w \in \Sigma^*}$, então $\boldsymbol{w \cdot \lambda = w}$
    * passo recursivo: se $\boldsymbol{w_1 \in \Sigma^*}$ e $\boldsymbol{w_2 \in \Sigma^*}$ e $\boldsymbol{x \in \Sigma}$, então:
      $\boldsymbol{w_1 \cdot (w_2 x) = (w_1 \cdot w_2) x}$

- Uma aplicação repetida da definição recursiva mostra que a concatenação de duas strings $\boldsymbol{w_1}$ e $\boldsymbol{w_2}$ consiste dos símbolos em $\boldsymbol{w_1}$ seguidos pelos símbolos em $\boldsymbol{w_2}$.

- **Exemplo**: concatenação de $\boldsymbol{ab}$ e $\boldsymbol{cde}$:

$$\boldsymbol{(ab) \cdot (cde) = (ab \cdot cd)e = (ab \cdot c)de = (ab \cdot \lambda)cde = abcde} \qquad \square$$

- **Exemplo:** Forneça uma definição recursiva de $\boldsymbol{l(w)}$, o comprimento de uma string $\boldsymbol{w}$

  Solução: $\boldsymbol{l(\lambda) = 0}$

  se $\boldsymbol{w \in \Sigma^*}$ e $\boldsymbol{x \in \Sigma}$: $\boldsymbol{l(wx) = l(w) + 1}$ $\square$

Fórmulas bem formadas

- Um outro importante exemplo do uso de definições recursivas é na definição "fórmulas bem formadas" (FBFs) de vários tipos.

- **Exemplo**: FBFs para formatos de proposições compostas:
  - envolvem **V**, **F** e:
    * variáveis proposicionais
    * operadores do conjunto: $\boldsymbol{\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}}$
  - e são definidas como:
    * **Passo básico**: **V**, **F**, e $\boldsymbol{p}$ (uma variável proposicional), são fórmulas bem formadas.
    * **Passo recursivo**: se $\boldsymbol{E}$ e $\boldsymbol{F}$ já são fórmulas bem formadas, então também o serão:
      $\boldsymbol{(\neg E)}$, $\boldsymbol{(E \wedge F)}$, $\boldsymbol{(E \vee F)}$, $\boldsymbol{(E \rightarrow F)}$, e $\boldsymbol{(E \leftrightarrow F)}$

- Pelo passo básico, sabemos que:

  V, **F**, $\boldsymbol{p}$ e $\boldsymbol{q}$ são fórmulas bem formadas.

- Após uma aplicação inicial do passo recursivo:

  $\boldsymbol{(p \vee q), (p \rightarrow \mathrm{F}), (\mathrm{F} \rightarrow q)}$ e $\boldsymbol{(q \wedge \mathrm{F})}$ são fórmulas bem formadas

- Uma $\mathbf{2^a}$ aplicação do passo recursivo mostra que são FBFs:

  $((\boldsymbol{p} \vee \boldsymbol{q}) \rightarrow (\boldsymbol{q} \wedge \mathbf{F}))$

  $(\boldsymbol{q} \vee (\boldsymbol{p} \vee \boldsymbol{q}))$

  $((\boldsymbol{p} \rightarrow \mathbf{F}) \rightarrow \mathbf{V})$

- Note que não são fórmulas bem formadas: $\boldsymbol{p}\neg \wedge \boldsymbol{q}$, $\boldsymbol{pq}\wedge$ e $\neg \wedge \boldsymbol{pq}$

- **Exemplo**: FBFs para operadores e operandos:
  - envolvem variáveis, numerais e operadores do conjunto $\{+, -, *, /, \uparrow\}$
  - e são definidas como:
    - **Passo básico**: $\boldsymbol{x}$ é uma FBF se $\boldsymbol{x}$ é um número ou variável.
    - **Passo recursivo**: se $\boldsymbol{F}$ e $\boldsymbol{G}$ já são fórmulas bem formadas, então também o serão: $(\boldsymbol{F} + \boldsymbol{G})$, $(\boldsymbol{F} - \boldsymbol{G})$, $(\boldsymbol{F} * \boldsymbol{G})$, $(\boldsymbol{F}/\boldsymbol{G})$, e $(\boldsymbol{F} \uparrow \boldsymbol{G})$

- Pelo passo básico, sabemos que: $\boldsymbol{x}$, $\boldsymbol{y}$, $\mathbf{0}$ e $\mathbf{3}$ são fórmulas bem formadas.

- FBFs geradas por uma aplicação do passo recursivo incluem:

  $(\boldsymbol{x} + \mathbf{3}),\ (\mathbf{3} + \boldsymbol{y}),\ (\boldsymbol{x} - \boldsymbol{y}),\ (\mathbf{3} - \mathbf{0}),\ (\boldsymbol{x} * \mathbf{3}),\ (\mathbf{3} * \boldsymbol{y})$

  $(\mathbf{3}/\mathbf{0}),\ (\boldsymbol{x}/\boldsymbol{y}),\ (\mathbf{3} \uparrow \boldsymbol{x}),\ (\mathbf{0} \uparrow \mathbf{3})$

- Uma $\mathbf{2^a}$ aplicação do passo recursivo mostra que são FBFs:

  $((\boldsymbol{x} + \mathbf{3}) + \mathbf{3})$ e $(\boldsymbol{x} - (\mathbf{3} * \boldsymbol{y}))$

- Note que não são fórmulas bem formadas: $\boldsymbol{x}\mathbf{3}+$, $\boldsymbol{y} * +\boldsymbol{x}$ e $*\boldsymbol{x}/\boldsymbol{y}$
  - (não podem ser obtidas usando: passo básico + aplicações do recursivo)

Leitura sobre Definições recursivas

- Rosen6: item 4.3

5) Recursão

5.2) Algoritmos Recursivos

Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications"*, 6^{th} *ed., McGraw-Hill, 2007.*

Algoritmos Recursivos

- Um algoritmo **recursivo** resolve um problema reduzindo-o para uma instância do mesmo problema com dados de entrada menores.

- **Exemplo**: Algoritmo para computar $\boldsymbol{mdc(a,b)}$, onde $\boldsymbol{a > b}$, é baseada em:

  $$\boldsymbol{mdc(a,b) = mdc(b, a\, mod\, b)}$$

  – Redução continua até que o menor dos dois seja zero, pois: $\boldsymbol{mdc(b,0) = b}$

  – Algoritmo recursivo:

```
function mdc(a, b)
 if b == 0 then
   return  a
 else
   return  mdc(b, a  mod  b)
```

  – Algoritmo não-recursivo:

```
function mdc(a,b)
  while b ≠ 0
    r = a  mod  b
    a = b
    b = r
  return  a
```

  – Aplicação: $\boldsymbol{mdc(8,5) = mdc(5,3) = mdc(3,2) = mdc(2,1) = mdc(1,0) = 1}$

Complexidade do alg. de Euclides

- O algoritmo de Euclides usa $\boldsymbol{O(log\, b)}$ divisões para obter o mdc dos inteiros positivos $\boldsymbol{a}$ e $\boldsymbol{b}$ (onde $\boldsymbol{a \geq b}$).

  – Nota (princípio do algoritmo): $\boldsymbol{mdc(a,b) = mdc(b, a\, mod\, b)}$

- Para mostrar isto, precisamos do resultado a seguir...

- **Teorema de Lamé:**

  Se $\boldsymbol{a}$ e $\boldsymbol{b}$ são inteiros positivos com $\boldsymbol{a \geq b}$, o nro de divisões usado pelo algoritmo de Euclides para computar $\boldsymbol{mdc(a, b)}$ é $\leq$ a 5 vezes o nro de dígitos decimais em $\boldsymbol{b}$.

  Prova:

  – Seja uma aplicação do algoritmo ($\boldsymbol{a = r_0}$ e $\boldsymbol{b = r_1}$):

  $$\begin{array}{ll} r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2 \\ \quad \cdots & \\ r_{n-2} = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_n q_n & \end{array}$$

  – note que:

  $\boldsymbol{n}$ divisões foram usadas para chegar a $\boldsymbol{r_n = mdc(a, b)}$

  $\boldsymbol{q_1, q_2, \ldots, q_{n-1}}$ são todos $\boldsymbol{\geq 1}$

  $\boldsymbol{q_n \geq 2}$, pois $\boldsymbol{r_n < r_{n-1}}$

  – em uma aplicação do algoritmo:

  $\boldsymbol{n}$ divisões usadas para chegar a $\boldsymbol{r_n = mdc(a, b)}$

  todos os $\boldsymbol{q_i \geq 1}$, mas $\boldsymbol{q_n \geq 2}$ (pois $\boldsymbol{r_n < r_{n-1}}$)

  – o que permite escrever:

  $$\begin{array}{l} r_n \geq 1 = f_2, \\ r_{n-1} \geq 2r_n \geq 2f_2 = f_3, \\ r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4, \\ \qquad \vdots \\ r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n, \\ b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1} \end{array}$$

  – logo, se $\boldsymbol{n}$ divisões são usadas pelo algoritmo, temos que:

  $\boldsymbol{b \geq f_{n+1} > \phi^{n-1}}$ (para $\boldsymbol{n > 2}$)

  $\Rightarrow \boldsymbol{log_{10}\, b > (n-1)/5}$

  $\Rightarrow \boldsymbol{n - 1 < 5 \cdot log_{10}\, b}$

  – agora suponha que $\boldsymbol{b}$ tem $\boldsymbol{k}$ dígitos decimais:

  * então: $\boldsymbol{b < 10^k}$ aonde: $\boldsymbol{k = \lfloor log_{10}\, b \rfloor + 1}$
  * de modo que: $\boldsymbol{log_{10}\, b < k \leq log_{10}\, b + 1}$

  – segue que: $\boldsymbol{n - 1 < 5k \Rightarrow n \leq 5k}$ □

- Voltando à demonstração de que o algoritmo de Euclides utiliza $\boldsymbol{O(log\, b)}$ divisões para encontrar o $\boldsymbol{mdc(a, b)}$:

  – Pelo teorema de Lamé, sabemos que:

  "nro de divisões para obter mdc$\boldsymbol{(a, b) \leq 5(log_{10}\, b + 1)}$"

  – Logo: $\boldsymbol{O(log\, b)}$ divisões são necessárias para obter mdc$\boldsymbol{(a, b)}$ pelo algoritmo de Euclides. □

- **Exemplo:** Algoritmo recursivo para computar $\boldsymbol{a^n}$, onde $\boldsymbol{a}$ é um real não-nulo e $\boldsymbol{n}$ é um inteiro não-negativo
  - Uma solução baseada em definição recursiva de $\boldsymbol{a^n}$:

    condição inicial: $\boldsymbol{a^0 = 1}$

    para $\boldsymbol{n > 0}$: $\boldsymbol{a^{n+1} = a \times a^n}$
  - "Use o passo recursivo até que o expoente fique nulo":

```
function potencia(a, n)
  if n == 0 then
    return  1
  else
    return  a × potencia(a, n-1)
```

- **Exemplo:** Algoritmo recursivo para computar $\boldsymbol{a^n \, mod \, m}$
  - solução *poderia* ser baseada em: $\boldsymbol{a^n \, mod \, m = (a \cdot (a^{n-1} \, mod \, m)) \, mod \, m}$
  - mais eficiente:
    - $\boldsymbol{n}$ par: $\boldsymbol{n = 2 \times (n/2)}$

      $\boldsymbol{a^n \, mod \, m \; = \; (a^{n/2} \; mod \, m)^2 \; mod \, m}$
    - $\boldsymbol{n}$ ímpar: $\boldsymbol{n = 2 \times \lfloor n/2 \rfloor + 1)}$

      $\boldsymbol{a^n \, mod \, m \; = \; (\; (a^{\lfloor n/2 \rfloor} \, mod \, m)^2 \, mod \, m \quad \cdot \quad a^1) \;\; mod \, m}$

```
function mpotencia(a, n, m)}
   if n==0 then
      return 1
   else if n == par then
      return mpotencia(a, n/2, m)^2 mod m
  else
      return (mpotencia(a, floor(n/2), m)^2 mod m x a) mod m
```

ALGORITMO MERGE-SORT

- Uma abordagem comum no projeto de algoritmos é a técnica "Dividir e Conquistar":
  - Divida o problema em alguns subproblemas
  - Conquiste os subproblemas resolvendo-os recursivamente
    - Caso base: se os problemas são pequenos o suficiente, a solução é simples força bruta
  - Combine as soluções dos subproblemas para fornecer uma solução para o problema original

- **Exemplo:** Algoritmo de ordenação Merge-Sort

  Merge-Sort ($A[1..n]$)

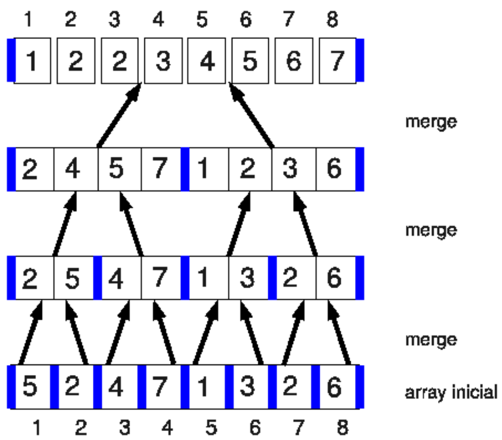
  1) if $n = 1$ feito
  2) ordene *recursivamente*: $A[1..\lceil n/2 \rceil]$ e $A[(\lceil n/2 \rceil + 1)..n]$
  3) "misture" (merge) as duas listas ordenadas

  – Segue à risca o paradigma Dividir e Conquistar
  – Recursão "toca o fundo" quando subarray fica só com um elemento (ordenado trivialmente)

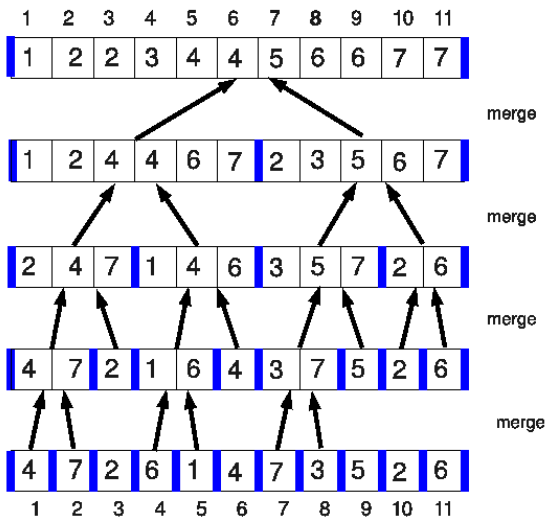
  ```
  MERGE-SORT(A, p, r)
  if p < r                      // testando o caso base
     q = ⌊(p + r)/2⌋            // dividindo
     MERGE-SORT(A, p, q)        // conquistando
     MERGE-SORT(A, q + 1, r)    // conquistando
     MERGE(A, p, q, r)          // combinando
  ```

  – Chamada inicial: Merge-Sort$(A, 1, n)$

- Exemplo: recursão para $n = 8$



- Exemplo: recursão para $n = 11$



- Função chave: MERGE

20	12
13	11
7	9
2	1

  - duas listas pré-ordenadas
  - dois apontadores indicam o menor em cada lista
  - o menor dos apontados vai para o início da nova lista
  - atualiza apontadores e volta ao item anterior

- Operação fundamental: só comparar "apontados" (independente do tamanho do array) $\Rightarrow \boldsymbol{\Theta(n)}$

Função Merge(A, p, q, r)

$n_1 = q - p + 1 \quad , \quad n_2 = r - q$
criar arrays $L[1..n_1 + 1]$ e $R[1..n_2 + 1]$

```
for i = 1 to n1
    L[i] = A[p − 1 + i]
for j = 1 to n2
    R[j] = A[q + j]
L[n1 + 1] = ∞   ,   R[n2 + 1] = ∞

i = j = 1
for k = p to r
    if L[i] ≤ R[j]
        A[k] = L[i]
        i = i + 1
    else
        A[k] = R[j]
        j = j + 1
```

- Tempo do Merge-Sort:

  $O(log\, n)$ níveis de recursão

  $O(n)$ operações para "mesclar" (=combinar) em cada nível

  - Logo: custo $O(n.log\, n)$ para ordenar n elementos

Prova de Algoritmos Recursivos

- Pode-se usar indução para provar que um algoritmo recursivo está correto
  - (ou seja, para provar que ele produz a saída desejada para todas as entradas possíveis)
- Os exemplos a seguir ilustram este recurso...

- **Exemplo:** Prove que está correto o algoritmo que computa a^n:

```
function potencia(a, n)
  if n==0 then
    return  1
  else
    return  a × potencia(a, n-1)
```

Solução: indução sobre o expoente n

- Passo básico: $n = 0 \;\Rightarrow\; potencia(a, 0) = 1$,
  - correto, pois $a^0 = 1$
- Passo indutivo:
  - hipótese: o algoritmo computa $a^k = potencia(a, k)$ corretamente
    - (a partir disto, queremos concluir que ele sempre computa a^{k+1} corretamente)
  - ora, o algoritmo vai computar a^{k+1} como: $a \cdot potencia(a, k)$
  - mas, pela hipótese, $potencia(a, k)$ computa a^k corretamente (sempre)
  - logo, sabemos que sempre vale:
    $potencia(a, k + 1) = a \cdot potencia(a, k) = a \cdot a^k = a^{k+1}$ □

- **Exemplo:** Prove que está correto o algoritmo que computa potenciações modulares:

```
function mpotencia(a, n, m)
  if n==0 then
     return 1
  else if n == par then
      return mpotencia(a, n/2, m)² mod m
   else
      return (mpotencia(a,⌊n/2⌋,m)²  mod  m  ×  a)  mod  m
```

Solução: indução forte sobre o expoente n

- Passo básico: quando $n = 0$, o algoritmo fixa o resultado como 1
  - o que está correto, pois $a^0 \; mod \; m = 1$
- Passo indutivo:
  - hipótese: $mpotencia(a, j, m) = a^j \; mod \; m$, $\; 0 \leq j < k$
    - (se isto está correto, então deve ocorrer: $mpotencia(a, k, m) = a^k \; mod \; m$)
  - se k é par, temos que:
    $$mpotencia(a, k, m) = mpotencia(a, k/2, m)^2 \; mod \; m$$
    $$= (a^{k/2} \; mod \; m)^2 \; mod \; m = a^k \; mod \; m$$
  - se k é ímpar, temos que:
    $$mpotencia(a, k, m) =$$
    $$= ((mpotencia(a, \lfloor k/2 \rfloor, m))^2 \; mod \; m \;\; \cdot \;\; a \; mod \; m) \; mod \; m$$
    $$= ((a^{\lfloor k/2 \rfloor} \; mod \; m)^2 \; mod \; m \;\; \cdot \;\; a \; mod \; m) \; mod \; m$$
    $$= a^{2\lfloor k/2 \rfloor + 1} \; mod \; m = a^k \; mod \; m \qquad \square$$

Leituras sobre Algoritmos Recursivos

- Rosen6: item 4.4

INE5403 - Fundamentos de Matemática Discreta para a Computação

6) Relações

6.1) Definição e Representação

6.2) Caminhos em Relações e Digrafos

6.3) Propriedades de Relações

6.4) Relações de Equivalência

6.5) Manipulação e Fecho de Relações

Relações

- Ligações entre elementos de conjuntos são representadas utilizando uma estrutura chamada *relação*.

- Relações podem ser usadas para:
  - Determinar quais pares de cidades são ligadas por linhas aéreas em uma rede
  - Busca de uma ordem viável para as diferentes fases de um projeto
  - Elaboração de um modo útil de armazenar informação em bancos de dados computacionais

Relações

Def: Um par ordenado (a,b) é uma lista de objetos a e b em uma ordem estabelecida, com a aparecendo em primeiro e b em segundo.

- dois pares ordenados (a_1,b_1) são ditos iguais (a_2,b_2) se e somente se $a_1=a_2$ e $b_1=b_2$.

Def: Se A e B são dois conjuntos não-vazios, define-se o produto cartesiano $A\times B$ como o conjunto de *todos* os pares ordenados (a,b), com $a\in A$ e $b\in B$:

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

Exemplo: $A=\{1,2,3\}$ e $B=\{r,s\}$

$A\times B = \{(1,r),(1,s),(2,r),(2,s),(3,r),(3,s)\}$

Relações

- Para quaisquer conjuntos finitos não-vazios A e B, temos:

$|A\times B| = |A|.|B|$

Relações

Def: Sejam A e B conjuntos. Uma *relação binária* R de A em B é um subconjunto de $A\times B$.

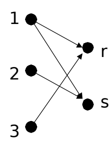
- Ou: um conjunto R de pares ordenados, onde o 1º elemento de cada par vem de A e o 2º vem de B,
  - ou seja, $R \subseteq A\times B$

- Quando $(a,b) \in R$, diz-se que *a está relacionado com b* por R.
- Usa-se a notação *a R b* para denotar que $(a,b)\in R$.
- Se a não está relacionado com b por R, escreve-se $a \not R\, b$.
- Relações binárias representam ligações entre elementos de 2 conjuntos
  - vamos omitir a palavra "binária"

Relações

Exemplo: Sejam $A=\{1,2,3\}$ e $B=\{r,s\}$.

- $R=\{(1,r),(1,s),(2,s),(3,r)\}$ é uma relação de A em B.
- Pode-se dizer: 1 R r, 1 R s, 2 R s, 3 R r
- Mas: $3 \not R\, s$
- Esta relação também pode ser representada por:



R	r	s
1	×	×
2		×
3	×	

Relações

Exemplo: Seja A=B={1,2,3,4,5}. Define-se a relação R (menor do que) sobre A como:

- a R b se e somente se a<b.
- Neste caso: R={(1,2),(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5),(4,5)}

Exemplo: Seja A o conjunto de todas as cidades e seja B o conjunto dos 3 estados da região sul do Brasil.

- (a,b) $\in$ R se a cidade a está no estado b
- Por exemplo, (Florianópolis, SC), (Maringá, PR), (Curitiba,PR) e (Porto Alegre,RS) estão em R.

Relações

- O que realmente importa em uma relação é que nós saibamos precisamente quais elementos em A estão relacionados a quais elementos em B.

Exemplo: A={1,2,3,4} e R é uma relação de A em A.

- Se sabemos que 1R2, 1R3, 1R4, 2R3, 2R4 e 3R4, então sabemos tudo que é preciso saber sobre R
- Na verdade, R é a relação < (menor do que), mas isto nós não precisamos saber: a lista é suficiente.
- R é completamente determinada pela lista de pares

Relações sobre um conjunto

Def: Uma *relação sobre o conjunto A* é uma relação de A para A.

- ou seja, é um subconjunto de A×A

Exemplo: Seja A o conjunto {1,2,3,4}. Quais pares ordenados estão na relação R={(a,b) | a divide b}?

R={(1,1),(1,2),(1,3),(1,4),(2,2),(2,4),(3,3),(4,4)}

Note que:

A×A={(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(3,3),(3,4),(4,1),(4,2),(4,3),(4,4)}

Relações sobre um conjunto

Exemplo: Considere as seguintes relações sobre o conjunto dos inteiros:

R_1 = { (a,b) | a $\le$ b }
R_2 = { (a,b) | a > b }
R_3 = { (a,b) | a = b ou a = -b }
R_4 = { (a,b) | a = b }
R_5 = { (a,b) | a = b+1 }
R_6 = { (a,b) | a+b $\le$ 3 }

Quais destas relações contêm: (1,1),(1,2),(2,1),(1,-1) e (2,2)?

Resp.: (1,1) está em R_1, R_3, R_4 e R_6
(1,2) está em R_1 e R_6
(2,1) está em R_2, R_5 e R_6
(1,-1) está em R_2, R_3 e R_6
(2,2) está em R_1, R_3 e R_4

Relações sobre um conjunto

- Quantas relações podem ser construídas sobre um conjunto com n elementos?
  - Uma relação sobre A é um subconjunto de A×A
  - A×A tem n^2 elementos
  - Um conjunto com m elementos tem 2^m subconjuntos
  - Logo, há 2^{n^2} subconjuntos de A×A
  - O que significa que há 2^{n^2} relações possíveis sobre um conjunto com n elementos.

Conjuntos originados de relações

Def: Seja R $\subseteq$ A×B uma relação de A em B. Então:

a) ***Domínio*** de R, denotado por Dom(R):
- Conjunto dos elementos em A que estão relacionados com algum elemento em B
- ou: Dom(R) é o subconjunto de A formado por todos os primeiros elementos nos pares que aparecem em R

b) ***Imagem*** de R, denotado por Im(R):
- Conjunto dos elementos em B que são segundos elementos de pares de R
- ou: conjunto de todos os elementos em B que são relacionados a algum elemento em A

- elementos de A que não estão em Dom(R) não estão envolvidos na relação R de modo algum
- idem para elementos de B que não estão em Im(R)

Conjuntos originados de relações

Exemplo: Se R é a relação sobre A={1,2,3,4,5} dada por a R b se e somente se a<b, então:

Dom(R) = {1,2,3,4}

Im(R) = {2,3,4,5}

Nota: R = {(1,2),(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5),(4,5)}

Conjuntos originados de relações

Def: Se x∈A, define-se o conjunto R(x) dos *R-relativos de x* como sendo o conjunto de todos os y em B com a propriedade de que x está relacionado a y por R (x R y).

- ou: R(x) = { y ∈ B | x R y }

Def: se $A_1 \subseteq A$, então $R(A_1)$, o conjunto dos *R-relativos de A_1* é o conjunto de todos os y em B com a propriedade de que x está relacionado a y por R com $x \in A_1$.

- ou: $R(A_1) = \{ y \in B \mid x \, R \, y \text{ para algum } x \in A_1 \}$

- ou ainda: união dos conjuntos R(x), onde $x \in A_1$

Conjuntos R-relativos

Exemplo: Seja A=B={a,b,c,d} e seja R={(a,a),(a,b),(b,c),(c,a),(d,c),(c,b)}
Então:

R(a) = {a,b}

R(b) = {c}

se A_1={c,d}, então $R(A_1)$={a,b,c}

Dom(R) = {a,b,c,d}

Im(R) = {a,b,c}

Conjuntos originados de relações

- Note que os conjuntos R(a), para a em A, determinam completamente uma relação R.

- **Teorema**: Sejam R e S relações de A em B. Se R(a)=S(a) para todo a∈A, então R=S.

  Prova:

- Se a R b, então b∈R(a). Portanto, b∈S(a) e a S b. (R⊆S)
- Se a S b, então b∈S(a). Portanto, b∈R(a) e a R b. (S⊆R)
- Logo, R=S

Representando relações

- Há muitas maneiras de representar uma relação entre conjuntos finitos.
- Uma maneira é listar os pares ordenados.
- Também se pode usar:
  - matrizes de zeros e 1's
  - grafos direcionados (digrafos)

Matrizes de relações

Def: Se $A=\{a_1,a_2,\ldots,a_m\}$ e $B=\{b_1,b_2,\ldots,b_n\}$ são conjuntos finitos e R é uma relação de A em B, então R pode ser representada pela matriz $m \times n$ $M_R=[m_{ij}]$, definida como:

$$m_{i,j} = \begin{cases} 1 & se \quad (a_i, b_j) \in R \\ 0 & se \quad (a_i, b_j) \notin R \end{cases}$$

- M_R é denominada de *matriz de R*

Exemplo: Sejam A={1,2,3} e B={r,s} e a relação R de A em B dada por R={(1,r),(2,s),(3,r)}. Então a matriz M_R de R é:

$$M_{R(3\times 2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Matrizes de relações

Exemplo: Defina a relação representada pela matriz:

$$M=\begin{bmatrix}1&0&0&1\\0&1&1&0\\1&0&1&0\end{bmatrix}$$

Solução: Como M é 3×4, fazemos:

$A=\{a_1,a_2,a_3\}$ e $B=\{b_1,b_2,b_3,b_4\}$

- Então, como $(a_i,b_j)\in R$ se e somente se $m_{ij}=1$, temos:

$R=\{(a_1,b_1),(a_1,b_4),(a_2,b_2),(a_2,b_3),(a_3,b_1),(a_3,b_3)\}$

Representação de relações com digrafos

- **Def**: Se A é um conjunto finito e R é uma relação sobre A, então R pode ser representada graficamente como segue:
  - desenhe um pequeno círculo para cada elemento de A e o nomeie com o correspondente elemento de A → *vértices*
  - desenhe uma linha orientada, chamada de *aresta*, do vértice a_i para o vértice a_j se $(a_i,a_j)\in R$

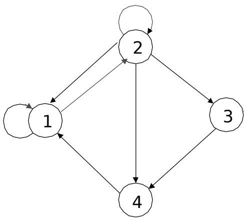
  A representação gráfica que resulta é chamada de “grafo direcionado” ou *digrafo* de R.

- Se R é uma relação sobre A, as arestas do dígrafo de R correspondem exatamente aos pares em R e os vértices correspondem aos elementos do conjunto A.

Representação de relações com digrafos

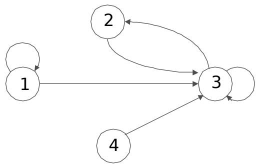
Exemplo: Sejam A={1,2,3,4} e
R={(1,1),(1,2),(2,1),(2,2),(2,3),(2,4),(3,4),(4,1)}

- O digrafo de R é:



Representação de relações com digrafos

Exemplo: Encontre a relação determinada pela figura abaixo:



Solução:

R={(1,1),(1,3),(2,3),(3,2),(3,3),(4,3)}

Representação de relações com digrafos

- Note que digrafos nada mais são do que representações geométricas de relações.

⇒ qualquer afirmação feita a respeito de um digrafo é na verdade uma afirmação sobre a relação correspondente

- Isto é especialmente importante para teoremas sobre relações e suas provas:
  - frequentemente é mais fácil ou mais claro estabelecer um resultado em termos gráficos
  - mas a prova vai sempre estar ligada à relação associada

Leituras sobre Relações e digrafos

- Kolman5: seções 4.1 e 4.2
- Rosen6: seções 8.1 e 8.3

INE5403 - Fundamentos de Matemática Discreta para a Computação

6) Relações

- 6.1) Definição e Representação
- 6.2) Caminhos em Relações e Digrafos
- 6.3) Propriedades de Relações
- 6.4) Relações de Equivalência
- 6.5) Manipulação e Fecho de Relações

Relações

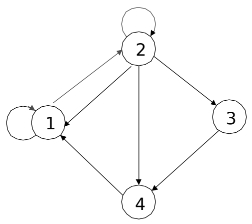
Definição: Sejam A e B conjuntos. Uma *relação binária* R de A em B é um subconjunto de $A \times B$.

- Ou: um conjunto R de pares ordenados, onde o 1º elemento de cada par vem de A e o 2º vem de B, ou seja, $R \subseteq A \times B$.
- Se $(a,b) \in R$, diz-se que *a está relacionado com b* por R.
- Usa-se a notação *a R b* para denotar que $(a,b) \in R$.

Representação de relações usando digrafos

Exemplo: Sejam A={1,2,3,4} e
R={(1,1),(1,2),(2,1),(2,2),(2,3),(2,4),(3,4),(4,1)}

- O digrafo de R é:



Caminhos em relações e digrafos

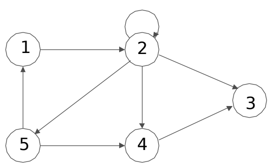
Def.: Seja R uma relação sobre o conjunto A. Um *caminho de comprimento n* em R de a para b é uma seqüência finita $\pi = a, x_1, x_2, \ldots, x_{n-1}, b$ tal que:

$$a\ R\ x_1,\ x_1\ R\ x_2,\ \ldots\ ,\ x_{n-1}\ R\ b$$

- Um caminho de comprimento n envolve n+1 elementos de A (não necessariamente distintos).
- O modo mais fácil de visualizar um caminho é com o digrafo de uma relação: sucessão de arestas, seguindo os sentidos indicados.

Caminhos em relações e digrafos

Exemplo: Considere o digrafo:



Então:

π_1 = 1,2,5,4,3 é um caminho de comprimento 4 de 1 a 3

π_2 = 1,2,5,1 é caminho de comprimento 3 do vért. 1 para ele mesmo

π_3 = 2,2 é caminho de comprimento 1 do vértice 2 para ele mesmo

Caminhos em relações e digrafos

- Um caminho que começa e termina no mesmo vértice é chamado de um <u>ciclo</u> (π_2 e π_3 são ciclos)
- Caminhos de comprimento 1 são identificados pelos pares ordenados (x,y) que pertencem a R

Caminhos em relações e digrafos

- Caminhos em relações R podem ser usados para definir novas relações bastante úteis

Def: (relação R^n sobre A)
x R^n y significa que há um *caminho de comprimento n* de x até y em R.

Def: (relação R^∞ sobre A)
x R^∞ y significa que há algum caminho em R de x até y.
(R^∞ é chamada de *relação de conectividade* para R)

Caminhos em relações e digrafos

- $R^n(x)$: todos os vértices que podem ser alcançados a partir de x por meio de um caminho em R de comprimento n.
- $R^\infty(x)$: todos os vértices que podem ser alcançados a partir de x por meio de *algum* caminho em R.

Exemplo1: Seja A o conjunto de todos os seres humanos vivos e seja R a relação “conhecimento mútuo” (a R b se a e b se conhecem). Então:

- a R^2 b significa que a e b têm um conhecido em comum.
- Em geral, *a* R^n *b* se *a* conhece alguém (x_1), que conhece x_2, ..., que conhece x_{n-1}, que conhece *b*.
- Finalmente, a R^∞ b significa que existe alguma lista encadeada de conhecidos que começa em a e termina em b.
- Será que toda dupla de brasileiros está relacionada por R^∞?

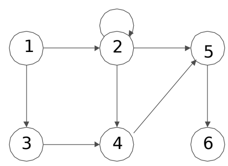
Caminhos em relações e digrafos

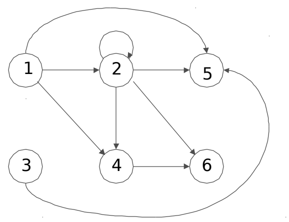
Exemplo2: Seja A o conjunto de cidades brasileiras, e seja x R y se há algum vôo direto (de alguma cia aérea) de x para y.

- x e y estão relacionados por R^n se for possível agendar um vôo de x para y com exatamente n-1 paradas intermediárias
- x R^∞ y se for possível ir de avião de x para y.

Caminhos em relações e digrafos

Exemplo3: Seja A={1,2,3,4,5,6} e sejam os digrafos das relações R e R^2 sobre A dados por:





Caminhos em relações e digrafos

Exemplo3 (cont.):

- Uma linha conecta 2 vértices no dígrafo para R_2 somente se existir um caminho de comprimento 2 conectando os mesmos vértices no digrafo para R_1.
- Portanto:

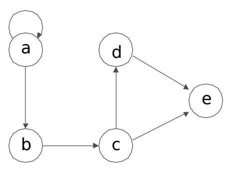
  1 R^2 2 porque 1 R 2 e 2 R 2
  1 R^2 4 porque 1 R 2 e 2 R 4
  1 R^2 5 porque 1 R 2 e 2 R 5
  2 R^2 2 porque 2 R 2 e 2 R 2
  e assim sucessivamente.

- De modo similar, podemos construir o digrafo de R^n para qualquer n.

Caminhos em relações e digrafos

Exemplo4: Sejam A={a,b,c,d,e} e
R={(a,a),(a,b),(b,c),(c,e),(c,d),(d,e)}.
Compute (a) R^2 (b) R^∞

Solução: o digrafo de R é dado por:



(a) Portanto: R^2 = {(a,a),(a,b),(a,c),(b,e),(b,d),(c,e)}

Caminhos em relações e digrafos

Exemplo4 (cont.):

(b) R^∞ = "todos os pares ordenados de vértices para os quais há um caminho de qualquer comprimento do primeiro vértice para o segundo"

ou seja:

R^∞ = {(a,a),(a,b),(a,c),(a,d),(a,e),(b,c),(b,d),(b,e),(c,d),(c,e),(d,e)}

- Por exemplo, $(a,d)\in R^\infty$, já que há um caminho de comprimento 3 de a para d: "a,b,c,d".
- $(a,e)\in R^\infty$, já que há um caminho de comprimento 3 de a para e: "a,b,c,e" (assim como "a,b,c,d,e")

Produto booleano

Exemplo: Encontre o produto booleano de A e B, onde:

$$A=\begin{bmatrix}1&0\\0&1\\1&0\end{bmatrix} \qquad B=\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix}$$

$$A\otimes B=\begin{bmatrix}(1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1) & (1\wedge0)\vee(0\wedge1)\\(0\wedge1)\vee(1\wedge0) & (0\wedge1)\vee(1\wedge1) & (0\wedge0)\vee(1\wedge1)\\(1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1) & (1\wedge0)\vee(0\wedge1)\end{bmatrix}$$

$$A\otimes B=\begin{bmatrix}1\vee0 & 1\vee0 & 0\vee0\\0\vee0 & 0\vee1 & 0\vee1\\1\vee0 & 1\vee0 & 0\vee0\end{bmatrix}$$

Caminhos em relações e matrizes

Exemplo: Sejam A e R como no exemplo anterior. Então:

$$M_R=\begin{bmatrix}1&1&0&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\\0&0&0&0&0\end{bmatrix}$$

1 = $(0\wedge0)\vee(0\wedge0)\vee(1\wedge1)\vee(0\wedge0)\vee(0\wedge0)$

(2,4)

$$\Rightarrow M_{R^2}=M_R\otimes M_R=\begin{bmatrix}1&1&0&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\\0&0&0&0&0\end{bmatrix}\otimes\begin{bmatrix}1&1&0&0&0\\0&0&1&0&0\\0&0&0&1&1\\0&0&0&0&1\\0&0&0&0&0\end{bmatrix}=\begin{bmatrix}1&1&1&0&0\\0&0&0&\boxed{1}&1\\0&0&0&0&1\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}$$

Caminhos em relações e matrizes

- Seja R uma relação sobre A={$a_1,a_2,\ldots,a_n$} e seja M_R uma matriz $n\times n$ representando R.

Teorema: Se R é uma relação sobre A={$a_1,a_2,\ldots,a_n$} então:

$$M_{R^2}=M_R\otimes M_R$$

Prova:

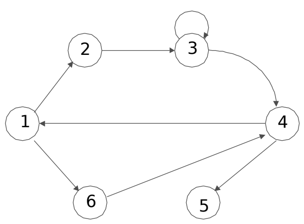
- Seja $M_R=[m_{ij}]$ and $M_{R^2}=[n_{ij}]$;
- o elemento n_{ij} de $M_R\otimes M_R$ será 1 se a *linha i* do 1º M_R e a *coluna j* do 2º M_R tiverem um 1 na mesma posição relativa (digamos **k**)
  - ou: $n_{ij}=1$ se $m_{ik}=1$ e $m_{kj}=1$ para algum **k**
    $\Rightarrow$ se $n_{ij}=1$, então: $a_i\,R\,a_k$ e $a_k\,R\,a_j$
- portanto, $n_{ij}=1 \Rightarrow a_i\,R^2\,a_j$.

- Esta idéia pode ser generalizada:

Teorema: Para $n\geq2$ e para uma relação R sobre A, temos:

$$M_{R^n}=M_R\otimes M_R\otimes\ldots\otimes M_R \quad \text{(n fatores)}$$

- Exercício: Para a relação R cujo digrafo é dado abaixo,
  a) Desenhe os digrafos de R^2 e R^∞
  b) Encontre M_{R^2} e M_{R^∞}



Leituras sobre Caminhos em Relações

- Kolman5: seção 4.3
- Rosen6: seção 8.1

INE5403 - Fundamentos de Matemática Discreta para a Computação

6) Relações

6.1) Definição e Representação

6.2) Caminhos em Relações e Digrafos

6.3) Propriedades de Relações

6.4) Relações de Equivalência

6.5) Manipulação e Fecho de Relações

Propriedades de relações

- Considere relações sobre um conjunto A:

Definição: (Reflexividade)

- Uma relação R sobre um conjunto A é dita *reflexiva* se $(a,a) \in R$ para todo $a \in A$,
  - ou seja, se aRa para todo $a \in A$.
- R sobre A é *irreflexiva* se $(a,a) \notin R$ para todo $a \in A$

Propriedades de relações (reflexividade)

Exemplos:

a) $\Delta = \{ (a,a) \mid a \in A\}$: relação de igualdade sobre A
Por definição, $(a,a) \in \Delta$, $\forall a \in A$.

b) $R = \{ (a,b) \in A \times A \mid a \neq b\}$
Irreflexiva pois $(a,a) \notin R$, $\forall a \in A$.

c) Seja $A = \{1,2,3\}$ e $R=\{(1,1),(1,2)\}$. Então:
R não é reflexiva pois $(2,2) \notin R$
R não é irreflexiva pois $(1,1) \in R$

Propriedades de relações (reflexividade)

Exemplo: Quais das relações a seguir são reflexivas?

$R_1 = \{ (a,b) \mid a \leq b \}$
$R_2 = \{ (a,b) \mid a > b \}$
$R_3 = \{ (a,b) \mid a = b \text{ ou } a = -b \}$
$R_4 = \{ (a,b) \mid a = b \}$
$R_5 = \{ (a,b) \mid a = b+1 \}$
$R_6 = \{ (a,b) \mid a+b \leq 3 \}$

<u>Resposta</u>:

- R_1: pois $a \leq a$ para todo inteiro a
- R_3 e R_4
- Para cada um dos outros casos, pode-se encontrar um par da forma (a,a) que não está na relação.

Propriedades de relações (reflexividade)

Caracterização de reflexividade e irreflexividade:

1. Matrizes:
   - R reflexiva $\Rightarrow$ a matriz M_R possui todos os elementos da diagonal principal iguais a 1
   - R irreflexiva $\Rightarrow$ a matriz M_R possui todos os elementos da diagonal principal iguais a 0
2. Digrafos:
   - R reflexiva $\Rightarrow$ para todos os vértices do digrafo existem arestas que ligam o vértice a ele mesmo
   - R irreflexiva $\Rightarrow$ para todos os vértices do digrafo não existem arestas que ligam o vértice a ele mesmo

- Note que, se R sobre A é reflexiva: Dom(R) = Im(R) = A

Propriedades de relações - simetria

Def.: Uma relação R sobre um conjunto A é dita *simétrica* se *sempre* que $(a,b) \in R$, então também $(b,a) \in R$.

- segue que R sobre A é uma relação *não-simétrica* se para algum $a,b \in A$ for verificado que $(a,b) \in R$ e $(b,a) \notin R$

Def.: Uma relação R sobre um conjunto A é dita *assimétrica* se *sempre* que $(a,b) \in R$, então $(b,a) \notin R$.

- uma relação R sobre A é *não-assimétrica* se para *algum* $a,b \in A$ for verificado que $(a,b) \in R$ e $(b,a) \in R$.

Def.: Uma relação R sobre um conjunto A é dita *antissimétrica* se *sempre* que $(a,b) \in R$ e $(b,a) \in R$, então a=b.

- equivalentemente, se $a \neq b$, então $(a,b) \notin R$ ou $(b,a) \notin R$
- uma relação R sobre A é *não-antissimétrica* se existir $a,b \in A$ com $a \neq b$ e tanto $(a,b) \in R$ como $(b,a) \in R$.

Propriedades de relações

- **Lembrete**: escrever $(a,b) \in R$ é equivalente a escrever aRb ("a está relacionado com b por R")
- **Obs**: para verificar se estas propriedades são ***válidas ou não*** para uma certa relação R, deve-se notar que:

1. Uma propriedade *não é válida* se puder ser encontrada uma situação onde ela não pode ser verificada

2. Se não houver situação em que a propriedade *falha*, deve-se concluir que a propriedade é válida

Propriedades de relações - exemplos

Exemplo 1: Seja A=Z (o conjunto dos inteiros) e seja R a relação $R=\{(a,b)\in A\times A \mid a \geq b\}$. Determine se R é simétrica, assimétrica ou antissimétrica.

Solução:

- simetria: se $a\geq b$, então não é sempre verdade que $b\geq a$ (exemplo: $2 \geq 1$ mas $1 < 2$) $\Rightarrow$ R é não-simétrica
- assimetria: R é não-assimétrica pois se a=2 e b=2 temos aRb e bRa
- antissimetria: R é antissimétrica pois $a\geq b$ e $b\geq a \Rightarrow a=b$

Propriedades de relações - exemplos

Exemplo 2: Seja A={1,2,3,4} e seja a relação:
R={(1,2),(2,2),(3,4),(4,1)}
Determine se R é simétrica, assimétrica ou antissimétrica

Solução:

- simetria: R é não-simétrica, pois, por exemplo, 1R2 e $2\not R1$
- assimetria: R é não-assimétrica pois $(2,2) \in R$
- antissimetria: R é antissimétrica pois se $a\neq b$, então ou $(a,b)\notin R$ ou $(b,a)\notin R$.

Propriedades de relações - exemplos

Exemplo 3: Seja A= Z^+ (inteiros positivos) e seja
$R = \{ (a,b)\in A\times A \mid a|b\}$ (a divide b)
Determine se R é simétrica, assimétrica ou antissimétrica

Solução:

- simetria: a|b não implica que b|a, então R é não-simétrica.
- assimetria: se a=b=5, por exemplo, então aRb e bRa. Assim, R é não-assimétrica.
- antissimetria: se a|b e b|a, então a=b, de modo que R é antissimétrica.

Propriedades de relações - exemplos

Ex. 4: Quais das relações a seguir são simétricas e quais são antissimétricas?

$R_1 = \{ (a,b) \mid a \leq b \}$
$R_2 = \{ (a,b) \mid a > b \}$
$R_3 = \{ (a,b) \mid a = b \text{ ou } a = -b \}$
$R_4 = \{ (a,b) \mid a = b \}$
$R_5 = \{ (a,b) \mid a = b+1 \}$
$R_6 = \{ (a,b) \mid a+b \leq 3 \}$

- R_3 é simétrica: se a=b ou a=-b, então b=a ou b=-a.
- R_4 é simétrica: $a=b \Rightarrow b=a$.
- R_6 é simétrica: $a+b\leq 3 \Rightarrow b+a\leq 3$.
- R_1 é antissimétrica: $a \leq b$ e $b \leq a \Rightarrow b=a$.
- R_2 é antissimétrica: é impossível a>b e b>a.
- R_4 é antissimétrica pela definição.
- R_5 é antissimétrica: impossível ter a=b+1 e b=a+1.

Caracterização de simetria, assimetria e antissimetria através da matriz de relação

- **Simetria**: A matriz $M_R=[m_{ij}]$ de uma relação simétrica satisfaz à propriedade:
  $m_{ij}=1 \Rightarrow m_{ji}=1$
  $m_{ij}=0 \Rightarrow m_{ji}=0$
  - Tem-se que $m_{ij}=m_{ji}$, ou seja, R é simétrica sse se $M_R=(M_R)^t$
- **Assimetria**: A matriz $M_R=[m_{ij}]$ de uma relação assimétrica satisfaz:
  $m_{ij}=1 \Rightarrow m_{ji}=0$
  Logo, se R é assimétrica, segue que $m_{ii}=0$ para todo i.
- **Antissimetria**: A matriz $M_R=[m_{ij}]$ de uma relação antissimétrica satisfaz:
  se $i\neq j$ então $m_{ij}=0$ ou $m_{ji}=0$

Propriedades de relações com matrizes

- **Exemplo1**:

$$M_{R1}=\begin{bmatrix}1&0&1\\0&0&1\\1&1&1\end{bmatrix}\quad M_{R2}=\begin{bmatrix}0&1&1&0\\1&1&0&0\\1&0&1&1\\0&0&1&1\end{bmatrix}\quad M_{R3}=\begin{bmatrix}1&1&1\\0&1&0\\0&0&0\end{bmatrix}$$

$$M_{R4}=\begin{bmatrix}0&0&1&1\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}\quad M_{R5}=\begin{bmatrix}1&0&0&1\\0&1&1&1\\0&0&1&0\\0&0&0&1\end{bmatrix}\quad M_{R6}=\begin{bmatrix}0&1&0&1\\0&0&1&1\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

Propriedades de relações - transitividade

- **Def**: Uma relação R sobre um conjunto A é dita transitiva se, sempre que a R b e b R c, então a R c.

- Por outro lado, R sobre A é uma relação **não-transitiva** se existir a, b e c em A tais que a R b e b R c, mas a $\not R$ c.
- se tais a, b e c não existirem, então R é ***transitiva***.

Propriedades de relações - transitividade

- Exemplo1: Seja A=Z+ e R={ (a,b) ∈ A×A | a|b } ("a divide b"). A relação R é transitiva?

Solução: suponha que a R b e que b R c, de modo que a|b e b|c. Então a|c, o que significa que a R c. Logo, R é transitiva.

- Exemplo2: A relação R={(1,2),(1,3),(4,2)} sobre A={1,2,3,4} é transitiva?
- Solução: como não é possível encontrar elementos a, b e c tais que (a,b)∈R, (b,c)∈R, mas (a,c)∉R, *R é transitiva*

Caracterização de relações transitivas por matrizes

- Se $M_R=[m_{ij}]$ é a matriz de uma relação transitiva R, então M_R satisfaz à propriedade:

  se $m_{ij}=1$ e $m_{jk}=1$, então $m_{ik}=1$

- a transitividade de R significa que se ($M_R \otimes M_R$) tem um 1 em qualquer posição, então M_R deve ter um 1 na mesma posição (o converso pode ser falso)

- ou seja: $M_R \otimes M_R \leq M_R$

Caracterização de relações transitivas por matrizes

- Exemplo: Mostre que a relação R sobre A={1,2,3} dada abaixo é transitiva:

$$M_R=\begin{bmatrix}1&1&1\\0&0&1\\0&0&1\end{bmatrix}$$

- Solução: Por cálculo direto, $M_R \otimes M_R = M_R$, de modo que R é transitiva.

Propriedades de relações - Exercícios

- Exerc1: Determine se as relações abaixo são reflexivas, irreflexivas, simétricas, assimétricas, antissimétricas ou transitivas:

  a) R={(1,3),(1,1),(3,1),(1,2),(3,3),(4,4)}

  b) R={(1,1),(1,2),(2,1),(2,2),(3,3),(3,4),(4,3),(4,4)}

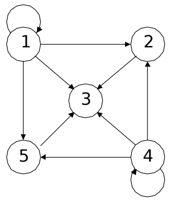
- Respostas:

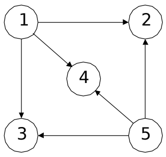
  a) N, N, N, N, N, N

  b) S, N, S, N, N, S

Propriedades de relações - Exercícios

- Exerc2: Seja A={1,2,3,4,5}. Determine se as relações definidas pelos digrafos abaixo são reflexivas, irreflexivas, simétricas, assimétricas, antissimétricas ou transitivas.





Resp. (a): N, N, N, N, S, S   Resp. (b): ?

Leituras sobre Propriedades de Relações

- Kolman5: seção 4.4
- Rosen6: seção 8.1

INE5403 - Fundamentos de Matemática Discreta para a Computação

6) Relações

6.1) Definição e Representação

6.2) Caminhos em Relações e Digrafos

6.3) Propriedades de Relações

6.4) Relações de Equivalência

6.5) Manipulação e Fecho de Relações

Relações de equivalência

- Ex.1: Suponha que a matrícula dos estudantes em uma dada universidade siga o esquema:

Inicial do nome :	Horário de matrícula :
A – G	8 :00 – 11 :00
H – N	11 :00 – 14 :00
O – Z	14 :00 – 17 :00

- Seja R a relação que contém (x,y) se x e y são estudantes com nomes começando com letras do mesmo bloco.
- Consequentemente, x e y podem se matricular na mesma hora sse $(x,y)\in R$

Relações de equivalência

- Ex.1: Esquema de matrícula:

Inicial do nome :	Horário de matrícula :
A – G	8 :00 – 11 :00
H – N	11 :00 – 14 :00
O – Z	14 :00 – 17 :00

- Seja R a relação que contém (x,y) se x e y são estudantes com nomes começando com letras do mesmo bloco
- x e y podem se matricular na mesma hora sse $(x,y)\in R$
- Pode-se notar que R é reflexiva, simétrica e transitiva.
- Além disto, R divide os estudantes em 3 classes (*equivalentes*)

Relações de equivalência

- Ex.2: dois horários (inteiros) a=20:00 e b=68:00 estão relacionados pela relação "congruência módulo 24", pois:

  $24 \mid (68-20)$ ou $68=20 + k.24$

- "Um inteiro a está relacionado a um inteiro b se ambos tiverem o mesmo resto quando divididos por 24"
  - pode-se mostrar que esta relação é reflexiva, simétrica e transitiva
- Esta relação subdivide o conjunto dos inteiros em 24 classes diferentes.
- Como o que nos interessa realmente é só o momento do dia, só precisamos saber a que *classe* pertence um valor dado.

Relações de equivalência

- Uma relação R sobre um conjunto A é chamada uma *relação de equivalência* se ela for uma relação reflexiva, simétrica e transitiva.
- Dois elementos relacionados por uma relação de equivalência são ditos *equivalentes*.

Relações de equivalência

- **Exemplo1**: Sejam A={1,2,3,4} e
  R={(1,1),(1,2),(2,1),(2,2),(3,4),(4,3),(3,3),(4,4)}.

  R é de equivalência, pois satisfaz às 3 propriedades:

  - Reflexividade: $\{(1,1),(2,2),(3,3),(4,4)\}\subseteq R$
  - Simetria: nota-se que $a\in R(b) \Leftrightarrow b\in R(a)$
  - Transitividade: nota-se que:
    $b\in R(a)$ e $c\in R(b) \Rightarrow c\in R(a)$

Relações de equivalência

- **Exemplo2**: Seja A=Z e seja R={(a,b)∈A×A|a≤b}.

  R não é de equivalência, pois:

  - Reflexividade: R é reflexiva, pois $a \leq a$, $\forall a \in A$
  - Simetria: $b \leq a$ não segue de $a \leq b \Rightarrow$ R não é simétrica
  - Transitividade: se $a \leq b$ e $b \leq c \Rightarrow a \leq c$, portanto se aRb e bRc então aRc. Assim, R é transitiva.

Relações de equivalência

- Exemplo3: Seja m um inteiro positivo > 1. Mostre que a relação

  R={ (a,b) | a≡b (mod m) }

  é uma *relação de equivalência* sobre o conjunto dos inteiros.

