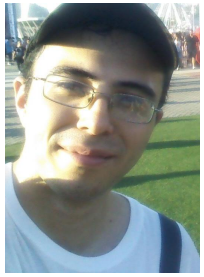
Matemática Discreta

Pedro Hokama

Fontes

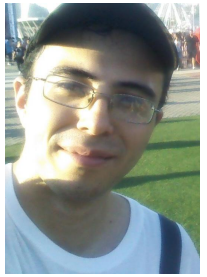
- Gomide, Anamaria; Stolfi, Jorge. Elementos de Matematica Discreta para Computação.
- Rosen, Kenneth H. Discrete mathematics and its applications. McGraw-Hill Education, 8th Edition, 2019.

Sobre o docente



- 2002 - 2004: Técnico em Programação e Desenvolvimento de Sistemas (CEFET-SP)
- 2006 - 2009: Bacharelado em Ciência da Computação (UNICAMP)
  - 2007-2008: IC - Algoritmos e Heurísticas para Empacotamento Tridimensional
  - 2008-2009: IC - Algoritmos e Heurísticas para o Problema de Roteamento Tridimensional
- 2009 - 2011: Mestrado em Ciência da Computação (UNICAMP) - O Problema do Caixeiro Viajante com Restrições de Empacotamento Tridimensional
- 2011 - 2016: Doutorado em Ciência da Computação (UNICAMP) - Algoritmos para Problemas com Restrições de Empacotamento

Sobre o docente



- 2016 - 2018: Pós-doutorado (UFSCar)
- 2018 - atual: Professor Adjunto no Instituto de Matemática e Computação da Universidade Federal de Itajubá
  - Programa de Pós-Graduação em Ciência e Tecnologia da Computação.
  - Orientador de IC, TFG e Pós-Graduação: Algoritmos, Otimização, Teoria dos Jogos, Aprendizado de Máquina, etc..
  - Coordenador do Projeto de Extensão DevU - Desenvolvimento de Jogos
  - Coordenador de Mobilidade Acadêmica dos Cursos de Sistemas de Informação e Ciência da Computação

Sobre a disciplina

- **Lógica matemática.** Professores das disciplinas dos cursos de computação, com conteúdo teórico, frequentemente observam a grande dificuldade que seus alunos tem em formalizar seu raciocínio.
- A raiz desse problema é a dificuldade que muitos alunos tem em perceber a diferença entre uma **prova rigorosa** e uma **coleção de frases aleatórias e inconclusivas**, mesmo que com vocabulário matemático, que termina com a conclusão esperada.

Sobre a disciplina

- A ideia da disciplina é alfabetizar vocês na linguagem lógica matemática, principalmente usada na computação.
- Dessa forma a disciplina é mais abrangente do que profunda. Mas o aluno interessado pode e deve se aprofundar do que tiver interesse

Sobre a disciplina

- Lógica Matemática: teoria dos conjuntos, lógica proposicional.
- Relações e Funções.
- Somatórias e produtórias.
- Sequências e recorrências.
- Contagem.
- Cardinalidade de conjuntos.
- Noções de Probabilidade.
- Noções de Grafos.

Introdução

Como ter certeza de que um programa que você escreveu está correto?

Testar para várias instâncias?

Programadores podem citar exemplos de programas que funcionaram perfeitamente em todos os testes mas falharam imediatamente quando usados na prática.

Questão: Como ter certeza de que nosso raciocínio é correto e como transmitir aos outros essa certeza?

A invenção da lógica

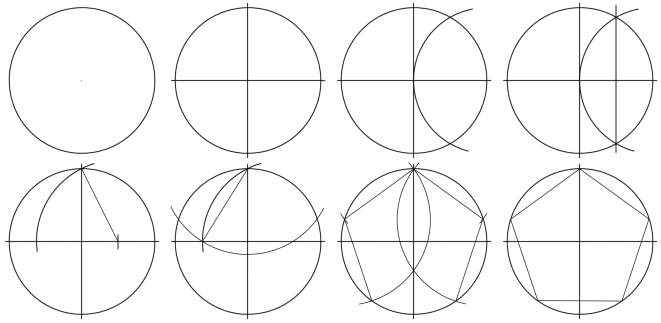
- Estudada pelos gregos pelo menos 4 séculos A.C.
- Observaram que uma maneira de transmitir essa certeza:
  - Começar com um conjunto de axiomas, fatos simples que todos concordam.
  - Desenvolver um raciocínio a partir desses axiomas, usando **regras de inferência**, maneiras de raciocinar que todos concordam que são válidas.
- Com isso inventaram a **lógica**, que era um ramo da **retórica**, a arte de discursar e convencer pessoas.

Silogismos

- Aristóteles (384–322 A.C.)
- Partindo de duas premissas cuja verdade é aceita
- obtém-se uma conclusão nova que é necessariamente verdade
- Exemplos:
  - "Todos os homens são mortais"
  - "Sócrates é um homem"
  - temos que acreditar que "Sócrates é mortal"
  - "Nenhum mamífero tem penas"
  - "Morcegos são mamíferos"
  - logo "Morcegos não tem penas"

Euclides e demonstrações geométricas

Os arquitetos e engenheiros gregos tinham preocupações semelhantes com os "Algoritmos geométricos". Considere o seguinte algoritmo para desenhar um pentágono:



- Podemos fazer no papel e medir.
- Mas os passos e a medida final podem ter pequenos erros.
- Se a diferença no papel for desprezível, será que ainda vai ser na construção de um anfiteatro?

Euclides (por volta do século III antes da era comum) descreveu um sistema lógico para a geometria da época no seu livro *Elementos de Geometria*.

10 axiomas sobre conceitos geométricos, como por exemplo:

- *Por dois pontos distintos do plano passa uma única reta.*
- *Qualquer segmento de reta pode ser prolongado indefinidamente nos dois sentidos.*
- *É possível contruir um círculo com quaisquer centro e raio dados.*
- *Todos os ângulos retos são iguais.*

E **demostrou** centenas de outras afirmações, por exemplo:

- *Se um triângulo tem os três lados iguais, ele tem os três ângulos iguais.*
- *Duas retas que são perpendiculares a uma terceira são paralelas entre si.*
- *Num triângulo retângulo, o quadrado do maior lado é a soma dos quadrados dos outros dois lados.*

Euclides e demonstrações geométricas

Para cada teorema, ele escreveu uma **prova** ou **demonstração** – uma sequência de passos lógicos que, começando com os axiomas e teoremas já provados, convence qualquer leitor de que o novo teorema é verdadeiro.

Álgebra

- A lógica de Euclides foi extensamente usada por mais de dois mil anos.
- Porém o hábito de provar as afirmações foi limitado à geometria.
- Os gregos conheciam muitas propriedades de números, por exemplo, divisor comum e número primo. Mas para demonstrar tais propriedades eles convertiam os números em comprimentos de retas e usavam a geometria.

- Na idáde média matemático árabe Al-Khowarizmi inventou a **álgebra**.
- Outra maneira de provar afirmações sobre números e convencer pessoas de que uma dada sequência de operações aritméticas alcança o resultado desejado.
- Os números são representados por letras.
- Operações e afirmações sobre esses números são indicadas com símbolos como ‘$+$’ ou ‘$>$’.

- A álgebra também fornece algumas fórmulas, como $A + B = B + A$ e $A \times (B + C) = (A \times B) + (A \times C)$, que representam afirmações que são sempre verdadeiras.
- Permite transformar uma fórmula em outra fórmula equivalente, ou combinar fórmulas corretas para produzir novas fórmulas corretas. Por exemplo, se sabemos que $A > B$ e $B > C$ podemos concluir com certeza que $A > C$.
- Geometria e Álgebra foram enfim unidas pelo matemático René Descartes (1596 - 1650) que mostrou como usar pares de números reais para representar pontos do plano. Essa ideia criou a área da geometria analítica e forneceu uma interpretação geométrica para álgebra linear.

As linguagens da lógica matemática

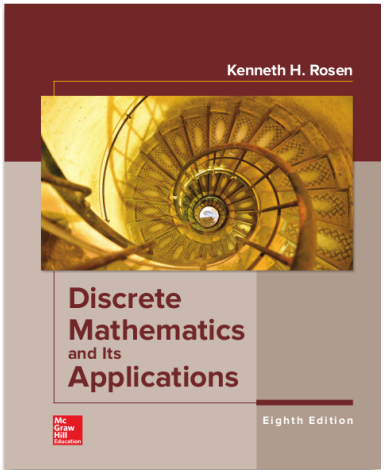
- Outros matemáticos, principalmente no século 19 mostraram como aplicar a ideia geral da álgebra também a lógica.
- Dispomos de dois principais sistemas de notação, ou **linguagens formais**, para expressar raciocínios lógicos de maneira matematicamente
  - clara,
  - sucinta, e
  - livre de ambiguidade
- Que são:
  - teoria dos conjuntos
  - cálculo de predicados

As linguagens da lógica matemática

- A lógica clássica está restrita a afirmações que são verdadeiras ou falsas.
- No sec. 16 e 17 estudaram chances em jogos de azar.
- Que no início do século 20 evoluíram para a **teoria da probabilidade** e a **estatística**.
- Em meados do século 20, motivada pela expansão do rádio, telefone e outros meios de comunicação a teoria da probabilidade deu origem à **teoria da informação**.
- Futuramente **análise de algoritmos**, **teoria da computabilidade** e complexidade

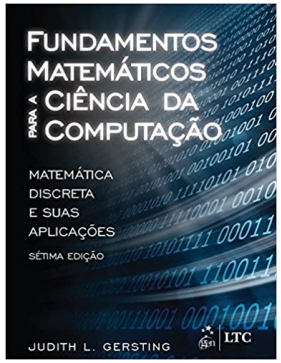
Referências

- Discrete Mathematics and Its Applications
- Kenneth H. Rosen
- Excelente Livro sobre o Tema.



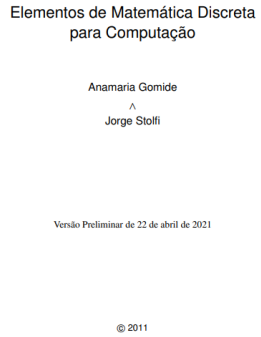
Referências

- Fundamentos Matemáticos para a Ciência da Computação
- Judith Gersting



Referências

- Elementos de Matemática Discreta para Computação
- Anamaria Gomide e Jorge Stolfi
- Em português e tem versão online.
- Mais simples e menos prolixo.
- Ainda em desenvolvimento (pode conter alguns erros)


Elementos de Matemática Discreta
para Computação

Anamaria Gomide
∧
Jorge Stolfi

Versão Preliminar de 22 de abril de 2021

© 2011

Teoria dos Conjuntos (Revisão)

- Um **conjunto** é um conceito primitivo, que informalmente pode ser entendido como uma coleção **não ordenada** de entidades distintas, chamadas de **elementos** do conjunto.
- Dizemos que um elemento x **pertence** a um conjunto A se x é um elemento de A. Denotamos este fato por
$$x \in A.$$

- Para denotar que x **não pertence** a A, ou seja, que x não é um elemento do conjunto A, escrevemos
$$x \notin A.$$
- A notação
$$x, y, z \in A$$
é muito usada como uma abreviação de $x \in A$ e $y \in A$ e $z \in A$

- Se x pertence a um conjunto A, diz-se também que A **tem** (ou **possui**) x, e escreve-se
$$A \ni x.$$
- A negação desta afirmação (A **não tem** ou **não possui** x) é denotada por
$$A \not\ni x.$$
- Não é correto dizer que A "contém" x, pois este termo é usado em matemática com um sentido diferente.

- Podemos especificar um conjunto de diversas formas. Se um conjunto tem poucos elementos, podemos listá-los, um a um, em qualquer ordem, entre chaves '{}'.
- Por exemplo, o conjunto cujos elementos são os números inteiros 2, 3 e 5 pode ser escrito $\{2, 3, 5\}$.
- Assim, por exemplo, temos que
$$3 \in \{2, 3, 5\},$$
mas
$$4 \notin \{2, 3, 5\}.$$

- Outra maneira de especificar um conjunto é através das propriedades de seus elementos.
- Para tanto, usamos a notação $\{ x : P(x) \}$, onde x é uma variável arbitrária e $P(x)$ uma afirmação matemática que depende do valor de x.
- Por exemplo, outra maneira de definir o conjunto $\{-4, -3, -2, -1, 0, +1, +2, +3, +4\}$ é
$$\{ x : x \text{ é um número inteiro e } -5 < x < 5 \}$$
- Comumente também é usado o simbolo '|' em vez de ':' para significar "tais que".

Existem alguns conjuntos de números que são muito usados em matemática, e tem notações convencionais bem estabelecidas:

- o conjunto dos **números inteiros** $\mathbb{Z}$,
- o conjunto dos **números naturais** $\mathbb{N} = \{ x : x \in \mathbb{Z} \text{ e } x \geq 0 \}$,
- Obs: Alguns autores entendem que o conjunto dos números naturais não inclui o zero. Em várias línguas não falamos "tenho zero bois". Em latim nem sequer existia uma palavra para esse número, que não pode ser escrito em algarismos romanos.

- o conjunto dos **números racionais** $\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z} \text{ e } b \neq 0 \right\}$, e
- o conjunto dos **números reais** $\mathbb{R}$.
- o conjunto dos **números complexos** $\mathbb{C} = \{ x + y\mathbf{i} : x, y \in \mathbb{R} \}$, em que $\mathbf{i} = \sqrt{-1}$.

Exercício

Escreva explicitamente os elementos dos seguintes conjuntos:

1. $A = \left\{ x : x \in \mathbb{Z} \text{ e } x^2 - 2x + 1 \leq 0 \right\}$.
2. $A = \{ x : x \in \mathbb{Z},\ 2 \leq x \leq 20 \text{ e } x \text{ é primo} \}$.
3. $A = \left\{ x : x \in \mathbb{R} \text{ e } x^2 - 2x = 0 \right\}$.

Definições circulares e contraditórias

- A definição de um conjunto pode usar outros conjuntos

  “seja X o conjunto de todos os elementos que estão no conjunto Y mas não no conjunto Z”.

- Porém, deve-se tomar cuidado para evitar definições circulares, que podem não ter sentido.

  “seja X o conjunto de todos os elementos que não pertencem a X”

- Esta “definição” não faz sentido pois diz que um elemento que está em X não está em X, e vice-versa.

- Suponha que o barbeiro de um quartel recebeu a ordem de fazer a barba de todos os que não fizessem sua própria barba, e apenas esses.
- O que o barbeiro faz com a sua barba?
- Este contra-exemplo teve um papel muito importante no desenvolvimento da teoria de conjuntos.
- Ele é conhecido pelo nome **Paradoxo de Russel**, por ter sido observado pelo matemático inglês Bertrand Russel (1872–1970).
- Ele é conhecido também como **Paradoxo do Barbeiro**

- Por outro lado, há definições circulares de conjuntos que são perfeitamente válidas.
- Por exemplo, considere o conjunto de inteiros X que possui o inteiro 1, não possui o inteiro 0, possui $x + 2$ e $x - 2$ qualquer que seja o elemento x de X.
- Pode-se verificar que o único conjunto X com estas propriedades é o conjunto dos inteiros ímpares.
- Para entender porque esta definição é válida vamos precisar do conceito de indução matemática, que será visto posteriormente.

Igualdade de conjuntos

- Por definição, um conjunto A **é igual a** um conjunto B se, e somente se, todo elemento de A é elemento de B, e todo elemento de B é elemento de A.
- Esta condição, denotada por
$$A = B,$$
significa que A, B são o mesmo conjunto.

- Dito de outra forma, dois conjuntos A e B são diferentes ($A \neq B$) se, e somente se, existe um elemento de A que não pertence a B, ou um elemento de B que não pertence a A.
- Observe que, como os conjuntos não são ordenados, o conjunto $\{1, 2, 3\}$ é igual ao conjunto $\{3, 2, 1\}$.

Conjunto vazio

- É possível definir conjuntos sem elementos.
- Dizemos que tal conjunto é **vazio**.
- Por exemplo, considere o conjunto $A = \{ x : x \in \mathbb{R} \text{ e } x = x + 1 \}$.
- Todos os conjuntos vazios são iguais; ou seja existe um único conjunto vazio, que é geralmente denotado por

$$\emptyset.$$

Relação de inclusão

- Sejam A e B dois conjuntos. Dizemos que A é um **subconjunto** de B se, e somente se, todo elemento de A é um elemento de B.
- Neste caso, dizemos também que A **está contido em** B, denotado por

$$A \subseteq B,$$

- ou que B **contém** A. Denotamos esta condição por

$$B \supseteq A.$$

- Se existe um elemento de A que não pertence a B, então A não é subconjunto de B, e escrevemos

$$A \nsubseteq B.$$

- De acordo com esta definição, um conjunto está contido em si próprio? e contém o conjunto vazio? sim:

$$A \subseteq A \text{ e } \emptyset \subseteq A,$$

para qualquer conjunto A.

- Se $A \subseteq B$ mas $A \neq B$, dizemos que A é um sub-conjunto **próprio** de B, que denotamos por

$$A \subset B \text{ ou } B \supset A.$$

- Analogamente,

$$A \not\subset B$$

significa que A não é um subconjunto próprio de B.

Cardinalidade

- Informalmente, dizemos que um conjunto A é **finito** se ele tem um número finito $n \in \mathbb{N}$ de elementos.
- Este número é a **cardinalidade** de A, denotada por $|A|$ ou $\# A$.
- Observe que $|A| = 0$ se e somente se $A = \emptyset$.
- Dizemos que um conjunto é **infinito** se ele não é finito.

- Os conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, e $\mathbb{R}$ são infinitos.
- Conjuntos infinitos não podem ter seus elementos listados explicitamente.
- Informalmente, é comum usar '. . . ' nesses casos, por exemplo
  - $\mathbb{N} = \{0, 1, 2, \ldots\}$
  - $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\}$

  Entretanto, esta notação deve ser evitada pois pode ser ambígua. Por exemplo, o que é o conjunto $\{2, 3, 5, 7, \ldots\}$?

Operações com conjuntos

União e interseção

Para os próximos conceitos sejam A e B dois conjuntos.

- A **união** de A e B, denotada por $A \cup B$, é o conjunto de todos os elementos que estão em pelo menos um dos conjuntos, A ou B.
  Exemplo: Se $A = \{1, 2, 3\}$ e $B = \{2, 3, 4, 5\}$ então $A \cup B = \{1, 2, 3, 4, 5\}$.

- A **intersecção** de A e B, denotada por $A \cap B$, é o conjunto de todos os elementos que estão em ambos os conjuntos, A e B.
  Exemplo: Se $A = \{1, 2, 3\}$ e $B = \{2, 3, 4, 5\}$ então $A \cap B = \{2, 3\}$.
- Se $A \cap B = \emptyset$ dizemos que os conjuntos A e B são **disjuntos**, ou **não tem intersecção**, ou **não se intersectam**.
- Diz também que três ou mais conjuntos são **disjuntos dois a dois** se todos os pares desses conjuntos são disjuntos.

- A **diferença de** A **e** B é o conjunto de todos os elementos de A que não estão em B. Este conjunto é também chamado A **menos** B, ou o **complemento de** B **em** A, e é denotado por

$$A - B \text{ ou } A \setminus B.$$

- Em certos casos, é conveniente supor que todos os elementos de todos os conjuntos que nos interessam pertencem a um **conjunto universal** ou **universo**, que denotaremos por $\mathcal{U}$. Se A é o conjunto universo $\mathcal{U}$, então $\mathcal{U} - B$ é chamado o **complemento** de B e denotado por $\overline{B}$ ou B^c.
- Observe que se $A \subseteq B$ então $A \cup B = B$, $A \cap B = A$ e $\overline{B} \subseteq \overline{A}$.

Exercício: Dê exemplos em que:

- $(A \cup B) - B = A$
- $(A \cup B) - B \neq A$

Exercício: Sejam A e B dois conjuntos finitos quaisquer. Encontre uma fórmula matemática que relaciona $|A|$, $|B|$, $|A \cap B|$ e $|A \cup B|$.

Outra operação entre conjuntos é a **diferença simétrica**, denotada por $A \oplus B$ ou $A \triangle B$, que consiste de todos os elementos que estão em **exatamente** em um dos dois conjuntos. Isto é,

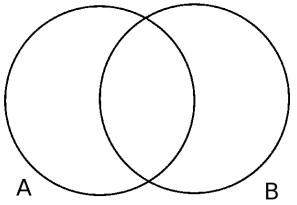
$$A \triangle B = (A \setminus B) \cup (B \setminus A) \tag{1}$$

Exercício: Se $A \triangle B = A$ o que se pode dizer dos conjuntos A e B?

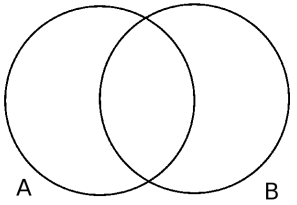
Operações com conjuntos

Diagrama de Venn

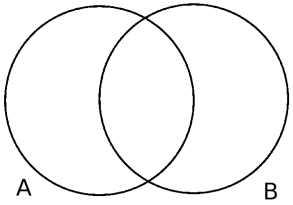
Esta representação gráfica para conjuntos é chamada de **diagrama de Venn**, por ter sido introduzida pelo matemático inglês John Venn (1834–1923).



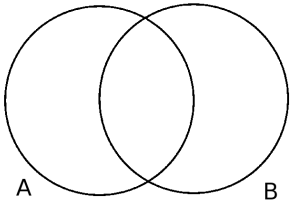
A



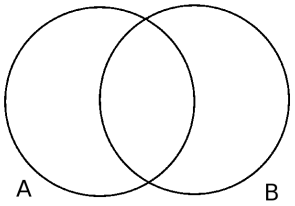
B



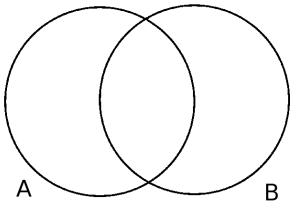
$A \cup B$



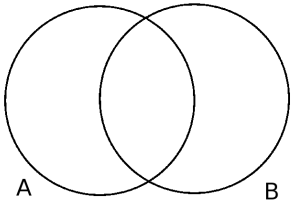
$A \cap B$



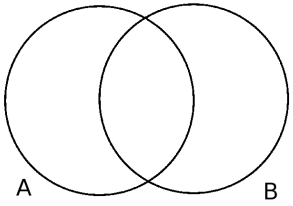
$A \setminus B$



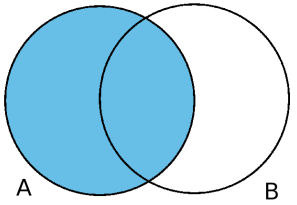
$B \setminus A$



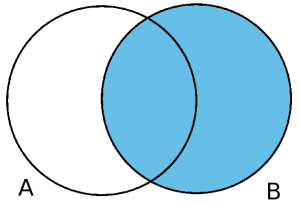
$A \triangle B$



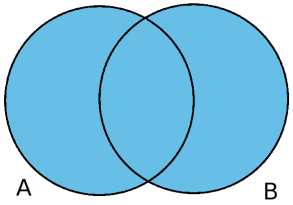
$\overline{A}$



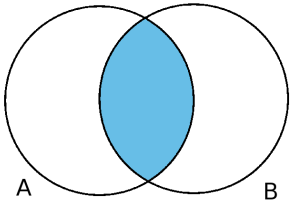
A



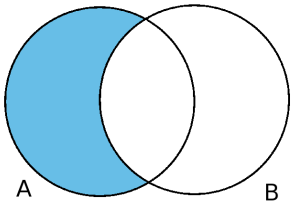
B



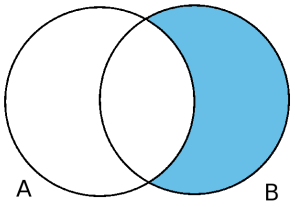
$A \cup B$



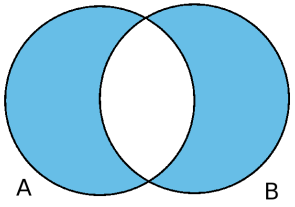
$A \cap B$



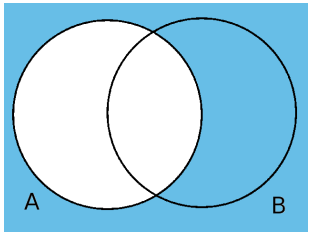
$A \setminus B$



$B \setminus A$



$A \triangle B$



$\overline{A}$

Operações com conjuntos

Propriedades das operações com conjuntos

- **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**:
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Operações com conjuntos

Propriedades das operações com conjuntos

- **Idempotência**:
  - $A \cup A = A$.
  - $A \cap A = A$.
- **Leis de De Morgan**:
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

  Estas leis levam o nome do matemático inglês Augustus de Morgan (1806–1871), mas eram conhecidas desde a Antiguidade.

- **Propriedades do complemento**:
  - $\overline{\overline{A}} = A$.
  - $A \cup \overline{A} = \mathcal{U}$.
  - $A \cap \overline{A} = \emptyset$.
  - $\overline{\mathcal{U}} = \emptyset$.
  - $\overline{\emptyset} = \mathcal{U}$.

- **Propriedades do conjunto universal**:
  - $A \cup \mathcal{U} = \mathcal{U}$.
  - $A \cap \mathcal{U} = A$.
- **Propriedades do conjunto vazio**:
  - $A \cup \emptyset = A$.
  - $A \cap \emptyset = \emptyset$.

Exercício: Usando diagramas de Venn, verifique que a diferença simétrica também é uma operação associativa e comutativa; isto é, que $A \triangle B = B \triangle A$ e $(A \triangle B) \triangle C = A \triangle (B \triangle C)$, para quaisquer conjuntos A, B e C.

Exercício: Use diagramas de Venn para verificar as seguintes identidades:

1. $A \setminus (A \cap B) = A \setminus B$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
3. $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.
4. $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$.

Exercício: Sejam A, B e C três conjuntos finitos quaisquer. Encontre uma fórmula matemática para $|A \cup B \cup C|$ em função de $|A|$, $|B|$, $|C|$, $|A \cap B|$, $|A \cap C|$, $|B \cap C|$ e $|A \cap B \cap C|$.

Conjuntos de conjuntos

- Conjuntos podem ser elementos de outros conjuntos.
- Por exemplo, o conjunto

$$A = \{\emptyset, \{2,3\}, \{2,4\}, \{2,4,7\}\}$$

  é um conjunto com quatro elementos.
- Se B é o conjunto $\{2,3\}$, temos que B é elemento de A ($B \in A$), mas B não é sub-conjunto de A ($B \not\subseteq A$).

$$A = \{\emptyset, \{2,3\}, \{2,4\}, \{2,4,7\}\}$$

- Note que $\emptyset$ é elemento de A e também subconjunto de A, enquanto que $\{2\}$ não é nem uma coisa nem outra.
- Em particular, o conjunto $C = \{\emptyset\}$ **não** é vazio, pois ele tem um elemento — o conjunto vazio. Observe que $|C| = 1$, enquanto que $|\emptyset| = 0$.

Conjunto potência

- O conjunto de todos os subconjuntos de um conjunto A é chamado de **conjunto potência** de A, e denotado por $\mathbb{P}(A)$.
  Exemplo: Se $A = \{1,2,3\}$ então
  $\mathbb{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.
- Observe que se $A = \emptyset$ então $\mathbb{P}(A) = \{\emptyset\}$, e se $A = \{\emptyset\}$ então $\mathbb{P}(A) = \{\emptyset, \{\emptyset\}\}$.

Conjunto potência

- Se A é um conjunto finito, quanto é $\left|\mathbb{P}(A)\right|$?
- Se A é um conjunto finito, então $\left|\mathbb{P}(A)\right| = 2^{|A|}$. Por esta razão, muitos autores denotam o conjunto potência de A por 2^A.

Partição

- Seja A um conjunto, e P um conjunto cujos elementos são sub-conjuntos de A (isto é, $P \subseteq \mathbb{P}(A)$).
- Dizemos que P é uma **partição** de A se os elementos de P são não vazios, disjuntos dois a dois, e a união de todos os elementos de P é A.
- Nesse caso, cada elemento de P é também chamado de uma **parte** ou **bloco** da partição.

Exemplo: Se $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, o conjunto $P = \{\{1, 2, 5, 6, 7\}, \{3\}, \{4, 8, 10\}, \{9\}\}$ é uma partição de A.

Exercício: Quais dos conjuntos abaixo são partições do conjunto $\mathbb{Z}$ dos números inteiros?

a) $\{P, I\}$ onde P é o conjunto dos pares e I é o conjunto dos ímpares.
b) $\{\mathbb{Z}^+, \mathbb{Z}^-\}$ onde $\mathbb{Z}^+$ é o conjunto dos inteiros positivos, e $\mathbb{Z}^-$ é o conjunto dos inteiros negativos.
c) $\{R_0, R_1, R_2\}$ onde, para $i = \{0, 1, 2\}$, R_i é o conjunto dos inteiros que tem resto i na divisão por 3.
d) $\{A, B, C\}$ onde A é o conjunto dos inteiros menores que -100, B é o conjunto dos inteiros com valor absoluto menor ou igual a 100, e C é o conjunto dos inteiros maiores que 100.

Exercício: Quais dos conjuntos abaixo são partições do conjunto $\mathbb{Z}$ dos números inteiros?

e) $\{P_0, P_1, P_2, \ldots, P_9\}$, onde P_k é o conjunto de todos os inteiros cujo quadrado termina com o algarismo k. (Por exemplo, $P_6 = \{4, -4, 6, -6, 14, \ldots\}$.)
f) $\{\{0\}\} \cup \{ P_k : k \in \mathbb{N} \}$, onde P_k é o conjunto de todos os inteiros cujo valor absoluto está entre 2^k (inclusive) e 2^{k+1} (exclusive).

Produto cartesiano

- Indicamos por (a, b) um **par ordenado** de elementos, no qual a é o **primeiro elemento** e b é o **segundo elemento**.

- Um par ordenado não deve ser confundido com um conjunto de dois elementos, pois a ordem é importante (por exemplo, o par $(10, 20)$ é diferente do par $(20, 10)$) e os dois elementos podem ser iguais (como por exemplo no par $(10, 10)$).
- Dois pares ordenados (a, b) e (c, d) são iguais (são o mesmo par) se, e somente se, $a = c$ e $b = d$.

Produto cartesiano

Produto cartesiano de dois conjuntos

- Sejam A e B dois conjuntos. O **produto cartesiano**, denotado por $A \times B$, é o conjunto de todos os pares ordenados (a, b) com $a \in A$ e $b \in B$.
- Como os pares são ordenados, temos que $A \times B \neq B \times A$ (exceto quando $A = B$ ou $A = \emptyset$ ou $B = \emptyset$).

  Exercício: Quanto elementos tem o conjunto $A \times B$ se o conjunto A tem m elementos, e o conjunto B tem n?

Produto cartesiano

Produto cartesiano de vários conjuntos

- Definimos uma **ênupla ordenada**, ou simplesmente **ênupla**, como sendo uma sequência finita de m elementos $(x_1, x_2, \ldots, x_m)$.
- Observe que, como em um par ordenado, a ordem dos elementos é importante, e pode haver repetições. Assim, por exemplo, as $(10, 20, 20)$, $(10, 10, 20)$ e $(20, 10, 20)$ são três ênuplas diferentes.

- Uma ênupla com dois elementos pode ser considerada um par ordenado, e é geralmente chamada por esse nome.
- Para $m \geq 3$ usam-se os nomes **tripla**, **quádrupla**, **quíntupla**, **sêxtupla**, **séptupla**, **óctupla**, etc..
- Não há um nome especial consagrado quando $m = 1$.
- Na escrita usam-se também as notações 2-upla, 3-upla, etc., e m-upla quando m é genérico.

Produto cartesiano

Produto cartesiano de vários conjuntos

- Em particular, uma 1-upla é uma sequência (a_1) com apenas um elemento. Note que a 1-upla (10) não é a mesma coisa que o inteiro 10.
- Há uma única 0-upla, a **ênupla vazia**, denotada por $()$.
- O **produto cartesiano** de m conjuntos $A_1, A_2, \ldots, A_m$, denotado por $A_1 \times A_2 \times \cdots \times A_m$, é o conjunto das m-uplas $(a_1, a_2, \ldots, a_m)$, com $a_i \in A_i$ para $i = 1, 2, \ldots, m$.

Produto cartesiano

Produto cartesiano de conjunto consigo mesmo

- Se todos os conjuntos $A_1, A_2, \ldots, A_m$ são o mesmo conjunto, o produto cartesiano $A_1 \times A_2 \times \ldots \times A_m$ é denotado por A^m.
- Por exemplo, se $A = \{10, 20, 30\}$ temos

$$A^3 = \{(10,10,10), (10,10,20), (10,10,30), (10,20,10), \ldots, (30,30,30)\}$$

$$A^2 = \{(10,10), (10,20), (10,30), (20,10), \ldots, (30,30)\}$$

$$A^1 = \{(10), (20), (30)\}$$

$$A^0 = \{()\}$$

Intervalos

- Em matemática, um **intervalo real** ou simplesmente **intervalo** geralmente significa o conjunto de todos os números reais em $\mathbb{R}$ compreendidos entre dois valores específicos. Há quatro variações principais deste conceito:
- $(a, b) = \{x : x \in \mathbb{R} \text{ e } a < x < b\}$ (intervalo aberto),
- $[a, b] = \{x : x \in \mathbb{R} \text{ e } a \leq x \leq b\}$ (intervalo fechado),

- $(a, b] = \{x : x \in \mathbb{R} \text{ e } a < x \leq b\}$ (intervalo fechado à direita),
- $[a, b) = \{x : x \in \mathbb{R} \text{ e } a \leq x < b\}$ (intervalo fechado à esquerda),
- a e b são números reais, chamados extremos, limites ou pontas do intervalo.
- Intervalos com as formas acima são ditos **limitados**. O termo finito também é usado, embora esses conjuntos em geral tenham infinitos elementos.

Intervalos

- Também é comum usarmos intervalos **semi-infinitos** que são limitados em apenas um lado.
- $(-\infty, a) = \{x : x \in \mathbb{R} \text{ e } x < a\}$,
- $(-\infty, a] = \{x : x \in \mathbb{R} \text{ e } x \leq a\}$,
- $(a, +\infty) = \{x : x \in \mathbb{R} \text{ e } a < x\}$,
- $[a, +\infty) = \{x : x \in \mathbb{R} \text{ e } a \leq x\}$.

Intervalos

Exercício: Explique o significado das notações $[a, b]$, (a, b), $[a, b)$ e $(a, b]$ quando $a = b$ e quando $a > b$.

Exercício: Descreva os conjuntos abaixo:

1. $(-\infty, 2) \cap [-1, 3]$
2. $\overline{(0, 5]}$

Caixas

- O produto cartesiano $[10, 20] \times [2, 4]$ é um retângulo no plano cartesiano $\mathbb{R}^2$.
- O produto cartesiano $[10, 20] \times [2, 4] \times [60, 70]$ é um paralelepípedo no espaço cartesiano $\mathbb{R}^3$.

Lógica matemática

Uma **proposição** é uma sentença declarativa que ou é verdadeira ou é falsa. Exemplos:

1. **O morcego é um mamífero**.
2. **Rio de Janeiro é a capital do Brasil**.
3. **Há 36 macacos no zoológico de Londres**.
4. **A taxa de juros do Banco Central vai subir amanhã**.
5. **O trilionésimo algarismo decimal de π é 7**.

Não é necessário que saibamos se a sentença é verdadeira ou falsa.

1. Este fato pode depender de informações que não temos no momento: **Há 36 macacos no zoológico de Londres**.
2. de eventos que ainda não aconteceram: **A taxa de juros do Banco Central vai subir amanhã**.
3. ou de cálculos que não temos recursos para realizar: **O trilionésimo algarismo decimal de π é 7**.

Não são proposições:

1. frases interrogativas, como "**O que é isto?**",
2. frases imperativas, como "**Leia com cuidado**",
3. certas sentenças auto referentes, como "**Esta frase é falsa**".

Uma sentença declarativa que **depende de variáveis** pode ser considerada uma proposição em um contexto onde as variáveis **tem valor determinado**.

- "x **é menor que 3**" isoladamente não é uma proposição.
- se x for definido, ela se torna uma proposição.

Dizemos que o **valor lógico** ou **valor-verdade** de uma proposição é **verdadeiro** se ela for verdadeira, e **falso** caso contrário.

Todas as línguas naturais possuem **conectivos lógicos**, como “e”, “ou”, “não”, “se . . . então”, que permitem combinar proposições simples para formar proposições mais complexas. Por exemplo,

- [**Brasília é a capital do Brasil,**] **e** [**Montevidéu é a capital da Argentina**].
- [**Brasília é a capital do Brasil,**] **ou** [**Montevidéu é a capital da Argentina**].

- **Se** [**a taxa de juros cair amanhã**], **então** [**a inflação vai aumentar neste mês**].
- **Não** [**haverá sessão da meia-noite hoje neste cinema**].

- Uma proposição que não pode ser decomposta em proposições menores ligadas por conectivos lógicos é dita uma **proposição simples** ou **atômica**.
- O valor lógico (**verdadeiro** ou **falso**) de uma proposição deste tipo depende do valor lógico das proposições simples que a compõem, e da maneira como elas são combinadas pelos conectivos.

- se sabemos que a proposição “**Brasília é a capital do Brasil**” é verdadeira,
- e “**Montevidéu é a capital da Argentina**” é falsa,
- [**Brasília é a capital do Brasil,**] **e** [**Montevidéu é a capital da Argentina**]. É falsa.
- [**Brasília é a capital do Brasil,**] **ou** [**Montevidéu é a capital da Argentina**]. É verdadeira.

