

# Elementos de Matemática Discreta para Computação

Anamaria Gomide

^

Jorge Stolfi

Versão Preliminar de 25 de junho de 2024

© 2011



# Sumário

|                                                    |           |
|----------------------------------------------------|-----------|
| <b>Prefácio</b>                                    | <b>21</b> |
| Agradecimentos . . . . .                           | 28        |
| <b>1 Introdução à lógica matemática</b>            | <b>29</b> |
| 1.1 Como ter certeza? . . . . .                    | 29        |
| 1.2 A invenção da lógica . . . . .                 | 30        |
| 1.3 Euclides e demonstrações geométricas . . . . . | 30        |
| 1.4 Álgebra . . . . .                              | 33        |
| 1.5 As linguagens da lógica matemática . . . . .   | 34        |
| <b>2 Teoria dos Conjuntos</b>                      | <b>35</b> |

|       |                                                        |    |
|-------|--------------------------------------------------------|----|
| 2.1   | Conjuntos, elementos e pertinência . . . . .           | 36 |
| 2.1.1 | Igualdade de conjuntos . . . . .                       | 37 |
| 2.1.2 | Especificando conjuntos explicitamente . . . . .       | 37 |
| 2.1.3 | Especificando conjuntos por propriedades . . . . .     | 38 |
| 2.1.4 | Conjunto vazio . . . . .                               | 39 |
| 2.1.5 | Conjuntos importantes . . . . .                        | 39 |
| 2.1.6 | Conjuntos finitos e infinitos; cardinalidade . . . . . | 41 |
| 2.1.7 | Definições circulares e contraditórias . . . . .       | 42 |
| 2.2   | Relações de inclusão . . . . .                         | 43 |
| 2.3   | Operações com conjuntos . . . . .                      | 44 |
| 2.3.1 | União e interseção . . . . .                           | 44 |
| 2.3.2 | Diagrama de Venn . . . . .                             | 45 |
| 2.3.3 | Diferença . . . . .                                    | 46 |
| 2.3.4 | Conjunto universal e complemento . . . . .             | 47 |
| 2.3.5 | Diferença simétrica . . . . .                          | 48 |
| 2.3.6 | Propriedades das operações com conjuntos . . . . .     | 49 |
| 2.4   | Conjuntos de conjuntos . . . . .                       | 53 |
| 2.4.1 | Conjunto potência . . . . .                            | 54 |

|          |                                                        |           |
|----------|--------------------------------------------------------|-----------|
| 2.5      | Partição . . . . .                                     | 55        |
| 2.6      | Produto cartesiano . . . . .                           | 57        |
| 2.6.1    | Produto cartesiano de vários conjuntos . . . . .       | 58        |
| 2.6.2    | Produto cartesiano de conjunto consigo mesmo . . . . . | 59        |
| 2.7      | Intervalos reais . . . . .                             | 62        |
| 2.7.1    | Intervalos ilimitados . . . . .                        | 63        |
| 2.7.2    | Caixas . . . . .                                       | 66        |
| 2.8      | Intervalos inteiros . . . . .                          | 67        |
| 2.8.1    | Intervalos inteiros ilimitados . . . . .               | 68        |
| 2.8.2    | Grades inteiras . . . . .                              | 69        |
| <b>3</b> | <b>Lógica matemática</b>                               | <b>71</b> |
| 3.1      | Cálculo proposicional . . . . .                        | 73        |
| 3.1.1    | Proposições e valores lógicos . . . . .                | 73        |
| 3.1.2    | Conetivos lógicos e proposições compostas . . . . .    | 75        |
| 3.1.3    | Notação para cálculo proposicional . . . . .           | 76        |
| 3.1.4    | Operador de conjunção . . . . .                        | 77        |
| 3.1.5    | Operador de disjunção . . . . .                        | 78        |