  - Lembre que: $a \equiv b \pmod m \Leftrightarrow m | (a-b)$

  – Reflexividade: $a \equiv a \pmod m$ pois $a-a=0$ e $m|0 \Rightarrow$ aRa

  – Simetria: se $a \equiv b \pmod m$, então $a-b=k.m \Rightarrow b-a=(-k).m$
  $\Rightarrow b \equiv a \pmod m$
  assim: aRb ⇒ bRa

  – Transitividade: suponha que $a \equiv b \pmod m$ e $b \equiv c \pmod m$
  ⇒ m divide tanto (b-a) como (c-b)
  $\Rightarrow a-b=k.m$ e $b-c=l.m$
  $\Rightarrow a-c = (a-b)+(b-c) = (k+l).m$
  $\Rightarrow a \equiv c \pmod m$
  portanto, aRb e bRc ⇒ aRc e R é transitiva.

Relações de equivalência e partições

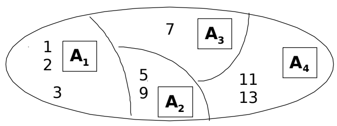
- Uma ***partição*** ou ***conjunto quociente*** de um conjunto não vazio A é uma coleção ***P*** de subconjuntos não vazios de A tal que:

  1. Cada elemento de A pertence a algum dos conjuntos em ***P***
  2. Se A_1 e A_2 são elementos distintos em ***P***, então $A_1 \cap A_2 = \emptyset$.

  – Os conjuntos em P são chamados de ***blocos*** ou ***células*** da partição.

Relações de equivalência e partições

- Exemplo: A={1,2,3,5,7,9,11,13}



- $A_1=\{1,2,3\}$ $A_2=\{5,9\}$ $A_3=\{7\}$ $A_4=\{11,13\}$
- $\boldsymbol{P}=\{A_1, A_2, A_3, A_4\}$ é uma partição do conjunto A em 4 blocos.

Relações de equivalência e partições

- Uma partição ***P*** pode ser usada para construir uma relação de equivalência sobre A.
- **Teorema**: Seja ***P*** uma partição sobre um conjunto A. Defina uma relação R sobre A como:

  aRb sse a e b são membros do mesmo bloco.

  Então R é uma *relação de equivalência* sobre A (determinada por ***P***).

Prova:

(1) Se a∈A, então a está no mesmo bloco que ele mesmo, de modo que aRa ⇒ R é reflexiva

(2) Se aRb então a e b estão no mesmo bloco, logo bRa ⇒ R é simétrica

(3) Se aRb e bRc, então a, b e c estão no mesmo bloco ***P***, logo aRc. Portanto: aRb e bRc ⇒ aRc (R é transitiva).

Relações de equivalência e partições

- Exemplo: Seja A={1,2,3,4} e considere uma partição ***P***={{1,2,3}, {4}}. Ache a relação de equivalência determinada por ***P***.
- Solução: cada elemento do bloco deve estar relacionado com todos os outros elementos no mesmo bloco e somente com estes elementos:

R={(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3),(4,4)}

Relações de equivalência e partições

- **Teorema**: Seja R uma relação de equivalência sobre A e seja ***P*** a coleção de todos os conjuntos relativos R(a), para todo a∈A. Então ***P* é uma partição de A**, e R é a relação de equivalência determinada por ***P***.
  - Os conjuntos R(a) são chamados de *classes de equivalência* de R
  - A partição ***P*** construída no teorema acima consiste portanto de todas as classes de equivalência de R e esta partição é denotada por A/R
  - Partições de um conjunto A também são chamadas de "conjuntos quocientes" de A
  - A/R é o conjunto quociente de A que é construído e determinado por R

Relações de equivalência e partições

- Exemplo1: Seja A={1,2,3,4} e seja a relação de equivalência R sobre A definida por

  R={(1,1), (1,2), (2,1), (2,2), (3,4), (4,3), (3,3), (4,4)}.

  Determine A/R (todas as classes de equivalência de R).

- Solução: R(1) = {1,2}
  R(2) = {1,2}
  R(3) = {3,4}
  R(4) = {3,4}

  ⇒ **A/R = {{1,2} , {3,4}}**

Relações de equivalência e partições

- Exemplo2: Seja A=**Z** e seja R={(a,b)∈A×A | 2|(a-b)} (como já visto, R é uma relação de equivalência). Determinar A/R.
- Solução:
  - R(0)={⋯ -6, -4, -2, 0, 2, 4, 6, ⋯} (O conjunto dos inteiros pares, pois 2 divide a diferença entre quaisquer dois inteiros pares.)
  - R(1)={ ⋯ -5, -3, -1, 0, 1, 3, 5, ⋯} (O conjunto dos inteiros ímpares, pois 2 divide a diferença entre quaisquer dois inteiros ímpares.)
  - Assim: A/R={R(0), R(1)}

Procedimento geral para determinar partições A/R

- ***Passo 1***. *Escolha um elemento qualquer de A, digamos a, e calcule a classe de equivalência R(a).*
- ***Passo 2***. *Se R(a)≠A, escolha um elemento b não incluído em R(a) e calcule a classe de equivalência R(b).*
- ***Passo 3***. *Se A não é igual a união das classes de equivalência previamente calculadas, então escolha um elemento x de A que não esteja em nenhuma dessas classes de equivalência e calcule R(x).*
- ***Passo 4***. *Repita o passo 3 até que todos os elementos de A estejam em classes de equivalência já calculadas.*
  - *Se A é infinito este processo pode continuar indefinidamente.*
  - *Neste caso, continue até que apareça um padrão que permita descrever ou dar uma fórmula para todas as classes*

Relações de equivalência - Exercícios

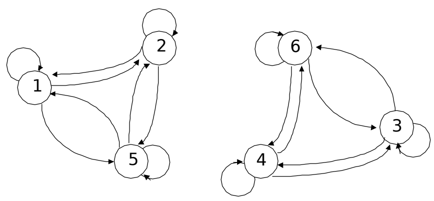
- Exercício 1: Seja A={a,b,c}. Determine se a relação R cuja matriz é dada abaixo é uma relação de equivalência.

$$M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

- Resp.: SIM. (Por quê?)

Relações de equivalência - Exercícios

- Exercício 2: Determine se a relação R cujo dígrafo é dado abaixo é uma relação de equivalência.



- Resp.: SIM. (Por quê?)

Relações de equivalência - Exercícios

- Exercício 3: Se {{1,3,5}, {2,4}} é uma partição do conjunto A={1,2,3,4,5}, determine a relação de equivalência R correspondente.

- Resp.:

R={(1,1),(1,3),(1,5),(3,1),(3,3),(3,5),(5,1),(5,3),(5,5),
(2,2),(2,4),(4,2),(4,4)}

Leituras sobre Relações de Equivalência

- Kolman5: seção 4.5

- Rosen6: seção 8.5

INE5403 - Fundamentos de Matemática Discreta para a Computação

6) Relações

6.1) Definição e Representação

6.2) Caminhos em Relações e Digrafos

6.3) Propriedades de Relações

6.4) Relações de Equivalência

6.5) Manipulação e Fecho de Relações

Combinação de relações

- Exemplo: Sejam A={1,2,3} e B={1,2,3,4}. As relações R_1={(1,1),(2,2),(3,3)} e R_2={(1,1),(1,2),(1,3),(1,4)} podem ser combinadas para obter:

$R_1 \cup R_2$={(1,1),(1,2),(1,3),(1,4),(2,2),(3,3)}

$R_1 \cap R_2$={(1,1)}

$R_1 - R_2$={(2,2),(3,3)}

$R_2 - R_1$={(1,2),(1,3),(1,4)}

Manipulação de relações (operações)

- Da mesma forma que podemos manipular números usando as regras da álgebra, podemos operar com relações

- Com estas operações, podemos modificar, combinar e refinar relações existentes para produzir relações novas

- Uma vez que relações de A para B são subconjuntos de A×B, duas relações de A para B podem ser combinadas de todos os modos em que se puder combinar 2 conjuntos

Operações entre relações

- **Def.**: Sejam R e S duas relações de A em B. Então as seguintes relações são definidas:

1) $\overline{R}$: a ***relação complementar*** de R é definida como:

$(a,b)\in\overline{R} \Leftrightarrow (a,b)\notin R$

– Nota: A *matriz da relação* $\overline{R}$ é obtida a partir da matriz de R trocando-se todos os 0's por 1's e vice-versa:

$$M_{\overline{R}} = \overline{M_R}$$

Operações entre relações

2) R∩S: a ***relação intersecção*** de R com S é definida como:

$(a,b)\in R\cap S \Leftrightarrow (a,b)\in R \wedge (a,b)\in S$

– Nota: $M_{R\cap S} = M_R \wedge M_S$ (operação matricial lógica "∧" sobre as matrizes booleanas M_R e M_S).

Operações entre relações

2) R∩S: a ***relação intersecção*** de R com S é definida como:

$(a,b)\in R\cap S \Leftrightarrow (a,b)\in R \wedge (a,b)\in S$

– Nota: $M_{R\cap S} = M_R \wedge M_S$ (operação matricial lógica "∧" sobre as matrizes booleanas M_R e M_S).

3) R∪S: a ***relação união*** de R com S é definida como:

$(a,b)\in R\cup S \Leftrightarrow (a,b)\in R \vee (a,b)\in S$

– Nota: $M_{R\cup S} = M_R \vee M_S$ (operação matricial lógica "∨" sobre as matrizes booleanas M_R e M_S).

Operações entre relações

4) R^{-1}: a ***relação inversa*** de R é definida por:

$$(a,b)\in R^{-1} \Leftrightarrow (b,a)\in R$$

– Nota: $M_{R^{-1}} = (M_R)^T$ (transposta da matriz M_R)

Operações entre relações

- **Ex.**: A={1,2,3,4}, B={a,b,c} e R e S de A em B definidas por:

R={(1,a),(1,b),(2,b),(2,c),(3,b),(4,a)}
S={(1,b),(2,c),(3,b),(4,b)}

Computar a) $\overline{R}$ b) $R\cap S$ c) $R\cup S$ d) R^{-1}

- **Solução**:

a) $A\times B$={(1,a),(1,b),(1,c),(2,a),(2,b),(2,c),(3,a),(3,b),(3,c),(4,a),(4,b),(4,c)}
$\Rightarrow \overline{R}$={(1,c),(2,a),(3,a),(3,c),(4,b),(4,c)}

b) $R\cap S$={(1,b),(2,c),(3,b)}

c) $R\cup S$={(1,a),(1,b),(2,b),(2,c),(3,b),(4,a),(4,b)}

d) R^{-1}={(a,1),(b,1),(b,2),(c,2),(b,3),(a,4)}

Operações entre relações

- **Ex.**: A={1,2,3,4}, B={a,b,c} e R e S de A em B definidas por:

R={(1,a),(1,b),(2,b),(2,c),(3,b),(4,a)}
S={(1,b),(2,c),(3,b),(4,b)}

Calcular: a) M_R b) M_S c) $M_{\overline{R}}$ d) $M_{R^{-1}}$ e) $M_{R\cap S}$ f) $M_{R\cup S}$

a) $M_R=\begin{bmatrix}1&1&0\\0&1&1\\0&1&0\\1&0&0\end{bmatrix}$ b) $M_S=\begin{bmatrix}0&1&0\\0&0&1\\0&1&0\\0&1&0\end{bmatrix}$

c) $\overline{R}$={(1,c),(2,a),(3,a),(3,c),(4,b),(4,c)} $\Rightarrow$ $M_{\overline{R}}=\begin{bmatrix}0&0&1\\1&0&0\\1&0&1\\0&1&1\end{bmatrix}$

Operações entre relações

- **Ex.**: A={1,2,3,4}, B={a,b,c} e R e S de A em B definidas por:

R={(1,a),(1,b),(2,b),(2,c),(3,b),(4,a)}
S={(1,b),(2,c),(3,b),(4,b)}

d) R^{-1}={(a,1),(b,1),(b,2),(c,2),(b,3),(a,4)}

$$\Rightarrow \quad M_{R^{-1}}=(M_R)^T=\begin{bmatrix}1&0&0&1\\1&1&1&0\\0&1&0&0\end{bmatrix}$$

e) $R\cap S$={(1,b),(2,c),(3,b)}

$$M_{R\cap S}=M_R\wedge M_S=\begin{bmatrix}1&1&0\\0&1&1\\0&1&0\\1&0&0\end{bmatrix}\wedge\begin{bmatrix}0&1&0\\0&0&1\\0&1&0\\0&1&0\end{bmatrix}=\begin{bmatrix}0&1&0\\0&0&1\\0&1&0\\0&0&0\end{bmatrix}$$

Operações entre relações

- **Ex.**: A={1,2,3,4}, B={a,b,c} e R e S de A em B definidas por:

R={(1,a),(1,b),(2,b),(2,c),(3,b),(4,a)}
S={(1,b),(2,c),(3,b),(4,b)}

f) $R\cup S$={(1,a),(1,b),(2,b),(2,c),(3,b),(4,a),(4,b)}

$$M_{R\cup S}=M_R\vee M_S=\begin{bmatrix}1&1&0\\0&1&1\\0&1&0\\1&0&0\end{bmatrix}\vee\begin{bmatrix}0&1&0\\0&0&1\\0&1&0\\0&1&0\end{bmatrix}=\begin{bmatrix}1&1&0\\0&1&1\\0&1&0\\1&1&0\end{bmatrix}$$

Manipulação de relações

Teorema: Suponha que R e S são relações de A em B.

(a) Se $R\subseteq S$, então $R^{-1}\subseteq S^{-1}$

(b) Se $R\subseteq S$, então $\overline{S}\subseteq\overline{R}$

(c) $(R\cap S)^{-1} = R^{-1}\cap S^{-1}$ e $(R\cup S)^{-1} = R^{-1}\cup S^{-1}$

(d) $\overline{(R\cap S)} = \overline{R}\cup\overline{S}$ e $\overline{(R\cup S)} = \overline{R}\cap\overline{S}$

Manipulação de relações

Teorema: Suponha que R e S são relações de A em B.

(a) Se $R \subseteq S$, então $R^{-1} \subseteq S^{-1}$

(b) Se $R \subseteq S$, então $\overline{S} \subseteq \overline{R}$

(c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ e $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

(d) $(\overline{R \cap S}) = \overline{R} \cup \overline{S}$ e $(\overline{R \cup S}) = \overline{R} \cap \overline{S}$

Prova: os itens (b) e (d) são casos particulares de propriedades gerais de conjuntos.

(a) Suponha que $R \subseteq S$ e seja $(a,b) \in R^{-1}$,

- então $(b,a) \in R$ (definição de R^{-1})
- segue que, como $R \subseteq S$, $(b,a) \in S$
- como $(b,a) \in S$, segue que $(a,b) \in S^{-1}$ (definição de S^{-1})
- portanto, $R^{-1} \subseteq S^{-1}$

Manipulação de relações

Prova da 1ra parte do item (c):

(c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ → temos que provar que:

i) $(R \cap S)^{-1} \subseteq R^{-1} \cap S^{-1}$
ii) $R^{-1} \cap S^{-1} \subseteq (R \cap S)^{-1}$

i) $(R \cap S)^{-1} \subseteq R^{-1} \cap S^{-1}$

- suponha que $(a,b) \in (R \cap S)^{-1}$.
- então $(b,a) \in R \cap S$ ⇒ $(b,a) \in R$ e $(b,a) \in S$
- isto significa que $(a,b) \in R^{-1}$ e $(a,b) \in S^{-1}$
- de modo que $(a,b) \in R^{-1} \cap S^{-1}$

ii) $R^{-1} \cap S^{-1} \subseteq (R \cap S)^{-1}$ (converso)

- basta reverter os passos acima.

Manipulação de relações

- Exercício: Seja A=B={1,2,3} e

  S={(1,2),(2,3),(3,1),(3,2),(3,3)}
  T={(2,1),(2,3),(3,2),(3,3)}

  – Verifique o item (c) do teorema com S e T
  – Verifique o item (d) do teorema com S e T

  – NOTA:

  (c) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ e $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

  (d) $(\overline{R \cap S}) = \overline{R} \cup \overline{S}$ e $(\overline{R \cup S}) = \overline{R} \cap \overline{S}$

Manipulação de relações

- Os teoremas a seguir mostram o efeito que as operações têm sobre algumas das propriedades vistas.

Teorema: Sejam R e S relações sobre A. Então:

(a) Se R é reflexiva, então R^{-1} também o é;

(b) R é reflexiva se e somente se $\overline{R}$ é irreflexiva;

(c) Se R e S são reflexivas, então $R \cap S$ e $R \cup S$ também o são.

Manipulação de relações

- Os teoremas a seguir mostram o efeito que as operações têm sobre algumas das propriedades vistas.

Teorema: Sejam R e S relações sobre A. Então:

(a) Se R é reflexiva, então R^{-1} também o é;

(b) R é reflexiva se e somente se $\overline{R}$ é irreflexiva;

(c) Se R e S são reflexivas, então $R \cap S$ e $R \cup S$ também o são.

Exemplo: Seja A={1,2,3} e sejam:
R={(1,1),(1,2),(1,3),(2,2),(3,3)} S={(1,1),(1,2),(2,2),(3,2),(3,3)}

(a) R^{-1}={(1,1),(2,1),(3,1),(2,2),(3,3)} ⇒ R e R^{-1} são ambas reflexivas

(b) $\overline{R}$={(2,1),(2,3),(3,1),(3,2)} é irreflexiva enquanto R é reflexiva

(c) $R \cap S$={(1,1),(1,2),(2,2),(3,3)} e
$R \cup S$={(1,1),(1,2),(1,3),(2,2),(3,2),(3,3)} são ambas reflexivas

Manipulação de relações

Teorema: Seja R uma relação sobre A. Então:

(a) R é simétrica se e somente se $R = R^{-1}$

(b) R é antissimétrica sse $R \cap R^{-1} \subseteq \Delta$ (Δ: rel. de igualdade)

(c) R é assimétrica se e somente se $R \cap R^{-1} = \emptyset$

Teorema: Sejam R e S relações sobre A.

(a) Se R é simétrica, então R^{-1} e $\overline{R}$ também o são;

(b) Se R e S são simétricas, então $R \cap S$ e $R \cup S$ também o são.

Manipulação de relações

Exemplo: Seja A={1,2,3} e considere as relações simétricas:

R={(1,1),(1,2),(2,1),(1,3),(3,1)}
S={(1,1),(1,2),(2,1),(2,2),(3,3)}

(a) R^{-1}={(1,1),(2,1),(1,2),(3,1),(1,3)}
$\overline{R}$={(2,2),(2,3),(3,2),(3,3)}
→ ambas simétricas

(b) R∩S = {(1,1),(1,2),(2,1)}
R∪S = {(1,1),(1,2),(1,3),(2,1),(2,2),(3,1),(3,3)}
→ ambas simétricas

Manipulação de relações

- Exercício: Seja A={1,2,3,4,5,6} e sejam as relações de equivalência sobre A seguintes:

R={(1,1),(1,2),(2,1),(2,2),(3,3),(4,4),(5,5),(5,6),(6,5),(6,6)}

S={(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3),(4,4),
(4,6),(5,5),(6,4),(6,6)}

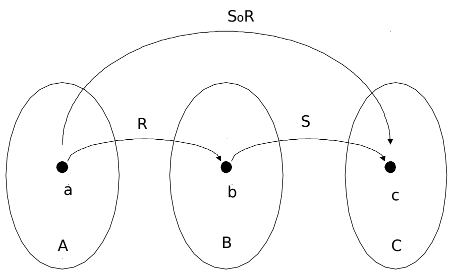
Compute a partição correspondente a R∩S.

Composição de relações

Def.: Sejam A, B e C conjuntos, R uma relação de A em B e S uma relação de B em C.

- Então a relação de ***composição*** de R e S, escrita como S ∘ R, é definida como:
  - Se a∈A e c∈C, então (a,c)∈S∘R se e somente se existir algum b∈B tal que (a,b)∈R e (b,c)∈S
  - "S em seguida a R" (primeiro R, depois S).

Composição de relações



Composição de relações

- Ex.: Sejam A={1,2,3,4} e as relações R e S sobre A:

R={(1,2),(1,1),(1,3),(2,4),(3,2)}
S={(1,4),(1,3),(2,3),(3,1),(4,1)}

- Como (1,2)∈R e (2,3)∈S, então temos que (1,3)∈ S∘R.
- Também (1,1)∈R e (1,4)∈S, assim (1,4)∈ S∘R.
- Continuando com este processo, encontra-se que:
S∘R ={(1,4),(1,1),(1,3),(2,1),(3,3)}

Composição de relações

- Teorema: Se R é uma relação de A em B e S é uma relação de B em C, então:

$$M_{S \circ R} = M_R \otimes M_S$$

- Além disto, se |A|=m, |B|=n e |C|=p:
  - M_R tem ordem mxn
  - M_S tem ordem nxp
  - $M_{S \circ R}$ tem ordem mxp

Composição de relações

- Ex.: A={a,b,c} e R e S relações sobre A com matrizes:

$$M_R=\begin{bmatrix}1&0&1\\1&1&1\\0&1&0\end{bmatrix} \qquad M_S=\begin{bmatrix}1&0&0\\0&1&1\\1&0&1\end{bmatrix}$$

⇒ R = {(a,a),(a,c),(b,a),(b,b),(b,c),(c,b)}

⇒ S = {(a,a),(b,b),(b,c),(c,a),(c,c)}

⇒ SoR = {(a,a),(a,c),(b,a),(b,b),(b,c),(c,b),(c,c)}

Composição de relações

- Ex.: A={a,b,c} e R e S relações sobre A com matrizes:

$$M_R=\begin{bmatrix}1&0&1\\1&1&1\\0&1&0\end{bmatrix} \qquad M_S=\begin{bmatrix}1&0&0\\0&1&1\\1&0&1\end{bmatrix}$$

⇒ R = {(a,a),(a,c),(b,a),(b,b),(b,c),(c,b)}

⇒ S = {(a,a),(b,b),(b,c),(c,a),(c,c)}

⇒ SoR = {(a,a),(a,c),(b,a),(b,b),(b,c),(c,b),(c,c)}

– E a matriz da relação composta SoR é:

$$M_{S\circ R}=\begin{bmatrix}1&0&1\\1&1&1\\0&1&1\end{bmatrix}=M_R\otimes M_S$$

Composição de relações

- Teorema: Sejam A, B, C e D conjuntos e:
  - R uma relação de A em B,
  - S uma relação de B em C, e
  - T uma relação de C em D.

  Então:

  To(SoR) = (ToS)oR
- Prova no livro: teorema 7, pág. 140, usando matrizes.

Composição de relações

- Em geral: SoR ≠ RoS
- Exemplo: Sejam:

  A={a,b}

  R={(a,a),(b,a),(b,b)}

  S={(a,b),(b,a),(b,b)}

  Então:

  SoR = {(a,b),(b,a),(b,b)}

  enquanto que:

  RoS = {(a,a),(a,b),(b,a),(b,b)}

Composição de relações

- Teorema: Sejam A, B e C conjuntos, R uma relação de A em B e S uma relação de B em C. Então:

  $(SoR)^{-1} = R^{-1} o S^{-1}$
- Prova: seja c∈C e a∈A.
  - Então $(c,a)\in(S\circ R)^{-1} \Leftrightarrow (a,c)\in S\circ R$

Composição de relações

- Teorema: Sejam A, B e C conjuntos, R uma relação de A em B e S uma relação de B em C. Então:

  $(SoR)^{-1} = R^{-1} o S^{-1}$
- Prova: seja c∈C e a∈A.
  - Então $(c,a)\in(S\circ R)^{-1} \Leftrightarrow (a,c)\in S\circ R$
  - ou seja, sse existe b∈B com (a,b)∈ R e (b,c)∈S;
  - isto é equivalente a ter $(b,a)\in R^{-1}$ e $(c,b)\in S^{-1}$
  - o que, pela definição de composição, significa que $(c,a) \in R^{-1}\circ S^{-1}$

Fechos de relações

- Pode acontecer que uma relação R sobre A não possua propriedades importantes, tais como reflexividade, simetria e transitividade
- Neste caso, pode-se querer *adicionar os pares necessários* para que ela adquira a propriedade desejada

Fechos de relações

- Pode acontecer que uma relação R sobre A não possua propriedades importantes, tais como reflexividade, simetria e transitividade
- Neste caso, pode-se querer *adicionar os pares necessários* para que ela adquira a propriedade desejada
- Mas: deseja-se adicionar o menor nro de pares possível, de modo a obter *a menor relação R_1 sobre A que possui a propriedade desejada*
- Eventualmente R_1 pode não existir → se a relação R_1 existe, ela é chamada de "*fecho de R* com respeito à propriedade em questão"

Fechos de relações

- Ex.1: Seja R uma relação não-reflexiva sobre um conjunto A.
  - Isto somente pode acontecer quando alguns pares da relação diagonal $\Delta=\{(a,a)|a\in A\}$ não estão em R
  - Assim, $R_1=R\cup\Delta$ é a menor relação reflexiva sobre A que contém R
  - Em outras palavras, $R\cup\Delta$ é o *fecho reflexivo* de R.

Fechos de relações

- Ex.2: Seja A={a,b,c} e R sobre A definida por

  R={(a,a),(a,b),(a,c),(b,b),(c,c)}

- R não é simétrica pois (b,a) e (c,a) não pertencem a R
- Então o *fecho simétrico* de R é a relação R_1 a seguir:

$$R_1 = R \cup \{(b,a),(c,a)\}$$

Fechos de relações

- Ex.3 (simetria): Suponha que R é uma relação sobre um conjunto A e que R não é simétrica.
  - Então, devem existir pares $(x,y)\in R$ tais que $(y,x)\notin R$
  - Por outro lado, $(y,x)\in R^{-1}$
  - Portanto, para R se tornar simétrica, deve-se adicionar todos os pares de R^{-1} ⇒ R deve ser aumentada para $R\cup R^{-1}$
  - $R\cup R^{-1}$ é a menor relação simétrica que contém R, ou seja, $R\cup R^{-1}$ é o *fecho simétrico* de R.
- Ex.: A={a,b,c,d} e R={(a,b),(b,c),(a,c),(d,c)}
  ⇒ R^{-1}={(b,a),(c,b),(c,a),(c,d)}
  ⇒ o *fecho simétrico* de R é:
  $R\cup R^{-1}$={(a,b),(b,c),(a,c),(d,c),(b,a),(c,b),(c,a),(c,d)}

Fecho Transitivo

- Será que o fecho transitivo de uma relação pode ser produzido pela adição de pares (a,c), onde (a,b) e (b,c) já estão na relação?
- Ex.: considere R={(1,3),(1,4),(2,1),(3,2)} sobre {1,2,3,4}
- R não é transitiva, pois faltam (1,2),(2,3),(2,4),(3,1)

Fecho Transitivo

- Será que o fecho transitivo de uma relação pode ser produzido pela adição de pares (a,c), onde (a,b) e (b,c) já estão na relação?

- Ex.: considere R={(1,3),(1,4),(2,1),(3,2)} sobre {1,2,3,4}
  - R não é transitiva, pois faltam (1,2),(2,3),(2,4),(3,1)
  - Adicionando o que falta:

    R={(1,3),(1,4),(2,1),(3,2),(1,2),(2,3),(2,4),(3,1)}

Fecho Transitivo

- Será que o fecho transitivo de uma relação pode ser produzido pela adição de pares (a,c), onde (a,b) e (b,c) já estão na relação?

- Ex.: considere R={(1,3),(1,4),(2,1),(3,2)} sobre {1,2,3,4}
  - R não é transitiva, pois faltam (1,2),(2,3),(2,4),(3,1)
  - Adicionando o que falta:

    R={(1,3),(1,4),(2,1),(3,2),(1,2),(2,3),(2,4),(3,1)}
  - Agora R contém (3,1) e (1,4) mas não (3,4) !

Fecho Transitivo

- Será que o fecho transitivo de uma relação pode ser produzido pela adição de pares (a,c), onde (a,b) e (b,c) já estão na relação?

- Ex.: considere R={(1,3),(1,4),(2,1),(3,2)} sobre {1,2,3,4}
  - R não é transitiva, pois faltam (1,2),(2,3),(2,4),(3,1)
  - Adicionando o que falta:

    R={(1,3),(1,4),(2,1),(3,2),(1,2),(2,3),(2,4),(3,1)}
  - Agora R contém (3,1) e (1,4) mas não (3,4) !
- *Fechos transitivos dependem de algoritmos especiais...*

Leituras sobre Manipulação e Fechos

- Kolman5: seção 4.7

- Rosen6: seção 8.4

6) Relações

6.5) Manipulação e Fecho de Relações: Fecho transitivo de Relações

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Fecho transitivo

- Construção com várias interpretações e muitas aplicações importantes.
- Suponha que R é uma relação sobre um conjunto A e que R não é transitiva.
  - O **fecho transitivo** de R é simplesmente a relação de conectividade R^∞.

Propriedades da Transitividade

- Vimos que, geometricamente, a transitividade por ser descrita como:
  - se a e c estão conectados por um caminho de tamanho 2 em R, também o estão por um caminho de tamanho 1
  - ou: se $a\ R^2\ c$, então $a\ R\ c$
    - ou seja: $R^2 \subseteq R$ (como subconjuntos de $A \times A$)
- O Teorema a seguir generaliza esta caracterização geométrica da transitividade.

- **Teorema:** Se uma relação R é transitiva, ela satisfaz à seguinte propriedade:
  - "Se existe um caminho de comprimento > 1 do vértice a para o b, também existe um caminho de comprimento 1 de a para b ($a\ R\ b$)."
  - Algebricamente: "Se R é transitiva, então $R^n \subseteq R$ para todo $n \geq 1$".

  Prova: indução sobre n.

  - Passo básico: $P(1)$ é V, pois "se R é transitiva, vale que $R^1 \subseteq R$".
  - Passo indutivo:
    - Hipótese indutiva: $P(k)$ é V ("se R é transitiva, vale que $R^k \subseteq R$")
      - *Ou seja: "se a e b estão conectados por um caminho de tamanho k em R, também o estão por um caminho de tamanho 1"*
    - Agora, será que $P(k+1)$ é V?
      - *Ou seja: será que "se R é transitiva, sempre que há caminho de tamanho $k+1$ entre a e b, há caminho de tamanho 1 entre eles também"??*
    - Ora, se a e b estão conectados por um caminho de tamanho $k+1$, este caminho tem duas partes: uma de tamanho k, indo de a até um c, e outra de tamanho 1, de c até b
    - Pela hipótese indutiva, há um caminho de tamanho 1 de a até c.
    - Então, como R é transitiva, tem que haver um caminho de tamanho 1 entre a e b $\square$

- **Teorema 1:** Seja $\boldsymbol{R}$ uma relação sobre um conjunto $\boldsymbol{A}$. Então $\boldsymbol{R}^{\infty}$ é o fecho transitivo de $\boldsymbol{R}$.

  Prova:

  - $\boldsymbol{a}\ \boldsymbol{R}^{\infty}\ \boldsymbol{b} \quad \Leftrightarrow \quad$ existe um caminho em $\boldsymbol{R}$ de $\boldsymbol{a}$ para $\boldsymbol{b}$
  - Note que $\boldsymbol{R}^{\infty}$ é certamente transtitiva, pois:
    - se $\boldsymbol{a}\ \boldsymbol{R}^{\infty}\ \boldsymbol{b}$ e $\boldsymbol{b}\ \boldsymbol{R}^{\infty}\ \boldsymbol{c}$:
      - existem em $\boldsymbol{R}$ dois caminhos: $\boldsymbol{a} \to \boldsymbol{b}$ e $\boldsymbol{b} \to \boldsymbol{c}$
      - logo: existe um caminho de $\boldsymbol{a}$ para $\boldsymbol{c}$ em $\boldsymbol{R}$
      - de modo que: $\boldsymbol{a}\ \boldsymbol{R}^{\infty}\ \boldsymbol{c}$

  - *Falta mostrar que $\boldsymbol{R}^{\infty}$ é a menor relação transitiva que contém $\boldsymbol{R}$*
    - *Ou seja, precisamos ainda mostrar que:*
      - *se: $\boldsymbol{S}$ é qualquer relação transitiva sobre $\boldsymbol{A}$ e: se $\boldsymbol{R} \subseteq \boldsymbol{S}$*
      - *então: $\boldsymbol{R}^{\infty} \subseteq \boldsymbol{S}$*

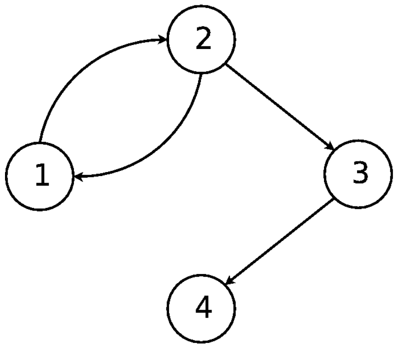
  - Propriedade da transitividade (teorema visto):
    - Se $\boldsymbol{S}$ é transitiva, então $\boldsymbol{S}^{\boldsymbol{n}} \subseteq \boldsymbol{S}$ para todo $\boldsymbol{n}$
      - ("$\boldsymbol{a}$ e $\boldsymbol{b}$ conectados por caminho de comprimento $\boldsymbol{n} \Rightarrow \boldsymbol{a}\ \boldsymbol{S}\ \boldsymbol{b}$")
    - Segue que: $\quad \boldsymbol{S}^{\infty} = \cup_{\boldsymbol{n}=\boldsymbol{1}}^{\infty} \boldsymbol{S}^{\boldsymbol{n}} \quad \subseteq \quad \boldsymbol{S}$

  - Também é verdade que: se $\boldsymbol{R} \subseteq \boldsymbol{S}$, então $\boldsymbol{R}^{\infty} \subseteq \boldsymbol{S}^{\infty}$
    - pois: todo caminho em $\boldsymbol{R}$ também é um caminho em $\boldsymbol{S}$

  - Juntando tudo, vemos que:
    - se $\boldsymbol{R} \subseteq \boldsymbol{S}$ e se $\boldsymbol{S}$ é transitiva sobre $\boldsymbol{A}$, então: $\boldsymbol{R}^{\infty} \subseteq \boldsymbol{S}^{\infty} \subseteq \boldsymbol{S}$
    - ou seja, $\boldsymbol{R}^{\infty}$ é a menor de todas as relações transitivas que contêm $\boldsymbol{R}$. $\square$

- Vemos que $\boldsymbol{R}^{\infty}$ tem diversas interpretações:
  - de um ponto de vista geométrico, é a relação de conectividade
    - especifica quais os vértices que estão conectados (por caminhos) a outros
  - de um ponto de vista algébrico, $\boldsymbol{R}^{\infty}$ é o fecho transitivo de $\boldsymbol{R}$
    - papel importante na teoria de relações de equivalência

- **Exemplo 1:** Sejam $\boldsymbol{A} = \{1, 2, 3, 4\}$ e $\boldsymbol{R} = \{(1, 2), (2, 3), (3, 4), (2, 1)\}$. Ache o fecho transitivo de $\boldsymbol{R}$.
  - **Método 1:** geometricamente, pelo digrafo de $\boldsymbol{R}$:



  - já que $\boldsymbol{R}^{\infty}$ é o fecho transitivo, computamos todos os caminhos:
    * a partir do vértice 1, temos caminhos para: 2, 3, 4 e 1
    * a partir do vértice 2, temos caminhos para: 2, 1, 3 e 4
    * o único outro caminho é aquele que vai do vértice 3 para o 4
  - assim: $\boldsymbol{R}^{\infty} = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4)\}$

  - **Método 2:** algebricamente, computando potências da matriz de $\boldsymbol{R}$:

$$\boldsymbol{M_R} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad (\boldsymbol{M_R})^{2}_{\odot} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$(\boldsymbol{M_R})^{3}_{\odot} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad (\boldsymbol{M_R})^{4}_{\odot} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

    * notamos que $(\boldsymbol{M_R})^{\boldsymbol{n}}_{\odot}$ se iguala a: $\begin{cases} (\boldsymbol{M_R})^{2}_{\odot}\ , & \text{se } \boldsymbol{n} \text{ é par} \\ (\boldsymbol{M_R})^{3}_{\odot}\ , & \text{se } \boldsymbol{n} \text{ é ímpar} \end{cases}$

    * portanto:

$$\boldsymbol{M_{R^{\infty}}} = \boldsymbol{M_R} \ \vee\ (\boldsymbol{M_R})^{2}_{\odot} \ \vee\ (\boldsymbol{M_R})^{3}_{\odot} \ = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \square$$

- No exemplo anterior, note que não foi preciso considerar todas as potências $\boldsymbol{R}^{\boldsymbol{n}}$ para obter $\boldsymbol{R}^{\infty}$.
- O teorema a seguir mostra que isto é verdade sempre que $\boldsymbol{A}$ é finito...

- **Teorema 2:** Seja $\boldsymbol{A}$ um conjunto com $|\boldsymbol{A}| = \boldsymbol{n}$, e seja $\boldsymbol{R}$ uma relação sobre $\boldsymbol{A}$. Então:

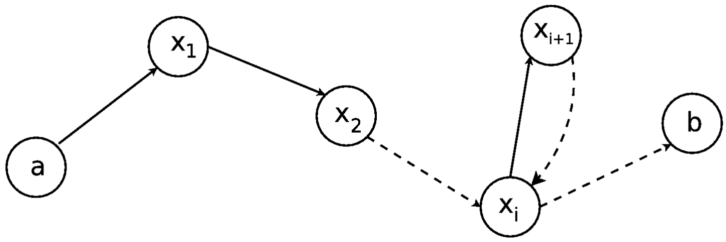
$$\boldsymbol{R}^{\infty} = \boldsymbol{R} \cup \boldsymbol{R}^{2} \cup \cdots \cup \boldsymbol{R}^{n}$$

  - *"Potências de $\boldsymbol{R}$ maiores do que $\boldsymbol{n}$ não são necessárias para computar $\boldsymbol{R}^{\infty}$".*

Prova: sejam $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{A}$:

- suponha que $\boldsymbol{a}, \boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_m}, \boldsymbol{b}$ é um caminho de $\boldsymbol{a}$ para $\boldsymbol{b}$ em $\boldsymbol{R}$
  * ou seja: $(\boldsymbol{a}, \boldsymbol{x_1}), (\boldsymbol{x_1}, \boldsymbol{x_2}), \ldots, (\boldsymbol{x_m}, \boldsymbol{b})$ estão todos em $\boldsymbol{R}$
- se $\boldsymbol{x_i}$ e $\boldsymbol{x_j}$ são o mesmo vértice (seja $\boldsymbol{i} < \boldsymbol{j}$), o caminho pode ser dividido em 3:

  [um caminho de $\boldsymbol{a}$ para $\boldsymbol{x_i}$] + [um de $\boldsymbol{x_i}$ para $\boldsymbol{x_j}$] + [um de $\boldsymbol{x_j}$ para $\boldsymbol{b}$]
- o caminho do meio é um ciclo, pois $\boldsymbol{x_i} = \boldsymbol{x_j}$:
  * deixando-o fora e unindo os outros, temos um caminho mais curto de $\boldsymbol{a}$ até $\boldsymbol{b}$:



- Agora seja $\boldsymbol{a}, \boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_k}, \boldsymbol{b}$ o caminho mais curto de $\boldsymbol{a}$ para $\boldsymbol{b}$:
  * se $\boldsymbol{a} \neq \boldsymbol{b}$, todos os vértices são distintos
    · (caso contrário, sempre se pode encontrar um caminho mais curto)
    · portanto, o comprimento deste caminho é $\leq \boldsymbol{n} - \boldsymbol{1}$ (pois $|\boldsymbol{A}| = \boldsymbol{n}$)
  * se $\boldsymbol{a} = \boldsymbol{b}$, os vértices $\boldsymbol{a}, \boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_k}$ são distintos
    · então o comprimento deste caminho é no máximo $\boldsymbol{n}$
- ou seja, se $\boldsymbol{a}\ \boldsymbol{R}^{\infty}\ \boldsymbol{b}$, então:
  * $\boldsymbol{a}\ \boldsymbol{R}^{k}\ \boldsymbol{b}$, para algum $\boldsymbol{k}$ (onde $\boldsymbol{1} \leq \boldsymbol{k} \leq \boldsymbol{n}$)
- Portanto: $\boldsymbol{R}^{\infty} = \boldsymbol{R} \cup \boldsymbol{R}^{2} \cup \cdots \cup \boldsymbol{R}^{n}$ $\square$

- Ambos os métodos usados no exemplo 1 apresentam dificuldades:
  - método gráfico:
    * impraticável para conjuntos e relações grandes
    * não pode ser automatizado
  - método matricial:
    * suficientemente sistemático para ser resolvido por um computador
    * mas ineficiente: custo proibitivo para matrizes grandes

- Método mais eficiente para computar fechos transitivos:
  - algoritmo de Warshall...

O Algoritmo de Warshall

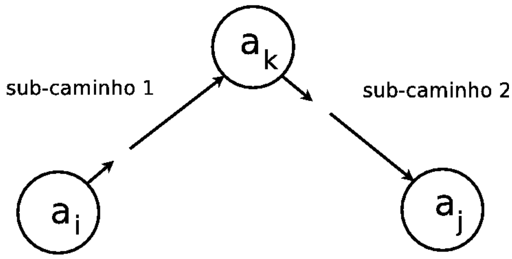
- Seja R uma relação sobre um conjunto $A = \{a_1, a_2, \ldots, a_n\}$.
- Se $x_1, x_2, \ldots, x_m$ é um caminho em R, então:
  - todo vértice $\neq x_1$ e $\neq x_m$ é um **vértice interno** do caminho
- Para $1 \leq k \leq n$, definimos a seguinte **matriz Booleana** W_k:
  - W_k tem um 1 na posição i, j sse:
    * existe um caminho de a_i para a_j
    * cujos vértices internos (se existirem) vêm de $\{a_1, a_2, \ldots, a_k\}$
- Já que todo vértice deve vir do conjunto $\{a_1, a_2, \ldots, a_n\}$, segue que:
  - a matriz W_n tem um 1 na posição i, j sse:
    * algum caminho em R conecta a_i a a_j
  - ou seja: $W_n = M_{R^\infty}$

- Se definimos W_0 como M_R, teremos uma seqüência $W_0, W_1, \ldots, W_n$
  - cujo primeiro termo é M_R
  - e o último é M_{R^∞}
- A seguir, veremos como computar cada matriz W_k a partir da sua antecessora W_{k-1} :
  - o que permitirá começar com a matriz de R
  - e avançar passo-a-passo
    * até que, em n passos, alcançaremos a matriz de R^∞.

- *Note que as matrizes W_k são diferentes das potências da matriz M_R*
  - *esta diferença resulta em uma economia considerável de passos na computação do fecho transitivo de R...*

- Suponha que $W_k = [t_{ij}]$ e que $W_{k-1} = [s_{ij}]$.
- Se $t_{ij} = 1$, então deve haver um caminho de a_i para a_j
  - cujos vértices internos vêm de $\{a_1, a_2, \ldots, a_k\}$
- Se o vértice a_k não é interno deste caminho, então todos os vértices internos virão, na verdade, de $\{a_1, a_2, \ldots, a_{k-1}\}$
  - e, neste caso: $s_{ij} = 1$

- Agora, se a_k é um vértice interno do caminho, a situação é:



  - Como na prova do Teor 2, podemos assumir que todos os vértices internos são distintos.
  - Logo, a_k aparece apenas uma vez no caminho
    * daí: todos os vértices internos dos subcaminhos 1 e 2 devem vir de $\{a_1, a_2, \ldots, a_{k-1}\}$
    * o que significa que: $s_{ik} = 1$ e $s_{kj} = 1$

- Resumindo, sendo $W_k = [t_{ij}]$ e $W_{k-1} = [s_{ij}]$, temos que:

  $t_{ij} = 1$ se e somente se:

  (1) $s_{ij} = 1$, ou:

  (2) $s_{ik} = 1$ e $s_{kj} = 1$.

- Esta é a base para o algoritmo de Warshall:
  - (1) se W_{k-1} tem um 1 em i, j, W_k também vai ter
  - (2) um novo 1 pode ser inserido na posição i, j de W_k sse:
    * a coluna k de W_{k-1} tem um 1 na posição i, e:
    * a linha k de W_{k-1} tem um 1 na posição j

- Procedimento para computar W_k a partir de W_{k-1}:

  - **Passo 1:** Transferir para W_k todos os 1's que estão em W_{k-1}.

  - **Passo 2:** Listar:
    * as posições $p_1, p_2, \ldots,$ na coluna k de W_{k-1} que valem 1
    * as posições $q_1, q_2, \ldots,$ na linha k de W_{k-1} que valem 1

  - **Passo 3:** Colocar 1's em todas as posições p_i, q_j de W_k
    * se eles já não estiverem lá.

- **Exemplo 2:** Seja $R = \{(1,2),(2,3),(3,4),(2,1)\}$ sobre $A = \{1,2,3,4\}$:

  – Neste caso, $n = 4$ e:

$$W_0 = M_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

  – Primeiro, vamos encontrar W_1 $(\Rightarrow k = 1)$:

    * W_0 tem 1's na posição 2 da coluna 1 e na posição 2 da linha 1
    * portanto, W_1 é simplesmente W_0 com um novo 1 na posição 2,2:

$$W_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

  – W_1, por sua vez, tem 1's nas posições 1 e 2 da coluna 2 e 1, 2 e 3 da linha 2:

    * para obter W_2, devemos colocar 1's nas posições 1,1; 1,2; 1,3; 2,1; 2,2 e 2,3 da matriz W_1 (se já não estiverem lá):

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

  – A coluna 3 de W_2 tem 1's nas posições 1 e 2 e a linha 3 tem um 1 na posição 4:

    * logo, para obter W_3, devemos inserir 1's nas posições 1,4 e 2,4 de W_2:

$$W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

  – W_3 tem 1's nas posições 1, 2 e 3 da coluna 4 e não tem 1's na linha 4.

    * Logo, não há mais 1's a inserir e: $M_{R^\infty} = W_4 = W_3$ □

  – (Mesmo resultado obtido no exemplo 1.)

- O procedimento ilustrado no exemplo anterior leva ao seguinte algoritmo para computar a matriz ("$FECHO$"), do fecho transitivo de uma relação R representada pela matriz $N \times N$ MAT:

  Algoritmo WARSHALL:

```
FECHO ← MAT
FOR K = 1 TO N
  FOR I = 1 TO N
    FOR J = 1 TO N
      FECHO[I,J]  ←  FECHO[I,J]  ∨ ( FECHO[I,K] ∧ FECHO[K,J] )
```

- Complexidade do algoritmo WARSHALL: n^3 passos
  - um passo = "um teste + uma atribuição"

- Nota: o cálculo pelas matrizes:

  $$M_{R^\infty} = M_R \vee (M_R)^2_\odot \vee \cdots \vee (M_R)^n_\odot$$

  - exige $n-1$ produtos booleanos de matrizes $n \times n$
  - o que é feito em $(n-1).n^3$ passos
  - levando a uma complexidade de cerca de n^4 passos

Leituras sobre Fecho Transitivo de Relações

- Kolman5: item 4.8
- Rosen6: item 8.4

INE5403 - Funds de MTM Discreta para a Computação

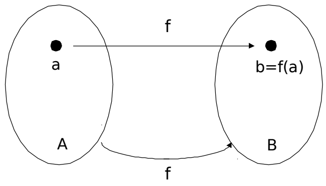
7) Funções

7.1) Definições e Tipos

7.2) Crescimento de Funções

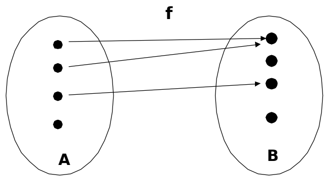
Funções

- Sejam A e B conjuntos não-vazios. Uma **função** f de A em B, denotada por $f:A \to B$, é uma *relação* de A em B tal que:
  - para todo $a \in Dom(f)$, f(a) contém *apenas um elemento*.

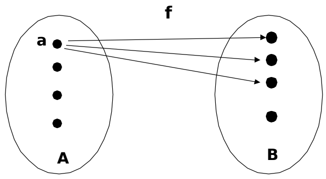


Funções

Exemplo de função:



<u>NÃO</u> é função:



Funções

- Observações:
  - Se $a \notin Dom(f)$, então $f(a)=\varnothing$
  - Se f(a)={b}, escreve-se f(a)=b
  - A relação f como definida acima pode ser escrita como o conjunto dos pares:

    $\{(a,f(a)) \mid a \in Dom(f)\}$
  - o elemento a é chamado de **argumento** da função
  - f(a) é chamado de **valor** de f para o argumento a
    - também designado por **imagem** de a sob f

Funções

- <u>Exemplo1</u>: Sejam A={1,2,3,4} e B={a,b,c,d} e seja

  f={(1,a),(2,a),(3,d),(4,c)}
  - Assim, os valores de f de x, para cada $x \in A$ são:

    f(1)={a}, f(2)={b}, f(3)={d}, f(4)={c}
  - como cada conjunto f(x), para $x \in A$, tem um único valor, então *f é uma função*.

Funções

- <u>Exemplo2</u>: Sejam A={1,2,3} e B={x,y,z} e considere as relações

  R={(1,x),(2,x)} e S={(1,x),(1,y),(2,z),(3,y)}

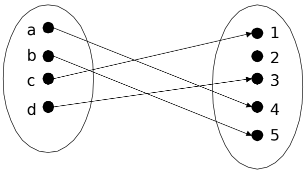
  Então:
  - R é uma função com Dom(R)={1,2} e Im(R)={x}
  - S *não é uma função* pois S(1)={x,y}

- <u>Exemplo3</u>: Seja A um conjunto arbitrário não-vazio. A função **identidade de A**, denotada por $\mathbf{1}_A$, é definida por

  $1_A(a)=a$

Tipos especiais de funções

- Uma função f de A em B é dita “um-para-um” ou **injetora** se e somente se f(a) ≠ f(b) sempre que a ≠ b.
  - Também: se f(a)=f(a’) então a=a’
- Exemplo1: Determine se a função f de {a,b,c,d} em {1,2,3,4,5}, com f(a)=4, f(b)=5, f(c)=1 e f(d)=3 é injetora.



Funções injetoras

- Exemplo2: Determine se a função $f(x)=x^2$, dos inteiros para os inteiros, é injetora.

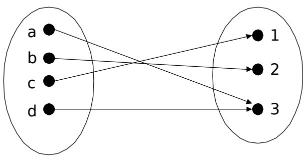
  Solução: A função $f(x)=x^2$ ***não é injetora***
  - pois, por exemplo, f(1)=f(-1)=1, mas 1 ≠ -1.

- Exemplo3: Determine se a função f(x)=x+1 é injetora.

  Solução: A função f(x)=x+1 ***é injetora***.
  - Para provar isto, note que x+1 ≠ y+1 quando x ≠ y.

Tipos especiais de funções

- Uma função f de A em B é chamada de **sobrejetora** sse para todo elemento b∈B há um elemento a∈A com f(a)=b.
  - Equivalentemente, f é sobrejetora se Im(f)=B (inteiro)
- Exemplo1: Seja f a função de {a,b,c,d} em {1,2,3}, definida por f(a)=3, f(b)=2, f(c)=1 e f(d)=3. Esta função é sobrejetora?



Funções sobrejetoras

- Exemplo2: A função f(x) = x^2, *dos inteiros para os inteiros*, é sobrejetora?

  Solução: A função f ***não é sobrejetora***
  - pois, por exemplo, não há inteiro x que forneça x^2 = -1.

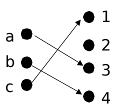
- Exemplo3: Determine se a função f(x)=x+1, dos inteiros para os inteiros, é sobrejetora.

  Solução: Esta função ***é sobrejetora***, pois:
  - para todo inteiro y, **sempre há** um inteiro x tal que f(x)=y.

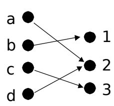
Tipos especiais de funções

- Uma função f é uma correspondência de um-para-um, ou uma *função* **bijetora**, se ela for ***injetora*** e ***sobrejetora***.
- Resumindo: Exemplos de diferentes tipos de correspondências:

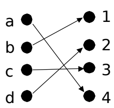
a) Injetora, mas não sobrejetora:



b) Sobrejetora, mas não injetora:



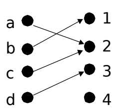
c) Injetora e sobrejetora:



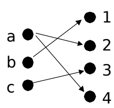
Tipos especiais de funções

- Resumindo: diferentes tipos de correspondências (continuação):

d) Nem injetora, nem sobrejetora:



e) Não é função:



Tipos especiais de funções

- Def.: Seja $f:A \to B$ uma função bijetora. A **função inversa de f** é a função que associa a um elemento $b \in B$ o elemento único *a* em A tal que $f(a)=b$.
  - A função inversa de f é denotada por f^{-1}.
  - Portanto, $f^{-1}(b) = a$ quando $f(a)=b$.
  - Uma função bijetora é chamada de inversível.

Funções inversas

- Exemplo1: Seja f a função de {a,b,c} para {1,2,3} tal que f(a)=2, f(b)=3 e f(c)=1. Verifique se a função f é inversível e, em caso afirmativo, determine a sua inversa.

- Solução: A função f é inversível, pois é bijetora. A função f^{-1} é dada por:

  $f^{-1}(1)=c$, $f^{-1}(2)=a$ e $f^{-1}(3)=b$.

Funções inversas

- Exemplo2: Seja f a função de Z para Z com $f(x)=x^2$. Esta função é inversível?

- Solução:
  - Como $f(-1)=f(1)=1$, f não é injetora.
  - Se uma f^{-1} fosse definida, ela teria que associar dois elementos a 1 ⇒ f não é inversível.

Composição de funções

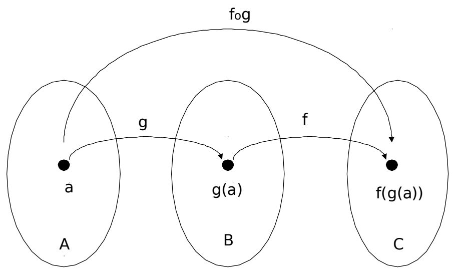
- Sejam:
  - g uma função do conjunto A para o conjunto B e
  - f uma função do conjunto B para o conjunto C.

  A **composição** das funções f e g, denotada por $f \circ g$, é definida por:

  $$(f \circ g)(a) = f(g(a))$$

- ou seja, $f \circ g$ é a função que associa ao elemento $a \in A$ o elemento associado por f a g(a)

Composição de funções



Composição de funções

- Exemplo1:
  - Seja g a função do conjunto {a,b,c} para ele mesmo tal que
    g(a)=b, g(b)=c e g(c)=a
  - Seja f a função de {a,b,c} para {1,2,3} tal que:
    f(a)=3, f(b)=2 e f(c)=1.
  - Determine a composição de f e g e a composição de g e f
- Solução:
  - A composição $f \circ g$ é definida por:
    $(f \circ g)(a) = f(g(a)) = f(b)=2$
    $(f \circ g)(b) = f(g(b)) = f(c)=1$
    $(f \circ g)(c) = f(g(c)) = f(a)=3$
  - Note que $g \circ f$ não está definida, pois o contradomínio de f não é um subconjunto do domínio de g.