Notação para cálculo proposicional

Lógica proposicional, ou **cálculo proposicional**: Permite determinar o valor lógico de proposições compostas, se soubermos os valores lógicos das proposições simples que a compõem.

Para **eliminar as ambiguidades** das linguagens naturais iremos usar uma **notação algébrica**.

Proposições serão representadas por letras minúsculas ($p, q, r, ...$).

Podem ter dois valores:

V representando verdadeiro e **F** representando falso.

Os conectivos lógicos serão representados por sinais algébricos especiais (**operadores**) aplicados a essas variáveis. Os mais importantes são:

- **conjunção**: $p \wedge q$, significando "p e q".
- **disjunção**: $p \vee q$, significando "p ou q".
- **negação**: $\neg p$, significando "não p".
- **implicação**: $p \rightarrow q$, significando "se p, então q".
- **equivalência**: $p \leftrightarrow q$, significando "p se, e somente se, q".

Operador de conjunção

Se p, q são duas proposições, então "p e q", denotado por $p \wedge q$ também é uma proposição, chamada **conjunção** de p e q. $p \wedge q$ é verdadeiro se p e q forem verdadeiros.

p	q	$p \wedge q$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**F**

Operador de conjunção

A frase “José compra tijolos e vende casas” é uma conjunção de duas proposições atômicas, “(José compra tijolos) $\wedge$ (José vende casas).”

A palavra “e” em português tem vários sentidos diferentes.

“Maria gosta de arroz e feijão”

Não significa “(Maria gosta de arroz) e (Maria gosta de feijão)”

Mas sim “Maria gosta de arroz misturado com feijão” (uma proposição atômica).

Operador de disjunção

Se p, q são duas proposições, então “p ou q” também é uma proposição, chamada de **disjunção** de p e q.

$$p \vee q$$

É Verdadeiro se pelo menos uma das duas proposições for verdadeira. Se ambas forem falsa $p \vee q$ é falso.

Operador de disjunção

p	q	$p \vee q$
V	**V**	**V**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

Operador de disjunção

A frase “O cliente tem celular ou laptop” é uma disjunção de duas proposições atômicas, “(O cliente tem celular) $\vee$ (O cliente tem laptop)”.

Este conectivo é também chamado de “ou inclusivo”.

Operador de negação

A partir de uma proposição p, podemos formar uma nova proposição com o valor lógico oposto ao de p.

Essa nova proposição é chamada a **negação** de p e denotada por $\neg p$.

p	$\neg p$
V	**F**
F	**V**

A frase “A casa é de qualquer cor menos branca.” é uma negação, “¬(A casa é branca).”

Exercício

Uma proposição composta é **viável** ou **possível** se existe uma atribuição de valores verdades para as variáveis da proposição que a torna verdadeira. Verifique quais das proposições abaixo são viáveis.

a) $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$.

Exercício

b) $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$.

c) $(p \vee q \vee r) \wedge (p \vee \neg q \vee \neg s) \wedge (q \vee \neg r \vee s) \wedge (\neg p \vee r \vee s) \wedge (p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee s) \wedge (\neg p \vee \neg r \vee \neg s)$.

Operador de implicação

Sejam p, q duas proposições. A proposição "se p então q", que denotaremos por $p \to q$, é chamada de **implicação** ou **condicional**.

O valor lógico de $p \to q$ é falso apenas se p for verdadeiro e q for falso. Nos demais casos, o valor de $p \to q$ é verdadeiro.

Operador de implicação

p	q	$p \to q$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

Operador de implicação

Em lógica, este conectivo não pressupõe uma relação causal entre p e q.

Por exemplo a sentença:

"se 2 é par então Brasília é a capital do Brasil" é verdadeira apesar de não haver nenhuma relação conhecida entre os dois fatos.

Uma outra notação usada para este operador é $p \Rightarrow q$.

Operador de implicação

A frase "se José foi para casa, ele perdeu a reunião" contém uma implicação: "(José foi para casa) $\to$ (José perdeu a reunião)."

Operador de implicação

Muitos teoremas em matemática estão na forma de implicações:

Se determinada afirmação p (a **hipótese**, **premissa**, ou **antecedente**) é verdadeira, então outra afirmação q (a **tese**, **conclusão** ou **consequência**) também é verdadeira.

Operador de implicação

Em português, a implicação pode ser expressa de muitas outras formas:

- se p então q.
- quando p, temos q.
- caso p, vale q.
- q segue de p.
- p implica q.
- q se p.
- q sempre que p.

Operador de implicação

Em matemática, as seguintes expressões também são muito usadas para indicar a implicação $p \to q$:

- p é condição suficiente para q.
- p somente se q.
- Uma condição suficiente para q é p.
- p é uma condição mais forte que q.

Operador de implicação - Reciproca

Dizemos que a implicação

$$q \to p$$

é a **recíproca** de

$$p \to q.$$

Observe que que há casos em que $p \to q$ é verdadeira, mas sua reciproca $q \to p$ é falsa.

Operador de implicação - Inversa

A proposição $(\neg p) \rightarrow (\neg q)$ é chamada de **inversa** de $p \rightarrow q$. Observe que há casos em que $p \rightarrow q$ é verdadeira, mas sua inversa é falsa; e vice-versa

Operador de implicação - Contrapositiva

Dizemos também que proposição

$$(\neg q) \rightarrow (\neg p)$$

é a **contrapositiva** de

$$p \rightarrow q.$$

A contrapositiva tem sempre o mesmo valor lógico que a proposição $p \rightarrow q$, quaisquer que sejam os valores lógicos de p e de q.

Em vista deste resultado, a implicação $p \rightarrow q$ é frequentemente enunciada na forma contrapositiva:

- se não q, então não p.
- se q não vale, então p não vale.
- quando q é falsa, p também é falsa.
- não q implica não p.
- não p se não q.
- p é falsa sempre que q é falsa.
- q é mais fraco que p.
- q é condição necessária para p.
- Uma condição necessária para p é q.

Exercício

Encontre:

a) A contrapositiva de $\neg p \rightarrow q$.
b) A recíproca de $\neg q \rightarrow p$.
c) A inversa da recíproca de $q \rightarrow \neg p$.
d) A negação de $p \rightarrow \neg q$.
e) A recíproca de $\neg p \rightarrow q$.

Operador de equivalência

Se p, q são duas proposições, a proposição "p se, e somente se, q" é chamada de **equivalência** ou **bicondicional** de p e q.

$$p \leftrightarrow q$$

O valor lógico de $p \leftrightarrow q$ é verdadeiro quando p e q tem o mesmo valor lógico, e falso caso contrário.

Operador de equivalência

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

Operador de equivalência

A frase "a encomenda será enviada se, e somente se, o cheque tiver fundo" afirma uma equivalência lógica: "[a encomenda será enviada] $\leftrightarrow$ [o cheque tem fundo]."

Outros símbolos usados para este operador são $p \Leftrightarrow q$, $p \equiv q$, e $p = q$.

O conectivo lógico "se e somente se" também é muito usado em matemática, e pode ser expresso de várias outras maneiras; como, por exemplo:

- p é condição necessária e suficiente para q.
- as condições p e q são equivalentes.
- se p então q, e se q então p.
- p implica q, e vice-versa.

Alguns autores usam a abreviação "p sse q" (com dois "s") para significar "p se e somente se q". (em inglês iff)

Operador de disjunção exclusiva

Se p, q são duas proposições, denotamos por $p \oplus q$ a proposição "ou p ou q, mas não ambos." Este conectivo é chamado de **disjunção exclusiva** de p e q.

O valor lógico de $p \oplus q$ é verdadeiro se p e q tem valores lógicos opostos, ou seja, exatamente um deles é verdadeiro.

Operador de disjunção exclusiva

p	q	$p \oplus q$
V	**V**	**F**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

Operador de disjunção exclusiva

É importante observar que, em português, o conectivo "ou" pode significar tanto a disjunção inclusiva ($\vee$) quanto a disjunção exclusiva ($\oplus$).

"o original foi enviado pelo correio, ou pelo malote,"

"a bateria está descarregada ou o tanque está vazio"

Precedência dos operadores lógicos

Qual o valor lógico de:

$$p \vee q \wedge r$$

Podemos sempre usar parênteses para indicar a ordem correta, por exemplo $(p \vee q) \wedge r$ ou $p \vee (q \wedge r)$.

Precedência dos operadores lógicos

Operador	*Precedência*
$\neg$	1
$\wedge$	2
$\vee$,$\oplus$	3
$\rightarrow$,$\leftrightarrow$	4

Precedência dos operadores lógicos

Associatividade

Em matemática, diz-se que uma operação $\star$ é **associativa** se $(x \star y) \star z$ é igual a $x \star (y \star z)$, quaisquer que sejam x, y, e z. Nesse caso, podemos omitir os parênteses dessas duas fórmulas, e escrever simplesmente $x \star y \star z$.
A soma e a multiplicação de números reais, por exemplo, são operações associativas; enquanto que a subtração não é.

Precedência dos operadores lógicos

Dentre os conectivos lógicos que vimos até agora, $\vee$, $\wedge$, $\oplus$ e $\leftrightarrow$ são associativos. Portanto, podemos escrever $p \vee q \vee r$, $p \wedge q \wedge r$, ou $p \oplus q \oplus r$, ou $p \leftrightarrow q \leftrightarrow r$, sem risco de ambiguidade.

Por outro lado, a fórmula $p \rightarrow q \rightarrow r$ é ambígua, pois $(p \rightarrow q) \rightarrow r$ não é equivalente a $p \rightarrow (q \rightarrow r)$.

Precedência dos operadores lógicos

Normalmente avaliamos operadores de mesma precedência da esquerda para a direita. Porém é aconselhável sempre usar parênteses.

Note que esta convenção também é usada em álgebra: a fórmula $x - y - z$ deve ser entendida como $(x - y) - z$, e não como $x - (y - z)$. A mesma regra poderia ser usada para interpretar $p \oplus q \vee r$.

Afirmações auto-referentes

Já mencionamos que a afirmações que referem a si mesmas, como “esta sentença é falsa”, não são proposições lógicas. Tais afirmações, relacionadas com o Paradoxo do Barbeiro, sempre foram um problema para a lógica matemática, que não tem maneiras satisfatórias de lidar com elas.

Afirmações auto-referentes

Este problema surge mesmo quando há várias afirmações que se referenciam entre si. Por exemplo, na frase “a sentença seguinte é falsa, e a sentença anterior é verdadeira”, embora possa ser analisada como uma conjunção $p \wedge q$, não é uma afirmação lógica porque p é uma afirmação sobre q e vice-versa.

Manipulação lógica de proposições

O objetivo da lógica proposicional é identificar as deduções e transformações de proposições compostas cuja validade independe da natureza das suas proposições atômicas, e dos valores lógicos destas.

$p \wedge (p \wedge q)$ pode ser substituída por $p \wedge q$;

Tautologias e contradições

Uma **tautologia** é uma proposição composta que é sempre verdadeira, quaisquer que sejam os valores lógicos das proposições simples que a compõem.

Ou seja, uma proposição composta é uma tautologia se e somente se a coluna de resultado de sua tabela-verdade contém somente valores lógicos verdadeiros (**V**).

Tautologia

Por exemplo, a proposição $p \vee (\neg p)$ tem a seguinte tabela-verdade:

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

A tautologia mais simples é V.

Contradição

Uma **contradição** é uma proposição composta que é sempre falsa, quaisquer que sejam os valores lógicos das suas proposições atômicas.
Portanto, uma proposição composta é uma contradição se, e somente se, sua tabela-verdade contém somente **F** na sua coluna final.
É fácil ver que a proposição $p \wedge (\neg p)$ é uma contradição.

Contradição

Em particular, a negação de uma tautologia é sempre uma contradição, e a negação de uma contradição é uma tautologia.

A contradição mais simples é **F**.

Construa as tabelas-verdade das proposições abaixo, e determine se elas são tautologias, contradições, ou nem uma nem outra.

a) $(p \wedge \neg q) \rightarrow (q \vee \neg p)$.
b) $\neg p \rightarrow p$.
c) $\neg p \leftrightarrow p$.
d) $(p \wedge \neg p) \rightarrow p$.
e) $(p \wedge \neg p) \rightarrow q$.
f) $(p \wedge \neg q) \leftrightarrow (p \rightarrow q)$.
g) $((p \oplus q) \oplus (q \oplus p))$.

Equivalência lógica

Duas proposições compostas $\mathcal{P}$ e $\mathcal{Q}$ são ditas **equivalentes** se elas têm valores lógicos iguais, para quaisquer combinações de valores lógicos que sejam atribuídos às suas proposições atômicas.

Em outras palavras, $\mathcal{P}$ e $\mathcal{Q}$ são equivalentes se e somente se $\mathcal{P} \leftrightarrow \mathcal{Q}$ é uma tautologia.

Equivalência lógica

Por exemplo, podemos verificar, pela tabela-verdade, que as proposições compostas "$p \wedge (\neg q)$"e "$\neg((\neg p) \vee q)$"são equivalentes, ou seja, que $p \wedge (\neg q) \leftrightarrow \neg((\neg p) \vee q)$"é uma tautologia:

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

Equivalência lógica

Assim como a propriedade de ser tautologia ou de ser contradição, a equivalência lógica de duas proposições depende apenas da sua forma, e não depende do significado das proposições atômicas que ocorrem nela. Assim, por exemplo, a proposição $p \leftrightarrow q$ pode ser verdadeira, dependendo das proposições p e q; mas nem por isso p é logicamente equivalente a q.

Equivalência lógica

- Uma tautologia é logicamente equivalente a **V**.
- Uma contradição é logicamente equivalente a **F**.

Alguns autores escrevem usam $\Leftrightarrow$ ou $\equiv$ para dizer que p é logicamente equivalente a q, mas isso não deve ser confundido com o operador lógico.

Equivalências lógicas importantes

- **Leis de elemento identidade**:
  - $p \wedge \mathbf{V}$ equivale a p
  - $p \vee \mathbf{F}$ equivale a p
  - $p \leftrightarrow \mathbf{V}$ equivale a p
  - $p \oplus \mathbf{F}$ equivale a p
- **Leis da negação dupla**
  - $\neg(\neg p)$ equivale a p
- **Leis da idempotência**:
  - $p \wedge p$ equivale a p
  - $p \vee p$ equivale a p

- **Leis de dominação**:
  - $p \vee \mathbf{V}$ equivale a $\mathbf{V}$
  - $p \wedge \mathbf{F}$ equivale a $\mathbf{F}$
- **Leis da comutatividade**:
  - $p \vee q$ equivale a $q \vee p$
  - $p \wedge q$ equivale a $q \wedge p$
  - $p \leftrightarrow q$ equivale a $q \leftrightarrow p$
  - $p \oplus q$ equivale a $q \oplus p$
- **Leis da associatividade**:
  - $(p \vee q) \vee r$ equivale a $p \vee (q \vee r)$
  - $(p \wedge q) \wedge r$ equivale a $p \wedge (q \wedge r)$
  - $(p \leftrightarrow q) \leftrightarrow r$ equivale a $p \leftrightarrow (q \leftrightarrow r)$
  - $(p \oplus q) \oplus r$ equivale a $p \oplus (q \oplus r)$

- **Leis da distributividade**:
  - $p \vee (q \wedge r)$ equivale a $(p \vee q) \wedge (p \vee r)$
  - $p \wedge (q \vee r)$ equivale a $(p \wedge q) \vee (p \wedge r)$
  - $p \wedge (q \oplus r)$ equivale a $(p \wedge q) \oplus (p \wedge r)$
- **Leis de De Morgan**:
  - $\neg(p \wedge q)$ equivale a $\neg p \vee \neg q$
  - $\neg(p \vee q)$ equivale a $\neg p \wedge \neg q$
- **Leis da implicação**
  - $(p \rightarrow q)$ equivale a $(\neg p \vee q)$
  - $\neg(p \rightarrow q)$ equivale a $(p \wedge \neg q)$

- **Leis da equivalência**
  - $(p \leftrightarrow q)$ equivale a $(p \rightarrow q) \wedge (q \rightarrow p)$
  - $(p \leftrightarrow q)$ equivale a $\neg(p \oplus q)$
- **Lei da contrapositiva**:
  - $(p \rightarrow q)$ equivale a $(\neg q) \rightarrow (\neg p)$
- **Lei da redução ao absurdo**:
  - $p \rightarrow q$ equivale a $(p \wedge \neg q) \rightarrow \mathbf{F}$

Exercício: Verifique quais das seguintes afirmações são corretas:

1. $(\neg p \wedge (p \vee q))$ é logicamente equivalente a q.
2. $((p \rightarrow q) \rightarrow r)$ é logicamente equivalente a $(p \rightarrow (q \rightarrow r))$

Implicação entre fórmulas lógicas

- Sejam $\mathcal{F}$ e $\mathcal{G}$ duas fórmulas lógicas que dependem de uma certa coleção de variáveis lógicas. Dizemos que $\mathcal{F}$ **implica logicamente** $\mathcal{G}$ se a fórmula $\mathcal{F} \rightarrow \mathcal{G}$ é uma tautologia.
- Para qualquer combinação de valores atribuídos às variáveis que ocorrem nessas fórmulas, a proposição $\mathcal{F}$ é falsa, ou $\mathcal{F}$ e $\mathcal{G}$ são ambas verdadeiras.

- Essa afirmação é denotada $\mathcal{F} \Rightarrow \mathcal{G}$, que pode ser interpretada como "$\mathcal{G}$ é uma consequência lógica de $\mathcal{F}$"

Exemplo: Seja $\mathcal{F}$ a fórmula $p \wedge q$ e $\mathcal{G}$ a fórmula $p \vee q$. As tabelas-verdade de $\mathcal{F}$, $\mathcal{G}$ e $\mathcal{F} \rightarrow \mathcal{G}$ são

		$\mathcal{F}$	$\mathcal{G}$	$(\mathcal{F}) \rightarrow \mathcal{G})$
p	q	$p \wedge q$	$p \vee q$	$(p \wedge q) \rightarrow (p \vee q)$
V	**V**	**V**	**V**	**V**
V	**F**	**F**	**V**	**V**
F	**V**	**F**	**V**	**V**
F	**F**	**F**	**F**	**V**

Implicação entre fórmulas lógicas

Mais geralmente, sejam $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_n$ uma coleção de proposições. Dizemos que essas proposições **implicam logicamente** $\mathcal{G}$ se, e somente se,

$$(\mathcal{F}_1 \wedge \mathcal{F}_2 \wedge \cdots \wedge \mathcal{F}_n) \rightarrow \mathcal{G}$$

é uma tautologia.

Implicação lógica

Listaremos algumas implicações lógicas mais conhecidas. As letras p, q, r representam proposições arbitrárias.

- **Lei da adição**:
  - p implica logicamente $p \vee q$
- **Lei da simplificação**:
  - $p \wedge q$ implica logicamente p
- **Lei do modus ponens**:
  - p e $p \to q$ implicam logicamente q
- **Lei do modus tollens**:
  - $p \to q$ e $\neg q$ implicam logicamente $\neg p$

- **Silogismo hipotético**:
  - $p \to q$ e $q \to r$ implicam logicamente $p \to r$
- **Silogismo disjuntivo**:
  - $p \vee q$ e $\neg p$ implicam logicamente q
- **Demonstração por absurdo**:
  - $p \to \mathbf{F}$ implica logicamente $\neg p$

Equivalência em contexto específico

As fórmulas $p \leftrightarrow q$ e $p \wedge q$ não são equivalentes; pois, quando substituímos $p = \mathbf{F}$ e $q = \mathbf{F}$, a primeira é verdadeira e a segunda é falsa.

Porém, se soubermos de alguma maneira, que a afirmação $p \vee q$ é verdadeira, então a combinação $p = \mathbf{F}$ e $q = \mathbf{F}$ não pode ocorrer.

Equivalência em contexto específico

p	q	$p \leftrightarrow q$	$p \wedge q$	$p \vee q$
F	**F**	**V**	**F**	**F**
F	**V**	**F**	**F**	**V**
V	**F**	**F**	**F**	**V**
V	**V**	**V**	**V**	**V**

$p \leftrightarrow q$ é logicamente equivalente à $p \wedge q$, se $p \vee q$ for verdadeira.

Síntese de proposições

Dada uma tabela-verdade com determinadas variáveis lógicas, é sempre possível construir uma proposição composta com essas mesmas variáveis que tem essa tabela-verdade.

Escrevendo para cada linha com o resultado verdadeiro uma sub-fórmula lógica que é verdadeira para essa combinação de valores das variáveis, e falsa para todas as outras combinações.

p	q	$\mathcal{F}$
F	**F**	**F**
F	**V**	**V**
V	**F**	**V**
V	**V**	**F**

Para a linha 2, precisamos de uma sub-fórmula que seja **V** apenas quando $p = \mathbf{F}$ e $q = \mathbf{V}$. Para isso podemos usar a fórmula $(\neg p) \wedge q$. Para a linha 3, a fórmula é $p \wedge (\neg q)$. A proposição desejada é então

$$((\neg p) \wedge q) \vee (p \wedge (\neg q))$$

Forma normal disjuntiva

A sub-fórmula correspondente a cada linha com resultado **V** é uma conjunção de todas variáveis ou de suas negações. Especificamente, uma variável deve ser negada na sub-fórmula se e somente se nessa linha ela tem valor **F**.

A fórmula obtida desta maneira — uma disjunção de conjunções, cujos termos são variáveis ou suas negações — é chamada de **forma normal disjuntiva**.

Forma normal conjuntiva

Outra maneira de construir uma proposição a partir de sua tabela-verdade é considerar cada linha em que o resultado desejado é **F**, e escrever uma fórmula que é falsa apenas para essa combinação de variáveis.

Esta fórmula pode ser uma disjunção das variáveis e suas negações. A conjunção dessas fórmulas é a proposição desejada.

p	q	$\mathcal{F}$
F	**F**	**F**
F	**V**	**V**
V	**F**	**V**
V	**V**	**F**

- Primeira linha: $(p \vee q)$
- Quarta linha: $((\neg p) \vee (\neg q))$
- A formula obtida: $(p \vee q) \wedge ((\neg p) \vee (\neg q))$
- A fórmula assim obtida é chamada de **forma normal conjuntiva**.

Sistemas completos de operadores

A construção da forma normal disjuntiva (ou conjuntiva) permite concluir que toda proposição composta, usando quaisquer conectivos, é logicamente equivalente a outra proposição que usa apenas os conectivos $\vee$, $\wedge$ e $\neg$. Dizemos então que estes três conectivos formam um **sistema completo** de operadores lógicos.

Dualidade lógica

Seja p uma proposição que usa apenas os conectivos $\vee$, $\wedge$, e $\neg$. A **proposição dual** é obtida a partir de p trocando-se toda ocorrência de $\vee$ por $\wedge$, e vice-versa; bem como toda ocorrência de **V** por **F**, e vice-versa. Por exemplo, a dual da proposição $(p \wedge \neg q) \vee r$ é $(p \vee \neg q) \wedge r$. A dual de uma proposição p é geralmente denotada por p^*. Note que $(p^*)^*$, a dual da dual, é a proposição original p.

Lógica de Predicados

Proposição aberta

Uma **proposição aberta** é uma proposição que depende de uma ou mais variáveis, por exemplo

- "$x + 1$ é maior que x".
- "o quadrado de x é 16".
- "x é um número primo".
- "x é maior que y".
- "$x + y = 2x + z$"

Proposição aberta

- Em geral, o valor lógico de uma proposição aberta depende dos valores das variáveis que nela ocorrem.

Por exemplo:

- "x é maior que y" é verdadeira se os valores de x e y forem 7 e 4,
- é falsa se os valores forem 10 e 21.

Proposição aberta

Para certos valores, a frase pode até mesmo não fazer sentido: por exemplo, "x é maior que y" não faz sentido se x e y forem números complexos, ou se x for uma matriz e y for um número real.
Sempre que substituímos as variáveis de uma proposição aberta por valores aceitáveis obtemos uma **proposição fechada** que não depende de nenhuma variável — e que portanto pode ser tratada como uma proposição atômica do cálculo proposicional.

Proposição aberta

- Usaremos letras minúsculas x, y, z para denotar variáveis.
- Usaremos letras maiúsculas P, Q, R, ..., seguidas por uma lista de variáveis distintas entre parênteses, para denotar proposições abertas que dependem dessas variáveis.
- Por exemplo, a notação $P(x)$ pode representar a frase "x é um número primo", e $Q(x, y)$ pode representar "y é maior que x".

Predicados

- Os símbolos P, Q, R, ... são chamados de **predicados**
- Podem ser entendidos como funções que, dados valores das variáveis, assumem um valor lógico (**F** ou **V**).
- Como na álgebra, depois de definido um predicado $P(x_1, x_2, \ldots, x_n)$, usaremos a notação $P(v_1, v_2, \ldots, v_n)$ para indicar a substituição da variável x_1 pelo valor v_1, x_2 pelo valor v_2, etc..

Predicados

- $Q(x, y)$ foi definido como a proposição aberta "y é maior que x".
- $Q(3, z + 1)$ representa a afirmação "$z + 1$ é maior que 3"
- Supõe-se, também, que todas as ocorrências da mesma variável na proposição são substituídas pelo mesmo valor.

Quantificação universal

Outra maneira de transformar uma proposição aberta em uma fechada é usando a chamada **quantificação universal**.

Afirmações do tipo "para todo x no conjunto D, $P(x)$".

"para todo x no conjunto D, $P(x)$"
Denotaremos esta frase por $(\forall x \in D)P(x)$.
Nesta frase, D (o **domínio** da quantificação) pode ser qualquer conjunto previamente definido, x pode ser qualquer variável, e $P(x)$ qualquer proposição que depende dessa variável, que tenha valor lógico bem definido sempre que x for substituído por um elemento de D.

Por definição, a frase $(\forall x \in D)\, P(x)$ é verdadeira se, e somente se, a proposição $P(x)$ for sempre verdadeira quando substituímos variável x por qualquer elemento do conjunto D.

Se houver um (ou mais de um) elemento de D que torna $P(x)$ falsa quando atribuído à variável x, então a frase $(\forall x \in D)\, P(x)$ é falsa.

Por exemplo, se $P(x)$ representa a frase
"$x + 1$ é maior que x",
então a frase
"$(\forall x \in \mathbb{Z})\, P(x)$"
é verdadeira, pois, se substituirmos x por qualquer número inteiro, a afirmação $P(x)$ será sempre verdadeira.

Por outro lado, se $P(x)$ representa a frase

"x é um número primo",

então a frase "$(\forall x \in \mathbb{N})\, P(x)$" é falsa; pois, embora as afirmações $P(3)$ e $P(13)$ sejam verdadeiras, a afirmação $P(6)$ (por exemplo) é falsa.

Em geral, se o domínio D é um conjunto finito, com elementos $v_1, v_2, \cdots, v_n$, então a frase $(\forall x \in D)\, P(x)$ é equivalente a $P(v_1) \wedge P(v_2) \wedge \cdots \wedge P(v_n)$.

Quantificação existencial

Outra maneira de transformar uma proposição aberta em fechada é através da **quantificação existencial**, que tem a forma "existe um x no conjunto D tal que $P(x)$".
Denotaremos esta frase por $(\exists x \in D)\, P(x)$.
Aqui também, o domínio D da quantificação pode ser qualquer conjunto já definido; x pode ser qualquer variável; e $P(x)$ qualquer proposição que depende dessa variável.

Por definição, a frase "$(\exists x \in D)\, P(x)$" é verdadeira se, e somente se, existir pelo menos um elemento de D que, atribuído à variável x, torna a afirmação $P(x)$ verdadeira. A frase "$(\exists x \in D)\, P(x)$" é falsa se, e somente se, não existe nenhum elemento de D com essa propriedade.

Quantificação existencial

Se D é um conjunto finito com elementos $v_1, v_2, \cdots, v_n$, então a frase $(\exists x \in D)\, P(x)$ é equivalente a $P(v_1) \vee P(v_2) \vee \cdots \vee P(v_n)$.

Exemplo:
Denotemos por $P(x)$ o predicado "x é um número primo".

A proposição $(\exists x \in \mathbb{N})\, P(x)$ é verdadeira, pois, por exemplo, a afirmação $P(7)$ ("7 é um número primo") é verdadeira, e 7 é um elemento de $\mathbb{N}$.

Se $Q(y)$ é a proposição aberta

"y é igual a $y + 1$",

então a frase "$(\exists y \in \mathbb{R})\, Q(y)$" é falsa; pois, qualquer número real que for atribuído a y, a afirmação $Q(y)$ ("y é igual a $y + 1$") é falsa.

Quantificador de existência e unicidade

"existe um **único** x no conjunto D tal que $P(x)$."

$$(\exists! x \in D)\, P(x)$$

Quantificação sobre o conjunto vazio

A afirmação "existe um estudante com mais de duzentos anos que gosta de física" é verdadeira?

$(\exists x \in D)\, P(x)$, onde D é o conjunto dos estudantes com mais de duzentos anos de idade, e $P(x)$ denota a afirmação "x gosta de física". De modo geral, se o domínio D é vazio, a afirmação "$(\exists x \in D)\, P(x)$" é **falsa, qualquer que seja o predicado** P.

Considere agora a afirmação: "todos os estudantes com mais de duzentos anos de idade gostam de física." Qual o valor lógico desta frase?

Na notação acima, esta afirmação pode ser escrita $(\forall x \in D)\, P(x)$. A questão é: qual o valor lógico da afirmação "$P(x)$ é verdadeira, para qualquer elemento x de D", se D não tem nenhum elemento?

Dizemos que tais afirmações são **verdadeiras por vacuidade**.

Cálculo de predicados

A área da lógica que trata de predicados e quantificadores é chamada **cálculo de predicados**.

Estudam-se as regras de raciocínio que valem para **quaisquer** predicados.

Em particular, estamos interessados em **equivalências lógicas** e **implicações lógicas** entre proposições com quantificadores.

- Tautologia
  Exemplo “$(\forall x \in D)\, P(x) \vee \neg P(x)$”
- Contradição
  Exemplo, “$(\exists x \in D)\, P(x) \wedge \neg P(x)$”
- Equivalência Lógica
  Se $P \leftrightarrow Q$ é uma tautologia
- Implicação lógica
  Se $P \rightarrow Q$ é uma tautologia

- Negação de quantificadores
  - $\neg[(\forall x \in D)\, P(x)]$ é equivalente a $(\exists x \in D)\, \neg P(x)$
  - $\neg[(\exists x \in D)\, P(x)]$ é equivalente a $(\forall x \in D)\, \neg P(x)$

Cálculo de predicados

- Distributividade de quantificadores
  - $(\forall x \in D)\, (P(x) \wedge Q(x))$ equivale a $((\forall x \in D)\, P(x)) \wedge ((\forall x \in D)\, Q(x))$.
  - $(\exists x \in D)\, (P(x) \vee Q(x))$ equivale a $((\exists x \in D)\, P(x)) \vee ((\exists x \in D)\, Q(x))$.

Linguagem natural

Traduzindo linguagem natural para proposições quantificadas

- “macacos gostam de bananas."
- “**todos** os macacos gostam de bananas. ”

$$(\forall x \in M)\, B(x)$$

onde M é o conjunto dos macacos, e $B(x)$ é o predicado “x gosta de banana.”

Linguagem natural

É preciso tomar cuidado com certas frases em língua natural cujo sentido é ambíguo. Por exemplo, “um elemento x de D satisfaz $P(x)$” pode significar tanto $(\forall x \in D)\, P(x)$ quanto $(\exists x \in D)\, P(x)$.

Exercício: Escreva as afirmações abaixo na forma simbólica, definindo os predicados e os domínios dos quantificadores.

a) Todo triângulo equilátero é equiângulo.

b) Todos os estudantes gostam de física.

c) Alguns estudantes não gostam de física.

d) Cada pessoa tem uma mãe.

e) Pelo menos uma das letras da palavra **banana** é uma vogal.

Expresse, em português (e em forma simbólica), a negação de cada uma das proposições

Mudança de domínio

Podemos restringir o domínio das quantificações universais:

- As afirmações $D \subseteq E$ e $(\forall x \in E)\, P(x)$ implicam logicamente $(\forall x \in D)\, P(x)$.

“todo ruminante tem quatro patas”, e que as zebras são um subconjunto dos ruminantes, podemos concluir que “todas as zebras tem quatro patas”.

Mudança de domínio

Podemos ampliar o domínio de quantificações existenciais:

- As afirmações $D \subseteq E$ e $(\exists x \in D)\, P(x)$ implicam logicamente $(\exists x \in E)\, P(x)$.

“existe um boi preto”, e que os bois são um subconjunto dos ruminantes, podemos concluir que “existe um ruminante preto”.

- Se $D \subseteq E$, a afirmação $(\forall x \in D)\, P(x)$ é logicamente equivalente a $(\forall x \in E)\, (x \in D \to P(x))$.
- Se $D \subseteq E$, a afirmação $(\exists x \in D)\, P(x)$ é logicamente equivalente a $(\exists x \in E)\, (x \in D \wedge P(x))$.

"todo papagaio tem um bico" equivale a dizer "todo animal, se for um papagaio, tem um bico;"

"existe um papagaio amarelo" equivale a dizer que "existe um animal que é papagaio e é amarelo."

Erro comum: confundir as duas regras, e mudar o domínio do quantificador universal com $\wedge$ ao invés de $\to$.

- "todo macaco gosta de banana"

$$(\forall x \in A)\, (x \in M) \wedge B(x) \quad \textit{ERRADO}!$$

Onde A é o conjunto dos animais, M é o conjunto dos macacos, e $B(x)$ significa "x gosta de banana".

- na verdade quer dizer: "todo animal é macaco e gosta de banana"

- "existe um macaco que voa"

$$(\exists x \in A)\, (x \in M) \to V(x) \quad \textit{ERRADO}!$$

Onde A é o conjunto dos animais, M é o conjunto dos macacos, e $V(x)$ significa "x voa".

- na verdade quer dizer: "existe um animal que, se for macaco, voa"

Esta afirmação é verdadeira, pois basta considerar um x em $A \setminus M$ (um animal que não é macaco) e a frase $(x \in M) \to V(x)$ fica $\mathbf{F} \to V(x)$ e portanto verdadeira.

Quantificadores múltiplos

Se uma proposição aberta menciona mais de uma variável, é preciso mais de um quantificador — um para cada variável distinta — para transformá-la numa proposição fechada. Por exemplo, se escolhermos $\mathbb{Z}$ como o domínio, há oito maneiras de transformar a afirmação aberta "$x + y = 2x$" em uma proposição fechada:

$$\begin{array}{ll} (\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})\, x + y = 2x & (\forall y \in \mathbb{Z})(\forall x \in \mathbb{Z})\, x + y = 2x \\ (\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})\, x + y = 2x & (\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z})\, x + y = 2x \\ (\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})\, x + y = 2x & (\forall y \in \mathbb{Z})(\exists x \in \mathbb{Z})\, x + y = 2x \\ (\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})\, x + y = 2x & (\exists y \in \mathbb{Z})(\exists x \in \mathbb{Z})\, x + y = 2x \end{array}$$

- $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})\ x + y = 2x$
  - "para todo inteiro x, existe um inteiro y (que pode ser diferente para cada x!) tal que $x + y = 2x$".
  - Esta afirmação é verdadeira.
- $(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z})\ x + y = 2x$
  - "existe um inteiro y tal que, para todo inteiro x (e esse mesmo y!), $x + y = 2x$".
  - Esta frase é falsa.
  - Como $x + y = 2x$ é o mesmo que $y = x$, ela equivale a dizer que "existe um inteiro y que é igual a todos os inteiros".

De modo geral, sempre podemos trocar a ordem de dois quantificadores do mesmo tipo (ambos $\forall$, ou ambos $\exists$). Ou seja, para quaiquer variáveis, domínios e predicados,

- A fórmula $(\forall x \in D)(\forall y \in E)\ P(x, y)$ é logicamente equivalente a $(\forall y \in E)(\forall x \in D)\ P(x, y)$
- A fórmula $(\exists x \in D)(\exists y \in E)\ P(x, y)$ é logicamente equivalente a $(\exists y \in E)(\exists x \in D)\ P(x, y)$

Quando um quantificador sobre uma variável é aplicado dizemos que cada ocorrência dessa variável está **amarrada**. Todas as demais variáveis que ocorrem na proposição continuam **livres**.

Por exemplo, na fórmula $(\forall x \in \mathbb{R})\ x^2 + x - y > z/(x + y)$, as três ocorrências de x em $x^2 + x - y > z/(x + y)$ estão amarradas.

Enquanto houver variáveis livres, a fórmula continua sendo uma proposição aberta.

Escopo de um quantificador

- A parte da fórmula onde um quantificador tem efeito é chamada de **escopo** do quantificador.
- É toda a parte da fórmula que segue ao quantificador; mas podemos usar parênteses para limitar esse escopo.

- $((\forall x \in D)\, P(x)) \wedge ((\exists x \in E)\, Q(x)) \vee R(x)$
- o escopo do primeiro quantificador é apenas $P(x)$, o do segundo quantificador é $Q(x)$
- e a fórmula $R(x)$ está fora do escopo de ambos — ou seja, a ocorrência de x em $R(x)$ ainda está livre.

Omissão do domínio

O domínio da quantificação pode ser omitido em dois casos:

- Todos os quantificadores tiverem o mesmo domínio D, podemos anunciar esse fato no início, e escrever apenas $(\forall x)\, P(x)$ ou $(\exists x)\, P(x)$, em vez de $(\forall x \in D)\, P(x)$ ou $(\exists x \in D)\, P(x)$.