|        |                                                            |     |
|--------|------------------------------------------------------------|-----|
| 3.1.6  | Operador de negação . . . . .                              | 79  |
| 3.1.7  | Operador de implicação . . . . .                           | 82  |
| 3.1.8  | Operador de igualdade lógica . . . . .                     | 87  |
| 3.1.9  | Operador de diferença . . . . .                            | 89  |
| 3.1.10 | Tabela-verdade de uma fórmula . . . . .                    | 90  |
| 3.2    | Manipulação de fórmulas lógicas . . . . .                  | 92  |
| 3.2.1  | Tautologias . . . . .                                      | 92  |
| 3.2.2  | Contradições . . . . .                                     | 93  |
| 3.2.3  | Equivalência lógica de fórmulas . . . . .                  | 94  |
| 3.2.4  | Equivalências lógicas importantes . . . . .                | 96  |
| 3.2.5  | Substituição de variáveis em equivalências . . . . .       | 101 |
| 3.2.6  | Dominância de fórmulas lógicas . . . . .                   | 102 |
| 3.2.7  | Equivalência e dominância em contexto específico . . . . . | 106 |
| 3.2.8  | Precedência dos operadores lógicos . . . . .               | 107 |
| 3.2.9  | Associatividade de operadores . . . . .                    | 108 |
| 3.3    | Síntese de fórmulas . . . . .                              | 109 |
| 3.3.1  | Forma normal disjuntiva . . . . .                          | 109 |
| 3.3.2  | Forma normal conjuntiva . . . . .                          | 110 |

|        |                                                                    |     |
|--------|--------------------------------------------------------------------|-----|
| 3.3.3  | Sistemas completos de operadores . . . . .                         | 113 |
| 3.4    | Dualidade lógica . . . . .                                         | 114 |
| 3.5    | Afirmações auto-referentes . . . . .                               | 116 |
| 3.6    | Cálculo de Predicados . . . . .                                    | 117 |
| 3.6.1  | Quantificação universal . . . . .                                  | 119 |
| 3.6.2  | Quantificação existencial . . . . .                                | 121 |
| 3.6.3  | Quantificador de existência e unicidade . . . . .                  | 123 |
| 3.6.4  | Quantificação sobre o conjunto vazio . . . . .                     | 124 |
| 3.6.5  | Quantificação sobre o conjunto universo . . . . .                  | 125 |
| 3.6.6  | Escopo de um quantificador . . . . .                               | 126 |
| 3.6.7  | Equivalência e dominância com quantificadores . . . . .            | 128 |
| 3.6.8  | Negação de quantificadores . . . . .                               | 128 |
| 3.6.9  | Distributividade de quantificadores . . . . .                      | 129 |
| 3.6.10 | Traduzindo linguagem natural para fórmulas quantificadas . . . . . | 130 |
| 3.6.11 | Mudança de domínio . . . . .                                       | 134 |
| 3.6.12 | Quantificadores múltiplos . . . . .                                | 136 |

|       |                                                         |     |
|-------|---------------------------------------------------------|-----|
| 4.1   | Introdução . . . . .                                    | 143 |
| 4.1.1 | Definições . . . . .                                    | 143 |
| 4.1.2 | Conjecturas . . . . .                                   | 147 |
| 4.1.3 | Métodos de demonstração . . . . .                       | 149 |
| 4.2   | Demonstração de implicações . . . . .                   | 149 |
| 4.2.1 | Método direto . . . . .                                 | 150 |
| 4.2.2 | Método da contrapositiva . . . . .                      | 153 |
| 4.2.3 | Método de redução ao absurdo . . . . .                  | 155 |
| 4.2.4 | Implicação com tese conjuntiva . . . . .                | 159 |
| 4.2.5 | Implicação com hipótese disjuntiva . . . . .            | 160 |
| 4.3   | Demonstrações de afirmações “se e somente se” . . . . . | 163 |
| 4.4   | Regras para quantificadores universais . . . . .        | 167 |
| 4.4.1 | Instanciação universal . . . . .                        | 167 |
| 4.4.2 | Generalização universal . . . . .                       | 167 |
| 4.4.3 | Demonstração por vacuidade . . . . .                    | 168 |
| 4.5   | Regras para quantificadores existenciais . . . . .      | 169 |
| 4.5.1 | Instanciação existencial . . . . .                      | 169 |
| 4.5.2 | Demonstrações construtivas . . . . .                    | 170 |