Composição de funções

- Exemplo2: Sejam f e g as funções do conjunto dos inteiros para o conjunto dos inteiros definidas por:

  $f(x) = 2x + 3$
  $g(x) = 3x + 2$

  Determine a composição de f e g e a composição de g e f.

- Solução:

  $(f \circ g)(x) = f(g(x)) = f(3x+2) = 2.(3x+2) + 3 = 6x+7$

  $(g \circ f)(x) = g(f(x)) = g(2x+3) = 3.(2x+3) + 2 = 6x + 11$

Funções

- Exemplo3: Seja A=Z, B=Z e C o conjunto dos inteiros pares. Seja $f:A\rightarrow B$ e $g:B\rightarrow C$ definida por

  $f(a)=a+1$, para $a\in A$
  $g(b)=2.b$, para $b\in B$

  Encontre $g\circ f$.

  Solução: $g\circ f(a) = g(f(a)) = g(a+1) = 2.(a+1)$

  $\Rightarrow \; g\circ f(a) = 2.(a+1)$

Composição de funções

- Note que a composição de funções *não é comutativa*.
- A composição de uma função e sua inversa, em qualquer ordem, leva à função identidade:
  - Suponha que f é uma função bijetora de A para B
  - A função inversa reverte a correspondência da função original:

    $f^{-1}(b)=a$ quando $f(a)=b$
    $f(a)=b$ quando $f^{-1}(b)=a$

  - Portanto:

    $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$
    $(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(a) = b$

  - Consequentemente,

    $f^{-1} \circ f = 1_A$
    $f \circ f^{-1} = 1_B$

Leituras sobre funções

- Kolman5: item 5.1
- Rosen6: item 2.3

7) Funções

7.2) Crescimento de Funções

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Funções & Complexidade

- Para cada método de solução de um problema (algoritmo), pode-se definir funções que relacionam:
  - o espaço necessário para guardar os dados
  - a quantidade de passos para resolvê-lo

  com o tamanho (magnitude) dos dados de entrada.
- Estas funções permitem concluir sobre:
  - memória necessária para armazenar todos os dados
  - tempo de execução de algoritmos
- Comparações de ordens de grandeza destas funções equivalem a comparar os custos computacionais de diferentes métodos de solução de um problema.
- **Exemplo:** Solução de um sistema linear $n \times n$:

método	nro de OPFs	tempo para $n = 30$ (*)
Regra de Cramer	$\sim (n+1)!$	1.4×10^{12} *anos*
Eliminação gaussiana	$\sim n^3/3$	0.05×10^{-9} *s*

(*) *em um supercomputador BlueGene (∼180 TFlops)*

- A primeira função cresce muito mais rapidamente do que a 2a.
- Assunto relacionado com o tema complexidade de algoritmos.

Crescimento de Funções

- **Exemplo 1:** Considere o problema de determinar a transitividade de uma relação R sobre um conjunto A com n elementos.
  - número de passos necessários (média) pelo método 1: $t(n) = \frac{1}{2}n^3 + \frac{1}{2}n^2$
  - número de passos necessários (média) pelo método 2: $s(n) = \frac{1}{8}n^4$
  - A tabela mostra que s "cresce mais rápido" do que t:

n	$t(n)$	$s(n)$
2	6	2
5	75	78
10	550	1250
50	63750	781250
100	505000	12500000

- Sejam f e g funções cujos domínios são subconjuntos de $\mathbb{Z}^+$:
  - dizemos que f é $O(g)$ se existem constantes c e k tais que:

$$|f(n)| \leq c \cdot |g(n)|, \qquad \forall n \geq k$$

- Ou seja: se f é $O(g)$, então f não cresce mais rápido do que g.
- Vantagem da notação big-O:
  - pode-se estimar o crescimento de uma função sem ligar para multiplicadores constantes ou termos de ordem menor
  - ou seja: usando notação big-O, não precisamos ligar para o hardware e o software usados para implementar um algoritmo.

- **Exemplo 2:** A função $f(n) = \frac{1}{2}n^3 + \frac{1}{2}n^2$ é $O(g)$ para $g(n) = n^3$.
  - Para ver isto, note que:
    $\frac{1}{2}n^3 + \frac{1}{2}n^2 \leq \frac{1}{2}n^3 + \frac{1}{2}n^3 \qquad$ se $n \geq 1$
  - Portanto:
    $\frac{1}{2}n^3 + \frac{1}{2}n^2 \leq 1 \cdot n^3 \qquad$ se $n \geq 1$
  - Daí, escolhendo $c = 1$ e $k = 1$, obtemos:
    $|f(n)| \leq |g(n)| \qquad \forall n \geq 1$
  - O que mostra que f é $O(g)$ $\qquad \square$

- Note que são possíveis outras escolhas para c, k e até mesmo g.
- Note que, se $|f(n)| \leq c \cdot |g(n)|$, $\forall n \geq k$, então:
  - $|f(n)| \leq C \cdot |g(n)|$, $\forall n \geq k$, $\forall C \geq c$, e
  - $|f(n)| \leq c \cdot |g(n)|$, $\forall n \geq K$, $\forall K \geq k$
  - ou seja: quando existe um par de constantes, existem infinitos
- Agora seja novamente a função $t(n) = \frac{1}{2}n^3 + \frac{1}{2}n^2$:
  - t é $O(h)$ para $h(n) = dn^3$, se $d \geq 1$, pois:
    * $|t(n)| \leq 1 \cdot |g(n)| \leq |h(n)|$
  - Observe também que t é $O(r)$ para $r(n) = n^4$, pois:
    * $\frac{1}{2}n^3 + \frac{1}{2}n^2 \leq n^3 \leq n^4$, $\forall n \geq 1$

- Ao analisar algoritmos, buscamos a função simples g de "crescimento mais lento" para a qual f é $O(g)$.
  - algumas vezes ela vem de um "conjunto de referência"
    * tal como as funções da forma x^n, para n dado

- É comum substituirmos g em $O(g)$ pela fórmula que define g:
  - portanto, escrevemos que "t é $O(n^3)$"
  - esta é a chamada notação "big-O"
- Ainda: dizemos que f e g possuem <u>mesma ordem</u> se:

  f é $O(g)$ E g é $O(f)$

- **Exemplo 3:** As funções $f(n) = 3n^4 - 5n^2$ e $g(n) = n^4$, definidas para inteiros positivos n, possuem mesma ordem.
  - Primeiro, note que:

    $$\begin{aligned} 3n^4 - 5n^2 &\leq 3n^4 + 5n^2 \\ &\leq 3n^4 + 5n^4, \qquad \text{se } n \geq 1 \\ &= 8n^4. \end{aligned}$$

    * daí, fazendo $c = 8$ e $k = 1$, temos $|f(n)| \leq c \cdot |g(n)|$, $\forall n \geq k$
  - Conversamente:

    $n^4 = 3n^4 - 2n^4 \leq 3n^4 - 5n^2$, se $n \geq 2$

    * isto ocorre porque, se $n \geq 2$, então: $2n^4 > 5n^2$
    * daí, usando 1 para c e 2 para k, concluímos que g é $O(f)$.

- Se f é $O(g)$ mas g não é $O(f)$, dizemos que:

  f é de <u>ordem mais baixa</u> do que g , ou que:

  f cresce mais lentamente do que g

- **Exemplo 4:** $f(n) = n^5$ é de ordem mais baixa do que $g(n) = n^7$.
  - É claro que, se $n \geq 1$, então $n^5 \leq n^7$.
  - Agora suponha que existam c e k tais que:

    $n^7 \leq cn^5$, $\forall n \geq k$

    * então <u>escolha</u> um N tal que $N > k$ e $N^2 > c$
    * daí: $N^7 \leq cN^5 < N^2 \cdot N^5$
    * mas isto é uma contradição!
  - Portanto, f é $O(g)$ mas g não é $O(f)$
    * e f é de ordem mais baixa do que g
    * o que, é claro, concorda com a idéia usual sobre n^5 e n^7

- Com a ajuda da notação big-O, podemos determinar se é prático usar um certo algoritmo para resolver um problema à medida que o tamanho dos dados de entrada cresce.
  - Exemplo:
    - temos dois algoritmos para resolver um problema:
      - um utiliza $100n^2 + 17n + 4$ operações
      - o outro utiliza n^3 operações
    - a notação big-O mostra que o primeiro usa muito menos operações quando n é grande
      - embora gaste menos operações para n pequeno $(n = 10$, por exemplo)

- Note que a notação big-O também funciona com funções definidas sobre os reais.

- Para encontrar as constantes:
  - primeiro, selecione um valor de k para o qual o tamanho de $|f(x)|$ pode ser prontamente estimado quando $x \geq k$
  - verificar se é possível encontrar um valor de C para o qual $|f(x)| \leq C|g(x)|$ para $x \geq k$

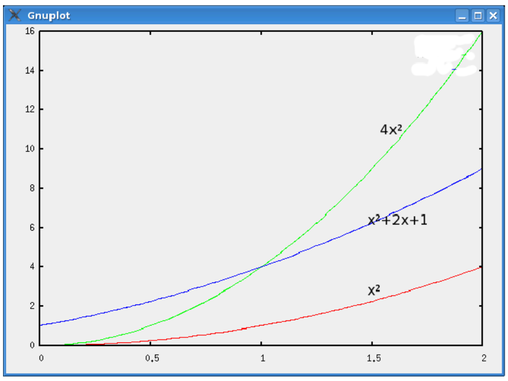
- **Exemplo:** Mostre que $f(x) = x^2 + 2x + 1$ é $O(x^2)$

  Solução:
  - podemos prontamente estimar o tamanho de $f(x)$ quando $x \geq 1$:

    $x \leq x^2$ e $1 \leq x^2$ quando $x \geq 1$
  - segue então que:

    $0 \leq x^2 + 2x + 1 \leq x^2 + 2x^2 + x^2 = 4x^2$
  - assim, fazendo $c = 4$ e $k = 1$, temos que $f(x)$ é $O(x^2)$, pois:

    $f(x) = x^2 + 2x + 1 \leq 4x^2$, sempre que $x \geq 1$



- Observe que na relação "$f(x)$ é $O(x)$", x^2 pode ser trocada por qualquer função com valores maiores do que x^2.
  - Exemplo:

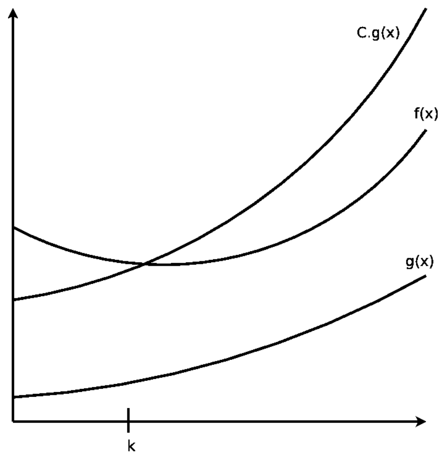
    $f(x)$ é $O(x^3)$

    $f(x)$ é $O(x^2 + 2x + 1)$, etc.

- Mas $f(x) = x^2 + 2x + 1$ e $g(x) = x^2$ possuem mesma ordem.

- Note ainda que não é aceitável escrever: $f(x) = O(g(x))$
  - big-O só significa que existe uma desigualdade válida relacionando valores das funções f e g
  - para valores suficientemente grandes nos respectivos domínios
- Mas está correto dizer que: $f(x) \in O(g(x))$
  - $O(g(x))$ representa o conjunto de todas as funções que são $O(g(x))$

- Ilustração de "$f(x)$ é $O(g(x))$" (ou: $f(x) < c.g(x)$ para $x > k$)



- **Exemplo:** Mostre que $7x^2$ é $O(x^3)$

  Solução:
  - Note que, quando $x \geq 7$, temos: $7x^2 \leq x^3$
    - (multiplicar ambos os lados de $x \geq 7$ por x^2)
  - Logo, as constantes $c = 1$ e $k = 7$ mostram que $7x^2$ é $O(x^3)$
  - Alternativamente:
    - quando $x \geq 1$, temos que $7x^2 \leq 7x^3$
    - de modo que $c = 7$ e $k = 1$ também servem

- **Exemplo:** Mostre que n^2 não é $O(n)$

  Solução:
  - Temos que mostrar que nenhum par de constantes c e k satisfaz:
    $n^2 \leq cn$, sempre que $n \geq k$
  - Para ver que as constantes não existem, note que, quando $n > 0$:
    - pode-se dividir ambos os lados de $n^2 \leq cn$ por n
    - obtendo: $n \leq c$
  - Note, então, que, não importa quem sejam c e k:
    - a desigualdade $n \leq c$ não pode valer para todo n, com $n \geq k$

- **Exemplo:** Mostre que x^3 não é $O(7x^2)$

  Solução:

  – Temos que mostrar que nenhum par de constantes c e k satisfaz:

  $x^3 \leq c(7x^2)$, sempre que $x \geq k$

  – A desigualdade $x^3 \leq c(7x^2)$ é equivalente a: $x \leq 7c$

  – Note que não existe c para o qual $x \leq 7c$ para todo $x \geq k$

  * não importa quem seja k, pois x pode ser tornado tão grande quanto se queira

  – Segue que não existem c e k para os quais exista a relação proposta.

Resultados "big-O" importantes

- É comum o uso de polinômios para estimar o crescimento de funções.
- O teorema a seguir mostra que o termo principal de um polinômio domina o seu crescimento.
- **Teorema 1:** Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, aonde $a_0, a_1, \ldots, a_{n-1}, a_n$ são números reais. Então $f(x)$ é $O(x^n)$.

- **Exemplo 1(/3):** Use notação big-O para estimar a quantidade de operações envolvida na soma dos primeiros n inteiros positivos.

  Solução:

  – Como cada inteiro da soma é $< n$, segue que:

  $1 + 2 + \cdots + n \leq n + n + \cdots + n = n^2$

  – Então, tomando-se $c = 1$ e $k = 1$, concluímos que:

  $1 + 2 + \cdots + n$ é $O(n^2)$ $\square$

- **Exemplo 2(/3):** Forneça estimativas big-O para a função fatorial e para o seu logaritmo.

  – Nota: a função fatorial é definida por: $n! = 1 \cdot 2 \cdot 3 \cdots n$, $(0! = 1)$

  – Note que a função fatorial crece rapidamente:

  $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, ..., $20! = 2.432.902.008.176.640.000$

  Solução:

  – Note que cada termo no produto não excede n.

  – Portanto: $$\begin{aligned} n! &= 1 \cdot 2 \cdot 3 \cdots n \\ &\leq n \cdot n \cdot n \cdots n \\ &= n^n \end{aligned}$$

  – o que mostra que $n!$ é $O(n^n)$ (tomando $c = 1$ e $k = 1$)

- **Exemplo 2 (cont.):** Estimativa big-O para o log da função fatorial:
  - Tomando log de ambos os lados, obtemos:
    $log\ n! \leq log\ n^n = n.log\ n$
  - o que significa que:
    $log\ n!$ é $O(n.log\ n)$ (tomando $c = 1$ e $k = 1$)

- **Exemplo 3(/3):** No cap sobre indução vimos que, para $n \in \mathbb{Z}^+$: $n \leq 2^n$
  - Isto permite concluir que: n é $O(2^n)$ $(k = 1, c = 1)$
  - Como o logaritmo é crescente, podemos tomar log desta desigualdade: $log\, n \leq n$
  - Segue que $log\, n$ é $O(n)$ $(k = 1,\ c = 1)$

Leituras sobre Crescimento de funções

- Kolman5: item 5.3
- Rosen6: item 3.2

8) Contagem I

8.1) O Princípio do Pombal

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

O Princípio do Pombal

- Consiste em outra técnica de prova (que frequentemente usa algum método de contagem)

- **Teorema:** Se n pombos ocupam m cubículos de um pombal, e $m < n$, então pelo menos um cubículo contém 2 ou mais pombos.

  Prova:
  - suponha que cada cubículo contém no máximo um pombo
  - então no máximo m pombos ocupam cubículos
  - mas, uma vez que $m < n$, nem todos os pombos ocupam cubículos no pombal $\Rightarrow$ contradição
  - ou seja, pelo menos um cubículo contém 2 ou mais pombos $\square$

- Quase trivial, muito fácil de usar, e inesperadamente poderoso em situações muito interessantes...

- **Exemplo 1:** se 8 pessoas são escolhidas de qualquer modo de algum grupo, pelo menos duas delas terão nascido no mesmo dia da semana.
  - Aqui cada pessoa (pombo) é associada ao dia da semana (cubículo) em que nasceu.
  - Como há 8 pessoas e 7 dias da semana, o princípio leva ao resultado.

- Nota 1: note que o princípio provê uma prova de existência:
  - "deve haver um objeto (ou objetos) com uma certa característica".
  - No exemplo anterior, o princípio garante que deve haver duas pessoas com uma característica
    * mas não ajuda a identificá-las.

- Nota 2: para poder aplicar o princípio, temos que identificar pombos (objetos) e cubículos (categorias da característica desejada).
  - E temos que ser capazes de <u>contar</u> o número de pombos e o número de cubículos...

- **Exemplo 2:** mostre que, se escolhermos 5 números quaisquer de 1 a 8, então existirão dois deles cuja soma será igual a 9
  - construa 4 conjuntos diferentes com dois números cuja soma é 9:

$$A_1 = \{1, 8\}, \quad A_2 = \{2, 7\}, \quad A_3 = \{3, 6\}, \quad A_4 = \{4, 5\}$$

- cada um dos 5 números tem que pertencer a um destes conjuntos
- uma vez que existem apenas 4 conjuntos, o princípio do pombal garante que 2 dos nros escolhidos devem pertencer ao mesmo conjunto
  * a soma destes números é 9 □

- **Exemplo 3:** mostre que, se escolhermos 11 números quaisquer em $\{1, 2, \ldots, 20\}$, então algum deles será um múltiplo de algum outro.
  - Chave para a solução: criar 10 ou menos "cubículos de pombo"
    * de modo que cada número escolhido seja associado a apenas um cubículo
    * e também que, quando x e y sejam associados ao mesmo cubículo, nós tenhamos certeza de que $x|y$ ou $y|x$
  - Fatores são uma característica natural para explorar:
    * existem 8 números primos entre 1 e 20
    * só que: saber que x e y são múltiplos do mesmo primo não garante que $x|y$ ou $y|x$...
  - Outra tentativa: existem 10 ímpares entre 1 e 20
    * todo inteiro > 0 pode ser escrito como $n = 2^k m$, onde m é ímpar e $k \geq 0$
      · (basta fatorar todas as potências de 2 em n)
      · m é "a parte ímpar de n"
    * se 11 nros são escolhidos de $\{1, 2, \ldots, 20\}$, então 2 deles deverão ter a mesma parte ímpar
      · do princípio: existem 11 nros (pombos) mas apenas 10 ímpares entre 1 e 20 (cubículos)
      · (apenas 10 "candidatos a partes ímpares" dos 11)
    * sejam n_1 e n_2 dois nros escolhidos com mesma parte ímpar
    * então devemos ter, para algum k_1 e algum k_2:
      $n_1 = 2^{k_1} m \quad \text{e} \quad n_2 = 2^{k_2} m$
      · se $k_1 \geq k_2$, então n_1 é um múltiplo de n_2
      · caso contrário, n_2 é um múltiplo de n_1 □

- **Exemplo 3a:** Mostre que no meio de $n + 1$ inteiros positivos $\leq 2n$ deve existir um inteiro que divide um dos outros.
  - Escreva cada um dos $n + 1$ inteiros como:
    $a_j = 2^{k_j}.q_j \quad (j = 1, 2, \ldots, n + 1) \quad \text{onde:} \quad k_j \geq 0$
    $q_1, q_2, \ldots, q_{n+1}$: ímpares e $< 2.n$
  - Mas: existem apenas n ímpares $< 2.n$
  - Logo: pelo Princípio do Pombal, dois destes q_i's devem ser iguais
    * ou seja, $\exists i, j$ tais que: $q_i = q_j = q$
    * então: $a_i = 2^{k_i}.q$ e $a_j = 2^{k_j}.q$
    * daí: se $k_i < k_j$, então: $a_i | a_j$
      se $k_i > k_j$, então: $a_j | a_i$ □

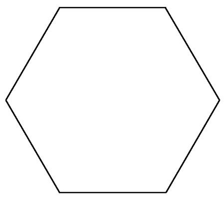
- **Exemplo 4:** Durante um mês de 30 dias, um carteiro entrega *pelo menos uma carta por dia*, mas não mais do que 45 cartas. Mostre que deve existir algum período de dias consecutivos durante o qual este carteiro entrega exatamente 14 cartas.

- Seja $\boldsymbol{a_j} =$ nro de cartas entregues no j-ésimo dia do mês ou antes
- Então $\boldsymbol{a_1, a_2, \ldots, a_{30}}$ é uma sequência *crescente* de inteiros positivos distintos,

  aonde: $\boldsymbol{1 \leq a_j \leq 45}$
- Além disto: $\boldsymbol{a_1 + 14, a_2 + 14, \ldots, a_{30} + 14}$ *também é* uma sequência crescente de inteiros positivos distintos

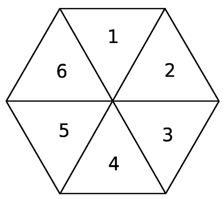
  aonde: $\boldsymbol{15 \leq a_j + 14 \leq 59}$
- E os 60 inteiros positivos $\boldsymbol{a_1, a_2, \ldots, a_{30}, a_1 + 14, a_2 + 14, \ldots, a_{30} + 14}$ são todos $\boldsymbol{\leq 59}$
- Pelo princípio, dois destes inteiros são iguais
- Daí, como os $\boldsymbol{a_j}$ *são distintos* e os $\boldsymbol{a_j + 14}$ *também*, $\exists \boldsymbol{i}$ e $\boldsymbol{j}$ tais que:
  - $\boldsymbol{a_i = a_j + 14}$
- Logo: $\boldsymbol{14}$ cartas *foram entregues* do dia $\boldsymbol{j+1}$ ao dia $\boldsymbol{i}$ $\square$

- **Exemplo 5:** considere a região abaixo, limitada por um hexágono cujos lados têm comprimento de 1 unidade.



Mostre que, se quaisquer 7 pontos são escolhidos nesta região, então deve haver dois destes que não estão distantes mais do que uma unidade.

- Divida a região em 6 triângulos equiláteros:



- Se 7 pontos são escolhidos na região, podemos associar cada um deles ao triângulo que o contém.
  - (Se o ponto pertencer a mais de um triângulo, associe-o a um deles.)
- Assim, são 7 pontos em 6 regiões:
  - pelo princípio do pombal, pelo menos 2 pontos pertencerão à mesma região
  - estes dois não podem estar afastados mais do que uma unidade. $\square$

- **Exemplo 6:** Camisetas numeradas consecutivamente de 1 a 20 são usadas por 20 alunos candidatos a formar equipe para a maratona de programação da SBC. O treinador propõe que cada equipe de 3 alunos seja identificada por um "número código" igual à soma dos números das camisetas. Mostre que, se forem selecionados 8 (para 2 equipes de 3 alunos + 2 reservas) entre os 20, pode-se formar pelo menos dois times diferentes com o mesmo número código.
  - com os 8 selecionados, pode-se formar $\boldsymbol{{}_8C_3 = 56}$ times diferentes (=pombos)
  - maior número-código possível: $\boldsymbol{18 + 19 + 20 = 57}$
    - menor: $\boldsymbol{1 + 2 + 3 = 6}$

    * portanto, apenas os números-código de 6 a 57 estão disponíveis para os 56 possíveis times
  - pelo princípio, pelo menos dois times poderão ficar com o mesmo número-código
  - o treinador terá que escolher uma outra forma de atribuir números às equipes...

- **Exemplo 7:** Uma função $\boldsymbol{f}$, de um conjunto com $\boldsymbol{k+1}$ ou mais elementos, para um conjunto com $\boldsymbol{k}$ elementos não pode ser injetora.

  Solução:

  - suponha que para cada $\boldsymbol{y}$ no contradomínio de $\boldsymbol{f}$ tenhamos uma caixa contendo todos os elementos $\boldsymbol{x}$ do domínio de $\boldsymbol{f}$ tais que $\boldsymbol{f(x) = y}$
  - uma vez que o domínio contém $\boldsymbol{k+1}$ ou mais elementos, e o contradomínio apenas $\boldsymbol{k}$ elementos, o princípio indica que:
    * uma destas caixas contém dois ou mais elementos $\boldsymbol{x}$ do domínio
  - logo, $\boldsymbol{f}$ não pode ser injetora $\square$

- **Exemplo 8:** Mostre que para todo inteiro $\boldsymbol{n}$, existe um múltiplo de $\boldsymbol{n}$ que possui apenas **0**s e **1**s na sua expansão decimal.

  Solução:

  - seja $\boldsymbol{n}$ um inteiro positivo
  - considere os $\boldsymbol{n+1}$ inteiros $\boldsymbol{1, 11, 111, \ldots, 11\cdots 1}$
  - note que há $\boldsymbol{n}$ restos possíveis quando um inteiro é dividido por $\boldsymbol{n}$
  - uma vez que há $\boldsymbol{n+1}$ inteiros nesta lista:
    * pelo P.P., deve haver dois com o mesmo resto quando divididos por $\boldsymbol{n}$
  - o maior destes inteiros *menos o menor* leva a um múltiplo de $\boldsymbol{n}$
    * o qual possui uma expansão decimal consistindo inteiramente de **0**s e **1**s $\square$

- **Exemplo 9:** Prove o teorema: "Toda sequência de $\boldsymbol{n^2+1}$ nros reais distintos contém uma subsequência de comprimento $\boldsymbol{n+1}$ que ou é estritamente crescente ou estritamente decrescente."

- **Nota:**
  - seja uma sequência de nros reais dada por: $\boldsymbol{a_1, a_2 \ldots, a_N}$
  - uma subsequência desta sequência é uma sequência da forma $\boldsymbol{a_{i_1}, a_{i_2}, \ldots, a_{i_m}}$, aonde: $\boldsymbol{1 \leq i_1 < i_2 < \cdots < i_m \leq N}$
    * "inclui alguns termos da sequência original na sua ordem original"
  - estritamente crescente: cada termo é ¿ do que aquele que o precede
  - estritamente decrescente: cada termo é ¡ do que aquele que o precede

- **Ilustração:**
  - na sequência $\boldsymbol{8, 11, 9, 1, 4, 6, 12, 10, 5, 7}$, com 10 termos,
  - há 4 subsequências crescentes de tamanho 4:
    * $\boldsymbol{1, 4, 6, 12}$
    * $\boldsymbol{1, 4, 6, 7}$

    * $\boldsymbol{1, 4, 6, 10}$
    * $\boldsymbol{1, 4, 5, 7}$
  - e também há uma subsequência decrescente de tamanho 4:
    * $\boldsymbol{11, 9, 6, 5}$

- **Prova: (contradição)**
  - seja $a_1, a_2, \ldots, a_{n^2+1}$ uma sequência de $n^2 + 1$ nros reais distintos
  - vamos associar o par (i_k, d_k) com cada termo a_k da sequência, aonde:
    * i_k: comprimento da subsequência *crescente* mais longa que começa em a_k
    * d_k: comprimento da subseq. *decrescente* mais longa que começa em a_k
  - suponha que não existam subsequências crescentes e nem decrescentes de tamanho $\geq n + 1$
  - então, para $1 \leq k \leq n^2 + 1$, temos que: $1 \leq i_k, d_k \leq n$
  - daí, pela regra do produto, existem n^2 opções para os pares (i_k, d_k)
  - logo, pelo P.P., dois destes $n^2 + 1$ pares teriam que ser iguais
    * ou seja, deveriam existir a_s e a_t, com $s < t$, tais que $i_s = i_t$ e $d_s = d_t$
    * porém, como os termos são *distintos*, temos que: ou $a_s < a_t$ ou $a_t < a_s$
    * se $a_s < a_t$: já que $i_s = i_t$, poderíamos construir uma subsequência crescente de tamanho $i_t + 1$ a partir de a_s ($= a_s$ seguido pela subseq. crescente de tamanho i_t que começa em a_t) $\Rightarrow$ contradição (!!)
    * se $a_s > a_t$, pode-se mostrar que d_s teria que ser $> d_s$ (!!) $\square$

O Princípio do Pombal Estendido

- Note que, se existem m cubículos e mais do que $2m$ pombos:
  - 3 ou mais pombos terão que acomodados em, pelo menos, um dos cubículos
  - (considere a distribuição mais uniforme possível para os pombos)

- Em geral, se o número de pombos é muito maior do que o de cubículos, podemos reescrever o princípio do pombal, de modo a obter uma conclusão mais forte.

- Nota: se n e m são inteiros positivos:

  $\lfloor n/m \rfloor$ significa: "o maior inteiro $\leq n/m$"

  Exemplos: $\lfloor 3/2 \rfloor = 1$, $\lfloor 9/4 \rfloor = 2$, $\lfloor 6/3 \rfloor = 2$

- **Teorema:** Se n pombos são acomodados em m cubículos de um pombal, então um dos cubículos deve conter pelo menos $\lfloor (n-1)/m \rfloor + 1$ pombos.

  Prova (por contradição):
  - se cada cubículo não contém mais do que $\lfloor (n-1)/m \rfloor$ pombos, então o total de pombos é, no máximo:

    $$m \cdot \lfloor (n-1)/m \rfloor \quad \leq \quad m \cdot (n-1)/m \quad = \quad n - 1$$
  - isto contradiz a hipótese, de modo que um dos cubículos deve conter, pelo menos,

    $\lfloor (n-1)/m \rfloor + 1$ pombos. $\square$

- **Exemplo 9:** (extensão do ex. 1) Mostre que, se 30 pessoas quaisquer são selecionadas, então é possível escolher um subconjunto de 5 de modo que todas as 5 tenham nascido no mesmo dia da semana.
  - Associe cada pessoa ao dia da semana em que nasceu
  - Ou seja: 30 pombos estão sendo associados a 7 cubículos
  - Então, pelo P.P.E., com $\boldsymbol{n = 30}$ e $\boldsymbol{m = 7}$:
    * pelo menos $\boldsymbol{\lfloor (30 - 1)/7 \rfloor + 1 = 5}$ destas pessoas devem ter nascido no mesmo dia da semana. □

- **Exemplo 10:** Mostre que, se 30 dicionários em uma biblioteca contêm um total de 61327 páginas, então um dos dicionários deve ter, pelo menos, 2045 páginas.
  - as páginas são os pombos e os dicionários são os cubículos
  - atribua cada página ao dicionário em que aparece
  - então, pelo P.P.E., um dicionário deve conter pelo menos:

    $\boldsymbol{\lfloor 61326/30 \rfloor + 1 \;=\; 2045}$ páginas. □

- **Exemplo 11:** Suponha que se queira conectar **15** PCs e **10** impressoras por meio de cabos. Um cabo pode ser usado para conectar diretamente <u>um</u> PC a <u>uma</u> impressora. Cada impressora aceita apenas uma conexão direta ativa de cada vez. Queremos garantir que, a qualquer momento, qualquer conjunto de **10** PCs ou menos possa acessar simultaneamente impressoras diferentes por meio de conexões diretas. Embora isto possa ser feito conectando-se diretamente todo PC com todas as impressoras (c 150 conexões), qual o mínimo de conexões diretas necessárias para atingir este objetivo?
  - Sejam $\boldsymbol{P_1, P_2, \ldots, P_{15}}$ os PCs e $\boldsymbol{I_1, I_2, \ldots, I_{10}}$ as impressoras
  - Agora suponha que conectemos $\boldsymbol{P_k}$ a $\boldsymbol{I_k}$ para $\boldsymbol{k = 1, 2, \ldots, 10}$
    * e cada um dos $\boldsymbol{P_{11}}$, $\boldsymbol{P_{12}}$, $\boldsymbol{P_{13}}$, $\boldsymbol{P_{14}}$ e $\boldsymbol{P_{15}}$ a todas as 10 impressoras
    * em um total de 60 conexões diretas
  - Com isto, é claro que qualquer conjunto de 10 PCs ou menos pode acessar simultaneamente impressoras diferentes, pois:
    * se o PC $\boldsymbol{P_j}$ estiver incluído ($\boldsymbol{1 \leq j \leq 10}$), ele pode acessar a impressora $\boldsymbol{I_j}$
    * e, para cada inclusão de um PC $\boldsymbol{P_k}$ tal que $\boldsymbol{k \geq 11}$:
      deve haver um PC $\boldsymbol{P_j}$ correspondente não incluído
      de modo que $\boldsymbol{P_k}$ pode acessar a impressora $\boldsymbol{I_j}$
  - Conclusão: **60** conexões são suficientes para resolver o problema
  - Mas será que não dá para resolver com <u>menos</u> conexões??
  - Agora suponha que existam $<$ 60 conexões diretas entre PCs e impressoras:
    * então alguma impressora $\boldsymbol{I_x}$ estaria conectada a no máximo $\boldsymbol{\lfloor 59/10 \rfloor = 5}$ PCs
    * pois: se todas as impressoras estivessem conectadas a 6 PCs ou mais, teria que haver, no mínimo, $\boldsymbol{6 \cdot 10 = 60}$ conexões
      · *"se o total não é 60, algum não chegou a 6"*
    * isto significa que as 9 impressoras restantes não são suficientes para permitir que os outros 10 PCs (os que não estão conectados a esta $\boldsymbol{I_x}$) acessem simultaneamente impressoras diferentes
    * consequentemente, pelo menos 60 conexões diretas são necessárias □

- Exemplo a seguir: aplicação do P.P.E. à "Teoria de Ramsey" (Análise Combinatória - ver Rosen6)

- **Exemplo 12:** Assuma que, em um grupo de *6 pessoas*, cada par de indivíduos consiste de *2 amigos* ou *2 inimigos*. Mostre que, neste caso, existem *3 amigos mútuos* ou *3 inimigos mútuos* no grupo.

  Solução: Seja $\boldsymbol{A}$ uma das seis pessoas:

  – das outras 5 do grupo, tem que existir:
    1. 3 ou mais que são amigos de $\boldsymbol{A}$ OU
    2. 3 ou mais que são inimigos de $\boldsymbol{A}$

  – isto segue do P.P.E., pois se trata de dividir 5 objetos em 2 conjuntos
    * um dos conjuntos vai conter, pelo menos, 3 elementos

  – no caso 1, sejam $\boldsymbol{B}$, $\boldsymbol{C}$ e $\boldsymbol{D}$ os amigos de $\boldsymbol{A}$:
    * se quaisquer 2 destes forem amigos, eles e $\boldsymbol{A}$ formam 3 amigos mútuos
    * caso contrário, $\boldsymbol{B}$, $\boldsymbol{C}$ e $\boldsymbol{D}$ formam um conjunto com 3 inimigos mútuos

  – o caso 2 é similar $\square$

- Nota: sejam os inteiros positivos $\boldsymbol{m, n \geq 2}$:

  – o nro de Ramsey, $\boldsymbol{R(m,n)}$, denota o mínimo de pessoas em uma festa tal que existam $\boldsymbol{m}$ amigos mútuos ou $\boldsymbol{n}$ inimigos mútuos
    * assumindo que todo par de pessoas na festa é de amigos ou de inimigos

  – o exemplo anterior mostra que $\boldsymbol{R(3,3) \leq 6}$
    * na verdade: $\boldsymbol{R(3,3) = 6}$
    * com 5 pessoas, amigas ou inimigas aos pares, pode não ocorrer nem 3 amigos e nem 3 inimigos mútuos (prove!)

- Curiosidades:

  – Difícil achar os valores exatos dos nros de Ramsey

  – Mas pode-se provar propriedades deles, tais como:

    $\boldsymbol{R(m,n) = R(n,m)}$

    $\boldsymbol{R(2,n) = n}, \quad \boldsymbol{\forall n \geq 2}$ inteiro e positivo

  – São conhecidos os valores exatos de apenas 9 nros:

    $\boldsymbol{3 \leq m \leq n}$ e $\boldsymbol{R(4,4)}$

  – Muitos outros estão apenas delimitados, tais como: $\boldsymbol{43 \leq R(5,5) \leq 49}$

Leituras sobre Princípio do Pombal

- Kolman5: item 3.3
- Rosen6: item 5.2

8) Contagem I

8.2) Contagem de conjuntos

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.*

Contagem

- Problemas de Contagem aparecem muito em CC
- Por exemplo: precisamos contar o nro de operações executadas por um algoritmo para poder avaliar a sua complexidade no tempo

Contagem

- Veremos dois princípios básicos da contagem:
  - a regra da soma (ou: "Princípio da Adição")
  - a regra do produto (ou: "Princípio da Multiplicação")

Princípio da adição

- Suponha que uma tarefa pode ser feita em um entre $\boldsymbol{n_1}$ modos possíveis ou um entre $\boldsymbol{n_2}$ modos possíveis
  - onde nenhum dos $\boldsymbol{n_1}$ modos de fazer a tarefa coincide com nenhum dos $\boldsymbol{n_2}$ modos de fazer a mesma tarefa
  - então há $\boldsymbol{n_1 + n_2}$ modos de realizar a tarefa

- Em termos de conjuntos, temos que: $|\boldsymbol{A} \cup \boldsymbol{B}| = |\boldsymbol{A}| + |\boldsymbol{B}|$
  - desde que não haja duas tarefas que possam ser realizadas ao mesmo tempo

- o que pode ser estendido para:

  $$|\boldsymbol{A_1} \cup \boldsymbol{A_2} \cup \ldots \cup \boldsymbol{A_m}| = |\boldsymbol{A_1}| + |\boldsymbol{A_2}| + \ldots + |\boldsymbol{A_m}|$$

  - desde que não haja duas tarefas que possam ser realizadas ao mesmo tempo

Princípio da adição estendido

- Suponha que uma tarefa pode ser feita em:
  - um entre n_1 modos possíveis
  - ou: um entre n_2 modos possíveis
  - ou: etc...
  - ou: um entre n_m modos possíveis

  onde nenhum n_i modos de fazer a tarefa é o mesmo que nenhum dos n_j modos $(i < j)$

  então o número de modos de realizar a tarefa é $n_1 + n_2 + \cdots + n_m$

- **Exemplo 1:** Um estudante tem que escolher um projeto em uma de 3 listas. As 3 listas contêm 23, 15 e 19 possíveis projetos, respectivamente. Quantas possibilidades de projetos há para escolher?

- **Exemplo 2:** Qual o valor de k após a execução do código:

```
k = 0
for i₁ = 1 to n₁
   k = k + 1
end
for i₂ = 1 to n₂
   k = k + 1
end
...
for iₘ = 1 to nₘ
   k = k + 1
end
```

Princípio da multiplicação

- Suponha que um procedimento possa ser subdividido em uma sequência de duas tarefas,
- daí, se:
  - há n_1 modos de fazer a 1^a tarefa
  - e n_2 modos de fazer a 2^a tarefa *depois que a* 1^a *esteja pronta*

  então:

  - há $n_1 \times n_2$ modos de executar o procedimento

- Em termos de conjuntos, se A e B são conjuntos finitos, temos que:

$$|A \times B| = |A|.|B|$$

- **Exemplo 1:** A última parte de um número de telefone tem 4 dígitos. Quantos números de 4 dígitos existem?
  - podemos imaginar como o total de possibilidades de uma seqüência de 4 etapas de escolha de 1 dígito:

    $\mathbf{10 \times 10 \times 10 \times 10 \ = \ 10000}$ $\square$

- **Exemplo 2:** Quantos números de 4 dígitos sem repetições de dígitos existem?
  - novamente temos uma seqüência de 4 etapas
  - mas não podemos usar o que já foi usado
  - assim: $\mathbf{10 \times 9 \times 8 \times 7 \ = \ 5040}$ $\square$

- **Exemplo 3:** Uma empresa com 2 empregados, Luís e Inácio, aluga um andar de um prédio com 12 salas. De quantos modos se pode atribuir salas diferentes a estes 2 empregados?
  - tarefa de atribuir salas aos dois consiste de:
    1. atribuir sala a Luís: o que pode ser feito de 12 modos
    2. então: atribuir sala a Inácio, o que pode ser feito de 11 modos
  - logo, pela regra do produto, existem:

    $\mathbf{12 \times 11 \ = \ 132}$ opções para isto $\square$

- A regra do produto pode ser estendida
- Suponha que um procedimento consiste na execução das tarefas $\boldsymbol{T_1, T_2, \ldots, T_m}$ em sequência

  se:
  - cada tarefa $\boldsymbol{T_i}$ pode ser feita de $\boldsymbol{n_i}$ modos,
  - independente de como as anteriores foram feitas,

  então:
  - há $\boldsymbol{n_1 \times n_2 \times \ldots n_m}$ modos de executar o procedimento
- (Isto pode ser *provado por indução*, a partir da regra do produto para 2 tarefas)

- Em termos de conjuntos:

  $$\boldsymbol{|A_1 \times A_2 \times \ldots \times A_m| = |A_1|.|A_2|.\ldots.|A_m|}$$

- Relação com a regra do produto:
  - execução da tarefa "escolher um elemento em $\boldsymbol{|A_1 \times A_2 \times \ldots \times A_m|}$":
    * escolher um elemento em $\boldsymbol{A_1}$
    * escolher um elemento em $\boldsymbol{A_2}$
    * $\boldsymbol{\ldots}$
    * escolher um elemento em $\boldsymbol{A_m}$

- **Exemplo 4:** Quantas strings de 7 bits existem?
  - cada um dos 7 bits pode ser escolhido de 2 formas (0 ou 1)
  - a regra do produto mostra que existe um total de:

    $\mathbf{2^7 \; = \; 128}$ strings diferentes de 7 bits $\square$

- **Exemplo 5:** Quantas placas de carro estão disponíveis?
  - cada placa é uma sequência de 3 letras e 4 números
  - temos 26 opções para as letras e 10 opções para os números
  - logo, pela regra do produto, temos:

    $\mathbf{26 \times 26 \times 26 \times 10 \times 10 \times 10 \times 10 \; = \; 17576000}$ placas $\square$

- **Exemplo 6:** Quantas funções injetoras existem, de um conjunto com $\boldsymbol{m}$ elementos para um conjunto com $\boldsymbol{n}$ elementos?
  - Nota: quando $\boldsymbol{m > n}$ não existem tais funções
  - Então seja $\boldsymbol{m \leq n}$:
    * suponha que os elementos no domínio sejam $\boldsymbol{a_1, a_2, \ldots, a_m}$
    * temos $\boldsymbol{n}$ modos de escolher $\boldsymbol{f(a_1)}$
    * já que a $\boldsymbol{f}$ é injetora, restam $\boldsymbol{n-1}$ modos de escolher $\boldsymbol{f(a_2)}$
    * em geral: $\boldsymbol{f(a_k)}$ pode ser escolhido de $\boldsymbol{n-k+1}$ modos
  - logo, pela regra do produto, existem:

    $\boldsymbol{n \times (n-1) \times (n-2) \times \cdots \times (n-m+1)}$ funções deste tipo $\square$

- **Exemplo 7:** Qual o valor de $\boldsymbol{k}$ após a execução do código abaixo?

```
k = 0
for i₁ = 1 to n₁
    for i₂ = 1 to n₂
           ⋮
        for iₘ = 1 to nₘ
              k = k + 1
```

  - Seja $\boldsymbol{T_i}$ a tarefa: "passar pelo $\boldsymbol{i}$-ésimo loop"
  - #-vezes em que o loop aninhado é percorrido = #-modos de realizar $\boldsymbol{T_1, \ldots, T_m}$
  - mas: nro de modos de realizar a tarefa $\boldsymbol{T_j}$ é $\boldsymbol{n_j}$
    * passa-se pelo $\boldsymbol{j}$-ésimo loop uma vez para cada inteiro $\boldsymbol{i_j}$ $\boldsymbol{(1 \leq i_j \leq n_j)}$
  - pela regra do produto, o loop aninhado é percorrido $\boldsymbol{n_1 \times n_2 \times \cdots n_m}$ vezes

Ambos os Princípios

- **Exemplo:** Cada usuário em um dado sistema tem uma senha com **6** a **8** caracteres, onde:
  - cada caracter é uma letra maiúscula ou um número
  - cada senha tem que conter pelo menos 1 número

  então quantas possibilidades de senhas existem?

  Resposta:
  - Sejam $\boldsymbol{P_6}$, $\boldsymbol{P_7}$, $\boldsymbol{P_8}$ = senhas com 6, 7 e 8 caracteres
  - Cálculo de $\boldsymbol{P_6}$:
    * strings de letras maiúsculas e números com 6 caracteres = $36^{\mathbf{6}}$
      · *incluindo as sem número algum*
    * strings de letras maiúsculas e sem nro algum = $26^{\mathbf{6}}$
    * logo: $\boldsymbol{P_6 = 36^6 - 26^6}$
  - De maneira similar: $\boldsymbol{P_7 = 36^7 - 26^7}$

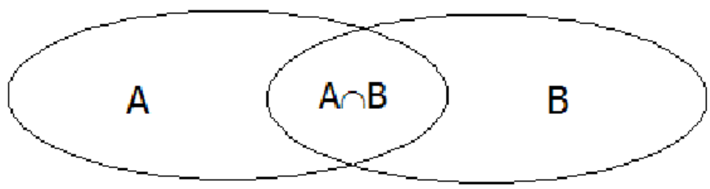
    $\boldsymbol{P_8 = 36^8 - 26^8}$
  - Total = $\boldsymbol{P_6 + P_7 + P_8 = 2.684.483.063.360}$ senhas □

Princípio da inclusão e exclusão

- **Exemplo:** Sabe-se que em uma aula de uma certa disciplina da Medicina há 10 mulheres e 40 formandos. Quantos estudantes desta aula são mulheres ou formandos?
  - Provavelmente, a resposta correta não é "adicionar a quantidade de mulheres e formandos"
    * mulheres formandas seriam contadas duas vezes
  - Logo, o nro de mulheres ou formandos é
    * a soma do nro de mulheres com o nro de formandos
    * menos o nro de mulheres formandas

- Se $\boldsymbol{A}$ e $\boldsymbol{B}$ são conjuntos finitos, então:

$$|\boldsymbol{A} \cup \boldsymbol{B}| = |\boldsymbol{A}| + |\boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{B}|$$



- **Exemplo:** Sejam $A = \{a, b, c, d, e\}$ e $B = \{c, e, f, h, k, m\}$
  - $A \cup B = \{a, b, c, d, e, f, h, k, m\}$
  - $A \cap B = \{c, e\}$
  - $|A \cup B| = 9 \qquad |A| = 5 \qquad |B| = 6 \qquad |A \cap B| = 2$
  - Verificando:

    $|A \cup B| = 9 = 5 + 6 - 2 = |A| + |B| - |A \cap B|$

- **Exemplo:** Suponha que haja 450 calouros no CTC da UFSC. Destes, 48 estão cursando Computação, 98 estão cursando Eng. Mecânica e 18 estão em ambos os cursos. Quantos não estão cursando Computação nem Eng. Mecânica?
  - seja $A =$ conjunto dos calouros em Computação
  - e seja $B =$ conjunto dos calouros em Eng. Mecânica
    - então: $|A| = 48 \qquad |B| = 98 \qquad |A \cap B| = 18$
  - logo: $|A \cup B| = |A| + |B| - |A \cap B| = 48 + 98 - 18 = 128$
    - (**128** calouros estão cursando Comp. ou Eng. Mec.)
  - Assim: há $450 - 128 = 322$ calouros que não estão em nenhum dos 2 cursos.

- **Exemplo:** Uma companhia de computação deve contratar 25 programadores para lidar com tarefas de programação de sistemas e 40 programadores para programação de aplicativos. Dos contratados, 10 terão que realizar tarefas de ambos os tipos. Quantos programadores devem ser contratados?
  - $A =$ conjunto de programadores para sistemas
  - $B =$ conjunto de programadores para aplicativos
  - Deve-se ter $|A \cup B|$ programadores = 55

- **Exemplo:** Quantas strings de **8** bits começam com um **1** ou terminam com **00**?
  - Pela regra do produto:
    - podemos construir uma string de **8** bits que começa com **1** de 2^7 modos
    - podemos construir uma string de **8** bits que termina com **00** de 2^6 modos
  - Porém, alguns modos de construir uma string começando com **1** são os mesmos que os de construir uma string terminando com **00**:
    - existem 2^5 modos de construir uma string assim
  - Logo, a resposta é: $128 + 64 - 32 = 160$ $\square$

- **Exemplo (aux):** Quantos inteiros positivos $\leq n$ são divisíveis por um inteiro d?
  - os inteiros positivos divisíveis por d são todos os inteiros na forma $d.k$
  - logo, o "nro de inteiros positivos $\leq n$ divisíveis por d" =

    = "nro de inteiros k tais que $0 < d.k \leq n$ "

    = "nro de inteiros k tais que $0 < k \leq n/d$ "
  - portanto, existem $\lfloor n/d \rfloor$ inteiros positivos $\leq n$ que são divisíveis por d $\square$

- **Exemplo:** Quantos inteiros positivos $\leq \mathbf{1000}$ são divisíveis por $\mathbf{7}$ ou por $\mathbf{11}$?

  - Seja $\boldsymbol{A} = \{$ inteiros positivos $\leq \mathbf{1000}$ que são divisíveis por $\mathbf{7}\}$
  - Seja $\boldsymbol{B} = \{$ inteiros positivos $\leq \mathbf{1000}$ que são divisíveis por $\mathbf{11}\}$
  - Então:

    $\boldsymbol{A} \cup \boldsymbol{B} = \{$ inteiros positivos $\leq \mathbf{1000}$ que são divisíveis por $\mathbf{7}$ ou $\mathbf{11}\}$
    $\boldsymbol{A} \cap \boldsymbol{B} = \{$ inteiros positivos $\leq \mathbf{1000}$ que são divisíveis por $\mathbf{7}$ e $\mathbf{11}\}$
  - Do ex. anterior, sabemos que, entre os inteiros positivos $\leq \mathbf{1000}$, existem:

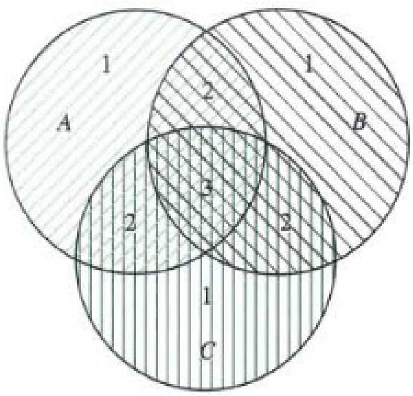
    $\lfloor \mathbf{1000/7} \rfloor$ inteiros divisíveis por $\mathbf{7}$ e
    $\lfloor \mathbf{1000/11} \rfloor$ inteiros divisíveis por $\mathbf{11}$
  - Mas, como $\mathbf{7}$ e $\mathbf{11}$ são relativamente primos:
    * os inteiros divisíveis por $\mathbf{7}$ e por $\mathbf{11}$ são os divisíveis por $\mathbf{7 \times 11}$
    * logo: há $\lfloor \mathbf{1000/(7 \times 11)} \rfloor$ inteiros $\leq \mathbf{1000}$ divisíveis por $\mathbf{7}$ e por $\mathbf{11}$
  - A quantidade procurada é, portanto, dada por:

$$\begin{aligned} |\boldsymbol{A} \cup \boldsymbol{B}| &= |\boldsymbol{A}| + |\boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{B}| \\ &= \lfloor \tfrac{\mathbf{1000}}{\mathbf{7}} \rfloor + \lfloor \tfrac{\mathbf{1000}}{\mathbf{11}} \rfloor - \lfloor \tfrac{\mathbf{1000}}{\mathbf{7 \times 11}} \rfloor \\ &= \mathbf{142 + 90 - 12} \\ &= \mathbf{220} \qquad \square \end{aligned}$$

- Vamos agora deduzir uma fórmula para o nro de elementos na união de um nro finito ($\boldsymbol{n}$) de conjuntos
  - esta fórmula é chamada de Princípio da inclusão e exclusão
- Vamos iniciar pelo caso em que temos 3 conjuntos $\boldsymbol{A}, \boldsymbol{B}$ e $\boldsymbol{C}$...

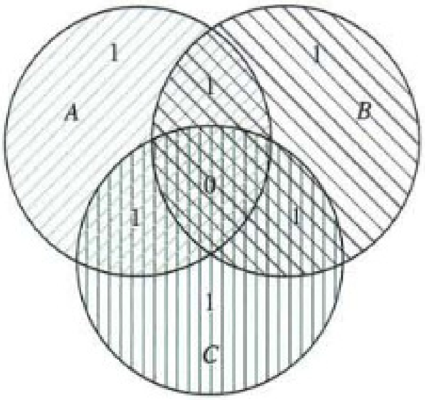
NRO DE ELEMENTOS NA UNIÃO DE 3 CONJUNTOS

- Primeiro, note que $|\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}|$ conta:
  - $\mathbf{1}\times$ cada elemento que está em exatamente um dos 3 conjuntos
  - $\mathbf{2}\times$ os elementos que estão em exatamente dois dos 3 conjuntos
  - $\mathbf{3}\times$ os elementos que estão em todos os 3 conjuntos



- Para remover o excesso, subtraímos os elementos nas intersecções de todos os pares dos 3 conjuntos, obtendo:

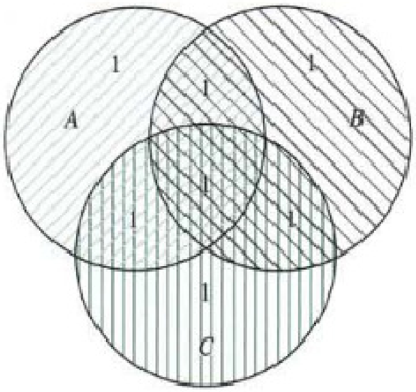
$$|\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}| - |\boldsymbol{A} \cap \boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{C}| - |\boldsymbol{B} \cap \boldsymbol{C}|$$



- Problema: a contagem dos elementos que ocorrem em todos os conjuntos foi zerada
  - pois eles ocorrem em todas as 3 intersecções de conjuntos tomadas 2 a 2

- Para consertar esta "sub-avaliação", adicionamos os elementos que estão na intersecção dos 3 conjuntos:

$$|\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}| = |\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}| - |\boldsymbol{A} \cap \boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{C}| - |\boldsymbol{B} \cap \boldsymbol{C}| + |\boldsymbol{A} \cap \boldsymbol{B} \cap \boldsymbol{C}|$$



- Esta expressão final conta cada elemento apenas uma vez
  - não importando se ele está em 1, 2 ou 3 dos conjuntos

- **Exemplo 1:** Sejam $\boldsymbol{A = \{a, b, c, d, e\}}$, $\boldsymbol{B = \{a, b, e, g, h\}}$, e $\boldsymbol{C = \{b, d, e, g, h, k, m, n\}}$. Verifique o princípio da inclusão-exclusão neste caso.