- Se supõem que existe um **conjunto universal** U cujos elementos são todos os elementos de todos os conjuntos que podem vir a ser usados em quantificadores. Nesse caso, podemos usar equivalências para trocar qualquer domínio D pelo domínio universal U:
  - $(\forall x \in D)\, P(x)$ equivale a $(\forall x \in U)\, (x \in D) \rightarrow P(x)$.
  - $(\exists x \in D)\, P(x)$ equivale a $(\exists x \in U)\, (x \in D) \wedge P(x)$.
- em vez de $(\forall x \in D)\, P(x)$, pode-se escrever $(\forall x)\, (x \in D) \rightarrow P(x)$.
- em vez de $(\exists x \in D)\, P(x)$, pode-se escrever $(\exists x)\, (x \in D) \wedge P(x)$.

Métodos de Demonstração

Métodos de Demonstração

- **Demonstrações** são instrumentos usados por uma pessoa para convencer outras pessoas (ou a si mesma) de que uma afirmação é verdadeira.
- Toda demonstração precisa partir de
  - definições e afirmações básicas, chamadas **axiomas** ou **postulados** e
  - afirmações que foram previamente demonstradas.

- Para ser convincente, uma demonstração somente pode usar afirmações e regras de raciocínio que as duas partes consideram válidas.
  - equivalências e implicações lógicas.
  - regras de manipulação de fórmulas da álgebra e da teoria de conjuntos.

- Uma afirmação devidamente demonstrada é chamada de **teorema**
  - expressão grega que significa “verdade dos Deuses”.
- Um teorema que é demonstrado apenas para ajudar na prova de um outro teorema é chamado de **lema**.
- Um **corolário** de um teorema é outro teorema que é consequência do primeiro, e cuja demonstração é relativamente simples.

Definições

Uma demonstração também pode usar **definições**.

- Uma definição precisa ser **completa**, isto é, deve especificar todas as propriedades que identificam exatamente o conceito definido.
- Deve ser também **precisa**, de modo que o leitor não tenha dúvidas sobre seu significado.

- Por convenção, o termo definido é enfatizado por ocasião de sua definição. Por exemplo:

Definição 4.1: Um inteiro n é um **múltiplo** de um inteiro p se, e somente se, existe um inteiro q tal que $n = pq$.

Definição 4.1: Um inteiro n é um **múltiplo** de um inteiro p se, e somente se, existe um inteiro q tal que $n = pq$.

- Esta definição não deixa dúvidas: para quaisquer inteiros n e p, ela permite ao leitor decidir se n é ou não múltiplo de p.

- Criamos um novo predicado “é multiplo de”, em notação formal, podemos denotar por M.
- Então $M(n, p)$ é lido “n é multiplo de p”.
- a parte que vem depois do “se, e somente se” seria escrita formalmente “$(\exists q \in \mathbb{Z})\ n = pq$”.
- Depois de enunciarmos essa definição então, podemos tratar a fórmula abaixo como um axioma

$$(\forall n, p \in \mathbb{Z})\ M(n, p) \leftrightarrow (\exists q \in \mathbb{Z})\ n = pq$$

- Ou ainda supor que $M(n, p)$ é logicamente equivalente a $(\exists q \in \mathbb{Z})\ n = pq$

- O número π é um múltiplo de $\sqrt{17}$?
- essa frase não tem sentido: ela não é nem verdadeira nem falsa, e portanto não é uma proposição lógica (enquanto o conceito de “múltiplo” não for definido para números reais)

- Uma vez que um conceito foi definido, ele pode ser usado em outras definições:
  Definição 4.2: Um inteiro p **divide** um inteiro n (é um **divisor** de n) se, e somente se, n é múltiplo de p.
- Esta definição introduz um predicado "é divisor de" em termos do predicado "é multiplo de". Formalmente podemos denotar esse predicado por D e introduzir o axioma:

$$(\forall n, p \in \mathbb{Z})\, D(p, n) \leftrightarrow M(n, p)$$

$$(\forall n, p \in \mathbb{Z})\, D(p, n) \leftrightarrow M(n, p)$$

Observe o uso do conectivo lógico "se e somente se" ($\leftrightarrow$) nestas definições. Este conectivo permite ao leitor decidir se uma entidade qualquer do domínio se enquadra **ou não** na definição.

- Portanto toda definição é se e somente se.

É comum encontrar definições que usam apenas a palavra "se" quando o autor na verdade quer dizer "se e somente se". Ou ainda outras que não usam nenhuma delas. Por exemplo:

- **Definição 4.3:** Um inteiro n é **par** se ele é múltiplo de 2.
- **Definição 4.4:** Se um inteiro não é par, dizemos que ele é **ímpar**.
- **Definição 4.5:** Um **número primo** é um número inteiro maior que 1, que não tem nenhum divisor exceto 1 e ele mesmo.

Conjecturas

- Uma **conjectura** (ou **conjetura**) é uma afirmação para a qual ainda não existe prova. Em geral, este termo é usado quando se suspeita que a afirmação seja verdadeira.
- Se uma conjetura é finalmente demonstrada, ela se torna um teorema.

- Por outro lado, se for encontrada uma demonstração da negação da conjetura, dizemos que a mesma foi **refutada**.
- Enquanto nenhuma das duas coisas ocorre, diz-se que a conjetura continua **aberta**.

Conjectura de Fermat

Um exemplo famoso é a **conjectura de Fermat**:

- "se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas."
- Foi encontrada em um livro que pertenceu ao matemático Pierre de Fermat (1601–1665).

"se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas."

- Escreveu na margem "tenho uma linda demonstração, mas ela não cabe nesta margem."
- Apesar de inúmeros esforços por matemáticos de todo o mundo, a afirmação permaneceu como conjetura por mais de 300 anos.

- Em 1995, finalmente, o matemático inglês Andrew Wiles publicou uma demonstração com mais de 200 páginas.
- Hoje a conjetura é conhecida como **o último teorema de Fermat**.

Conjetura das quatro cores

Outro exemplo famoso é a **conjetura das quatro cores**:

- "todo mapa pode ser pintado com no máximo quatro cores, de modo que regiões vizinhas tenham cores diferentes."
- Enunciada em 1852 por Francis Guthrie (1831–1899).

- Foi provada em 1976 por Kenneth Appel e Wolfgang Haken, utilizando um computador.
- Em 1994 foi produzida uma prova simplificada por Paul Seymour, Neil Robertson, Daniel Sanders e Robin Thomas, mas ainda utilizando um computador.

- Há várias conjeturas famosas que ainda estão abertas. A **conjetura de Goldbach**, formulada pelo matemático alemão Christian Goldbach em 1742.
- **todo número inteiro par maior que 2 é a soma de dois números primos.**
- Testes com computadores mostram que esta afirmação é verdadeira para todos os inteiros pares entre 4 e 4×10^{18};
- mas obviamente estes testes não constituem uma prova.

- O monge e matemático francês Marin Mersenne (1585–1648) investigou os números $M_n = 2^n - 1$, onde n é um número primo.
- Ele observou que os números $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, e $M_7 = 127$ são primos; mas o número seguinte, $M_{11} = 2047$, não é primo ($2047 = 23 \times 89$).
- Ele conjecturou que M_n é primo para todo n em $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$

M_n é primo para todo n em $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$

- Em 1876 Edouard Lucas (1842–1891) provou que $M_{67} = 2^{67} - 1$ não era primo, e portanto a conjetura de Mersenne era falsa.
- Entretanto, sua prova não exibia os fatores de M_{67}, apenas provava que eles existiam.
- Em 1903, Frank Nelson Cole (1861–1926) apresentou uma palesta em uma conferência de matemática, com o título vago **On the Factorisation of Large Numbers**.

- Sem dizer nada, Cole primeiro escreveu $2^{67} - 1$ no quadro negro, e fez os cálculos à mão, obtendo o valor 147573952589676412927.
- Na outra metade do quadro, ele escreveu o produto $193707721 \times 761838257287$, e fez a multiplicação à mão, obtendo o mesmo resultado, e a plateia aplaudiu de pé.
- Depois ele contou que tinha levado três anos, trabalhando todos os domingos, para encontrar essa fatoração.

Métodos de demonstração

- Existem teoremas que tem muitas demonstrações diferentes.
- Qual é a melhor é, até certo ponto, uma questão de gosto, e depende para quem a demonstração é dirigida.

- Em geral, quanto mais curta a prova, melhor;
- mas há outros critérios, como a facilidade de compreensão, a simplicidade dos passos, etc..
- Para convencer outras pessoas, devemos cuidar para que a demonstração seja, além de correta, também simples, clara e objetiva, tanto quanto possível.

Demonstração de implicações

- Muitas vezes temos que provar implicações da forma $p \to q$,
- **se** p é verdadeira, **então** q também é.
- A afirmação p é chamada de **hipótese**, **premissa** ou **condição**.
- A afirmação q é chamada de **tese** ou **conclusão**.

Método direto

- Supomos que a hipótese p é verdadeira.
- Usamos uma sequência de proposições que são consequências lógicas das anteriores,
- até obter a tese q.
- Esta sequência de passos prova a implicação $p \to q$.

Teorema 4.1: Se m e n são inteiros pares, então $m + n$ é par.
Prova:

1. Suponha que m é par. (Hipótese.)
2. Suponha que n é par. (Hipótese.)
3. Existe um inteiro r tal que $m = 2r$. (Definição de "par").
4. Existe um inteiro s tal que $n = 2s$. (Definição de "par").
5. $m + n = 2r + 2s = 2(r + s)$. (De 3 e 4, por álgebra.)
6. Seja $t = r + s$. (Introdução de variável.)
7. Existe um inteiro t tal que $m + n = 2t$. (De 6.)
8. $m + n$ é par. (Definição de "par", dada 6. Tese.)

Fim.

- Cada um dos passos da prova é um raciocínio simples o bastante para ser aceito como válido pelo leitor.
- Cada passo deveria ser uma aplicação de uma **regra de inferência**, tirada de uma lista fixa de regras que todos aceitam como válidas e fundamentais.
- Uma das regras comumente aceitas, por exemplo, é a regra de **modus ponens**
  - se já demonstramos que uma proposição p é verdade,
  - e que $p \to q$,
  - então podemos considerar a proposição q demonstrada

Na prática, os passos são escritos mais abreviados:
Teorema 4.1: Se m e n são inteiros pares, então $m + n$ é par.
Prova:
Suponha que m e n são inteiros pares. Por definição de número "par", existem inteiros r e s tais que $m = 2r$ e $n = 2s$. Logo $m + n = 2r + 2s = 2(r + s)$. Como $r + s$ é inteiro, concluímos que o inteiro $m + n$ é par, pela definição. Isto prova que, se m e n são pares, $m + n$ é par.
Fim

Exercícios

- Demonstre que o produto de um inteiro par por um inteiro ímpar é par.
- Demonstre que se r é um número racional diferente de zero, então $\frac{1}{r}$ é racional.
- Demonstre que, para quaisquer conjuntos A, B, C e D, as seguintes afirmações são sempre verdadeiras
  - Se $x \in A$, $(A \setminus B) \subseteq (C \cap D)$ e $x \notin D$, então $x \in B$.
  - Se B e C são disjuntos, $A \subseteq C$ e $x \in A$, então $x \notin B$.
  - Se $x \in C$ e $(A \cap C) \subseteq B$, então $x \notin (A \setminus B)$.

Método da contrapositiva

Demonstração de implicações

- Queremos provar que $p \rightarrow q$.
- Supomos que a negação da tese $\neg q$ é verdadeira.
- Procuramos uma sequência de deduções lógicas que termina com a negação da hipótese $\neg p$.
- Ou seja, provamos que $(\neg q) \rightarrow (\neg p)$.
- esta afirmação é logicamente equivalente a $p \rightarrow q$, que portanto também está provada.

Teorema 4.2: Se n^2 é um inteiro par, então n é par.
Prova:
Suponha que n é ímpar. Pela definição de "ímpar", existe um inteiro k tal que $n = 2k + 1$. Portanto $n^2 = (2k + 1)^2$ $= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Como $2k^2 + 2k$ é um inteiro, pela definição de "ímpar" concluímos que n^2 é impar.
Pela regra da contrapositiva, isto prova que, se n^2 é um inteiro par, então n é um inteiro par.
Fim.

- Demonstre que, para todo inteiro n, se $n^3 + 5$ é impar, então n é par.

Dica: $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Método de redução ao absurdo

- Também chamado de **prova indireta** ou **por contradição**
- Baseia-se na equivalência lógica entre a fórmula $(p \rightarrow q)$ e a fórmula $(p \wedge \neg q) \rightarrow \mathbf{F}$

- Queremos mostrar que $p \rightarrow q$
- Supomos que tanto a hipótese p quanto a **negação** da tese $\neg q$ são verdadeiras
- Procuramos uma sequência de deduções lógicas que termina com uma contradição (uma afirmação com valor lógico **F**).
- Isto prova a afirmação $(p \wedge \neg q) \rightarrow \mathbf{F}$, e portanto também a afirmação equivalente a $p \rightarrow q$.

Teorema 4.3: Se m e n são inteiros pares, então $m + n$ é um inteiro par.
Prova:
Suponhamos que m e n são inteiros pares e $m + n$ é um inteiro ímpar; e isso leva a uma contradição.
Por definição existem r e s inteiros tais que $m = 2r$ e $n = 2s$. Pela definição de "ímpar", existe um inteiro j tal que $m + n = 2j + 1$.
Logo $2r + 2s = 2j + 1$, ou seja, $r + s - j = 1/2$. Isto é falso pois $r + s - j$ é um inteiro.
Esta contradição prova que, se m e n são inteiros pares, $m + n$ é um inteiro par. **Fim.**

Exercícios

1. Demonstre que a soma de um número racional com um número irracional é um número irracional.
2. Demonstre que o número $\sqrt{2}$ é irracional.
3. Sejam x, y, z números reais. Demonstre que pelo menos um deles é maior ou igual à média aritmética dos três.

Implicação com tese conjuntiva

- Queremos provar que $p \rightarrow (q \wedge r)$
- Que é logicamente equivalente à $(p \rightarrow q) \wedge (p \rightarrow r)$
- Basta provar cada uma separadamente.

Teorema 4.4: Se 6 divide um inteiro n, então 2 divide n e 3 divide n.
Prova:
Se 6 divide n então existe um inteiro k tal que $n = 6k$. Então, $n = 2(3k)$, logo 2 divide n. Temos também que $n = 3(2k)$, logo 3 divide n. Portanto 2 divide n e 3 divide n.
Fim.

Implicação com hipótese disjuntiva

- Queremos provar $(p \vee q) \rightarrow r$
- Equivale à $(p \rightarrow r) \vee (q \rightarrow r)$
- Basta provar cada uma dessas partes.

Teorema 4.5: Para quaisquer inteiros m e n, se m for par ou n for par, então mn é par.

Prova:

Sejam m e n inteiros quaisquer. Temos dois casos:

- Caso 1: m é par. Pela definição, existe um inteiro q tal que $m = 2q$. Nesse caso, $mn = (2q)n = 2(nq)$, e portanto mn é par.
- Caso 2: n é par. Pela definição, existe um inteiro r tal que $n = 2r$. Nesse caso $mn = m(2r) = 2(mr)$, e portanto mn é par.

Portanto, se m é par ou n é par, mn é par. **Fim.**

Demonstrações de afirmações “se e somente se”

Outro tipo comum de teorema tem a forma $p \leftrightarrow q$, ou seja, “p vale se e somente se q vale.”

- Equivalente à $(p \rightarrow q) \wedge (q \rightarrow p)$
- Dividimos a demostração em duas partes.
  - (1) prova que $p \rightarrow q$ (ida);
  - (2) prova que $q \rightarrow p$ (volta);

Teorema 4.7: Os inteiros x e y são ambos ímpares se, e somente se, o produto xy é ímpar.

Prova:

Sejam x e y inteiros quaisquer.

- Parte (1) ($\rightarrow$): provaremos que, se x e y são ímpares, então xy é ímpar.Se x e y são ímpares, por definição existem inteiros r e s tais que $x = 2r + 1$ e $y = 2s + 1$. Portanto $xy = (2r + 1)(2s + 1) = 2(rs + r + s) + 1$. Como $rs + r + s$ é um inteiro, concluímos que xy é ímpar.

- Parte (2) ($\leftarrow$): provaremos que, se xy é ímpar, então x e y são ambos ímpares. Ou seja (pela contrapositiva), que se x é par ou y é par, então xy é par. Temos dois casos (não exclusivos):
  - Caso (a): x é par. Neste caso existe um inteiro r tal que $x = 2r$. Portanto $xy = (2r)y = 2(ry)$. Como ry é inteiro, concluímos que xy é par.
  - Caso (b): y é par. Então existe um inteiro s tal que $y = 2s$. Portanto $xy = x(2s) = 2(xs)$. Como xs é inteiro, concluímos que xy é par.

Fim.

Regras para quantificadores universais

Instanciação universal

- Se provarmos que $(\forall x \in D)\, P(x)$,
- podemos afirmar $P(c)$ para qualquer elemento c do domínio D.
- "para todo inteiro x maior que 5, $2^x > x^2$", podemos imediatamente concluir que $2^{418} > 418^2$.
- Esta regra é chamada de **instanciação universal**.

Generalização universal

- Agora suponha que desejamos provar $(\forall x \in D)\, P(x)$
- começar supondo que x é um elemento de D escolhido arbitrariamente
- Se, com essa suposição, conseguirmos provar a afirmação $P(x)$, provamos que o teorema original é verdadeiro.
- Este último passo é chamado de **generalização universal** ou **suspensão do quantificador universal**.

Teorema 4.10: Para quaisquer números reais x e y, $(x+y)^2 - (x-y)^2 = 4xy$.
Prova:
Sejam x e y dois números reais quaisquer.
Pelo teorema do binômio, temos $(x+y)^2 = x^2 + 2xy + y^2$, e $(x-y)^2 = x^2 - 2xy + y^2$. Portanto,
$(x+y)^2 - (x-y)^2 = (x^2 + 2xy + y^2) - (x^2 - 2xy + y^2) = 4xy$.
Fim.

Demonstração por vacuidade

Lembre-se que se E é o conjunto vazio, a afirmação $(\forall x \in E)\, Q(x)$ é verdadeira, qualquer que seja o predicado Q.
Esta afirmação é verdadeira **por vacuidade**.

- Queremos demostrar $(\forall x \in D)\, P(x)$ para um domínio arbitrário D.
- Mostrar que ela é equivalente a outra afirmação $(\forall x \in E)\, Q(x)$
- Então mostrar que E é vazio.

Teorema: Para todo número inteiro x, se $x^2 = 5$ então x é par.

- $(\forall x \in \mathbb{Z})\, Q(x) \rightarrow P(x)$
- $Q(x)$ significa "$x^2 = 5$", e $P(x)$ é "x é par".
- $E = \{\forall x \in \mathbb{Z} : Q(x)\}$
- equivale à $(\forall x \in E)\, P(x)$.
- ou seja, E é o conjunto dos inteiros cujo quadrado é 5.
- Como E é vazio, a afirmação é verdadeira por vacuidade.

Regras para quantificadores existenciais

- Se provamos que $(\exists x \in D)\, P(x)$,
- podemos supor, dali em diante, que a variável x é um dos elementos cuja existência é afirmada.
- Esta regra é chamada de **instanciação existencial**.
- Exemplo: Considere as seguintes premissas: "Um aluno desse curso não estudou" e "Todos os alunos desse curso foram aprovados" podemos concluir que "Algum aluno não estudou e foi aprovado".

Demonstrações construtivas

- Agora suponha que queremos provar que $(\exists x \in D)\, P(x)$.
- Exibimos um elemento específico a do domínio D (explicitamente, ou através de uma construção algorítmica)
- $P(a)$ é verdadeira, para esse elemento.
- **Demonstração construtiva**

Demonstrações construtivas

Teorema 4.11: Existem três números inteiros positivos tais que $x^2 + y^2 = z^2$.
Prova:
Sejam $x = 3$, $y = 4$, e $z = 5$. Como
$x^2 + y^2 = 3^2 + 4^2 = 25 = 5^2 = z^2$, a afirmação é verdadeira.
Fim.

Teorema do deserto de primos: Para todo número inteiro positivo n, existe uma sequência de n números inteiros consecutivos que não são primos.

Prova: Seja n um inteiro positivo, e seja $x = (n+1)! + 2$.
Observe que

$$\begin{aligned} 2 \text{ divide } x &= (n+1)! + 2, && (2)\\ 3 \text{ divide } x+1 &= (n+1)! + 3, && (3)\\ &\dots && (4)\\ n+1 \text{ divide } x+(n-1) &= (n+1)! + n + 1. && (5) \end{aligned}$$

Logo todos os inteiros $x + i$ com $0 \leq i < n$ são não primos; e eles formam uma sequência de n inteiros consecutivos.
Fim.

Exercício:

- Existem 100 inteiros consecutivos que não são quadrados perfeitos.

Demonstrações não construtivas

- Em alguns casos, é possível demonstrar a existência de um elemento que satisfaz uma dada condição mesmo sem exibir explicitamente tal elemento.
- Uma demonstração deste tipo é chamada de **demonstração não construtiva**

Teorema 4.14: Existem dois números reais irracionais x e y tais que x^y é racional.
Prova:
Sabemos que número $\sqrt{2}$ é irracional. Se $(\sqrt{2})^{\sqrt{2}}$ for racional, a afirmação está satisfeita tomando-se $x = \sqrt{2}$ e $y = \sqrt{2}$. Por outro lado, se $(\sqrt{2})^{\sqrt{2}}$ for irracional, podemos tomar $x = (\sqrt{2})^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$ que é racional.
Fim.

Demonstração de existência e unicidade

- Queremos provar $(\exists! x \in D)\, P(x)$
- Logicamente equivalente à

$$((\exists x \in D)\, P(x)) \wedge ((\forall x \in D)(\forall y \in D)\, ((P(x) \wedge P(y)) \rightarrow x = y))$$

Portanto, uma demonstração de existência e unicidade pode ser dividida em duas partes:

- **Existência:** prova-se-se que existe pelo menos um x em D que satisfaz $P(x)$.
- **Unicidade:** supõe-se que y também é um elemento de D que satisfaz $P(y)$, e prova-se que ele é igual ao x.

Teorema: Mostre que se a e b são números reais e $a \neq 0$, então existe um único número real r tal que $ar + b = 0$
Prova: Note que o número real $r = -b/a$ é uma solução para $ar + b = 0$. Suponha então que s é um número real, tal que $as + b = 0$. Então $ar + b = as + b$. Subtraindo b dos dois lados e dividindo por a (que é diferente de 0), encontramos que $r = s$.

Demonstração de falsidade por contra-exemplo

- Demonstrações de existência são usadas, em particular, para refutar conjeturas da forma $(\forall x \in D)\, P(x)$; pois a negação desta afirmação é $(\exists x \in D)\, \neg P(x)$.
- Neste caso dizemos que o elemento x de D que comprovadamente não satisfaz $P(x)$.
- Portanto mostra a falsidade da conjetura

Considere a seguinte afirmação: “Para todo primo n, o inteiro $2^n - 1$ é primo.” Esta afirmação não é verdadeira, basta ver que o número $n = 11$ é um contra-exemplo, pois
$P(11) = 2^{11} - 1 = 2047 = 23 \times 89$.

Exercícios:
Demonstre (por meio de contra-exemplos) que as seguintes conjeturas são falsas:

- Todo inteiro positivo é soma dos quadrados de três inteiros.
- Se n é um número inteiro e $4n$ é par, então n é par.
- O produto de dois números irracionais é um número irracional.

Prove (ou mostre contra exemplos) de que as seguintes proposições são equivalentes

a) $(\forall x \in D)\, P(x) \vee Q(x)$ e $((\forall x \in D)\, P(x)) \vee ((\forall x \in D)\, Q(x))$.
b) $(\exists x \in D)\, P(x) \wedge Q(x)$ e $((\exists x \in D)\, P(x)) \wedge ((\exists x \in D)\, Q(x))$.

Indução Matemática

- Seja $P(n)$ uma sentença matemática que depende de uma variável natural n
- se torna verdadeira ou falsa quando substituimos n por um número natural dado qualquer
- Estas sentenças são chamadas **sentenças abertas definidas sobre o conjunto dos números naturais** $\mathbb{N}$.

1. $P(n)$: "n é ímpar." Observe que esta afirmação é verdadeira para alguns valores de n e falsa para outros.
2. $P(n)$: "$n^2 - n + 41$ é um número primo." Neste exemplo podemos verificar, não tão facilmente, que $P(1), P(2), \ldots, P(40)$ são verdadeiros mas $P(41) = 41^2$ é falso.

3. $P(n)$: "$2n + 6$ é par." É fácil ver que $2n + 6 = 2(n + 3)$ para qualquer n, portanto $P(n)$ é verdade para todo n.
4. $P(n)$: "$1 + 3 + 5 + \cdots + (2n - 1) = n^2$." Será que conseguiremos encontrar algum m tal que $P(m)$ seja falso?

Como mostrar que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

é verdade para qualquer n?

Princípio de Indução Matemática

O **princípio da indução matemática** (PIM) é a principal ferramenta para demonstrar sentenças da forma "$(\forall n \in \mathbb{N})\ P(n)$". Ele diz o seguinte:

Axioma: Seja $P(n)$ uma sentença aberta sobre $\mathbb{N}$. Suponha que:

1. $P(0)$ é verdade, e
2. Sempre que $P(k)$ é verdade, para algum $k \in \mathbb{N}$, temos que $P(k+1)$ é verdade.

Então $P(n)$ é verdade para todo $n \in \mathbb{N}$.

Para demonstrar uma afirmação "$(\forall n \in \mathbb{N})\ P(n)$" usando o PIM, podemos então seguir este roteiro:

- **Base da Indução**: Provar que $P(0)$ é verdade.
- **Hipótese de Indução**: Supor que para algum $k \in \mathbb{N}$, $P(k)$ é verdade.
- **Passo da Indução**: Provar que $P(k+1)$ é verdade.

Exemplo

Provar que, para todo $n \geq 0$:

$$1 + 3 + 5 + \cdots + (2n-1) = (n)^2$$

Prova: Vamos provar usando indução em n.

- **Base**: $P(0)$ é verdade pois a expressão acima é trivialmente válida para $n = 0$.
- **Hipótese de indução**: suponhamos que para algum k, $P(k)$ é verdade, isto é,

$$1 + 3 + 5 + \cdots + (2k-1) = (k)^2$$

.

Passo de indução: temos de provar que $P(k+1)$ é verdade, isto é temos que provar que:

$$1 + 3 + 5 + \cdots + (2k-1) + (2(k+1)-1) = (k+1)^2$$

Pela hipótese de indução, temos

$$\begin{aligned}
[1 + 3 + 5 + \cdots + (2k-1)] + (2(k+1)-1) &= \\
[k^2] + (2(k+1)-1) &= \\
k^2 + 2k + 2 - 1 &= \\
k^2 + 2k + 1 &= \\
(k+1)^2 &
\end{aligned}$$

Exemplo 2

Definição: Dizemos que um conjunto de n retas no plano **estão em posição geral** se não possui duas retas paralelas e nem três retas se interceptando num mesmo ponto.

Teorema

Um conjunto de n retas em posição geral divide o plano em $R_n = \frac{n(n+1)}{2} + 1$ *regiões.*

Vamos provar por indução no número n retas de retas.

- **Base**: Para $n = 0$ temos apenas uma região. Como $R_0 = 0(0+1)/2 + 1 = 1$, a fórmula é válida neste caso.
- **Hipótese de indução**: Suponhamos que para algum k a fórmula é válida, isto é quaisquer k retas em posição geral dividem o plano em $R_k = k(k+1)/2 + 1$ regiões.

Passo da indução: temos que provar que quaisquer $k+1$ retas em posição geral definem $R_{k+1} = (k+1)(k+2)/2 + 1$ regiões. Sejam $L_1, L_2, \ldots, L_{k+1}$ essas retas. Compare as regiões do plano definidas por elas, que chamaremos de **regiões novas**, com as **regiões velhas** definidas pelas primeiras k dessas retas. Observe que algumas das regiões velhas são divididas pela última reta L_{k+1}, cada uma delas formando duas regiões novas; enquanto que as demais regiões velhas são também regiões novas.

Como as retas estão em posição geral, a reta L_{k+1} cruza cada uma das k retas anteriores em k pontos distintos. Em cada um desses cruzamentos, a reta L_{k+1} passa de uma região velha para outra. Essas regiões são duas a duas distintas porque estão em lados opostos de alguma reta L_i, com $1 \leq i \leq k$. Portanto a reta L_{k+1} corta $k+1$ regiões velhas, que dão origem a $2(k+1)$ regiões novas. Ou seja,

$$R_{k+1} = R_k - (k+1) + 2(k+1) = R_k + (k+1)$$

Como as retas $L_1, L_2, \ldots, L_k$ estão em posição geral, podemos usar a hipótese de indução. Obtemos

$$R_k + (k+1) = k(k+1)/2 + 1 + k + 1 =$$

$$(k+1)(k+2)/2 + 1.$$

Generalizações da Indução Matemática

Há muitas variações do princípio da indução matemática, que são no fundo equivalentes, mas podem tornar algumas demonstrações mais simples.
Muitas vezes precisamos provar que uma sentença aberta $P(n)$ vale para todos os números naturais maiores ou iguais a um certo n_0; ou seja, que "$(\forall n \in \mathbb{N})\ n \geq n_0 \rightarrow P(n)$".

Por exemplo, a afirmação $n^2 > 3n$ é verdadeira para todo natural n maior ou igual a 4, embora não seja verdadeira se n for 0, 1, 2 ou 3.
Podemos usar o PIM para provar esse tipo de afirmação, de maneira indireta. Primeiro definimos um outro predicado $Q(m)$ como sendo equivalente a $P(n_0 + m)$. Provamos então a afirmação $(\forall m \in \mathbb{N})\ Q(m)$, usando o PIM. Essa afirmação então implica $(\forall n \in \mathbb{N})\ n \geq n_0 \rightarrow P(n)$.

Este raciocínio nos permite provar tais afirmações por indução matemática de maneira mais direta, usando n_0 como base em vez de 0:
Teorema: Seja $P(n)$ uma sentença aberta sobre $n \in \mathbb{N},\ n \geq n_0$, n_0 um número natural qualquer. Se

1. $P(n_0)$ é verdadeira, e
2. Para todo $k \geq n_0$, $(P(k) \rightarrow P(k+1))$,

então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$ com $n \geq n_0$.

Exemplo

Prove que $n^2 > 3n$ para todo $n \in \mathbb{N}$ com $n \geq 4$.
Prova:

- **Base**: $n = 4$ é verdade pois $16 > 12$.
- **Hipótese de indução**: suponhamos que para algum $k \geq 4$, $k^2 > 3k$.

- **Passo da indução**: provar que $(k+1)^2 > 3(k+1)$. Temos que

$$(k+1)^2 = k^2 + 2k + 1$$

Por hipótese de indução $k^2 > 3k$, então

$$k^2 + 2k + 1 > 3k + 2k + 1.$$

Como $k \geq 4$ temos que $2k + 1 > 3$, logo

$$3k + 2k + 1 \geq 3k + 3 = 3(k+1)$$

portanto, destas duas desigualdades,

$$(k+1)^2 > 3(k+1).$$ **Fim.**

Passo genérico constante

Numa prova por indução, além de começar com uma base n_0 arbitrária, é possível usar um incremento maior que 1 no passo da indução. Ou seja, o passo da indução pode ser a demonstração de que $P(k) \rightarrow P(k+p)$, em vez de $P(k) \rightarrow P(k+1)$.

Teorema: Seja $P(n)$ uma sentença aberta sobre $n \in \mathbb{N}$, $n \geq n_0$, n_0 um número natural qualquer, e p um inteiro positivo. Se

1. $P(n_0), P(n_0+1), \ldots, P(n_0+p-1)$ são verdadeiros, e
2. Para todo k tal que $k \geq n_0$, $P(k) \rightarrow P(k+p)$.

então $P(n)$ é verdade para todo $n \geq n_0$.

Exemplo

Prove que qualquer valor postal inteiro $n \geq 8$ pode ser obtido utilizando apenas selos com valores 3 e 5.
Podemos provar esta afirmação usando o teorema da indução geral com incremento $p = 3$:

- **Bases**: $n = 8$, $n = 9$, $n = 10$. Como $8 = 5 + 3$, $9 = 3 + 3 + 3$ e $10 = 5 + 5$ temos que a proposição é válida para as bases.
- **Hipótese de indução**: Suponhamos que $P(k)$ é verdadeira para algum valor $k \geq 8$.
- **Passo**: Vamos provar que a proposição é válida para $k + 3$. Podemos obter o valor $k + 3$ acrescentando um selo de valor 3 aos selos usados para obter k.

Troca de variável na hipótese

Na hipótese de indução, podemos fazer uma troca de variável, usando k no lugar de $k + 1$. Nesse caso, o roteiro da demonstração fica assim:

- **Base da Indução**: Provar que $P(0)$ é verdade.
- **Hipótese de Indução**: Supor que para algum inteiro **positivo** k, $P(k - 1)$ é verdade.
- **Passo da Indução**: Provar que $P(k)$ é verdade.

Usos indevidos da indução matemática

É importante entender e verificar as condições em que a indução matemática se aplica. Se mal utilizada, ela pode levar a conclusões absurdas. Nos exemplos a seguir, tente encontrar o erro na demonstração.

Todos os cavalos têm a mesma cor.
Seja a sentença aberta $P(n)$: “Num conjunto com n cavalos, todos os cavalos têm a mesma cor.”
Prova: Vamos provar que $P(n)$ é verdadeira para todo $n \geq 1$, por indução.

- **Base**: Para $n = 1$ a sentença $P(n)$ é verdadeira.
- **Hipótese de indução**: Suponha que $P(k)$ é verdadeira para algum $k \geq 1$; isto é, em todo conjunto com k cavalos, todos têm a mesma cor.

- **Passo de indução**: Vamos provar que, em todo conjunto com $k + 1$ cavalos, todos têm a mesma cor. Considere um conjunto $C = \{c_1, c_2, \ldots, c_k, c_{k+1}\}$ com $k + 1$ cavalos. Podemos escrever o conjunto C como união de dois conjuntos, cada um com k cavalos,da seguinte forma:

$$C = C' \cup C'' = \{c_1, \ldots, c_k\} \cup \{c_2, \ldots, c_{k+1}\}$$

$$C = C' \cup C'' = \{c_1, \ldots, c_k\} \cup \{c_2, \ldots, c_{k+1}\}$$

Pela hipótese de indução, todos os cavalos de C' têm a mesma cor. O mesmo é verdade para C''. Como c_2 pertence a C' e a C'', concluímos que os cavalos de C' têm a mesma cor que os cavalos de C''. **Logo todos os cavalos de C têm a mesma cor.** Absurdo!

Paradoxo dos cavalos

Este exemplo, conhecido como **paradoxo dos cavalos**, foi inventado pelo matemático húngaro George Pólya (1887-1995). O exemplo a seguir ilustra um erro similar na aplicação do PIM, com “conclusão” igualmente absurda:

Todos os números naturais são iguais.
Prova: Seja $P(n)$ a sentença aberta "todos os números naturais menores ou iguais a n são iguais." Vamos provar que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, por indução.

- **Base**: $P(0)$ é obviamente verdadeira.
- **Hipótese de indução**: Suponha que $P(k)$ é verdadeira para algum $k \geq 0$, ou seja, todos os números menores ou iguais a k são iguais.

- **Passo de indução**: Vamos provar que $P(k+1)$ é verdadeira. Pela hipótese de indução, $k - 1 = k$. Somando 1 em ambos os lados da iqualdade temos $k = k + 1$. **Portanto** $P(k+1)$ **também é verdadeira.** Absurdo!

Exercícios:

- Seja C um conjunto com $n \geq 2$ elementos. Prove que C tem $n(n-1)/2$ subconjuntos com exatamente dois elementos.
- Prove que a soma dos cubos de três números naturais consecutivos é sempre divisível por 9.

Exemplo: [Descobrindo a Moeda Falsa] Num conjunto de 2^n moedas de ouro temos uma que é falsa, ou seja pesa menos que as outras. Prove, por indução, que é possível achar a moeda falsa com n pesagens usando uma balança de dois pratos sem usar peso.

Prova:

- **Base**: Para $n = 1$ temos duas moedas e, portanto, basta colocar uma em cada prato para descobrir a falsa.
- **Hipótese de indução**: Usando k pesagens podemos descobrir a moeda falsa dentre 2^k moedas.

- **Passo**: Provar que, num conjunto de 2^{k+1} moedas, podemos descobrir a moeda falsa com $k + 1$ pesagens. Divida o conjunto de 2^{k+1} moedas em dois conjuntos de 2^k moedas. Coloca-se esses conjuntos em cada prato da balança. Dessa forma descobrimos em qual conjunto de 2^k moedas se encontra a falsa. Pela hipótese de indução descobre-se a moeda com k pesagens, e, mais a pesagem anterior temos um total de $k + 1$ pesagens. **Fim**

Princípio das casas de pombos

O matemático alemão Johann Dirichlet (1805-1859) enunciou em 1834 o seguinte fato, conhecido como **princípio dos escaninhos** (ou **das gavetas**, **das casas de pombos** etc.):

Teorema: Se em n caixas ($n \geq 1$) colocarmos mais de n objetos, então alguma caixa conterá mais de um objeto.