|          |                                                        |            |
|----------|--------------------------------------------------------|------------|
| 4.5.3    | Demonstrações não construtivas . . . . .               | 173        |
| 4.5.4    | Demonstração de existência e unicidade . . . . .       | 174        |
| 4.5.5    | Demonstração de falsidade por contra-exemplo . . . . . | 176        |
| <b>5</b> | <b>Indução Matemática</b>                              | <b>179</b> |
| 5.1      | Introdução . . . . .                                   | 180        |
| 5.2      | Princípio de Indução Matemática . . . . .              | 181        |
| 5.2.1    | Formulação do PIM usando conjuntos . . . . .           | 184        |
| 5.3      | Generalizações da Indução Matemática . . . . .         | 186        |
| 5.3.1    | Base genérica . . . . .                                | 187        |
| 5.3.2    | Passo genérico constante . . . . .                     | 188        |
| 5.3.3    | Troca de variável na hipótese . . . . .                | 190        |
| 5.3.4    | Exercícios . . . . .                                   | 190        |
| 5.4      | Usos indevidos da indução matemática . . . . .         | 192        |
| 5.5      | Mais exemplos de indução matemática . . . . .          | 195        |
| 5.6      | Princípio da Indução Completa . . . . .                | 199        |
| 5.6.1    | Indução completa sem prova da base . . . . .           | 201        |
| 5.6.2    | Indução completa com base genérica . . . . .           | 202        |

|          |                                                                |            |
|----------|----------------------------------------------------------------|------------|
| 5.6.3    | Indução completa com vários casos na base . . . . .            | 203        |
| 5.6.4    | Formulação do PIC usando conjuntos . . . . .                   | 205        |
| 5.7      | Exercícios . . . . .                                           | 205        |
| 5.8      | Princípio da Boa Ordenação . . . . .                           | 208        |
| 5.9      | Formas equivalentes do princípio da indução . . . . .          | 210        |
| 5.9.1    | PIM implica PBO . . . . .                                      | 210        |
| 5.9.2    | PBO implica PIC . . . . .                                      | 211        |
| 5.9.3    | PIC implica PIM . . . . .                                      | 212        |
| 5.10     | Exercícios adicionais . . . . .                                | 213        |
| <b>6</b> | <b>Relações</b>                                                | <b>219</b> |
| 6.1      | Conceitos básicos . . . . .                                    | 220        |
| 6.1.1    | Especificando uma relação . . . . .                            | 221        |
| 6.1.2    | Domínio e imagem . . . . .                                     | 225        |
| 6.1.3    | Restrição de relações . . . . .                                | 227        |
| 6.1.4    | Relações de identidade . . . . .                               | 227        |
| 6.1.5    | Relação inversa . . . . .                                      | 228        |
| 6.1.6    | Imagem e imagem inversa de conjuntos sob uma relação . . . . . | 230        |

|       |                                                     |     |
|-------|-----------------------------------------------------|-----|
| 6.2   | Composição de relações . . . . .                    | 230 |
| 6.2.1 | Notação alternativa . . . . .                       | 234 |
| 6.2.2 | Composição com identidade . . . . .                 | 234 |
| 6.2.3 | Composição com a relação inversa . . . . .          | 235 |
| 6.2.4 | Inversa da composição . . . . .                     | 235 |
| 6.2.5 | Composição e inclusão . . . . .                     | 237 |
| 6.2.6 | Potências de uma relação . . . . .                  | 238 |
| 6.2.7 | Potências negativas de uma relação . . . . .        | 240 |
| 6.2.8 | Potência nula de uma relação . . . . .              | 240 |
| 6.3   | Tipos de relações . . . . .                         | 240 |
| 6.3.1 | Composição e transitividade . . . . .               | 243 |
| 6.4   | Representação de relações usando matrizes . . . . . | 245 |
| 6.4.1 | Matriz booleana de uma relação . . . . .            | 245 |
| 6.4.2 | Operações com relações usando matrizes . . . . .    | 247 |
| 6.4.3 | Propriedades de relações usando matrizes . . . . .  | 249 |
| 6.5   | Fechos de uma relação . . . . .                     | 250 |
| 6.5.1 | Fecho reflexivo . . . . .                           | 250 |
| 6.5.2 | Fecho simétrico . . . . .                           | 251 |