  $\boldsymbol{A \cup B \cup C = \{a, b, c, d, e, g, h, k, m, n\}}$

  $\boldsymbol{A \cap B = \{a, b, e\}}$, $\quad \boldsymbol{A \cap C = \{b, d, e\}}$, $\quad \boldsymbol{B \cap C = \{b, e, g\}}$

  $\boldsymbol{A \cap B \cap C = \{b, e\}}$

  De modo que:

  $\boldsymbol{|A \cup B \cup C| = 10}$

  $\boldsymbol{|A| = 5}$, $\quad \boldsymbol{|B| = 5}$, $\quad \boldsymbol{|C| = 8}$

  $\boldsymbol{|A \cap B| = 3}$, $\quad \boldsymbol{|A \cap C| = 3}$, $\quad \boldsymbol{|B \cap C| = 4}$

  $\boldsymbol{|A \cap B \cap C| = 2}$

  - Portanto:

    $\boldsymbol{|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C| = 5+5+8-3-3-4+2 = 10}$

  - O princípio é verificado. $\square$

- **Exemplo 2:** Uma pesquisa de opinião foi feita sobre as formas de deslocamento para o trabalho dos cidadãos de Fpolis. Solicitou-se a cada entrevistado que marcasse ÔNIBUS, AMARELINHO ou CARRO como o seu modo preferencial de se deslocar. Era permitido marcar mais de uma resposta. Os resultados foram os seguintes: ÔNIBUS, 30 pessoas; AMARELINHO, 35; CARRO, 100; ÔNIBUS e AMARELINHO, 15; ÔNIBUS e CARRO, 15; AMARELINHO e CARRO, 20; todos os 3 modos, 5. Pergunta: quantas pessoas responderam à pesquisa?

  - Sejam $\boldsymbol{O, A}$ ***e*** $\boldsymbol{C}$ os conjuntos das pessoas que marcaram ÔNIBUS, AMARELINHO E CARRO
  - Então, sabemos que:
    - $\boldsymbol{|O| = 30}$, $\quad \boldsymbol{|A| = 35}$, $\quad \boldsymbol{|C| = 100}$
    - $\boldsymbol{|O \cap A| = 15}$, $\quad \boldsymbol{|O \cap C| = 15}$, $\quad \boldsymbol{|A \cap C| = 20}$
    - $\boldsymbol{|O \cap A \cap C| = 5}$
  - portanto: $\boldsymbol{|O| + |A| + |C| - |O \cap A| - |O \cap C| - |A \cap C| + |O \cap A \cap C| = 30 + 55 + 100 - 15 - 15 - 20 + 5}$
    - ou seja, qtde de pessoas que responderam $\boldsymbol{= 120 = |O \cup A \cup C|}$ $\square$

- **Exemplo 3:** Um mercadinho vende apenas brócolis, cenoura e batata. Em determinado dia, este mercadinho atendeu 208 pessoas. Se 114 compraram apenas brócolis, 152 compraram apenas cenouras, 17 apenas batatas, 64 apenas brócolis e cenouras, 12 apenas cenouras e batatas e 8 apenas brócolis e batatas, determine se alguém comprou os 3 produtos simultaneamente.

  - $\boldsymbol{A = \{}$pessoas que compraram brócolis$\boldsymbol{\}}$
  - $\boldsymbol{B = \{}$pessoas que compraram cenouras$\boldsymbol{\}}$
  - $\boldsymbol{C = \{}$pessoas que compraram batatas$\boldsymbol{\}}$

  $\boldsymbol{|A \cup B \cup C| = 208} \quad \boldsymbol{|A| = 114} \quad \boldsymbol{|B| = 152} \quad \boldsymbol{|C| = 17}$

  $\boldsymbol{|A \cap B| = 64} \quad \boldsymbol{|A \cap C| = 8} \quad \boldsymbol{|B \cap C| = 12} \quad \boldsymbol{|A \cap B \cap C| = ?}$

  $\boldsymbol{|A \cap B \cap C| = 208 - 114 - 152 - 17 + 64 + 12 + 8 = 9}$ $\square$

- A seguir, provaremos o Princípio da Inclusão e Exclusão Geral
  - o qual determina quantos elementos estão na união de um nro finito de conjuntos finitos

- **Teorema:** Sejam $A_1, A_2, \ldots, A_n$ conjuntos finitos. Então:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| +$$

$$+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \cdots +$$

$$+ (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

Prova: (mostrar que cada elemento da união é contado exatamente uma vez pelo lado direito da equação)

  - Suponha que a é membro de exatamente r dos conjuntos $A_1, A_2, \ldots, A_n$:
    * então a é contado é contado $\binom{r}{1}$ vezes por $\sum |A_i|$
    * e a é contado $\binom{r}{2}$ vezes por $\sum |A_i \cap A_j|$
    * em geral: ele é contado $\binom{r}{m}$ vezes pela soma que envolve m dos A_i
    * ou seja, este elemento é contado exatamente:
      $\binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \cdots + (-1)^{r+1}\binom{r}{r}$ vezes pelo lado direito desta equação
  - Mas (propriedade dos coefs binomiais): $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$
  - De modo que: $\binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \cdots + (-1)^{r+1}\binom{r}{r} = \binom{r}{0} = 1$
  - Portanto, cada elemento na união é contado exatamente 1 vez pelo lado direito da equação □

- O princípio da inclusão-exclusão fornece uma fórmula para o nro de elementos na união de n conjuntos, para todo inteiro positivo n

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| +$$

$$+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \cdots +$$

$$+ (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

  - há termos nesta fórmula para o nro de elementos na intersecção de todo subconjunto não vazio da coleção de n conjuntos
  - logo, existem $2^n - 1$ termos nesta fórmula

- **Exemplo:** Forneça uma fórmula para o nro de elementos na união de 4 conjuntos

  Solução: o princípio da inclusão-exclusão mostra que:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4| = {} & |A_1| + |A_2| + |A_3| + |A_4| + \\ & -|A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| \\ & -|A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + \\ & +|A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_4|\end{aligned}$$

  - Note que esta fórmula contém 15 termos diferentes
    * *um para cada subconjunto não vazio de* $\{A_1, A_2, A_3, A_4\}$

FORMA ALTERNATIVA

- Há uma forma alternativa do princípio da inclusão-exclusão
  - útil, por exemplo, em problemas que pedem o nro de elementos, em um dado conjunto, que não possuem nenhuma das n propriedades $P_1, P_2, \ldots, P_n$

- Seja A_i o subconjunto contendo os elementos que possuem a propriedade P_i

- Nro de elementos com todas as propriedades $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$:

  $N(P_{i_1}, P_{i_2}, \ldots, P_{i_k})$

- Em termos de conjuntos, temos: $|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = N(P_{i_1}, P_{i_2}, \ldots, P_{i_k})$

- Daí, o nro de elementos <u>sem nenhuma das propriedades $P_1, P_2, \ldots, P_n$</u> fica:

$$N(P_1' P_2' \cdots P_n') = N - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

  - $N =$ nro de elementos no conjunto

- Então, do Princípio da Inclusão-Exclusão, vemos que:

$$N(P_1' P_2' \cdots P_n') = N - |A_1 \cup A_2 \cup \cdots \cup A_n| =$$

$$= N - \sum_{1 \le i \le n} N(P_i) + \sum_{1 \le i < j \le n} N(P_i P_j) +$$

$$- \sum_{1 \le i < j \le n} N(P_i P_j P_k) + \cdots + (-1)^n N(P_1 P_2 \cdots P_n)$$

- **Exemplo:** Quantas soluções existem em: $\boldsymbol{x_1 + x_2 + x_3 = 11}$?

  $\boldsymbol{x_1, x_2}$ e $\boldsymbol{x_3}$ são inteiros não-negativos

  $\boldsymbol{x_1 \leq 3}$, $\boldsymbol{x_2 \leq 4}$ e $\boldsymbol{x_3 \leq 6}$

  Solução:

  - Uma solução tem propriedade $\boldsymbol{P_1}$ se $\boldsymbol{x_1 > 3}$, $\boldsymbol{P_2}$ se $\boldsymbol{x_2 > 4}$ e $\boldsymbol{P_3}$ se $\boldsymbol{x_3 > 6}$
  - E o nro de soluções satisfazendo $\boldsymbol{x_1 \leq 3}$, $\boldsymbol{x_2 \leq 4}$ e $\boldsymbol{x_3 \leq 6}$ é:

    $$\boldsymbol{N(P_1'P_2'P_3') = N - N(P_1) - N(P_2) - N(P_3) +}$$
    $$\boldsymbol{+N(P_1P_2) + N(P_1P_3) + N(P_2P_3) - N(P_1P_2P_3)}$$

    $\boldsymbol{N}$ = nro total de soluções = $\boldsymbol{C(3+11-1, 11) = 78}$

    $\boldsymbol{N(P_1)}$ = nro de soluções com $\boldsymbol{x_1 > 3 = C(3+7-1,7) = C(9,7) = 36}$

    $\boldsymbol{N(P_2)}$ = nro de soluções com $\boldsymbol{x_2 > 4 = C(3+6-1,6) = C(8,6) = 28}$

    $\boldsymbol{N(P_3)}$ = nro de soluções com $\boldsymbol{x_3 > 6 = C(3+4-1,4) = C(6,4) = 15}$

    $\boldsymbol{N(P_1P_2)}$ = sols com $\boldsymbol{x_1 > 3}$ e $\boldsymbol{x_2 > 4 = C(3+2-1,2) = C(4,2) = 6}$

    $\boldsymbol{N(P_1P_3)}$ = sols com $\boldsymbol{x_1 > 3}$ e $\boldsymbol{x_3 > 6 = C(3+0-1,0) = 1}$

    $\boldsymbol{N(P_2P_3)}$ = sols com $\boldsymbol{x_2 > 4}$ e $\boldsymbol{x_3 > 6 = 0}$

    $\boldsymbol{N(P_1P_2P_3)}$ = sols com $\boldsymbol{x_1 > 3}$, $\boldsymbol{x_2 > 4}$ e $\boldsymbol{x_3 > 6 = 0}$

    $\boldsymbol{N(P_1'P_2'P_3') = 78 - 36 - 28 - 15 + 6 + 1 + 0 - 0 = 6}$ $\square$

O Crivo de Eratóstenes

- O Princípio pode ser usado para achar: nro de primos $\leq$ inteiro positivo dado.

- **Exemplo:** encontrar o nro de primos ≤ 100:

  - Lembre que um inteiro composto $\boldsymbol{n}$ é divisível por um primo $\leq \boldsymbol{\sqrt{n}}$
    - *Seja* $\boldsymbol{n = a \times b}$: *se* $\boldsymbol{a > \sqrt{n}}$ *e* $\boldsymbol{a > \sqrt{n}}$, *então* $\boldsymbol{a \times b > n}$ *(??)*
  - Compostos $\leq \boldsymbol{100}$ devem possuir um fator primo $\leq \boldsymbol{10}$
  - Logo, os primos $\leq \boldsymbol{100}$ são: $\boldsymbol{2, 3, 5}$ e $\boldsymbol{7}$ e
    - todos os inteiros $\leq \boldsymbol{100}$ que não são divisíveis por nenhum deles
  - Aplicando o Princípio da Inclusão-Exclusão:

    propriedade $\boldsymbol{P_1}$ = "um inteiro é divisível por 2"
    propriedade $\boldsymbol{P_2}$ = "um inteiro é divisível por 3"
    propriedade $\boldsymbol{P_3}$ = "um inteiro é divisível por 5"
    propriedade $\boldsymbol{P_4}$ = "um inteiro é divisível por 7"

  - De modo que: "nro de primos $\leq \boldsymbol{100}$" $\boldsymbol{= 4 + N(P_1'P_2'P_3'P_4')}$
  - Como há $\boldsymbol{99}$ nros $\leq \boldsymbol{100}$ e $\geq \boldsymbol{1}$, o princípio estabelece que:

$$N(P_1'P_2'P_3'P_4') = 99 - N(P_1) - N(P_2) - N(P_3) - N(P_4)$$
$$+N(P_1P_2) + N(P_1P_3) + N(P_1P_4) + N(P_2P_3) + N(P_2P_4) + N(P_3P_4)$$
$$-N(P_1P_2P_3) - N(P_1P_2P_4) - N(P_1P_3P_4) - N(P_2P_3P_4)$$
$$+N(P_1P_2P_3P_4)$$

– Consequentemente:

$$N(P_1'P_2'P_3'P_4') = 99 - \lfloor\tfrac{100}{2}\rfloor - \lfloor\tfrac{100}{3}\rfloor - \lfloor\tfrac{100}{5}\rfloor - \lfloor\tfrac{100}{7}\rfloor$$
$$+\lfloor\tfrac{100}{2\cdot 3}\rfloor + \lfloor\tfrac{100}{2\cdot 5}\rfloor + \lfloor\tfrac{100}{2\cdot 7}\rfloor + \lfloor\tfrac{100}{3\cdot 5}\rfloor + \lfloor\tfrac{100}{3\cdot 7}\rfloor + \lfloor\tfrac{100}{5\cdot 7}\rfloor$$
$$-\lfloor\tfrac{100}{2\cdot 3\cdot 5}\rfloor - \lfloor\tfrac{100}{2\cdot 3\cdot 7}\rfloor - \lfloor\tfrac{100}{2\cdot 5\cdot 7}\rfloor - \lfloor\tfrac{100}{3\cdot 5\cdot 7}\rfloor$$
$$+\lfloor\tfrac{100}{2\cdot 3\cdot 5\cdot 7}\rfloor$$
$$= 99 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 + 0$$
$$= 21$$

– Logo, existem $4 + 21 = 25$ primos ≤ 100 □

- O <u>Crivo de Eratóstenes</u> serve para encontrar todos os primos $\leq$ um inteiro dado
- **Exemplo:** procedimento para encontrar todos os primos ≤ 100 é:

  – marcar os inteiros $\neq 2$ que são divisíveis por 2:

1	2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	9	$\underline{10}$
11	$\underline{12}$	13	$\underline{14}$	15	$\underline{16}$	17	$\underline{18}$	19	$\underline{20}$
21	$\underline{22}$	23	$\underline{24}$	25	$\underline{26}$	27	$\underline{28}$	29	$\underline{30}$
31	$\underline{32}$	33	$\underline{34}$	35	$\underline{36}$	37	$\underline{38}$	39	$\underline{40}$
41	$\underline{42}$	43	$\underline{44}$	45	$\underline{46}$	47	$\underline{48}$	49	$\underline{50}$
51	$\underline{52}$	53	$\underline{54}$	55	$\underline{56}$	57	$\underline{58}$	59	$\underline{60}$
61	$\underline{62}$	63	$\underline{64}$	65	$\underline{66}$	67	$\underline{68}$	69	$\underline{70}$
71	$\underline{72}$	73	$\underline{74}$	75	$\underline{76}$	77	$\underline{78}$	79	$\underline{80}$
81	$\underline{82}$	83	$\underline{84}$	85	$\underline{86}$	87	$\underline{88}$	89	$\underline{90}$
91	$\underline{92}$	93	$\underline{94}$	95	$\underline{96}$	97	$\underline{98}$	99	$\underline{100}$

  – 1ro inteiro > 2 que sobra é 3

  – marcar os inteiros $\neq 3$ que são divisíveis por 3:

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{10}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{20}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	25	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{30}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	35	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{40}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{45}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{50}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	55	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{60}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	65	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{70}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{75}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{80}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	85	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{90}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	95	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{100}$

  – 5 é o próximo inteiro que sobra depois do 3

– marcar os inteiros $\neq \mathbf{5}$ que são divisíveis por **5**:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

– o próximo inteiro que sobra é o **7**

<u>Algoritmo</u>:

1. Crie uma lista de inteiros consecutivos de **2** a $\boldsymbol{n}$
2. Faça $\boldsymbol{p} = \mathbf{2}$ (o primeiro primo)
3. Marque todos os múltiplos de $\boldsymbol{p}$
   - pode começar em $\boldsymbol{p^2}$
4. Encontre o primeiro nro que resta na lista depois de $\boldsymbol{p}$ (é o próximo primo)
   - faça $\boldsymbol{p} =$ este nro
5. Repita **3** e **4** até chegar a $\boldsymbol{p^2 > n}$
6. Todos os nros restantes são primos

- Complexidade do algoritmo: $\boldsymbol{O(n \times \log n \times \log\log n)}$

Nro de funções sobrejetoras

- O Princípio da I-E também serve para determinar o nro de funções sobrejetoras de um conjunto com $\boldsymbol{m}$ para um com $\boldsymbol{n}$ elementos

- **Exemplo:** Quantas funções sobrejetoras existem de um conjunto com 6 elementos para um com 3?
  - Suponha que os elementos no codomínio sejam $\boldsymbol{b_1, b_2, b_3}$
  - Seja $\boldsymbol{P_i}$ a propriedade: "$\boldsymbol{b_i}$ não está na imagem da função"
  - Uma função é sobrejetora sse não tiver nenhuma das propriedades $\boldsymbol{P_1, P_2, P_3}$
  - Pelo Princípio da I-E:
  $$\boldsymbol{N(P_1'P_2'P_3') = N - [N(P_1) + N(P_2) + N(P_3)] +}$$
  $$\boldsymbol{+ [N(P_1P_2) + N(P_1P_3) + N(P_2P_3)] - N(P_1P_2P_3)}$$
  onde $\boldsymbol{N} =$ total de funções de um conjunto com 6 elementos para outro com 3
  - Temos que avaliar cada um dos termos do lado direito desta equação...

- **Exemplo:** Funções sobrejetoras de um conjunto com 6 elementos para um com 3:
  - Cálculo de $\boldsymbol{N}$:
    - uma função corresponde à escolha de um dos 3 elementos no codomínio para cada um dos 6 no domínio
    - pela regra do produto: $\boldsymbol{N = 3^6}$
  - Cálculo de $\boldsymbol{N(P_i)}$ (="nro de funções que não possuem $\boldsymbol{b_i}$ em sua imagem"):
    - há duas escolhas para o valor da função em cada elemento do domínio
    - de modo que: $\boldsymbol{N(P_i) = 2^6}$
    - e note que há $\boldsymbol{C(3,1)}$ termos deste tipo
  - Cálculo de $\boldsymbol{N(P_iP_j)}$ (="nro de funções sem $\boldsymbol{b_i}$ nem $\boldsymbol{b_j}$ em sua imagem"):
    - apenas uma escolha para o valor da função em cada elemento do domínio
    - portanto: $\boldsymbol{N(P_iP_j) = 1^6}$
    - e note que há $\boldsymbol{C(3,2)}$ termos deste tipo

$$\boldsymbol{N(P_1'P_2'P_3') = N - [N(P_1) + N(P_2) + N(P_3)] + \\ +[N(P_1P_2) + N(P_1P_3) + N(P_2P_3)] - N(P_1P_2P_3)}$$

  - Temos que:

    $\boldsymbol{N = 3^6}$

    $\boldsymbol{N(P_i) = 2^6}$, com $\boldsymbol{C(3,1)}$ termos deste tipo

    $\boldsymbol{N(P_iP_j) = 1^6}$, com $\boldsymbol{C(3,2)}$ termos deste tipo
  - Ainda: $\boldsymbol{N(P_1P_2P_3) = 0}$
  - Resposta: $\boldsymbol{3^6 - C(3,1) \times 2^6 + C(3,2) \times 1^6 = 540}$ □

- A seguir: generalização deste resultado...

- **Teorema:** Sejam $\boldsymbol{m}$ e $\boldsymbol{n}$ inteiros positivos $\boldsymbol{(m \geq n)}$. Existem:

$$\boldsymbol{n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - \cdots + (-1)^{n-1}C(n,n-1) \times 1^m}$$

funções sobrejetoras de um conjunto com $\boldsymbol{m}$ elementos para um conjunto com $\boldsymbol{n}$ elementos.

Prova: generalização direta do exercício anterior.

- **Exemplo:** De quantos modos se pode atribuir **5** tarefas diferentes a **4** empregados diferentes se cada empregado deve receber pelo menos uma tarefa?
  - atribuição de tarefas = função do conjunto de 5 tarefas para o conjunto de 4 empregados
  - uma atribuição em que cada empregado recebe pelo menos uma tarefa é o mesmo que:
    - um função sobrejetora do conjunto de tarefas para o conjunto de empregados
  - de modo que a resposta é:

    $\boldsymbol{4^5 - C(4,1).3^5 + C(4,2).2^5 - C(4,3).1^5 = 240}$ modos □

- Uma função sobrejetora de um conjunto com $\boldsymbol{m}$ elementos para outro com $\boldsymbol{n}$ elementos corresponde a:
  - um modo de distribuir os $\boldsymbol{m}$ elementos do domínio em $\boldsymbol{n}$ caixas indistinguíveis
    - de maneira que *nenhuma caixa fique vazia*
  - e então associar cada elemento do codomínio a uma caixa

- Ou seja, é o nro de maneiras de distribuir $\boldsymbol{m}$ objetos distinguíveis em $\boldsymbol{n}$ caixas indistinguíveis de modo que nenhuma caixa fique vazia,
  - multiplicado pelo nro de permutações de um conjunto com $\boldsymbol{n}$ elementos

- Logo, o nro de funções sobrejetoras de $\boldsymbol{m}$ para $\boldsymbol{n}$ é $\boldsymbol{n! \times S(m, n)}$
  - aonde $\boldsymbol{S(m, n)}$ é o nro de Stirling do 2o tipo (ver cap 6)
  - o que consiste em uma *outra forma* de deduzir a fórmula para $\boldsymbol{S(m, n)}$

Leituras sobre Contagem

- Rosen6: itens 5.1, 7.5 e 7.6

8) Contagem I

8.3) Arranjos e combinações

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Análise Combinatória

- Técnicas para a contagem de conjuntos são importantes na Ciência da Computação.
- Especialmente na análise de algoritmos

Princípio da Multiplicação

- **Teorema 1 ("Princípio da Multiplicação para a Contagem"):**

  Suponha que duas tarefas devem ser executadas em sequência:

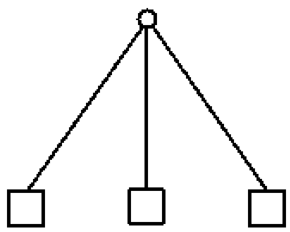
  - se há $\boldsymbol{n_1}$ modos de executar a tarefa $\boldsymbol{T_1}$
  - e se, para um destes modos, $\boldsymbol{T_2}$ pode ser realizada de $\boldsymbol{n_2}$ maneiras

  então a sequência $\boldsymbol{T_1 T_2}$ pode ser realizada de $\boldsymbol{n_1} \times \boldsymbol{n_2}$ formas diferentes.

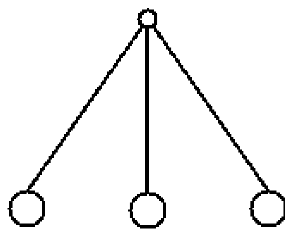
- **Prova:**

  - cada escolha de método para $\boldsymbol{T_1}$ resulta em um caminho diferente para a sequência
    - existem $\boldsymbol{n_1}$ destes métodos
    - para cada um deles, podemos escolher $\boldsymbol{n_2}$ maneiras de realizar $\boldsymbol{T_2}$
  - logo, no todo, serão $\boldsymbol{n_1 n_2}$ opções para a sequência $\boldsymbol{T_1 T_2}$. $\square$

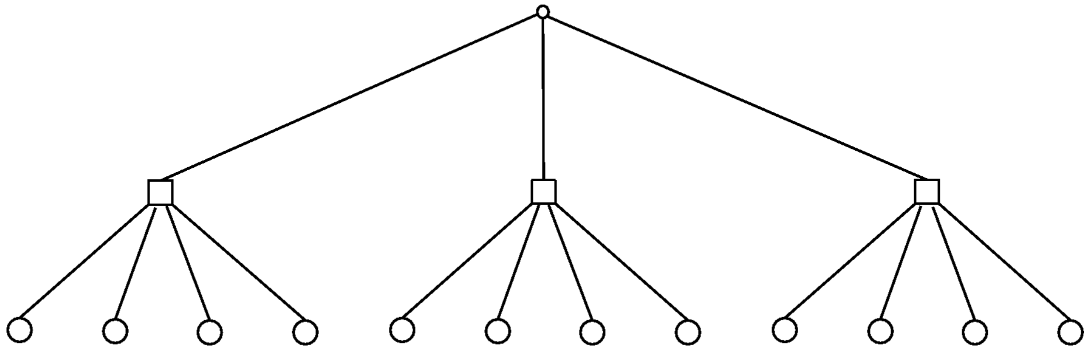
- Ilustração ($\boldsymbol{n_1 = 3}$ e $\boldsymbol{n_2 = 4}$):



modos possíveis para a tarefa 1



modos possíveis para a tarefa 2



modos possíveis para realizar a tarefa 1 e depois a tarefa 2

- Este teorema pode ser estendido...
- **Teorema 2:** suponha que as tarefas $T_1, T_2, \ldots, T_k$ devem ser realizadas em sequência:
  - se T_1 pode ser realizada de n_1 maneiras,
  - e para cada uma destas maneiras, T_2 pode ser realizada de n_2 maneiras,
  - e para cada um dos $n_1 n_2$ modos de realizar $T_1 T_2$ em sequência, T_3 pode ser realizada de n_3 maneiras,
  - e assim por diante,

  então a sequência $T_1 T_2 \cdots T_k$ pode ser realizada de exatamente $n_1 n_2 \cdots n_k$ modos.

  Prova: indução sobre k.

- **Exemplo:** Seja A um conjunto com n elementos. Quantos subconjuntos A possui?

  Solução:
  - cada subconjunto é formado por alguns dos n elementos de A
  - a participação de cada elemento em um dado subconjunto pode ser representada como um "0" ou um "1" em um vetor de comprimento n
  - ora, pelo princípio visto, existem:

    $$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{n\ fatores} = 2^n \quad \text{modos de preencher o vetor}$$

  - e, portanto, 2^n subconjuntos de A. $\square$

- **Questão:**
  - Seja A qualquer conjunto com n elementos e $1 \leq r \leq n$.
  - Quantas sequências diferentes de comprimento r podem ser formadas usando elementos de A se:

    (a) elementos na sequência podem ser repetidos?

    (b) todos os elementos na sequência devem ser distintos?

- Qualquer sequência de comprimento r pode ser formada pelo preenchimento de r "caixas", em ordem, da esquerda para a direita:

			$\cdots$		
caixa 1	caixa 2	caixa 3		caixa $r-1$	caixa r

  - Seja T_i a tarefa: "preencha a caixa i".
  - Então, $T_1 T_2 \cdots T_r$ representa a formação da sequência.

- Caso **(a)** (elementos podem ser repetidos):
  - para cada posição "i", podemos copiar qualquer elemento de A
  - ou seja, há sempre n modos de realizar cada tarefa
  - então, pelo princípio da multiplicação estendido, o número de sequências que podem ser formadas é:

$$\underbrace{n \cdot n \cdot \cdots \cdot n}_{r \ fatores} = n^r$$

- **Teorema 3:**
  - Seja A um conjunto com n elementos e seja $1 \leq r \leq n$.
  - Então o número de sequências de comprimento r que podem ser formadas com elementos de A, permitindo repetições, é n^r.

- **Exemplo:** Quantas "palavras" de 3 letras podem ser formadas com letras do conjunto $\{a, b, y, z\}$, se for permitido repetição?

Arranjos

- Caso **(b)** (elementos distintos):
  - T_1 ainda pode ser realizada de n modos
  - mas aí, qualquer que seja o escolhido, restam só $(n-1)$ opções
    - ou seja: há apenas $(n-1)$ maneiras de realizar T_2
  - isto continua até vermos que T_r pode ser realizada de $(n-(r-1)) = (n-r+1)$ modos
  - portanto, pelo princípio da multiplicação, uma sequência de r elementos distintos de A pode ser montada de $n(n-1)(n-2)\cdots(n-r+1)$ modos

- Uma sequência de r elementos distintos de A é chamada de "**arranjo** (ou permutação) de A tomado r a r".
  - Note que a quantidade destas sequências depende apenas de n.

- **Teorema 4:** Se $\boldsymbol{1 \leq r \leq n}$, então o número de **arranjos** de $\boldsymbol{n}$ objetos tomados $\boldsymbol{r}$ a $\boldsymbol{r}$ é dado por:

  $$\boldsymbol{{}_nP_r = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-r+1) = \frac{n!}{(n-r)!}}$$

  - Nota: na verdade, está fórmula vale para $\boldsymbol{n \geq 0}$ e $\boldsymbol{0 \leq r \leq n}$

- **Exemplo:** Seja $\boldsymbol{A}$ dado por $\boldsymbol{\{1, 2, 3, 4\}}$.
  - Alguns arranjos de $\boldsymbol{A}$ tomados 3 a 3: **124**,**421**,**341**,**243**,...
  - Nro total de arranjos de $\boldsymbol{A}$ tomados 3 a 3:

    $\boldsymbol{{}_4P_3 = 4 \cdot 3 \cdot 2 = 24}$
  - Alguns arranjos de $\boldsymbol{A}$ tomados 2 a 2: **12**,**43**,**31**,**24**,**21**,...
  - Nro total de arranjos de $\boldsymbol{A}$ tomados 2 a 2:

    $\boldsymbol{{}_4P_2 = 4 \cdot 3 = 12}$

- Quando $\boldsymbol{r = n}$, estamos contando todos os distintos arranjos de $\boldsymbol{A}$ em sequências de comprimento $\boldsymbol{n}$
  - Estas sequências são chamadas de permutações.
  - Número de permutações de $\boldsymbol{A}$: $\boldsymbol{{}_nP_n = n!}$

- **Exemplo:** As possíveis permutações de $\boldsymbol{A = \{a, b, c\}}$ são:

  $\boldsymbol{abc, acb, bac, bca, cab}$ e $\boldsymbol{cba}$.

  - Note que o número destas permutações é $\boldsymbol{3! = 6}$.

- **Exemplo:** Quantas "palavras" com 3 letras distintas podem ser formadas das letras da palavra $\boldsymbol{CASO}$?

  Solução: O número é $\boldsymbol{{}_4P_3 = \frac{4!}{(4-3)!} = 24}$ □

COMBINAÇÕES

- O princípio da multiplicação e os métodos de contagem para arranjos e permutações são todos aplicáveis a situações aonde a ordem é importante.
- Combinações estão relacionadas a alguns problemas de contagem aonde a ordem não importa.
- **Questão:**
  - Seja $\boldsymbol{A}$ qualquer conjunto com $\boldsymbol{n}$ elementos e $\boldsymbol{0 \leq r \leq n}$.
  - Quantos subconjuntos diferentes de $\boldsymbol{A}$ existem com $\boldsymbol{r}$ elementos?
  - Os subconjuntos com $\boldsymbol{r}$ elementos de um conjunto $\boldsymbol{A}$ com $\boldsymbol{n}$ elementos são chamados de combinações de $\boldsymbol{A}$ tomado $\boldsymbol{r}$ a $\boldsymbol{r}$.

- **Exemplo:** Seja $\boldsymbol{A = \{1, 2, 3, 4\}}$.
  - Combinações 3 a 3 distintas de $\boldsymbol{A}$:

$$A_1 = \{1,2,3\},\ A_2 = \{1,2,4\},\ A_3 = \{1,3,4\},\ A_4 = \{2,3,4\}$$

- Note que se trata de subconjuntos e não de sequências.
- Portanto: $A_1 = \{2,1,3\} = \{2,3,1\} = \{1,3,2\} = \{3,1,2\} = \{3,2,1\}$

- Agora queremos contar o número de subconjuntos com r elementos para um conjunto A com n elementos (partindo do que já sabemos sobre arranjos):
  - Note que todo arranjo ${}_nA_r$ pode ser produzido pela sequência:

    Tarefa 1: escolha um subconjunto B de A contendo r elementos

    Tarefa 2: escolha uma permutação em particular de B
  - Estamos tentando computar o número de modos de escolher B:
    * vamos chamar este número de C
    * a tarefa 1 pode ser realizada de C modos
    * a tarefa 2 pode ser realizada de $r!$ modos
    * portanto, pelo princípio da multiplicação, o número de modos de realizar ambas as tarefas é dado por: $C \times r!$
    * mas isto também é ${}_nP_r$, logo: $C \times r! = {}_nP_r = \frac{n!}{(n-r)!}$
    * de onde tiramos que: $\boxed{C = \dfrac{n!}{r!(n-r)!}}$

- **Teorema:** Seja A um conjunto com $|A| = n$ e seja $0 \leq r \leq n$.
  - O número de combinações dos elementos de A tomados r a r é:

$$_nC_r = \frac{n!}{r!(n-r)!}$$

    * (que também é o nro de subconjuntos de A com r elementos)

- Observe novamente que o número de combinações r a r de A não depende de A:
  - depende apenas de n e r.

- **Exemplo:** O número de "mãos" de 5 cartas distintas que podem ser distribuídas a partir de um baralho de 52 cartas é:

$$_{52}C_5 = \frac{52!}{5!.47!} = 2598960$$

  - pois a ordem em que as cartas são dadas é irrelevante

- Alguns problemas requerem que a contagem de combinações seja suplementada pelo princípio da multiplicação (ou pelo da adição).

- **Exemplo:** Suponha que uma senha válida consista de 7 caracteres:
  - o 1^o é uma letra escolhida do conjunto $\{A, B, C, D, E, F, G\}$
  - cada um dos outros seis é uma letra qualquer ou um dígito

  Quantas senhas diferentes são possíveis?

- Uma senha pode ser construída pela execução em sequência das tarefas:

  Tarefa 1: escolha uma letra inicial do conjunto dado.

  Tarefa 2: escolha uma sequência de letras e dígitos (pode repetir).
- A tarefa 1 pode ser realizada de $\boldsymbol{{}_7C_1 = 7}$ modos.
- A tarefa 2 pode ser realizada de $\mathbf{36^6 = 2176782336}$ modos
- Daí, pelo Princípio da Multiplicação, existem:

  $\mathbf{7 \times 2176782336 = 15237476352}$ senhas diferentes □

- **Exemplo:** Quantos comitês diferentes de 7 pessoas podem ser formado se cada comitê contém 3 mulheres de um conjunto de 20 e 4 homens de um conjunto de 30 ?
  - Um comitê pode ser formado pela execução das seguintes tarefas em sucessão:

    Tarefa 1: escolha 3 mulheres do conjunto de 20
    - Pode ser realizada de $\boldsymbol{{}_{20}C_3 = 1140}$ modos.

    Tarefa 2: escolha 4 homens do conjunto de 30
    - Pode ser realizada de $\boldsymbol{{}_{30}C_4 = 27405}$ modos.
  - Logo, pelo Princípio da Multiplicação, existem:

    $\mathbf{(1140)(27405) = 31241700}$ comitês diferentes. □
  - *Note que a ordem das escolhas não importa.*

Leituras sobre Arranjos & Combinações

- Kolman5: itens 3.1 e 3.2
- Rosen6: item 5.3

8) Contagem I

8.4) Coeficientes binomiais

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.*

Coeficientes Binomiais

- O nro de combinações $\boldsymbol{r}$ a $\boldsymbol{r}$ de $\boldsymbol{n}$ elementos pode ser denotado por $\binom{n}{r}$
- Estes nros também são chamados de coeficientes binomiais, pois:
  - ocorrem como coeficientes na expansão de potências de expressões binomiais
  - tais como: $(a+b)^n$
- Veremos o Teorema Binomial
  - e algumas das identidades que relacionam coeficientes binomiais
- Expressão binomial: simplesmente a soma de dois termos $(x+y)$
- Teorema Binomial: coeficientes da expansão de potências de expressões binomiais
- Antes um exemplo...

O Teorema Binomial

- **Exemplo:** expansão de $(x+y)^3$

$$(x+y)^3 = (x+y)(x+y)(x+y) = (xx+xy+yx+yy)(x+y) =$$
$$= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$$
$$= x^3 + 3x^2y + 3xy^2 + y^3$$

  - esta expansão também pode ser obtida por raciocínio combinatório:
    - quando $(x+y)^3$ é expandida, são adicionados todos os produtos do tipo: "um termo na 1ra soma" × "um termo na 2a soma" × "um termo na 3a soma"
    - para obter x^3, o x deve ser escolhido em cada uma das somas
      - e isto só pode ser feito de uma forma
      - de modo que o termo x^3 terá coeficiente $1 = \binom{3}{3}$
    - para obter x^2y:
      - um x deve ser escolhido em 2 das 3 somas (y na outra)
      - quantidade destes termos = nro de combinações **2** a **2** de 3 objetos = $\binom{3}{2}$
    - nro de termos da forma xy^2:
      - formas de pegar uma das 3 somas para obter um x (e y das outras 2)

· o que pode ser feito de $\binom{3}{1}$ modos

∗ finalmente, o único modo de obter um termo y^3 é:

· escolher o y em cada uma das 3 somas (ou nenhum x)

· o que pode ser feito de $1 = \binom{3}{0}$ modo

- **Teorema:** Sejam x e y variáveis e n um inteiro não-negativo. Então:

$$
\begin{aligned}
(x+y)^n &= \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j \\
&= \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n
\end{aligned}
$$

Prova:

– os termos no produto expandido são da forma $x^{n-j}y^j$, $(j = 0, 1, \ldots, n)$

– para obter um termo assim, é necessário escolher $n - j$ xs das n somas

∗ (outros j termos no produto são ys)

– portanto, o coeficiente de $x^{n-j}y^j$ é $\binom{n}{n-j} = \binom{n}{j}$ □

- **Exemplo:** A expansão de $(x+y)^4$ é:

$$
\begin{aligned}
(x+y)^4 &= \sum_{j=0}^{4} \binom{4}{j} x^{4-j} y^j \\
&= \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} x y^3 + \binom{4}{4} y^4 \\
&= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4
\end{aligned}
$$

- **Exemplo:** Qual é o coeficiente de $x^{12}y^{13}$ na expansão de $(2x - 3y)^{25}$?

– 1ro, note que: $(2x - 3y)^{25} = ((2x) + (-3y))^{25}$

– então, pelo teorema, temos:

$$((2x) + (-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j$$

– o coeficiente de $x^{12}y^{13}$ na expansão é obtido quando $j = 13$, ou seja:

$$\binom{25}{13} 2^{12} (-3)^{13} = -\frac{25!}{13!12!} 2^{12} 3^{13} = 33959763545702400$$

- O Teorema Binomial permite provar muitas identidades úteis...

- **Corolário 1/3:** Seja n um inteiro não-negativo. Então:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Prova: usando o Teorema Binomial com $\boldsymbol{x = y = 1}$, obtemos:

$$\boldsymbol{2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k}} \qquad \square$$

Prova combinatorial:

- um conjunto com $\boldsymbol{n}$ elementos tem um total de $\boldsymbol{2^n}$ subconjuntos diferentes
- cada subconjunto contém $\boldsymbol{0, 1, 2, \ldots}$ ou $\boldsymbol{n}$ elementos
- existem $\binom{n}{0}$ subconjuntos com **0** elementos, $\binom{n}{1}$ subconjuntos com **1** elemento, $\binom{n}{2}$ subconjuntos com **2** elementos, $\boldsymbol{\ldots}$ e $\binom{n}{n}$ subconjuntos com $\boldsymbol{n}$ elementos
- logo, $\sum_{k=0}^{n} \binom{n}{k}$ conta total de subconjuntos de um conjunto com $\boldsymbol{n}$ elementos
- o que mostra que:

$$\boldsymbol{\sum_{k=0}^{n} \binom{n}{k} = 2^n} \qquad \square$$

- **Corolário 2/3:** Seja $\boldsymbol{n}$ um inteiro positivo. Então:

$$\boldsymbol{\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0}$$

Prova: usando o Teorema Binomial com $\boldsymbol{x = 1}$ e $\boldsymbol{y = -1}$, obtemos:

$$\boldsymbol{0 = (1 + (-1))^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^{n} \binom{n}{k} (-1)^k} \qquad \square$$

- **Nota:** este Corolário implica em:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$$

- **Corolário 3/3:** Seja $\boldsymbol{n}$ um inteiro não-negativo. Então:

$$\boldsymbol{\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n}$$

Prova: observe que $\sum_{k=0}^{n} 2^k \binom{n}{k}$ é a expansão de $\boldsymbol{(1+2)^n}$ pelo T.B.

- logo:

$$\boldsymbol{3^n = (1+2)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 2^k = \sum_{k=0}^{n} \binom{n}{k} 2^k} \qquad \square$$

- **Teorema (Identidade de Pascal):**

  Sejam $\boldsymbol{n}$ e $\boldsymbol{k}$ inteiros positivos com $\boldsymbol{n \geq k}$. Então:

$$\binom{\boldsymbol{n+1}}{\boldsymbol{k}} = \binom{\boldsymbol{n}}{\boldsymbol{k-1}} + \binom{\boldsymbol{n}}{\boldsymbol{k}}$$

Prova:

- Suponha que $\boldsymbol{T}$ é um conjunto com $\boldsymbol{n+1}$ elementos
- Seja $\boldsymbol{a}$ um elemento em $\boldsymbol{T}$ e seja $\boldsymbol{S = T - \{a\}}$
- Seja $\boldsymbol{a}$ um elemento em $\boldsymbol{T}$ e seja $\boldsymbol{S = T - \{a\}}$
- Note que há $\binom{\boldsymbol{n+1}}{\boldsymbol{k}}$ subconjuntos de $\boldsymbol{T}$ com $\boldsymbol{k}$ elementos
- Mas um subconjunto de $\boldsymbol{T}$ com $\boldsymbol{k}$ elementos:
  * ou: contém $\boldsymbol{a}$ junto com $\boldsymbol{k-1}$ elementos de $\boldsymbol{S}$
  * ou: contém $\boldsymbol{k}$ elementos de $\boldsymbol{S}$ e não contém $\boldsymbol{a}$
- Há $\binom{\boldsymbol{n}}{\boldsymbol{k-1}}$ subconjuntos de $\boldsymbol{k}$ elementos de $\boldsymbol{T}$ que contêm $\boldsymbol{a}$
  * pois: existem $\binom{\boldsymbol{n}}{\boldsymbol{k-1}}$ subconjuntos de $\boldsymbol{k-1}$ elementos de $\boldsymbol{S}$
- E há $\binom{\boldsymbol{n}}{\boldsymbol{k}}$ subconjuntos de $\boldsymbol{k}$ elementos de $\boldsymbol{T}$ que não contêm $\boldsymbol{a}$
  * pois: existem $\binom{\boldsymbol{n}}{\boldsymbol{k}}$ subconjuntos de $\boldsymbol{k}$ elementos de $\boldsymbol{S}$
- Logo: $\binom{\boldsymbol{n+1}}{\boldsymbol{k}} = \binom{\boldsymbol{n}}{\boldsymbol{k-1}} + \binom{\boldsymbol{n}}{\boldsymbol{k}}$ □
- *Também é possível provar por manipulações algébricas* (ver exercícios).

- A Identidade de Pascal: $\binom{\boldsymbol{n+1}}{\boldsymbol{k}} = \binom{\boldsymbol{n}}{\boldsymbol{k-1}} + \binom{\boldsymbol{n}}{\boldsymbol{k}}$

  junto com as condições iniciais: $\forall \boldsymbol{n},\ \binom{\boldsymbol{n}}{\boldsymbol{0}} = \binom{\boldsymbol{n}}{\boldsymbol{n}} = \boldsymbol{1}$,

  pode ser usada para definir os coeficientes binomiais recursivamente

- Esta definição é útil na computação dos coeficientes pois só requer adição

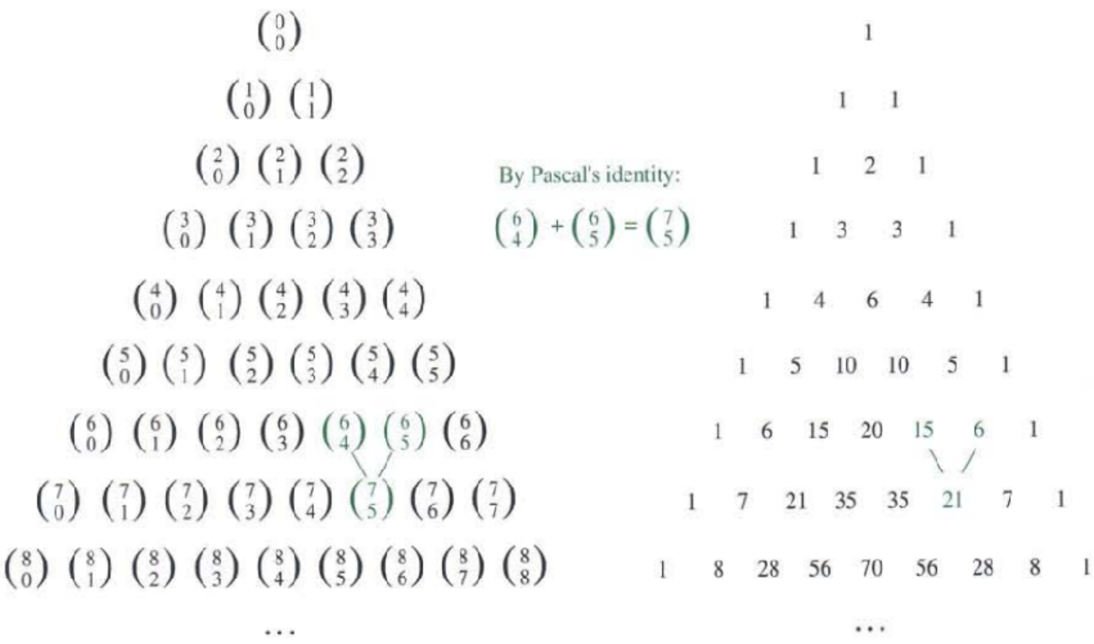
- **Exemplo:** computar $\binom{\boldsymbol{4}}{\boldsymbol{3}}$

$$\binom{3}{2} \qquad \binom{3}{3}$$

$$\binom{2}{1} \qquad \binom{2}{2}$$

$$\binom{1}{0} \qquad \binom{1}{1}$$

- A Identidade de Pascal $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$, é base para um arranjo geométrico dos coeficientes binomiais como um triângulo:



- A seguir: prova combinatorial de mais uma identidade importante...

- **Teorema (Identidade de Vandermonde):**

  Sejam $\boldsymbol{m, n}$ e $\boldsymbol{r}$ inteiros não-negativos, $\boldsymbol{r \le m}$ e $\boldsymbol{r \le n}$. Então: $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \cdot \binom{n}{k}$

  Prova:

  - suponha que há $\boldsymbol{m}$ ítens em um conjunto e $\boldsymbol{n}$ ítens em um 2o conjunto
  - então o nro de modos de pegar $\boldsymbol{r}$ elementos da união destes conjuntos é $\binom{m+n}{r}$
  - um outro modo de pegar $\boldsymbol{r}$ elementos desta união é:
    * pegar $\boldsymbol{k}$ elementos do 1ro conjunto e então
    * pegar $\boldsymbol{r-k}$ elementos do 2do conjunto
    * aonde $\boldsymbol{k}$ é um inteiro com $\boldsymbol{0 \le k \le r}$
    * pela regra do produto, isto pode ser feito de $\binom{m}{k}\binom{n}{r-k}$ modos
  - logo, o nro total de modos de pegar $\boldsymbol{r}$ elementos da união também vale:

    $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \cdot \binom{n}{k}$ □

- **Corolário:** Seja $\boldsymbol{n}$ um inteiro não-negativo. Então: $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

  Prova: usando a identidade de Vandermonde com $\boldsymbol{m = r = n}$, obtemos:

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{n-k}\binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}^2 \qquad \square$$

Leitura sobre Coeficientes Binomiais

- Rosen6: item 5.4

8) Contagem I

8.5) Arranjos e Combinações Generalizados (Contagem de multiconjuntos)

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.*

Arranjos e Combinações Generalizados

- Há problemas de contagem em que elementos distinguíveis podem ser usados repetidamente:
  - um número pode aparecer mais de uma vez em uma placa de carro
  - quando uma dúzia de bolos são selecionados entre 4 opções, cada tipo pode ser escolhido várias vezes
- Além disto, alguns problemas de contagem envolvem elementos usados uma vez só, mas indistinguíveis:
  - ex.: para contar o nro de modos em que as letras da palavra SUCESSO podem ser rearranjadas, o uso de letras idênticas deve ser considerado

Arranjos com repetição

- Seja $\boldsymbol{A}$ qualquer conjunto com $\boldsymbol{n}$ elementos e $\boldsymbol{1 \leq r \leq n}$.
- Quantas sequências diferentes de comprimento $\boldsymbol{r}$ podem ser formadas usando elementos de $\boldsymbol{A}$ se os elementos na sequência podem ser repetidos?
  - para cada posição "$\boldsymbol{i}$", podemos copiar qualquer elemento de $\boldsymbol{A}$
  - ou seja, há sempre $\boldsymbol{n}$ modos de realizar cada tarefa
  - então, pelo princípio da multiplicação estendido, o número de sequências que podem ser formadas é:

$$\underbrace{\boldsymbol{n \cdot n \cdot \cdots \cdot n}}_{\boldsymbol{r\ fatores}} = \boldsymbol{n^r}$$

- **Teorema:** Seja $\boldsymbol{A}$ um conjunto com $\boldsymbol{n}$ elementos e seja $\boldsymbol{1 \leq r \leq n}$:
  - Então o número de sequências de comprimento $\boldsymbol{r}$ que podem ser formadas com elementos de $\boldsymbol{A}$, permitindo repetições, é $\boldsymbol{n^r}$.
- **Exemplo:** Quantas "palavras" de 3 letras podem ser formadas com letras do conjunto $\boldsymbol{\{a, b, y, z\}}$, se for permitido repetição?

- A seguir: combinações de objetos distinguíveis em que a repetição é permitida...

- **Exemplo:** De quantos modos se pode selecionar 4 frutas de um cesto contendo maçãs, laranjas e peras, se:
  - a ordem na qual os exemplares são selecionados não importa;
  - importa apenas o tipo de fruta e não cada exemplar individualmente;
  - existem pelo menos 4 exemplares de cada tipo de fruta no cesto?

  Solução: 15 modos possíveis de selecionar as frutas:

4 maçãs	4 laranjas	4 peras
3 maçãs, 1 laranja 3 laranjas, 1 pera	3 maçãs, 1 pera 3 peras, 1 maçã	3 laranjas, 1 maçã 3 peras, 1 laranja
2 maçãs, 2 laranjas	2 maçãs, 2 peras	2 laranjas, 2 peras
2 maçãs, 1 laranja, 1 pera	2 laranjas, 1 maçã, 1 pera	2 peras, 1 maçã, 1 laranja

  = "nro de combinações 4 a 4, com repetição permitida, de um conjunto de 3 elementos"

- Próximo exemplo ilustra método geral para contar combinações r a r de um conjunto com n elementos, com repetição permitida...

- **Exemplo:** De quantos modos se pode selecionar 5 notas de um caixa contendo notas de R$ 1, R$ 2, R$ 5, R$ 10, R$ 20, R$ 50 e R$ 100? Assuma que:
  - A ordem em que as notas são escolhidas não importa
  - As notas de cada denominação são indistinguíveis
  - Existem pelo menos 5 notas de cada tipo
  - Envolve contagem de combinações 5 a 5, com permissão de repetição, de um conjunto com 7 elementos

  Solução: Imagine uma caixa com 7 compartimentos (um para cada nota):

R$100	R$50	R$20	R$10	R$5	R$2	R$1

  - Estes compartimentos são separados por 6 divisores
  - Escolha das 5 notas $\Leftrightarrow$ posicionar 5 marcadores nos compartimentos
  - Ilustração:
    - 2 notas de R$ 10 e 3 de R$ 1: | | |∗∗| | |∗∗∗
    - 1 nota de R$ 100, 1 de R$ 50, 2 de R$ 20 e 1 de R$ 5: ∗|∗|∗∗| |∗| |
    - 1 nota de R$ 100, 2 de R$ 10, 1 de R$ 2 e 1 de R$ 1: ∗| | |∗∗| |∗|∗

- Nro de modos de selecionar 5 notas $=$ nro de modos de arranjar 6 barras e 5 asteriscos
  $=$ nro de modos de *selecionar posições* para os 5 asteriscos, a partir de 11 possibilidades
  $=$ nro de seleções não ordenadas de 5 objetos a partir de um conjunto de 11 objetos
- O que pode ser feito de: $\boldsymbol{{}_{11}C_5 = \frac{11!}{5!6!} = 462}$ modos $\square$

- O teorema a seguir generaliza esta discussão...

- **Teorema:** existem $\boxed{\boldsymbol{{}_{n+r-1}C_r = {}_{n+r-1}C_{n-1}}}$ combinações $\boldsymbol{r}$ a $\boldsymbol{r}$ de um conjunto com $\boldsymbol{n}$ elementos quando a repetição de elementos é permitida.

  Prova:

  - Representar cada combinação $\boldsymbol{r}$ a $\boldsymbol{r}$ por uma lista de $\boldsymbol{n-1}$ barras e $\boldsymbol{r}$ asteriscos:
    - $\boldsymbol{n-1}$ barras demarcam $\boldsymbol{n}$ diferentes células
    - $\boldsymbol{i}$-ésima célula contém um $*$ para cada vez que $\boldsymbol{i}$-ésimo elemento ocorre
  - Cada lista diferente de $\boldsymbol{n-1}$ barras e $\boldsymbol{r}$ $*$'s $\Leftrightarrow$ uma combinação $\boldsymbol{r}$ a $\boldsymbol{r}$ dos $\boldsymbol{n}$ elementos
  - Quantidade destas listas é $\boldsymbol{{}_{n-1+r}C_r}$, pois:
    - cada lista $\Leftrightarrow$ uma escolha de $\boldsymbol{r}$ posições para colocar os $\boldsymbol{r}$ $*$'s em $\boldsymbol{n-1+r}$ possibilidades (para $\boldsymbol{r}$ $*$'s e $\boldsymbol{n-1}$ barras)
    - (ou a uma escolha de $\boldsymbol{n-1}$ posições para colocar as $\boldsymbol{n-1}$ barras) $\square$

- **Exemplo:** Em uma certa confeitaria, são vendidos 4 tipos de bolos. De quantas formas diferentes pode-se escolher 6 bolos?