Prova:

- **Base**: Para $n = 1$ o resultado é trivial pois, se há mais de um objeto, essa caixa terá mais de um objeto.
- **Hipótese de indução**: Suponhamos que o resultado é válido para algum número $k \geq 1$ de caixas, contendo mais do que k objetos.

- **Passo**: Queremos provar que o resultado é válido para $k+1$ caixas contendo mais do que $k+1$ objetos. Seja $m > k+1$ o número de objetos. Escolha uma caixa ao acaso. Se essa caixa contiver mais de um objeto, a proposição está provada. Se nessa caixa não há nenhum objeto, nas k caixas restantes estão acomodados $m > k+1 > k$ objetos; pela hipótese de indução, uma delas deve conter mais de um objeto. ...

... Finalmente, se na caixa escolhida há apenas um objeto, temos que, nas k caixas restantes estão distribuídos $m - 1 > (k+1) - 1 = k$ objetos, o que, novamente pela hipótese de indução, implica que uma das caixas contém mais de um objeto.**Fim**

Princípio da Indução Completa

Vamos agora enunciar o **princípio da indução completa** (PIC), também chamado de **princípio da indução forte**. Esta versão alternativa do princípio da indução matemática serve, como a anterior, para demonstrar sentenças na forma "$(\forall n \in \mathbb{N})\ P(n)$". Em alguns casos essa técnica torna a demonstração da sentença mais fácil que a técnica anterior.

1. **Base da indução**: Provar que $P(0)$ é verdade.
2. **Hipótese de indução**: Supor que, para algum $k \in \mathbb{N}$, $P(0)$, $P(1)$, ... $P(k)$ são verdadeiros.
3. **Passo da indução**: Provar que $P(k+1)$ é verdade.

Definimos que um número inteiro p é **primo** quando ele é maior que 1 e seus únicos divisores são 1 e p. Vamos provar que todo inteiro maior ou igual a 2 é primo ou é um produto de primos.

Prova: Seja $P(n)$ a sentença aberta "n é primo ou é um produto de primos." Vamos provar que $(\forall n \in \mathbb{N})\ n \geq 2 \to P(n)$, por indução completa.

- **Base**: $P(2)$ é verdade pois 2 é primo.
- **Hipótese de indução**: Suponha que, para algum $k \geq 2$, $P(i)$ é verdade para todo $i \in \mathbb{N}$ com $2 \leq i \leq k$.

- **Passo da indução**: Vamos provar que $P(k+1)$ também é verdade. Se $k+1$ é primo então $P(k+1)$ é verdadeiro. Se $k+1$ não é primo, como $k+1 \geq 2$, ele deve ter algum divisor diferente de 1 e de $k+1$. Ou seja, $k+1 = ab$ para algum a e b, com $1 < a \leq k$. Como $a > 1$, concluímos que $b < k+1$; como $a < k+1$, concluímos que $b > 1$. Ou seja, $2 \leq a \leq k$ e $2 \leq b \leq k$. Pela hipótese de indução, portanto, a e b são primos ou produtos de primos. Portanto $k+1 = a \cdot b$ também é um produto de primos. **Fim.**

Os **números de Lucas** $A_1, A_2, \ldots$ são definidos pelas seguintes regras: $A_1 = 1$, $A_2 = 3$, e $A_n = A_{n-1} + A_{n-2}$ para todo número inteiro n maior ou igual a 3.
Vamos provar $A_n < (\frac{7}{4})^n$ para todo inteiro $n \geq 1$, por indução completa.

Prova:
Seja $P(n)$ a sentença aberta "$A_n < \left(\frac{7}{4}\right)^n$."

- **Base**:
  - $P(1)$ é verdade pois $A_1 = 1 < \frac{7}{4}$.
  - $P(2)$ é verdade pois $A_2 = 3 < \left(\frac{7}{4}\right)^2 = \frac{49}{16}$.
- **Hipótese de indução**: Suponha que, para algum inteiro $k \geq 2$, $P(i)$ é verdade para todo $i \in \mathbb{N}$ com $1 \leq i \leq k$.

- **Passo da indução**: Vamos provar que $P(k+1)$ também é verdade, ou seja $A_{k+1} < (\frac{7}{4})^{k+1}$. Como $k+1 \geq 3$, pela definição temos que $A_{k+1} = A_k + A_{k-1}$. Então, pela hipótese de indução, temos

$$A_{k+1} < \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} = \left(\frac{7}{4} + 1\right)\left(\frac{7}{4}\right)^{k-1} = \frac{11}{4}\left(\frac{7}{4}\right)^{k-1}$$

Como $\frac{11}{4} < 3 < \left(\frac{7}{4}\right)^2$ temos que,

$$A_{k+1} < \left(\frac{7}{4}\right)^2 \left(\frac{7}{4}\right)^{k-1} = \left(\frac{7}{4}\right)^{k+1}$$

.

Exercícios:

- Prove que todo inteiro maior ou igual a 5, par ou ímpar, é a soma de números primos ímpares (isto é, primos diferentes de 2). Por exemplo, $6 = 3 + 3$, $7 = 7$, e $10 = 3 + 7$.
- Seja x um número real diferente de zero, tal que $x + \frac{1}{x}$ é um número inteiro. Prove que, para todo número natural n, $x^n + \frac{1}{x^n}$ é inteiro.

Princípio da Boa Ordenação

Uma outra maneira de provar sentenças abertas sobre número naturais é usar uma propriedade dos números naturais conhecida como o **princípio da boa ordenação** (PBO).
Seja S um conjunto de números reais. Um **elemento mínimo** de S é um $y \in S$ tal que para todo $x \in S$, $y \leq x$. O princípio da boa ordenação diz que

Teorema: Todo subconjunto não vazio S de $\mathbb{N}$ tem um elemento mínimo.

Note que esta afirmação não é válida para subconjuntos de $\mathbb{R}$ ou $\mathbb{Z}$; isto é, existem subconjuntos de $\mathbb{R}$ e de $\mathbb{Z}$ que não tem elemento mínimo.

Como exemplo de uso do PBO, vamos provar o **Teorema da Divisão de Euclides**:

Teorema: Sejam $a, b \in \mathbb{N}$, com $b \neq 0$. Então existem $q, r \in \mathbb{N}$ tais que $a = bq + r$ com $0 \leq r < b$.

Prova:
Sejam $a, b \in \mathbb{N}$, com $b \neq 0$, e seja

$$S = \{\, a - bk : k \in \mathbb{N}, a - bk \geq 0 \,\}.$$

Observe que $S \subseteq \mathbb{N}$ pois $a - bk \geq 0$; e que $S \neq \emptyset$ pois contem $a = a - b0$. Então pelo PBO, o conjunto S tem um elemento mínimo. Seja $r = a - bq$ esse elemento. ...

$r = a - bq$
Suponha agora que $r \geq b$. Nesse caso $a - b(q+1) = r - b \geq 0$, e portanto $r - b$ está também em S. Como $b > 0$, temos $r - b < r$. Isto contraria a escolha de r como o menor elemento de S. Portanto $r < b$.

Formas equivalentes do princípio da indução

O princípio da indução matemática, o princípio da indução completa e o princípio da boa ordenação (PBO) são equivalentes.
Mais precisamente, podemos provar que
PIM $\rightarrow$ **PBO** $\rightarrow$ **PIC** $\rightarrow$ **PIM**.
Exercício.

Exercício: Considere o seguinte jogo para duas pessoas. Coloca-se um número qualquer $n \geq 1$ de botões na mesa, e cada jogador, alternadamente, retira no mínimo 1 e no máximo 4 botões da pilha. Quem tira o último botão perde.

Vamos definir f_n como sendo 1 se o jogador da vez consegue ganhar quando há n botões na mesa, se jogar corretamente; e 0 se ele vai sempre perder, não importa como jogue. Por exemplo, f_1 é zero, por definição; mas f_5 é 1 pois o jogador da vez consegue ganhar (tirando 4 botões).

a) Determine f_n para n entre 1 e 30.
b) Determine uma fórmula eficiente para f_n e prove-a por indução.

Relações

Relações

Uma **relação binária** (ou simplesmente uma **relação**) $\mathcal{R}$ **de** um conjunto A **para** um conjunto B é um sub-conjunto de $A \times B$. Em outras palavras, é um conjunto de pares ordenados (a, b) com $a \in A$ e $b \in B$.
Em geral usa-se a notação $a\mathcal{R}b$ para dizer que $(a, b) \in \mathcal{R}$ e $a\not\mathcal{R}b$ para dizer que $(a, b) \notin \mathcal{R}$. Se $(a, b) \in \mathcal{R}$ dizemos que a **está relacionado com** b pela relação $\mathcal{R}$.

Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$. Então
$\mathcal{R} = \{(1, 4), (2, 5), (3, 5), (3, 6)\}$ é uma relação de A para B. Neste exemplo, temos $2\mathcal{R}5$ e $3\mathcal{R}5$, mas $2\not\mathcal{R}4$ e $5\not\mathcal{R}2$.

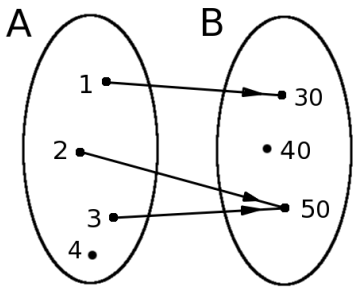


Diagrama da relação $\mathcal{R} = \{(1, 30), (2, 50), (3, 50)\}$ do conjunto $A = \{1, 2, 3, 4\}$ para o conjunto $B = \{30, 40, 50\}$.

- O conjunto de pares $\left\{ (x,\ \sqrt{x}) : x \in \mathbb{N} \right\}$ é um exemplo de uma relação de $\mathbb{N}$ para $\mathbb{R}$.
- Se R é uma relação de A para A, dizemos que $\mathcal{R}$ é uma relação **em** A ou **sobre** A.
- Observe que os sinais de comparação da álgebra ("<", "≤", etc.) são relações binárias definidas sobre os números reais.
- Observe também que "∈" é uma relação binária entre o conjunto $\mathcal{U}$ de todos os elementos, e o conjunto $\mathbb{P}(\mathcal{U})$ de todos os conjuntos; e que "⊆" é uma relação binária definida sobre o conjunto $\mathbb{P}(\mathcal{U})$.

Domínio

O **domínio** de uma relação $\mathcal{R}$, denotado por $\mathrm{Dom}(\mathcal{R})$, é o conjunto de todos os primeiros elementos dos pares ordenados que estão em $\mathcal{R}$. Isto é:

$$\mathrm{Dom}(\mathcal{R}) = \{\, a : (\exists b)\, (a, b) \in \mathcal{R} \,\}$$

Imagem

A **imagem** ou **contra-domínio** de uma relação $\mathcal{R}$, denotado por $\mathrm{Img}(\mathcal{R})$, é o conjunto de todos os segundos elementos dos pares ordenados que estão em $\mathcal{R}$. Isto é:

$$\mathrm{Img}(\mathcal{R}) = \{\, b : (\exists a)\,(a, b) \in \mathcal{R} \,\}$$

Observe que um conjunto de pares ordenados $\mathcal{R}$ é uma relação de A para B se, e somente se, $\mathrm{Dom}(\mathcal{R}) \subseteq A$ e $\mathrm{Img}(\mathcal{R}) \subseteq B$.

Exemplo: Seja $\mathcal{R}$ a relação $\{(1,4),(2,5),(3,5),(3,6)\}$. Temos que $\mathrm{Dom}(\mathcal{R}) = \{1,2,3\}$ e $\mathrm{Img}(\mathcal{R}) = \{4,5,6\}$.

Exemplo: Seja $\mathcal{R}$ a relação $\left\{ (x, x^2) : x \in \mathbb{Z} \right\}$. Observe que $\mathrm{Dom}(\mathcal{R})$ é o conjunto de todos os inteiros $\mathbb{Z}$, mas $\mathrm{Img}(\mathcal{R})$ é o conjunto dos quadrados perfeitos $\{0, 1, 4, 9, \ldots\}$.

Exemplo: Seja A o conjunto dos presidentes do Brasil, de 1889 a 2010. Seja $\mathcal{R}$ a relação sobre A tal que $a\mathcal{R}b$ se e somente se o presidente b foi o sucessor de a. Assim, por exemplo, temos que 'Figueiredo' $\mathcal{R}$ 'Tancredo' e 'Fernando Henrique' $\mathcal{R}$ 'Lula', mas 'Lula' $\not\mathcal{R}$ 'Fernando Henrique'. Observe que o domínio desta relação são todos os presidentes menos Lula (que terminou o mandato em 2010), e a imagem são todos os presidentes menos Floriano Peixoto.

Restrição de relações

- Seja $\mathcal{R}$ uma relação, e sejam A' e B' conjuntos quaiquer. A **restrição de** $\mathcal{R}$ **a** A' **e** B' é o conjunto de pares de $(a, b) \in \mathcal{R}$ tais que $a \in A'$ e $b \in B'$; ou seja, $\mathcal{R} \cap A' \times B'$.
- A **restrição de** $\mathcal{R}$ **a** A' é geralmente entendida como $\mathcal{R} \cap A' \times A'$.

Exemplo: Seja $\mathcal{R}$ a relação dos inteiros positivos $\mathbb{N} \setminus \{0\}$ para os inteiros, tal que $x\mathcal{R}y$ se e somente se x é divisor de y. A restrição de $\mathcal{R}$ aos conjuntos $U = \{0, 2, 3, 5, 6\}$ e $V = \{0, 1, 2, \ldots, 9\}$ é o conjunto de pares

$$\{(2,0),(2,2),(2,4),(2,6),(2,8),(3,0),(3,3)$$
$$(3,6),(3,9),(5,0),(5,5),(6,0),(6,6)\}$$

A restrição de $\mathcal{R}$ ao conjunto U é

$$\{(2,0),(2,2),(2,6),(3,0),(3,3),$$
$$(3,6),(5,0),(5,5),(6,0),(6,6)\}$$

Relações de identidade

Para qualquer conjunto A, a relação **identidade sobre** A, denotada por $\mathcal{I}_A$, é definida por

$$\mathcal{I}_A = \{(x, x) : x \in A\}$$

Esta relação nada mais é que a relação de igualdade "$=$", restrita ao conjunto A.

Exemplo: Se $A = \{1, 2, 3\}$ então $\mathcal{I}_A = \{(1,1),(2,2),(3,3)\}$.

Relação inversa

- Seja $\mathcal{R}$ uma relação do conjunto A para o conjunto B.
- A **relação inversa** denotada por $\mathcal{R}^{-1}$, é a relação do conjunto B para o conjunto A definida da seguinte forma:

$$\mathcal{R}^{-1} = \{\,(x, y) : (y, x) \in \mathcal{R}\,\}$$

- Ou seja, $\mathcal{R}^{-1}$ é a relação tal que $a\mathcal{R}^{-1}b$ se e somente se $b\mathcal{R}a$, para quaisquer a e b.
- Note que $\mathrm{Dom}(\mathcal{R}^{-1}) = \mathrm{Img}(\mathcal{R})$ e $\mathrm{Img}(\mathcal{R}^{-1}) = \mathrm{Dom}(\mathcal{R})$.

Imagem e imagem inversa de conjuntos sob uma relação

Sejam $\mathcal{R}$ uma relação de um conjunto A para um conjunto B, e X um conjunto qualquer.
A **imagem de X** sob $\mathcal{R}$ é o conjunto

$$\{\,b : (\exists a \in X)\,(a, b) \in \mathcal{R}\,\}$$

A **imagem inversa** de X sob $\mathcal{R}$ é o conjunto

$$\{\,a : (\exists b \in X)\,(a, b) \in \mathcal{R}\,\}$$

A **imagem de X** sob $\mathcal{R}$ é o conjunto

$$\{\, b : (\exists a \in X)\, (a, b) \in \mathcal{R} \,\}$$

A **imagem inversa** de X sob $\mathcal{R}$ é o conjunto

$$\{\, a : (\exists b \in X)\, (a, b) \in \mathcal{R} \,\}$$

Observe que a imagem inversa de X sob $\mathcal{R}$ é a imagem de X sob a relação inversa $\mathcal{R}^{-1}$. A imagem de X sob $\mathcal{R}$ costuma ser indicada por $\mathcal{R}(X)$. A imagem inversa então pode ser indicada por $\mathcal{R}^{-1}(X)$.

Composição de relações

Sejam $\mathcal{R}$ e $\mathcal{S}$ duas relações. A **composição de $\mathcal{R}$ com $\mathcal{S}$** é a relação denotada por $\mathcal{S} \circ \mathcal{R}$, e definida da seguinte forma:

$$\mathcal{S} \circ \mathcal{R} = \{(a, c) : (\exists b)\, (a, b) \in \mathcal{R} \wedge (b, c) \in \mathcal{S}\}$$

Exemplo: Considere as relações

$$\mathcal{R} = \{(1,1), (1,4), (2,3), (3,1), (3,4)\}$$

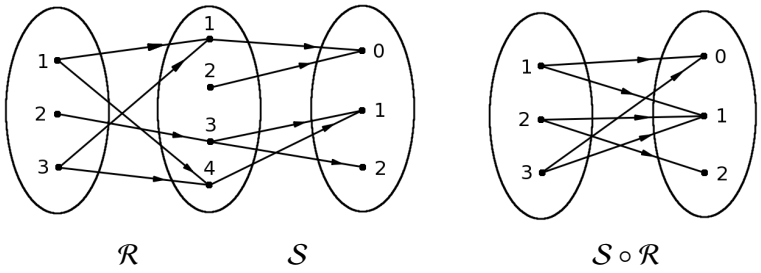
$$\mathcal{S} = \{(1,0), (2,0), (3,1), (3,2), (4,1)\}$$

A composição delas é

$$\mathcal{S} \circ \mathcal{R} = \{(1,0), (1,1), (2,1), (2,2), (3,0), (3,1)\}$$

Observe que

- $(1,0) \in \mathcal{S} \circ \mathcal{R}$ porque $(1,1) \in \mathcal{R}$ e $(1,0) \in \mathcal{S}$,
- $(1,1) \in \mathcal{S} \circ \mathcal{R}$ porque $(1,4) \in \mathcal{R}$ e $(4,1) \in \mathcal{S}$,
- $(2,1) \in \mathcal{S} \circ \mathcal{R}$ porque $(2,3) \in \mathcal{R}$ e $(3,1) \in \mathcal{S}$,
- $(2,2) \in \mathcal{S} \circ \mathcal{R}$ porque $(2,3) \in \mathcal{R}$ e $(3,2) \in \mathcal{S}$,
- $(3,0) \in \mathcal{S} \circ \mathcal{R}$ porque $(3,1) \in \mathcal{R}$ e $(1,0) \in \mathcal{S}$,
- $(3,1) \in \mathcal{S} \circ \mathcal{R}$ porque $(3,4) \in \mathcal{R}$ e $(4,1) \in \mathcal{S}$.



Exemplo:

- Seja $\mathcal{R}$ a relação de $\mathbb{Z}$ para $\mathbb{Z}$ definida por $x\mathcal{R}y \leftrightarrow x = y + 1$.
- Seja $\mathcal{S}$ a relação de $\mathbb{Z}$ para $\mathbb{Z}$ definida por $y\mathcal{S}z \leftrightarrow y = 2z$.
- A composição $\mathcal{S} \circ \mathcal{R}$ é a relação de $\mathbb{Z}$ para $\mathbb{Z}$ definida por

$$x(\mathcal{S} \circ \mathcal{R})z \leftrightarrow (\exists y \in \mathbb{Z})\, x = y + 1 \wedge y = 2z$$

- Ou seja, $x(\mathcal{S} \circ \mathcal{R})z \leftrightarrow x = 2z + 1$.
- Observe que $(5, 2) \in \mathcal{S} \circ \mathcal{R}$, porque $(5, 4) \in \mathcal{R}$ e $(4, 2) \in \mathcal{S}$.
- Observe também que $(6, 2) \notin \mathcal{S} \circ \mathcal{R}$, porque o único elemento relacionado com 6 por $\mathcal{R}$ é 5, mas $(5, 2) \notin \mathcal{S}$.
- e $(\mathcal{R} \circ \mathcal{S})$?

- Sejam $\mathcal{R}$ e $\mathcal{S}$ as mesmas relações.
  - Seja $\mathcal{R}$ a relação de $\mathbb{Z}$ para $\mathbb{Z}$ definida por $x\mathcal{R}y \leftrightarrow x = y + 1$.
  - Seja $\mathcal{S}$ a relação de $\mathbb{Z}$ para $\mathbb{Z}$ definida por $y\mathcal{S}z \leftrightarrow y = 2z$.
- A composição $\mathcal{R} \circ \mathcal{S}$ é a relação de $\mathbb{Z}$ para $\mathbb{Z}$ definida por

$$x(\mathcal{R} \circ \mathcal{S})z \leftrightarrow (\exists y \in \mathbb{Z})\, x = 2y \wedge y = z + 1$$

- Ou seja, $x(\mathcal{R} \circ \mathcal{S})z \leftrightarrow x = 2z + 2$.
- Observe que $(5, 2) \notin \mathcal{R} \circ \mathcal{S}$, mas $(6, 2) \in \mathcal{R} \circ \mathcal{S}$.
- Podemos observar então que $\mathcal{S} \circ \mathcal{R} \neq \mathcal{R} \circ \mathcal{S}$, ou seja, a composição de relações não é comutativa.

- Observe que, para quaisquer relações $\mathcal{R}$ e $\mathcal{S}$, temos

$$\mathrm{Dom}(\mathcal{S} \circ \mathcal{R}) \subseteq \mathrm{Dom}(\mathcal{R})$$

- e

$$\mathrm{Img}(\mathcal{S} \circ \mathcal{R}) \subseteq \mathrm{Img}(\mathcal{S})$$

Exercício: Seja $\mathcal{R}$ o conjunto de todos os pares (x, x^2) onde x é um número inteiro. Seja $\mathcal{S}$ o conjunto de todos os pares $(3y, y)$ onde y é um número natural. Descreva as relações $\mathcal{R} \circ \mathcal{S}$ e $\mathcal{S} \circ \mathcal{R}$.

Notação alternativa

- A notação $\mathcal{S} \circ \mathcal{R}$ para composição de $\mathcal{R}$ com $\mathcal{S}$ é muito comum, especialmente para funções.
- Em algumas áreas da matemática, entretanto, a composição de uma relação $\mathcal{R}$ com uma relação $\mathcal{S}$ é denotada pela justaposição $\mathcal{RS}$.
- Observe que, nesta notação, a ordem das relações é oposta à da notação tradicional.

Composição com identidade

Observe que, para qualquer relação $\mathcal{R}$ de um conjunto A para um conjunto B, as composições $\mathcal{I}_B \circ \mathcal{R}$ e $\mathcal{R} \circ \mathcal{I}_A$ são sempre a própria relação $\mathcal{R}$.

Composição com a relação inversa

Exemplo: Seja $A = \{1, 2, 3\}$ e seja $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$, uma relação sobre A. Lembramos que a relação inversa $\mathcal{R}^{-1}$ é $\{(2, 1), (3, 1), (3, 2)\}$, e que $\mathcal{I}_A = \{(1, 1), (2, 2), (3, 3)\}$. Então:

- $\mathcal{R}^{-1} \circ \mathcal{R} = \{(1, 1), (1, 2), (2, 2), (2, 1)\}$.
- $\mathcal{R} \circ \mathcal{R}^{-1} = \{(2, 2), (2, 3), (3, 3), (3, 2)\}$.
- $\mathcal{R} \circ \mathcal{R} = \{(1, 3)\}$.
- $\mathcal{R}^{-1} \circ \mathcal{R}^{-1} = \{(3, 1)\}$.

Observamos que neste exemplo $\mathcal{R} \circ \mathcal{R}^{-1}$ é diferente de $\mathcal{R}^{-1} \circ \mathcal{R}$, e ambas são diferentes da identidade $\mathcal{I}_A$.

Inversa da composição

Pode-se verificar que, para quaisquer relações $\mathcal{R}$ e $\mathcal{S}$,

$$(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$$

Ou seja, a **inversa da composição é a composição das inversas, na ordem inversa**.

Exemplo:

- Sejam as relações

$$\mathcal{R} = \{(1,20),(1,30),(2,40),(3,20)\}$$

$$\mathcal{S} = \{(20,200),(20,300),(40,200)\}$$

- Observe que
  - $\mathcal{S} \circ \mathcal{R} = \{(1,200),(1,300),(2,200),(3,200),(3,300)\}$.
  - $\mathcal{R}^{-1} = \{(20,1),(30,1),(40,2),(20,3)\}$.
  - $\mathcal{S}^{-1} = \{(200,20),(300,20),(200,40)\}$.
  - $\mathcal{R}^{-1} \circ \mathcal{S}^{-1} = \{(200,1),(300,1),(200,3),(200,2),(300,3)\}$.
  - $(\mathcal{S} \circ \mathcal{R})^{-1} = \{(200,1),(300,1),(200,3),(300,3),(200,2)\}$.

Composição e inclusão

Para quaisquer relações $\mathcal{R}_1, \mathcal{R}_2, \mathcal{S}_1, \mathcal{S}_2$, se $\mathcal{R}_1 \subseteq \mathcal{R}_2$ e $\mathcal{S}_1 \subseteq \mathcal{S}_2$, então $\mathcal{R}_1 \circ \mathcal{S}_1 \subseteq \mathcal{R}_2 \circ \mathcal{S}_2$.

Potências de uma relação

Seja $\mathcal{R}$ uma relação. A **potência** $\mathcal{R}^n$, $n = 1, 2, \cdots$ é definida como:

$$\begin{aligned} \mathcal{R}^1 &= \mathcal{R} \\ \mathcal{R}^{n+1} &= \mathcal{R}^n \circ \mathcal{R} \end{aligned}$$

Teorema: Para quaisquer relações $\mathcal{R}$ e $\mathcal{S}$, e qualquer inteiro $n \geq 1$, se $\mathcal{R} \subseteq \mathcal{S}$ então $\mathcal{R}^n \subseteq \mathcal{S}^n$.

Tipos de relações

Seja $\mathcal{R}$ uma relação sobre um conjunto A.

- $\mathcal{R}$ é **reflexiva** sobre A se, e somente se, para todo $a \in A$ o par (a,a) está em $\mathcal{R}$.
- $\mathcal{R}$ é **irreflexiva** se, e somente se, ela não possui nenhum par da forma (a,a).
- $\mathcal{R}$ é **simétrica** se, e somente se, $(\forall a, b \in A)\, a\mathcal{R}b \rightarrow b\mathcal{R}a$. Ou seja, se um par (a,b) está em $\mathcal{R}$ então o par (b,a) também está em $\mathcal{R}$.

- $\mathcal{R}$ é **anti-simétrica** se, e somente se, $(\forall a, b \in A)\,(a\mathcal{R}b) \wedge (b\mathcal{R}a) \rightarrow a = b$. Ou seja, para quaisquer elementos distintos a e b em A, no máximo um dos pares (a, b) e (b, a) está em $\mathcal{R}$.
- $\mathcal{R}$ é **transitiva** se, e somente se, $(\forall a, b, c \in A)\,(a\mathcal{R}b) \wedge (b\mathcal{R}c) \rightarrow a\mathcal{R}c$. Ou seja, se dois pares (a, b) e (b, c) estão em $\mathcal{R}$ então o par (a, c) também está em $\mathcal{R}$.

- Note que dizer que $\mathcal{R}$ é reflexiva sobre A equivale a dizer que $\mathcal{I}_A \subseteq \mathcal{R}$;
- dizer que $\mathcal{R}$ é irreflexiva equivale a dizer que $\mathcal{R} \cap \mathcal{I}_A = \emptyset$.
- Observe que há relações que não são nem reflexivas e nem irreflexivas, como por exemplo a relação $\mathcal{R}_1 = \{(1,1), (2,1), (1,2)(3,1)\}$ sobre o conjunto $A = \{1, 2, 3\}$.
- Porém, se o conjunto A não é vazio, uma relação não pode ser ao mesmo tempo reflexiva sobre A e irreflexiva.

- Observe também que os termos simétrica e anti-simétrica não são opostos: qualquer relação de identidade, por exemplo, é ao mesmo tempo simétrica e anti-simétrica.
- Além disso, há relações que não são nem simétricas nem anti-simétricas. Por exemplo, a relação $\mathcal{R}_1 = \{(1,1), (2,1), (1,2)(3,1)\}$ sobre o conjunto $A = \{1, 2, 3\}$ não é simétrica, pois ela tem o par $(3, 1)$ mas não tem o par $(1, 3)$; e nem anti-simétrica, pois ela tem os dois pares $(2, 1)$ e $(1, 2)$.

- Finalmente, observe que uma relação pode satisfazer qualquer uma das propriedades por vacuidade, se não existirem elementos em A que satisfaçam as condições no lado esquerdo do conectivo '$\rightarrow$'.
- Por exemplo, a relação $\mathcal{R}_3 = \{(1, 2)\}$ é transitiva, porque não existem a, b e c tais que $(a\mathcal{R}_3 b) \wedge (b\mathcal{R}_3 c)$.

$$\begin{aligned}
\mathcal{R}_1 =& \{(1,1),(1,2),(2,1),(2,2),\\
& (3,3),(3,4),(4,1),(4,4)\}.\\
\mathcal{R}_2 =& \{(1,1),(1,2),(2,1)\}.\\
\mathcal{R}_3 =& \{(1,1),(1,2),(2,1),(2,2),\\
& (3,3),(4,1),(1,4),(4,4)\}.\\
\mathcal{R}_4 =& \{(2,1),(3,1),(3,2),(4,1),(4,2),(4,3)\}.\\
\mathcal{R}_5 =& \{(1,1),(1,2),(1,3),(1,4),(2,2),\\
& (2,3),(2,4),(3,3),(3,4),(4,4)\}.\\
\mathcal{R}_6 =& \{(3,4)\}.
\end{aligned}$$

- São reflexivas sobre A: $\mathcal{R}_1$, $\mathcal{R}_3$ e $\mathcal{R}_5$.
- São irreflexivas sobre A: $\mathcal{R}_4$ e $\mathcal{R}_6$.
- São simétricas: $\mathcal{R}_2$ e $\mathcal{R}_3$.
- São anti-simétricas: $\mathcal{R}_4$, $\mathcal{R}_5$ e $\mathcal{R}_6$.
- São transitivas: $\mathcal{R}_4$, $\mathcal{R}_5$ e $\mathcal{R}_6$.

Composição e transitividade

Teorema: Uma relação $\mathcal{R}$ é transitiva se, e somente se $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.
Prova: Seja $\mathcal{R}$ uma relação sobre um conjunto A. Vamos primeiro provar que, se $\mathcal{R}$ é transitiva, então $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$. Seja $(a,b) \in \mathcal{R} \circ \mathcal{R}$. Pela definição de composição de relações, temos que $(\exists x)\,(a,x) \in \mathcal{R} \wedge (x,b) \in \mathcal{R}$. Como $\mathcal{R}$ é transitiva, concluimos que $(a,b) \in \mathcal{R}$. Logo $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.

Vamos provar agora que, se $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$, então $\mathcal{R}$ é transitiva. Sejam a, b, c três elementos de A. Se $(a,b) \in \mathcal{R}$ e $(b,c) \in \mathcal{R}$, então, pela definição de composição, temos que $(a,c) \in \mathcal{R} \circ \mathcal{R}$. Como $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$, então $(a,c) \in \mathcal{R}$. Logo $\mathcal{R}$ é transitiva. □

Uma **matriz booleana** é uma matriz cujos elementos são valores lógicos, **F** ou **V**. Ao escrever tais matrizes, é conveniente usar 0 e 1, respectivamente, para indicar esses valores.

Sejam $A = \{a_1, a_2, \cdots, a_m\}$ e $B = \{b_1, b_2, \cdots, b_n\}$ conjuntos finitos com $|A| = m$, $|B| = n$ e $\mathcal{R}$ uma relação de A para B. Uma maneira de representar esta relação é através de uma matriz booleana M de m linhas e n colunas definida da seguinte maneira:

$$M_{i,j} = \begin{cases} 1 & \text{se } a_i \mathcal{R} b_j \\ 0 & \text{se } a_i \mathcal{R} b_j \end{cases}$$

Exemplo: Seja $\mathcal{R}$ a relação $\{(20, 20), (30, 20), (30, 30)\}$. Se escolhermos $A = \{10, 20, 30, 40\}$ e $B = \{10, 20, 30\}$, listados nessa ordem, a matriz da relação será

$$M = \left(\begin{array}{c|ccc} & 10 & 20 & 30 \\ \hline 10 & 0 & 0 & 0 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 1 & 1 \\ 40 & 0 & 0 & 0 \end{array}\right)$$

Observe que a matriz M depende da escolha dos conjuntos A e B, e também da ordem em que listamos seus elementos.

- A composição de relações também pode ser entendida em termos de matrizes.
- Sejam $\mathcal{R}$ uma relação de $A = \{a_1, a_2, \ldots a_m\}$ para $B = \{b_1, b_2, \ldots b_n\}$
- $\mathcal{S}$ uma relação de $B = \{b_1, b_2, \ldots b_n\}$ para $C = \left\{c_1, c_2, \ldots c_p\right\}$
- $\mathcal{R}$ está representado por uma matriz $M(m \times n)$ e $\mathcal{S}$ está representado por uma matriz $N(n \times p)$.

Pela definição, a matriz P que representa a composição $\mathcal{S} \circ \mathcal{R}$ é tal que $P_{i,j} = 1$ se e somente se existe um inteiro $k \in \{1, 2, \ldots, n\}$ tal que $M_{i,k} = 1$ e $N_{k,j} = 1$. Ou seja,

$$P_{i,j} = (M_{i,1} \wedge N_{1,j}) \vee (M_{i,2} \wedge N_{2,j}) \vee \cdots \vee (M_{i,n} \wedge N_{n,j})$$

$$P_{i,j} = \bigvee_{k=1}^{n} M_{i,k} \wedge N_{k,j}.$$

Sejam $A = \{10, 20, 30, 40\}$, $B = \{20, 40, 60\}$, e $C = \{35, 55, 75, 95\}$. Sejam

$$\mathcal{R} = \{(10, 20), (10, 60), (20, 40), (40, 60)\}$$

$$\mathcal{S} = \{(20, 35), (20, 55), (40, 55), (40, 75), (60, 95)\}$$

As matrizes booleanas que representam $\mathcal{R}$, $\mathcal{S}$ e $\mathcal{S} \circ \mathcal{R}$ são

$$M = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 1 \end{array}\right) N = \left(\begin{array}{c|cccc} & 35 & 55 & 75 & 95 \\ \hline 20 & 1 & 1 & 0 & 0 \\ 40 & 0 & 1 & 1 & 0 \\ 60 & 0 & 0 & 0 & 1 \end{array}\right)$$

$MN =$?

$$M = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 1 \end{array}\right) N = \left(\begin{array}{c|cccc} & 35 & 55 & 75 & 95 \\ \hline 20 & 1 & 1 & 0 & 0 \\ 40 & 0 & 1 & 1 & 0 \\ 60 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$MN = \left(\begin{array}{c|cccc} & 35 & 55 & 75 & 95 \\ \hline 10 & 1 & 1 & 0 & 1 \\ 20 & 0 & 1 & 1 & 0 \\ 30 & 0 & 0 & 0 & 0 \\ 40 & 0 & 0 & 0 & 1 \end{array}\right)$$

União de relações. Sejam $\mathcal{R}$ e $\mathcal{S}$ duas relações de um conjunto A para um conjunto B, com matrizes booleanas M e N, respectivamente.A matriz booleana P que representa a união $\mathcal{R} \cup \mathcal{S}$ é tal que $P_{i,j} = 1$ se, e somente se, $M_{i,j} = 1$ ou $N_{i,j} = 1$. Ou seja, $P_{i,j} = M_{i,j} \vee N_{i,j}$. Podemos denotar essa matriz por $M \vee N$.

Intersecção de relações. Analogamente, a matriz Q que representa a interseção $\mathcal{R} \cap \mathcal{S}$ é tal que $Q_{i,j} = 1$ se e somente se $M_{i,j} = 1$ e $N_{i,j} = 1$; ou seja $Q_{i,j} = M_{i,j} \wedge N_{i,j}$. Podemos denotar essa matriz por $M \wedge N$.

Sejam $A = \{10, 20, 30, 40\}$ e $B = \{20, 40, 60\}$, e sejam

$$\mathcal{R} = \{(10, 20), (10, 60), (20, 40), (40, 60)\}$$

$$\mathcal{S} = \{(10, 20), (20, 60), (30, 40), (40, 20)\}$$

As matrizes booleanas que representam $\mathcal{R}$, $\mathcal{S}$, $\mathcal{R} \cup \mathcal{S}$ e $\mathcal{R} \cap \mathcal{S}$ são

$$M = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 1 \end{array}\right) \qquad N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 0 \\ 20 & 0 & 0 & 1 \\ 30 & 0 & 1 & 0 \\ 40 & 1 & 0 & 0 \end{array}\right)$$

$$M = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 1 \end{array}\right) \qquad N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 0 \\ 20 & 0 & 0 & 1 \\ 30 & 0 & 1 & 0 \\ 40 & 1 & 0 & 0 \end{array}\right)$$

$$M \vee N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 1 \\ 30 & 0 & 1 & 0 \\ 40 & 1 & 0 & 1 \end{array}\right) \qquad M \wedge N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 0 \\ 20 & 0 & 0 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 0 \end{array}\right)$$

Seja $\mathcal{R}$ uma relação sobre A. Se M é a matriz que representa essa relação, várias propriedades de $\mathcal{R}$ podem ser facilmente verificadas na matriz M:

- Uma relação $\mathcal{R}$ é reflexiva sobre A se, e somente se $(\forall i \in \{1, 2, \cdots, n\})\, a_i \mathcal{R} a_i$. Portanto $\mathcal{R}$ é reflexiva sobre A e somente se $(\forall i \in \{1, 2, \cdots, n\})\, M_{i,i} = 1$; isto é, os elementos da diagonal de M são todos 1.