|          |                                         |            |
|----------|-----------------------------------------|------------|
| 6.5.3    | Fecho transitivo . . . . .              | 252        |
| 6.5.4    | Fecho em geral . . . . .                | 255        |
| 6.6      | Relações $n$ -árias . . . . .           | 259        |
| 6.6.1    | Definição . . . . .                     | 259        |
| 6.6.2    | Projeção . . . . .                      | 260        |
| 6.6.3    | Permutação de componentes . . . . .     | 261        |
| 6.6.4    | Restrição . . . . .                     | 262        |
| 6.6.5    | Junção . . . . .                        | 262        |
| <b>7</b> | <b>Relações de ordem e equivalência</b> | <b>267</b> |
| 7.1      | Relações de ordem . . . . .             | 270        |
| 7.1.1    | Relações de ordem estrita . . . . .     | 273        |
| 7.1.2    | Ordem total . . . . .                   | 274        |
| 7.1.3    | Ordem lexicográfica . . . . .           | 275        |
| 7.1.4    | Ordens “parciais” . . . . .             | 277        |
| 7.1.5    | Diagrama de Hasse . . . . .             | 278        |
| 7.1.6    | Elementos mínimos e máximos . . . . .   | 281        |
| 7.1.7    | Elementos minimais e maximais . . . . . | 284        |

|          |                                                  |            |
|----------|--------------------------------------------------|------------|
| 7.2      | Relações de equivalência . . . . .               | 288        |
| 7.2.1    | Classes de equivalência . . . . .                | 290        |
| 7.2.2    | Relações de equivalência e partições . . . . .   | 292        |
| <b>8</b> | <b>Funções</b>                                   | <b>297</b> |
| 8.1      | Conceito . . . . .                               | 298        |
| 8.1.1    | Especificando uma função . . . . .               | 299        |
| 8.1.2    | Domínio e imagem de uma função . . . . .         | 302        |
| 8.2      | Inversa de função . . . . .                      | 303        |
| 8.3      | Imagem e imagem inversa de um conjunto . . . . . | 305        |
| 8.4      | Restrição . . . . .                              | 306        |
| 8.5      | Composição de funções . . . . .                  | 307        |
| 8.5.1    | Função idempotente . . . . .                     | 310        |
| 8.6      | Tipos de funções . . . . .                       | 310        |
| 8.6.1    | Função injetora . . . . .                        | 310        |
| 8.6.2    | Função sobrejetora . . . . .                     | 312        |
| 8.6.3    | Função bijetora . . . . .                        | 312        |
| 8.7      | Função permutação . . . . .                      | 314        |

|          |                                           |            |
|----------|-------------------------------------------|------------|
| 8.8      | Funções piso e teto . . . . .             | 317        |
| 8.9      | Quociente inteiro e resto . . . . .       | 320        |
| 8.10     | Fatorial e função gama . . . . .          | 324        |
| 8.11     | Função característica . . . . .           | 326        |
| 8.12     | Multiconjunto . . . . .                   | 326        |
| 8.13     | Sequências finitas . . . . .              | 328        |
| 8.13.1   | Notação para sequências finitas . . . . . | 329        |
| 8.13.2   | Índice inicial padrão . . . . .           | 329        |
| 8.13.3   | Comprimento . . . . .                     | 330        |
| 8.13.4   | Concatenação . . . . .                    | 330        |
| 8.13.5   | Subsequências e subcadeias . . . . .      | 331        |
| <b>9</b> | <b>Somatórias e produtórias</b>           | <b>333</b> |
| 9.1      | Introdução . . . . .                      | 334        |
| 9.2      | Somatórias básicas . . . . .              | 337        |
| 9.3      | Manipulação de somatórias . . . . .       | 338        |
| 9.4      | Somatórias múltiplas . . . . .            | 345        |
| 9.4.1    | Mudança de ordem de somatórias . . . . .  | 346        |