  - (Assuma que só interessa o tipo de bolo e não o bolo individual e nem a ordem em que eles são escolhidos)

  Solução: nro de modos de escolher os 6 bolos =

  = nro de combinações 6 a 6 de conjunto com 4 elementos

  $\boldsymbol{= {}_{4+6-1}C_6 = {}_9C_6 = {}_9C_3 = 84}$ $\square$

- **Exemplo:** Quantas soluções possui a equação: $\boldsymbol{x_1 + x_2 + x_3 = 11}$

  aonde $\boldsymbol{x_1,\ x_2}$ e $\boldsymbol{x_3}$ são inteiros não-negativos?

  Solução:

  - uma solução corresponde a um modo de selecionar 11 itens de um conjunto com 3 elementos, de modo que sejam escolhidos:
    - $\boldsymbol{x_1}$ itens do tipo 1, $\boldsymbol{x_2}$ itens do tipo 2 e $\boldsymbol{x_3}$ itens do tipo 3
  - portanto: nro de soluções = nro de combinações 11 a 11, com repetição, a partir de um conjunto com 3 elementos
  - então, pelo teorema, existem: $\boldsymbol{{}_{3+11-1}C_{11} = {}_{13}C_2 = 78}$ soluções $\square$

- **Exemplo:** Quantas soluções possui a equação: $\boldsymbol{x_1 + x_2 + x_3 = 11}$

  aonde $\boldsymbol{x_1,\ x_2}$ e $\boldsymbol{x_3}$ são inteiros tais que: $\boldsymbol{x_1 \geq 1}$, $\boldsymbol{x_2 \geq 2}$ e $\boldsymbol{x_3 \geq 3}$?

  - agora uma solução corresponde a uma seleção de 11 itens com:
    * $\boldsymbol{x_1}$ itens do tipo 1, $\boldsymbol{x_2}$ itens do tipo 2 e $\boldsymbol{x_3}$ itens do tipo 3
    * (+) existem pelo menos 1 item do tipo 1, 2 itens do tipo 2 e 3 itens do tipo 3

  - então escolha 1 item do tipo 1, 2 do tipo 2 e 3 do tipo 3 e daí:
    * selecione 5 itens adicionais
    * pelo teorema, isto pode ser feito de: $\boldsymbol{{}_{3+5-1}C_5 = 21}$ modos $\square$

- **Exemplo:** Qual é o valor de $\boldsymbol{k}$ depois da execução de:

```
k = 0
for i_1 = 1 to n
    for i_2 = 1 to i_1
        ⋮
        for i_m = 1 to i_{m-1}
            k = k + 1
```

  Solução:

  - O contador $\boldsymbol{k}$ começa em $\boldsymbol{0}$ e é incrementado cada vez que o loop aninhado é percorrido com uma sequência $\boldsymbol{i_1, i_2, \ldots, i_m}$ tal que: $\boldsymbol{1 \leq i_m \leq i_{m-1} \leq \cdots \leq i_1 \leq n}$
  - nro de seqs = nro de modos de escolher $\boldsymbol{m}$ ints de $\boldsymbol{\{1, 2, \ldots, n\}}$, com repetição

    ($\Rightarrow$) se ordenarmos os ints de uma destas seleções em ordem não decrescente, teremos uma atribuição única a $\boldsymbol{i_m, i_{m-1}, \ldots, i_1}$

    ($\Leftarrow$) cada atribuição destas corresponde a um conjunto não ordenado único
  - segue que $\boxed{\boldsymbol{k \ = \ {}_{n+m-1}C_m}}$ após a execução deste código $\square$

Resumo - Objetos Distinguíveis

tipo	repetição permitida?	fórmula
arranjo $\boldsymbol{r}$ a $\boldsymbol{r}$	não	$\frac{n!}{(n-r)!}$
combinação $\boldsymbol{r}$ a $\boldsymbol{r}$	não	$\frac{n!}{r!(n-r)!}$
arranjo $\boldsymbol{r}$ a $\boldsymbol{r}$	sim	n^r
combinação $\boldsymbol{r}$ a $\boldsymbol{r}$	sim	$\frac{(n+r-1)!}{r!(n-1)!}$

- Alguns elementos podem ser indistinguíveis em problemas de contagem
- Neste caso, deve-se tomar cuidado para não contar as coisas mais do que uma vez...

Permutações com objetos indistinguíveis

- **Exemplo (1/2):** Quantos permutações distinguíveis existem com as letras da palavra $\boldsymbol{BANANA}$?

  Solução:

  - Começar rotulando os $\boldsymbol{A}$'s e os $\boldsymbol{N}$'s.
  - Para $\boldsymbol{B, A_1, N_1, A_2, N_2, A_3}$ existem $\mathbf{6! = 720}$ permutações.
  - Só que algumas destas permutações são idênticas, exceto pela ordem em que os $\boldsymbol{N}$'s aparecem:
    * exemplo: $\boldsymbol{A_1A_2A_3BN_1N_2}$ e $\boldsymbol{A_1A_2A_3BN_2N_1}$
    * de fato, as **720** podem ser listadas em pares que diferem apenas na ordem dos dois $\boldsymbol{N}$'s
    * isto significa que, tirando os rótulos dos $\boldsymbol{N}$'s, restam apenas $\frac{\mathbf{720}}{\mathbf{2}} = \mathbf{360}$ permutações distinguíveis
  - De modo similar, notamos que estas **360** podem ser agrupadas em grupos de $\mathbf{3! = 6}$ que diferem apenas na ordem dos 3 $\boldsymbol{A}$'s
    * um destes grupos de 6 seria:
      $\boldsymbol{BNNA_1A_2A_3}$, $\boldsymbol{BNNA_1A_3A_2}$, $\boldsymbol{BNNA_2A_1A_3}$,
      $\boldsymbol{BNNA_2A_3A_1}$, $\boldsymbol{BNNA_3A_1A_2}$, $\boldsymbol{BNNA_3A_2A_1}$
  - Portanto, existem $\frac{\mathbf{360}}{\mathbf{6}} = \mathbf{60}$ permutações distinguíveis das letras de $\boldsymbol{BANANA}$. □

- **Exemplo (versão 2):** Quantas permutações distinguíveis existem com as letras da palavra $\boldsymbol{BANANA}$?

  Solução: esta palavra contém 1 B, 3 As e 2 Ns

  - 1ro note que os 3 As podem ser colocados entre as 6 posições de $\boldsymbol{{}_6C_3}$ modos
    * deixando 3 posições livres
  - Então os 2 Ns podem ser colocados em $\boldsymbol{{}_3C_2}$ modos, deixando 1 posição livre
  - E o B pode ser colocado de $\boldsymbol{{}_1C_1}$ modo
  - Então, da regra do produto, o nro de strings diferentes que podem ser feitas é:

$$\boldsymbol{{}_6C_3 \times_3 C_2 \times_1 C_1 = \frac{6!}{3!3!} \cdot \frac{3!}{2!1!} \cdot \frac{1!}{1!0!} = \frac{6!}{3!2!1!}} \qquad \square$$

- Esta "versão 2" mostra a ideia da prova do teorema a seguir...

- **Teorema:** O número de permutações distintas que pode ser formado com uma coleção de $\boldsymbol{n}$ objetos, aonde o $\mathbf{1^o}$ objeto aparece $\boldsymbol{k_1}$ vezes, o $\mathbf{2^o}$ objeto aparece $\boldsymbol{k_2}$ vezes, etc...

  é dado por: $\boxed{\boldsymbol{\frac{n!}{k_1!k_2!\cdots k_t!}}}$ aonde: $\boldsymbol{k_1 + k_2 + \cdots + k_t = n}$

  Prova: generalização direta do exemplo anterior.

- **Exemplo:** O número de "palavras" distintas que podem ser formadas a partir das letras de $\boldsymbol{MISSISSIPPI}$ é:

$$\mathbf{\frac{11!}{1!.4!.4!.2!} = 34650}$$

Arranjos e Combinações Generalizados

- Ler: Rosen6, item 5.5

8) Contagem I

8.6) Princípio da Inclusão-Exclusão generalizado

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.*

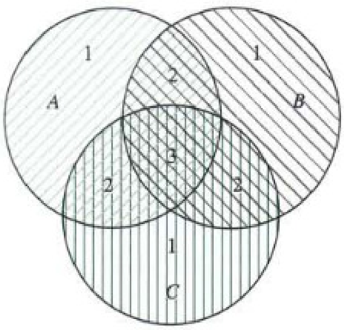
Princípio da inclusão-exclusão

- Vamos agora deduzir uma fórmula para o nro de elementos na união de um nro finito ($\boldsymbol{n}$) de conjuntos
  - esta fórmula é chamada de Princípio da inclusão e exclusão
- Vamos iniciar pelo caso em que temos 3 conjuntos A, B e C...

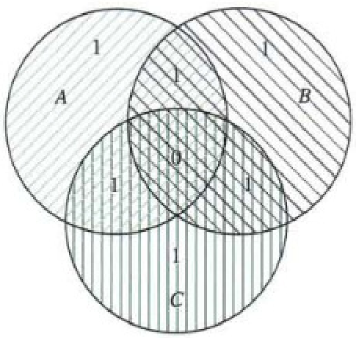
Nro de elementos na união de 3 conjuntos

- Primeiro, note que $|\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}|$ conta:

  1$\times$ cada elemento que está em exatamente um dos 3 conjuntos
  2$\times$ os elementos que estão em exatamente dois dos 3 conjuntos
  3$\times$ os elementos que estão em todos os 3 conjuntos



- Para remover o excesso, subtraímos os elementos nas intersecções de todos os pares dos 3 conjuntos, obtendo: $|\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}| - |\boldsymbol{A} \cap \boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{C}| - |\boldsymbol{B} \cap \boldsymbol{C}|$

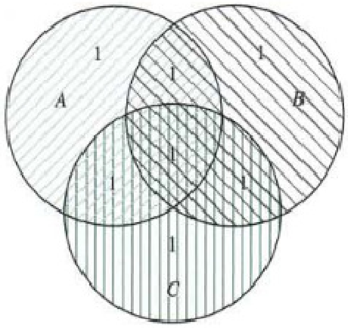


- Problema: a contagem dos elementos que ocorrem em todos os conjuntos foi zerada

– pois eles ocorrem em todas as 3 intersecções de conjuntos tomadas 2 a 2

- Para consertar esta "sub-avaliação", adicionamos os elementos que estão na intersecção dos 3 conjuntos:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$



- Esta expressão final conta cada elemento apenas uma vez
  – não importando se ele está em 1, 2 ou 3 dos conjuntos

- **Exemplo 1:** Sejam $A = \{a, b, c, d, e\}$, $B = \{a, b, e, g, h\}$, e $C = \{b, d, e, g, h, k, m, n\}$. Verifique o princípio da inclusão-exclusão neste caso.

  Solução:

  $A \cup B \cup C = \{a, b, c, d, e, g, h, k, m, n\}$
  $A \cap B = \{a, b, e\}$, $\quad A \cap C = \{b, d, e\}$, $\quad B \cap C = \{b, e, g\}$
  $A \cap B \cap C = \{b, e\}$

  – De modo que:

  $|A \cup B \cup C| = 10$
  $|A| = 5$, $\quad |B| = 5$, $\quad |C| = 8$
  $|A \cap B| = 3$, $\quad |A \cap C| = 3$, $\quad |B \cap C| = 4$
  $|A \cap B \cap C| = 2$

  – Portanto:

  $$|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C| = 5+5+8-3-3-4+2 = 10$$

  – O princípio é verificado $\square$

- **Exemplo 2:** Uma pesquisa de opinião foi feita sobre as formas de deslocamento para o trabalho dos cidadãos de Fpolis. Solicitou-se a cada entrevistado que marcasse ÔNIBUS, AMARELINHO ou CARRO como o seu modo preferencial de se deslocar. Era permitido marcar mais de uma resposta. Os resultados foram os seguintes: ÔNIBUS, 30 pessoas; AMARELINHO, 35; CARRO, 100; ÔNIBUS e AMARELINHO, 15; ÔNIBUS e CARRO, 15; AMARELINHO e CARRO, 20; todos os 3 modos, 5. Pergunta: quantas pessoas responderam à pesquisa?

  Solução:

  – Sejam O, A e C os conjuntos das pessoas que marcaram ÔNIBUS, AMARELINHO E CARRO

  – Então, sabemos que:

  $|O| = 30$, $\quad |A| = 35$, $\quad |C| = 100$

$$|O \cap A| = 15, \qquad |O \cap C| = 15, \qquad |A \cap C| = 20$$
$$|O \cap A \cap C| = 5$$

– Portanto: $|O| + |A| + |C| - |O \cap A| - |O \cap C| - |A \cap C| + |O \cap A \cap C| = 30 + 35 + 100 - 15 - 15 - 20 + 5$

– Ou seja: qtde de pessoas que responderam $= 120 \; = \; |O \cup A \cup C|$ □

- A seguir, provaremos o Princípio da Inclusão e Exclusão Geral
  – o qual determina quantos elementos estão na união de um nro finito de conjuntos finitos

Princípio da inclusão-exclusão generalizado

- **Teorema:** Sejam $A_1, A_2, \ldots, A_n$ conjuntos finitos. Então:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \;=\; \sum_{1 \le i \le n} |A_i| \;-\; \sum_{1 \le i < j \le n} |A_i \cap A_j| \;+$$
$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \;\cdots\; +$$
$$+ \;\; (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

Prova: (mostrar que cada elemento da união é contado exatamente uma vez pelo lado direito da equação)

– Suponha que a é membro de exatamente r dos conjuntos $A_1, A_2, \ldots, A_n$:
  * então a é contado é contado $\binom{r}{1}$ vezes por $\sum |A_i|$
  * e a é contado $\binom{r}{2}$ vezes por $\sum |A_i \cap A_j|$
  * em geral: ele é contado $\binom{r}{m}$ vezes pela soma que envolve m dos A_i
  * ou seja, este elemento é contado exatamente:
    $\binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \cdots + (-1)^{r+1}\binom{r}{r}$ vezes
    pelo lado direito desta equação

– Mas (propriedade dos coefs binomiais): $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

$\Rightarrow \;\; \binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \cdots + (-1)^{r+1}\binom{r}{r} = \binom{r}{0} = 1$

– Logo, cada elemento na união é contado exatamente uma vez pelo lado direito da equação □

- O princípio da inclusão-exclusão fornece uma fórmula para o nro de elementos na união de n conjuntos, para todo inteiro positivo n

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \;=\; \sum_{1 \le i \le n} |A_i| \;-\; \sum_{1 \le i < j \le n} |A_i \cap A_j| \;+$$
$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \;\cdots\; +$$

$$+ \;\; (-1)^{n+1}|A_1 \cap A_2 \cap \cdots \cap A_n|$$

- Há termos nesta fórmula para o nro de elementos na intersecção de todo subconjunto não vazio da coleção de n conjuntos
- Logo, existem $2^n - 1$ termos nesta fórmula

- **Exemplo:** Forneça uma fórmula para o nro de elementos na união de 4 conjuntos

  Solução: o princípio da inclusão-exclusão mostra que:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4| = {} & |A_1| + |A_2| + |A_3| + |A_4| \\ & -|A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| \\ & -|A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| \\ & +|A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_4|\end{aligned}$$

  - Note que esta fórmula contém 15 termos diferentes
  - Um para cada subconjunto não vazio de $\{A_1, A_2, A_3, A_4\}$

Forma alternativa

- Há uma forma alternativa do princípio da inclusão-exclusão
  - útil, por exemplo, em problemas que pedem o nro de elementos, em um dado conjunto, que não possuem nenhuma das n propriedades $P_1, P_2, \ldots, P_n$
- Seja A_i o subconjunto contendo os elementos que possuem a propriedade P_i
- Nro de elementos com todas as propriedades $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$:

$$N(P_{i_1}, P_{i_2}, \ldots, P_{i_k})$$

- Em termos de conjuntos, temos:

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = N(P_{i_1}, P_{i_2}, \ldots, P_{i_k})$$

- Daí, o nro de elementos sem nenhuma das propriedades $P_1, P_2, \ldots, P_n$ fica:

$$N(P_1'P_2'\cdots P_n') = N - |A_1 \cup A_2 \cup \cdots \cup A_n|$$

  onde: $N =$ nro de elementos no conjunto

- Então, do Princípio da Inclusão-Exclusão, vemos que:

$$N(P_1'P_2'\cdots P_n') = N - |A_1 \cup A_2 \cup \cdots \cup A_n| =$$

$$= N - \sum_{1\le i\le n} N(P_i) + \sum_{1\le i<j\le n} N(P_iP_j) +$$

$$- \sum_{1\le i<j\le n} N(P_iP_jP_k) + \cdots + (-1)^n N(P_1P_2\cdots P_n)$$

- **Exemplo:** Quantas soluções existem para: $\boldsymbol{x_1 + x_2 + x_3 = 11}$ tais que:

  $\boldsymbol{x_1 \leq 3}$, $\boldsymbol{x_2 \leq 4}$ e $\boldsymbol{x_3 \leq 6}$?

  Solução:

  $\boldsymbol{N}$ = nro total de soluções = $\boldsymbol{C(3+11-1, 11) = 78}$

  $\boldsymbol{N(P_1)}$ = nro de soluções com $\boldsymbol{x_1 > 3 = C(3+7-1, 7) = C(9,7) = 36}$
  $\boldsymbol{N(P_2)}$ = nro de soluções com $\boldsymbol{x_2 > 4 = C(3+6-1, 6) = C(8,6) = 28}$
  $\boldsymbol{N(P_3)}$ = nro de soluções com $\boldsymbol{x_3 > 6 = C(3+4-1, 4) = C(6,4) = 15}$

  $\boldsymbol{N(P_1P_2)}$ = sols com $\boldsymbol{x_1 > 3}$ e $\boldsymbol{x_2 > 4 = C(3+2-1, 2) = C(4,2) = 6}$
  $\boldsymbol{N(P_1P_3)}$ = sols com $\boldsymbol{x_1 > 3}$ e $\boldsymbol{x_3 > 6 = C(3+0-1, 0) = 1}$
  $\boldsymbol{N(P_2P_3)}$ = sols com $\boldsymbol{x_2 > 4}$ e $\boldsymbol{x_3 > 6 = 0}$

  $\boldsymbol{N(P_1P_2P_3)}$ = sols com $\boldsymbol{x_1 > 3}$, $\boldsymbol{x_2 > 4}$ e $\boldsymbol{x_3 > 6 = 0}$

  $\boldsymbol{N(P_1'P_2'P_3') = 78 - 36 - 28 - 15 + 6 + 1 + 0 - 0 = 6}$ □

O Crivo de Eratóstenes

- O Princípio pode ser usado para achar: nro de primos $\leq$ inteiro positivo dado

- **Exemplo:** encontrar o nro de primos ≤ 100:
  - Lembre que um inteiro composto $\boldsymbol{n}$ é divisível por um primo $\leq \sqrt{\boldsymbol{n}}$
  - Compostos $\leq$ **100** devem possuir um fator primo $\leq$ **10**
  - Logo, os primos $\leq$ **100** são **2, 3, 5, 7** e :

    todos os inteiros $\leq$ **100** que não são divisíveis por nenhum deles
  - Aplicando o Princípio da Inclusão-Exclusão:

    propriedade $\boldsymbol{P_1}$ = "um inteiro é divisível por 2"
    propriedade $\boldsymbol{P_2}$ = "um inteiro é divisível por 3"
    propriedade $\boldsymbol{P_3}$ = "um inteiro é divisível por 5"
    propriedade $\boldsymbol{P_4}$ = "um inteiro é divisível por 7"

  - De modo que: "nro de primos $\leq$ **100**" $\boldsymbol{= 4 + N(P_1'P_2'P_3'P_4')}$

  - Como há **99** nros $\leq$ **100** e $\geq$ **2**, o Princípio estabelece que:

$$\begin{aligned}\boldsymbol{N(P_1'P_2'P_3'P_4')} &\boldsymbol{= 99 - N(P_1) - N(P_2) - N(P_3) - N(P_4)} \\ &\boldsymbol{+N(P_1P_2) + N(P_1P_3) + N(P_1P_4) + N(P_2P_3) + N(P_2P_4) + N(P_3P_4) +} \\ &\boldsymbol{-N(P_1P_2P_3) - N(P_1P_2P_4) - N(P_1P_3P_4) - N(P_2P_3P_4)} \\ &\boldsymbol{+N(P_1P_2P_3P_4)}\end{aligned}$$

  - Consequentemente:

$$
\begin{aligned}
N(P_1'P_2'P_3'P_4') = 99 &- \lfloor \tfrac{100}{2} \rfloor - \lfloor \tfrac{100}{3} \rfloor - \lfloor \tfrac{100}{5} \rfloor - \lfloor \tfrac{100}{7} \rfloor \\
&+ \lfloor \tfrac{100}{2\cdot 3} \rfloor + \lfloor \tfrac{100}{2\cdot 5} \rfloor + \lfloor \tfrac{100}{2\cdot 7} \rfloor + \lfloor \tfrac{100}{3\cdot 5} \rfloor + \lfloor \tfrac{100}{3\cdot 7} \rfloor + \lfloor \tfrac{100}{5\cdot 7} \rfloor \\
&- \lfloor \tfrac{100}{2\cdot 3\cdot 5} \rfloor - \lfloor \tfrac{100}{2\cdot 3\cdot 7} \rfloor - \lfloor \tfrac{100}{2\cdot 5\cdot 7} \rfloor - \lfloor \tfrac{100}{3\cdot 5\cdot 7} \rfloor \\
&+ \lfloor \tfrac{100}{2\cdot 3\cdot 5\cdot 7} \rfloor
\end{aligned}
$$

$$
\begin{aligned}
&= 99 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 + 0 \\
&= 21
\end{aligned}
$$

  - Logo, existem $4 + 21 = 25$ primos ≤ 100 □

- O Crivo de Eratóstenes serve para encontrar todos os primos $\leq$ um inteiro dado

- **Exemplo:** O procedimento para encontrar todos os primos ≤ 100 é:

  - Marcar os inteiros $\neq 2$ que são divisíveis por 2:

1	2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	9	$\underline{10}$
11	$\underline{12}$	13	$\underline{14}$	15	$\underline{16}$	17	$\underline{18}$	19	$\underline{20}$
21	$\underline{22}$	23	$\underline{24}$	25	$\underline{26}$	27	$\underline{28}$	29	$\underline{30}$
31	$\underline{32}$	33	$\underline{34}$	35	$\underline{36}$	37	$\underline{38}$	39	$\underline{40}$
41	$\underline{42}$	43	$\underline{44}$	45	$\underline{46}$	47	$\underline{48}$	49	$\underline{50}$
51	$\underline{52}$	53	$\underline{54}$	55	$\underline{56}$	57	$\underline{58}$	59	$\underline{60}$
61	$\underline{62}$	63	$\underline{64}$	65	$\underline{66}$	67	$\underline{68}$	69	$\underline{70}$
71	$\underline{72}$	73	$\underline{74}$	75	$\underline{76}$	77	$\underline{78}$	79	$\underline{80}$
81	$\underline{82}$	83	$\underline{84}$	85	$\underline{86}$	87	$\underline{88}$	89	$\underline{90}$
91	$\underline{92}$	93	$\underline{94}$	95	$\underline{96}$	97	$\underline{98}$	99	$\underline{100}$

  - 1ro inteiro > 2 que sobra é o 3

  - Marcar os inteiros $\neq 3$ que são divisíveis por 3:

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{10}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{20}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	25	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{30}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	35	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{40}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{45}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{50}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	55	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{60}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	65	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{70}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{75}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{80}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	85	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{90}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	95	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{100}$

  - 5 é o próximo inteiro que sobra depois do 3

  - Marcar os inteiros $\neq 5$ que são divisíveis por 5:

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{\underline{10}}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{\underline{15}}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{\underline{20}}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{\underline{30}}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{35}$	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{\underline{40}}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{\underline{45}}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{\underline{50}}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	$\underline{55}$	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{\underline{60}}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	$\underline{65}$	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{\underline{70}}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{\underline{75}}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{\underline{80}}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{\underline{90}}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{\underline{100}}$

  - o próximo inteiro que sobra é o 7

– Marcar os inteiros $\neq \mathbf{7}$ que são divisíveis por $\mathbf{7}$:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

O Crivo de Eratóstenes

Algoritmo:

1. Crie uma lista de inteiros consecutivos de $\mathbf{2}$ a $\boldsymbol{n}$
2. Faça $\boldsymbol{p} = \mathbf{2}$ (o primeiro primo)
3. Marque todos os múltiplos de $\boldsymbol{p}$
   - pode começar em $\boldsymbol{p^2}$
4. Encontre o primeiro nro que resta na lista depois de $\boldsymbol{p}$ (é o próximo primo)
   - faça $\boldsymbol{p} =$ este nro
5. Repita $\mathbf{3}$ e $\mathbf{4}$ até chegar a $\boldsymbol{p^2 > n}$
6. Todos os nros restantes são primos

- Complexidade: o tempo para calcular todos os primos abaixo de n é $\boldsymbol{O(n \times log\, log\, n)}$ operações
- Ou: $\boldsymbol{O(n \times log\, n \times log\, log\, n)}$ operações em bits
- (Ver Wikipedia)

Nro de funções sobrejetoras

- O Princípio da I-E também serve para determinar o nro de funções sobrejetoras de um conjunto com $\boldsymbol{m}$ para um com $\boldsymbol{n}$ elementos

- **Exemplo:** Quantas funções sobrejetoras existem de um conjunto com 6 elementos para um com 3?
  - suponha que os elementos no codomínio sejam $\boldsymbol{b_1, b_2, b_3}$
  - seja $\boldsymbol{P_i}$ a propriedade: "$\boldsymbol{b_i}$ não está na imagem da função"
  - uma função é sobrejetora sse não tiver nenhuma das propriedades $\boldsymbol{P_1, P_2, P_3}$
  - pelo Princípio da I-E:

$$\begin{aligned} \boldsymbol{N(P_1'P_2'P_3')} &= \boldsymbol{N - [N(P_1) + N(P_2) + N(P_3)] +} \\ &\quad \boldsymbol{+ [N(P_1P_2) + N(P_1P_3) + N(P_2P_3)] - N(P_1P_2P_3)} \end{aligned}$$

onde $\boldsymbol{N}$ = total de funções de um conjunto com 6 elementos para outro com 3

– temos que avaliar cada um dos termos do lado direito desta equação...

- **Exemplo:** Funções sobrejetoras de um conjunto com 6 elementos para um com 3:
  – Cálculo de $\boldsymbol{N}$:
    * uma função corresponde à escolha de um dos 3 elementos no codomínio para cada um dos 6 no domínio
    * pela regra do produto: $\boldsymbol{N = 3^6}$
  – Cálculo de $\boldsymbol{N(P_i)}$ (="nro de funções que não possuem $\boldsymbol{b_i}$ em sua imagem"):
    * há duas escolhas para o valor da função em cada elemento do domínio
    * de modo que: $\boldsymbol{N(P_i) = 2^6}$
    * e note que há $\boldsymbol{C(3,1)}$ termos deste tipo
  – Cálculo de $\boldsymbol{N(P_iP_j)}$ (="nro de funções sem $\boldsymbol{b_i}$ nem $\boldsymbol{b_j}$ em sua imagem"):
    * apenas uma escolha para o valor da função em cada elemento do domínio
    * portanto: $\boldsymbol{N(P_iP_j) = 1^6}$
    * e note que há $\boldsymbol{C(3,2)}$ termos deste tipo

$$\boldsymbol{N(P_1'P_2'P_3') = N - [N(P_1) + N(P_2) + N(P_3)] +}$$
$$\boldsymbol{+[N(P_1P_2) + N(P_1P_3) + N(P_2P_3)] - N(P_1P_2P_3)}$$

  – Temos que:
    * $\boldsymbol{N = 3^6}$
    * $\boldsymbol{N(P_i) = 2^6}$, com $\boldsymbol{C(3,1)}$ termos deste tipo
    * $\boldsymbol{N(P_iP_j) = 1^6}$, com $\boldsymbol{C(3,2)}$ termos deste tipo
  – Ainda: $\boldsymbol{N(P_1P_2P_3) = 0}$
  – Resposta: $\boldsymbol{3^6 - C(3,1) \times 2^6 + C(3,2) \times 1^6 = 540}$ □

- A seguir: generalização deste resultado...

- **Teorema:** Sejam $\boldsymbol{m}$ e $\boldsymbol{n}$ inteiros positivos $\boldsymbol{(m \geq n)}$. Existem:

$$\boxed{\boldsymbol{n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - \cdots + (-1)^{n-1}C(n,n-1) \times 1^m}}$$

  funções sobrejetoras de um conjunto com $\boldsymbol{m}$ elementos para um conjunto com $\boldsymbol{n}$ elementos.

  Prova: generalização direta do exercício anterior.

- **Exemplo:** De quantos modos se pode atribuir **5** tarefas diferentes a **4** empregados diferentes se cada empregado deve receber pelo menos uma tarefa?
  – Atribuição de tarefas = função do conjunto de 5 tarefas para o conjunto de 4 empregados

- Uma atribuição em que cada empregado recebe pelo menos uma tarefa é o mesmo que:
    * uma função sobrejetora do conjunto de tarefas para o conjunto de empregados
- De modo que a resposta é:

  $\boldsymbol{4^5 - C(4,1).3^5 + C(4,2).2^5 - C(4,3).1^5 = 240}$ modos $\square$

- Uma função sobrejetora de um conjunto com $\boldsymbol{m}$ elementos para outro com $\boldsymbol{n}$ elementos corresponde:
  - a um modo de distribuir os $\boldsymbol{m}$ elementos do domínio em $\boldsymbol{n}$ caixas indistinguíveis
    * de maneira que *nenhuma caixa fique vazia*
  - e então associar cada elemento do codomínio a uma caixa

- Ou seja, é o nro de maneiras de distribuir $\boldsymbol{m}$ objetos distinguíveis em $\boldsymbol{n}$ caixas indistinguíveis de modo que nenhuma caixa fique vazia,
  - multiplicado pelo nro de permutações de um conjunto com $\boldsymbol{n}$ elementos

- Logo, o nro de funções sobrejetoras de $\boldsymbol{m}$ para $\boldsymbol{n}$ é $\boldsymbol{n!} \times \boldsymbol{S(m,n)}$
  - aonde $\boldsymbol{S(m,n)}$ é o "nro de Stirling do 2o tipo"
  - o que consiste em uma *outra forma* de deduzir a fórmula para $\boldsymbol{S(m,n)}$

Leituras sobre Contagem

- Rosen6: itens 7.5 e 7.6

9) Contagem II

9.1) Relações de Recorrência

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Relações de Recorrência

- Uma relação de recorrência para a sequência $\{a_n\}$ é uma equação que, $\forall n$ inteiro, $n \geq n_0$, expressa a_n em função de um ou mais termos anteriores $(a_0, a_1, \ldots, a_{n-1})$
  - n_0 é um inteiro não negativo
- Há uma importante conexão entre recursão e relações de recorrência:
  - Algoritmo recursivo: solução de um problema de tamanho n em termos de soluções de instâncias do mesmo problema com tamanho menor
  - Logo, a análise de complexidade de um algoritmo recursivo leva a uma relação de recorrência que expressa:

    "*nro de operações para resolver um problema de tamanho* n "

    em termos de:

    "*nro de operações para resolver instâncias de menor tamanho do mesmo problema*"

- **Exemplo:** Seja $\{a_n\}$ uma sequência que satisfaz a relação:

  $$a_0 = 3 \quad \text{e} \quad a_1 = 5$$
  $$a_n = a_{n-1} + a_{n-2}, \quad \text{para} \ \ n = 2, 3, 4, \ldots$$

  O que são a_2 e a_3?

  Solução:

  $$a_2 = a_1 - a_0 = 5 - 3 = 2$$
  $$a_3 = a_2 - a_1 = 2 - 5 = -3 \qquad \square$$

- Uma sequência é uma <u>solução</u> de uma relação de recorrência se os seus termos satisfazem esta relação de recorrência

- **Exemplo:** Determine se as sequências $\{a_n\}$, n inteiro e não negativo, dadas por:

  $a_n = 3n$, $\quad a_n = 2^n$ $\quad$ e $\quad a_n = 5$

  são soluções da relação de recorrência dada por: $\quad a_n = 2a_{n-1} - a_{n-2}$

  Solução:

  1. se $a_n = 3n$, então, para $n \geq 2$:
     - $2a_{n-1} - a_{n-2} = 2[3(n-1)] - 3(n-2) = 3n = a_n$
  2. se $a_n = 2^n$, temos que: $\quad a_0 = 1$, $\quad a_1 = 2$ $\quad$ e $\quad a_2 = 4$
     - então: $2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a_2$
  3. se $a_n = 5$, então, para $n \geq 2$:
     - $2a_{n-1} - a_{n-2} = 2 \cdot 5 - 5 = 5 = a_n$

  Conclusão: 1 e 3 são soluções e 2 não o é. □

- Condições iniciais para uma sequência: especificam os termos que precedem o 1ro termo aonde a relação de recorrência atua

- **Exemplo:**

  $a_0 = 3$ e $a_1 = 5$

  $a_n = a_{n-1} + a_{n-2}$, $\quad$ para $\quad n = 2, 3, 4, \ldots$

- A relação de recorrência e as condições iniciais definem unicamente uma sequência
  - pois juntos são uma definição recursiva da sequência: "qualquer termo pode ser encontrado a partir das cindições iniciais utilizando-se a relação um nro suficiente de vezes"

Modelando com Relações de Recorrência

- **Exemplo:** Seja $A = \{0, 1\}$. Forneça uma relação de recorrência para:

  c_n: "nro de strings de comprimento n em A^* que não contêm $\mathbf{0}$'s adjacentes"

  Solução:

  $\mathbf{0}$ e $\mathbf{1}$ são as únicas strings de comprimento $\mathbf{1}$ $\quad \Rightarrow \quad c_1 = 2$

  $c_2 = 3$: as únicas strings deste tipo são $01, 10, 11$

  - Em geral, seja uma string w de comprimento $n - 1$ que (já) não contem $\mathbf{00}$:
    * se concatenada com $\mathbf{1}$, forma uma string $1 \cdot w$
    * de comprimento n e que não contem $\mathbf{00}$
  - Única outra possibilidade de início para uma string "boa" de comprimento n: $\mathbf{01}$
    * "pode até começar com $\mathbf{0}$, desde que seguido por $\mathbf{1}$"
    * estas strings são da forma $01 \cdot v$
    * onde v é uma string "boa" de comprimento $n - 2$
  - Portanto: $c_n = c_{n-1} + c_{n-2}$
    * com as condições iniciais: $c_1 = 2$ $\quad$ e $\quad c_2 = 3$ □

- **Exemplo:** Listar todas as sequências de n elementos sem repetições que podem ser construídas a partir de $\{1, 2, 3, \ldots, n\}$

  Solução: uma abordagem para resolver este problema é proceder recursivamente:

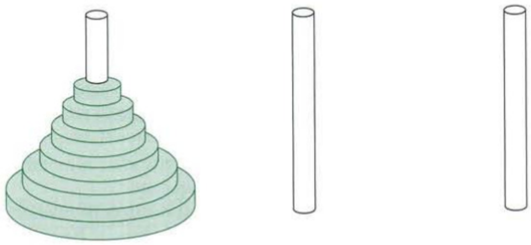
  - **Passo 1**: listas todas as sequências sem repetições a partir de $\{1, 2, 3, \ldots, n-1\}$
  - **Passo 2**: para cada sequência, inserir n em cada um dos n locais possíveis:
    * no início, no final ou entre cada par de números na sequência

    imprimir resultado e remover n
  - nro de ações do tipo "inserir-imprimir-remover":

    $= n \times$ nro de sequências produzidas no passo 2

    $=$ nro de sequências de n elementos
  - logo: nro de seqs de n elems $= n \times$ (nro de seqs de $(n-1)$ elems)
    * fórmula recursiva para o número de sequências de n elementos
    * condição inicial?

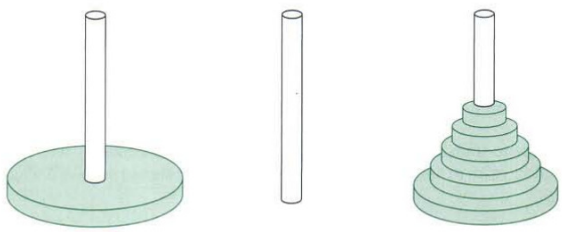
- **Exemplo (Torre de Hanói)**: Sejam 3 pinos fixos e discos de diferentes tamanhos:



  - inicialmente: discos colocados sobre o 1ro pino em ordem de tamanho, com o maior ao fundo
  - os discos podem ser movidos um a um, de um pino para outro
  - um disco nunca pode ser colocado sobre um menor do que ele
  - objetivo: colocar todos os discos no 2o pino, com o maior ao fundo

  Seja $H_n =$ nro de movimentos para resolver a torre com n discos

  Questão: obter uma relação de recorrência para a sequência $\{H_n\}$:
  - comece com n discos no pino 1
  - transfira os $n-1$ discos do topo para o pino 3 usando H_{n-1} movimentos:



  - então use um movimento para transferir o disco maior para o pino 2
  - mais H_{n-1} movimentos deixam os $n-1$ discos do pino 3 no pino 2
  - como não é possível resolver em menos passos, obtemos:

    $H_n = 2H_{n-1} + 1$ (para $H_1 = 1$)
  - resolvendo:

    $H_n = 2^n - 1$ (prove isto) □

- **Exemplo**: Encontre uma relação de recorrência para:

  C_n: nro de modos de parentetizar o produto de $n+1$ nros $x_0 \cdot x_1 \cdot x_2 \cdots x_n$

  – Nota: $C_3 = 5$, pois há 5 modos de especificar a ordem do produto de 4 nros:

  $((x_0 \cdot x_1) \cdot x_2) \cdot x_3$, $(x_0 \cdot (x_1 \cdot x_2)) \cdot x_3$, $(x_0 \cdot x_1) \cdot (x_2 \cdot x_3)$

  $x_0 \cdot ((x_1 \cdot x_2) \cdot x_3)$ e $x_0 \cdot (x_1 \cdot (x_2 \cdot x_3))$

  Solução:

  – Note que, independente do modo como inserimos ()s no produto, um "·" fica fora
    * (o operador correspondente à última multiplicação)

  – Digamos que este operador final aparece entre os nros x_k e x_{k+1}:
    * Neste caso, há $C_k C_{n-k-1}$ modos de inserir ()s, pois:
      · Há C_k modos de inserir ()s no produto $x_0 \cdot x_1 \cdots x_k$ e:
      · Há C_{n-k-1} modos de inserir ()s no produto $x_{k+1} \cdot x_{k+2} \cdots x_n$

  – Como o final pode ser qualquer uma das multiplicações: $\boxed{C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1}}$
    * Condições iniciais: $C_0 = 1$ e $C_1 = 1$
      · $C_2 = C_0C_1 + C_1C_0 = 2$
      · $C_3 = C_0C_2 + C_1C_1 + C_2C_0 = 5$
      · $C_4 = 14, \quad C_5 = 42, \quad \ldots$

  – Esta é a sequência dos Números de Catalão

  – Pode-se mostrar que a solução desta relação é:

$$C_n = \frac{{}_{2n}C_n}{n+1} = {}_{2n}C_n - {}_{2n}C_{n-1} \qquad \square$$

Resolvendo Relações de Recorrência

- Uma técnica para encontrar uma fórmula explícita para a sequência definida por uma relação de recorrência é o backtracking (ou "técnica iterativa")

Backtracking

- **Exemplo 1:** A relação de recorrência $a_n = a_{n-1} + 3$ com $a_1 = 2$ define a sequência: $2, 5, 8, \ldots$.

  – Fazemos o "backtracking" de a_n substituindo a definição de a_{n-1}, a_{n-2} e assim por diante

  – Até que um padrão fique claro:

  $$\begin{aligned} a_n &= a_{n-1} + 3 \\ &= (a_{n-2} + 3) + 3 \\ &= ((a_{n-3} + 3) + 3) + 3 \end{aligned} \qquad \text{ou} \qquad \begin{aligned} a_n &= a_{n-1} + 3 \\ &= a_{n-2} + 2 \cdot 3 \\ &= a_{n-3} + 3 \cdot 3 \end{aligned}$$

– Eventualmente, chegaremos a:

$$a_n = a_{n-(n-1)} + (n-1)\cdot 3 = a_1 + (n-1)\cdot 3 = 2 + (n-1)\cdot 3$$

– Logo, uma fórmula explícita para a sequência é: $a_n = 2 + (n-1).3$ $\square$

- **Exemplo 2:** Use o backtracking para encontrar uma fórmula explícita para a sequência definida pela relação de recorrência $b_n = 2.b_{n-1} + 1$ com condição inicial $b_1 = 7$.

  Solução:

  – Substituir definição do termo anterior na fórmula:

  $$\begin{aligned} b_n &= 2b_{n-1} + 1 \\ &= 2(2b_{n-2} + 1) + 1 \\ &= 2[2(2b_{n-3} + 1) + 1] + 1 \\ &= 2^3 b_{n-3} + 4 + 2 + 1 \\ &= 2^3 b_{n-3} + 2^2 + 2^1 + 1 \end{aligned}$$

  – Note que um padrão está aparecendo com as re-escritas de b_n.

  – O backtracking terminará em:

  $$\begin{aligned} b_n &= 2^{n-1} b_{n-(n-1)} + 2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2^1 + 1 \\ &= 2^{n-1} b_1 + 2^{n-1} - 1 && \text{(ver exerc. de indução)} \\ &= 7 \cdot 2^{n-1} + 2^{n-1} - 1 && \text{(usando } b_1 = 7\text{)} \\ &= 8 \cdot 2^{n-1} - 1 = 2^{n+2} - 1 && \square \end{aligned}$$

- **Nota 1**: não há regras prontas para esta "re-escrita":

  – pode ser necessário experimentar um pouco

- **Nota 2:** duas somas muito úteis, que já foram provadas:

  $$1 + a + a^2 + a^3 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$$

  $$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

- **Nota 3:** o backtracking pode nunca chegar a revelar um padrão explícito

  – em seguida, veremos uma técnica mais geral para resolver uma relação de recorrência...

Relações de Recorrência Homogêneas

- Uma relação de recorrência é uma relação homogênea linear de grau k se for da forma:

  $$a_n = r_1 a_{n-1} + r_2 a_{n-2} + \cdots + r_k a_{n-k}$$

  – aonde os r_i's são constantes

  Descrição:

  – cada parcela é construída do mesmo ("homogêneo") modo

  – cada parcela é um múltiplo de um dos k ("grau k") termos que antecedem a_n ("linear")

Exemplos:

(a) A relação $c_n = (-2)c_{n-1}$ é uma relação de recorrência homogênea linear de grau 1.

(b) A relação $a_n = a_{n-1} + 3$ não é uma relação de recorrência homogênea linear.

(c) A relação $f_n = f_{n-1} + f_{n-2}$ é uma relação de recorrência homogênea linear de grau 2.

(d) A relação $g_n = g_{n-1}^2 + g_{n-2}$ não é uma relação homogênea linear.

- Seja uma relação de recorrência homogênea linear de grau k:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

- Abordagem básica para resolvê-la:
  - buscar soluções da forma $a_n = r^n$, aonde r é uma constante
  - note que $a_n = r^n$ é uma solução se e somente se:

    $$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k}$$

    * dividindo os dois lados por r^{n-k}, obtemos a equação característica:

    $$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$$

- Logo: $a_n = r^n$ é solução da recorrência linear, sse r é solução da equação acima
  - as soluções desta equação são as raízes características da relação
  - estas raízes características fornecerão uma fórmula explícita para todas as soluções da relação de recorrência

- Primeiro, veremos o grau 2 em detalhes
- Então os resultados correspondentes para grau > 2 serão apenas enunciados

- **Teorema 1:**

(a) Se a equação característica $r^2 - c_1.r - c_2 = 0$, da relação de recorrência $a_n = c_1.a_{n-1} + c_2.a_{n-2}$, tem duas raízes distintas
r_1 e r_2, então a fórmula explícita para a sequência é dada por:

$$a_n = u.r_1^n + v.r_2^n$$

(b) Se a equação característica $r^2 - c_1.r - c_2 = 0$ tem uma raiz única r_0, a fórmula explícita é dada por:

$$a_n = u.{r_0}^n + v.n.{r_0}^n$$

* aonde u e v dependem das condições iniciais.

- **Prova de (a):** (duas raízes distintas: $a_n = u.r_1^n + v.r_2^n$)
  - Vamos mostrar que: $a_n = u.r_1^n + v.r_2^n, \quad n \geq 1$

    define a mesma sequência que: $a_n = c_1.a_{n-1} + c_2 a_{n-2}$
  - Primeiro, note que as condições iniciais são satisfeitas, pois u e v vêm de:

    $a_1 = u.r_1 + v.r_2$ e $a_2 = u.r_1^2 + v.r_2^2$
  - Já que r_1 e r_2 são raízes de $r^2 - c_1.r - c_2 = 0$, temos:

    $r_1^2 - c_1.r_1 - c_2 = 0$ e $r_2^2 - c_1.r_2 - c_2 = 0$
  - Então:
$$\begin{aligned} a_n &= u.r_1^n + v.r_2^n \\ &= u.r_1^{n-2}r_1^2 + v.r_2^{n-2}r_2^2 \\ &= u.r_1^{n-2}(c_1.r_1 + c_2) + v.r_2^{n-2}(c_1.r_2 + c_2) \\ &= (c_1.u.r_1^{n-1} + c_2.u.r_1^{n-2}) + (c_1.v.r_2^{n-1} + c_2.v.c_2^{n-2}) \\ &= (c_1.u.r_1^{n-1} + c_1.v.r_2^{n-1}) + (c_2.u.r_1^{n-2} + c_2.v.r_2^{n-2}) \\ &= c_1.a_{n-1} + c_2.a_{n-2} \qquad \Box \end{aligned}$$

- **Prova de (b):** totalmente similar.

- **Exemplo:** Encontre uma fórmula explícita para a sequência:

  $a_n = 3.a_{n-1} - 2.a_{n-2}$

  aonde: $a_1 = 5$ e $a_2 = 3$

  Solução:
  - A relação dada é homogênea linear de grau 2
  - Equação associada: $r^2 = 3r - 2$
    * ou: $r^2 - 3r + 2 = 0$, raízes: 1 e 2
  - O teorema 1 mostra que u e v vêm da solução de:

    $a_1 = u.(1) + v.(2)$ e $a_2 = u.(1)^2 + v.(2)^2$
    * levando a: $u = 7$ e $v = -1$
  - Daí, pelo teorema 1, temos:

    $a_n = 7 \cdot 1^n + (-1) \cdot 2^n = 7 - 2^n \qquad \Box$

- **Exemplo:** Resolva: $d_n = 2d_{n-1} - d_{n-2}$, com condições iniciais $d_1 = 1.5$ e $d_2 = 3$

  Solução:
  - Equação associada: $r^2 - 2.r + 1 = 0$
    * com uma raiz múltipla: 1
  - Pelo teorema 1(b): $d_n = u.(1)^n + v.n.(1)^n$
  - Usando esta fórmula e as condições iniciais, temos que:

    $d_1 = 1.5 = u + v.(1)$

    $d_2 = 3 = u + v.(2)$
    * cuja solução é: $u = 0$ e $v = 1.5$
  - Logo: $d_n = 1.5 \times n \qquad \Box$

- Nota: apesar da sequência de Fibonacci ser bem conhecida, a sua forma explícita levou mais de 200 anos para ser encontrada...

- **Exemplo:** Encontre uma fórmula explícita para a sequência de Fibonacci:

  $$f_n = f_{n-1} + f_{n-2}, \quad \text{onde} \quad f_1 = f_2 = 1$$

  Solução:

  - Relação de recorrência homogênea linear de grau 2
  - Equação característica: $r^2 - r - 1 = 0$
    * cujas raízes são: $r_1 = \frac{1+\sqrt{5}}{2}$ e $r_2 = \frac{1-\sqrt{5}}{2}$
  - O u e o v do teorema 1 vêm da solução de:

  $$\begin{cases} u.(\frac{1+\sqrt{5}}{2}) + v.(\frac{1-\sqrt{5}}{2}) = 1 \\ u.(\frac{1+\sqrt{5}}{2})^2 + v.(\frac{1-\sqrt{5}}{2})^2 = 1 \end{cases}$$

  - O que leva a: $u = \frac{1}{\sqrt{5}}$ e $v = -\frac{1}{\sqrt{5}}$
  - E a fórmula explícita para a sequência de Fibonacci é:

  $$\boxed{f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n} \qquad \square$$

- A seguir, resultado geral sobre:

  - solução de relações de recorrência homogêneas lineares
  - com coeficientes constantes
  - aonde o grau pode ser > 2
  - assumindo que a equação característica tem raízes distintas

- **Teorema:** Suponha que a equação característica $r^k - c_1.r^{k-1} - \cdots - c_k = 0$ (c_i's reais) tem k raízes distintas $r_1, r_2, \ldots, r_k$.

  - Então uma sequência $\{a_n\}$ é uma solução da relação de recorrência:

    $$a_n = c_1.a_{n-1} + c_2.a_{n-2} + \cdots + c_k.a_{n-k}$$

  - se e somente se:

    $$a_n = \alpha_1.{r_1}^n + \alpha_2.{r_2}^n + \cdots + \alpha_k.{r_k}^n$$

    aonde $\alpha_1, \alpha_2, \ldots, \alpha_k$ são constantes

  Prova: extensão do caso $k = 2$.

- **Exemplo:** Encontre a solução de: $\boldsymbol{a_n = 6.a_{n-1} - 11.a_{n-2} + 6.a_{n-3}}$

  aonde: $\boldsymbol{a_0 = 2}$, $\boldsymbol{a_1 = 5}$ e $\boldsymbol{a_2 = 15}$

- **Solução:**
  - Polinômio característico: $\boldsymbol{r^3 - 6.r^2 + 11.r - 6 = 0}$
  - Raízes características: $\boldsymbol{r = 1}$, $\boldsymbol{r = 2}$ e $\boldsymbol{r = 3}$
  - De modo que as soluções para esta recorrência são da forma:

    $\boldsymbol{a_n = \alpha_1 \cdot 1^n + \alpha_2 \cdot 2^n + \alpha_3 \cdot 3^n}$
  - As condições iniciais fornecem:

    $$\begin{array}{l} \boldsymbol{a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3} \\ \boldsymbol{a_1 = 5 = \alpha_1 + \alpha_2 \cdot 2 + \alpha_3 \cdot 3} \\ \boldsymbol{a_2 = 15 = \alpha_1 + \alpha_2 \cdot 4 + \alpha_3 \cdot 9} \\ \Rightarrow \quad \boldsymbol{\alpha_1 = 1, \quad \alpha_2 = -1} \quad \text{e} \quad \boldsymbol{\alpha_3 = 2} \end{array}$$
  - Solução da relação de recorrência: $\boldsymbol{a_n = 1 - 2^n + 2 \cdot 3^n}$ $\square$

Leituras sobre Relações de Recorrência

- Kolman5: item 3.5
- Rosen6: itens 7.1 e 7.2

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

10) Relações de ordenamento

10.1) Conjuntos parcialmente ordenados (posets)

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*
- *Rosen, "Discrete Mathematics and its Aplications",* 6^{th} *ed., McGraw-Hill, 2007.*

Ordenamentos parciais

- Algumas relações são usadas para ordenar elementos de conjuntos (alguns ou todos):
  - ordenamos palavras usando xRy, onde x vem antes de y no dicionário
  - fazemos a programação de um projeto com xRy, onde x e y são tarefas tais que x deve ser concluída antes de y começar
- Quando adicionamos todos os pares (x, x), obtemos uma relação que é reflexiva, antissimétrica e transitiva.
- **Ordenamento Parcial**: relação R sobre um conjunto A que é reflexiva, antissimétrica e transitiva.

  Reflexividade: $(a, a) \in R, \quad \forall a \in A$

  Antissimetria: $(a, b) \in R \;\text{ e }\; (b, a) \in R \;\rightarrow\; a = b$

  $*$ para $a \neq b$: ou $(a, b) \notin R$ ou $(b, a) \notin R$

  Transitividade: $(a, b) \in R \;\text{ e }\; (b, c) \in R \;\rightarrow\; (a, c) \in R$

- Um conjunto A, junto com seu Ordenamento Parcial R é chamado de **conjunto parcialmente ordenado ("poset")**.
  - Denotado por (A, R).
- **Exemplo1**: A relação $\leq$ é um ordenamento parcial sobre o conjunto dos inteiros (assim como $\geq$).
  - $\leq = \{\, (n_1, n_2) \in Z \times Z \mid n_1$ "é menor ou igual a" $n_2 \,\}$
    - $a \leq a$ para todo inteiro a $\Rightarrow$ $\leq$ é reflexiva
    - se $a \leq b$ e $b \leq a$, então $a = b$ $\Rightarrow$ $\leq$ é antissimétrica
    - se $a \leq b$ e $b \leq c$, então $a \leq c$ $\Rightarrow$ $\leq$ é transitiva
  - conclui-se que $\leq$ é um ordenamento parcial sobre o conjunto dos inteiros e $(Z, \leq)$ é um poset
- **Exemplo2**: A relação de divisibilidade ($a\ R\ b$ se e somente se $a \mid b$) é um ordenamento parcial sobre Z^+.
  - Ela é reflexiva, antissimétrica e transitiva.
  - Conclui-se que $(Z^+, |)$ é um poset.

- **Exemplo3**: A relação de inclusão, ($\subseteq$) é um ordenamento parcial sobre o conjunto $P(S)$ (= "todos os subconjuntos de S").
  - $\subseteq \; = \; \{(S_1, S_2) \in P(S) \times P(S) \mid S_1 \subseteq S_2\}$
  - Seja $S_1 \in P(S)$:
    - como $S_1 \subseteq S_1$, $\subseteq$ é reflexiva
    - $\subseteq$ é antissimétrica, pois:
      $S_1 \subseteq S_2$ e $S_2 \subseteq S_1 \;\; \rightarrow \;\; S_1 = S_2$
    - $\subseteq$ é transitiva, pois:
      $S_1 \subseteq S_2$ e $S_2 \subseteq S_3 \;\; \rightarrow \;\; S_1 \subseteq S_3$
  - Portanto, $(P(S), \subseteq)$ é um poset.

- **Exemplo4**: Seja W o conjunto de todas as relações de equivalência sobre um conjunto A.
  - W consiste de subconjuntos de $A \times A$
  - Então W é um poset (sob o ordenamento parcial de inclusão)
  - Se R e S são relações de equivalência sobre A, o mesmo pode ser expresso como:
    - $R \subseteq S$ se e somente se $x \; R \; y \;\Rightarrow\; x \; S \; y$ para todo x, y *em* A
  - Então $(W, \subseteq)$ é um poset. $\square$

- **Exemplo5**: A relação $<$ sobre Z^+ <u>não é</u> um ordenamento parcial, pois não é reflexiva.