- Uma relação $\mathcal{R}$ é irreflexiva sobre A se, e somente se $(\forall i \in \{1, 2, \cdots, n\})\, a_i \not\mathcal{R} a_i$. Portanto $\mathcal{R}$ é irreflexiva sobre A e somente se os elementos da diagonal de M são todos 0.

- Uma relação $\mathcal{R}$ é simétrica se, e somente se $(\forall i, j \in \{1, 2, \cdots, n\})\, a_i \mathcal{R} a_j \leftrightarrow a_j \mathcal{R} a_i$. Portanto $\mathcal{R}$ é simétrica se, e somente se, a matriz M é simétrica, ou seja, ela é igual à sua transposta.
- Uma relação $\mathcal{R}$ é anti-simétrica se, e somente se $(\forall i, j \in \{1, 2, \cdots, n\})\, (a_i \mathcal{R} a_j \wedge a_j \mathcal{R} a_i) \rightarrow a_i = a_j$. Portanto $\mathcal{R}$ é anti-simétrica se, e somente se não existem índices i e j com $i \neq j$ tais que $M_{i,j}$ e $M_{j,i}$ são simultaneamente iguais a 1.

Seja $\mathcal{R}$ uma relação sobre um conjunto $A = \{a_1, a_2, a_3\}$ cuja matriz é

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Observe que:

- $\mathcal{R}$ é reflexiva sobre A pois $m_{i,i} = 1$ para todo i.
- $\mathcal{R}$ é simétrica pois M é simétrica.
- $\mathcal{R}$ não é anti-simétrica pois $m_{1,2} = m_{2,1} = 1$.

Fecho reflexivo
Seja $\mathcal{R}$ uma relação sobre um conjunto A. Se $\mathcal{R}$ não é reflexiva sobre A, é porque não possui um ou mais pares da forma (a, a) com $a \in A$. Se acrescentarmos todos esses pares a $\mathcal{R}$, obtemos uma relação $\mathcal{S}$ que é reflexiva sobre A e contém $\mathcal{R}$. Essa relação é chamada de **fecho reflexivo de $\mathcal{R}$ sobre A**.

Exemplo: Sejam $A = \{a, b, c\}$ e $\mathcal{R} = \{(a, a), (a, b), (b, a), (c, b)\}$. A relação
$\mathcal{S} = \{(a, a), (a, b), (b, a), (c, b), (b, b), (c, c)\}$ é o fecho reflexivo de $\mathcal{R}$ sobre A.

Fecho simétrico
Se $\mathcal{R}$ é uma relação qualquer, obtemos seu **fecho simétrico** acrescentando a $\mathcal{R}$ todos os pares necessários para torná-la uma relação simétrica; isto é, todo par da forma (b, a) tal que $(a, b) \in \mathcal{R}$.

Exemplo: Sejam $A = \{a, b, c\}$ e
$\mathcal{R} = \{(a, a), (a, b), (b, b), (b, c), (c, a), (c, b)\}$. A relação
$\mathcal{S} = \{(a, a), (a, b), (b, a), (b, b), (c, a), (a, c), (b, c), (c, b)\}$ é o fecho simétrico de $\mathcal{R}$.

Fecho transitivo
Considere o problema de completar uma relação $\mathcal{R}$, se necessário, de modo a torná-la transitiva.Para isso, precisamos garantir que, para quaisquer pares (a, b) e (b, c) na relação, o par (a, c) também está na relação.

$$\mathcal{R} = \{(1,2),(2,3),(3,4)\}$$

Esta relação falha a definição de relação transitiva em exatamente dois casos:

$$(1,2) \in \mathcal{R} \wedge (2,3) \in \mathcal{R} \quad \text{mas} \quad (1,3) \notin \mathcal{R}$$
$$(2,3) \in \mathcal{R} \wedge (3,4) \in \mathcal{R} \quad \text{mas} \quad (2,4) \notin \mathcal{R}$$

Se acrescentarmos os pares $(1,3)$ e $(2,4)$, obtemos a relação

$$\mathcal{R}' = \{(1,2),(1,3),(2,3),(2,4),(3,4)\}$$

$$\mathcal{R}' = \{(1,2),(1,3),(2,3),(2,4),(3,4)\}$$

Mas esta relação ainda não é transitiva; pois ela possui $(1,3)$ e $(3,4)$ mas não possui $(1,4)$. Observe que esta falha de transitividade foi revelada quando acrescentamos o par $(1,3)$ à relação. Se acrescentarmos o par que falta, $(1,4)$, obtemos

$$\mathcal{R}'' = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$$

que é transitiva.

O **fecho transitivo** de $\mathcal{R}$, denotado por $\mathcal{R}^*$ é definido como sendo a união de todas as potências de $\mathcal{R}$, isto é

$$\mathcal{R}^* = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \cdots \tag{6}$$

Esta fórmula pode ser escrita mais sucintamente da seguinte maneira

$$\mathcal{R}^* = \bigcup_{k=1}^{\infty} \mathcal{R}^k \tag{7}$$

Fecho em geral
De maneira geral, sejam $\mathcal{R}$ uma relação em um conjunto A, **P** uma propriedade de relações, e $\mathcal{S}$ uma relação em A com a propriedade **P**. Dizemos que $\mathcal{S}$ é o **fecho** da relação $\mathcal{R}$ com respeito à **propriedade P**, se $\mathcal{S}$ contém $\mathcal{R}$ e está contida em toda relação que possui a propriedade **P** e contém $\mathcal{R}$.

Relações n-árias

- Sejam $A_1, A_2, A_3, \ldots, A_n$, conjuntos.
- Uma **relação n-ária entre** estes conjuntos é um sub-conjunto $\mathcal{R}$ de $A_1 \times A_2 \times A_3 \times \cdots \times A_n$.
- Isto é, um elemento de $\mathcal{R}$ é uma n-upla $(a_1, a_2, \ldots, a_n)$, tal que $a_i \in A_i$ para cada i.

Relações n-árias

- O inteiro n é chamado de **grau** ou **ordem** da relação.
- Para $n \geq 2$ usam-se os nome **binária**, **ternária**, **quaternária.**, etc.
- O **i-ésimo domínio** da relação é o conjunto $\mathrm{Dom}_i(\mathcal{R})$ de todos os elementos de A_i que ocorrem na posição i das suas n-uplas.
- Ou seja, um elemento x pertence a $\mathrm{Dom}_i(\mathcal{R})$ se, e somente se, existe uma n-upla $(a_1, a_2, \ldots, a_n)$ em $\mathcal{R}$ com $a_i = x$.

Projeção

Seja $\mathcal{R}$ uma relação n-ária e sejam $i_1, i_2, \ldots, i_m$ inteiros distintos entre 1 e n. A **projeção de $\mathcal{R}$ sobre as componentes** $i_1, i_2, \ldots, i_m$ é a relação m-ária $\mathcal{S}$ tal que uma m-upla $(b_1, b_2, \ldots, b_m)$ está em $\mathcal{S}$ se e somente se existe uma n-upla $(a_1, a_2, \ldots, a_n)$ em $\mathcal{R}$ tal que $b_1 = a_{i_1}$, $b_2 = a_{i_2}$, $\ldots$, $b_m = a_{i_m}$.

Seja $\mathcal{R} \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ a relação ternária formada pelas triplas

$$\{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 300)\}.$$

Eis algumas projeções dessa relação sobre diversas listas de componentes:

- Sobre 2 e 3: $\{(10, 200), (20, 200), (30, 100), (30, 300)\}$
- Sobre 1 e 3: $\{(1, 200), (2, 200), (2, 100), (3, 300)\}$
- Sobre 2 e 1: $\{(10, 1), (20, 1), (20, 2), (30, 2), (30, 3)\}$
- Sobre 1, 2 e 3:

$$\{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 300)\} = \mathcal{R}$$

Permutação de componentes

Para relações binárias temos o conceito de relação inversa em que é trocada a ordem das duas componentes de cada par. Sua generalização para relações n-árias é a operação de **permutação de componentes**, que rearranja a ordem das componentes de todas as n-uplas, da mesma maneira.

Mais precisamente, dada uma relação n-ária $\mathcal{R}$ e uma permutação $i_1, i_2, \ldots, i_n$ dos inteiros $1, 2, \ldots, n$, esta operação produz a relação n-ária $\mathcal{S}$ que consiste de todas as n-uplas $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$ tais que $(a_1, a_2, \ldots, a_n)$ está em $\mathcal{R}$.

Restrição

Sejam $\mathcal{R}$ uma relação n-ária, e $X_1, X_2, \ldots, X_n$ conjuntos arbitrários. Da mesma forma que para relações binárias, definimos a **restrição de $\mathcal{R}$ a esses conjuntos** como a relação $\mathcal{S}$ das n-uplas $(a_1, a_2, \ldots, a_n)$ de $\mathcal{R}$ que tem $a_j \in X_j$, para cada j; ou seja

$$\mathcal{S} = \mathcal{R} \cap (X_1 \times X_2 \times \cdots\cdots \times X_n)$$

Exemplo: Considere a relação

$$\mathcal{R} = \{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 100), (3, 30, 300)\}.$$

Observe que esta é uma relação entre os conjuntos $A_1 = \{1, 2, 3\}$, $A_2 = \{10, 20, 30\}$, e $A_3 = \{100, 200, 300\}$.

Sejam $X_1 = \{1, 2, 3, 4\}$, $X_2 = \{20, 30, 40\}$, e $X_3 = \{200, 300\}$. A restrição de $\mathcal{R}$ a X_1, X_2 e X_3 é

$$\mathcal{S} = \{(1, 20, 200), (2, 20, 200), (3, 30, 300)\}$$

Junção

$\mathcal{R}$			
Nome	Função	Chefe	Sala
José	Secretário	Aníbal	S.102
José	Digitação	Aníbal	S.103
Maria	Digitação	Sônia	S.103
Maria	Secretária	Sônia	S.202
Pedro	Assistente	José	S.102
Luiz	Despacho	Carlos	S.301
Luiz	Motorista	Carlos	S.307

$\mathcal{S}$		
Sala	Ramal	Setor
S.101	8233	Vigilância
S.102	8247	Financeiro
S.102	8250	Patrimônio
S.103	8288	Vendas
S.103	8289	Vendas
S.104	8300	Pessoal
S.301	8380	Compras
S.303	8350	Contabilidade
S.307	8380	Transporte

Note que há empregados que trabalham em várias salas, salas com vários empregados, salas com mais de um ramal, ramais que servem mais de uma sala, etc.
Cruzando estes dados, podemos obter outras relações entre essas entidades.
Por exemplo, casando o número da sala nas duas relações, podemos construir a relação $\mathcal{T}$

$\mathcal{T}$					
Nome	Função	Chefe	sala	Ramal	Setor
José	Secretário	Aníbal	S.102	8247	Financeiro
José	Secretário	Aníbal	S.102	8250	Patrimônio
José	Digitação	Aníbal	S.103	8288	Vendas
José	Digitação	Aníbal	S.103	8289	Vendas
Maria	Digitação	Sônia	S.103	8288	Vendas
Maria	Digitação	Sônia	S.103	8289	Vendas
Pedro	Assistente	José	S.102	8247	Financeiro
Pedro	Assistente	José	S.102	8250	Patrimônio
Luiz	Despacho	Carlos	S.301	8380	Compras
Luiz	Motorista	Carlos	S.307	8380	Transporte

Note que, por exemplo, a linha "(José, Digitação, Aníbal, 8289, Vendas)" foi incluída na relação $\mathcal{T}$ porque existe a quádrupla "(José, Digitação, Aníbal, S.103)" na relação $\mathcal{R}$, e a tripla "(S.103, 8288, Vendas)" — com o mesmo número de sala — na relação $\mathcal{S}$.

Formalmente, seja $\mathcal{R}$ uma relação m-ária e $\mathcal{S}$ uma relação n-ária.
Define-se a **junção** das relações $\mathcal{R}$ e $\mathcal{S}$ como sendo a relação $(m+n-1)$-ária $\mathcal{T}$ consistindo de todas as tuplas $(a_1, a_2, \ldots, a_{m-1}, c, b_1, b_2, \ldots, b_{n-1})$, tais que $(a_1, a_2, \ldots, a_{m-1}, c) \in \mathcal{R}$ e $(c, b_1, b_2, \ldots, b_{n-1}) \in \mathcal{S}$.

Podemos generalizar ainda mais esta operação casando dois ou mais campos ao mesmo tempo. Seja $\mathcal{R}$ uma relação m-ária, $\mathcal{S}$ uma relação n-ária, e p um inteiro positivo menor que m e n. A **junção em p campos** das relações $\mathcal{R}$ e $\mathcal{S}$ é a relação $(m+n-p)$-ária $\mathcal{T}$ consistindo de todas as tuplas $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2, \ldots, c_p, b_1, b_2, \ldots, b_{n-p})$, tais que $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2, \ldots, c_p) \in \mathcal{R}$, e $(c_1, c_2, \ldots, c_p, b_1, b_2, \ldots, b_{n-p}) \in \mathcal{S}$.

Relações de ordem e equivalência

Relações de ordem

Definição: Uma relação $\mathcal{R}$ sobre um conjunto A é uma **relação de ordem** se ela é reflexiva sobre A, anti-simétrica e transitiva.

Exemplo: Sejam $A = \mathbb{R}$ e $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R}, : x \leq y\}$.

- $\mathcal{R}$ é reflexiva sobre A pois $(\forall x \in \mathbb{R})\, x \leq x$ logo $(\forall x \in \mathbb{R})\, x\mathcal{R}x$.

$\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R}, : x \leq y\}$.

- $\mathcal{R}$ é transitiva pois $(\forall x, y, z \in \mathbb{R})\, ((x \leq y \wedge y \leq z) \rightarrow x \leq z))$. Portanto
$$(\forall x, y, z \in \mathbb{R})\, (x\mathcal{R}y \wedge y\mathcal{R}z) \rightarrow x\mathcal{R}z.$$
- $\mathcal{R}$ é anti-simétrica pois $(\forall x, y \in \mathbb{R})\, (x \leq y \wedge y \leq x) \rightarrow x = y$. Portanto
$$(\forall x, y \in \mathbb{R})\, (x\mathcal{R}y \wedge y\mathcal{R}x) \rightarrow x = y.$$

Se $\mathcal{R}$ é uma relação de ordem sobre um conjunto A, o par $(A, \mathcal{R})$ é chamado um **conjunto ordenado**. Por exemplo, $(\mathbb{N}, \leq)$ é um conjunto ordenado (entendendo-se que '$\leq$' aqui é a restrição da relação "menor ou igual" aos números naturais). Outro exemplo de conjunto ordenado é $(\mathbb{P}(A), \subseteq)$, para qualquer conjunto A.

Relações de ordem estrita

Definição: Uma relação $\mathcal{R}$ sobre um conjunto A é uma **relação de ordem estrita** se ela é irreflexiva sobre A, anti-simétrica e transitiva.

Exemplo: Sejam $A = \mathbb{R}$ e $\mathcal{R} = \{ (x, y) \in \mathbb{R} \times \mathbb{R}, : x < y \}$.

- $\mathcal{R}$ é irreflexiva sobre A pois $(\forall x \in \mathbb{R})\, \neg(x < x)$ logo $(\forall x \in \mathbb{R})\, x \not\mathcal{R} x$.

$\mathcal{R} = \{ (x, y) \in \mathbb{R} \times \mathbb{R}, : x < y \}$.

- $\mathcal{R}$ é transitiva pois $(\forall x, y, z \in \mathbb{R})\, ((x < y \wedge y < z) \rightarrow x < z))$. Portanto
$$(\forall x, y, z \in \mathbb{R})\, (x \mathcal{R} y \wedge y \mathcal{R} z) \rightarrow x \mathcal{R} z.$$
- $\mathcal{R}$ é anti-simétrica, pois $(\forall x, y \in \mathbb{R})\, \neg((x < y \wedge y < x)$. Portanto, por vacuidade,
$$(\forall x, y \in \mathbb{R})\, (x \mathcal{R} y \wedge y \mathcal{R} x) \rightarrow x = y.$$

- Note que uma relação de ordem estrita não é um tipo particular de relação de ordem.
- Porém, toda relação de ordem estrita $\mathcal{R}$ pode ser obtida de uma relação de ordem $\mathcal{S}$ excluindo-se todos os pares da forma (a, a).
- Reciprocamente, toda relação de ordem $\mathcal{S}$ sobre um conjunto A é a união $\mathcal{R} \cup \mathcal{I}_A$ onde $\mathcal{R}$ é uma relação de ordem estrita sobre A.

- Seja $\mathcal{R}$ relação de ordem estrita e $\mathcal{S} = \mathcal{R} \cup \mathcal{I}_A$
- Note que, para quaisquer $a, b \in A$

$$a\mathcal{R}b \leftrightarrow (a\mathcal{S}b \wedge a \neq b)$$

$$a\mathcal{S}b \leftrightarrow (a\mathcal{R}b \vee a = b)$$

- Dizemos que $\mathcal{R}$ é a **ordem estrita associada à ordem** $\mathcal{S}$, e vice-versa.

Exemplo: A relação $\leq$ é uma ordem total sobre $\mathbb{R}$, pois $(\forall a, b \in \mathbb{R})\, a \leq b \vee b \leq a$.

A relação $\subseteq$ não é uma ordem total quando A tem pelo menos dois elementos, pois nesse caso existem subconjuntos distintos X e Y em $\mathbb{P}(A)$

Ordem total

Definição: Uma relação $\mathcal{R}$ é uma **ordem total** sobre um conjunto A (ou **ordem linear**) se, e somente se $\mathcal{R}$ é uma relação de ordem sobre A e quaisquer dois elementos de A são comparáveis por $\mathcal{R}$.

Portanto uma relação de ordem $\mathcal{R}$ é total se, quaisquer que sejam a e b em A, $(a, b) \in \mathcal{R}$ ou $(b, a) \in \mathcal{R}$. Se $\mathcal{R}$ é uma relação de ordem total sobre A, o par $(A, \mathcal{R})$ é chamado de **conjunto totalmente ordenado**.

Ordem lexicográfica

- Uma ordem muito importante no dia a dia, e em computação, é a **ordem alfabética** definida sobre palavras, nomes, etc.. Por exemplo, nesta ordem "`hoje`" vem antes de "`ontem`", "`biscoito`" vem antes de "`bolacha`", "`porco`" vem antes de `porta`", e "`sol`" vem antes de "`soldado`".

- Observe que esta ordem é baseada na ordem tradicional das letras do alfabeto: a, b, c, . . . , z.
- Compara-se a primeira letra de uma com a primeira letra da outra. Se forem diferentes, a ordem das palavras é a mesma das letras.
- Se as palavras começam com a mesma letra, compara-se a segunda letra de uma com a segunda da outra.

- Se persistir o empate, consideram-se as terceiras letras, as quartas letras, e assim por diante — até haver um desempate (letras diferentes na mesma posição das duas palavras), ou uma das palavras terminar. Neste último caso (como no exemplo de "`sol`" e "`soldado`"), convenciona-se que a palavra que termina primeiro vem antes da outra.

- Relação $\leq_2$ definida sobre os pares $\mathbb{R} \times \mathbb{R}$, pela fórmula

$$(a_1, a_2) \leq_2 (b_1, b_2) \leftrightarrow (a_1 < b_1) \vee (a_1 = b_1 \wedge a_2 \leq b_2)$$

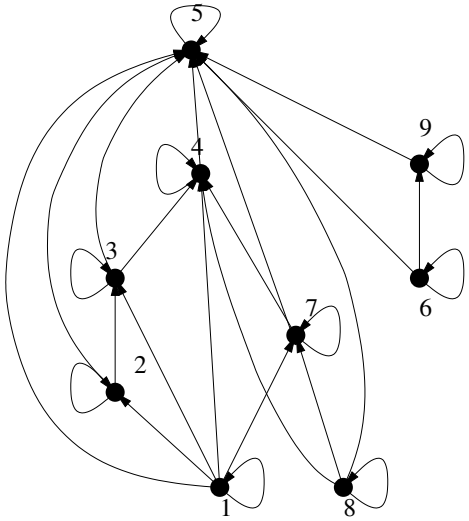
Diagrama de Hasse

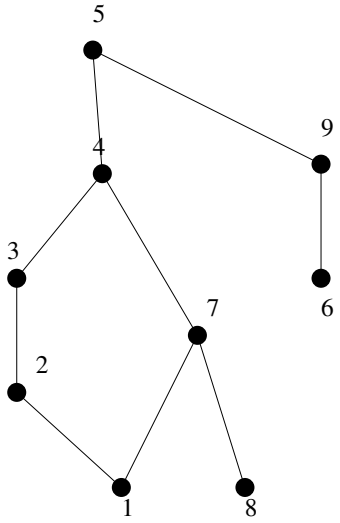
Podemos representar graficamente um conjunto ordenado $(A, \mathcal{R})$, onde A é finito e não muito grande, por um diagrama de pontos e linhas, chamado **diagrama de Hasse** (em homenagem ao matemático alemão Helmut Hasse, 1898–1979).

- cada elemento de A é representado por um ponto do plano, com posição arbitrária,
- exceto pela regra de que, para todo par $(a, b) \in \mathcal{R}$ com $a, b \in A$ e $a \neq b$, o ponto que representa a deve estar abaixo do ponto que representa b
- Cada um desses pares é representado por uma linha reta ligando a com b, exceto que pares que podem ser deduzidos por transitividade não são desenhados.

Para ilustrar a construção, vamos usar o conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, e a relação sobre A:

$$\begin{aligned}\mathcal{R} = \{\ & (1,1),\ (1,2),\ (1,3),\ (1,4),\ (1,5),\ (1,7),\\ & (2,2),\ (2,3),\ (2,4),\ (2,5),\\ & (3,3),\ (3,4),\ (3,5),\\ & (4,4),\ (4,5),\\ & (5,5),\\ & (6,6),\ (6,9),\ (6,5),\\ & (7,7),\ (7,4),\ (7,5),\\ & (8,8),\ (8,7),\ (8,4),\ (8,5),\\ & (9,9),\ (9,5)\ \}\end{aligned}$$





Elementos mínimos e máximos

Seja $\mathcal{R}$ uma relação de ordem sobre um conjunto X, e A um subconjunto de X. Um **elemento mínimo de A sob $\mathcal{R}$** é um elemento $m \in A$ se $(m, a) \in \mathcal{R}$ para todo $a \in A$.

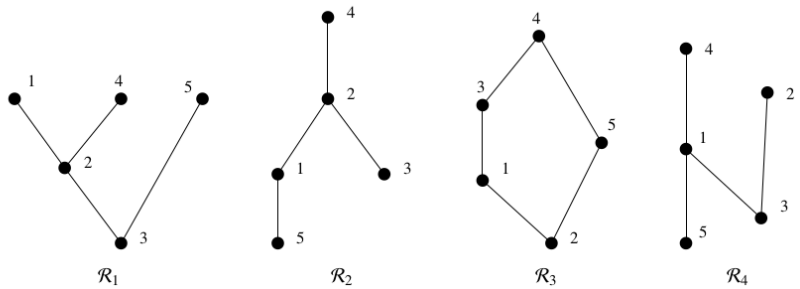
Exemplo: Considere o conjunto de conjuntos

$$A = \{\{1, 2, 4\}, \{2, 4\}, \{2, 3, 4\}, \{2, 4, 5\}, \{2, 3, 4, 6\}\}$$

e seja $\mathcal{R}$ a relação "$\subseteq$" entre conjuntos. O elemento $\{2, 4\}$ de A é mínimo sob $\mathcal{R}$, pois $\{2, 4\} \subseteq b$ para todo conjunto $b \in A$.

Um elemento m de A é **máximo** sob uma relação $\mathcal{R}$ se $(a, m) \in \mathcal{R}$ para todo $a \in A$.

No diagrama de Hasse de $\mathcal{R}$, o elemento mínimo existe se há um único ponto no diagrama a partir do qual é possível alcançar qualquer outro ponto por uma sequência de linhas, todas elas percorridas no sentido de baixo para cima. O elemento máximo, se existe, pode ser identificado de maneira análoga, isto é, se a partir dele podemos alcançar qualquer outro ponto percorrendo uma sequência de linhas no sentido descendente.



Diagramas de Hasse sobre o conjunto $\{1, 2, 3, 4, 5\}$. Na relação $\mathcal{R}_1$, mínimo: 3, máximo: não há. Na relação $\mathcal{R}_2$, mínimo: não há, máximo: 4. Na relação $\mathcal{R}_3$, mínimo: 2, máximo: 4. Na relação $\mathcal{R}_4$, mínimo: não há, máximo: não há.

Elementos minimais e maximais

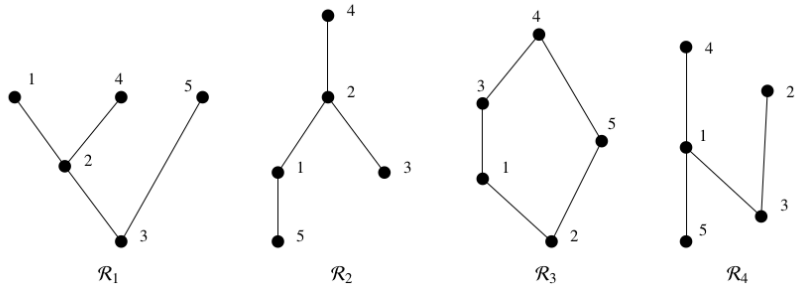
Seja $\mathcal{R}$ uma relação de ordem sobre um conjunto X, e A um subconjunto de X. Um **elemento minimal de** A **sob** $\mathcal{R}$ é um elemento $m \in A$ tal que não existe nenhum $a \in A$, diferente de m, com $(a, m) \in \mathcal{R}$.

Seja $A = \{1, 2, 3, 4, 5, 6\}$ e

$$\mathcal{R} = \{(1,1), (1,3), (2,2), (2,3), (3,3), (1,4), \\ (4,4), (2,4), (3,4), (5,5), (5,6), (6,6)\}.$$

O inteiro 2, por exemplo, é um elemento minimal de A sob $\mathcal{R}$, pois não existe nenhum par $(a, 2)$ na relação. Os elementos minimais de A sob $\mathcal{R}$ são 1, 2, e 5.

Um **elemento maximal de A sob** $\mathcal{R}$ é um elemento m de A tal que não existe nenhum a em A, diferente de m, tal que $(m, a) \in \mathcal{R}$.



Na relação $\mathcal{R}_1$, minimal: 3, maximais: 1, 4 e 5. Na relação $\mathcal{R}_2$, minimais: 3, 5, maximal: 4. Na relação $\mathcal{R}_3$, minimal: 2, maximal: 4. Na relação $\mathcal{R}_4$, minimais: 3 e 5, maximais: 2 e 4.

Os conceitos de minimal e maximal são muito usados quando A é um conjunto de conjuntos, e $\mathcal{R}$ é a relação '$\subseteq$'. Neste caso, um elemento minimal de A é um conjunto que não contém propriamente nenhum outro elemento de A. Por exemplo, seja

$$A = \{\{2\}, \{1,2\}, \{1,3\}, \{1,2,4\}, \{3,4,5\}\}$$

$$A = \{\{2\}, \{1,2\}, \{1,3\}, \{1,2,4\}, \{3,4,5\}\}$$

Neste conjunto, o elemento $\{1,2,4\}$ não é minimal, pois ele contém propriamente o conjunto $\{1,2\}$ que também está em A.
Por outro lado, $\{2\}$, $\{1,3\}$, e $\{3,4,5\}$ são minimais sob a relação '$\subseteq$'.
Analogamente o elemento $\{2\}$ não é maximal pois $\{2\} \subseteq \{1,2,4\}$.
Os elementos maximais de A sob $\subseteq$ são $\{1,3\}$, $\{1,2,4\}$ e $\{3,4,5\}$.

Relações de equivalência

Definição: Uma **relação de equivalência sobre** um conjunto A é uma relação $\mathcal{R}$ sobre A que é reflexiva sobre A, simétrica e transitiva.

Exemplo: Seja A o conjunto de todas as retas do plano, e seja $\mathcal{R}$ a relação $X\mathcal{R}Y$ se, e somente se, $X = Y$ ou $X \cap Y = \emptyset$. Esta relação é simplesmente a relação de paralelismo da geometria plana. Claramente a relação é reflexiva sobre A, simétrica e transitiva, logo é uma relação de equivalência.

Classes de equivalência

Seja $\mathcal{R}$ uma relação de equivalência sobre um conjunto A. Para todo elemento $a \in A$, o conjunto

$$[a]_{\mathcal{R}} = \{x \in A : x\mathcal{R}a\}$$

é denominado a **classe de equivalência** do elemento a na relação $\mathcal{R}$.

Exemplo: Vamos construir as classes de equivalência da relação $\mathcal{R}$ de congruência módulo 5. A classe de equivalência de um inteiro i na relação $\mathcal{R}$, é o conjunto

$$[i]_{\mathcal{R}} = \{x \in \mathbb{Z} : (\exists s \in \mathbb{Z})\, x - i = 5s\}$$

Ou seja, $x \in [i]_{\mathcal{R}}$ se e somente se $x = 5k + i$ para algum $k \in \mathbb{Z}$; isto é, se e somente se x tem o mesmo resto que i quando dividido por 5. Portanto existem apenas 5 classes de equivalência, que correspondem aos possíveis restos da divisão por 5:

- $[0]_{\mathcal{R}} = \{\cdots, -10, -5, 0, 5, 10, \cdots\}$.
- $[1]_{\mathcal{R}} = \{\cdots, -9, -4, 1, 6, 11 \cdots\}$.
- $[2]_{\mathcal{R}} = \{\cdots, -8, -3, 2, 7, 12 \cdots\}$.
- $[3]_{\mathcal{R}} = \{\cdots, -7, -2, 3, 8, 13, \cdots\}$.
- $[4]_{\mathcal{R}} = \{\cdots, -6, -1, 4, 9, 14, \cdots\}$.

Relações de equivalência e partições

Classes de uma relação de equivalência $\mathcal{R}$ sobre um conjunto A são duas a duas disjuntas. Como todo elemento de A está em alguma classe, a união de todas as classes é o conjunto A. Isto significa que as classes de equivalência de $\mathcal{R}$ formam uma partição do conjunto A.

Funções

Conceito

Uma **relação** $\mathcal{F}$ de A para B é uma **função de** A **para** B se, e somente se, para todo $a \in A$ existe **exatamente um** $b \in B$ tal que $(a, b) \in \mathcal{F}$.

- Usa-se geralmente a notação $\mathcal{F} : A \to B$.
- Para cada elemento a de A, é costume indicar por $\mathcal{F}(a)$ o **valor de** $\mathcal{F}$ **em** a,
- isto é, o único elemento b de B tal que $(a, b) \in \mathcal{F}$.
- Observe que esta notação só tem sentido para funções, e não para relações em geral.

Exemplo: A relação $\mathcal{F} = \{(1, 40), (2, 30), (3, 30)\}$ é uma função do conjunto $X = \{1, 2, 3\}$ para o conjunto $Y = \{20, 30, 40\}$, isto é $\mathcal{F} : X \to Y$.

Exemplo: A relação $\mathcal{F} = \{(1, 40), (3, 30)\}$ **não** é uma função de $X = \{1, 2, 3\}$ para $Y = \{20, 30, 40\}$, pois para $a = 2 \in X$ **não** existe um $b \in Y$ tal que $(a, b) \in \mathcal{F}$.

Exemplo: A relação $\mathcal{F} = \{(1, 40), (2, 20), (2, 30), (3, 30)\}$ **não** é uma função de $X = \{1, 2, 3\}$ para $Y = \{20, 30, 40\}$, pois para $a = 2 \in X$ existem **dois** valores distintos $b' = 20 \in Y$ e $b'' = 30 \in Y$ tais que $(a, b') \in \mathcal{F}$ e $(a, b'') \in \mathcal{F}$.

Exemplo: A relação $\mathcal{F} = \left\{(x, x^2) : x \in \mathbb{Z}\right\}$ é uma função do conjunto $\mathbb{Z}$ para o conjunto $\mathbb{N}$, isto é $\mathcal{F} : \mathbb{Z} \to \mathbb{N}$.

Exemplo: A relação $\mathcal{F} = \left\{(x^2, x) : x \in \mathbb{Z}\right\}$ **não** é uma função do conjunto $\mathbb{N}$ para o conjunto $\mathbb{Z}$, pois há elementos $a \in \mathbb{N}$ (como $a = 5$) para os quais não existe par $(a, b) \in \mathcal{F}$, e há elementos $a \in \mathbb{N}$ (como $a = 4$) para os quais existem dois pares $(a, b) \in \mathcal{F}$ (no caso, $(4, 2)$ e $(4, -2)$).

Em geral, usaremos letras minúsculas, como f, g, etc., para relações que são funções.

Domínio e imagem de uma função

- Todos os conceitos introduzidos para relações (como domínio, composição, inversa, etc.) valem também para funções.

- Se f é uma função de A para B, então, de acordo com a definição, o domínio $\mathrm{Dom}(f)$ de f é sempre o conjunto A.
- A imagem ou contra-domínio $\mathrm{Img}(f)$ de f é o conjunto

$$Img(f) = \{f(a) : a \in A\} = \{b \in B : (\exists a \in A)\, b = f(a)\}$$

Observe que a imagem está contida no conjunto B, mas nem sempre é igual a B.

Exercício: Seja f uma função e $\mathcal{R}$ uma relaçao sobre $\mathrm{Dom}(f)$ tal que para todo x e y $x\mathcal{R}y \leftrightarrow f(x) = f(y)$ para todo $x, y \in \mathrm{Dom}(f)$.

- Prove que $\mathcal{R}$ é uma relação de equivalência.
- Encontre as classes de equivalência de $\mathcal{R}$.

Inversa de função

A inversa de uma função f é a relação

$$f^{-1} = \{\, (y, x) : (x, y) \in f \,\}$$

Note que a inversa de uma função nem sempre é uma função.

Exemplo: Seja f a função de $\mathbb{R}$ para $\mathbb{R}$ tal que $f(x) = x^2$. Sua inversa é a relação

$$f^{-1} = \left\{ (x^2, x) : x \in \mathbb{R} \right\}$$

que associa a cada número real $y \geq 0$ suas duas raízes quadradas $-\sqrt{y}$ e $+\sqrt{y}$.

Composição de funções

A composição de duas funções f e g é definida da mesma forma que para relações,

$$g \circ f = \{\, (a, c) : (\exists b)\, (a, b) \in f \wedge (b, c) \in g \,\}$$

Em particular, se $f : A \to B$ e $g : B \to C$, então verifica-se que $g \circ f$ é uma função de A para C, e para todo $a \in A$ o valor de $g \circ f$ em a é definido pela fórmula:

$$(g \circ f)(a) = g(f(a))$$

Por exemplo
$f : \mathbb{R} \to \mathbb{R}$ com $f(x) = 2x + 3$,
$g : \mathbb{R} \to \mathbb{R}$ com $g(x) = 3x + 2$. Então
$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11$ e
$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$.
Este exemplo mostra que a composição de funções não é comutativa.

Função injetora
Uma função f de A para B é **injetora** se, e somente se, $(\forall x, y \in A)\,(f(x) = f(y) \rightarrow (x = y)$.
Ou seja, se e somente se ela atribui um valor diferente para cada elemento do domínio.

Uma função injetora **preserva informação**, pois o valor de $f(x)$ determina univocamente o valor de x. Funções injetoras também são chamadas de funções **um para um**.

Exercício: Sejam f e g duas funções. Prove que se $g \circ f$ não é injetora então pelo menos uma dentre f e g não é injetora.

Função sobrejetora
Dizemos que uma função f de A para B é **sobrejetora em** B (ou é uma função de A **sobre** B) se, e somente se, $(\forall b \in B)\,(\exists a \in A)\,f(a) = b$. Ou seja, f é uma função sobre B se e somente se $B = Img(f)$. Note que não tem sentido dizer que uma função "é sobrejetora" sem especificar em qual conjunto. Por exemplo, a função f com domínio $\mathbb{Z}$ tal que $f(x) = |x|$ é tanto uma função de $\mathbb{Z}$ para $\mathbb{Z}$ quanto de $\mathbb{Z}$ para $\mathbb{N}$; ela é sobrejetora em $\mathbb{N}$, mas não em $\mathbb{Z}$.

Exercício: Sejam $f : A \to B$, $g : B \to C$. Prove que se f é sobrejetora em B, e g é sobrejetora em C, então $g \circ f$ é sobrejetora em C.

Função bijetora

Definição: Uma função f de A para B é **bijetora de A para B** (ou é uma **bijeção de A para B**) se, e somente se, f é injetora e sobrejetora em B.

Funções bijetoras são muito importantes em matemática e computação. Entre outras coisas, elas permitem definir o "tamanho" de conjuntos infinitos.

Função permutação

Uma **função permutação** de um conjunto A, ou uma **permutação** de A, é uma função bijetora de A para A. Observe que a relação de identidade sobre A é uma permutação (trivial) de A.

Exemplo: A função

$$f = \{(10, 10), (11, 12), (12, 13), (13, 11), (14, 15), (15, 14)\}$$

é uma permutação do conjunto $A = \{10, 11, 12, 13, 14, 15\}$.

Exemplo: Sejam m, n inteiros positivos quaisquer, e seja $A = \{ x \in \mathbb{N} : x < n \}$. Seja $f : A \to A$ tal que $f(x)$ é o resto da divisão de $x + m$ por n. Verifica-se que f é uma permutação de A

Exercício: Liste todas as permutações do conjunto $A = \{10, 20, 30\}$.