|           |                                              |            |
|-----------|----------------------------------------------|------------|
| 9.4.2     | Distributividade generalizada . . . . .      | 349        |
| 9.5       | Majoração de somatórias . . . . .            | 350        |
| 9.5.1     | Majoração dos termos . . . . .               | 350        |
| 9.5.2     | Majoração por indução matemática . . . . .   | 351        |
| 9.5.3     | Majoração por integrais . . . . .            | 353        |
| 9.5.4     | Minoração por integrais . . . . .            | 358        |
| 9.6       | Somas infinitas . . . . .                    | 361        |
| 9.7       | Produtórias . . . . .                        | 363        |
| 9.8       | Iteração de outras operações . . . . .       | 365        |
| <b>10</b> | <b>Sequências infinitas e recorrências</b>   | <b>367</b> |
| 10.1      | Sequências infinitas . . . . .               | 367        |
| 10.2      | Especificando sequências infinitas . . . . . | 369        |
| 10.3      | Recorrência . . . . .                        | 369        |
| 10.4      | Resolução de recorrências . . . . .          | 371        |
| 10.4.1    | Recorrência aditiva simples . . . . .        | 372        |
| 10.4.2    | Recorrência multiplicativa simples . . . . . | 374        |
| 10.4.3    | Recorrências lineares homogêneas . . . . .   | 375        |

|           |                                                            |            |
|-----------|------------------------------------------------------------|------------|
| 10.5      | Recorrências lineares não homogêneas . . . . .             | 379        |
| 10.6      | Majoração e minoração de recorrências . . . . .            | 381        |
| <b>11</b> | <b>Contagem</b>                                            | <b>385</b> |
| 11.1      | Contagem de relações . . . . .                             | 387        |
| 11.2      | Contagem de funções . . . . .                              | 388        |
| 11.3      | Princípio multiplicativo da contagem . . . . .             | 389        |
| 11.4      | Permutações . . . . .                                      | 392        |
| 11.4.1    | Fórmula de Stirling . . . . .                              | 394        |
| 11.5      | Arranjos . . . . .                                         | 395        |
| 11.6      | Combinações . . . . .                                      | 397        |
| 11.6.1    | Casos especiais . . . . .                                  | 399        |
| 11.6.2    | Propriedades . . . . .                                     | 400        |
| 11.6.3    | Fórmula do Binômio de Newton . . . . .                     | 402        |
| 11.6.4    | Fórmula recursiva . . . . .                                | 403        |
| 11.6.5    | Partições rotuladas e combinações com repetições . . . . . | 405        |
| 11.7      | Permutações e arranjos circulares . . . . .                | 407        |
| 11.8      | Contagem por divisão . . . . .                             | 408        |

|           |                                                                |            |
|-----------|----------------------------------------------------------------|------------|
| 11.9      | Permutações e arranjos com elementos indistinguíveis . . . . . | 409        |
| 11.10     | Combinações múltiplas . . . . .                                | 410        |
| 11.11     | Princípio aditivo da contagem . . . . .                        | 414        |
| 11.12     | Princípio subtrativo da contagem . . . . .                     | 416        |
| 11.13     | Princípio da inclusão e exclusão . . . . .                     | 417        |
| <b>12</b> | <b>Probabilidade</b>                                           | <b>421</b> |
| 12.1      | Definição . . . . .                                            | 423        |
| 12.1.1    | Distribuição uniforme . . . . .                                | 424        |
| 12.1.2    | Princípio da exclusão mútua . . . . .                          | 425        |
| 12.1.3    | Princípio da exaustão . . . . .                                | 426        |
| 12.1.4    | Princípio da complementaridade . . . . .                       | 426        |
| 12.1.5    | Princípio da exclusão e inclusão . . . . .                     | 427        |
| 12.1.6    | Princípio da independência . . . . .                           | 428        |
| 12.1.7    | Relação com a lógica clássica . . . . .                        | 430        |
| 12.2      | Variável aleatória . . . . .                                   | 431        |
| 12.2.1    | Variáveis aleatórias independentes . . . . .                   | 432        |
| 12.3      | Valor esperado . . . . .                                       | 434        |