INVERSAS E DUAIS

- **Exemplo6**: A relação inversa R^{-1} de um ordenamento parcial R sobre um conjunto A também é um ordenamento parcial.
  - Se R é reflexiva, antissimétrica e transitiva, então:
    - $\Delta \subseteq R$
    - $R \cap R^{-1} \subseteq \Delta$
    - $R^2 \subseteq R$
  - A relação R^{-1} também é um poset, pois, tomando inversas, vêm:
    - $\Delta^{-1} = \Delta \subseteq R^{-1}$
    - $R^{-1} \cap (R^{-1})^{-1} = R^{-1} \cap R \subseteq \Delta$
    - $(R^{-1})^2 \subseteq R^{-1}$ $\square$

- (A, R^{-1}) é o **poset dual** de (A, R).
  - O ordenamento parcial R^{-1} é o **dual** de R.
  - Exemplo de posets duais: $(Z, \leq)$ e $(Z, \geq)$

Convenção

- O símbolo "$\leq$" vai denotar qualquer relação de ordem parcial.
  - Não apenas as do tipo "menor ou igual".
  - Propriedades ficam mais familiares.
  - Mas, em geral, os posets não terão nada em comum entre si, ou com a relação "$\leq$" usual.
    - Quando necessário, usaremos algo como "$\leq_1$" ou "$\leq'$"
- Sempre usaremos o símbolo $\geq$ para o ordenamento parcial $\leq^{-1}$
- A notação $a < b$ significa "$a \leq b$, mas $a \neq b$".

Comparabilidade

- Quando a e b são elementos do poset $(A, \leq)$, não é necessário que ocorra sempre $a \leq b$ ou $b \leq a$.
- **Exemplo**: em $(Z, |)$, 2 não está relacionado com 3 e nem 3 com 2.
- Os elementos a e b de um poset $(A, \leq)$ são **comparáveis** se ou $a \leq b$ ou $b \leq a$.
  - Se nem $a \leq b$ nem $b \leq a$, a e b são ditos **incomparáveis**.

- **Exemplo**: No poset $(Z^+, |)$:
  - Os inteiros 3 e 9 são comparáveis, pois $3 \mid 9$.
  - Já os inteiros 5 e 7 são incomparáveis, pois $5 \nmid 7$ e $7 \nmid 5$.

Ordenamentos totais

- O adjetivo "parcial" é usado porque pode haver pares de elementos incomparáveis.
- Se todos os elementos em um poset $(A, \leq)$ são comparáveis, o conjunto A é dito **totalmente ordenado**.
  - Neste caso, o ordenamento parcial é chamado de **ordenamento linear**.
  - Diz-se também que A é uma **cadeia**.

- **Exemplo1**: O poset $(Z, \leq)$ é totalmente ordenado, pois $a \leq b$ ou $b \leq a$ sempre que a e b são inteiros.

- **Exemplo2**: O poset $(Z^+, |)$ não é totalmente ordenado, pois ele contém elementos incomparáveis (por ex., 5 e 7).

Ordenamento produto

- **Teorema**: Se $(A, \leq_1)$ e $(B, \leq_2)$ são posets, então $(A \times B, \leq_3)$ também é um poset, com ordenamento parcial definido por:

  $(a, b) \leq_3 (a', b')$ se $a \leq_1 a'$ em A e $b \leq_2 b'$ em B

- **Prova**: mostrar que $\leq_3$ é reflexiva, antissimétrica e transitiva:
  - Reflexividade: se $(a,b) \in A \times B$, então $(a,b) \leq_3 (a,b)$, pois:

    $a \leq_1 a$ em A e $b \leq_2 b$ em B
  - Antissimetria: suponha que $(a,b) \leq_3 (a',b')$ e que $(a',b') \leq_3 (a,b)$, com $a,a' \in A$ e $b,b' \in B$.

    Então:
    * em A: $a \leq_1 a'$ e $a' \leq_1 a \Rightarrow a = a'$
    * em B: $b \leq_2 b'$ e $b' \leq_2 b \Rightarrow b = b'$
    * ou seja:
      $(a,b) \leq_3 (a',b')$ e $(a',b') \leq_3 (a,b) \Rightarrow (a,b) = (a',b')$
  - Transitividade: suponha $(a,b) \leq_3 (a',b')$ e $(a',b') \leq_3 (a'',b'')$.
    * Pela propriedade transitiva da ordem parcial em A:
      $$a \leq_1 a' \quad \text{e} \quad a' \leq_1 a'' \quad \Rightarrow \quad a \leq_1 a''$$
    * Pela propriedade transitiva em B:
      $$b \leq_2 b' \quad \text{e} \quad b' \leq_2 b'' \quad \Rightarrow \quad b \leq_2 b''$$
    * Logo:
      $$(a,b) \leq_3 (a',b') \quad \text{e} \quad (a',b') \leq_3 (a'',b'') \quad \Rightarrow \quad (a,b) \leq_3 (a'',b'')$$
  - Conclusão: $(A \times B, \leq_3)$ é um poset. $\square$

Ordenamentos Lexicográficos

- Uma ordem parcial $\leq$ definida sobre o produto cartesiano como acima é chamada de **ordem parcial produto**.
- Sejam os posets $(A, \leq_1)$ e $(B, \leq_2)$. Define-se a **ordem lexicográfica** (ou "dicionário") sobre $A \times B$ como:

  $(a,b) \prec (a',b')$ se: $a <_1 a'$ em A

  ou se: $a = a'$ em A e $b \leq_2 b'$ em B
  - "O ordenamento dos elementos na 1ra variável domina, exceto no caso de coincidir, quando a atenção passa para a 2a. variável".
- A ordem lexicográfica pode ser estendida para os produtos cartesianos $A_1 \times A_2 \times ... \times A_n$ como:

  $(a_1, a_2, ..., a_n) \prec (a'_1, a'_2, ..., a'_n)$ se e somente se:

  $$\begin{array}{l} a_1 < a'_1 \quad \text{ou} \\ a_1 = a'_1 \quad \text{e} \quad a_2 < a'_2 \quad \text{ou} \\ a_1 = a'_1 \ , \ a_2 = a'_2 \quad \text{e} \quad a_3 < a'_3 \quad \text{ou ...} \\ \qquad \vdots \\ a_1 = a'_1 \ , \ a_2 = a'_2 \ , \ \ldots \ , \ a_{n-1} = a'_{n-1} \quad \text{e} \quad a_n \leq a'_n \end{array}$$
  - "A 1ra coordenada domina, exceto para igualdade, caso em que se considera a 2a coordenada - e assim por diante".

- **Exemplo**: Seja $S = \{a, b, c, ..., z\}$ o alfabeto comum, ordenado da forma usual.
- Então S^n pode ser identificado como o conjunto de todas as palavras de comprimento n.
- Uma ordem lexicográfica sobre S^n tem a propriedade de que, se $w1 \prec w2$, então w1 precederia w2 em uma listagem de dicionário.
- Portanto:

  livre $\prec$ livro

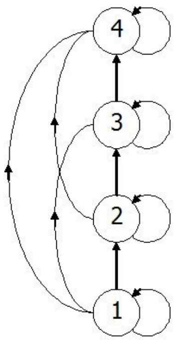
  firma $\prec$ forma

  carro $\prec$ carta.

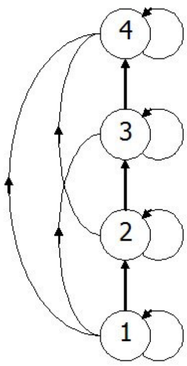
Diagramas de Hasse de Posets

- Posets são relações e pode-se sempre desenhar seus digrafos.
- No entanto, muitas arestas não precisam ser mostradas, já que devem necessariamente estar presentes (digrafo sempre reflexivo e transitivo).
- Pode-se retirar as arestas que sempre devem estar presentes.
- As estruturas obtidas desta forma são chamadas de **Diagramas de Hasse** dos posets.

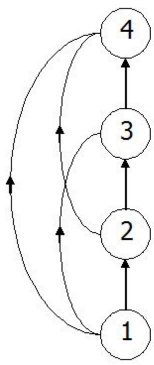
- **Exemplo1**: Considere o digrafo da ordem parcial, sobre o conjunto $A = \{1, 2, 3, 4\}$, dado por $\leq = \{(a, b) \in A \times A \mid a \leq b\}$:

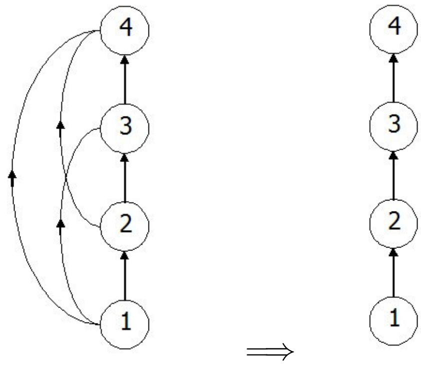


  - Esta relação é uma ordem parcial $\Rightarrow$ $\leq$ é automaticamente reflexiva $\Rightarrow$ possui vértices em todos os loops $\Rightarrow$ os loops podem ser omitidos:



$\Longrightarrow$

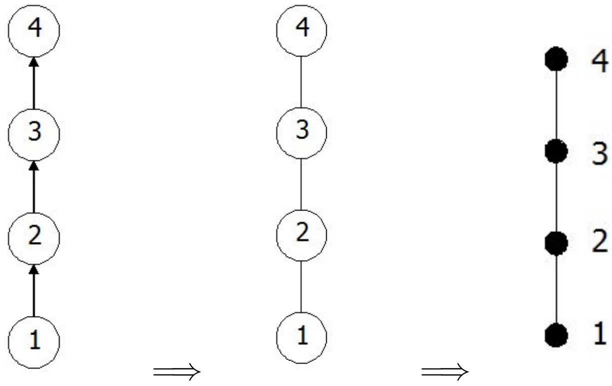




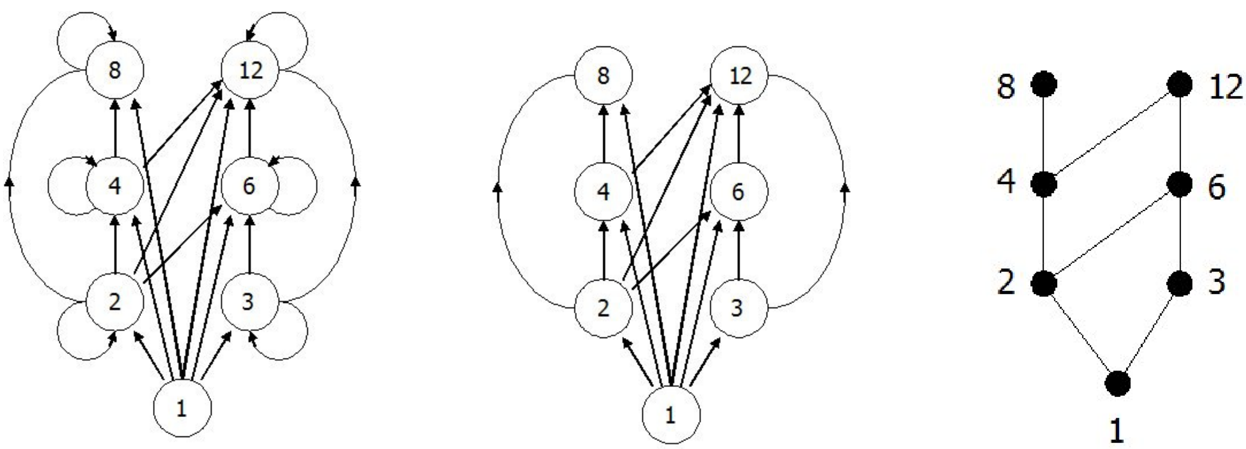
- Esta relação é uma ordem parcial $\Rightarrow$ $\leq$ é automaticamente transitiva $\Rightarrow$ as arestas presentes por causa da transitividade não precisam ser mostradas:

- Ainda, assumindo-se que se desenhe todas as arestas apontadas para cima, pode-se omitir a sua orientação.

- Finalmente, substitui-se os círculos por pontos:



- **Exemplo2**: Seja $A = \{1, 2, 3, 4, 6, 8, 12\}$. A ordem parcial é a de divisibilidade sobre A (ou seja, $a \leq b \Leftrightarrow a \mid b$). Desenhe o diagrama de Hasse do poset $(A, \leq)$.



Posets - definições

- Se $(A, \leq)$ é um poset e $a, b \in A$, então:
  1. Se $a \leq b$, diz-se que "a **precede** b"
  2. Se $a < b$, diz-se que "a **precede** b **estritamente**"
  3. Se $a \geq b$, diz-se que "a **sucede** b"
  4. Se $a > b$, diz-se que "a **sucede** b **estritamente**"

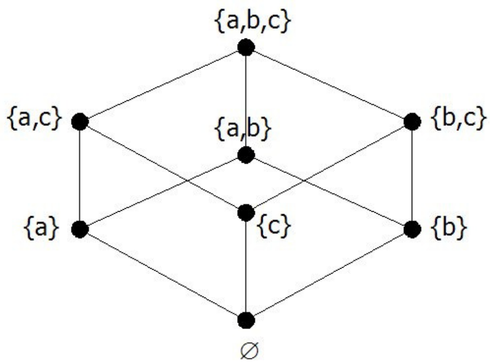
- Seja $(A, \leq)$ um poset e $a, b \in A$. Diz-se que a é um **predecessor imediato** de b e b é um **sucessor imediato** de a se $a < b$ mas não existe nenhum elemento $c \in A$ tal que $a < c < b$
  - escreve-se: $a \angle b$

Diagramas de Hasse de Posets

- **Outra maneira** de construir o Diagrama de Hasse de um poset:
  - O Diagrama de Hasse de um poset $(A, \leq)$ é o digrafo no qual os vértices são elementos de A.
    - Existe aresta de um vértice a para um vértice b sempre que $a \angle b$.
  - Então:
    - Ao invés de desenhar uma seta de a para b, coloca-se b mais alto do que a e desenha-se uma linha entre eles.
    - Fica subentendido que o movimento para cima indica sucessão.
    - No diagrama de Hasse existe um caminho orientado de um vértice x para um vértice y se e somente se $x \angle y$.

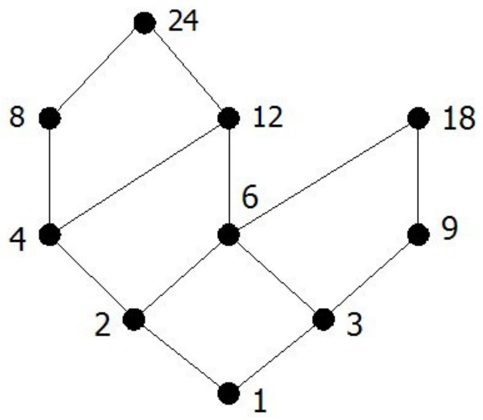
- **Exemplo1**: Seja $S = \{a, b, c\}$ e seja $A = 2^S$ (o conjunto de todas as partes de S). Desenhe o diagrama de Hasse do poset $(A, \subseteq)$.

  $A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$



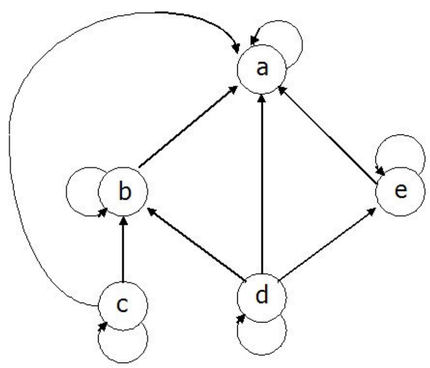
- **Procedimento**:
  - Eliminar loops
  - Eliminar arestas ligadas à transitividade: $(\emptyset, \{a, b\})$, $(\emptyset, \{a, c\})$, $(\emptyset, \{b, c\})$, $(\emptyset, \{a, b, c\})$, $(\{a\}, \{a, b, c\})$, $(\{b\}, \{a, b, c\})$, $(\{c\}, \{a, b, c\})$,

- **Exemplo2**: Seja $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$. A ordem parcial é a divisibilidade sobre A (ou seja, $a \leq b \Leftrightarrow a \mid b$). Desenhe o diagrama de Hasse do poset $(A, \leq)$.

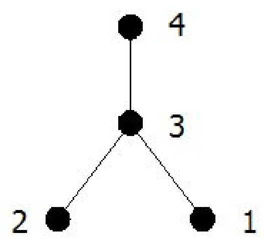


EXERCÍCIOS

- **Exerc1**: Determine o diagrama de Hasse do ordenamento parcial que tem o seguinte digrafo:



- **Exerc2**: Descreva os pares ordenados na relação determinada pelo diagrama de Hasse sobre o conjunto $A = \{1, 2, 3, 4\}$, dado abaixo:

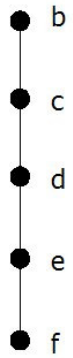


- **Exerc3**: Determine o diagrama de Hasse da relação sobre o conjunto $A = \{1, 2, 3, 4, 5\}$ cuja matriz é dada por:

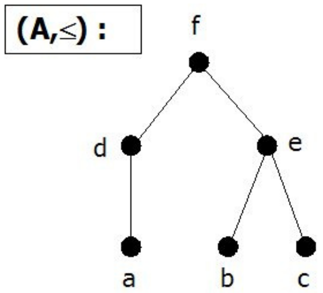
$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

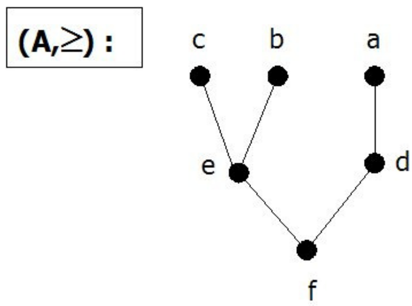
Observações

- O diagrama de Hasse de um conjunto linearmente ordenado tem sempre a forma de uma linha:



- O diagrama de Hasse de $(A, \geq)$ é o diagrama de Hasse do seu dual $(A, \leq)$ de cabeça para baixo:





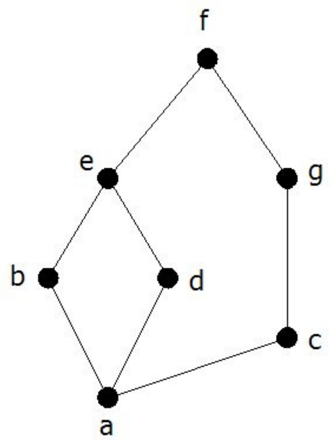
Ordenamento topológico

- Dado um poset $(A, \leq)$, às vezes é preciso encontrar uma ordem linear $\prec$ para o conjunto A que seja simplesmente uma extensão da ordem parcial dada:

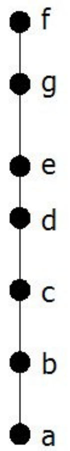
  se $\;a \leq b,\;$ então (na nova ordem) $\;a \prec b$

- O processo de construir uma ordem linear do tipo $\prec$ é chamado de **ordenamento topológico**.
- **Exemplo**: suponha que um projeto seja composto de 20 tarefas diferentes:
  - Algumas tarefas só podem ser completadas depois que outras tenham sido acabadas.
  - Como encontrar uma ordem para estas tarefas?
- Para modelar este problema, monta-se uma ordem parcial sobre o conjunto de tarefas, de modo que:
  - "$a < b$" $\Leftrightarrow$ "b é uma tarefa que não pode ser iniciada até que a esteja completa"
  - Para produzir uma programação para este projeto, é preciso uma ordem para todas as 20 tarefas que seja compatível com esta ordem parcial.
- Uma ordem linear total $\prec$ é dita ser **compatível** com uma ordem parcial $\leq$ se:
  - $a \prec b$ sempre que $a \leq b$.
- O problema de obter ordens lineares a partir de uma ordem parcial é chamado de **ordenamento topológico**.

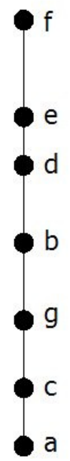
- **Exemplo**: Algumas ordens lineares compatíveis com um poset dado:



$\Longrightarrow$



$\Longrightarrow$



- *Questão: Como encontrar ordenamentos topológicos??*

Isomorfismo em posets

- Lembrete: Uma função $f : A \to B$ é chamada de uma bijeção (correspondência um-para-um) entre A e B se:
  - f é uma função injetora: $f(a) = f(b) \Rightarrow a = b$
  - f é sobrejetora: $Im(f) = B$
- Sejam $(A, \leq)$ e $(A', \leq')$ posets e seja $f : A \to A'$ uma bijeção:
  - esta função f é chamada de um **isomorfismo** de $(A, \leq)$ para $(A', \leq')$ se, para quaisquer elementos $a, b \in A$:

    $\boxed{a \leq b \;\; \Rightarrow \;\; f(a) \leq' f(b)}$.

- **Exemplo**: Sejam:

  $A = Z^+$ (inteiros positivos) e seja $\leq$ a ordem usual sobre A.

  A' = inteiros pares e seja $\leq'$ a ordem usual sobre A'.

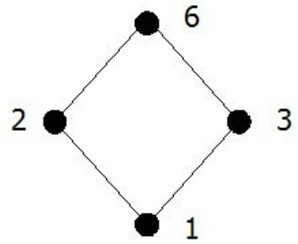
  Mostre que a função $f : A \to A'$ dada por $f(a) = 2.a$ é um isomorfismo de $(A, \leq)$ para $(A', \leq')$.

  1. a função f é uma bijeção, ou seja, f é injetora e sobrejetora:
     - f é injetora pois se $f(a) = f(b)$, então pela definição de f tem-se que $2a = 2b$ e segue daí que $a = b$
     - se $c \in A'$, então c é par e sempre pode ser escrito como $c = 2a$ para algum $a \in A \;\; \Rightarrow$ $c = f(a) \Rightarrow f$ é sobrejetora
     - logo, f é uma bijeção.
  2. f preserva o ordenamento $\leq'$:
     - se $a, b \in A$, é claro que $a \leq b \Leftrightarrow 2a \leq 2b$, isto é:
       $a \leq b \;\Leftrightarrow\; f(a) \leq' f(b)$ $\square$

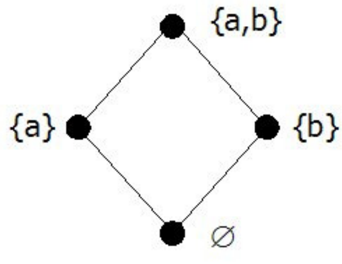
- 2 posets isomórficos têm os mesmos diagramas de Hasse.
- **Teorema**: Sejam $(A, \leq)$ e $(A', \leq')$ dois posets finitos, seja $f : A \to A'$ uma bijeção e seja H um diagrama de Hasse de $(A, \leq)$.
  - Então: se f é um isomorfismo e cada designação a de H for trocada por $f(a)$, então H torna-se um diagrama de Hasse de $(A', \leq')$.
  - *Reciprocamente*: se H se torna um diagrama de Hasse de $(A', \leq')$ sempre que a é substituído por $f(a)$ em H, então f é um isomorfismo.

- Se $f : A \to B$ é uma bijeção do poset $(A, \leq)$ para o conjunto B, podemos usar a função f para definir uma ordem parcial $\leq'$ sobre B:
  - construa o diagrama de Hasse para $(A, \leq)$
  - substitua cada elemento a pelo correspondente $f(a)$ em B
  - o resultado é o diagrama de Hasse da ordem parcial $\leq'$ sobre B

- **Exemplo**: Seja $A = \{1, 2, 3, 6\}$ e seja $\leq$ a relação de divisibilidade " | " cujo diagrama de Hasse é dado por:



  - Por outro lado, sejam:
    - $A' = P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}.\{a, b\}\}$
    - $\leq'$ a relação de inclusão de conjuntos $\subseteq$
  - Se $f : A \to A'$ é definida por:
    $f(1) = \emptyset \quad , \quad f(2) = \{a\} \quad , \quad f(3) = \{b\} \quad , \quad f(6) = \{a, b\}$
    é fácil ver que f é uma bijeção.
  - Substituindo cada a por $f(a)$ no diagrama de Hasse, obtemos:



    - que é o diagrama de Hasse de $(A', \leq')$
    - portanto, f é um isomorfismo entre $(A, \leq)$ e $(A', \leq')$ $\square$

Relações de Ordenamento

- Ler Kolman5, item 6.1
- Ler Rosen6, item 8.6

INE5403 - Fundamentos de Matemática Discreta para a Computação

10) Relações de Ordenamento

10.1) Conjuntos Parcialmente Ordenados (Posets)

10.2) Extremos de Posets

10.3) Reticulados

10.4) Álgebras Booleanas Finitas

- Material extraído dos livros-textos (Kolman/Rosen)

Elementos extremos de posets

Def.: Seja o poset $(A,\leq)$. Então:

a) um elem. $a\in A$ é um **elemento maximal** de A se não existe $c\in A$ tal que $a<c$ ($a\leq c$, $a\neq c$)

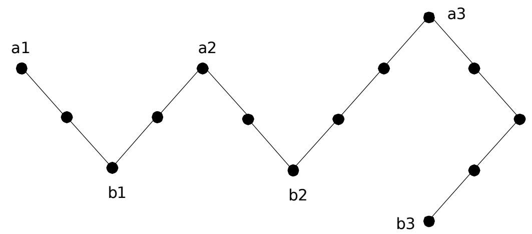
b) um elem. $b\in A$ é um **elemento minimal** de A se não existe $c\in A$ tal que $c<b$ ($c\leq b$, $c\neq b$)

Exemplos:

1. $(\mathbf{Z}^+,\leq)$: elemento minimal: 1, maximal: não tem
2. $(\mathbf{R},\leq)$: minimal: não tem, maximal: não tem
3. $(\{1,2,3,4\},\leq)$: minimal: 1, maximal: 4
4. $(\{1,2,3,4\},\geq)$: minimal: 4, maximal: 1

Elementos extremos de posets

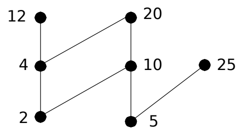
Exemplo: Considere o poset A a seguir:



- a1, a2 e a3 são elementos *maximais* de A
- b1, b2 e b3 são elementos *minimais* de A

Elementos extremos de posets

Exemplo: Quais elementos do poset $(\{2,4,5,10,12,20,25\},|)$ são maximais e quais são minimais?



- Elementos maximais: 12, 20 e 25
- Elementos minimais: 2 e 5
- Note que um poset pode ter mais do que um elemento maximal e mais do que um minimal.

Elementos extremos de posets

Teorema: Todo poset finito e não vazio $(A,\leq)$ tem pelo menos um elemento maximal e ao menos um elemento minimal.

Prova:

- Seja $a\in A$. Se a já não é maximal, então pode-se achar $a_1\in A$ com $a<a_1$
- Se a_1 não é maximal, pode-se achar $a_2\in A$ com $a_1<a_2$
- Este argumento não pode ser continuado indefinidamente, pois A é finito.
- Assim, eventualmente será formada a cadeia:
  $a < a_1 < a_2 < a_3 < \ldots < a_{k-1} < a_k$
- Não é possível encontrar mais algum $b\in A$ tal que $a_k<b$
- Logo, a_k é um elemento maximal de $(A,\leq)$

Ordenação topológica de posets

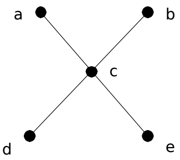
- Com o conceito de elementos minimais, pode-se estabelecer um *algoritmo* para encontrar uma ordenação topológica de um dado poset finito $(A,\leq)$.
- O algoritmo abaixo produz um vetor chamado *SORT* que satisfaz: SORT[1] < SORT[2] < ...
- A relação < sobre A definida desta forma é uma *ordenação topológica* de $(A,\leq)$.

Algoritmo SORT:

1) $I \leftarrow 1$
2) $S \leftarrow A$
3) Enquanto $S \neq \emptyset$
   - 3.1) Escolha um elemento minimal a do conjunto S
   - 3.2) $SORT[I] \leftarrow a$
   - 3.3) $I \leftarrow I+1$
   - 3.4) $S \leftarrow S - \{a\}$

Algoritmo para ordenação topológica de posets

<u>Exemplo</u>: Seja A={a,b,c,d,e} e seja o diagrama de Hasse de ≤ sobre A dado por:

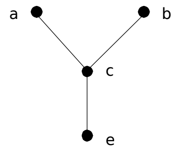


SORT				

Algoritmo para ordenação topológica de posets

<u>Exemplo (cont.)</u>: Seja A={a,b,c,d,e} e seja o diagrama de Hasse de ≤ sobre A dado por:

Passo 1:

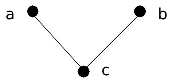


SORT				
d				

Algoritmo para ordenação topológica de posets

<u>Exemplo (cont.)</u>: Seja A={a,b,c,d,e} e seja o diagrama de Hasse de ≤ sobre A dado por:

Passo 2:



SORT				
d	e			

Algoritmo para ordenação topológica de posets

<u>Exemplo (cont.)</u>: Seja A={a,b,c,d,e} e seja o diagrama de Hasse de ≤ sobre A dado por:

Passo 3:

SORT				
d	e	c		

Algoritmo para ordenação topológica de posets

<u>Exemplo (cont.)</u>: Seja A={a,b,c,d,e} e seja o diagrama de Hasse de ≤ sobre A dado por:

Passo 4:

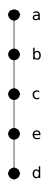
SORT				
d	e	c	b	

Algoritmo para ordenação topológica de posets

<u>Exemplo (cont.)</u>: Seja A={a,b,c,d,e} e seja o diagrama de Hasse de ≤ sobre A dado por:

Passo 5:

SORT				
d	e	c	b	a



Elementos extremos de posets

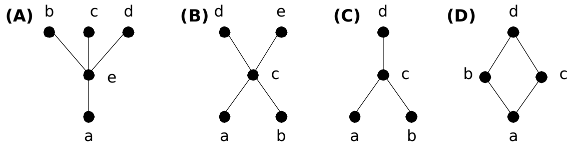
Def.: Seja o poset $(A,\leq)$. Então:

1) Um elemento $a \in A$ é chamado de um **maior elemento** de A se $b \leq a$ <u>para todo</u> $b \in A$

2) Um elemento $a \in A$ é chamado de um **menor elemento** de A se $a \leq b$ <u>para todo</u> $b \in A$.

Elementos extremos de posets

<u>Exemplo</u>:



(A): menor elemento é a, não tem maior elemento
(B): não tem menor nem maior elemento
(C): não tem menor elemento, maior elemento é d
(D): menor elemento é a, maior elemento é d

Elementos extremos em posets

<u>Exemplo</u>: Seja A um conjunto e seja o poset $(P(A),\subseteq)$.

- O menor elemento é o conjunto vazio, pois $\emptyset \subseteq T$ para qualquer subconjunto T de A
- O próprio A é o maior elemento deste poset, pois $T \subseteq A$ para todo subconjunto T de A

Elementos extremos em posets

<u>Exemplo</u>: Há um maior e um menor elementos em $(\mathbf{Z}^+,|)$?

- o inteiro 1 é o menor elemento, pois $1|n$ para todo n
- não há maior elemento, pois não existe inteiro que seja divisível por todos os inteiros positivos

Elementos extremos em posets

Def.: Sejam um poset $(A,\leq)$ e um ***subconjunto*** $B \subseteq A$. Então:

a) um elemento $a \in A$ é uma **cota superior** de B, se:

$b \leq a$, para todo $b \in B$

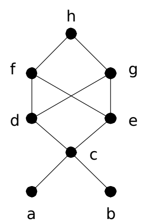
b) um elemento $a \in A$ éuma **cota inferior** de B, se:

$a \leq b$, para todo $b \in B$.

Elementos extremos em posets

<u>Exemplo</u>: Seja o poset com o diagrama de Hasse abaixo. Ache todas as cotas superiores e inferiores dos seguintes subconjuntos de A:

a) $B_1 = \{a,b\}$ b) $B_2 = \{c,d,e\}$

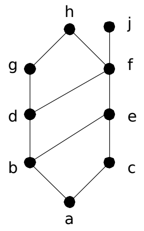


- B_1 não tem cotas inferiores
- suas cotas superiores são: c,d,e,f,g,h

- cotas superiores de B_2 : f,g,h
- suas cotas inferiores: c,a,b

Elementos extremos em posets

Exercício: Encontre as cotas superiores e inferiores dos subconjuntos {a,b,c},{j,h} e {a,c,d,f} no poset cujo diagrama de Hasse é dado por:



- cotas superiores de {a,b,c}: e,f,j,h
- única cota inferior: a

- não há cotas superiores de {j,h}
- suas cotas inferiores são: a,b,c,d,e,f

- cotas superiores de {a,c,d,f}: f,h,j
- sua cota inferior é: a

Elementos extremos em posets

Observações:

- Note que um subconjunto B de um poset pode ou não ter cotas inferiores ou superiores (em A)
- Além isto, uma cota superior ou inferior de B pode ou não pertencer ao próprio B.

Menor cota superior / Maior cota inferior

Def.: Um elemento x é chamado de **Supremo** de um subconjunto A se x é uma cota superior menor do que qualquer outra cota superior de A.

- ou seja, x será a menor cota superior de A se:

  $a \leq x \quad \forall a \in A$ e
  $x \leq z \quad \forall z$ que seja cota superior de A

Def.: Um elemento y é chamado de **Ínfimo** de um subconjunto A se:

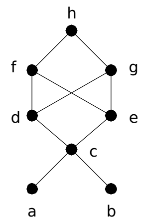
y é uma cota inferior de A e

$z \leq y \quad \forall z$ que seja uma cota inferior de A

Menor cota superior / Maior cota inferior

Exemplo: Para o poset com o diagrama de Hasse abaixo, ache os ínfimos e supremos de:

a) B_1 = {a,b} b) B_2 = {c,d,e}

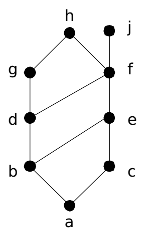


- Como B_1 não tem cotas inferiores, também não terá ínfimo
- $sup(B_1) = c$

- Como as cotas inferiores de B_2 são c,a,b, temos que $inf(B_2) = c$
- As cotas superiores de B_2 são f,g,h
- como f não é comparável com g, concluímos que B_2 não tem sup

Menor cota superior / Maior cota inferior

Exemplo: Encontre o supremo e o ínfimo de {b,d,g}, se existirem, no poset:



- cotas superiores de {b,d,g}: g,h
- como g<h, g é o supremo

- cotas inferiores de {b,d,g}: a,b
- como a<b, b é a maior cota inferior (inf)

Menor cota superior / Maior cota inferior

Exemplo: Encontre supremo e ínfimo de {3,9,12} e {1,2,4,5,10}, se existirem, no poset ($\mathbf{Z}^+$,|).

- Ínfimos:
  - um inteiro é cota inferior de {3,9,12} se 3,9, e 12 forem divisíveis por este inteiro
    → os únicos inteiros deste tipo são 1 e 3
    → então, como 1|3, 3 é o ínfimo de {3,9,12}
  - a única cota inferior do conjunto {1,2,4,5,10} é o 1
    → portanto, 1 é o ínfimo para {1,2,4,5,10}

Menor cota superior / Maior cota inferior

Exemplo: Encontre supremo e ínfimo de {3,9,12} e {1,2,4,5,10}, se existirem, no poset ($\mathbf{Z}^+$,|).

- Supremos:
  - um inteiro é uma cota superior de {3,9,12} sse for divisível por 3, 9 e 12
    → inteiros com esta propriedade: os divisíveis pelo mmc de 3, 9 e 12, que é 36
    → então, 36 é o supremo de {3,9,12}
  - um inteiro é uma cota superior para {1,2,4,5,10} sse for divisível por 1,2,4,5,10
    → inteiros com esta propriedade: os divisíveis pelo mmc de 1,2,4,5,10, que é 20.
    → então, 20 é o supremo de {1,2,4,5,10}

Elementos extremos de posets

Teorema: Seja (A,≤) um poset. Então um subconjunto B qualquer de A tem no máx um supremo e um ínfimo

Extremos de Posets

- Ler Kolman5: seção 6.2
- Ler Rosen 6: seção 8.6

INE5403 - Fundamentos de Matemática Discreta para a Computação

10) Relações de Ordenamento

10.1) Conjuntos Parcialmente Ordenados (Posets)

10.2) Extremos de Posets

10.3) Reticulados

10.4) Álgebras Booleanas Finitas

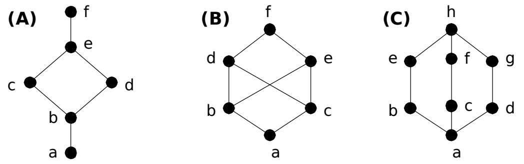
- Material extraído dos livros-textos (Kolman/Rosen)

Reticulados (*lattices*)

Def.: Um poset $(L,\leq)$ é chamado de *reticulado* se *todo* par de elementos $\{a,b\}$ possui tanto uma menor cota superior como uma maior cota inferior.

- Reticulados possuem muitas propriedades especiais.
- São usados em muitas aplicações diferentes tais como modelos de fluxo de informação.
- Eles também têm um papel importante em álgebra booleana.
- Observação: denota-se $\sup(\{a,b\})$ por $a\vee b$ (operação de *junção*) e denota-se $\text{ínf}(\{a,b\})$ por $a\wedge b$ (operação de *encontro*).

Exemplo: Determine se os posets representados por cada um dos diagramas de Hasse abaixo são reticulados.



- Os posets (A) e (C) são reticulados, pois cada par de elementos tem tanto um sup como um inf.
- Já o poset (B) não é um reticulado, pois os elementos b e c não possuem menor cota superior → note que d, e, f são cotas superiores, mas nenhum destes 3 elementos precede os outros 2 com respeito ao ordenamento deste poset.

Reticulados (*lattices*)

Exemplo: Determine se $(P(S),\subseteq)$ é um reticulado, onde S é um conjunto.

- Sejam A e B dois subconjuntos de S. Então:
  - O sup (junção) de A e B é a sua união $A\cup B$ e
  - O inf (encontro) de A e B é a sua intersecção $A\cap B$
  - logo, $(P(S),\subseteq)$ é um reticulado.

Exemplo: Considere o poset $(\mathbf{Z}^+,\leq)$, onde $a \leq b$ se e somente se $a|b$. Então $(\mathbf{Z}^+,\leq)$ é um reticulado em que as operações de junção e encontro de a e b são, respectivamente:

$$a\vee b = \text{mmc}(a,b) \quad \text{e} \quad a\wedge b = \text{mdc}(a,b)$$

Reticulados (*lattices*)

Exemplo: Determine se os posets $(\{1,2,3,4,5\},|)$ e $(\{1,2,4,8,16\},|)$ são reticulados.

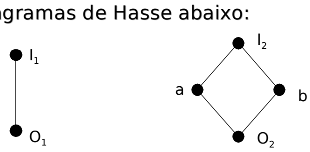
- Solução:
  - Uma vez que 2 e 3 não possuem cotas superiores em $(\{1,2,3,4,5\},|)$, eles certamente não têm uma menor cota superior e *o primeiro poset não é um reticulado*.
  - Cada 2 elementos do segundo poset possuem tanto uma menor cota superior como uma maior cota inferior.
    → sup de 2 elementos neste poset: maior deles
    → inf de 2 elementos neste poset: menor deles
    → logo, *o 2º poset é um reticulado*.

Reticulados (*lattices*)

Teorema: Se $(\mathbf{L}_1,\leq_1)$ e $(\mathbf{L}_2,\leq_2)$ são reticulados, então $(\mathbf{L},\leq_3)$ é um reticulado, onde $L=L_1\times L_2$ e a ordem parcial $\leq_3$ é a *ordem parcial produto* definida por

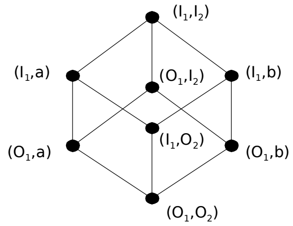
$$(a,b) \leq_3 (a',b'), \quad \text{se} \quad a\leq_1 a' \text{ em } L_1 \quad \text{e} \quad b\leq_2 b' \text{ em } L_2 .$$

- Exemplo: Sejam L_1 e L_2 os reticulados representados pelos diagramas de Hasse abaixo:



Reticulados (*lattices*)

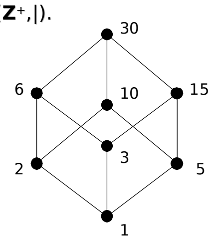
- Exemplo (cont.): Então $\mathbf{L} = \mathbf{L}_1 \times \mathbf{L}_2$ é o reticulado:



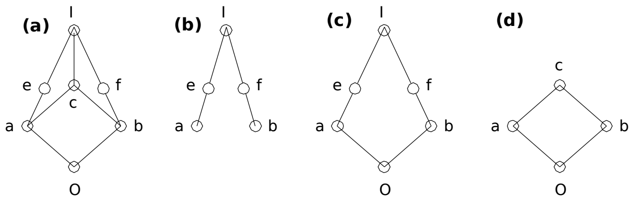
Sub-reticulados (*sublattices*)

Def: Seja $(L,\leq)$ um reticulado. Um subconjunto S de L, $S \subseteq L$, é chamado de um *sub-reticulado* de L se $a \vee b \in S$ e $a \wedge b \in S$ sempre que $a \in S$ e $b \in S$.

Exemplo: Os reticulados $(D_n,|)$, de todos os divisores de n com a relação de divisibilidade, são sub-reticulados do reticulado $(\mathbf{Z}^+,|)$.



- Exemplo: Considere o reticulado L mostrado na fig. (a).



- O subconjunto parcialmente ordenado (b) não é um sub-reticulado de L pois $a \wedge b \notin S_b$ e $a \vee b \notin S_b$.
- O subconjunto parcialmente ordenado (c) não é um sub-reticulado de L pois $a \vee b = c \notin S_b$
  - entretanto, S_c é um reticulado por si mesmo.
- O subconjunto parcialmente ordenado (d) é um sub-reticulado de L.

Propriedades de reticulados

- Relembrando os significados de $a \vee b$ e $a \wedge b$:

1) $a \leq a \vee b$ e $b \leq a \vee b$ ($a \vee b$ é uma cota superior de a e de b)

2) se $a \leq c$ e $b \leq c$, então $a \vee b \leq c$ ($a \vee b$ é a *menor* das cotas superiores de a e de b);

- Analogamente:

1') $a \wedge b \leq a$ e $a \wedge b \leq b$ ($a \wedge b$ é uma cota inferior de a e de b)

2')se $c \leq a$ e $c \leq b$, então $c \leq a \wedge b$ ($a \wedge b$ é a *maior* das cotas inferiores de a e de b).

Propriedades de reticulados

Teorema: Seja L um reticulado. Então, para todo a e b em L:

a) $a \vee b = b \Leftrightarrow a \leq b$

b) $a \wedge b = a \Leftrightarrow a \leq b$

c) $a \wedge b = a \Leftrightarrow a \vee b = b$

Prova (a):

($\rightarrow$) suponha que $a \vee b = b$. Como $a \vee b$ é o sup({a,b}), tem-se que $a \leq a \vee b = b$

($\leftarrow$) como $a \leq b$, temos que b é uma cota superior de {a,b} e, pela definição de sup, temos que $a \vee b \leq b$
- mas como também $a \vee b$ é uma cota superior de {a,b}, temos que $b \leq a \vee b$ e portanto $a \vee b = b$.

Propriedades de reticulados

Teorema: Seja L um reticulado. Então, para todo a e b em L:

a) $a \vee b = b \Leftrightarrow a \leq b$

b) $a \wedge b = a \Leftrightarrow a \leq b$

c) $a \wedge b = a \Leftrightarrow a \vee b = b$

Prova (b):

($\rightarrow$) suponha que $a \wedge b = a$. Como $a \wedge b$ é o inf({a,b}), tem-se que $a = a \wedge b \leq b$;

($\leftarrow$) como $a \leq b$, temos que a é uma cota inferior de {a,b} e, pela definição de inf, temos que $a \leq a \wedge b$
- mas como também $a \wedge b$ é uma cota inferior de {a,b}, temos que $a \wedge b \leq a$ e portanto $a \wedge b = a$.

Propriedades de reticulados

Teorema: Seja L um reticulado. Então, para todo a e b em L:

a) $a \vee b = b \Leftrightarrow a \leq b$

b) $a \wedge b = a \Leftrightarrow a \leq b$

c) $a \wedge b = a \Leftrightarrow a \vee b = b$

Prova (c):

- De (a) temos que: $a \vee b = b \Leftrightarrow a \leq b$,
- mas, por (b): $a \leq b \Leftrightarrow a \wedge b = a$,
- portanto:

$$a \wedge b = a \Leftrightarrow a \vee b = b$$

Propriedades de reticulados

Teorema: Seja L um reticulado. Então:

a) $a \vee a = a$ b) $a \wedge a = a$	Idempotência
a) $a \vee b = b \vee a$ b) $a \wedge b = b \wedge a$	Comutatividade
a) $a \vee (b \vee c) = (a \vee b) \vee c$ b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$	Associatividade
a) $a \vee (a \wedge b) = a$ b) $a \wedge (a \vee b) = a$	Absorção

Propriedades de reticulados

Teorema: Seja L um reticulado. Então para todo $a,b,c \in L$:

1. Se $a \leq b$, então
   a) $a \vee c \leq b \vee c$
   b) $a \wedge c \leq b \wedge c$
2. $a \leq c$ e $b \leq c \Leftrightarrow a \vee b \leq c$
3. $c \leq a$ e $c \leq b \Leftrightarrow c \leq a \wedge b$
4. Se $a \leq b$ e $c \leq d$, então
   a) $a \vee c \leq b \vee d$
   b) $a \wedge c \leq b \wedge d$

Tipos especiais de reticulados

Def.: Um reticulado L é dito limitado se L tem um maior elemento **I** e um menor elemento **O**.

<u>Exemplos</u>:

- $\mathbf{Z}^+$, sob a ordem parcial de divisibilidade, tem um menor elemento mas não tem um maior elemento ⇒ não limitado.
- **Z**, sob a ordem parcial "menor ou igual a" não tem nem maior nem menor elemento ⇒ não limitado.
- O reticulado $(2^S, \subseteq)$, de todos os subconjuntos de um conjunto finito S, é limitado:
  I=S e **O**={ }

Tipos especiais de reticulados

- <u>Nota</u>: Se L é um reticulado limitado, então, $\forall a \in L$:

a) $\mathbf{O} \leq a \leq \mathbf{I}$

b) $a \vee \mathbf{O} = a$

c) $a \wedge \mathbf{O} = \mathbf{O}$

d) $a \vee \mathbf{I} = \mathbf{I}$

e) $a \wedge \mathbf{I} = a$

Teorema: Seja $L=\{a_1,a_2,a_3,\ldots,a_n\}$ um reticulado finito. Então L é limitado.

- <u>Prova</u>:
  O maior elemento de L é $a_1 \vee a_2 \vee a_3 \vee \ldots \vee a_n$
  O menor elemento de L é $a_1 \wedge a_2 \wedge a_3 \wedge \ldots \wedge a_n$

Tipos especiais de reticulados

Def.: Um reticulado é chamado distributivo se, para quaisquer elementos $a,b,c \in L$, valem as seguintes regras:

a) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

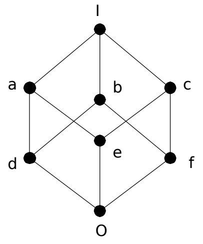
b) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

<u>Nota</u>: As leis distributivas valem quando quaisquer 2 dos elementos a, b, ou c são iguais, ou quando qualquer 1 dos elementos é **O** ou **I**.

- Esta observação reduz o número de casos que devem ser verificados na determinação da distributividade de um reticulado.
- Entretanto, a verificação da distributividade é geralmente trabalhosa.

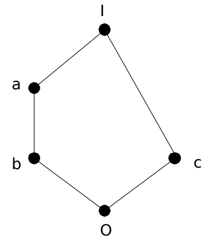
Reticulados distributivos

- Exemplo: O reticulado mostrado abaixo é distributivo:
  - a lei de distributividade vale para todos os trios ordenados escolhidos entre os elementos a,b,c,d,e,f.

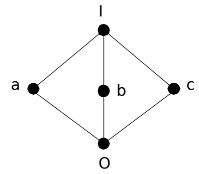


Reticulados distributivos

- Exemplo: Mostre que os reticulados mostrados abaixo não são distributivos:



(a)



(b)

Reticulados distributivos

- Exemplo (cont.): Mostre que os reticulados não são distributivos:
- Reticulado (a):
  - Temos: $a \wedge (b \vee c) = a \wedge \mathbf{I} = a$
  - enquanto: $(a \wedge b) \vee (a \wedge c) = b \vee \mathbf{O} = b$
- Reticulado (b):
  - Observe que: $a \wedge (b \vee c) = a \wedge \mathbf{I} = a$
  - enquanto: $(a \wedge b) \vee (a \wedge c) = \mathbf{O} \vee \mathbf{O} = \mathbf{O}$

Teorema: Um reticulado L é não-distributivo se e somente se contiver um sub-reticulado que seja isomórfico a um dos 2 reticulados do exemplo anterior.

Tipos especiais de reticulados

Def.: Seja L um reticulado limitado com maior elemento **I** e menor elemento **O**, e seja $a \in L$. Um elemento $a' \in L$ é chamado de um complemento de a se:

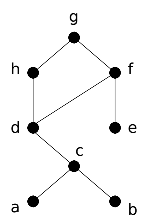
$a \vee a' = \mathbf{I}$ e $a \wedge a' = \mathbf{O}$.

- Observe que $\mathbf{O}' = \mathbf{I}$ e $\mathbf{I}' = \mathbf{O}$.
- Exemplo: O reticulado $(2^S, \subseteq)$ é tal que todo elemento tem um complemento, pois se $A \in 2^S$, então o seu complementar tem as propriedades:

  $A \vee A' = S\ (=\mathbf{I})$ e $A \wedge A' = \{\ \}\ (=\mathbf{O})$
  - ele também é distributivo, pois as operações de união e intersecção satisfazem às leis de distributividade para reticulados.

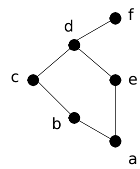
Reticulados (*lattices*)

- Exercício: Determine se o diagrama de Hasse abaixo representa um reticulado.



Reticulados (*lattices*)

- Exercício: Determine se o poset A={2,3,6,12,24,36,72}, sob a relação de divisibilidade (|), representa um reticulado.
- Exercício: Determine se o reticulado abaixo é distributivo e também se os seus elementos possuem complementos.



Reticulados

- Ler Kolman5: seção 6.3
- Ler Rosen6: seção 8.6

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

10) Relações de ordenamento

10.4) Álgebras Booleanas Finitas

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds, 5^{th} ed., 2003.*

Reticulados $(P(S), \subseteq)$

- Vamos restringir nossa atenção aos reticulados do tipo $(P(S), \subseteq)$, onde S é um conjunto finito.
  - Muitas propriedades que não valem para reticulados em geral.
  - Por isto, são mais fáceis de trabalhar
  - Têm papel importante em muitas aplicações na Ciência da Computação:
    - construção de representações lógicas para os circuitos do computador
    - estudo de cifradores simétricos, na Criptografia

- **Teorema**: Sejam $S_1 = \{x_1, x_2 ..., x_n\}$ e $S_2 = \{y_1, y_2 ..., y_n\}$ dois conjuntos finitos quaisquer com n elementos.
  - Então os reticulados $(P(S_1), \subseteq)$ e $(P(S_2), \subseteq)$ são isomórficos
    - ou seja, seus diagramas de Hasse são idênticos

Prova: arranjar os conjuntos e definir a seguinte f:

$$\begin{array}{ll} S_1: & x_1 \; x_2 \ldots x_n \\ & \updownarrow \;\; \updownarrow \quad\; \updownarrow \\ S_2: & y_1 \; y_2 \ldots y_n \end{array} \qquad\qquad \begin{array}{ll} S_1: & x_1 \; \overbrace{x_2 \; x_3 \; x_4}^{\text{subconj. } A} \ldots x_n \\ & \\ S_2: & y_1 \; \underbrace{y_2 \; y_3 \; y_4}_{\text{subconj. } f(A)} \ldots y_n \end{array}$$

$f(A)$: elementos de S_2 que correspondem aos elementos de A

- f: bijeção de subconjuntos de S_1 para subconjuntos de S_2
- além disto, se A e B são subconjuntos quaisquer de S_1:

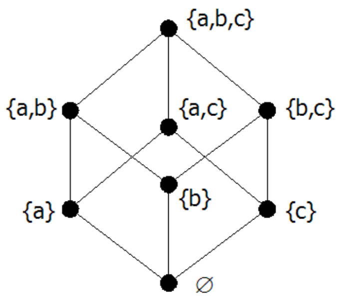
$$A \subseteq B \quad \Leftrightarrow \quad f(A) \subseteq f(B)$$

- Logo, os reticulados $(P(S_1), \subseteq)$ e $(P(S_2), \subseteq)$ são isomórficos. $\square$

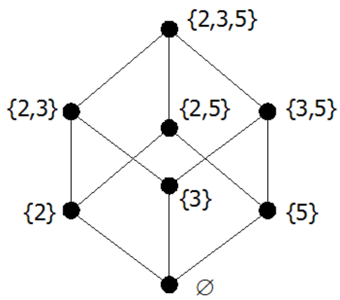
- A condição de poset do reticulado $(P(S), \subseteq)$ é determinada pelo número $|S|$ e não depende da natureza dos elementos de S.

- **Exemplo**: Sejam os posets:

$(P(S), \subseteq)$, $S = \{a, b, c\}$:

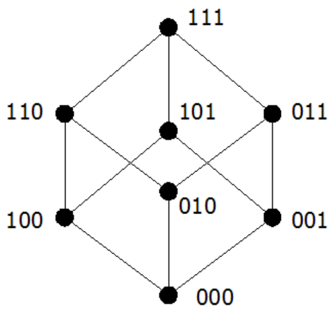


$(P(T), \subseteq)$, $T = \{2, 3, 5\}$:



- Note que os 2 reticulados são isomórficos.
- Para cada $n = 0, 1, 2, \ldots$, há apenas <u>um tipo</u> de reticulado com a forma $(P(S), \subseteq)$
  - o qual depende apenas de n (e não de S)
  - e tem 2^n elementos (= nro de possíveis subconjuntos de S).

- Pode-se, portanto, tomar um diagrama de Hasse genérico para $(P(S), \subseteq)$ e rotulá-lo assim:



- Desta forma, este diagrama serve para descrever <u>os 2 reticulados anteriores</u>.
  - E para descrever um reticulado $(P(S), \subseteq)$ originado de qualquer conjunto S com 3 elementos.