Por ser bijetora, toda permutação de um conjunto A tem uma inversa, que também é uma permutação de A. A composição de duas permutações de A é uma permutação de A.

Uma permutação f de um conjunto A pode ser interpretada como uma maneira de colocar os elementos de A em um conjunto de caixas, cada uma rotulada com um elemento de A. Ou seja, a permutação f está dizendo que o elemento x de A está na caixa de rótulo $f(x)$. Ou, alternativamente, que a caixa de rótulo x contém o elemento $f(x)$.

Permutações são muito importantes em computação. Por exemplo, a ordenação dos elementos de uma lista de n elementos, ou dos n registros de um arquivo, pode ser vista como a aplicação de uma permutação dos índices $\{0..\, n-1\}$.

Se f é função permutação de A, todas as potências de f, positivas e negativas, são permutações de A. Nesse caso define-se também a potência nula f^0 de f como sendo a identidade sobre o domínio A.

Funções piso e teto

Definição: A **função piso** (também chamada de **chão** ou **solo**) associa a cada número real x o maior inteiro que é menor ou igual a x. Este inteiro é denotado por $\lfloor x \rfloor$.

Observe que $\lfloor 1/3 \rfloor = \lfloor 2/3 \rfloor = 0$, $\lfloor -1/3 \rfloor = -1$, $\lfloor -2/3 \rfloor = -1$ e $\lfloor 5 \rfloor = 5$.

Definição: A **função teto** associa a cada número real x o menor inteiro que é maior ou igual a x. Este inteiro é denotado por $\lceil x \rceil$.

Observe que $\lceil 5/4 \rceil = 2$, $\lceil 7/4 \rceil = 2$, $\lceil -1/4 \rceil = 0$, $\lceil -3/4 \rceil = 0$ e $\lceil 4 \rceil = 4$

Tanto o piso quanto o teto são funções do conjunto $\mathbb{R}$ para o conjunto $\mathbb{Z}$. Essas funções tem algumas propriedades importantes:

- $\lfloor x \rfloor = n$ se, e somente se, $n \leq x < n + 1$.
- $\lfloor x \rfloor = n$ se, e somente se, $x - 1 < n \leq x$.
- $\lceil x \rceil = n$ se, e somente se, $n - 1 < x \leq n$.
- $\lceil x \rceil = n$ se, e somente se, $x \leq n < x + 1$.
- $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.
- $\lfloor -x \rfloor = -\lceil x \rceil$.
- $\lceil -x \rceil = -\lfloor x \rfloor$.

Em matemática, a divisão inteira é indicada às vezes pelo símbolo antigo '÷', e o resto pela sigla ' mod ', ambos usados como operações entre dois inteiros. Dessa forma podemos escrever $17 \div 3 = 5$ e $17 \bmod 3 = 2$.

Quociente inteiro e resto

Os conceitos de divisão (quociente) e resto de um número natural x por um inteiro positivo d são conhecidos e consensuais desde a antiguidade:
17 dividido por 3 é 5 com resto 2.
O resto dessa divisão é também chamado *x módulo d*

Estas operações podem ser definidas usando a função piso:

$$x \div d = \left\lfloor \frac{x}{d} \right\rfloor$$

$$x \bmod d = x - d(x \div d) = x - d\left\lfloor \frac{x}{d} \right\rfloor$$

$$x \div d = \left\lfloor \frac{x}{d} \right\rfloor$$

$$x \bmod d = x - d(x \div d) = x - d\left\lfloor \frac{x}{d} \right\rfloor$$

Em matemática, estas fórmulas são adotadas como definições dessas duas operações também no caso de x ser um inteiro negativo. Assim,
$(-17) \div 3 = \lfloor -17/3 \rfloor = -6$, e portanto
$(-17) \bmod 3 = (-17) - 3(-6) = 1$.

Algumas linguagens de programação modernas, como Python, usam as definições acima, embora com outros símbolos. Outras linguagens, como C e Fortran, calculam $|x| \div d$ e $|x| \bmod d$, e devolvem o resultado com o sinal de x.

Não há consenso sobre a definição de $x \div d$ ou $x \bmod d$ quando d é negativo. Felizmente, este caso raramente ocorre, na prática ou na teoria.

Exercício: O dia da semana do dia primeiro de janeiro de um ano $n \geq 1582$ pode ser determinado pela fórmula:

$$\left(n + \left\lfloor \frac{n-1}{4} \right\rfloor - \left\lfloor \frac{n-1}{100} \right\rfloor + \left\lfloor \frac{n-1}{400} \right\rfloor\right) \mod 7$$

Se o resultado for 0, o dia primeiro de janeiro cai num domingo, se for 1 numa segunda-feira, etc..

- Use essa fórmula para encontrar o dia da semana de primeiro de janeiro do ano de seu aniversário.
- Justifique esta fórmula.

Fatorial

Uma função importante em computação é o **fatorial** de um número natural n, denotado por $n!$ e definido como o produto

$$n! \;=\; \prod_{k=1}^{n} k \;=\; 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n \qquad (8)$$

Por exemplo, $1! = 1$, $2! = 1 \cdot 2 = 2$, $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$, etc.. Note que quando n é zero a produtória acima é vazia, portanto $0! = 1$.

Função característica

A **função característica** de uma conjunto A qualquer é uma função f cujo domínio é o conjunto universal $\mathcal{U}$,e tal que, para qualquer elemento z, $f(z)$ é um valor lógico, **V** se z pertence a A, e **F** caso contrário. Denotaremos esta função por χ_A.
Ou seja $\chi_A(z)$ tem o mesmo valor lógico que a fórmula "$z \in A$".
Podemos ver a função χ_A como uma representação do conjunto A.

Sequências finitas

Uma **sequência finita** é uma função x cujo domínio é um intervalo de inteiros $\{\, n \in \mathbb{Z} : r \le n \le s \,\}$, onde r e s são inteiros; que pode ser abreviado para $\{r..\, s\}$. Se os valores de x pertencem a um conjunto A, dizemos que x é uma sequência finita **sobre** A. Em algumas áreas da matemática e da computação, sequências finita também são chamadas de **listas**, **palavras**, **cadeias** ou **ênuplas**

A imagem de um inteiro n por uma sequência x é habitualmente denotada por x_n (em vez de $x(n)$). Os pares (n, x_n) são os **termos** ou **elementos** da sequência; o inteiro n é o **índice** do termo, e x_n é seu **valor**. Os inteiros r e s são o **índice inicial** e o **índice final** da sequência.

Exemplo: Seja $x : \{2..6\} \to \mathbb{R}$ cujos termos são $\{(2,4),(3,9),(4,16),(5,25),(6,36)\}$. Podemos então escrever que $x_2 = 4$, $x_3 = 9$, e $x_n = n^2$ para todo $n \in \{2..6\}$.

Note que uma sequência especifica não apenas os valores dos termos mas também sua ordem e seus índices. Note também que uma sequência pode ter mais de um termo com o mesmo valor. Duas sequências são iguais se, e somente se, elas tem exatamente os mesmos termos — mesmos índices e mesmos valores.

Notação para sequências finitas

Quando o índice inicial r é especificado pelo contexto, uma sequência finita é geralmente denotada colocando-se os valores dos termos entre parênteses e separados por vírgulas. Por exemplo, se convencionamos que os índices começam com zero, a notação $(1, 2, 2, 5)$ representa a sequência $\{(0, 1), (1, 2), (2, 2), (3, 5)\}$.

A sequência (2) não é a mesma coisa que o inteiro 2. Além disso, pela definição acima, a sequência $(2, 3)$ não é a mesma coisa que o par ordenado $(2, 3)$. Devido a esta confusão, alguns autores (e algumas linguagens de programação) usam outros símbolos, como colchetes angulares $\langle \ldots \rangle$, ou colchetes comuns $[\ldots]$, no lugar de parênteses para denotar sequências.

Índice inicial padrão

Em matemática (e em algumas linguagens de programação, como `FORTRAN`), o índice inicial de uma sequência é geralmente 1 por convenção. Uma vantagem desta escolha é que o n-ésimo elemento de uma sequência x é x_n.

Alguns autores, entretanto, preferem numerar os termos a partir de 0. Note que, neste caso, em uma sequência com n termos os índices variam de 0 a $n-1$. Além disso, o elemento de índice k (ou seja x_k) é o $k+1$-ésimo elemento da sequência. Mesmo assim, a numeração a partir de 0 tem certas vantagens em computação e é o padrão de várias linguagens de programação modernas, como `C`, `Java` e `Python`.

Comprimento

O **comprimento** de uma sequência finita é o número de termos, geralmente denotado por $|x|$.

> **Exercício:** Se uma sequência tem índice inicial r e índice final s, qual é o seu comprimento? Se ela tem índice inicial 0 e comprimento n, qual é o índice final? E se ela tem índice inicial 1 e comprimento n?

Há uma única sequência de comprimento zero, a **sequência vazia**, denotada por $()$, que tem domínio vazio e portanto não tem nenhum termo. Neste caso os índices inicial e final não são definidos. Note que o intervalo $\{r..s\}$ é vazio para quaisquer r e s com $r > s$.

Concatenação

Informalmente, a **concatenação** de duas sequências finitas x e y é uma sequência finita que tem todos os termos de x, seguidos de todos os termos de y. Por exemplo, a concatenação de $(10, 20, 30)$ e $(40, 50)$ é $(10, 20, 30, 40, 50)$.

Esta operação pode ser indicada de muitas maneiras, por exemplo com um ponto $x \cdot y$, com uma barra $x|y$ ou com a mera justaposição xy. Obviamente, o comprimento da concatenação é a soma dos comprimentos das duas sequências.

Para definir precisamente este conceito é preciso estabelecer um índice inicial para a sequência resultante. Por exemplo, se convencionarmos que todas as sequências tem índice inicial zero, a concatenação é a sequência z tal que

$$z_n = \begin{cases} x_n, & \text{se } 0 \le n < p \\ y_{n-p}, & \text{se } p \le n < p + q \end{cases} \quad (9)$$

onde $p = |x|$ e $q = |y|$.

Exercício: Adapte a fórmula da concatenação (9) para a convenção em que todas as sequências tem índice inicial 1.

Exercício: Escreva a fórmula geral da concatenação (9) para o caso em que os domínios de x e y são $\{r' .. s'\}$ e $\{r'' .. s''\}$, respectivamente, e o índice inicial do resultado é r.

Observe que, se o índice inicial é fixo, a concatenação com a sequência vazia não tem efeito nenhum: $x \cdot () = () \cdot x = x$ para qualquer sequência finita x.

Subsequências e subcadeias

Segundo alguns autores, uma **subsequência** de uma sequência x é simplesmente uma restrição y de x a um subconjunto R de seu domínio. Por exemplo, segundo esta definição, a função $y = \{(3, 30), (5, 20)\}$ é a subsequência de $x = \{(2, 20), (3, 30), (4, 30), (5, 20)\}$ determinada pelo conjunto $R = \{3, 5\}$.

Uma desvantagem desta definição é que a subsequência nem sempre é uma sequência, pois o novo domínio R nem sempre é um intervalo de inteiros consecutivos. Por esse motivo, alguns autores especificam que os termos da subsequência devem ter seus índices alterados para inteiros consecutivos a partir de um início convencional. Com esta definição, e com índice inicial 0, a função $y = \{(0, 30), (1, 20)\}$ é a subsequência de $x = \{(0, 20), (1, 30), (2, 30), (3, 20)\}$ determinada pelo conjunto $R = \{1, 3\}$.

Alguns autores usam a palavra **subcadeia** para indicar que o conjunto R é um intervalo de inteiros. Muitas linguagens de programação incluem funções para extrair subcadeias de cadeias dadas.

Somatórias e produtórias

Muitas quantidades importantes em matemática são definidas como a soma de uma quantidade variável de parcelas também variáveis, por exemplo a soma $2^1 + 2^2 + \cdots + 2^n$, para algum inteiro n. Para estas situações, uma notação muito prática é a **somatória** (também chamada **somatório** ou **notação sigma**), introduzida por Joseph Fourier em 1820. Nesta notação, a soma acima é escrita

$$\sum_{k=1}^{n} 2^k \qquad \text{ou} \qquad \sum\nolimits_{k=1}^{n} 2^k$$

Em geral, a notação sigma tem a forma

$$\sum_{k=m}^{n} f(k) \qquad \text{ou} \qquad \sum_{k=m}^{n} f(k)$$

onde k é uma variável arbitrária (o **índice** ou a **variável indexadora**), $f(k)$ é uma fórmula qualquer que depende de k (o **termo geral** da somatória), e m, n são inteiros que não dependem de k.

Esta soma também pode ser escrita

$$\sum_{\substack{k \\ m \le k \le n}} f(k)$$

Costuma-se simplificar esta notação para

$$\sum_{m \le k \le n} f(k)$$

quando a variável índice k é óbvia pelo contexto.

Uma variante mais geral da notação Σ é

$$\sum_{\substack{k \\ P(k)}} f(k)$$

$$\sum_{\substack{1 \le k \le 10 \\ k \text{ ímpar}}} k^2 = 1^2 + 3^2 + 5^2 + 7^2 + 9^2 \qquad (10)$$

$$\sum_{\substack{p \text{ primo} \\ p \text{ divide } 140}} \frac{1}{p} = \frac{1}{2} + \frac{1}{5} + \frac{1}{7} \qquad (11)$$

Outra variante similar desta notação é

$$\sum_{k \in K} f(k)$$

Observe que se o domínio é vazio, o valor da somatória é zero, por definição. Em particular, a somatória $\sum_{k=m}^{n} f(k)$ é zero sempre que $m > n$.

Somatórias básicas

$$\sum_{k=1}^{n} 1 = n$$

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} = \binom{n+1}{2}$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

$$\sum_{k=0}^{n-1} 2^k = 2^n - 1$$

Manipulação de somatórias

A notação Σ pode ser manipulada de várias maneiras. Em primeiro lugar, observe que a variável índice k pode ser substituída por qualquer outra letra $i, j, l, \ldots$ que não tenha significado definido no contexto. Podemos também trocar a variável indexadora k por uma variável relacionada a ela de maneira biunívoca, com o intervalo de variação devidamente ajustado.

Exemplo: Trocando a variável k pela variável $i = k - 1$, temos

$$\sum_{k=1}^{n} 2^k = \sum_{i=0}^{n-1} 2^{i+1}$$

Note que para identificar o intervalo da variável i usamos a equação $i = k - 1$, enquanto que para modificar o termo usamos a equação equivalente $k = i + 1$.

Exemplo: Podemos simplificar a somatória

$$\sum_{\substack{1 \le k \le 10 \\ k \text{ ímpar}}} k^2 = 1^2 + 3^2 + 5^2 + 7^2 + 9^2$$

trocando a variável k por $2i + 1$, resultando em

$$\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} (2i + 1)^2$$

Note que a equação

$$\sum_{\substack{p \text{ primo} \\ p \text{ divide } 140}} \frac{1}{p} = \frac{1}{2} + \frac{1}{5} + \frac{1}{7}$$

não pode ser simplificada desta maneira, pois não se conhece uma fórmula explícita para os números primos.

Distributividade: Para qualquer número c

$$\sum_{k \in K} cf(k) = c\left(\sum_{k \in K} f(k)\right)$$

Esta propriedade nos permite mover fatores constantes (que não dependem do índice) para dentro ou para fora da somatória.

Associatividade:

$$\sum_{k \in K} (f(k) + g(k)) = \sum_{k \in K} f(k) + \sum_{k \in K} g(k)$$

A associatividade nos permite substituir uma somatória de somas pela soma de somatórias sobre os mesmos índices, ou vice-versa.

Decomposição do domínio: Se $\{K_1, K_2\}$ é uma partição de K, então

$$\sum_{k \in K} f(k) = \left(\sum_{k \in K_1} f(k)\right) + \left(\sum_{k \in K_2} f(k)\right)$$

Esta regra diz que podemos quebrar uma somatória em duas somatórias parciais, desde que cada valor do índice apareça no domínio de uma, e apenas uma, dessas duas partes. Esta regra pode ser generalizada para partições do domínio K em qualquer número de partes.

Comutatividade: Se p é uma permutação qualquer de K,

$$\sum_{k \in K} f(k) = \sum_{k \in K} f(p(k))$$

A comutatividade nos diz que podemos colocar os termos em qualquer ordem. Uma versão mais geral desta regra é:

Troca de domínio: Se p é uma função bijetora qualquer de K para um conjunto $J \subseteq \mathbb{Z}$,

$$\sum_{k \in K} f(p(k)) = \sum_{j \in J} f(j)$$

Foi o que fizemos em:

$$\sum_{k=1}^{n} 2^k = \sum_{i=0}^{n-1} 2^{i+1}$$

Exemplo: Seja x uma sequência qualquer de números reais, e considere a somatória $\sum_{k=1}^{n}(x_{k+1} - x_k)$. Usando essas regras, podemos reescrever a somatória como segue:

$$\begin{aligned}
\sum_{k=1}^{n}(x_{k+1} - x_k) &= \sum_{k=1}^{n} x_{k+1} - \sum_{k=1}^{n} x_k \\
&= \sum_{i=2}^{n+1} x_i - \sum_{k=1}^{n} x_k \\
&= \sum_{i=2}^{n} x_i + x_{n+1} - x_1 - \sum_{k=2}^{n} x_k \\
&= x_{n+1} - x_1
\end{aligned}$$

A identidade do exemplo é conhecida como **somatória telescópica** porque uma parte de cada parcela "está encaixada em" (isto é, cancela) uma parte da parcela anterior, como ocorre com as peças de uma luneta.

Para calcular a somatória $\sum_{k=1}^{n} k^2$, observamos que $(k+1)^3 = k^3 + 3k^2 + 3k + 1$, portanto $(k+1)^3 - k^3 = 3k^2 + 3k + 1$. Temos então que

$$\sum_{k=1}^{n}((k+1)^3 - k^3) = \sum_{k=1}^{n}(3k^2 + 3k + 1)$$

O lado esquerdo é uma soma telescópica, portanto temos

$$(n+1)^3 - 1 = 3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1$$

ou seja

$$\begin{aligned} 3\sum_{k=1}^{n} k^2 &= (n+1)^3 - 1 - 3\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 \\ &= (n+1)^3 - 1 - 3n(n+1)/2 - n \\ &= (2n^3 + 3n^2 + n)/2 \end{aligned}$$

Logo

$$\sum_{k=1}^{n} k^2 = (n(n+1)(2n+1))/6$$

Exercício: [Soma de PA] Calcule a somatória $\sum_{k=1}^{n}(a + r(k-1))$, cujas n parcelas são parte de uma progressão aritmética com termo inicial a e passo r arbitrários.

Somatórias múltiplas

Os termos de uma somatória podem ser especificados por dois ou mais índices, como no exemplo abaixo:

$$\sum_{\substack{j,k \\ 1\le j\le 3 \\ 2\le k\le 4}} f(j,k) = \begin{aligned} & f(1,2) + f(1,3) + f(1,4) + \\ & f(2,2) + f(2,3) + f(2,4) + \\ & f(3,2) + f(3,3) + f(3,4) \end{aligned} \qquad (12)$$

Este mesmo exemplo pode ser também escrito usando duas vezes a notação Σ, isto é, como uma somatória de somatórias:

$$\sum_{\substack{j,k \\ 1\le j\le 3 \\ 2\le k\le 4}} f(j,k) = \sum_{1\le j\le 3} \sum_{2\le k\le 4} f(j,k) = \sum_{2\le k\le 4} \sum_{1\le j\le 3} f(j,k)$$

Podemos entender as fórmulas anteriores como duas maneiras de somar todos os elementos de uma matriz: coluna por coluna ou linha por linha.

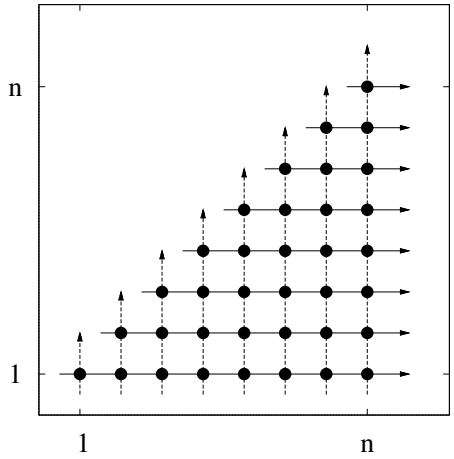
Mudança de ordem de somatórias

Podemos trocar a ordem de duas somatórias, quando o domínio de cada variável é independente da outra variável:

$$\sum_{j\in J}\sum_{k\in K} f(j,k) = \sum_{\substack{j\in J\\ k\in K}} f(j,k) = \sum_{k\in K}\sum_{j\in J} f(j,k).$$

Quando o domínio da soma interna depende da variável índice da somatória externa, a troca exige mais cuidado. Por exemplo,

$$\sum_{j=1}^{n}\sum_{k=j}^{n} a_{j,k} = \sum_{1\le j\le k\le n} a_{j,k} = \sum_{k=1}^{n}\sum_{j=1}^{k} a_{j,k}.$$



O eixo horizontal é a variável k, o eixo vertical é a variável j.

Exercício: Para todo número inteiro positivo n, o n-ésimo número hamônico é

$$H_n = \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} \cdots \frac{1}{n}.$$

Prove que, para todo inteiro n maior ou igual a 2,

$$\sum_{k=1}^{n} H_k = (n+1)H_n - n.$$

Distributividade generalizada

Outra regra importante para somatórias duplas é a da **distributividade generalizada**, que permite trocar o produto de duas somatórias por uma somatória dupla. Para quaisquer conjuntos $J, K \subseteq \mathbb{Z}$, e quaisquer funções $f : J \to \mathbb{R}$, $g : K \to \mathbb{R}$

$$\left(\sum_{j \in J} f(j)\right)\left(\sum_{k \in K} g(k)\right) = \sum_{\substack{j \in J \\ k \in K}} f(j)g(k) = \sum_{j \in J} \sum_{k \in K} f(j)g(k)$$

Note que esta regra também permite trocar uma somatória dupla por um produto de duas somatórias. Para isso basta que o domínio da somatória interna não dependa do índice da soma externa, e que o termo geral possa ser fatorado no produto de duas fórmulas, cada uma delas dependendo de um dos dois índices apenas.

Majoração de somatórias

Muitas vezes não precisamos saber o valor exato de uma somatória, basta saber um limitante superior ou inferior.

Majoração dos termos:
Algumas vezes um bom limitante para o valor de uma somatória pode ser obtido limitando cada um de seus termos pelo termo de maior valor. Por exemplo:

$$\begin{aligned}\sum_{k=1}^{n} \frac{k+1}{k} &= \frac{2}{1} + \frac{3}{2} + \cdots + \frac{n}{n-1} \\ &\leq \sum_{k=1}^{n} 2 \\ &= 2n.\end{aligned}$$

Também podemos majorar cada termo da somatória por alguma outra fórmula cuja somatória é conhecida. Por exemplo, observe que, para todo $k \in \mathbb{N}$, temos

$$\frac{k}{k+1} 2^k < 2^k$$

Podemos então concluir que

$$\begin{aligned}\sum_{k=0}^{n} \frac{k}{k+1} 2^k &< \sum_{k=0}^{n} 2^k \\ &= 2^{n+1} - 1.\end{aligned}$$

Majoração por integrais:
Suponha que f é uma função crescente de $\mathbb{N}$ para $\mathbb{R}$. Por exemplo $f(x) = x^2$.
Agora considere o seguinte somatório.

$$\sum_{x=m}^{n} x^2$$

Considere uma outra função $f^* : \mathbb{R} \leftarrow \mathbb{R}, f^*(x) = x^2$. Podemos observar que:

$$\begin{aligned}\sum_{x=m}^{n} x^2 &\leq \int_{m}^{n+1} x^2 \\ &= \frac{x^3}{3}\Big|_{n}^{n+1} \\ &= \frac{(n+1)^3 (m)^3}{3}\end{aligned}$$

Minoração por integrais: Analogamente podemos utilizar integrais para encontrar um limitante inferior para uma somatória. Por exemplo:

$$\sum_{x=1}^{n} \frac{1}{x} \geq \int_{1}^{n+1} \frac{1}{x} = \ln x \Big|_{1}^{n+1} = \ln(n+1) - \ln 1 = \ln(n+1)$$

Somas infinitas

A notação Σ é também usada para **somas infinitas**, também chamadas de **séries**. Uma somatória infinita é o limite de uma somatória finita, quando o valor máximo da variável indexada tende para infinito. Ou seja,

$$\sum_{k=0}^{\infty} f(k) = \lim_{n \to \infty} \sum_{k=0}^{n} f(k)$$

$$\sum_{k=0}^{\infty} \frac{1}{2^k} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 2$$

e

$$\sum_{k=0}^{\infty} 2^k = 1 + 2 + 4 + 8 + \ldots = +\infty$$

Observe que o limite pode não existir, ou pode ser infinito. Um exemplo clássico é a soma dos inversos dos inteiros positivos,

$$\sum_{k=1}^{\infty} \frac{1}{k}$$

A soma dos n primeiros termos é o número harmônico H_n que é maior ou igual a $\ln(n+1)$, e portanto tende a infinito quando n tende a infinito.

Produtórias

Sejam m, n números inteiros e f uma função definida sobre os inteiros. A notação

$$\prod_{k=m}^{n} f(k)$$

denota o produto dos valores $f(k)$ para todos os inteiros k tais que $m \leq k \leq n$.

Uma fórmula deste tipo é chamada de **produtória** ou **produtório**. Se não existe nenhum k no intervalo especificado (isto é, se $m > n$), o valor desta fórmula é 1 (e não zero!), por definição.

Exercício: Calcule o valor da produtória $\prod_{k=-2}^{+2} k^2 + 1$.

Exercício: Dê fórmulas explícitas (sem $\prod$ nem '...') para o valor das produtórias abaixo:

1. $\prod_{k=1}^{n} 3$
2. $\prod_{k=1}^{n} k$
3. $\prod_{k=-n}^{n} k$

Sequências infinitas e recorrências

Sequências infinitas

- Uma **sequência infinita** é uma função cujo domínio é um conjunto da forma $\{ n \in \mathbb{Z} : n \geq r \}$ para algum inteiro r.
- Tipicamente o índice inicial r é 1 ou 0 (especialmente para computação).
- Valem os mesmos conceitos vistos para sequências finitas. Vale lembrar:
- Definimos x_n como o **termo geral** da sequência.

Exemplo: Seja $x : \mathbb{N} \to \mathbb{R}$ onde $x_n = n^2$, para todo $n \in \mathbb{N}$. Os termos da sequência são: $x_0 = 0$, $x_1 = 1$, $x_2 = 4$, $x_3 = 9$, ...

- Também podemos definir sequências cujo domínio são todos os inteiros $\mathbb{Z}$, nesse caso dizemos que a sequência é bi-infinita.
- Também valem os conceitos de subsequência vistos anteriormente.

- Uma sequência infinita não pode ser especificada listando todos seus termos.
- Devemos definir o termo geral x_n por algum critério preciso que depende da variável índice n.
- Não precisa ser uma fórmula algébrica. Por exemplo, considere a sequência p cujos termos são os inteiros primos, em ordem crescente de valor. Os primeiros termos dessa sequência são $2, 3, 5, 7, 11, 13, 17 \ldots$.
- Os termos da sequência estão bem definidos, porém até hoje não se conhece nenhuma fórmula algébrica para o termo geral p_n.

Recorrência

- Muitas sequências importantes são definidas recursivamente.
  Exemplo: A sequência dos **números de Fibonacci** é definida por

$$f_0 = 0 \qquad f_1 = 1$$
$$f_n = f_{n-2} + f_{n-1} \quad \text{para todo } n \geq 2$$

  Os primeiros termos dessa sequência são $0, 1, 1, 2, 3, 5, 8, \ldots$.
- fornecendo-se um ou mais termos iniciais e uma fórmula que determina os demais termos. Essa fórmula é chamada de **recorrência**.

Exemplo: Uma **progressão aritmética** (PA) é uma sequência x definida pela recorrência

$$\begin{aligned} x_0 &= a \\ x_n &= x_{n-1} + r \quad \text{para todo } n > 0 \end{aligned}$$

onde a e r são valores reais, chamados de **termo inicial** e **passo** ou **incremento** da progressão.

Qual é o x_{10000} termo dessa sequência? Precisamos calcular todos os termos anteriores?

$$x_n = a + nr$$

Exemplo: Uma **progressão geométrica** (PG) é uma sequência x definida pela recorrência

$$\begin{aligned} x_0 &= a \\ x_n &= x_{n-1} \cdot r \quad \text{para todo } n \geq 1 \end{aligned}$$

onde a e r são valores reais, chamados de **termo inicial** e **razão** da progressão.

$$x_n = ar^n$$

Exercício: Suponha que um casal de tatus marciano começa a dar crias com dois anos de idade e produz 6 crias (três casais) de tatuzinhos a cada ano. Suponha que um rancho de criação de tatus começou com 1 casal recém-nascido em 2000, e que nenhum tatu foi acrescentado ou eliminado do "rebanho" desde essa época. Escreva uma definição recursiva para o número x_n de tatus que existem no ano n.

- Determinar uma fórmula explícita para uma sequência definida recursivamente é um problema difícil em geral, mas há técnicas que resolvem certos casos especiais.

Recorrência aditiva simples

- Um desses casos especiais são as recorrências da forma

$$x_0 = a$$
$$x_n = x_{n-1} + f(n) \text{ para todo } n \geq 1$$

onde f é uma função qualquer.

$$x_0 = a$$
$$x_n = x_{n-1} + f(n) \text{ para todo } n \geq 1$$

- Podemos verificar com indução que a solução desta recorrência é:

$$x_n = x_0 + \sum_{k=1}^{n} f(k)$$

Considere uma Progressão aritmética, onde $f(n) = r$ (e portanto não depende de n.

$$x_0 = a$$
$$x_n = x_{n-1} + r \text{ para todo } n \geq 1$$

$$x_n = x_0 + \sum_{k=1}^{n} f(k) = a + \sum_{k=1}^{n} r$$
$$x_n = a + nr$$

Exercício: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned} x_0 &= 0 \\ x_n &= x_{n-1} + 2n \quad \text{para todo } n \leq 1 \end{aligned}$$

Recorrência multiplicativa simples

- Outro caso especial são as recorrências da forma

$$\begin{aligned} x_0 &= a \\ x_n &= f(n) \cdot x_{n-1} \text{ para todo } n \geq 1 \end{aligned}$$

onde f é uma função qualquer.

$$\begin{aligned} x_0 &= a \\ x_n &= f(n) \cdot x_{n-1} \text{ para todo } n \geq 1 \end{aligned}$$

- Verificamos que para $n \geq 1$

$$x_n = x_0 \cdot \prod_{k=1}^{n} f(k)$$

- Uma Progressão geométrica é um caso particular onde $f(n) = r$ e não depende de n.

$$\begin{aligned} x_0 &= a \\ x_n &= r \cdot x_{n-1} \text{ para todo } n \geq 1 \end{aligned}$$

Então para $n \geq 1$

$$\begin{aligned} x_n &= a \cdot \prod_{k=1}^{n} r \\ x_n &= ar^n \end{aligned}$$

Exercício: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned} x_0 &= 1 \\ x_n &= \tfrac{2}{n} x_{n-1} \quad \text{para todo } n > 0 \end{aligned}$$

- O índice inicial (caso base) pode ser um m qualquer diferente de 0.
- As recorrências podem ser mais complexas do que as apresentadas. Algumas podem ter uma solução. Outras talvez não.
- As vezes pode ser suficiente encontrar uma majoração ou uma minoração para uma recorrência.
- Algumas recorrências podem ser resolvidas através do *Teorema Mestre*

Contagem

- Um problema comum em matemática, e especialmente em computação, é contar objetos matemáticos (conjuntos, funções, sequências, etc.) com determinadas propriedades.
- Por exemplo, quantas maneiras diferentes há de escolher 5 cartas de um baralho com 52 cartas?

- Quantas palavras (com ou sem significado) podem ser formadas com 5 letras distintas? Quantas maneiras há de ordenar um arquivo de n nomes?
- Já encontramos alguns problemas desse tipo nos capítulos anteriores. Por exemplo, vimos que o número de subconjuntos de um conjunto com n elementos é 2^n.

- é importante notar se os objetos que aparecem no enunciado são considerados distintos ou não.
- Por exemplo, observe a questão “quantos resultados é possivel obter quando dois dados são lançados sobre uma mesa?”

- Se os dados são considerados distintos (por exemplo, um vermelho e um verde), a resposta é $6 \times 6 = 36$. Note que o resultado “2 no vermelho e 4 no verde” é considerado diferente de “4 no vermelho e 2 no verde”.
- Porém, se os dados são considerados indistinguíveis, a resposta é apenas 21; pois, por exemplo, o resultado “2 em um dado e 4 no outro” é o mesmo que “4 em um dado e 2 no outro”.

Exercício: Liste e conte todas as maneiras possíveis de colocar 3 bolas, rotuladas de 1 a 3, em duas caixas rotuladas A e B. Note que cada caixa pode ficar vazia ou com mais de uma bola.

Agora responda à mesma pergunta, supondo que

a) As bolas são todas iguais e sem rótulos, mas as caixas ainda são distintas;
b) As bolas são todas distintas, mas as caixas são iguais e sem rótulos;
c) As bolas são todas iguais e as caixas também, todas sem rótulos.

Contagem de relações

- Suponha que X e Y são conjuntos finitos, com $|X| = m$ e $|Y| = n$. Quantas relações existem de X para Y? Lembramos que uma relação de X para Y é um subconjunto do produto cartesiano $X \times Y$, que tem mn elementos.
- Concluímos que a resposta é 2^{mn}. Pelo mesmo argumento, o número de relações sobre o conjunto X (isto é, de X para X) é 2^{m^2}.

- $|X| = m$.
- Quantas são as relações **reflexivas** sobre o conjunto X? Para responder a esta pergunta, basta lembrar que uma relação reflexiva sobre X deve conter a relação de identidade $\mathcal{I}_X$, que consiste dos pares (a, a) com $a \in X$. Então, cada relação que queremos contar consiste desses m pares, mais um subconjunto arbitrário dos demais $m^2 - m = m(m-1)$ pares de $X \times X$. Concluímos que o número de relações reflexivas sobre X é $2^{m(m-1)}$.

Contagem de funções

- Suponha ainda que X e Y são conjuntos finitos, com $|X| = m$ e $|Y| = n$. Quantas **funções** distintas existem de X para Y?
- Lembramos que, se $\mathcal{F}$ é uma dessas funções, então para cada elemento a de X deve existir um único par em $\mathcal{F}$ cujo primeiro membro é a.
- Portanto $\mathcal{F}$ tem apenas m pares. Em cada um desses pares, o segundo membro (o valor $\mathcal{F}(a)$ da função) pode ser qualquer um dos n elementos de Y.

- $|X| = m$, $|Y| = n$.
- Temos então n valores possíveis da função para cada um dos m elementos de X. Concluímos que o número de funções de X para Y é n^m.

  Exercício: Quantas maneiras há de empilhar cinco frutas, que podem ser laranjas (indistinguíveis entre si) ou maçãs (também indistinguíveis) dentro um vaso estreito de vidro?

- Temos então n valores possíveis da função para cada um dos m elementos de X. Concluímos que o número de funções de X para Y é n^m.

  Exercício: Quantas maneiras há de empilhar cinco frutas, que podem ser laranjas (indistinguíveis entre si) ou maçãs (também indistinguíveis) dentro um vaso estreito de vidro?

Princípio multiplicativo da contagem

- Quantas maneiras existem de enfileirar 7 crianças, sendo 4 meninas e 3 meninos, de modo a alternar meninos e meninas.
- Podemos pensar em formar a fila com 7 decisões sucessivas, onde na decisão número i escolhemos a criança que vai ficar na posição i da fila.
- Assim, começamos escolhendo uma meninas para ficar no começo da fila (pois se escolhermos um menino não será possível intercalar as demais).

- Em seguida temos que escolher um dos 3 meninos para ficar em segundo lugar.
- Depois temos que escolher outra menina, que não pode ser a que ficou em primeiro lugar; temos portanto apenas 3 alternativas possíveis nessa escolha.
- Analogamente, temos apenas 2 alternativas para o quarto lugar (um dos dois meninos ainda não escolhidos), 2 alternativas para o quinto (uma de duas meninas), e apenas 1 alternativa para o sexto e o sétimo lugares.

- Pode-se ver que qualquer disposição alternada das crianças pode ser obtida por esse processo; e que qualquer variação nas escolhas resultará em uma disposição diferente. Portanto, o numero de maneiras de arranjar as crianças é

$$4 \times 3 \times 3 \times 2 \times 2 \times 1 \times 1 = 144 \qquad (13)$$

Princípio multiplicativo da contagem

O raciocínio usado neste problema é uma instância do **princípio multiplicativo da contagem**, ou **princípio fundamental da contagem**.

- Para usar esse princípio, temos que imaginar o processo de construção ou escolha de um dos objetos a contar como uma sequência finita de decisões $D_1, D_2, \ldots, D_r$, de tal forma que cada combinação diferente de escolhas nessas decisões produza um objeto diferente, e todos os objetos possam ser obtidos por esse processo.
- Nesse caso, se cada decisão D_i pode ter n_i escolhas distintas, então o número de objetos será

$$n_1 \times n_2 \times \cdots \times n_r \tag{14}$$

Exercício: Quantos números inteiros existem entre 1000 e 9999 com todos os algarismos distintos?