|           |                                             |            |
|-----------|---------------------------------------------|------------|
| 12.3.1    | Propriedades do valor esperado . . . . .    | 438        |
| 12.4      | Mediana . . . . .                           | 439        |
| 12.5      | Moda . . . . .                              | 441        |
| 12.6      | Variância e desvio padrão . . . . .         | 442        |
| 12.6.1    | Propriedades da variância . . . . .         | 443        |
| 12.6.2    | Desvio padrão . . . . .                     | 444        |
| 12.6.3    | Covariância . . . . .                       | 446        |
| 12.6.4    | Coeficiente de correlação . . . . .         | 447        |
| 12.7      | Probabilidade condicional . . . . .         | 447        |
| 12.8      | Inferência bayesiana . . . . .              | 450        |
| 12.9      | Teoria da informação . . . . .              | 454        |
| 12.9.1    | Capacidade de informação . . . . .          | 454        |
| 12.9.2    | Quantidade de informação . . . . .          | 457        |
| 12.9.3    | Quantidade esperada de informação . . . . . | 459        |
| 12.10     | Exercícios adicionais . . . . .             | 460        |
| <b>13</b> | <b>Cardinalidade de conjuntos</b>           | <b>469</b> |
| 13.1      | Conjuntos finitos . . . . .                 | 471        |

|                                                  |     |
|--------------------------------------------------|-----|
| 13.2 Conjuntos infinitos . . . . .               | 472 |
| 13.3 Conjuntos enumeráveis e contáveis . . . . . | 476 |
| 13.4 Cardinalidade dos números reais . . . . .   | 478 |
| 13.5 Comparação de cardinalidades . . . . .      | 481 |
| 13.5.1 Teorema de Cantor . . . . .               | 482 |
| 13.5.2 A hipótese do contínuo . . . . .          | 484 |
| 13.6 Cardinalidade e Computabilidade . . . . .   | 484 |



# Prefácio

**Objetivos e escopo.** Este livro pretende ser um texto introdutório a algumas áreas da matemática discreta que são de especial importância para cursos de computação, ao nível de graduação e de mestrado.

Excluimos do escopo deste livro os fundamentos da matemática do contínuo — cálculo diferencial e integral, equações diferenciais e integrais, álgebra linear, e geometria analítica — pois acreditamos que um bom currículo, para os cursos de computação, deve cobrir esses assuntos através de várias disciplinas específicas, ainda nos primeiros anos de graduação. Pela mesma razão, excluimos cálculo numérico, e limitamos nossa exposição de probabilidade e estatística aos conceitos fundamentais. Ainda pela mesma razão, evitamos completamente a área de algoritmos, computabilidade e complexidade, bem como assuntos específicos (e quase obrigatórios) de currículos de computação, como programação inteira, autômatos e linguagens formais.

Na verdade, cada um dos capítulos deste livro poderia ser coberto por uma disciplina separada do currículo de computação. Este livro deve ser visto, em primeiro lugar, como um “ curso de

alfabetização”, que procura ensinar as definições e conceitos essenciais para comunicação técnica em teoria da computação.

Para atingir esse objetivo, tivemos que sacrificar a profundidade pela abrangência. Em um livro ou artigo sobre um assunto específico, é normal o autor escolher um conjunto de definições e notações, e usá-las consistentemente na obra toda, ignorando as outras escolhas possíveis. Mas esta atitude não seria adequada para este livro. Assim, por exemplo, dedicamos um bom espaço às múltiplas definições incompatíveis de conceitos fundamentais, como “número natural” (inclui ou não o zero?), “função”, “grafo”, e muitas outras, e às variações de notação que os estudantes podem vir a encontrar na literatura. Só depois dessas discussões é que adotamos uma definição ou notação específica, para uso no resto do livro.

Por outro lado, não nos preocupamos em enunciar, muito menos provar, os teoremas que são considerados fundamentais dessas áreas — exceto a título de exemplo de uso dos conceitos. Assim, nosso tratamento de grafos (capítulo ??) não pretende substituir disciplinas de teoria dos grafos, onde esses resultados devem ser cobertos em detalhe. Seu objetivo é apenas dar ao estudante familiaridade com os conceitos e vocabulário da área — para facilitar seu acompanhamento dessas disciplinas, e para que ele consiga entender e usar a linguagem de grafos em outras áreas da computação. O mesmo vale para todos os outros capítulos.

**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.

Acontece que essa não é uma habilidade nata. Seu apredizado requer, além de anos de prática, o conhecimento dos fundamentos da lógica. Embora as demonstrações que se encontram na literatura (e que os professores esperam que os alunos produzam) quase nunca são *formais* — sequências de fórmulas lógicas, encadeadas por aplicações de regras de inferência — o que caracteriza uma prova rigorosa é o fato de que ela pode ser *formalizada*. Assim, a lógica é o esqueleto *invisível* que sustenta e caracteriza uma demonstração válida.