- Se o diagrama de Hasse do reticulado correspondente a um conjunto com n elementos é rotulado desta forma (sequências de 0s e 1s de comprimento n), o reticulado resultante é chamado de B_n.

Propriedades do ordenamento parcial em B_n

- Sejam 2 elementos de B_n: $x = a_1 a_2 \ldots a_n$ e $y = b_1 b_2 \ldots b_n$.
- Então:
  - $x \leq y$ se e somente se $a_k \leq b_k$ para $k = 1, 2, \ldots, n$
  - $x \wedge y = c_1 c_2 \ldots c_n$, onde $c_k = min\{a_k, b_k\}$
  - $x \vee y = d_1 d_2 \ldots d_n$, onde $d_k = max\{a_k, b_k\}$
  - o complemento de x é dado por $x' = z_1 z_2 \ldots z_n$, onde:

$$\begin{cases} z_k = 1 & \text{se } x_k = 0 \\ z_k = 0 & \text{se } x_k = 1 \end{cases}$$

- Estas afirmações podem ser confirmadas pela observação de que $(B_n, \leq)$ é isomórfico a $(P(S), \subseteq)$:
  - $x, y \in B_n$ correspondem a subconjuntos A e B de S
  - então:

    $x \leq y$ corresponde a $A \subseteq B$
    $x \wedge y$ corresponde a $A \cap B$
    $x \vee y$ corresponde a $A \cup B$
    x' corresponde a $\overline{A}$

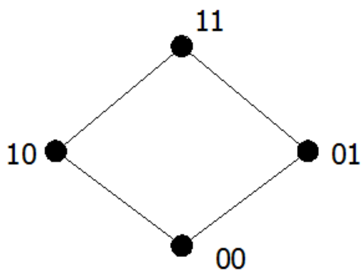
Reticulados B_n

- Diagramas de Hasse dos reticulados B_0, B_1, B_2 e B_3:

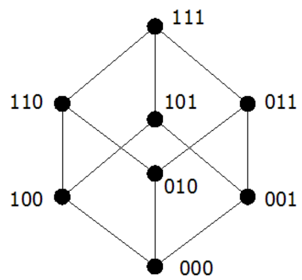
n=0: •

n=1:

n=2:



n=3:

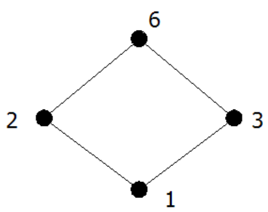


- Todo reticulado $(P(S), \subseteq)$ é isomórfico a B_n, onde $n = \mid S \mid$.

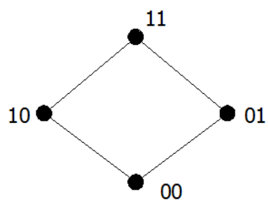
- Outros reticulados também podem ser isomórficos com algum B_n.
  - Possuindo todas as propriedades especiais que o B_n possui.

- **Exemplo**: D_6 (divisores de 6, ordem parcial de divisibilidade).
  - Isomorfismo $f : D_6 \rightarrow B_2$ dado por:

    $f(1) = 00 \qquad f(2) = 10 \qquad f(3) = 01 \qquad f(6) = 11$

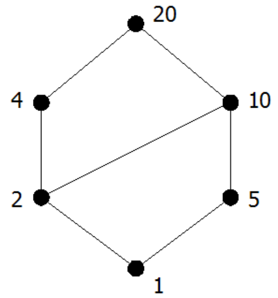


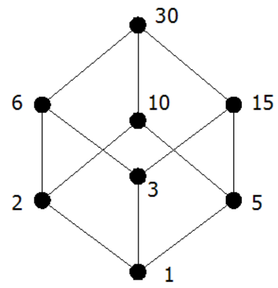
$\rightarrow$



- Em geral: um reticulado finito é chamado de **Álgebra Booleana** se for isomórfico a algum B_n.
- Portanto, todo B_n é uma Álgebra Booleana
  - assim como todo reticulado $(P(S), \subseteq)$.

- **Exemplo**: reticulados D_{20} e D_{30} (divisores de 20 e 30, ordem parcial de divisibilidade):





D_{20} tem 6 elementos:

  * $6 \neq 2^n$
  * D_{20} não é uma Álgebra Booleana

Já o poset D_{30} tem 8 elementos:

  * $8 = 2^3 \quad \Rightarrow$ chance de ser Álgebra Booleana
  * Note que D_{30} é isómórfico com B_3
    - com isomorfismo $f : D_{30} \to B_3$ dado por:

$$\begin{array}{llll} f(1) = 000 & f(2) = 100 & f(3) = 010 & f(5) = 001 \\ f(6) = 110 & f(10) = 101 & f(15) = 011 & f(30) = 111 \end{array}$$

  * Portanto, D_{30} é uma Álgebra Booleana. $\square$

- Conclusão:
  - Se um reticulado L não contém 2^n elementos, ele não pode ser uma Álgebra Booleana.
  - Se $\mid L \mid = 2^n$, então L pode ou não ser uma Álgebra Booleana.
  - Se L for pequeno, pode-se tentar comparar o seu diagrama de Hasse com o de B_n
    * Mas esta técnica pode não ser prática se L for grande
      - Aí tenta-se construir diretamente um isomorfismo com B_n ou com $(P(S), \subseteq)$

Álgebras Booleanas grandes

- Para ver se um dado reticulado D_n (n grande) é Álgebra Booleana:
- **Teorema**: Seja $n = p_1 p_2 \dots p_k$ onde os p_i são primos distintos. Então D_n é uma Álgebra booleana.

  Prova:
  - Seja $S = \{p_1, p_2, \dots, p_k\}$.
  - Todo divisor de n deve ser da forma a_T, onde:
    * a_T é o produto dos primos em algum subconjunto T de S (nota: $a_\emptyset = 1$)
  - Aí, se V e T são subconjuntos de S:

- * $V \subseteq T$ se e somente se $a_V \mid a_T$
  * $a_{V \cap T} = a_V \wedge a_T$ $(= MDC(a_V, a_T))$
  * $a_{V \cup T} = a_V \vee a_T$ $(= MMC(a_V, a_T))$

- Logo, $f : P(S) \to D_n$, dada por $f(T) = a_T$, é um isomorfismo de $P(S)$ para D_n
- Então, como $(P(S), \subseteq)$ é uma Álgebra Booleana, D_n também o é. $\square$

- **Exemplo**:

  $210 = 2.3.5.7 \Rightarrow D_{210}$ é Álgebra Booleana
  $66 = 2.3.11 \Rightarrow D_{66}$ é Álgebra Booleana
  $646 = 2.17.19 \Rightarrow D_{646}$ é Álgebra Booleana

- Para outros casos de reticulados L grandes:
  - Tentar mostrar que L não é uma Álgebra Booleana
  - Mostrando que o ordenamento parcial de L não apresenta as propriedades necessárias.

- Exemplo: uma Álg. Booleana é sempre isomórfica com algum B_n e, portanto, com algum reticulado $(P(S), \subseteq)$.
  - Logo, se o reticulado L for uma Álgebra Booleana:
    * ele deverá ser limitado (deverá possuir ínfimo e supremo)
    * cada um dos seus elementos deverá possuir um complemento
  - Ou seja, para que L seja reticulado:
    * L deverá ter um maior elemento $\mathbf{I}$ $(\Leftrightarrow S)$ e um menor elemento $\mathbf{O}$ $(\Leftrightarrow \emptyset)$
    * todo elemento x de L deverá ter um complemento x'

Álgebras Booleanas

- O Princípio da Correspondência entre posets ajuda a estabelecer propriedades das Álgebras Booleanas.

- **Teorema** (Regra da Substituição):
  Toda fórmula que envolve $\cup$ e $\cap$, ou que vale para subconjuntos arbitrários de um conjunto S, continuará a valer para elementos arbitrários de uma Álgebra Booleana L se:

  $\cap$ for substituído por $\wedge$

  $\cup$ for substituído por $\vee$

- **Exemplo**: Se x, y e z são elementos de uma Álgebra Booleana qualquer L, valem:

  (a) $(x')' = x$ $\longrightarrow$ involução

  (b) $(x \wedge y)' = x' \vee y'$ $\longrightarrow$ 1a. lei de De Morgan

  (c) $(x \vee y)' = x' \wedge y'$ $\longrightarrow$ 2a. lei de De Morgan

- Isto vale para Álgebras booleanas, pois sabemos que as fórmulas:

  (a') $\overline{\overline{(A)}} = A$

  (b') $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

  (c') $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$

  – valem para subconjuntos arbitrários A e B de um conjunto S.

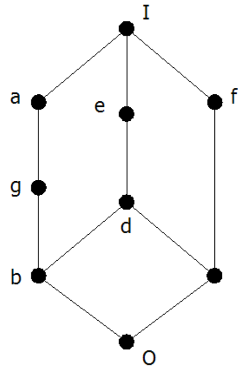
Propriedades das Álgebras Booleanas $(L, \leq)$

- De maneira similar, podemos listar outras propriedades que devem valer em qualquer Álgebra Booleana em consequência da regra de substituição.
- Nas tabelas a seguir:
  - x, y e z são elementos arbitrários em L
  - A, B e C são subconjuntos arbitrários de S
  - **I** e **O** denotam o maior e o menor elemento de L, respectivamente.

Algumas propriedades básicas de uma Álgebra Booleana $(L, \leq)$	Propriedade correspondente para subconjuntos de um conjunto S
1) $x \leq y$ se e somente se $x \vee y = y$	1') $A \subseteq B$ se e somente se $A \cup B = B$
2) $x \leq y$ se e somente se $x \wedge y = x$	2') $A \subseteq B$ se e somente se $A \cap B = A$
3) (a) $x \vee x = x$ (b) $x \wedge x = x$	3') (a) $A \cup A = A$ (b) $A \cap A = A$
4) (a) $x \vee y = y \vee x$ (b) $x \wedge y = y \wedge x$	4') (a) $A \cup B = B \cup A$ (b) $A \cap B = B \cap A$
5) (a) $x \vee (y \vee z) = (x \vee y) \vee z$ (b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$	5') (a) $A \cup (B \cup C) = (A \cup B) \cup C$ (b) $A \cap (B \cap C) = (A \cap B) \cap C$
6) (a) $x \vee (x \wedge y) = x$ (b) $x \wedge (x \vee y) = x$	6') (a) $A \cup (A \cap B) = A$ (b) $A \cap (A \cup B) = A$
7) $\mathbf{O} \leq x \leq \mathbf{I}, \quad \forall x \in L$	7') $\emptyset \subseteq A \subseteq S, \quad \forall A \in P(S)$
8) (a) $x \vee \mathbf{O} = x$ (b) $x \wedge \mathbf{O} = \mathbf{O}$	8') (a) $A \cup \emptyset = A$ (b) $A \cap \emptyset = \emptyset$
9) (a) $x \vee \mathbf{I} = \mathbf{I}$ (b) $x \wedge \mathbf{I} = x$	9') (a) $A \cup S = S$ (b) $A \cap S = A$
10) (a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ (b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	10') (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
11) Todo elemento x tem um único (a) $x \vee x' = \mathbf{I}$ (b) $x \wedge x' = \mathbf{O}$	11') Todo elemento A tem um único (a) $A \cup \overline{A} = S$ (b) $A \cap \overline{A} = \emptyset$
12) (a) $\mathbf{O}' = \mathbf{I}$ (b) $\mathbf{I}' = \mathbf{O}$	12') (a) $\overline{\emptyset} = S$ (b) $\overline{S} = \emptyset$
13) $(x')' = x$	13') $\overline{\overline{A}} = A$
14) (a) $(x \wedge y)' = x' \vee y'$ (b) $(x \vee y)' = x' \wedge y'$	14') (a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (b) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

- Talvez seja possível mostrar que um reticulado L não é Álgebra Booleana mostrando que ele não possui alguma propriedade básica.

- **Exemplo**: Mostre que o reticulado abaixo não é Álgebra Booleana:



  - Os elementos a e g são ambos complementos de c
    - ou seja, ambos satisfazem as propriedades 11(a) e 11(b) com respeito ao elemento c.
  - Mas a propriedade estabelece que tal elemento deve ser único em qualquer Álgebra booleana.
  - Logo, o reticulado dado não é uma Álgebra booleana. $\square$

- **Exemplo**: Mostre que se $p^2 \mid n$, onde p é um primo, então D_n não é uma Álgebra Booleana.
  - Suponha que $p^2 \mid n$
    - então $n = p^2.q$
  - Mas p também é divisor de n, de modo que $p \in D_n$
  - Se D_n é uma Álg. Booleana, p deve ter um complemento p'
    - de modo que $MDC(p, p') = 1$ e $MMC(p, p') = n$
    - daí temos que $p.p' = n$
    - de modo que $p' = n/p = p.q$
  - Mas isto significa que $MDC(p, p.q)$ teria que ser 1 (!!)
  - Logo, D_n não pode ser uma Álg. Booleana. $\square$

- Na verdade, de acordo com um teorema já visto,
  - "Seja $n = p_1 p_2 \ldots p_k$ onde os p_i são primos distintos. Então D_n é uma Álgebra booleana".

- Concluímos que:
  - D_n é uma Álgebra Booleana se e somente se nenhum primo divide n mais do que uma vez.

- **Exemplo**: $40 = 2^3.5$ e $125 = 5^3$
  - Então: nem D_{40} nem D_{125} podem ser Álgebras Booleanas.

Álgebras Booleanas

- Ler Kolman5: seção 6.4

11 - ESTRUTURAS ALGÉBRICAS

11.1) OPERAÇÕES BINÁRIAS

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*

ÁLGEBRA ABSTRATA

- Noção familiar: Álgebra Elementar.
  - Exemplo: adição e multiplicação sobre os inteiros.
  - Essência: "operação binária" sobre "um conjunto de elementos".
- Abstração: recurso poderoso.
  - Consiste em isolar a essência do problema.
  - Conexão entre problemas aparentemente não relacionados.
  - Problemas complexos viram simples casos particulares de esquema mais geral.
  - Uma vez identificada a "classe" de um problema, pode-se aproveitar resultados prontos.
- Ponto de vista de modelagem em Ciência da Computação:
  - interessa justamente mais o "esquema geral" do que os detalhes
  - abstração permite focar apenas no que interessa

OPERAÇÕES BINÁRIAS

- Precisamos de uma definição precisa desta idéia familiar.
- **Operação Binária** sobre um conjunto A:
  - função $f : A \times A \to A$
  - definida para todo par ordenado de elementos de A
  - apenas um elemento de A é atribuído a cada par de $A \times A$
- Ou seja: regra que atribui um único elemento de A a cada par ordenado de elementos de A.
- Notação:
  - como se trata de uma função, o normal seria denotar o elemento atribuído a (a, b) por $*(a, b)$
  - mas o usual é $a * b$
- Importante: lembrar que $a * b \in A$
  - também se diz que A é **fechado** sob a operação $*$

- **Exemplo 1:** Seja $A = \mathbb{Z}$.
  - Defina $a * b$ como $a + b$.
  - Então $*$ é uma operação binária sobre $\mathbb{Z}$ $\square$

- **Exemplo 2:** Seja $A = \mathbb{R}$.
  - Defina $a * b$ como a/b.
  - Então $*$ não é uma operação binária
    * pois não é definida para todo par ordenado de $A \times A$
    * por exemplo, $3 * 0$ não é definida $\square$

- **Exemplo 3:** Seja $A = \mathbb{Z}^+$.
  - Defina $a * b$ como $a - b$.
  - Então $*$ não é uma operação binária:
    * não atribui um elemento de A para todo par de $A \times A$
    * por exemplo, $2 * 5 \notin A$ $\square$

- **Exemplo 4:** Seja $A = \mathbb{Z}$.
  - Defina $a * b$ como um número menor do que a e do que b.
  - Então $*$ não é uma operação binária:
    * não atribui um elemento único de A para todo par de $A \times A$
    * por exemplo, $8 * 6$ poderia ser 5, 4, 3, 2, 1, etc.
  - Neste caso, $*$ seria uma relação de $A \times A$ para A
    * mas não uma função $\square$

- **Exemplo 5:** Seja $A = \mathbb{Z}$.
  - Defina $a * b$ como $\max\{a, b\}$.
  - Então $*$ é uma operação binária:
    * $2 * 4 = 4$
    * $-3 * (-5) = -3$ $\square$

- **Exemplo 6:** Seja $A = P(S)$, para algum conjunto S.
  - Sejam V e W dois subconjuntos de S.
  - $V * W$ definida como $V \cup W$ é uma operação binária sobre A.
  - Mas: $V * W$ definida como $V \cap W$ também. $\square$

- Note que é possível definir muitas operações binárias sobre o mesmo conjunto.

- **Exemplo:** Seja M o conjunto de todas as matrizes Booleanas.
  - São operações binárias:
    - $\mathbf{A} * \mathbf{B}$ definido como $\mathbf{A} \vee \mathbf{B}$
    - $\mathbf{A} * \mathbf{B}$ definido como $\mathbf{A} \wedge \mathbf{B}$ $\square$

- **Exemplo:** Seja L um reticulado.
  - São operações binárias sobre L:
    - $a * b$ def. como $a \wedge b$ (supremo ("menor cota sup") de a e b)
    - $a * b$ def. como $a \vee b$ (ínfimo ("maior cota inf") de a e b) $\square$

Operações Binárias & Tabelas

- Pode-se definir uma operação binária sobre um conjunto $A = \{a_1, a_2, \ldots, a_n\}$ por meio de uma tabela:

$*$	a_1	a_2	$\ldots$	a_j	$\ldots$	a_n
a_1						
a_2						
$\ldots$						
a_i				$a_i * a_j$		
$\ldots$						
a_n						

- Elemento na posição i, j denota $a_i * a_j$

- **Exemplo:** Operações $\vee$ e $\wedge$ sobre $A = \{0, 1\}$:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

Número de Operações Binárias

- Seja $A = \{a, b\}$. O número de operações binárias que podem ser definidas sobre A é:
  - Toda operação binária sobre A pode ser descrita pela tabela:

$*$	a	b
a		
b		

  - Como cada espaço vazio pode ser preenchido com a ou b:

    há $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$ modos de completar a tabela
  - Logo, existem 16 operações binárias possíveis sobre A. $\square$

- **Prop1:** Uma operação binária é **comutativa** se:

$$a * b = b * a \qquad \forall a, b \in A$$

- **Exemplo:** $a + b$ sobre $A = \mathbb{Z}$ é comutativa.

- **Exemplo:** $a - b$ sobre $A = \mathbb{Z}$ não é comutativa, pois:

  – $2 - 3 \neq 3 - 2$

- Uma operação binária definida por uma tabela é comutativa se e somente se a tabela é simétrica.

- **Exemplo:** Sejam as operações binárias sobre A:

$*$	a	b	c	d
a	a	c	b	d
b	b	c	b	a
c	c	d	b	c
d	a	a	b	b

$*$	a	b	c	d
a	a	c	b	d
b	c	d	b	a
c	b	b	a	c
d	d	a	c	d

- **Prop2:** Uma operação binária é **associativa** se:

$$a * (b * c) = (a * b) * c \qquad \forall a, b, c \in A$$

- **Exemplo:** $a + b$ sobre $A = \mathbb{Z}$ é associativa.

- **Exemplo:** $a - b$ sobre $A = \mathbb{Z}$ não é associativa, pois:

  – $2 - (3 - 5) \neq (2 - 3) - 5$

- **Exemplo:** Seja L um reticulado. A operação binária definida por $a * b = a \wedge b$ é comutativa e associativa.

  – Também é **idempotente**: $a \wedge a = a$.

  – *"Seja $(A, \leq)$ um reticulado e seja uma operação binária definida por $a * b = a \wedge b$. Então $a * b$ é comutativa, associativa e idempotente sobre A."*

- Uma parte do converso deste exemplo também é verdadeira:

- **Exemplo:**
  - Seja uma operação binária $*$ sobre A que satisfaz:
    - $a = a * a$ (idempotência)
    - $a * b = b * a$ (comutatividade)
    - $a * (b * c) = (a * b) * c$ (associatividade)
  - E seja uma relação $\leq$ sobre A definida por:
    - $a \leq b$ se e somente se $a = a * b$
  - Então, pode-se mostrar que:
    1) $(A, \leq)$ é um poset
    2) $infimo(a, b) = a * b, \quad \forall a, b \in A$

1) Mostrando que $(A, \leq)$ é um poset:

reflexiva: como $a = a * a$, temos que

- $a \leq a, \ \forall a \in A$

antissimétrica: se $a \leq b$ e $b \leq a$, então:

- $a = a * b = b * a = b$

transitiva: se $a \leq b$ e $b \leq c$, então:

- $a = a * b = a * (b * c) = (a * b) * c = a * c$

2) Mostrando que $a * b = a \wedge b$:

- Temos que: $a * b = a * (b * b) = (a * b) * b$
  - de modo que: $a * b \leq b$
  - similarmente: $a * b \leq a$
  - conclusão: $a * b$ é uma cota inferior para a e b
- Agora, se $c \leq a$ e $c \leq b$:
  - $c = c * a$ e $c = c * b$
  - portanto: $c = (c * a) * b = c * (a * b)$
  - de modo que: $c \leq a * b$
  - conclusão: $a * b$ é a maior cota inferior de a e b. $\square$

Leitura sobre Operações Binárias

- Ler Kolman5: seção 9.1

11 - Estruturas Algébricas

11.2) Semigrupos

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*

Semigrupos

- **Semigrupo:** conjunto S + oper. binária associativa definida sobre S.
  - Sistema algébrico simples.
  - Muitas aplicações importantes.
    - Ex.: máquinas de estados finitos
- Denotado por $(S, *)$.
  - Ou simplesmente por S (quando fica claro o que é "$*$").
- Também nos referimos a $a * b$ como o **produto** de a e b.
- $(S, *)$ é chamado de **comutativo** se $*$ é uma operação comutativa.

Exemplos de Semigrupos

- **Exemplo:** $(\mathbb{Z}, +)$ é um semigrupo comutativo.
- **Exemplo:** $(P(S), \cup)$ é um semigrupo comutativo.
- **Exemplo:** $(\mathbb{Z}, -)$ não é um semigrupo
  - pois a subtração não é associativa.
- **Exemplo:** Seja S um conjunto fixo não-vazio.
  - E seja S^S o conjunto de todas as funções $f : S \to S$
  - Então, sejam f e g dois elementos de S^S:
    - definimos $f * g$ como $f \circ g$ (função composta)
  - $*$ é uma operação binária associativa sobre S^S
  - Portanto, $(S^S, *)$ é um semigrupo (não-comutativo). $\square$

- **Exemplo:** Seja $(L, \leq)$ um reticulado.
  - Definição: $a * b = a \vee b$
  - Então, L é um semigrupo. $\square$

- **Exemplo:** Seja $\boldsymbol{A = \{a_1, a_2, \ldots, a_n\}}$.
  - Sejam $\boldsymbol{\alpha}$ e $\boldsymbol{\beta}$ dois elementos de $\boldsymbol{A^*}$.
  - Note que concatenação $(\cdot)$ é uma operação binaria sobre $\boldsymbol{A^*}$.
    - É associativa: se $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ e $\boldsymbol{\gamma}$ são elementos quaisquer de $\boldsymbol{A^*}$:

      $$\boldsymbol{\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma}$$
    - Logo, $\boldsymbol{(A^*, \cdot)}$ é um semigrupo.
      - (É o chamado "semigrupo livre gerado por $\boldsymbol{A}$")

Associatividade em Semigrupos

- Em um semigrupo $\boldsymbol{(S, *)}$ a propriedade associativa pode ser generalizada:

- **Teorema:** O produto dos elementos $\boldsymbol{a_1, a_2, \ldots, a_n}$ $\boldsymbol{(n \geq 3)}$, de um semigrupo, não depende da inserção de parênteses.
  - Ou seja, este produto pode ser escrito como: $\boldsymbol{a_1 * a_2 * \cdots * a_n}$

- **Exemplo:** São iguais os produtos:

$$\boldsymbol{((a_1 * a_2) * a_3) * a_4}$$
$$\boldsymbol{a_1 * (a_2 * (a_3 * a_4))}$$
$$\boldsymbol{(a_1 * (a_2 * a_3)) * a_4}$$

Identidades em Semigrupos

- Um **elemento identidade** de um semigrupo satisfaz a:

$$\boldsymbol{e * a = a * e = a} \quad , \qquad \boldsymbol{\forall a \in S}$$

- **Exemplo1:** O número 0 é uma identidade do semigrupo $\boldsymbol{(\mathbb{Z}, +)}$.

- **Exemplo2:** Seja $\boldsymbol{S = \{x, y, u, v\}}$ e defina $*$ como:

$*$	x	y	u	v
x	x	y	x	y
y	x	y	y	x
u	x	y	u	v
v	x	y	v	u

- **Teorema:** Se um semigrupo $(\boldsymbol{S}, *)$ tem uma identidade, ela é única.

- **Prova:**
  - Suponha que $\boldsymbol{e}$ e $\boldsymbol{e'}$ são identidades em $\boldsymbol{S}$.
  - Como $\boldsymbol{e}$ é uma identidade: $\boldsymbol{e} * \boldsymbol{e'} = \boldsymbol{e'}$
  - Também, como $\boldsymbol{e'}$ é uma identidade: $\boldsymbol{e} * \boldsymbol{e'} = \boldsymbol{e}$
  - Portanto: $\boldsymbol{e} = \boldsymbol{e'}$ $\square$

Monóides

- **Monóide:** semigrupo que tem identidade.

- **Exemplo:** O semigrupo $(\boldsymbol{P}(\boldsymbol{S}), \cup)$ é um monóide.
  - A identidade é o elemento $\emptyset$, pois:

$$\emptyset * \boldsymbol{A} \ = \ \emptyset \cup \boldsymbol{A} \ = \ \boldsymbol{A} \ = \ \boldsymbol{A} \cup \emptyset \ = \ \boldsymbol{A} * \emptyset \quad , \qquad \forall \boldsymbol{A} \in \boldsymbol{P}(\boldsymbol{S})$$

- **Exemplo:** O semigrupo $(\boldsymbol{A}^*, \cdot)$ é um monóide.
  - A identidade é o elemento $\boldsymbol{\Lambda}$, pois:

$$\boldsymbol{\alpha} \cdot \boldsymbol{\Lambda} \ = \ \boldsymbol{\Lambda} \cdot \boldsymbol{\alpha} = \boldsymbol{\alpha} \quad , \qquad \forall \boldsymbol{\alpha} \in \boldsymbol{A}^*$$

- **Exemplo:** O conjunto de todas as relações sobre um conjunto $\boldsymbol{A}$ é um monóide sob a operação de composição.
  - A identidade é a relação de igualdade $\boldsymbol{\Delta}$.

Subsemigrupos & Submonóides

- Sejam $(\boldsymbol{S}, *)$ um semigrupo e $\boldsymbol{T}$ um subconjunto de $\boldsymbol{S}$:
  - $(\boldsymbol{T}, *)$ é um **subsemigrupo** de $(\boldsymbol{S}, *)$ se $\boldsymbol{T}$ for fechado sob $*$
    - (fechado: $\boldsymbol{a} * \boldsymbol{b} \in \boldsymbol{T}$ sempre que $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{T}$)

Similarmente:

- Seja $(\boldsymbol{S}, *)$ um monóide (com identidade $\boldsymbol{e}$) e seja $\boldsymbol{T}$ um subconjunto de $\boldsymbol{S}$.
  - $(\boldsymbol{T}, *)$ é um **submonóide** de $(\boldsymbol{S}, *)$ se $\boldsymbol{T}$ for fechado sob $*$ e se $\boldsymbol{e} \in \boldsymbol{T}$.

- A associatividade vale em qualquer subconjunto de um semigrupo.

- Deste modo, um subsemigrupo $(\boldsymbol{T}, *)$ de um semigrupo $(\boldsymbol{S}, *)$ é por si mesmo um semigrupo.

- Da mesma forma: um submonóide de um monóide é ele próprio um monóide.

- **Exemplo:**
  - Seja $(S, *)$ um semigrupo. Então:
    - $(S, *)$ é um subsemigrupo de $(S, *)$
  - Seja $(S, *)$ um monóide. Então:
    - $(S, *)$ é um submonóide de $(S, *)$
    - $(\{e\}, *)$ também é um submonóide de $(S, *)$

$\square$

- **Exemplo:** Seja T o conjunto de todos os inteiros pares.
  - Então $(T, \times)$ é um subsemigrupo do monóide $(\mathbb{Z}, \times)$.
  - Mas não é um submonóide:
    - a identidade de $\mathbb{Z}$ (o número 1), não pertence a T. $\square$

Potências em semigrupos

- Seja a um elemento de um semigrupo $(S, *)$.
- Para $n \in \mathbb{Z}^+$, definimos recursivamente as potências a^n:

$$a^1 = a \qquad , \qquad a^n = a^{n-1} * a \quad (n \geq 2)$$

- Além disto:
  - se $(S, *)$ é um monóide, definimos: $a^0 = e$
  - se m e n são inteiros não-negativos: $a^m * a^n = a^{m+n}$

- **Exemplo:** Se $(S, *)$ é um semigrupo e:

$$a \in S$$
$$T = \{a^i \mid i \in \mathbb{Z}^+\}$$

  - Então $(T, *)$ é um subsemigrupo de $(S, *)$. $\square$

- **Exemplo:** Se $(S, *)$ é um monóide e:

$$a \in S$$
$$T = \{a^i \mid i \in \mathbb{Z}^+ \text{ ou } i = 0\}$$

  - Então $(T, *)$ é um submonóide de $(S, *)$. $\square$

Leitura sobre Semigrupos

- Ler Kolman5: seção 9.2

11 - Estruturas Algébricas

11.3) Grupos

NOTA: Este material foi elaborado com base nas seguintes referências:

- *Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds,* 5^{th} *ed., 2003.*

Grupos

- Tipo especial de monóide.

- Aplicações aonde ocorre simetria:
  - matemática, física, química...
  - aplicações recentes: física de partículas e cubo de Rubik

- Um grupo $(G, *)$ é um monóide (identidade e) com a seguinte propriedade adicional:

  $$\forall a \in G, \;\; \exists a' \in G \quad \text{tal que} \quad a * a' = a' * a = e$$

- Grupo = conjunto G + operação binária sobre G tal que:

  1) $(a * b) * c = a * (b * c) \;\; \forall a, b, c \in G$

  2) existe um *único* elemento em G tal que:
     $a * e = e * a, \;\; \forall a \in G$

  3) $\forall a \in G, \;\; \exists a' \in G$, chamada de inversa de a tal que:
     $a * a' = a' * a = e$

- Note que $*$ é uma operação binária sobre G, ou seja:

  $a * b \in G, \;\; \forall a, b \in G$

- Para simplificar notação:
  - escreveremos $a * b$ como ab
  - vamos nos referir a $(G, *)$ simplesmente como G

- Um grupo $\boldsymbol{G}$ é dito abeliano se $\boldsymbol{ab = ba, \ \forall a, b \in G}$
- **Exemplo 1:** O conjunto dos inteiros $\mathbb{Z}$, com a operação de adição simples, é um grupo abeliano.
  - Se $\boldsymbol{a} \in \mathbb{Z}$, a inversa de $\boldsymbol{a}$ é o seu negativo $\boldsymbol{-a}$.

- **Exemplo 2:** O conjunto $\mathbb{Z}^+$, sob a operação de multiplicação simples, não é um grupo:
  - o elemento $\mathbf{2}$ em $\mathbb{Z}^+$ não tem inversa
  - no entanto, este conjunto com a operação formam um monóide

- **Exemplo 3:** O conjunto dos reais não nulos, sob a operação de multiplicação simples, é um grupo.
  - A inversa de $\boldsymbol{a \neq 0}$ é $\boldsymbol{1/a}$

- **Exemplo 4:** $\boldsymbol{(G, *)}$, aonde $\boldsymbol{G}$ é o conjunto dos reais não-nulos e $\boldsymbol{a * b = (ab)/2}$ é um grupo abeliano.
  - a operação $*$ é binária:

    $\boldsymbol{a * b \ (= \ ab/2)}$ é um real não-nulo e, portanto, está em $\boldsymbol{G}$
  - a operação $*$ é associativa, pois:

    $\boldsymbol{(a * b) * c = (\frac{ab}{2}) * c = \frac{(ab)c}{4}}$

    $\boldsymbol{a * (b * c) = a * (\frac{bc}{2}) = \frac{a(bc)}{4} = \frac{(ab)c}{4}}$
  - o número $\mathbf{2}$ é a identidade em $\boldsymbol{G}$, pois:

    $\boldsymbol{a * 2 = \frac{(a)(2)}{2} = a = \frac{(2)(a)}{2} = 2 * a}$
  - $\boldsymbol{a \in G}$ tem uma inversa dada por $\boldsymbol{a' = 4/a}$, pois:

    $\boldsymbol{a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)(a)}{2} = \frac{4}{a} * a = a' * a}$
  - $\boldsymbol{G}$ é um grupo abeliano: $\boldsymbol{\forall a, b \in G, \quad a * b = b * a}$ $\square$

Propriedades dos Grupos

- **Teorema 1:** Todo elemento $\boldsymbol{a}$ em um grupo $\boldsymbol{G}$ tem apenas uma inversa em $\boldsymbol{G}$.

  Prova:
  - Sejam $\boldsymbol{a'}$ e $\boldsymbol{a''}$ ambas inversas de $\boldsymbol{a}$
  - então: $\boldsymbol{a'(aa'') = a'e = a'}$

    e: $\boldsymbol{(a'a)a'' = ea'' = a''}$
  - portanto, por associatividade: $\boldsymbol{a' = a''}$ $\square$

- Denotaremos a inversa de $\boldsymbol{a}$ por $\boldsymbol{a^{-1}}$: $\boldsymbol{aa^{-1} = a^{-1}a = e}$

- **Teorema 2:** Sejam $\boldsymbol{a}, \boldsymbol{b}$ e $\boldsymbol{c}$ elementos de um grupo $\boldsymbol{G}$. Então:

  (a) $\boldsymbol{ab = ac \quad \Rightarrow \quad b = c}$ (cancelamento à esquerda)

  (b) $\boldsymbol{ba = ca \quad \Rightarrow \quad b = c}$ (cancelamento à direita)

  Prova de (a):

  – Suponha que: $\boldsymbol{ab = ac}$

  – Multiplicando os dois lados à esquerda por $\boldsymbol{a^{-1}}$:

  $$\boldsymbol{a^{-1}(ab) = a^{-1}(ac)}$$

  $$\boldsymbol{(a^{-1}a)b = (a^{-1}a)c} \quad \text{(por associatividade)}$$

  $$\boldsymbol{eb = ec} \quad \text{(pela definição de inversa)}$$

  $$\boldsymbol{b = c} \quad \text{(pela definição de identidade)} \qquad \square$$

  Prova de (b): similar.

- **Teorema 3:** Sejam $\boldsymbol{a}$ e $\boldsymbol{b}$ elementos de um grupo $\boldsymbol{G}$. Então:

  (a) $\boldsymbol{(a^{-1})^{-1} = a}$

  (b) $\boldsymbol{(ab)^{-1} = b^{-1}a^{-1}}$

  Prova de (a):

  – Temos: $\boldsymbol{aa^{-1} = a^{-1}a = e}$

  – Como a inversa é única, concluímos que: $\boldsymbol{(a^{-1})^{-1} = a}$.

  Prova de (b):

  – Temos que: $\boldsymbol{(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) =}$

  $$\boldsymbol{= a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e}$$

  – e também: $\boldsymbol{(b^{-1}a^{-1})(ab) = e}$

  – de modo que: $\boldsymbol{(ab)^{-1} = b^{-1}a^{-1}}$ $\square$

- **Teorema 4:** Sejam $\boldsymbol{a}$ e $\boldsymbol{b}$ elementos de um grupo $\boldsymbol{G}$. Então:

  (a) A equação $\boldsymbol{ax = b}$ tem uma solução única em $\boldsymbol{G}$

  (b) A equação $\boldsymbol{ya = b}$ tem uma solução única em $\boldsymbol{G}$

  Prova de (a):

  – O elemento $\boldsymbol{x = a^{-1}b}$ é uma solução da equação, pois:

  $$\boldsymbol{a(a^{-1}b) = (aa^{-1})b = eb = b}$$

  – Agora suponha que existam duas soluções: $\boldsymbol{x_1}$ e $\boldsymbol{x_2}$.

    * então: $\boldsymbol{ax_1 = b}$ e $\boldsymbol{ax_2 = b}$
    * logo: $\boldsymbol{x_1 = x_2}$ $\square$

  Prova de (b): Similar.

Representação em tabelas

- Se um grupo $\boldsymbol{G}$ tem um nro finito de elementos, então a sua operação binária pode ser dada por uma tabela.

- E esta tabela deve satisfazer às propriedades:
  * linha e coluna rotuladas por $\boldsymbol{e}$ devem conter todos os elementos
  * pelo Teor 4: cada elemento do grupo deve aparecer exatamente uma vez em cada linha e coluna da tabela
    · portanto, cada linha/coluna é uma permutação dos elementos de $\boldsymbol{G}$
    · e é uma permutação diferente.

- **Nota**: se $\boldsymbol{G}$ é um grupo com um número finito de elementos:
  * $\boldsymbol{G}$ é denominado um grupo finito
  * A <u>ordem</u> de $\boldsymbol{G}$ é o número de elementos $|\boldsymbol{G}|$ em $\boldsymbol{G}$

- Vamos agora determinar as tabelas de multiplicação de todos os grupos de ordens 1, 2, 3 e 4...

- Ordem 1: $\boldsymbol{G = \{e\}}$
  * $\boldsymbol{ee = e}$

- Ordem 2: $\boldsymbol{G = \{e, a\}}$
  * tabela de multiplicação:

	e	a
e	e	a
a	a	?

  * o espaço em branco pode ser preenchido por $\boldsymbol{e}$ ou por $\boldsymbol{a}$:
    · então, como não pode haver repetições:

	e	a
e	e	a
a	a	e

(satisfaz propriedades de grupo)

- Ordem 3: $\boldsymbol{G = \{e, a, b\}}$
  * tabela de multiplicação:

	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

  * experimentando um pouco:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

  * pode-se provar que esta tabela possui as propriedades de grupo (associatividade dá trabalho)

- Observe que:
  - os grupos de ordem 1, 2 e 3 são abelianos
  - existe apenas um grupo de cada ordem para uma dada rotulagem dos elementos

- Ordem 4: $\boldsymbol{G = \{e, a, b, c\}}$
  - tabela de multiplicação pode ser completada de 4 modos:

	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
e	e	a	b	c	e	a	b	c	e	a	b	c	e	a	b	c
a	a	e	c	b	a	e	c	b	a	b	c	e	a	c	e	b
b	b	c	e	a	b	c	a	e	b	c	e	a	b	e	c	a
c	c	b	a	e	c	b	e	a	c	e	a	b	c	b	a	e

  - pode-se provar que cada uma destas tabelas possui as propriedades de grupo
  - observe que um grupo de ordem 4 é abeliano
  - veremos que, na verdade, existem apenas 2 (e não 4) grupos diferentes de ordem 4...

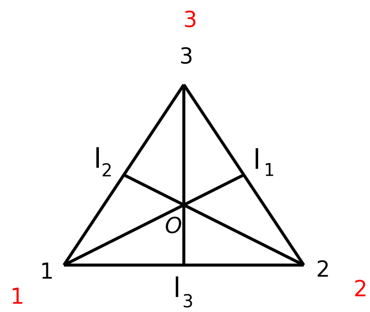
Exemplos de grupos

- **Exemplo 1:** Seja a operação $+$ sobre $\boldsymbol{B = \{0, 1\}}$ definida como:

+	0	1
0	0	1
1	1	0

  - $\boldsymbol{B}$ é um grupo.
  - Neste grupo, cada elemento é a sua própria inversa.

- **Exemplo 2:** Considere o seguinte triângulo equilátero:



  - **Nota:** Uma **simetria** de uma figura geométrica é uma bijeção do conjunto dos pontos que formam a figura para ele mesmo, preservando a distância entre pontos adjacentes.
  - Simetria de um triângulo: permutação dos vértices.

- Simetrias básicas do triângulo equilátero:
  - ($\boldsymbol{l_1}$, $\boldsymbol{l_2}$ e $\boldsymbol{l_3}$ são bissectores angulares dos respectivos ângulos)
  - (O é o seu ponto de intersecção)
  - (**1**, **2** e **3** são referências fixas)

1) rotação anti-horária de 120^o em torno de $\boldsymbol{O}$, dada pela permutação: $\boldsymbol{f_2} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} \end{pmatrix}$

2) rotação anti-horária de 240^o, dada pela permutação: $\boldsymbol{f_3} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{1} & \mathbf{2} \end{pmatrix}$

3) rotação anti-horária de 360^o, dada pela permutação: $\boldsymbol{f_1} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{2} & \mathbf{3} \end{pmatrix}$

$*$ ou: rotação de 0^o em torno de $\boldsymbol{O}$

- Também existem 3 simetrias adicionais:
  - Resultados da reflexão sobre $\boldsymbol{l_1}$, $\boldsymbol{l_2}$ e $\boldsymbol{l_3}$, respectivamente:

$$\boldsymbol{g_1} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{3} & \mathbf{2} \end{pmatrix} \quad \boldsymbol{g_2} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{2} & \mathbf{1} \end{pmatrix} \quad \boldsymbol{g_3} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{2} & \mathbf{1} & \mathbf{3} \end{pmatrix}$$

- Observe que o conjunto de todas as simetrias do triângulo é igual ao conjunto $\boldsymbol{S_3}$ das permutações do conjunto $\mathbf{\{1, 2, 3\}}$:

$$\mathbf{\{\{1, 2, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{1, 3, 2\}, \{3, 2, 1\}, \{2, 1, 3\}\}}$$

- Portanto: $\boldsymbol{S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}}$

$$\mathbf{= \{\{1, 2, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{1, 3, 2\}, \{3, 2, 1\}, \{2, 1, 3\}\}}$$

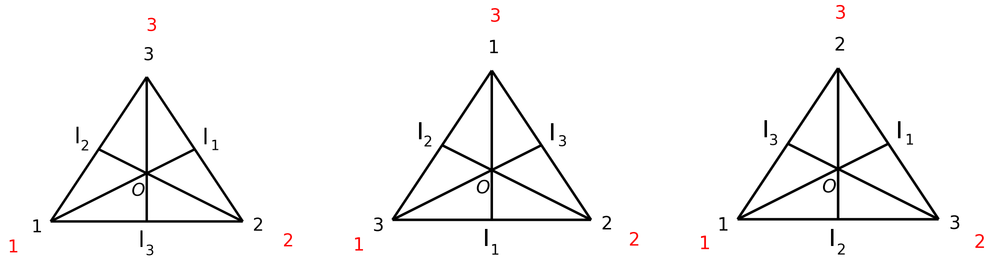
- Agora seja a operação de composição $*$ sobre $\boldsymbol{S_3}$:

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

- A operação $*$ pode ser algébrica ou geométrica.
  - Computando $\boldsymbol{f_2 * g_2}$ algebricamente $(* = \circ)$:

$$\boldsymbol{f_2 \circ g_2} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{2} & \mathbf{3} & \mathbf{1} \end{pmatrix} \circ \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{2} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{3} & \mathbf{2} \end{pmatrix} = \boldsymbol{g_1}$$

– Computando $f_2 * g_2$ geometricamente:

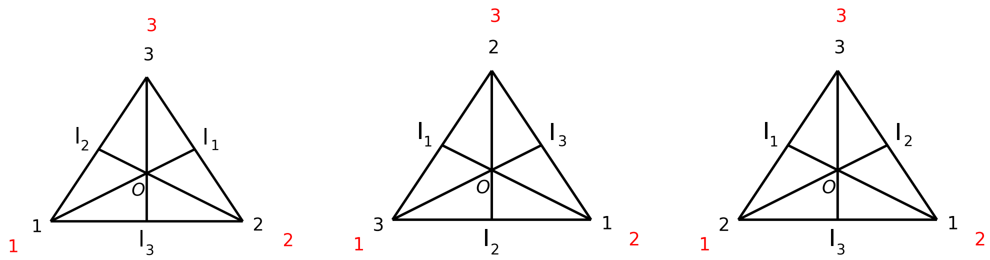


inicial   após g_2 após $f_2 * g_2$

– Computando $g_2 * f_2$ algebricamente $(* = \circ)$:

$$g_2 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = g_3$$

– Computando $g_2 * f_2$ geometricamente:



inicial   após f_2 após $g_2 * f_2$

- **Exemplo:** O conjunto de todas as permutações de n elementos sob a operação de composição:
  - grupo de ordem $n!$
  - denominado de **grupo simétrico sobre n letras**
  - denotado por S_n
  - S_3 coincide com o grupo de simetrias do triângulo equilátero

- **Nota**: também faz sentido considerar o grupo de simetrias de um quadrado.
  - Só que este grupo tem ordem 8.
  - Não coincide, portanto, com S_4, cuja ordem é $\mathbf{4! = 24}$

- **Exemplo:** O monóide $\mathbb{Z}_n$ (seção anterior) também é um grupo:
  - falta só provar que todo elemento de $\mathbb{Z}_n$ tem inversa:
    * seja $[a] \in \mathbb{Z}_n$
    * note que: $[n - a] \in \mathbb{Z}_n$
    * note também que: $[a] \oplus [n - a] = [a + n - a] = [n] = [0]$
    * ou seja: todo $[a]$ tem uma inversa dada por $[n - a]$
  - ex.: em $\mathbb{Z}_6$, $[2]$ é a inversa de $[4]$ $\square$

- Em seguida: subconjuntos de grupos que são importantes...

Subgrupos

- Seja $\boldsymbol{H}$ um subconjunto de um grupo $\boldsymbol{G}$ tal que:

  (a) a identidade $\boldsymbol{e}$ de $\boldsymbol{G}$ pertence a $\boldsymbol{H}$

  (b) se $\boldsymbol{a}$ e $\boldsymbol{b}$ pertencem a $\boldsymbol{H}$, então $\boldsymbol{ab} \in \boldsymbol{H}$

  (c) se $\boldsymbol{a} \in \boldsymbol{H}$, então $\boldsymbol{a^{-1}} \in \boldsymbol{H}$

  Então $\boldsymbol{H}$ é chamado de subgrupo de $\boldsymbol{G}$.

- **Nota 1**: subgrupo = subsemigrupo + (a) + (c)

- **Nota 2**: $\boldsymbol{H}$ também é um *grupo* com relação à operação de $\boldsymbol{G}$, pois a associatividade de $\boldsymbol{G}$ também vale em $\boldsymbol{H}$

Exemplos de subgrupos

- **Exemplo:** $\boldsymbol{G}$ e $\boldsymbol{\{e\}}$ são subgrupos triviais de um grupo $\boldsymbol{G}$

- **Exemplo:** Seja $\boldsymbol{S_3}$ (simetrias do triângulo equilátero), junto com a tabela de multiplicação dada.

  $\boldsymbol{H = \{f_1, f_2, f_3\}}$ é um subgrupo de $\boldsymbol{S_3}$ (confira!)

- **Exemplo:** Seja $\boldsymbol{G}$ um grupo e seja $\boldsymbol{a} \in \boldsymbol{G}$:
  - Como um grupo já é um monóide, já foi definido:

    $\boldsymbol{a^n} = \boldsymbol{aa \cdots a}$ ($\boldsymbol{n}$ fatores)

    aonde: $\boldsymbol{a^0 = e}$
  - Agora vamos definir:

    $\boldsymbol{a^{-n}} = \boldsymbol{a^{-1}a^{-1} \cdots a^{-1}}$ ($\boldsymbol{n}$ fatores)
  - Segue que, $\forall \boldsymbol{n, m} \in \mathbb{Z}$:

    $\boldsymbol{a^n a^m = a^{n+m}}$
  - Com isto, é fácil mostrar que é um subgrupo de $\boldsymbol{G}$:

    $\boldsymbol{H} = \{\boldsymbol{a^i} \mid \boldsymbol{i} \in \mathbb{Z}\}$ $\square$

Leitura sobre Grupos

- Ler Kolman5: seção 9.4

Universidade Federal de Santa Catarina
Centro Tecnológico
Depto de Informática e Estatística
INE5403-Fundamentos de Matemática Discreta para a Computação

12) Teoria de Números

12.1) Noções elementares (divisibilidade, fatoração, primos)

NOTA: Este material foi elaborado com base nas seguintes referências:

- Cormen, Leiserson, Rivest, Stein, Introduction to Algorithms, 2^{nd} ed., MIT Press, 2001.
- Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds, 5^{th} ed., 2003.
- Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.

Teoria de Números

- Teoria de Números já foi vista como "inútil" (?!!)
- Porém: base para esquemas criptográficos baseados em primos
  - exequibilidade destes esquemas depende da produção de primos grandes
  - sua segurança depende da nossa incapacidade de fatorar o produto de primos grandes
- Veremos parte da Teoria de Números e dos algoritmos associados a estas aplicações

Tamanho do input X Custo

- Vamos lidar com nros muito grandes
- Neste caso, "input grande" = "inteiro grande"
  - e não: "muitos inteiros" (cf. ordenamento)
- Daí: tamanho de input = # bits para representá-lo
- Um algoritmo com inputs inteiros $\boldsymbol{a_1, a_2, \ldots, a_k}$ é "de tempo polinomial" se:
  - roda em tempo polinomial em $\boldsymbol{log\ a_1, log\ a_2, \ldots, log\ a_k}$
  - ou seja: polinomial nos comprimentos dos inputs

Divisibilidade

- Inteiro divisível por outro: noção central na TN
- Dizemos que d divide a (ou $d|a$) se existe um inteiro k tal que $a = kd$
- Observações úteis:
  - Todo inteiro divide 0
  - Se $a > 0$ e $d|a$, então $|d| \leq |a|$
  - Se $d|a$: a é um múltiplo de d e d é um divisor de a
    - se d não divide a, escrevemos: $d \nmid a$

- Temos que $d|a$ se e somente se $-d|a$
  * não se perde generalidade por definir "divisores" como > 0
  * assim, se d é um divisor de um inteiro não-nulo a: $1 \leq d \leq |a|$
  * ex.: os divisores de 24 são $\{1, 2, 3, 4, 6, 8, 12, 24\}$
- Todo inteiro é divisível pelos divisores triviais 1 e a
- Divisores não triviais de a são também chamados de fatores de a
  * ex.: os fatores de 20 são $2, 4, 5$ e 10

Números Primos

- Primo: inteiro $a > 1$ cujos únicos divisores são os triviais 1 e a
  - $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, \ldots$
  - Muitas propriedades especiais
  - Papel crucial em TN: servem de "blocos" para a construção de qualquer inteiro
- Um inteiro $a > 1$ que não é primo é chamado de número composto
  - Ex.: 39 é composto pois $3|39$
- O 1 é chamado de unidade e não é primo nem composto
  - assim como o 0 e todos os inteiros negativos

- **Teorema1:** Existem infinitos números primos.

  Prova: Exercício.

O Teorema da Divisão

- Dado um inteiro $\boldsymbol{n}$, o conjunto $\mathbb{Z}$ pode ser particionado em:
  - os que são múltiplos de $\boldsymbol{n}$
  - os que não são
- Boa parte da Teoria de Números é baseada em um refinamento desta partição:
  - classificar os não-múltiplos de $\boldsymbol{n}$ de acordo com seus restos quando divididos por $\boldsymbol{n}$
- Teorema a seguir é a base para este refinamento...