Permutações

- Seja X um conjunto finito de n elementos. Informalmente, uma **permutação de** X é uma lista dos elementos de X em determinada ordem, sem repetições nem omissões.
- Mais precisamente, podemos definir uma permutação de X como uma função f bijetora do conjunto $\{0, 1, \ldots, n-1\}$ para o conjunto X. Podemos interpretar o valor de $f(k)$ como o elemento que está na posição k da lista, contando a partir de 0.

Por exemplo, suponha que X é o conjunto das vogais, $X = \{\mathtt{a}, \mathtt{e}, \mathtt{i}, \mathtt{o}, \mathtt{u}\}$. A função

$$\{(0, \mathtt{u}), (1, \mathtt{e}), (2, \mathtt{i}), (3, \mathtt{a}), (4, \mathtt{o})\}$$

é uma permutação de X. Esta função pode ser escrita também como

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ \mathtt{u} & \mathtt{e} & \mathtt{i} & \mathtt{a} & \mathtt{o} \end{pmatrix}$$

ou como a sequência $(\mathtt{u}, \mathtt{e}, \mathtt{i}, \mathtt{a}, \mathtt{o})$ ou, simplesmente, $\mathtt{ueiao}$; ficando subentendido que os índices da sequência começam com 0.

- Duas outras permutações, distintas dessa, são $\mathtt{uieao} = (\mathtt{u}, \mathtt{i}, \mathtt{e}, \mathtt{a}, \mathtt{o})$ e $\mathtt{eaoiu} = (\mathtt{e}, \mathtt{a}, \mathtt{o}, \mathtt{i}, \mathtt{u})$.
- Quantas permutações de $X = \{\mathtt{a}, \mathtt{e}, \mathtt{i}, \mathtt{o}, \mathtt{u}\}$ existem? Quando tentamos escrever uma permutação f, elemento a elemento, é fácil ver que temos n escolhas para o elemento $f(0)$ (qualquer elemento de X); $n-1$ escolhas para $f(1)$ (qualquer elemento de X, exceto $f(0)$); $n-2$ para $f(2)$ (qualquer elemento exceto $f(0)$ e $f(1)$); e assim por diante.

- Para o penúltimo elemento $f(n-2)$ temos apenas 2 possibilidades e para o último $f(n-1)$ temos apenas uma. Qualquer série de escolhas resulta em uma permutação distinta. Portanto o número de permutações distintas é

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n! \qquad (15)$$

- Assim, por exemplo, o número de permutações das cinco vogais é $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$.

- Observe que se o conjunto X é vazio (isto é, se $n = 0$) há apenas uma permutação possível, que é a sequência vazia $()$.
- Esta observação justifica a definição de $0!$ como sendo 1.
- Suponha que n pessoas (com $n \geq 2$) devem sentar em uma fila de n cadeiras, mas duas dessas pessoas, Alice e Beto, são um casal e devem ficar um ao lado do outro. De quantas maneiras isto pode ser feito?
- $2(n-1)!$

- O fatorial de n cresce muito rapidamente quando n aumenta. Por exemplo,

$$20! = 2.432.902.008.176.640.000$$

  ou seja, mais de dois quintilhões (bilhões de bilhões).
- O fatorial de 50 é aproximadamente 3.04×10^{64}, que é muito maior que o número de átomos no sistema solar.

- Assim, embora possamos facilmente calcular o **número** de permutações de um baralho de 52 cartas, é impossível **gerar** todas essas permutações em qualquer computador concebível atualmente.

Fórmula de Stirling

- A fórmula $n \times (n-1) \times \ldots \times 2! \times 1!$ não é adequada para calcular $n!$ quando n é muito grande.
- Por exemplo, para calcular 1000000! temos que multiplicar 1000000 de números, e o produto vai crescendo a cada passo; o resultado tem mais de 5 milhões de algarismos.

- Uma fórmula que permite estimar o valor aproximado do fatorial com menos trabalho foi encontrada por Abraham de Moivre (1667–1754) e James Stirling (1692–1770):

$$\ln n! \approx n \ln n - n + \frac{1}{2} \ln(2\pi n)$$

  onde $\ln$ é o logaritmo natural (na base $e = 2.7182818\ldots$). Aplicando $\exp(x) = e^x$ em ambos os lados temos

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Arranjos

- Dado um conjunto finito X de n elementos, e um inteiro $r \in \mathbb{N}$, definimos um **arranjo de r elementos de X** como uma sequência de elementos de X com comprimento r, em determinada ordem e sem repetições. Ou seja, uma função injetora dos inteiros $\{0..\, r-1\}$ para o conjunto X.

Por exemplo, os arranjos de 3 elementos do conjunto $X = \{\mathtt{a}, \mathtt{e}, \mathtt{i}, \mathtt{o}, \mathtt{u}\}$. Onde `aie` significa a sequência $(\mathtt{a}, \mathtt{i}, \mathtt{e})$, ou seja a função

$$\begin{pmatrix} 0 & 1 & 2 \\ \mathtt{a} & \mathtt{i} & \mathtt{e} \end{pmatrix}$$

e assim por diante.

```
aei  aie  eai  eia  iae  iea
aeo  aoe  eao  eoa  oae  oea
aio  aoi  iao  ioa  oai  oia
aeu  aue  eau  eua  uae  uea
aiu  aui  iau  iua  uai  uia
aou  auo  oau  oua  uao  uoa
eio  eoi  ieo  ioe  oei  oie
eiu  eui  ieu  iue  uei  uie
eou  euo  oeu  oue  ueo  uoe
iou  iuo  oiu  oui  uio  uoi
```


- Concluímos que o número de tais arranjos (ou seja, o número de funções injetoras de um conjunto de r elementos para um conjunto de n elementos) é

$$n \times (n-1) \times (n-2) \times \cdots \times (n-r+1) \qquad (16)$$

$$n \times (n-1) \times (n-2) \times \cdots \times (n-r+1)$$

- Em muitos livros este número é denotado por A_n^r (lê-se "arranjos de n, tomados r a r"). Alguns autores usam a notação A_r^n. Outra notação, usada por Knuth, é $n^{\underline{r}}$ (lê-se "n à potência r caindo"). Este número pode ser calculado a partir de fatoriais, pela fórmula

$$\frac{n!}{(n-r)!} \qquad (17)$$

$$\frac{n!}{(n-r)!}$$

- Note que os fatores do denominador cancelam uma parte dos fatores do numerador, deixando apenas os fatores da fórmula (16). Assim, por exemplo, o número de arranjos de 3 vogais, listados acima, é $5!/(5-3)! = 5 \times 4 \times 3 = 60$.

- Uma maneira de entender a fórmula $\frac{n!}{(n-r)!}$ é considerar todas as $n!$ permutações de n elementos, e imaginar o que ocorre se tomarmos apenas os r primeiros elementos de cada uma, para obter os arranjos. Note que duas permutações que diferem apenas na ordem dos $n-r$ elementos descartados produzem o mesmo arranjo. Há $(n-r)!$ maneiras de ordenar esses elementos descartados, sem mexer nos r primeiros. Portanto, das $n!$ permutações, $(n-r)!$ correspondem a um mesmo arranjo.

Combinações

- Outro problema muito comum é contar o **número de subconjuntos de tamanho** r de um conjunto X de n elementos.
- Diferente dos arranjos, neste caso a ordem dos elementos em cada subconjunto não interessa.

- Estes subconjuntos são também chamados de **combinações** de r elementos de X. Assim, por exemplo, as combinações de 3 vogais são

```
aei  aeo  aio  aeu  aiu
aou  eio  eiu  eou  iou
```

onde `aiu` significa o sub-conjunto $\{\mathtt{a}, \mathtt{i}, \mathtt{u}\}$, e assim por diante.

- O número de tais combinações acima é denotado por C_n^r (ou C_r^n) por alguns autores, porém a notação mais comum é $\binom{n}{r}$, que se lê "combinações de n, tomados r a r", ou "n escolhe r"
- Para contar as combinações, podemos determinar o número de arranjos de r elementos, e contar apenas uma vez todos os arranjos que diferem apenas na ordem dos elementos. Por exemplo, os seis arranjos `aio`, `aoi`, `iao`, `ioa`, `oai` e `oia` correspondem à mesma combinação $\{\mathtt{a}, \mathtt{i}, \mathtt{o}\}$.

- Como temos r elementos em cada arranjo, concluímos que cada combinação corresponde a $r!$ arranjos diferentes. Portanto, o número de combinações é

$$\frac{A_n^r}{r!} = \frac{n \times (n-1) \times \cdots \times (n-r+1)}{r \times (r-1) \times \cdots \times 1} \tag{18}$$

Esta fórmula pode ser escrita em termos de fatoriais

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} \tag{19}$$

Exercício: Quantas "mãos" diferentes de cinco cartas podem ser obtidas de um baralho de 52 cartas?

Casos especiais

- Alguns casos especiais são dignos de nota. Para todo $n \in \mathbb{N}$,

$$\binom{n}{0} = \binom{n}{n} = 1$$

- Para todo inteiro n positivo,

$$\binom{n}{1} = \binom{n}{n-1} = n$$

- e, para todo inteiro n maior que 1,

$$\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$$

- Além disso, é óbvio que $\binom{n}{r}$ é zero se r é maior que n.
- A definição de $\binom{n}{r}$ não faz muito sentido quando n e/ou r são negativos. Porém, a experiência mostra que muitos teoremas e fórmulas ficam mais simples quando definimos $\binom{n}{r} = 0$ quando $n < 0$ ou $r < 0$.

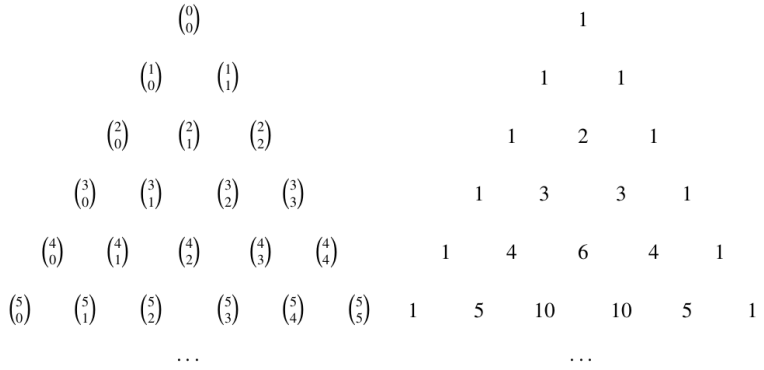
Propriedades

- A função $\binom{n}{r}$ tem várias propriedades interessantes. Por exemplo, para todo $n, r \in \mathbb{N}$, temos

$$\binom{n}{r} = \binom{n}{n-r}$$

- Considere um conjunto X de n elementos, e observe que para cada conjunto de r elementos existe um único conjunto de $n - r$ elementos que é seu complemento, e vice-versa.

Outra propriedade importante é a **identidade de Pascal**



- **identidade de Pascal**:

$$\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}$$

- Para provar esta identidade, considere um conjunto X' de $n+1$ elementos e escolha um elemento arbitrário x de X'.
- Seja X o conjunto dos demais elementos, $X = X' \setminus \{x\}$.

- Considere agora todos os subconjuntos de X' com $r+1$ elementos. Eles podem ser separados em dois grupos:
  - aqueles que contém o elemento escolhido x, e
  - aqueles que não contém x.
- Os primeiros são exatamente os $\binom{n}{r}$ subconjuntos de X de tamanho r, cada um deles acrescido do elemento x.
- Os segundos são exatamente os $\binom{n}{r+1}$ subconjuntos de X de tamanho $r+1$.

Fórmula do Binômio de Newton

Uma das propriedades mais famosas das combinações é a fórmula de Newton para as potências de um binômio (soma de dois termos):

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} b^r$$

Por exemplo, temos $(a+b)^4$

$$\begin{aligned} &= \binom{4}{0}a^4b^0 + \binom{4}{1}a^3b^1 + \binom{4}{2}a^2b^2 + \binom{4}{3}a^1b^3 + \binom{4}{4}a^0b^4 \\ &= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4 \end{aligned}$$

Por conta desta fórmula, os números $\binom{n}{r}$ são também chamados de **coeficientes binomiais**.

Fórmula recursiva

- A fórmula $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ não é muito eficiente quando n e r são números grandes, pois o numerador $n!$ e denominador $(n-r)!r!$ podem ser muito maiores que o resultado final $\binom{n}{r}$.
- Esta observação também vale se usarmos a fórmula, $C_n^r = A_n^r / r!$.

- Uma maneira mais eficiente é utilizar a recorrência

$$\binom{n}{r} = \begin{cases} \frac{n}{r}\binom{n-1}{r-1} & \text{se } n \geq r > 0, \\ 1 & \text{se } n \geq r = 0, \\ 0 & \text{se } n < r \text{ ou } r < 0. \end{cases}$$

- Esta recorrência pode ser demonstrada por indução em r. Para provar o passo da indução, basta observar que o lado direito da equação pode ser fatorada como segue

$$\binom{n}{r} = \frac{n}{r}\left(\frac{n-1}{r-1}\frac{n-2}{r-2}\cdots\frac{n-r+1}{1}\right)$$

e que a parte entre parênteses é $\binom{n-1}{r-1}$. Ou seja,

$$\binom{n}{r} = \prod_{k=1}^{r}\frac{n-r+k}{k}$$

- Podemos portanto calcular $\binom{n}{r}$ pelo seguinte algoritmo:
  1. Se $n < r$ ou $r < 0$, devolva 0. Senão
  2. $C \leftarrow 1$
  3. Para k variando de 1 a r, faça
  4. $\quad C \leftarrow (C \times (n-r+k))/k$
  5. Devolva C.
- Neste algoritmo é importante efetuar a multiplicação por $n-r+k$ antes de dividir por k. Isto garante que a divisão será exata.

Partições rotuladas e combinações com repetições

- Quantas maneiras há de distribuir 10 doces para 4 crianças, de modo que cada criança receba pelo menos um doce?

- Uma maneira de resolver este problema é imaginar que os 10 doces são colocados numa fileira, com barras separando os lotes dados a cada criança, numa ordem escolhida. Por exemplo, “ooo | oooo | o | oo” representaria a solução onde a primeira criança recebe 3 doces, a segunda recebe 4, a terceira 1, e a quarta 2.

- Observe que precisamos colocar 3 barras (para separar os lotes de 4 crianças), não podemos colocar duas barras na mesma posição, nem no início da fileira de doces, nem no fim dela (porque todas as crianças precisam receber pelo menos um doce).
- Há portanto 9 posições possíveis para as barras (para 10 doces), e cada solução válida é um subconjunto de 3 dessas posições. Portanto a resposta é $\binom{9}{3} = 84$.

- Mais geralmente, suponha que queremos repartir n elementos em p grupos distintos, sendo que cada grupo deve ter pelo menos um elemento. Ou seja, queremos saber quantas sequências $(x_1, x_2, \ldots, x_p)$ de inteiros positivos existem tais que $x_1 + x_2 + \cdots + x_p = n$.
- Pelo mesmo raciocínio acima, concluímos que a resposta é

$$\binom{n-1}{p-1} = \frac{(n-1)!}{(n-p)!(p-1)!} = \binom{n-1}{n-p} \tag{20}$$

- Suponha agora o poblema de dividir 6 doces para 4 crianças, mas permitindo que uma ou mais crianças fiquem sem nenhum doce.
- Podemos fazer este problema (P_0) recair no anterior, com o seguinte truque: distribuímos 10 doces para as 4 crianças, garantindo pelo menos um doce para cada uma; e então recolhemos 1 doce de cada criança.

- Pode-se verificar que cada solução para este problema (P_1) dá uma solução diferente para o problema P_0, e vice-versa.
- Portanto, o número de soluções do problema P_0 é também $\binom{9}{3} = 84$.

- Mais geralmente, suponha que queremos repartir n elementos em p grupos distintos, mas permitindo que cada grupo fique vazio.
- Matematicamente, queremos saber quantas soluções existem para a equação $x_1 + x_2 + \cdots + x_p = n$, sendo que cada incógnita x_i deve ser um número natural (incluindo 0).

- Podemos transformar este problema no anterior pela seguinte estratégia: contamos o número de soluções para $y_1 + y_2 + \cdots + y_p = n + p$ onde cada y_i é um inteiro positivo.
- Note que cada solução destas fornece uma solução distinta para o problema original, com $x_i = y_i - 1$; e vice-versa. Portanto, o número de soluções é

$$\binom{n+p-1}{p-1} = \frac{(n+p-1)!}{n!(p-1)!} = \binom{n+p-1}{n} \qquad (21)$$

- O problema de dividir 10 doces por 4 crianças pode também ser visto como escolher 10 elementos do conjunto $C = \{1, 2, 3, 4\}$, mas permitindo que cada elemento seja escolhido mais de uma vez; de modo que cada solução não é um conjunto, mas um **multiconjunto** — uma coleção de elementos onde a ordem não importa, mas importa quantas vezes cada elemento aparece.

- Por exemplo, uma solução seria $\{1, 1, 1, 2, 2, 2, 2, 3, 4, 4\}$ (3 doces para a criança 1, 4 doces para a criança 2, etc.), que é diferente da solução $\{1, 1, 2, 2, 2, 2, 3, 4, 4, 4\}$.

- Mais geralmente, queremos saber quantos multiconjuntos, cada um com n elementos no total, podem ser formados com os p elementos de um dado conjunto C.
- Estes multi-conjuntos são as **combinações com repetição desses p elementos tomados n a n**, e seu número é dado pela fórmula $\binom{n+p-1}{p-1} = \frac{(n+p-1)!}{n!(p-1)!} = \binom{n+p-1}{n}$.

- Note que esta contagem inclui também os multi-conjuntos que usam apenas alguns dos elementos de C. Se queremos considerar apenas as combinações com repetição que usam todo elemento de C pelo menos uma vez, devemos usar a fórmula $\binom{n-1}{p-1} = \frac{(n-1)!}{(n-p)!(p-1)!} = \binom{n-1}{n-p}$.

Exercício: De quantos modos podemos comprar 3 sorvetes numa sorveteria que oferece 7 sabores distintos? (Note que podemos comprar mais de um sorvete do mesmo sabor.)

Permutações e arranjos circulares

- Considere uma roleta dividida em 5 setores idênticos. De quantas maneiras podemos rotular esses setores com as vogais `A`, `E`, `I`, `O`, `U`, em ordem arbitrária?
- Se os setores fossem distinguíveis, a resposta seria o número de permutações de 5 elementos, isto é, 5!.

- Para justificar este resultado, basta imaginar os setores numerados de 1 a 5 em ordem horária a partir de um setor determinado.
- Cada rotulação é então uma função bijetora dos números de 1 a 5 para as 5 vogais.

- Porém, como os setores são idênticos, duas permutações distintas podem resultar em rotulações idênticas. Por exemplo, obteremos o mesmo resultado se rotularmos os setores, em ordem horária, $(\mathtt{A}, \mathtt{E}, \mathtt{I}, \mathtt{O}, \mathtt{U})$, ou com $(\mathtt{U}, \mathtt{A}, \mathtt{E}, \mathtt{I}, \mathtt{O})$, ou com $(\mathtt{O}, \mathtt{U}, \mathtt{A}, \mathtt{E}, \mathtt{I})$, etc..
- Observe que cada rotulação distinta corresponde a 5 permutações distintas das cinco vogais. Portanto, o número de rotulações distintas deve ser $5!/5 = 4!$.

- Outra maneira de obter este resultado é imaginar que as vogais são aplicadas uma de cada vez, em ordem alfabética, em setores arbitrários. Como os setores são indistinguíveis, há apenas uma maneira de aplicar a letra A (e não cinco).

- Já a vogal E pode ser aplicada de 4 maneiras distintas, pois os outros 4 setores agora podem ser distinguidos pela sua posição em relação ao setor já rotulado.
- Da mesma forma temos 3 escolhas distintas para a letra I, 2 para O, e 1 para U. Portanto o número configurações é $1 \times 4 \times 3 \times 2 \times 1 = 4!$.

- Este exemplo ilustra o conceito de **permutação circular**: uma configuração de elementos distintos dispostos em círculo, sendo que configurações que diferem apenas por rotação são consideradas indistinguíveis. Generalizando o raciocínio acima, concluímos que o número de permutações circulares de n elementos é

$$\frac{n!}{n} = (n-1)! \tag{22}$$

Exercício: Quantas rodas distintas de 5 crianças podemos formar numa classe de 10 crianças? E de quantas maneiras podemos formar duas rodas de 5 com essas 10 crianças?

Contagem por divisão

- Mais geralmente, suponha que temos que contar um conjunto Y da forma

$$Y = \{ f(x) : x \in X \} \tag{23}$$

onde X é algum outro conjunto finito, e f é uma função de X para Y. Se todo elemento de y é imagem de exatamente m elementos distintos de X, então $|Y| = |X| / m$.

- No exemplo das vogais, X é o conjunto de permutações das 5 vogais, Y são as rotulações distinguíveis dos setores da roleta, e $f(x)$ é a rotulação que se obtém quando os setores são rotulados segundo a permutação x.

Exercício: Em uma brincadeira com n crianças, $n-1$ crianças formam uma roda e uma delas fica no centro da roda. De quantas maneiras distintas é possível arranjar essas n crianças dessa forma?

Permutações e arranjos com elementos indistinguíveis

- Outro exemplo da técnica acima é contar os anagramas da palavra `BANANAS`; isto é, quantas sequências de 7 letras podem ser formadas rearranjando as letras da palavra `BANANAS`?

- Podemos obter cada uma dessas palavras tomando uma permutação dos números de 1 a 7, e aplicando à mesma uma função f que transforma o número 1 em `B`, os números 2 e 3 em `N`, os números 4, 5 e 6 em `A`, e o número 7 em `S`. Por exemplo,

$$\begin{array}{rcll} f(1,2,3,4,5,6,7) & = & \texttt{BNNAAAS} & \\ f(4,1,5,2,3,6,7) & = & \texttt{ABANNAS} & \\ f(1,4,2,5,3,6,7) & = & \texttt{BANANAS} & (24) \\ f(1,6,3,5,2,4,7) & = & \texttt{BANANAS} & \\ f(7,2,1,4,5,6,3) & = & \texttt{SABANAN} & \end{array}$$

  e assim por diante.

- Quantas permutações geram a mesma palavra? Observe que a palavra não muda se trocarmos as posições dos valores 2 e 3 entre si; e/ou se trocarmos os valores 4, 5 e 6 entre si, nas $3! = 6$ maneiras possíveis. Quaisquer outras trocas de valores causam a troca de letras distintas.
- Portanto, cada palavra possível é obtida a partir de exatamente $2 \times 6 = 12$ permutações distintas. O número de palavras distintas é então $7!/12 = 420$.

- Mais geralmente, considere o problema de contar as sequências $(x_1, x_2, \ldots, x_n)$ de n elementos, que podem ter p valores distintos $v_1, v_2, \ldots, v_p$; sendo que cada sequência deve ter exatamente m_i elementos iguais a v_i, para cada i.
- Pelo raciocínio acima, podemos concluir que o número de tais sequências é

$$\frac{n!}{m_1!\, m_2! \cdots, m_p!} \tag{25}$$

Combinações múltiplas

- O número $\binom{n}{r}$ pode ser definido também como o número de maneiras de colocar n objetos distintos em duas caixas distintas, com r elementos na primeira caixa, e $n - r$ na segunda caixa. (Comparando com a definição usada na aula anterior, pode-se ver que o conteúdo da primeira caixa corresponde ao sub-conjunto escolhido do conjunto X, com r elementos, e a segunda caixa ao complemento desse sub-conjunto em relação a X.)

- Esta definição alternativa pode ser generalizada para qualquer número positivo t de caixas. Ou seja, podemos perguntar quantas maneiras existem de distribuir n objetos em t caixas **distintas**, com r_1 elementos na caixa 1, r_2 elementos na caixa 2, e assim por diante. Obviamente isso é possível apenas se $r_1 + r_2 + \cdots + r_t = n$.

- Um raciocínio análogo ao utilizado na aula anterior permite concluir que esse número é

$$\binom{n}{r_1, r_2, \ldots, r_t} = \frac{n!}{r_1! r_2! \cdots r_t!} \tag{26}$$

- Por exemplo, suponha que temos 10 pessoas para distribuir em três comissões A, B e C com, respectivamente, 5, 3, e 2 membros. Isso pode ser feito de

$$\binom{10}{5,3,2} = \frac{10!}{5!3!2!} = 2520 \qquad (27)$$

maneiras distintas.

Exercício: Quantas maneiras existem de distribuir 5 cartas para cada um de 4 jogadores, de um baralho de 52 cartas?(Note que, além das 4 mãos distribuídas, há também um monte de 32 cartas não distribuídas.)

Exercício: Quantas maneiras distintas existem de pintar 20 casas com as cores vermelha, azul, verde e amarela (cada casa de uma só cor), sendo que deve haver o mesmo número de casas de cada cor?

Princípio aditivo da contagem

- Consideremos agora o problema de contar quantos números pares de 4 dígitos distintos existem. Ou seja, quantas sequências de 4 algarismos podemos formar, sendo o dígito dos milhares (o mais a esquerda) não pode ser ‘0’, e o dígito das unidades (o mais à direita) só pode ser ‘0’, ‘2’, ‘4’, ‘6’ ou ‘8’.

- Esta contagem não pode ser feita apenas com o princípio multiplicativo, pois o número de escolhas possíveis para o dígito das unidades depende de quantos dígitos pares foram escolhidos nas outras posições, e vice-versa. Por exemplo, se o dígito das unidades for ‘0’ há 9 possibilidades para o dos milhares, enquanto que se for ‘2’ há apenas 8 escolhas.

- Neste caso podemos separar os números a contar em dois casos: o conjunto A dos que terminam em '0', e o conjunto B dos que terminam com '2', '4', '6' ou '8'.
- No primeiro caso, temos uma escolha ('0') para as unidades, e 9 escolhas para as dezenas. Para cada uma destas escolhas temos 8 escolhas para as centenas; para cada destas, temos 7 escolhas para os milhares. Portanto, $|A| = 1 \times 9 \times 8 \times 7 = 504$.

- No segundo caso, temos 4 escolhas para as unidades. Para cada uma destas, temos 8 escolhas para os milhares (não pode ser o das unidades, nem '0'). Mas, para cada uma destas escolhas, temos também 8 escolhas para as centenas (pois nesta posição podemos usar '0'); e para cada destas temos 7 nas dezenas. Portanto, $|B| = 4 \times 8 \times 8 \times 7 = 1792$. A contagem de todas as possibilidades é então $|A| + |B| = 2296$.

- Este exemplo é uma instância do **princípio aditivo da contagem**, ou **contagem por casos**: se os objetos a serem contados podem ser divididos em conjuntos $A_1, A_2, \ldots, A_n$, **disjuntos dois a dois**, então o número total de objetos é $|A_1| + |A_2| + \cdots + |A_n|$.

Princípio subtrativo da contagem

- Considere agora o problema de contar os números de 1000 a 9999 (inclusive ambos) nos quais o algarismo '3' aparece pelo menos uma vez. A solução N deste problema apenas pelo método aditivo e multiplicativo é relativamente trabalhosa. Uma solução mais simples é contar todos os números entre 1000 e 9999 (que são 9000), e subtrair desse total a contagem K dos números nesse intervalo onde o algarismo '3' **não** aparece.

- Nesta contagem, há 8 possibilidades para o algarismo dos milhares, e 9 para cada um dos outros três algarismos. Portanto, $K = 8 \times 9^3 = 5832$, e $N = 9000 - K = 3168$.

- Podemos chamar a técnica ilustrada por este exemplo de **princípio subtrativo da contagem**. Em geral, para contar um conjunto X, podemos contar um conjunto Y que contém X, e subtrair o número de elementos que foram contados a mais, ou seja a cardinalidade do complemento de X em Y:

$$|X| = |Y| - |Y \setminus X| \qquad \text{se } X \subseteq Y \tag{28}$$

- Esta fórmula também pode ser escrita

$$|Y \setminus Z| = |Y| - |Z| \qquad \text{se } Z \subseteq Y \tag{29}$$

- Esta técnica é interessante quando o conjunto maior Y e o complemento $Z = Y \setminus X$ são mais fáceis de contar do que o conjunto desejado X.

  Exercício: Quantos números há entre 1000 e 9999, inclusive ambos, nos quais aparecem pelo menos dois algarismos consecutivos iguais?

Princípio da inclusão e exclusão

- Outra técnica importante de contagem baseia-se na seguinte identidade, que vale para quaisquer conjuntos finitos A e B:

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{30}$$

- Esta identidade é fácil de entender pelo diagrama de Venn: ao somar as contagens dos elementos de A e de B, estamos contando todos os elementos de $A \cup B$, mas contando em dobro os elementos de $A \cap B$.
- Pelo mesmo raciocínio podemos concluir que, para quaisquer conjuntos finitos A, B e C, vale a identidade

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

- As fórmulas podem ser generalizadas para n conjuntos finitos $A_1, A_2, \ldots, A_n$:

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| \quad = \quad & \sum_{\substack{i \\ 1 leq i \leq n}} |A_i| \\ & - \sum_{\substack{i,j \\ 1 \leq i < j \leq n}} \left|A_i \cap A_j\right| \\ & + \sum_{\substack{i,j,k \\ 1 \leq i < j < k \leq n}} \left|A_i \cap A_j \cap A_k\right| \\ & \cdots \\ & + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n| \end{aligned} \tag{31}$$

- Para simplificar esta fórmula, vamos denotar por C_n^r o conjunto de todas as combinações de r elementos do conjunto $\{1, 2, \ldots, n\}$. Podemos escrever então

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \left(\sum_{X \in C_n^r} \left| \bigcap_{k \in X} A_k \right| \right) \tag{32}$$

- Esta fórmula para a cardinalidade da união de conjuntos finitos é conhecida pelo nome de **princípio da inclusão e exclusão**. Observe que os princípios aditivo e subtrativo da contagem são casos particulares deste princípio.

Exercício: Quantos números entre 1 e 1.000.000 são divisíveis por 5, por 7, ou por 11?

Cardinalidade de conjuntos

- Anteriormente definimos informalmente a cardinalidade de conjuntos finitos.
- Agora temos condições de dar uma definição mais precisa de cardinalidade, inclusive para conjuntos infinitos.

  Definição: Sejam A e B dois conjuntos. Se existir uma função bijetora $f : A \to B$, então dizemos que A e B **tem a mesma cardinalidade**. Denotaremos este fato por $A \sim B$.

- Pode-se provar que "$\sim$" é uma **relação de equivalência**. As classes de equivalência da relação "$\sim$" são chamadas de **cardinalidades** ou **números cardinais**.
- A cardinalidade de um conjunto A é geralmente denotada por $|A|$ ou $\#A$. Portanto temos que $A \sim B$ se e somente se $|A| = |B|$.

Conjuntos finitos

- Para cada número natural n definimos $I_n = \{i \in \mathbb{N} : i < n\}$.
- Por exemplo, $I_5 = \{0, 1, 2, 3, 4\}$. Um conjunto A é dito **finito** se existe um número natural n tal que $A \sim I_n$.
- Neste caso, dizemos que n é o número de elementos de A.
- É fácil ver que dois conjuntos finitos tem a mesma cardinalidade se e somente se eles tem o mesmo número de elementos.

- Portanto a cardinalidade de um conjunto finito pode ser identificada com seu número de elementos.
- Observe que, de acordo com a definição, o conjunto vazio $\emptyset$ é finito e $|\emptyset| = 0$.

Conjuntos infinitos

- Para certos conjuntos A, não existe uma bijeção de A para I_n, para nenhum $n \in \mathbb{N}$.
- Exemplos incluem o próprio conjunto $\mathbb{N}$, bem como $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$. Dizemos que estes conjuntos são **infinitos**.
- Poderíamos supor que, como no caso dos conjuntos finitos, os subconjuntos próprios de um conjunto infinito A tem cardinalidades estritamente menores que $|A|$.

- Porém, os exemplos abaixo mostram que isso não é verdade:

Exemplo: Seja $\mathbb{E} \subset \mathbb{N}$ o conjunto dos números naturais **pares**, $\{2k : k \in \mathbb{N}\}$. Considere a funçao $f : \mathbb{N} \to \mathbb{E}$ definida por $f(n) = 2n$. A função f é uma bijeção do conjunto dos naturais no conjunto dos números pares. Portanto $\mathbb{N} \sim \mathbb{E}$ e portanto a cardinalidade de $\mathbb{N}$ é a mesma que $\mathbb{E}$.

- Ou seja, é possível retirar elementos de um conjunto infinito sem alterar sua cardinalidade.
- Verifica-se que esta é uma propriedade geral de conjuntos infinitos.
- Inclusive, muitos autores usam esta propriedade como definição, dizendo que um conjunto A é infinito se e somente se ele tem um subconjunto próprio B tal que $A \sim B$.

- O exemplo anterior foi enunciado pelo matemático alemão David Hilbert (1862–1943) na forma de uma anedota: um hotel com infinitos quartos, todos ocupados, de repente recebe infinitos novos hóspedes, e precisa arrumar quartos para eles.
- Dois outros exemplos importantes serão enunciados.

Exemplo: Considere a funçao $f : \mathbb{N} \to \mathbb{Z}$ definida por

$$f(n) \;=\; (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor \;=\; \begin{cases} k & \text{se } n \text{ é par } (n = 2k) \\ -(k+1) & \text{se } n \text{ é ímpar } (n = 2k+1) \end{cases} \tag{33}$$

A tabela abaixo ilustra a função f

n	0	1	2	3	4	5	6	7 ...
$f(n)$	0	−1	1	−2	2	−3	3	−4 ...

Esta função é uma bijeção de $\mathbb{N}$ para $\mathbb{Z}$, e portanto $\mathbb{N} \sim \mathbb{Z}$.

Exemplo: Considere a função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida pela fórmula

$$f(u, v) = \frac{(u+v)(u+v+1)}{2} + u$$

A tabela ilustra a função f. Ela associa a cada par (u, v) um número natural na sequência, segundo diagonais sucessivas.

Verifica-se que esta função é uma bijeção de $\mathbb{N} \times \mathbb{N}$ para $\mathbb{N}$, e portanto $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

		v					
		0	1	2	3	4	...
	0	0	1	3	6	10	...
	1	2	4	7	11	...	
u	2	5	8	12	...		
	3	9	13	...			
	4	14	...				
	⋮	⋮					

- Podemos demonstrar também que

  Teorema: Para todo inteiro positivo n, $\mathbb{N}^n \sim \mathbb{N}$.

- A demonstração pode ser feita por indução em n, usando a função f

$$f(u,v) = \frac{(u+v)(u+v+1)}{2} + u \qquad (34)$$

  e a bijeção g entre os conjuntos $\mathbb{N}^n$ e $(\mathbb{N}^{n-1}) \times \mathbb{N}$, definida por

$$g((a_1, a_2, \ldots, a_n)) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

  para toda ênupla $(a_1, a_2, \ldots, a_n)$ em $\mathbb{N}^n$.

Exemplo: Considere a função $f : [0,1] \to [1,3]$ definida por $f(x) = 2x + 1$. Verifica-se que esta função é uma bijeção do intervalo $[0,1]$ para o intervalo $[1,3]$, e portanto concluímos que $[0,1] \sim [1,3]$. Por raciocínio análogo, podemos concluir que todos os intervalos fechados $[a,b]$ de números reais tem a mesma cardinalidade.

Teorema: Seja X um conjunto finito não vazio, e X^* o conjunto de todas as sequências finitas de elementos de X, isto é $X^* = \cup_{k\in\mathbb{N}} X^k$. Então $X^* \sim \mathbb{N}$.

Prova:
Seja $m = |X|$. Note que $|X^n| = m^n$. Seja f_n uma bijeção qualquer do conjunto X^n para o conjunto $\{0, 1, \ldots, m^n - 1\}$. Considere a função $g : X^* \to \mathbb{N}$, definida por

$$g(x) = \left(\sum_{k=0}^{n-1} m^k\right) + f_n(x)$$

para todo $n \in \mathbb{N}$ e toda sequência $x \in X^n$.

Em particular,

se $x \in X^0$	então $g(x) = f_0(x)$	$= 0$;
se $x \in X^1$	então $g(x) = 1 + f_1(x)$	$\in \{1, \ldots, 1 + (m-1)\}$;
se $x \in X^2$	então $g(x) = 1 + m + f_2(x)$	$\in \left\{1 + m, \ldots, 1 + m + (m^2 - 1)\right\}$;
se $x \in X^3$	então $g(x) = 1 + m + m^2 + f_3(x)$	$\in \left\{1 + m + m^2, \ldots, 1 + m + m^2 + (m^3 - 1)\right\}$;

e assim por diante. Pode-se ver que a função g é uma bijeção de X^* para $\mathbb{N}$, e portanto $X^* \sim \mathbb{N}$.

Conjuntos enumeráveis e contáveis

- Um conjunto é dito **enumerável** se ele tem a mesma cardinalidade dos números naturais.
- Dizemos que um conjunto é **contável** se ele é finito ou enumerável.
- Observe que um conjunto A é enumerável se, e somente se é possível listar os elementos do conjunto como uma sequência infinita $a_0, a_1, a_2, \ldots$; isto é, podemos indexá-los pelos números naturais.

Exemplo: Todo subconjunto A de $\mathbb{N}$ é contável. Se A é finito, ele é contável. Se A não é finito, considere a função bijetora $f : A \to \mathbb{N}$ onde $f(a)$ é número de elementos de A que são menores que a, para todo $a \in A$.

Exemplo: Se B é um conjunto contável, todo subconjunto $C \subseteq B$ é contável. Para provar este fato, considere uma bijeção f de $\mathbb{N}$ para B. Seja A o subconjunto $f^{-1}(C)$ de $\mathbb{N}$. Pelo exemplo acima, A é contável. A restrição de f a A é uma bijeção de A para C, e portanto C também é contável.

- Conjuntos contáveis podem ser combinados de diversas maneiras e ainda continuam contáveis.
- Pode-se provar que a união de dois conjuntos contáveis é um conjunto contável.
- Por indução, o mesmo vale para a união de qualquer número finito de conjuntos contáveis. Mais ainda:

  Teorema: Seja X um conjunto enumerável cujos elementos são conjuntos enumeráveis, disjuntos dois a dois. A união de todos os elementos de X é enumerável.

- Usando este resultado, pode-se provar que, se X é um conjunto contável cujos elementos são conjuntos contáveis (não necessariamente disjuntos), a união de todos os elementos de X é contável.

Cardinalidade dos números reais

- Em vista dos exemplos acima, poderíamos ser levados a acreditar que todos os conjuntos infinitos têm a mesma cardinalidade, ou seja, que existe apenas um tipo de “infinito”.
- Essa conjetura foi derrubada pelo matemático Georg Cantor em 1879, que mostrou que os conjuntos $\mathbb{N}$ e $\mathbb{R}$ tem cardinalidades diferentes. Este fato decorre do seguinte teorema:

Teorema: O intervalo aberto $(0,1) = \{\, x \in \mathbb{R} : 0 < x < 1 \,\}$ não é contável.

Prova: O conjunto $(0,1)$ não é finito, portanto precisamos demonstrar apenas que ele não é enumerável. Seja f uma função qualquer de $\mathbb{N}$ para $(0,1)$ Para cada número real $f(i)$, considere uma representação decimal infinita $a_i = 0, a_{i0}a_{i1}a_{i2}\ldots$ do mesmo. Temos então uma lista infinita de sequências infinitas de algarismos

$$\begin{array}{rcccl} f(0) & = & a_0 & = & 0, a_{00}a_{01}a_{02}\ldots \\ f(1) & = & a_1 & = & 0, a_{10}a_{11}a_{12}\ldots \\ f(2) & = & a_2 & = & 0, a_{20}a_{21}a_{22}\ldots \\ \vdots & & & & \end{array}$$

Observe que alguns números reais tem duas representações. Por exemplo, o número $1/4$ pode ser escrito como $0,250000\ldots$ ou $0,249999\ldots$. Se $f(i)$ é um destes números, escolhemos para a_i qualquer das duas representações, arbitrariamente.

Todos os outros números reais tem uma, e apenas uma, representação decimal. Observe também que as sequências $0,000000\ldots$ e $0,999999\ldots$ representam os números 0 e 1, respectivamente, e portanto não estão no intervalo aberto $(0,1)$. Porém, exceto por esses dois casos, toda representação decimal infinita que começa com $0,\ldots$ representa algum número real no intervalo $(0,1)$.

Considere agora a representação decimal infinita $b = 0, b_0 b_1 b_2 \ldots$ onde

$$b_i = \begin{cases} 4 & \text{se } a_{ii} \neq 4 \\ 5 & \text{se } a_{ii} = 4 \end{cases}$$

A representação infinita b não aparece na lista acima, pois ela difere de cada a_i na posição i depois da vírgula. Como b usa apenas algarismos 4 e 5 depois da vírgula, o número real b^* que ela representa não é nem 0 nem 1, e portanto está no intervalo aberto $(0, 1)$.

Uma vez que b não termina nem em infinitos zeros nem em infinitos noves, o número b^* tem apenas essa representação, e portanto ele é diferente do número real $f(i)$, para todo i em $\mathbb{N}$. Concluímos que nenhuma função f de $\mathbb{N}$ para $(0, 1)$ pode ser sobrejetora. Logo $(0, 1)$ não é enumerável. □

- A técnica usada nesta demonstração para encontrar o contra exemplo b^* é conhecida como **método da diagonalização** (ou **método da diagonalização de Cantor**).
- Este método é muito usado em lógica matemática e na teoria da computação.

- Não é difícil encontrar uma bijeção entre o intervalo aberto $(0, 1)$ e o conjunto dos números reais $\mathbb{R}$. Portanto, em vista do teorema anterior a cardinalidade de $\mathbb{R}$ é estritamente maior que a cardinalidade de $\mathbb{N}$. Na verdade, pode-se demonstrar que

$$\left|\mathbb{P}(\mathbb{N})\right| = |\mathbb{R}| \tag{35}$$

Comparação de cardinalidades

- Sejam A e C conjuntos. Definimos a relação C **domina** A e escrevemos $A \preceq C$ se existe um conjunto B tal que $A \sim B$ e $B \subseteq C$.
- Em outras palavras, $A \preceq C$ se e somente se existe uma função injetora de A para C.
  Exemplo: Seja $\mathbb{C}$ o conjunto dos números primos, e $\mathbb{M}$ o conjunto dos quadrados perfeitos, $\left\{ n^2 : n \in \mathbb{N} \right\}$. Observe que a função f de $\mathbb{C}$ para $\mathbb{M}$ definida por $f(p) = p^2$ é uma função injetora. Portanto, concluímos que $\mathbb{C} \preceq \mathbb{M}$.

- Em particular, para quaisquer conjuntos A, B tais que $A \subseteq B$, a função identidade I_A é uma função injetora de A para B;
- portanto concluímos que $A \subseteq B$ implica $A \preceq B$. Em particular, $A \preceq A$ para qualquer conjunto A; ou seja, $\preceq$ é uma relação reflexiva.
- Prova-se também que, se $A \preceq B$ e $B \preceq C$, então $A \preceq C$; isto é, $\preceq$ é transitiva.
- Finalmente, prova-se que, se $A \preceq B$ e $B \preceq A$, então $A \sim B$ (isto é, A e B tem a mesma cardinalidade).

- Pode-se verificar também que se $A \sim A'$, $B \sim B'$, e $A \preceq B$, então $A' \preceq B'$. Portanto a relação $\preceq$ entre conjuntos depende apenas de suas cardinalidades, e não dos conjuntos em si.
- Podemos então substituir $\preceq$ por uma relação entre cardinalidades. Em vista das propriedades acima, esta é uma relação de ordem total, que denotaremos por $\leq$. Ou seja, dizemos **a cardinalidade de A é menor ou igual à de B**, e escrevemos $|A| \leq |B|$, se e somente se $A \preceq B$.

- Se $|A| \leq |B|$, mas $|A| \neq |B|$, dizemos que a cardinalidade de A é estritamente menor que a cardinalidade de B, e denotamos esse fato por $|A| < |B|$.
- Para conjuntos finitos, a relação de ordem $\leq$ entre cardinalidades coincide com a relação $\leq$ entre números naturais.

- É fácil ver também que a cardinalidade de um conjunto finito é sempre maior que a cardinalidade de qualquer subconjunto próprio.
- Ou seja, para qualquer conjunto finito A e qualquer conjunto B, temos $B \subset A \rightarrow |B| < |A|$.

Teorema de Cantor

- Cantor mostrou também o seguinte resultado importante:

  Teorema: Para todo conjunto A, $|A| < \left|\mathbb{P}(A)\right|$.
- Dito de outra forma, todo conjunto (finito ou infinito) tem mais subconjuntos do que elementos.
- Este resultado é óbvio para conjuntos finitos, pois se $|A| = n$ então $\left|\mathbb{P}(A)\right| = 2^n$ e $2^n > n$ para todo $n \in \mathbb{N}$.
- A contribuição de Cantor foi mostrar que o resultado vale também para conjuntos infinitos.

Teorema: Para todo conjunto A, $|A| < \left|\mathbb{P}(A)\right|$.

Prova: Sejam A um conjunto e f uma função qualquer de A para $\mathbb{P}(A)$, ou seja, uma função f que a cada elemento $a \in A$ associa um subconjunto $f(a) \subseteq A$. Vamos mostrar que f não pode ser uma bijeção de A para $\mathbb{P}(A)$.
Observe que o elemento a pode pertencer ou não ao subconjunto $f(a)$. Considere agora o seguinte conjunto:

$$X = \{\, a \in A : a \notin f(a) \,\}$$

$$X = \{\, a \in A : a \notin f(a) \,\}$$

Observe que X é um subconjunto de A, logo $X \in \mathbb{P}(A)$. Porém, para todo $a \in A$, temos $f(a) \neq X$, pois se $a \in f(a)$ então $a \notin X$, e se $a \notin f(a)$ então $a \in X$. Portanto f não é sobrejetora em $\mathbb{P}(A)$. Concluímos que, para qualquer conjunto A, não existe nenhuma bijeção de A para $\mathbb{P}(A)$; ou seja, estes dois conjuntos não tem a mesma cardinalidade.

Por outro lado, observe que existe uma bijeção de qualquer conjunto A para o conjunto $A' = \{\{a\} : a \in A\}$, que é um subconjunto de $\mathbb{P}(A)$. Isto mostra que $|A| \leq \left|\mathbb{P}(A)\right|$. Juntando estes dois resultados, concluímos que $|A| < \left|\mathbb{P}(A)\right|$. □

Em particular, a cardinalidade de $\mathbb{P}(\mathbb{N})$ é estritamente maior que a de $\mathbb{N}$.

A hipótese do contínuo

- Depois de mostrar que $\left|\mathbb{P}(\mathbb{N})\right| = |\mathbb{R}|$, Cantor conjecturou em 1878 que não é possível definir um conjunto com cardinalidade entre $|\mathbb{N}|$ e $|\mathbb{R}|$ — isto é, estritamente maior que $\mathbb{N}$ mas estritamente menor que $\mathbb{R}$.

- Esta conjetura ficou conhecida como a **hipótese do contínuo**, e ficou aberta até 1963, quando Paul Cohen (baseado em um teorema provado por Kurt Gödel em 1939) mostrou que, com os axiomas usuais da teoria dos conjuntos, não é possível demonstrar nem essa afirmação nem sua negação.
- Ou seja, pode-se supor que tais conjuntos existem, ou que não existem — e, nos dois casos, nunca se chegará a uma contradição.

Cardinalidade e Computabilidade

- Os conceitos de cardinalidade de conjuntos infinitos permitem responder a questão: “toda função pode ser computada?”.
- Observamos que qualquer programa de computador, pode ser visto como uma sequência finita de caracteres.

  Teorema: O conjunto de todos os programas em uma dada linguagem de programação é contável.

Por outro lado, temos também o seguinte fato:

Teorema: O conjunto $\mathcal{F}$ de todas as funções de $\mathbb{N}$ para $\mathbb{N}$ não é enumerável.

Prova:
Seja S o intervalo $(0,1) = \{ x \in \mathbb{R} : 0 < x < 1 \}$. Como visto anteriormente, todo número a nesse conjunto pode ser representado na notação decimal por uma sequência infinita $0, a_1 a_2 \ldots a_n \ldots$ onde cada a_i é um algarismo (um inteiro) entre 0 e 9.

Seja f a função com domínio S definida da seguinte maneira: para cada $a \in S$, $f(a) = f_a$ é a função de $\mathbb{N}$ para $\mathbb{N}$ que associa cada natural n com o dígito a_n de a. Note que f_a é um elemento de $\mathcal{F}$. A função f é injetora; pois, se $f_x = f_y$, cada dígito decimal de x é igual ao dígito decimal correspondente de y, portanto $x = y$. Portanto f é uma bijeção entre S e o conjunto $\mathcal{G} = \mathrm{Img}(f) \subset \mathcal{F}$. Vimos que S não é enumerável. Concluímos que $\mathcal{F}$ tem um subconjunto que não é enumerável. Portanto $\mathcal{F}$ não é enumerável. □

- Diz-se que uma função $f : \mathbb{N} \to \mathbb{N}$ é **computável** em uma dada linguagem se existe um programa nessa linguagem que, para todo $x \in \mathbb{N}$, devolve $f(x)$ quando seu dado de entrada é x.
- Seja $\mathcal{C}$ o conjunto de todas as funções computáveis de uma dada linguagem. Mostramos que $|\mathcal{C}| \leq |\mathbb{N}|$. Por outro lado mostramos que $|\mathcal{F}| > |\mathbb{N}|$. Logo, concluímos que existem funções de $\mathbb{N}$ para $\mathbb{N}$ que não são computáveis.

Probabilidade

- A lógica é uma ferramenta essencial pois nos permite deduzir o valor lógico de proposições complexas a partir dos valores lógicos de suas proposições e predicados elementares.
- Porém, para usá-la precisamos saber se as proposições e predicados são verdadeiros ou falsos.
- Na vida real, é raro sabermos com certeza se uma afirmação é verdadeira ou não.
- Como podemos então usar a lógica, ou tomar qualquer decisão, nessas condições?
- Além disso, há afirmações sobre as quais temos muito mais confiança do que outras.
- Podemos tratar a frase “ontem choveu na minha rua” como verdadeira, com confiança quase absoluta, se estávamos lá ontem.
- Por outro lado, se a previsão do tempo diz que “não vai chover manhã”, é prudente pensar na possibilidade de que chova.

- Para algumas proposições, nossa confiança pode se dividir igualmente entre as duas possibilidades.
- Alguém jogou uma moeda ao ar e ela caiu onde não podemos ver. Será que o resultado foi cara, ou coroa? Nossa experiência com moedas nos diz que às vezes o resultado é um e as vezes é outro.
- Da mesma forma, quando atiramos um dado, nossa experiência diz apenas que o resultado pode ser qualquer número entre 1 e 6, e que parece não haver diferença entre eles.
- Por essa experiência, a afirmação “o resultado será 3” merece tanta confiança quanto “o resultado será 5”.
- Na verdade, jogos de azar como dados e cara-ou-coroa baseiam-se inteiramente no fato de que todos resultados possíveis são igualmente plausíveis.

- Por outro lado, mesmo nesses jogos há afirmações que merecem mais confiança do que outras.
- Quando atiramos um dado, a afirmação “o resultado será 3” deve nos parecer menos plausível do que “o resultado será diferente de 3”.
- Esta confiança pode vir da experiência, mas também por raciocínio: se todos os 6 resultados tem chances iguais de acontecer, então o resultado 3 deve ter menos chances do que os outros cinco juntos.
- A teoria da probabilidade surgiu para formalizar este tipo de raciocínio, que tem o mesmo objetivo da lógica clássica — ajudar-nos a pensar e decidir — mas lida com graus de confiança, em vez de certezas absolutas.

Definição

- Nesta teoria, cada proposição P tem uma **probabilidade**: um valor real entre 0 e 1, que mede o grau de confiança ou expectativa que temos de que a proposição seja verdadeira.
- Denotaremos esse número por $\Pr(P)$.
- Probabilidade 1 significa que temos certeza absoluta de que a afirmação P é verdadeira.
- Probabilidade 0 significa que temos certeza absoluta que é falsa. O valor $1/2$ significa que não sabemos se P é falsa ou verdadeira, e que qualquer das duas possibilidades nos parece igualmente provável.
- Assim, por exemplo, quando vamos jogar uma moeda, podemos atribuir probabilidade $1/2$ à afirmação “o resultado será cara”.
- Uma probabilidade mais próxima de 1 significa que não temos certeza, mas acreditamos que é mais provável que a afirmação P seja verdadeira do que ela seja falsa.

- Na teoria da probabilidade, toda proposição P em tese continua tendo um valor lógico “verdadeiro” ou “falso”, mas a teoria não exige que esse valor seja conhecido.
- A probabilidade da afirmação reflete justamente nosso grau de conhecimento.
- Se conhecemos o valor lógico da afirmação devemos atribuir a ela probabilidade 0 ou 1.
- Neste caso, como veremos, a teoria da probabilidade se reduz à lógica clássica.
- As probabilidades são frequentemente expressas em percentagens. Assim, tanto faz dizer que uma probabilidade é 25% ou $25/100 = 0,25$.

Distribuição uniforme

- Em geral, quando temos n alternativas possíveis para uma situação qualquer, e não temos nenhuma informação, experiência ou raciocínio que justifique atribuir probabilidade maior a uma algumas do que outras, é razoável atribuir probabilidade $1/n$ a cada alternativa.
- Neste caso dizemos que essas alternativas tem uma **distribuição uniforme** de probabilidade.
- Um exemplo de distribuição uniforme é o sorteio de um item entre n outros. Para que o sorteio seja justo é importante que ele seja feito de modo que cada item tenha a mesma probabilidade de ser escolhido.
- Neste caso dizemos que a escolha é **perfeitamente aleatória**.
- Esse conceito é importante em muitos jogos “de azar”, como cara-ou-coroa, palitinho, par-ou-ímpar, dados, roletas, baralhos, etc..

- Esses jogos dependem de dispositivos ou ações que podem dar dois ou mais resultados distintos. Para que o jogo seja justo, é essencial que os jogadores não tenham nenhum conhecimento prévio sobre o resultado, de modo que todos atribuam uma distribuição uniforme de probabilidade ao mesmo.
- Por outro lado, é importante observar que a teoria não diz como atribuir as probabilidades de afirmações elementares, mas apenas como combiná-las para obter as probabilidades de afirmações compostas.
- É importante notar que as probabilidades dependem do observador: se um jogador troca o dado “honesto” por um viciado, ele pode (e deve) atribuir probabilidades diferentes a cada número.

Princípio da exclusão mútua

- Intuitivamente, parece pouco razoável termos confiança ao mesmo tempo em duas afirmações contraditórias.
- Na teoria da probabilidade, essa intuição é formalizada pelo **princípio da exclusão mútua**, ou **aditividade**: se duas proposições P e Q não podem ser verdadeiras ao mesmo tempo (isto é, $P \to \neg Q$ e $Q \to \neg P$), então devemos ter $\Pr(P) + \Pr(Q) \leq 1$.
- Por exemplo, considere as afirmações “o Diretor está agora em São Paulo” e “o Diretor está agora no Rio de Janeiro”.
- Quaisquer que sejam as informações que temos a respeito do paradeiro do Diretor, não faz sentido atribuir probabilidade 0,75 para a primeira e 0,80 para a segunda, pois se uma delas for verdadeira, a outra não é.

Princípio da exclusão mútua

- Essa regra pode ser generalizada para três ou mais proposições $P_1, P_2, \ldots, P_n$. Essas proposições são **mutuamente exclusivas** se sabemos que $P_i \to \neg P_j$, para quaisquer i e j entre 1 e n com $i \neq j$.
- Nesse caso, o princípio da exclusão mútua exige que $\Pr(P_1) + \Pr(P_2) + \cdots + \Pr(P_n) \leq 1$.

Princípio da exaustão

- Por outro lado, se sabemos que pelo menos uma dentre duas afirmações é verdadeira, não é razoável termos pouca confiança nas duas afirmações. Por exemplo, não é razoável não acreditar nem na afirmação "o lucro será maior que R$ 10.000" nem na afirmação "o lucro será menor que R$ 20.000", pois pelo menos uma dessas afirmações com certeza é verdadeira.
- Na teoria da probabilidade, essa regra é formalizada pelo **princípio da exaustão**: se sabemos que $P \vee Q$ é verdadeiro, então devemos ter $\Pr(P) + \Pr(Q) \geq 1$. No exemplo acima, podemos atribuir probabilidade $1/2$ ou $3/4$ para ambas, mas não $1/4$; se atribuirmos probabilidade $0,30$ para a primeira, podemos atribuir $0,80$ para a segunda, mas não $0,50$.
- Mais geralmente se sabemos que $P_1 \vee P_2 \vee \cdots \vee P_n$ é verdadeiro, então devemos ter $\Pr(P_1) + \Pr(P_2) + \cdots + \Pr(P_n) \geq 1$.

Princípio da complementaridade

- Juntando o princípio da exclusão e da exaustão, podemos concluir que se uma afirmação P é o oposto lógico (negação) da afirmação Q, então a soma das probabilidades deve ser exatamente 1. Ou seja, para qualquer afirmação P, temos

$$\Pr(P) + \Pr(\neg P) = 1 \tag{36}$$

  ou seja

$$\Pr(\neg P) = 1 - \Pr(P) \tag{37}$$

- Por exemplo, se a probabilidade de "vai chover amanhã" é $3/4$, a probabilidade de "não vai chover amanhã" tem que ser $1/4$. Esta regra é conhecida como o **princípio da complementaridade**.

- Esta regra também pode ser generalizada para três ou mais afirmações. Suponha que sabemos que exatamente uma das afirmações $P_1, P_2, \ldots, P_n$ é verdadeira. Isto é, sabemos que elas são mutuamente exclusivas, mas também que uma delas tem que ser verdadeira.
- Então devemos ter

$$\Pr(P_1) + \Pr(P_2) + \cdots + \Pr(P_n) = 1 \tag{38}$$

- Por exemplo, suponha que alguém escolheu e retirou uma carta de um baralho comum.
- Considere as afirmações "a carta é ouros", "a carta é copas", "a carta é paus", "a carta é espadas", ou "a carta é um coringa". Como a carta só pode ser de um tipo, e tem que ser de um desses cinco tipos, então as probabilidades dessas afirmações devem somar 1.
- Observe que este princípio é respeitado quando atribuímos probabilidade $1/n$ para n alternativas igualmente prováveis.

Princípio da exclusão e inclusão

- Os princípios acima podem ser vistos como corolários de um princípio mais geral: para quaisquer afirmações P e Q, devemos ter

$$\Pr(P \vee Q) = \Pr(P) + \Pr(Q) - \Pr(P \wedge Q) \tag{39}$$

- Compare este princípio com a fórmula para cardinalidade de conjuntos

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{40}$$

Exercício: Contagens em uma fábrica mostraram que 5% dos parafusos tem um defeito na rosca, 4% tem um defeito na cabeça, e 2% tem um defeito em ambas as partes. Qual é a probabilidade de que um desses parafusos, escolhido ao acaso, tenha algum defeito?

Princípio da independência

- **Um dado** e **uma moeda** são atirados ao mesmo tempo. Como discutimos acima, é razoável atribuir probabilidade 1/6 à afirmação “o resultado do dado será 3” e probabilidade 1/2 à afirmação “o resultado da moeda será cara”.
- Que probabilidade devemos atribuir à **conjunção** dessas duas frases, ou seja “**o resultado do dado será 3 e o da moeda será cara**”?
- Uma maneira de fazer esta escolha é observar que há 12 possíveis resultados para os dois lances. Vamos denotar por $D(x)$ e $M(y)$, respectivamente, os predicados ”o resultado do dado será x”, e “o resultado da moeda será y”.
- As 12 possibilidades correspondem às afirmações

$$\begin{array}{ll} D(1) \wedge M(\texttt{cara}) & D(1) \wedge M(\texttt{coroa}) \\ D(2) \wedge M(\texttt{cara}) & D(2) \wedge M(\texttt{coroa}) \\ D(3) \wedge M(\texttt{cara}) & D(3) \wedge M(\texttt{coroa}) \\ D(4) \wedge M(\texttt{cara}) & D(4) \wedge M(\texttt{coroa}) \\ D(5) \wedge M(\texttt{cara}) & D(5) \wedge M(\texttt{coroa}) \\ D(6) \wedge M(\texttt{cara}) & D(6) \wedge M(\texttt{coroa}) \end{array} \tag{41}$$

- Estas afirmações são mutuamente exclusivas e esgotam todas as possibilidades, portanto a soma de suas probabilidades deve ser 1. Se não temos nenhuma razão para suspeitar que o dado de alguma maneira influencie a moeda, ou vice-versa, então é razoável atribuir a mesma probabilidade (1/12) a estas 12 afirmações.
- Note que 1/12 é o produto de $\Pr(D(x)) = 1/6$ e $\Pr(M(y)) = 1/2$.
- Temos portanto que $\Pr(D(x) \wedge M(y)) = \Pr(D(x)) \Pr(M(y))$ para quaisquer x e y.
- Este é um exemplo de uma regra geral, o **princípio da independência**.
- Por definição, duas afirmações P e Q são ditas **independentes** se e somente se

$$\Pr(P \wedge Q) = \Pr(P) \Pr(Q) \tag{42}$$

Exercício: Dois dados, um vermelho e um verde, são atirados ao mesmo tempo. Qual é a probabilidade de que o resultado do dado vermelho seja menor que 4, e o do dado verde seja maior que 1?

Relação com a lógica clássica

- A teoria da probabilidade inclui a lógica clássica como caso particular. Mais precisamente, atribuir probabilidade 0 a uma afirmação equivale a acreditar que a afirmação é falsa; e atribuir probabilidade 1 equivale a acreditar que ela é verdadeira.
- Se todas as afirmações tem probabilidade 0 ou 1, as regras e conceitos da lógica clássica podem ser traduzidos por regras e conceitos da probabilidade. Por exemplo, o conetivo $P \to Q$ equivale a afirmar que $\Pr(Q|P) = 1$.

Variável aleatória

- Uma **variável aleatória** é uma variável (parâmetro, quantia) X cujo valor é conhecido apenas parcialmente, no sentido probabilístico.
- Isto é, sabemos que o valor de X é algum elemento de um certo conjunto D, o **domínio** da variável; e, para qualquer v em D, temos uma medida de probabilidade $\Pr(X = v)$ para a afirmação "$X = v$".
- A função que a cada $v \in D$ associa a probabilidade $\Pr(X = v)$ é chamada de **distribuição de probabilidade** (ou simplesmente **distribuição**) da variável X.

- Observe que, se u e v são elementos distintos de D, então as afirmações "$X = u$" e "$X = v$" são mutuamente exclusivas.
- Além disso, sabemos que existe algum elemento v em D tal que a afirmação "$X = v$" é verdadeira. Pelo princípio de inclusão e exclusão, temos portanto que

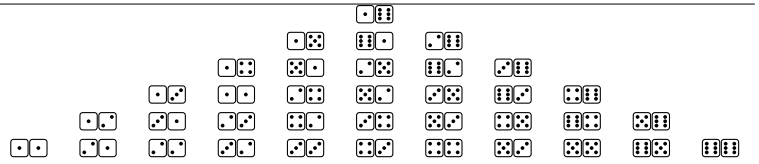
$$\sum_{v \in D} \Pr(X = v) = 1$$

- Observe também que, nestas condições, temos que atribuir $\Pr(X = v) = 0$ para qualquer valor v que não está no conjunto D.

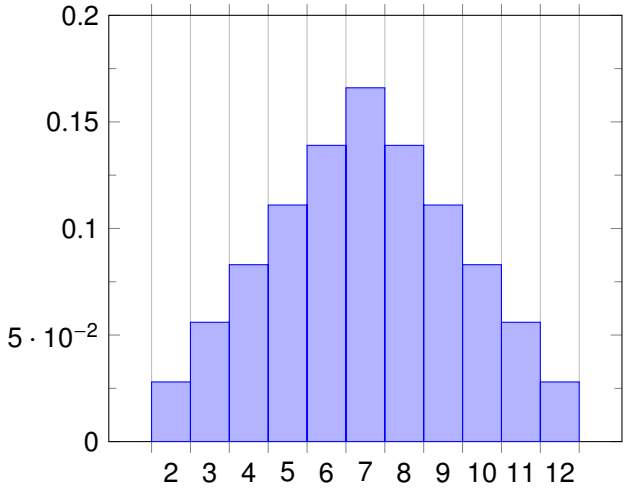
Exemplo:

- Um dado foi lançado, mas o resultado da jogada ainda está oculto.
- Seja X a variável aleatória cujo valor é esse resultado. Sabemos que o domínio de X é o conjunto $D = \{1, 2, \ldots, 6\}$.
- Como não temos motivos para distinguir entre esses resultados, é razoável atribuir probabilidades iguais ($1/6$) para cada valor em D, e probabilidade zero para qualquer outro valor.
- Em particular, $\Pr(X = 3) = \Pr(X = 5) = 1/6$, e $\Pr(X = 0) = \Pr(X = 7) = \Pr(X = 1/2) = 0$.

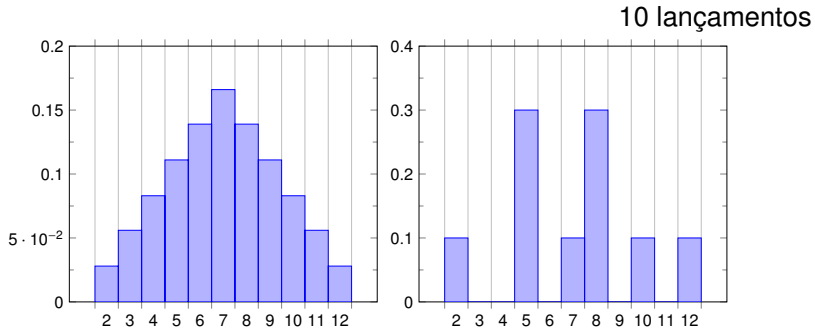
Distribuição de probabilidade

x	2	3	4	5	6	7	8	9	10	11	12
S'											
$\lvert S' \rvert$	1	2	3	4	5	6	5	4	3	2	1
p	0,028	0,056	0,083	0,111	0,139	0,166	0,139	0,111	0,083	0,056	0,028

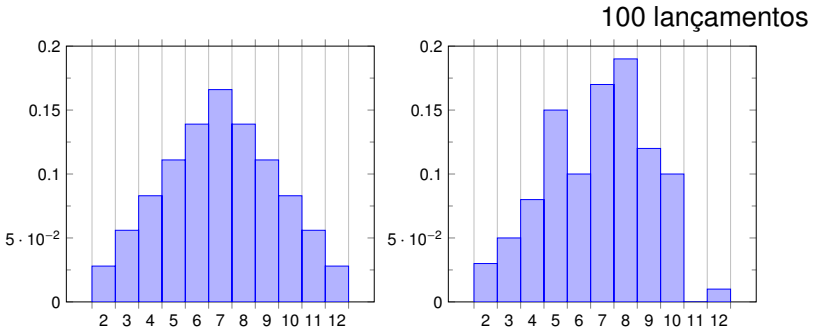
Distribuição de probabilidade - histograma



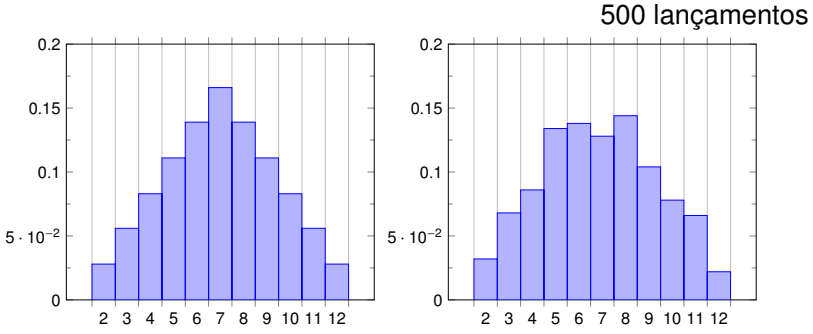
Experimento



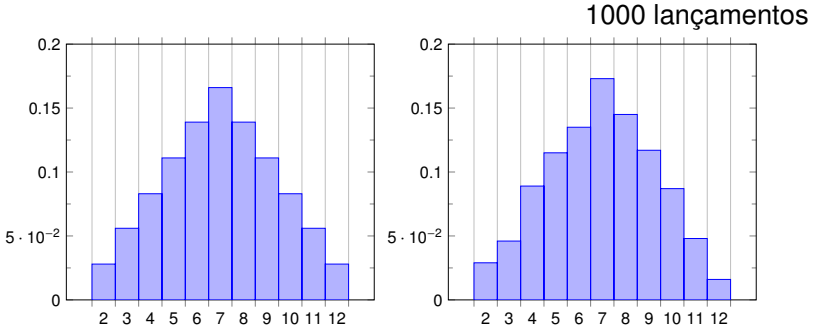
Experimento



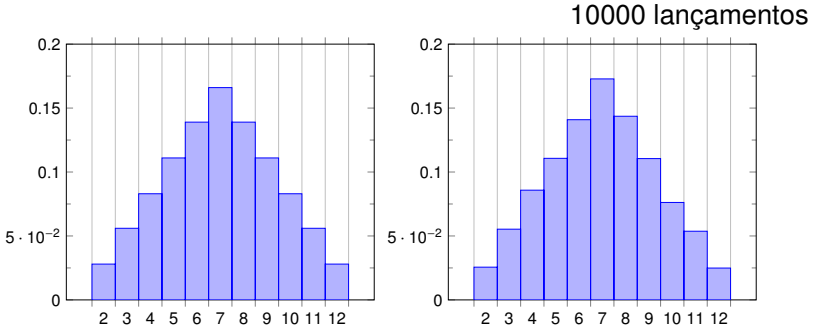
Experimento



Experimento



Experimento



- Variáveis aleatórias com valores numéricos podem ser combinadas com operações aritméticas e funções matemáticas, resultando em outras variáveis aleatórias.
- Por exemplo, se α é um número real, a fórmula $\alpha X + \sqrt{Y}$ denota a variável aleatória cujo valor é $\alpha u + \sqrt{v}$, onde u é o valor de X e v o valor de Y.
- A distribuição dessa nova variável é determinada pelas distribuições de probabilidades de X e de Y.

  Exercício: Sejam X e Y os resultados obtidos atirando-se dois dados de cores diferentes, cada um com distribuição uniforme de probabilidades. Determine a distribuição das seguintes variáveis derivadas de X e Y:

  1. X^2
  2. $X \bmod 3$
  3. $X + Y$
  4. $\min\{X, Y\}$

- Só vamos tratar de variáveis aleatórias cujos domínios são conjuntos discretos (finitos ou enumeráveis).
- A teoria pode ser estendida para variáveis com domínios não enumeráveis, como os números reais, mas esse assunto merece uma disciplina à parte.

Variáveis aleatórias independentes

- Dizemos que duas variáveis aleatórias X e Y são **independentes** se e somente se, para quaisquer valores u e v em seus respectivos domínios,

$$Pr(X = u \wedge Y = v) = Pr(X = u)Pr(Y = v) \qquad (43)$$

- Como no caso de proposições, é razoável supor que duas variáveis aleatórias são independentes quando **não** temos razão para supor que **o valor de uma tenha alguma influência no valor da outra**, ou que ambas sejam influenciadas por algum fator comum.
- Assim, por exemplo, é razoável supor que os valores obtidos por dois lances consecutivos do mesmo dado são variáveis independentes; pois os movimentos do dado durante o primeiro lance não influenciam seus movimentos no segundo lance.
- Por outro lado, não é razoável supor independência entre a altura e o peso de uma pessoa escolhida ao acaso; pois é razoável supor que pessoas mais altas tendem a ter peso maior.

- Também podemos supor que duas variáveis aleatórias **são independentes** mesmo que haja alguma **conexão física entre elas**, mas **não** temos razão para supor que essa conexão **afete as probabilidades** dos valores em alguma direção específica.
- Por exemplo, imagine que dois dados são colocados dentro de um copo que é agitado e entornado sobre a mesa.
- O movimento de cada dado afeta o movimento do outro, e ambos são afetados pelos movimentos do copo; mesmo assim, não temos razão para supor que obter um valor u em um dado aumente ou diminua as chances de obter valor v no outro dado.

Exercício: Sejam X e Y os resultados obtidos atirando-se dois dados de cores diferentes, cada um com distribuição uniforme de probabilidades. Suponha que as variáveis X e Y são independentes.

a) Sejam $S = X + Y$ e $D = X - Y$. As variáveis S e D são independentes? Justifique.

Valor esperado

- Um uso importante (e o mais antigo) da teoria da probabilidade é avaliar o ganho ou perda que pode decorrer de uma escolha ou acontecimento cujo resultado é desconhecido, como por exemplo uma aposta ou um investimento na bolsa.
- Suponha por exemplo que atiramos uma moeda e apostamos $\mathrm{R\$}\,30$ contra $\mathrm{R\$}\,10$ que o resultado será cara.
- Temos igual chance de ganhar $\mathrm{R\$}\,10$ (se sair cara) e perder $\mathrm{R\$}\,30$ (se sair coroa).
- Ou seja,

$$\Pr(\text{“nosso ganho será } \mathrm{R\$}\,{+}10\text{”}) \;=\; \Pr(\text{“nosso ganho será } \mathrm{R\$}\,{-}30\text{”}) \;=\; \frac{1}{2}$$

- Intuitivamente, se repetirmos essa aposta n vezes, em aproximadamente metade das vezes vamos ganhar 10 e na outra metade perder 30; portanto o ganho por aposta, em média, será aproximadamente

$$\frac{\frac{n}{2}(\mathrm{R\$}\,{+}10) + \frac{n}{2}(\mathrm{R\$}\,{-}30)}{n} = \mathrm{R\$}\,{-}10 \qquad (44)$$

- Em geral, suponha que temos uma variável aleatória X que pode assumir qualquer valor de um conjunto de valores numéricos D. O **valor médio esperado** (ou simplesmente o **valor esperado**) de X é, por definição

$$\mathcal{E}(X) = \sum_{v \in D} v \Pr(X = v) \qquad (45)$$

- Para entender esta fórmula, suponha que temos uma coleção grande com N variáveis, todas elas semelhantes a X mas tais que o valor de uma delas não tem influência nos valores das outras. Nesse caso, o número de variáveis que tem valor v será aproximadamente $N \Pr(X = v)$.

- Observe que se D tem um número finito n valores distintos, e todos os valores de D são igualmente prováveis, então $\Pr(X = v) = 1/n$, e a fórmula do valor esperado (45) reduz-se à média aritmética dos elementos de D.

  Exercício: Furar um poço de petróleo em determinada região custa R$500.000, e tem 30% de chance de encontrar óleo. Se isso acontecer, o poço pode ser vendido por R$800.000. Caso contrário o investimento é totalmente perdido. Qual o ganho esperado por poço?