- **Teorema2:** Para todo inteiro $\boldsymbol{a}$ e para todo inteiro positivo $\boldsymbol{n}$, existem inteiros únicos $\boldsymbol{q}$ e $\boldsymbol{r}$ tais que:

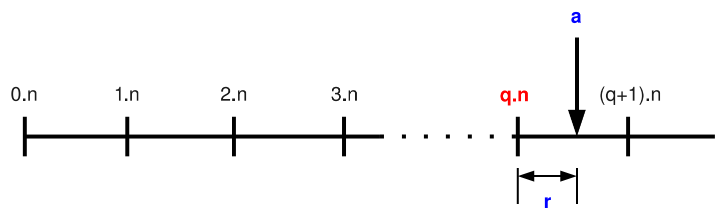
  $$\boldsymbol{0 \leq r < n} \quad \text{e} \quad \boldsymbol{a = qn + r}$$

  $\boldsymbol{q = \lfloor a/n \rfloor}$ é o quociente da divisão

  $\boldsymbol{r = a \; mod \; n}$ é o resto (ou resíduo) da divisão

  Prova: (ver *Niven & Zuckerman*)

- Note que: $\boldsymbol{n|a}$ se e somente se $\boldsymbol{a \ mod \ n = 0}$
- (Ilustração) Seja $\boldsymbol{qn}$ o 1ro múltiplo de $\boldsymbol{n}$ à esquerda de $\boldsymbol{a}$:



- Note que: $\boldsymbol{a \ mod \ n = a - \lfloor a/n \rfloor n}$

DIVISORES COMUNS

- Se $\boldsymbol{d}$ é um divisor de $\boldsymbol{a}$ **e** de $\boldsymbol{b}$, então $\boldsymbol{d}$ é um divisor comum de $\boldsymbol{a}$ e $\boldsymbol{b}$
- Exemplo:
  - divisores de **24**: $\boldsymbol{\{1, 2, 3, 4, 6, 8, 12, 24\}}$
  - divisores de **30**: $\boldsymbol{\{1, 2, 3, 5, 6, 10, 15, 30\}}$
  - divisores comuns de **24** e **30**: $\boldsymbol{\{1, 2, 3, 6\}}$
- Note que o **1** é um divisor comum de quaisquer dois inteiros

- Propriedade importante dos divisores comuns:

  Se $\boldsymbol{d|a}$ e $\boldsymbol{d|b}$, então $\boldsymbol{d|(a+b)}$

  - Exemplo: $\boldsymbol{7|14}$ e $\boldsymbol{7|21}$, então $\boldsymbol{7|35}$

  Prova:

  - Se $\boldsymbol{d|a}$ e $\boldsymbol{d|b}$, existem inteiros $\boldsymbol{k}$ e $\boldsymbol{m}$, tais que: $\boldsymbol{a = k.d}$ e $\boldsymbol{b = m.d}$
  - Portanto: $\boldsymbol{a + b = k.d + m.d = (k + m).d}$
  - Logo, $\boldsymbol{d|(a+b)}$ $\square$

- Esta propriedade pode ser generalizada para: Se $\boldsymbol{d|a}$ e $\boldsymbol{d|b}$, então $\boldsymbol{d|(ax+by)}$
  - para quaisquer inteiros $\boldsymbol{x}$ e $\boldsymbol{y}$

- Além disto, se $\boldsymbol{a|b}$ então:
  - ou $\boldsymbol{|a| \le |b|}$ ou $\boldsymbol{b = 0}$
  - logo: $\boldsymbol{a|b}$ e $\boldsymbol{b|a}$ implica que $\boldsymbol{a = \pm b}$

- Máximo Divisor Comum de dois inteiros $\boldsymbol{a}$ e $\boldsymbol{b}$:
  - *maior dos divisores comuns* de $\boldsymbol{a}$ e $\boldsymbol{b}$
  - denotado por: $\boldsymbol{mdc(a,b)}$
- Exemplos:

$$\boldsymbol{mdc(24,30)} = \text{máx}\boldsymbol{\{1,2,3,6\} = 6}$$
$$\boldsymbol{mdc(5,7) = 1}$$
$$\boldsymbol{mdc(0,9) = 9}$$

- Se tanto $\boldsymbol{a}$ como $\boldsymbol{b}$ forem não-nulos: $\boldsymbol{1 \leq mdc(a,b) \leq min(|a|,|b|)}$
- Definimos: $\boldsymbol{mdc(0,0) = 0}$
- Propriedades elementares da função mdc:

$$\boldsymbol{mdc(a,b) = mdc(b,a)}$$
$$\boldsymbol{mdc(a,b) = mdc(-a,b)}$$
$$\boldsymbol{mdc(a,b) = mdc(|a|,|b|)}$$
$$\boldsymbol{mdc(a,0) = |a|}$$
$$\boldsymbol{mdc(a,ka) = |a|}, \quad \forall \boldsymbol{k} \in \mathbb{Z}$$

- **Teorema3:** Se $\boldsymbol{a}$ e $\boldsymbol{b}$ são inteiros quaisquer, (um não nulo), então:

  $\boldsymbol{mdc(a,b)}$ é o menor elemento *positivo* do conjunto: $\boldsymbol{\{ax + by : x, y \in \mathbb{Z}\}}$

  Prova:

  - Seja $\boldsymbol{s}$ o menor inteiro positivo que pode ser escrito como $\boldsymbol{ax + by}$
  - Agora considere a divisão $\boldsymbol{a/s}$:
    - sabemos que: $\boldsymbol{a = qs + r}$, para $\boldsymbol{0 \leq r < s}$
    - de modo que: $\boldsymbol{r = a - qs = a - q(ax + by) \;=\; a.(1 - qx) + b.(-qy)}$
    - ou seja, $\boldsymbol{r}$ é *também uma combinação linear de* $\boldsymbol{a}$ *e* $\boldsymbol{b}$
  - Isto indica que $\boldsymbol{r}$ *deve ser zero*, pois:
    - $\boldsymbol{0 \leq r < s}$ e $\boldsymbol{s}$ já é a *menor* combinação deste tipo que é positiva
  - Logo, $\boldsymbol{s|a}$ e, por raciocínio análogo, $\boldsymbol{s|b}$
    - ou seja, $\boldsymbol{s}$ é <u>um</u> *divisor comum* de $\boldsymbol{a}$ e de $\boldsymbol{b}$
  - Por outro lado, seja $\boldsymbol{d}$ um divisor comum de $\boldsymbol{a}$ e de $\boldsymbol{b}$:
    - já que $\boldsymbol{d}$ divide tanto $\boldsymbol{a}$ como $\boldsymbol{b}$, $\boldsymbol{d|s}$
    - de modo que: $\boldsymbol{d \leq s}$
    - ou seja, qualquer *outro* divisor comum de $\boldsymbol{a}$ e $\boldsymbol{b}$ divide $\boldsymbol{s}$
  - Logo: $\boldsymbol{s}$ é o maior divisor comum de $\boldsymbol{a}$ e de $\boldsymbol{b}$ $\square$

- Em resumo: se $\boldsymbol{s}$ é o $\boldsymbol{mdc(a,b)}$, então:

  $\boldsymbol{s = a.x + b.y}$, para alguns inteiros $\boldsymbol{x}$ e $\boldsymbol{y}$

  se $\boldsymbol{d}$ é qualquer outro divisor de $\boldsymbol{a}$ e $\boldsymbol{b}$, então $\boldsymbol{d|s}$ (Corolário1 $\rightarrow$)

- Exemplos:

  $\boldsymbol{mdc(12,30) = (-2) \times 12 + (1) \times 30}$

  $\boldsymbol{mdc(17,95) = (28) \times 17 + (-5) \times 95}$

- **Corolário1:** $\boldsymbol{\forall a, b \in \mathbb{Z}}$, se $\boldsymbol{d|a}$ e $\boldsymbol{d|b}$ então $\boldsymbol{d|mdc(a,b)}$

  Prova:

  - Já vimos que $\boldsymbol{d|a}$ e $\boldsymbol{d|b}$ implica que $\boldsymbol{d|(ax+by)}$
    - ($\boldsymbol{d}$ divide qualquer combinação linear de $\boldsymbol{a}$ e $\boldsymbol{b}$)
  - Pelo Teorema: $\boldsymbol{mdc(a,b)}$ é uma combinação linear de $\boldsymbol{a}$ e $\boldsymbol{b}$ $\square$

- Exemplo: $\boldsymbol{mdc(24,36) = max\{1,2,3,4,6,12\}}$

- **Corolário2:** $\boldsymbol{\forall a, b \in \mathbb{Z}}$ e para todo inteiro não-negativo $\boldsymbol{n}$: $\boldsymbol{mdc(a.n, b.n) = n.mdc(a,b)}$

  Prova:

  - Se $\boldsymbol{n = 0}$: trivial
  - Se $\boldsymbol{n > 0}$:
    - $\boldsymbol{mdc(a.n, b.n)}$ é o menor elemento positivo do conjunto:

      $\boldsymbol{\{a.n.x + b.n.y\}}$
    - o qual é $\boldsymbol{n}$ vezes o menor elemento positivo do conjunto:

      $\boldsymbol{\{a.x + b.y\}}$ $\square$

- **Corolário3:** $\boldsymbol{\forall n, a, b \in \mathbb{Z}^+}$, se $\boldsymbol{n|ab}$ e $\boldsymbol{mdc(a,n) = 1}$, então $\boldsymbol{n|b}$

  Prova: $\boldsymbol{mdc(a,n) = 1 \quad \Rightarrow \quad ax + ny = 1 \quad \Rightarrow \quad abx + nby = b}$

  - Então, como $\boldsymbol{n|ab}$, temos que $\boldsymbol{n|b}$ $\square$

Primos Entre Si

- 2 inteiros $\boldsymbol{a}$ e $\boldsymbol{b}$ são primos entre si se o seu *único divisor comum* é $\mathbf{1}$
  - ou seja, se: $\boldsymbol{mdc(a,b) = 1}$
- Exemplo: $\mathbf{8}$ e $\mathbf{15}$ são primos entre si, pois:
  - os divisores de $\mathbf{8}$ são: $\boldsymbol{\{1,2,4,8\}}$
  - os divisores de $\mathbf{15}$ são: $\boldsymbol{\{1,3,5,15\}}$

- **Teorema4:** $\forall a, b, p \in \mathbb{Z}$,
  - se tanto $mdc(a, p) = 1$ como $mdc(b, p) = 1$,
  - então: $mdc(ab, p) = 1$ (também)

  Prova:
  - Pelo Teorema3, sabemos que existem inteiros x, y, x', y' tais que:
    $ax + py = 1$ e $bx' + py' = 1$
  - Multiplicando estas duas equações e rearranjando, temos:
    $ab(xx') + p(ybx' + y'ax + pyy') = 1$
  - Ou seja, 1 é uma combinação linear de ab e p
  - Portanto, pelo Teor3: $mdc(ab, p) = 1$ □

- Inteiros $n_1, n_2, \ldots, n_k$ são Primos Entre Si aos Pares se:

  $mdc(n_i, n_j) = 1$ sempre que $i \neq j$

- Exemplo: $\{10, 17, 21\}$ são primos entre si aos pares e $\{10, 19, 22\}$ não são

Fatoração Única

- **Teorema5:** Para todo primo p e $\forall a, b \in \mathbb{Z}$:

  se $p|ab$, então: $p|a$ ou $p|b$ (ou ambos)

  Prova: (por contradição)
  - assuma que $p|ab$, mas que $p \nmid a$ e $p \nmid b$
  - então: $mdc(a, p) = 1$ e $mdc(b, p) = 1$
    - (únicos divisores de p são 1 e p)
    - (p não divide a e nem b)
  - daí, o Teor4 implica que: $mdc(ab, p) = 1$
  - mas: $p|ab \Rightarrow mdc(ab, p) = p$ (contradição) □

- **Teorema6 (Teor. Fundamental da Aritmética):** Um inteiro composto a *pode* ser escrito de exatamente *uma maneira* como um produto da forma:

  $$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

  - os p_i's são primos tais que $p_1 < p_2 < \cdots < p_r$
  - os e_i's são inteiros positivos
  - note que $p_i \neq 1$ (1 não é primo)

- Exemplo: $6000 = 2^4 \cdot 3 \cdot 5^3$

- **Teor6:** Um inteiro composto $\boldsymbol{a}$ *pode* ser escrito de exatamente *uma maneira* como um produto da forma: $\boldsymbol{a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}}$

  Prova:

  - Suponha que $\exists$ inteiros que não podem ser escritos como produto de primos
  - Então deve existir um nro $\boldsymbol{n}$ que é o menor destes ("bom-ordenamento")
    - $\boldsymbol{n \neq 1}$, em virtude da "regra do produto vazio"
    - $\boldsymbol{n}$ não pode ser primo também, pois aí teríamos $\boldsymbol{n = p_1}$
  - Então $\boldsymbol{n}$ deve ser composto, ou seja, $\boldsymbol{n = ab}$
    - aonde tanto $\boldsymbol{a}$ como $\boldsymbol{b}$ são inteiros $\boldsymbol{< n}$
    - os quais *podem* ser escritos como um produto de primos (pois são $\boldsymbol{< n}$)
  - Mas então: $\boldsymbol{n(= ab)}$ também pode ser escrito como um produto de primos
    - Contradição. $\square$

  Prova de Unicidade:

  - Seja $\boldsymbol{s}$ o menor inteiro positivo que pode ser escrito como (pelo menos) dois produtos diferentes de primos: $\boldsymbol{s = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n}$
  - Pelo Teorema5: ou $\boldsymbol{p_1 | q_1}$ ou $\boldsymbol{p_1 | (q_2 \cdots q_n)}$
  - Mas tanto $\boldsymbol{q_1}$ como $\boldsymbol{(q_2 \cdots q_n)}$ devem possuir fatorações únicas em primos (ambos são $\boldsymbol{< s}$)
    - de modo que: $\boldsymbol{p_1 = q_j}$ para algum $\boldsymbol{j}$
  - Logo, podemos remover $\boldsymbol{p_1}$ e $\boldsymbol{q_j}$ da igualdade inicial
    - chegando a um inteiro $\boldsymbol{< s}$ que pode ser fatorado de duas maneiras (contradição!)
  - Portanto, um $\boldsymbol{s}$ assim não pode existir
    - ou seja: todos os inteiros positivos possuem fatoração única em primos $\square$

- **Teor7:** Dado um nro $\boldsymbol{n}$ e sua fatoração em primos $\boldsymbol{n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}}$, o nro de divisores positivos de $\boldsymbol{n}$ é dado por:

  $$\boldsymbol{(1 + e_1) \times (1 + e_2) \times \ldots \times (1 + e_r)}$$

  Prova: Todo divisor de $\boldsymbol{n}$ é da forma: $\boxed{\boldsymbol{p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}}}$, com: $\boldsymbol{0 \leq \beta_i \leq e_i}$

  - Com isto, temos: $\boldsymbol{1 + e_1}$ escolhas para $\boldsymbol{\beta_1}$,
    $\boldsymbol{1 + e_2}$ escolhas para $\boldsymbol{\beta_2}$,
    $\vdots$
    $\boldsymbol{1 + e_r}$ escolhas para $\boldsymbol{\beta_r}$.
  - Ao todo, são $\boldsymbol{(1 + e_1)(1 + e_2) \ldots (1 + e_r)}$ escolhas para os $\boldsymbol{\beta}$'s
  - Finalmente, note que <u>cada escolha define um divisor</u> $\square$

- **Exemplo:** Determine a quantidade de divisores de $\boldsymbol{n = 15}$
  - Note que: $\boldsymbol{n = 3^1 \times 5^1}$
  - Então, pelo Teor7, o nro **15** possui $\boldsymbol{(1 + 1) \times (1 + 1) = 4}$ divisores
  - De fato, os divisores de **15** são: $\boldsymbol{3^0 \times 5^0,\ 3^1 \times 5^0,\ 3^0 \times 5^1,\ 3^1 \times 5^1}$

12) Teoria de Números

12.2) MDCs e algoritmos de Euclides

NOTA: Este material foi elaborado com base nas seguintes referências:

- Cormen, Leiserson, Rivest, Stein, Introduction to Algorithms, 2^{nd} ed., MIT Press, 2001.
- Kolman, Busby, Ross, "Discrete Mathematical Structures", Prentice-Hall Intl. Eds, 5^{th} ed., 2003.
- Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.

Cálculo do MDC

- Em princípio, pode-se computar $\boldsymbol{mdc(a,b)}$ a partir das fatorações em primos de $\boldsymbol{a}$ e $\boldsymbol{b}$:
- De fato, se:

$$\boldsymbol{a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}}$$
$$\boldsymbol{b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}}$$

  – (expoentes nulos tornam idênticos os conjuntos de primos)
  – então: $\boldsymbol{mdc(a,b) = p_1^{min(e_1,f_1)} p_2^{min(e_2,f_2)} \cdots p_r^{min(e_r,f_r)}}$

- Exemplo: $\boldsymbol{mdc(60,18)} =?$

$$\boldsymbol{60 = 2^2 3^1 5^1} \quad \text{e} \quad \boldsymbol{18 = 2^1 3^2 5^0}$$
$$\Rightarrow \quad \boldsymbol{mdc(60,18) = 2^1 3^1 5^0 = 6}$$

- Problema: melhores algoritmos de fatoração atuais *não rodam* em tempo polinomial...
- Algoritmo eficiente para o cálculo de MDCs: Algoritmo de Euclides
- Baseado no Teorema a seguir...

- **Teorema (da Recursão do MDC):**

  Para todo inteiro *não negativo* $\boldsymbol{a}$ e para todo inteiro *positivo* $\boldsymbol{b}$:

$$\boldsymbol{mdc(a,b) = mdc(b, a\ mod\ b)}$$

- Exemplo1: $\boldsymbol{mdc(30,21)} = \boldsymbol{mdc(21,9)} = \boldsymbol{mdc(9,3)} = \boldsymbol{mdc(3,0)} = \boldsymbol{3}$
- Exemplo2: $\boldsymbol{mdc(190,34)} = \boldsymbol{mdc(34,20)} = \boldsymbol{mdc(20,14)} =$

$$= \boldsymbol{mdc(14,6)} = \boldsymbol{mdc(6,2)} = \boldsymbol{mdc(2,0)} = \boldsymbol{2}$$

- **Teorema (da Recursão do MDC):**

  Para todo inteiro *não negativo* $\boldsymbol{a}$ e para todo inteiro *positivo* $\boldsymbol{b}$:

  $$\boldsymbol{mdc(a,b) = mdc(b, a\ mod\ b)}$$

  Prova:

  - Vamos mostrar que $\boldsymbol{mdc(a,b)}$ e $\boldsymbol{mdc(b, a\ mod\ b)}$ dividem-se mutuamente
  - Isto vai indicar que eles devem ser iguais, pois:
    * $\boldsymbol{a|b \quad \Rightarrow \quad |a| \leq |b| \ \ ou \ \ b = 0}$
    * de onde temos que: $\boldsymbol{(a|b \ \wedge \ b|a) \ \Rightarrow \ a = \pm b}$

  Prova (1/2):

  - Seja $\boldsymbol{d = mdc(a,b)}$
    * então: $\boldsymbol{d|a}$ e $\boldsymbol{d|b}$
  - Mas: $\boldsymbol{a\ mod\ b = a - q.b}$ (onde $\boldsymbol{q = \lfloor a/b \rfloor}$)
    * ou seja, $\boldsymbol{a\ mod\ b}$ é uma combinação linear de $\boldsymbol{a}$ e $\boldsymbol{b}$
    * de modo que: $\boldsymbol{d|(a\ mod\ b)}$
  - Portanto, como $\boldsymbol{d|b}$ e $\boldsymbol{d|(a\ mod\ b)}$, temos que:
    * $\boldsymbol{d|mdc(b, a\ mod\ b)}$
    * ou seja: $\boldsymbol{mdc(a,b) \mid mdc(b, a\ mod\ b)}$

  Prova (2/2): (quase o mesmo)

  - Seja $\boldsymbol{d = mdc(b, a\ mod\ b)}$
    * então: $\boldsymbol{d|b}$ e $\boldsymbol{d|(a\ mod\ b)}$
  - Mas: $\boldsymbol{a = qb + a\ mod\ b}$ (onde $\boldsymbol{q = \lfloor a/b \rfloor}$)
    * ou seja, $\boldsymbol{a}$ é uma combinação linear de $\boldsymbol{b}$ e $\boldsymbol{a\ mod\ b}$
    * de modo que: $\boldsymbol{d|a}$
  - Portanto, como $\boldsymbol{d|b}$ e $\boldsymbol{d|a}$, temos que:
    * $\boldsymbol{d|mdc(a,b)}$
    * ou seja: $\boldsymbol{mdc(b, a\ mod\ b) \mid mdc(a,b)}$ $\square$

O Algoritmo de Euclides

- Versão recursiva (baseada diretamente no Teorema):

```
EUCLIDES(a,b)
 if b==0
   return a
 else
   return Euclides(b,a mod b)
```

- Exemplo: `Euclides(30,21)` = `Euclides(21,9)` = `Euclides(9,3)` = `Euclides(3,0)` = 3

- Versão não recursiva:

```
MDC(a,b)
   while b≠0
      r = a mod b
      a = b
      b = r
   return a
```

- Exemplo: sejam $a = 190$ e $b = 34$:

$$\begin{aligned}
190 &= (5) \times 34 + 20 \\
34 &= (1) \times 20 + 14 \\
20 &= (1) \times 14 + 6 \\
14 &= (2) \times 6 + 2 \\
6 &= (3) \times 2 + 0
\end{aligned}$$

$(mdc(190, 34) = mdc(34, 20) = mdc(20, 14) = mdc(14, 6) = mdc(6, 2) = mdc(2, 0) = 2)$

Complexidade do Algoritmo de Euclides

```
1 while b≠0
2      a ← a mod b
3      a ↔ b
4 return a
```

- **Fato:** Cada execução do passo **2** corta, pelo menos, metade do valor de a

  Prova:
  - após **2**, temos $a < b$ devido à função "*mod*"
  - após **3**, temos $a > b$ porque os dois foram trocados
  - logo, quando **2** é novamente executado, temos $b < a$:
    * daí, se $b \leq a/2$, então: $a \bmod b < b \leq a/2$
    * mas, se $b > a/2$, então: $a \bmod b < a - b \leq a/2$
    * logo, o novo valor a ser atribuído a a ($a \bmod b$) é $\leq a/2$ □

- Mas a e b trocam de valor cada vez que **3** é executado:
  - logo, cada um dos valores de a e b é reduzido por, pelo menos, a metade a cada vez que o loop é executado

- Então o máx de vezes que **2** e **3** são executados é o menor entre $log_2 a$ e $log_2 b$
  - estes logs são proporcionais aos comprimentos (n) das entradas, logo:

    nro de estágios executados $= O(n)$
  - daí, como cada estágio usa apenas tempo polinomial ($O(n^2)$), o tempo total é polinomial

- **Teorema2 (de Lamé):** O mdc de dois inteiros positivos a e b, com $a > b$, pode ser encontrado usando $O((log\, a)^3)$ operações entre eles

Algoritmo de Euclides Estendido Recursivo

- O próprio algoritmo de Euclides pode ser adaptado para fornecer valores de $\boldsymbol{x}$ e $\boldsymbol{y}$ para:

$$\boldsymbol{a.x + b.y = mdc(a,b)}$$

  - desde que sejam usados os *quocientes*

- Exemplo: sejam $\boldsymbol{a = 190}$ e $\boldsymbol{b = 34}$:

$$\begin{aligned}\boldsymbol{mdc(190,34)} &= \mathbf{2 = 14 - 2 \times (6)} \\ &= \mathbf{14 - 2 \times [20 - 1 \times 14]} \\ &= \mathbf{3 \times [14] - 2 \times (20)} \\ &= \mathbf{3 \times [34 - 1 \times 20] - 2 \times (20)} \\ &= \mathbf{3 \times (34) - 5 \times [190 - 5 \times 34]} \\ &= \mathbf{28 \times (34) - 5 \times (190)}\end{aligned}$$

portanto: $\boldsymbol{x = -5}$ e $\boldsymbol{y = 28}$ $\square$

- Relembrando: a versão recursiva do algoritmo de Euclides é dada por:

```
Euclides(a,b)
 if b==0
   return a
 else
   return Euclides(b, a mod b)
```

O Algoritmo de Euclides Estendido Recursivo

- Computa inteiros $\boldsymbol{(d,x,y)}$ tais que: $\boldsymbol{d = mdc(a,b) = a.x + b.y}$

```
Euclides-estendido(a,b)
  1  if  b==0
  2      return(a,1,0)      // (ax + by = a)
  3  (d',x',y') = Euclides-estendido(b,a mod b)
  4  (d,x,y) = (d',y',x'-⌊a/b⌋y')
  5  return (d,x,y)
```

- Em **3**: $\boldsymbol{d' = mdc(b, a\ mod\ b) = b.x' + (a\ mod\ b).y'}$
  - *como para o Euclides*: $\boldsymbol{d' = mdc(b, a\ mod\ b) = d = mdc(a,b)}$

- Em **4**: para obter $\boldsymbol{x}$ e $\boldsymbol{y}$ tais que $\boldsymbol{d = a.x + b.y}$, é só rearranjar:

$$\boldsymbol{d = d' = b.x' + (a - \lfloor a/b \rfloor b).y' = a.(y') + b.(x' - \lfloor a/b \rfloor y')}$$

- Exemplo: EUCLIDES-ESTENDIDO$(\mathbf{99, 78})$
  - Retorna: $\mathbf{(3, -11, 14)}$
  - De modo que:

    $\boldsymbol{mdc}\mathbf{(99, 78) = 3 = 99 \times (-11) + 78 \times (14)}$

a	b	$\lfloor a/b \rfloor$	d	x	y
99	**78**	**1**	**3**	$\mathbf{-11}$	**14**
78	**21**	**3**	**3**	**3**	$\mathbf{-11}$
21	**15**	**1**	**3**	$\mathbf{-2}$	**3**
15	**6**	**2**	**3**	**1**	$\mathbf{-2}$
6	**3**	**2**	**3**	**0**	**1**
3	**0**	-	**3**	**1**	**0**

Leituras sugeridas sobre MDCs

- Ler Cormen2: seção 31.2
- Ler Kolman5: seção 1.4
- Ler Rosen6: seção 3.5

Teoria de Números

12.1) Noções Elementares
12.2) MDCs e algoritmos de Euclides
12.3) Aritmética modular
12.4) Aplics da MD: O sistema criptográfico RSA

- Material extraído dos livros-textos (Cormen)
- E também do livro de Criptografia do Stinson

Aritmética modular

Def.: Para a inteiro e n inteiro positivo, a **mod** n é o resto que é obtido quando a é dividido por n.

- a mod n é o inteiro r tal que a=q.n+r e 0≤ r<n

Exemplos: 17 mod 5 = 2 (17=3×5 + 2)
-133 mod 9 = 2 (-133 = -15×9 + 2)
2001 mod 101 = 82 (2001=19×101 + 82)

Aritmética modular e congruências

- Existe também notação para indicar que 2 ints têm o mesmo resto quando divididos por um mesmo int n.

Def.: Se ***a*** e ***b*** são inteiros e ***n*** é um inteiro positivo, então "**a** é congruente a **b** módulo n" sse n|(a-b)

- "Inteiros a e b congruentes têm mesmo resto quando divididos por um mesmo inteiro n"
- Usa-se a notação: a ≡ b (mod n)
- Note que a ≡ b (mod n) sse a mod n = b mod n

Aritmética Modular

- Exemplos:

(i) 24 ≡ 9 (mod 5) pois: 24-9 = 3×5

(ii) 17 ≡ 5 (mod 6) pois: 17-5 = 2×6

(iii) -11 ≡ 17 (mod 7) pois: -11-17 = -4×7

O conjunto Z_n

- "Congruência módulo n" particiona ℤ em "classes de equivalência":
  - todo inteiro a é "≡ mod n" a um único r entre 0 e n-1, pois:
    - se a=q.n+r, onde 0≤ r<n, então a ≡ r (mod n)

Def.: Uma ***classe de equivalência*** de um inteiro a pode ser definida como o conjunto de todos os inteiros congruentes a ***a mod n***.

Def.: Os "inteiros módulo n", representados por Z_n, são o conjunto dos inteiros {0,1,2,...,n-1}.
- Adição, multiplicação e subtração em Z_n são realizadas mod n.

Aritmética modular e congruências

Teorema: Seja **n** um inteiro positivo. Os inteiros **a** e **b** são congruentes módulo **n** sse existe um inteiro **k** tal que

a = b + k × n

Prova:

1) se a≡b (mod n), então n|(a-b)
⇒ existe um inteiro k tal que a-b=k×n
⇒ a=b+k×n

2) conversamente:
se existe um inteiro k tal que a=b+k×n, então k×n=b-a
⇒ n divide a-b
⇒ a≡b (mod n) □

Aritmética modular e congruências

Teorema: Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

$a+c \equiv b+d \pmod{n}$

$a \times c \equiv b \times d \pmod{n}$

Prova: como $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, há inteiros s e t com
$b = a+s \times n$ e $d = c+t \times n$

- $b + d = (a+s \times n) + (c+t \times n) = (a+c) + (s+t) \times n$
  $\Rightarrow a+c \equiv b+d \pmod{n}$

- $b \times d = (a+s \times n) \times (c+t \times n) = a \times c + (a \times t + c \times s + s \times t \times n) \times n$
  $\Rightarrow a \times c \equiv b \times d \pmod{n}$

Aritmética modular e congruências

Exemplo: Como $7 \equiv 2 \pmod{5}$ e $11 \equiv 1 \pmod{5}$, o teorema anterior garante que:

$7+11 \equiv 2+1 \pmod{5}$, ou seja,
$18 \equiv 3 \pmod{5}$

$7 \times 11 \equiv 2 \times 1 \pmod{5}$, ou seja,
$77 \equiv 2 \pmod{5}$

Operações com Aritmética modular

Teorema: A aritmética modular exibe as propriedades:

$[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

$[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Exemplo: Encontre $11^7 \bmod 13$:

$11^2 = 121 \equiv 4 \bmod 13$

$11^4 \equiv 4^2 \equiv 3 \bmod 13$

$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \bmod 13$

Propriedades da Aritmética Modular sobre $\mathbb{Z}_n$

- Se $(a+b) \equiv (a+c) \pmod{n}$, então $b \equiv c \pmod{n}$
- Porém:
  - Se $(a \times b) \equiv (a \times c) \pmod{n}$, então $b \equiv c \pmod{n}$
    somente se: $mdc(a,n)=1$
- Para a divisão modular, é preciso usar inversas

Aritmética modular - Divisão

- Regra: pode-se "dividir por a (mod n)" se $mdc(a,n)=1$

Proposição: Sejam a,b,c,n inteiros com $mdc(a,n)=1$.
Se $ab \equiv ac \pmod{n}$, então $b \equiv c \pmod{n}$.
- "Se a e n são relativamente primos, pode-se dividir os 2 lados da congruência por a".

Prova:
- Como $mdc(a,n)=1$, existem inteiros x,y tais que $ax+ny=1$.
- Multiplicando por (b-c): $(ab-ac).x + n.(b-c).y = b-c$
  - *por hipótese*, (ab-ac) é múltiplo de n
  - mas n.(b-c).y também o é
- Daí: (b-c) também deve ser múltiplo de n
- Logo: $b \equiv c \pmod{n}$ □

Equações lineares modulares

Exemplo: Resolver $5x+6 \equiv 13 \pmod{11}$

Solução: $5x \equiv 7 \pmod{11}$

- como $7 \equiv 18 \equiv 29 \equiv 40 \equiv \ldots \pmod{11}$, isto é o mesmo que:
  $5x \equiv 40 \pmod{11} \Rightarrow x \equiv 8 \pmod{11}$

- ou, como $5.9 \equiv 1 \pmod{11}$:
  $x \equiv 45x \equiv 63 \equiv 8 \pmod{11}$

Equações lineares modulares

- Estas mesmas equações podem ser resolvidas utilizando-se inversas multiplicativas em $\mathbb{Z}_n$

Inversas multiplicativas

Def.: Seja $a \in \mathbb{Z}_n$. A *inversa multiplicativa* de a módulo n é um inteiro $x \in \mathbb{Z}_n$ tal que:

$$a \cdot x \equiv 1 \pmod{n}$$

– Se tal x existe, ele é único e é denotado por a^{-1}

Fato: $a \in \mathbb{Z}_n$ é inversível sse mdc(a,n)=1 .

Inversas multiplicativas

- A inversa multiplicativa pode ser eficientemente calculada com o algoritmo de Euclides estendido

Proposição: Seja mdc(a,n)=1 e sejam x e y inteiros tais que a.x+n.y=1 (do AEE). Então:
- a.x ≡ 1 (mod n)
- x é a inversa multiplicativa para a (mod n)

Prova:
Como a.x-1=-n.y, nota-se que a.x-1 é múltiplo de n □

Inversas multiplicativas

Resumo: para encontrar a^{-1} (mod n):

- Use Euclides estendido para encontrar inteiros x e y tais que a.x + n.y = 1
- Então: $a^{-1} \equiv x \pmod{n}$

Inversas multiplicativas

Exemplo: encontrar 11111^{-1} (mod 12345).

Solução: Do cálculo de mdc(11111, 12345) obtemos:

x = 2471

ou seja: 11111.2471 ≡ 1 (mod 12345) □

Os conjuntos z_n e z_p**

Def.: O grupo multiplicativo de $\mathbb{Z}_n$ é definido como:

$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid mdc(a,n)=1 \}$$

Em particular:

$$\mathbb{Z}_p^* = \{1,2, \dots , p-1\} \text{ , se p é primo}$$

Quantidade de inversas multiplicativas

- A quantidade de inteiros em $\mathbb{Z}_n$ relativamente primos a n é dada por $\varphi(n)$, *a função φ de Euler:*

$$\varphi(n) = |\mathbb{Z}_n^*|$$

- Exemplo: Os inversíveis em $\mathbb{Z}_9$ são: 1, 2, 4, 5, 7 e 8
  - Neste caso: $\varphi(9) = 6$

Quantidade de inversas multiplicativas

- Se $n = p^r$, teremos que *remover todo p-ésimo nro* a fim de obter a lista dos a's com mdc(a,n)=1

o que leva a: $\varphi(p^r) = (1 - 1/p).p^r$

- Em particular: $\varphi(p) = (p - 1)$

Quantidade de inversas multiplicativas

- Em geral, pode-se mostrar que, para qualquer n (com TCR):

$$\boxed{\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)}$$

- Exemplos: $\varphi(10) = 2.5.(1\text{-}1/2).(1\text{-}1/5) = (2\text{-}1).(5\text{-}1) = 4$
  $\varphi(120) = 120.(1\text{-}1/2).(1\text{-}1/3).(1\text{-}1/5) = 32$

- Em particular, quando $n = p.q$ (produto de 2 primos), temos:

$$\varphi(p.q) = (p\text{-}1).(q\text{-}1)$$

Potências de um elemento

- Assim como é natural considerar múltiplos "mod n" de um dado elemento a:
  - também existe a sequência de potências de a:

$a^0, a^1, a^2, a^3, \ldots$

O Teorema de Fermat

Teorema: Se p é primo e se mdc(a,p)=1:

$$a^{p-1} \equiv 1 \pmod p$$

O Teorema de Fermat

Teor. de Fermat: $a^{p-1} \equiv 1 \pmod p$

Ilustração (ideia da prova): Para p=7 e a=3, temos:

$1.3 \equiv 3 \pmod 7$ $2.3 \equiv 6 \pmod 7$ $3.3 \equiv 2 \pmod 7$
$4.3 \equiv 5 \pmod 7$ $5.3 \equiv 1 \pmod 7$ $6.3 \equiv 4 \pmod 7$

- Logo: $(1.3).(2.3).(3.3).(4.3).(5.3).(6.3) \equiv 3.6.2.5.1.4 \pmod 7$
- De modo que: $3^6.1.2.3.4.5.6 \equiv 3.6.2.5.1.4 \pmod 7$
- Portanto: $3^6.6! \equiv 6! \pmod 7$
  - ou: $3^6 \equiv 1 \pmod 7$

O Teorema de Fermat

Ex1.: 2^{53} (mod11) = $(2^{10})^5 2^3 \equiv 1^5 2^3 \equiv 8$ (mod 11)

- Note que, "trabalhando mod 11", estamos essencialmente trabalhando com os "expoentes mod 10"

Ex2.: 2^{43210} (mod 101) $\equiv (2^{100})^{432} 2^{10} \equiv 1^{432} 2^{10} \equiv 1024 \equiv 14$ (mod 101)

O Teorema de Fermat

- Obs.: Normalmente, se $2^{n-1} \equiv 1$ (mod n), o número é primo
- Esta seria uma maneira de verificar se um dado número é primo
- Mas há exceções: os "pseudoprimos"...
- Exemplo:
  $561 = 3 \times 11 \times 17$, mas: $2^{560} \equiv 1$ (mod 561)

Teorema de Euler

- Vamos precisar também do análogo do teorema de Fermat para um módulo composto...

Teorema de Euler

Se mdc(a,n)=1, então: $a^{\varphi(n)} \equiv 1$ (mod n)

Prova: semelhante à do teorema de Fermat.

Teorema de Euler: $a^{\varphi(n)} \equiv 1$ (mod n)

Exemplo: últimos 3 dígitos de 7^{803}:

- Mesmo que trabalhar mod 1000
- Como $\varphi(1000) = 1000.(1-1/2).(1-1/5) = 400$, temos:
  $7^{803} = (7^{400})^2 7^3 \equiv 7^3 \equiv 343$ (mod 1000)
- Portanto, os últimos 3 dígitos são 343
- NOTA: trocamos o expoente de 803 para 3 porque:
  $803 \equiv 3$ (mod $\varphi(1000)$)

Teorema de Euler

Então: sejam a,n,x,y inteiros com mdc(a,n)=1:

- se $x \equiv y$ (mod $\varphi(n)$), então $a^x \equiv a^y$ (mod n)
- "trabalhar mod n na base é equivalente a trabalhar mod $\varphi(n)$ no expoente"

Prova: Faça $x = y + \varphi(n).k$. Então:
$a^x = a^{y+\varphi(n).k} = a^y (a^{\varphi(n)})^k \equiv a^y 1^k \equiv a^y$ (mod n) □

O Teorema chinês do resto

- Resolver o sistema:

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

O Teorema Chinês do Resto

- **Teorema**: Sejam $m_1, m_2, \ldots, m_r$ inteiros positivos coprimos e sejam $a_1, \ldots, a_r$ inteiros. Então o sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv a_r \pmod{m_r}, \end{cases}$$

  - tem solução única módulo $M = m_1 \times m_2 \times \ldots \times m_r$, dada por:

$$\boxed{x = \sum_{i=1}^{r} a_i M_i y_i \mod M}$$

  - onde: $M_i = M/m_i$ e $y_i = M_i^{-1} \bmod m_i$, para $1 \le i \le r$.

O Teorema Chinês do Resto

Prova: precisamos mostrar que uma solução existe e que é única módulo M (vamos mostrar que ela existe por construção)

- Seja $M_k = M/m_k$, para $k = 1,2,\ldots,n$
  - note que $\text{mdc}(m_k, M_k) = 1$
  - pois, $\forall\, i \ne k$, m_i e m_k não têm fatores em comum > 1
- Logo, existe a inversa y_k tal que: $M_k y_k \equiv 1 \pmod{m_k}$
- Então, uma solução simultânea vem da soma:

  $$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r$$

  - como $M_j \equiv 0 \pmod{m_k}$, $\forall j \ne k$, todos os termos da soma são $\equiv 0 \pmod{m_k}$, exceto o k-ésimo
  - mas, como $M_k y_k \equiv 1 \pmod{m_k}$, este termo que sobra torna-se:
    $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, para $k = 1,2,\ldots,r$ □

O Teorema chinês do resto

Exemplo: Resolver o sistema:
$x \equiv 1 \pmod 3$
$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 7$

Solução:

- $M = 3.5.7 = 105$
- $M_1 = 105/3 = 35 \Rightarrow 35 y_1 \equiv 1 \pmod 3 \Rightarrow y_1 \equiv 2 \pmod 3$
- $M_2 = 105/5 = 21 \Rightarrow 21 y_2 \equiv 1 \pmod 5 \Rightarrow y_2 \equiv 1 \pmod 5$
- $M_3 = 105/7 = 15 \Rightarrow 15 y_3 \equiv 1 \pmod 7 \Rightarrow y_3 \equiv 1 \pmod 7$
- Logo: $x = 1.35.2 + 2.21.1 + 3.15.1 = 157 \equiv \mathbf{52} \pmod{105}$

Aritmética Modular

- Ler Cormen2: seções 31.6, 31.7 e 31.8
- Ler Rosen6: seção 3.7

12) Teoria de Números

12.4) Aplicações da MD: O sistema criptográfico RSA

NOTA: Este material foi elaborado com base nas seguintes referências:

- Cormen, Leiserson, Rivest, Stein, Introduction to Algorithms, 2^{nd} ed., MIT Press, 2001.
- Rosen, "Discrete Mathematics and its Aplications", 6^{th} ed., McGraw-Hill, 2007.

Princípios de Criptografia

- Métodos convencionais: baseados em engenharia
- Criptografia com chave pública:
  - baseada em funções matemáticas
  - assimétrica: duas chaves relacionadas
    - uma é amplamente divulgada: chave pública
    - a outra é guardada em segredo: chave privada
- Uso da chave privada (secreta, pessoal) pode ser comprovado sem a participação do seu proprietário:
  - integridade de dados
  - análogo eletrônico de uma assinatura manuscrita

Origem: troca de chaves

- Em 1976, Diffie e Hellman propuseram um modo seguro de trocar chaves criptográficas.
- Era baseado na suposição de existência de funções de mão única, que são funções em que:

  $\boldsymbol{y = f(x)}$ é fácil

  $\boldsymbol{y = f^{-1}(x)}$ é difícil

  - Exemplo: $\boldsymbol{f(x) = 12345^x \; mod \; 31469}$

- Exemplo deste esquema na comunicação entre $\boldsymbol{A}$ e $\boldsymbol{B}$:
  - $\boldsymbol{A}$ e $\boldsymbol{B}$ decidem usar a função (pública) $\boldsymbol{f(x) = 12345^x \; mod \; 31469}$
  - $\boldsymbol{A}$ gera $\boldsymbol{a = 27283}$ (secreto) e o envia para $\boldsymbol{B}$ "disfarçado" como:

    $\boldsymbol{12345^{27283}}$ mod $\boldsymbol{31469 = 9800}$
  - $\boldsymbol{B}$ gera $\boldsymbol{b = 12745}$ (secreto) e o envia para $\boldsymbol{B}$ "disfarçado" como:

    $\boldsymbol{12345^{12745}}$ mod $\boldsymbol{31469 = 26310}$

- $\boldsymbol{A}$ eleva o nro que recebeu ao seu expoente secreto, obtendo:

  $\mathbf{26310^{27283}} \bmod \mathbf{31469 = 27313}$
- $\boldsymbol{B}$ eleva o nro que recebeu ao seu expoente secreto, obtendo:

  $\mathbf{9800^{12745}} \bmod \mathbf{31469 = 27313}$
- ambos utilizam a chave $\mathbf{27313 = 12345^{\boldsymbol{a \times b}}} \bmod \mathbf{31469}$ $\square$

Criptografia com Chave Pública

- Problema do esquema anterior: só funcionava com troca simultânea de informações.
- Na sequência, Diffie e Hellman postularam a existência de um sistema criptográfico com duas chaves
- Chaves seriam "duais": o que uma faz, a outra desfaz
- Isto resolveria de uma vez o problema da troca de chaves:
  - uma das chaves poderia ser divulgada publicamente!
  - não seria mais preciso "combinar" uma chave secreta
- 1ra implementação do esquema imaginado por Diffie e Hellman:
  - Rivest, Shamir e Adleman (MIT, 1977)
- Baseada na dificuldade de fatoração de produtos de primos grandes
  - dados $\boldsymbol{p}$ e $\boldsymbol{q}$, calcular $\boldsymbol{n = p \times q}$: fácil
  - dado $\boldsymbol{n = p \times q}$, achar $\boldsymbol{p}$ e $\boldsymbol{q}$: difícil, se $\boldsymbol{p}$ e $\boldsymbol{q}$ forem *grandes*...

Fundamentos matemáticos (1): aritmética modular

- Aritmética "módulo n" ou "mod n"
- Usa inteiros não-negativos menores do que algum inteiro positivo n
- Operação: $\boldsymbol{a \ mod \ n}$ (resto da divisão de $\boldsymbol{a}$ por $\boldsymbol{n}$)
- Exemplo: hora do dia (mod 24)

Adição modular

- Vejamos adição "mod 10":

  $3 + 5 = 8$

  $7 + 6 = 13 \quad \rightarrow \quad$ resposta mod 10 = 3
  - só usar último dígito...
- Adição de constante mod 10 (tabela):
  - serve como esquema para cifragem de dígitos
  - chave secreta para cifrar = constante "k"
    - ∗ decifragem = subtrair "k" (mod 10)
      - · se resultado < 0, acrecentar 10

Adição módulo 10

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Subtração modular

- Subtração: *adicionar* $-\boldsymbol{k}$, a inversa aditiva de $\boldsymbol{k}$
- Inversa aditiva de $\boldsymbol{k}$:
  - "número que é preciso adicionar a k para obter 0"
    - $\boldsymbol{k + \text{“}-k\text{”} = 0}$
  - em aritmética mod 10:
    - $\mathbf{4 + 6 = 0 \quad \Rightarrow \quad \text{“}-4\text{”} = 6}$
      - também: $\mathbf{\text{“}-4\text{”} = -4 + 10}$
      - note que: $\mathbf{10 \equiv 0 \ (\boldsymbol{mod}\ 10)}$
- Cifragem com chave secreta = 4:
  - cifrar: somar $\mathbf{4\ (\boldsymbol{mod}\ 10)}$
  - decifrar: somar $\mathbf{6\ (\boldsymbol{mod}\ 10)}$

Multiplicação modular

x	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

- Multiplicação "$\boldsymbol{mod\ n}$" é uma cifra:
  - podemos "embaralhar" os dígitos multiplicando por $\boldsymbol{k\ (mod\ n)}$

- Decifragem:
  - efeito da multiplicação é desfeito com uma multiplicação pela inversa multiplicativa de $\boldsymbol{k}$:
    - $\boldsymbol{k^{-1}}$ é o número pelo qual se deve multiplicar $\boldsymbol{k}$ para obter $\mathbf{1}$
    - $\boldsymbol{k \times k^{-1} = 1}$
  - note que: $\boldsymbol{x \times k \times k^{-1} = x \times 1 = x}$
- Funcionam como cifradores: $\times\mathbf{3}$, $\times\mathbf{5}$, $\times\mathbf{7}$, $\times\mathbf{9}$
  - multiplicação por qualquer um dos outros não
  - logo: é preciso escolher bem o "multiplicador"
- Exemplo: $\boldsymbol{k = 7 \;\Rightarrow\; k^{-1} = 3}$
  - pois: $\boldsymbol{7 \times 3 = 1 \; (mod\ 10)}$
  - cifragem seria "$\times\mathbf{7}$" e decifragem seria "$\times\mathbf{3}$"

Fundamentos matemáticos (2): inversas multiplicativas

- Definição: $\mathbf{Z}_{\boldsymbol{n}} = \{\mathbf{0, 1, 2, \ldots,} \boldsymbol{n} - \mathbf{1}\}$
- Um elemento $\boldsymbol{a}$ de $\mathbf{Z}_{\boldsymbol{n}}$ tem inversa multiplicativa $\boldsymbol{a^{-1}}$ somente se $\boldsymbol{mdc(a, n) = 1}$
  - são os relativamente primos a $\boldsymbol{n}$
- O mdc entre dois valores $\boldsymbol{a}$ e $\boldsymbol{b}$ pode ser calculado pelo algoritmo de Euclides.
- O valor de $\boldsymbol{a^{-1}}$ pode ser calculado eficientemente por uma extensão do algoritmo de Euclides.
- Exemplo: $\mathbf{Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}}$
  - Há 6 elementos inversíveis: 1,2,4,5,7 e 8
    - $\mathbf{4^{-1} = 7}$ porque $\boldsymbol{4 \times 7 \equiv 1 \; (mod\ 9)}$
    - $\mathbf{5^{-1} = 2}$ porque $\boldsymbol{5 \times 2 \equiv 1 \; (mod\ 9)}$
  - Diz-se que: quantidade de inversíveis $= \mathbf{6} = \boldsymbol{\phi(9)}$
- Cálculo de inversas: Algoritmo de Euclides Estendido

Fundamentos matemáticos (3): Função $\boldsymbol{\phi(n)}$ de Euler

- $\boldsymbol{\phi(n)}$ = qtde de inteiros $\boldsymbol{a}$ para os quais $\boldsymbol{mdc(a, n) = 1}$
- **Teorema**: se mdc$\boldsymbol{(a, n) = 1}$, $\boldsymbol{a^{\phi(n)} \equiv 1 \; (mod\ n)}$
- Exemplo: $\mathbf{Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}}$
  - inversíveis: $\mathbf{\{1, 3, 7, 9\}}$
  - de modo que: $\boldsymbol{\phi(10) = 4}$
  - logo: $\boldsymbol{1^4 \equiv 3^4 \equiv 7^4 \equiv 9^4 \equiv 1 \; (mod\ 10)}$

- Exemplo: quais os *3 últimos dígitos* de $\mathbf{7^{803}}$?
  - mesmo que trabalhar "mod 1000"
  - então, como $\boldsymbol{\phi(1000) = 400}$, temos:
    $\boldsymbol{7^{803} = (7^{400})^2 \times 7^3 \equiv (1) \times 7^3 \equiv 343\ (mod\ 1000)}$
  - portanto, os 3 últimos dígitos são 343

Avaliação de $\phi(n)$

- Quantos números $< n$ são relativamente primos a n?
  - Se n é primo: $\boldsymbol{\phi(n) = n - 1}$
  - Se $\boldsymbol{n = p \times q}$ (produto de 2 primos):
    $$\boldsymbol{\phi(p \times q) = (p-1) \times (q-1)}$$
  - Exemplo: $\boldsymbol{\phi(10) = (2-1).(5-1) = 4}$

O sistema criptográfico RSA (1/5)

- Cifrador em blocos
- Computações são feitas "módulo n"
  - $\boldsymbol{n = p \times q}$ = produto de 2 números primos distintos
  - "$\boldsymbol{n}$" é um número muito grande
    - $|\boldsymbol{n}| > \mathbf{1024}$ bits (> **300** dígitos decimais)
  - textos são números inteiros entre **0** e $\boldsymbol{n-1}$
- Infelizmente: muito lento
  - na prática: usado só na troca de chaves simétricas...

O sistema criptográfico RSA (2/5)

- Cifrar: $\boldsymbol{y = x^e\ mod\ n}$
- Decifrar: $\boldsymbol{x = y^d\ mod\ n}$
- Configuração do sistema:

$\boldsymbol{p}$ e $\boldsymbol{q}$ são números primos	(secretos)
$\boldsymbol{n = p \times q}$	(público)
$\boldsymbol{\phi(n) = (p-1).(q-1)}$	(secreto)
$\boldsymbol{e}$ tal que: $\boldsymbol{mdc(e, \phi(n)) = 1}$	(público)
$\boldsymbol{d \equiv e^{-1}\ (mod\ \phi(n))}$	(secreto)

O sistema criptográfico RSA (3/5)

- Exemplo: Bob escolhe $\boldsymbol{p = 3119}$ e $\boldsymbol{q = 1571}$.
  - Configurando:
    - $\boldsymbol{n = p \times q = 5214149}$
    - $\boldsymbol{\phi(n) = (3119 - 1).(1571 - 1) = 5209260}$
  - Bob escolhe $\boldsymbol{e = 3533}$ e calcula (Euclides):
    - $\boldsymbol{d = 3533^{-1} = 4034117\ (mod\ 5209260)}$ (privado)
  - Bob publica em um diretório:
    - $\boldsymbol{e = 3533}$ e $\boldsymbol{n = 5214149}$

O sistema criptográfico RSA (4/5)

- Exemplo (cont.): $\boldsymbol{\{n = 5214149, e = 3533, d = 4034117\}}$
  - Para Alice enviar o texto **16597** para Bob, ela deve fazer:
    - $\boldsymbol{16597^{3533}\ mod\ 5214149 = 976827}$
  - Do outro lado, Bob decifra usando o expoente $\boldsymbol{d}$:
    - $\boldsymbol{976827^{4034117}\ mod\ 5214149} = \mathit{16597}$

O sistema criptográfico RSA (5/5)

- Como pode a decifragem ser o mesmo que a cifragem, mas com um expoente diferente??
- Note que: $\boldsymbol{e.d \equiv 1\ (mod\ \phi(n))}$

$$\Rightarrow \quad \boldsymbol{e.d = k.\phi(n) + 1}$$

- então:

$$\begin{aligned} (x^e)^d &\equiv x^{k.\phi(n)+1}\ (mod\ n) \\ &\equiv (x^{\phi(n)})^k.x^1\ (mod\ n) \\ &\equiv (1)^k.x\ (mod\ n) \\ &\equiv x\ (mod\ n) \qquad \square \end{aligned}$$

- **Nota**: tudo isto funciona também quando $\boldsymbol{mdc(x, n) \neq 1}$
- Neste caso, deve ocorrer: $\boldsymbol{mdc(x, n) = p}$ ou $\boldsymbol{mdc(x, n) = q}$
- Em ambos os casos, mostra-se que a análise anterior é válida utilizando-se o Teorema Chinês do Resto

Implementação do RSA

- Cifragem e decifragem:
  - exponenciação módulo n com inteiros (muito) grandes
  - exemplo: $\mathbf{9726^{3533}}\ \boldsymbol{mod}\ \mathbf{11413} =$??
- Executar exponenciações e só depois "reduzir módulo n":
  - valores intermediários astronômicos!
- A solução é explorar a propriedade:

  $(a \times b)\ mod\ n = ((a\ mod\ n) \times (b\ mod\ n))\ mod\ n$

- Exemplo1: $\mathbf{11^7}\ \boldsymbol{mod}\ \mathbf{13 = ??}$
  - pode ser calculado como: $\mathbf{19487171}\ \boldsymbol{mod}\ \mathbf{13}$
  - ou então como: $\mathbf{11^1.11^2.11^4 \equiv 11.4.3 \equiv 132 \equiv 2}\ \boldsymbol{mod}\ \mathbf{13}$
  - note que:
    - $\mathbf{11^2 = 121 \equiv 4}\ \boldsymbol{mod}\ \mathbf{13}$
    - $\mathbf{11^4 = 4^2 \equiv 3}\ \boldsymbol{mod}\ \mathbf{13}$

- Exemplo2: computar $\mathbf{2^{1234}}\ \boldsymbol{mod}\ \mathbf{789}$
  - Primeiro note que:

$$
\begin{array}{lll}
2^2 \equiv 4\ (mod\ 789) & \rightarrow & 2^4 \equiv 4^2 \equiv 16\ (mod\ 789) \\
2^8 \equiv 16^2 \equiv 256\ (mod\ 789) & \rightarrow & 2^{16} \equiv 256^2 \equiv 49\ (mod\ 789) \\
2^{32} \equiv 34\ (mod\ 789) & \rightarrow & 2^{64} \equiv 367\ (mod\ 789) \\
2^{128} \equiv 559\ (mod\ 789) & \rightarrow & 2^{256} \equiv 37\ (mod\ 789) \\
2^{512} \equiv 580\ (mod\ 789) & \rightarrow & 2^{1024} \equiv 286\ (mod\ 789)
\end{array}
$$

  - Em seguida note que: $\mathbf{1234 = (10011010010)_2 = 1024 + 128 + 64 + 16 + 2}$
  - De modo que: $\mathbf{2^{1234} \equiv 286.559.367.49.4 \equiv 481}\ (\boldsymbol{mod}\ \mathbf{789})$
  - Note que não foi preciso trabalhar com números $> \mathbf{788^2}$

Algoritmo "quadrado-e-multiplica"

- O exemplo anterior ilustra a justificativa para o algoritmo abaixo.
- Algoritmo para computar $\boldsymbol{x^b\ mod\ n}$:

```
z=1
for i=r-1 downto 0 do
   z=z^2 mod n
   if b_i=1 then z=z.x mod n
```

- "r" é o nro de bits na representação binária de b

- Exemplo3: cálculo de $\mathbf{9726^{3533}}$ $\boldsymbol{mod}$ $\mathbf{11413}$:

$$\mathbf{3533 = (110111001101)_2} \quad \Rightarrow \quad \mathbf{12}\,\boldsymbol{bits} \quad \Rightarrow \mathbf{20} \quad \text{multiplicações}$$

i	b_i	z
11	1	$\mathbf{1^2 \times 9726 = 9726}$
10	1	$\mathbf{9726^2 \times 9726 = 2659}$
9	0	$\mathbf{2659^2 = 5634}$
8	1	$\mathbf{5634^2 \times 9726 = 9167}$
7	1	$\mathbf{9167^2 \times 9726 = 4958}$
6	1	$\mathbf{4958^2 \times 9726 = 7783}$
5	0	$\mathbf{7783^2 = 6298}$
4	0	$\mathbf{6298^2 = 4629}$
3	1	$\mathbf{4629^2 \times 9726 = 10185}$
2	1	$\mathbf{10185^2 \times 9726 = 105}$
1	0	$\mathbf{105^2 = 11025}$
0	1	$\mathbf{11025^2 \times 9726 = 5761}$

Leituras sugeridas sobre o RSA:

- Ler Cormen2: seção 31.7
- Ler Rosen6: seção 3.7