Por esse motivo, optamos por iniciar nosso livro com uma exposição da lógica matemática, nas suas duas formulações clássicas — a teoria de conjuntos, por um lado, e a lógica proposicional e cálculo de predicados, pelo outro. Estamos supondo que os leitores deste livro já tiveram contato com o conceito de conjuntos, graças a disciplinas anteriores; portanto não julgamos necessário dedicar mais que algumas páginas a esse assunto. Os leitores interessados numa abordagem mais profunda podem consultar por exemplo o livro de Halmos [?]. Por outro lado, acreditamos que poucos leitores conhecem o cálculo de proposições e predicados (apesar do uso de operações booleanas em programação), e os conceitos de axiomas, teoremas, e demonstrações formais. Por essa razão, dedicamos três capítulos inteiros (3, 4 e 5) a esses tópicos — sendo que o último é inteiramente dedicado a técnicas de prova por indução.

**Relações e funções.** Outro tópico ao qual resolvemos dedicar bastante espaço é o conceito de relação. Relações são muito usadas em todas as áreas teóricas e práticas da computação, incluindo autômatos e circuitos lógicos, estruturas e bancos de dados, redes e comunicações digitais, etc..

Na literatura há duas principais abordagens para este conceito. Na primeira, uma relação entre dois conjuntos é uma tripla  $(A, B, R)$  onde  $A$  e  $B$  são conjuntos, e  $R$  é um subconjunto do produto cartesiano  $A \times B$ . Na outra, uma relação entre  $A$  e  $B$  é apenas um subconjunto de  $A \times B$ .

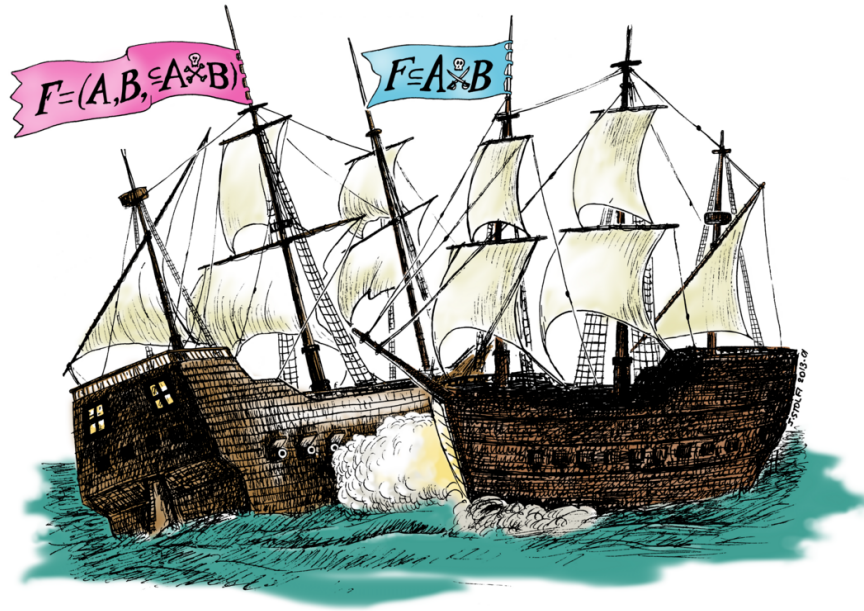


Figura 1: Debate acadêmico sobre definição de funções.

Esta diferença tem inúmeras repercussões em conceitos derivados, e inclusive na linguagem. Por exemplo, na primeira abordagem a relação tem um domínio “nominal” ( $A$ ), que é distinto de seu domínio “efetivo” (os elementos de  $A$  que aparecem no lado esquerdo de pares de  $R$ ). Na segunda abordagem, pelo contrário, existe apenas o domínio efetivo. A mesma observação vale para o contra-domínio. Na primeira abordagem existem infinitas relações vazias (com  $R = \emptyset = \{\}$ ), enquanto que na segunda só existe uma. Na primeira abordagem podemos dizer que uma relação é sobrejetora ou bijetora, enquanto que na segunda temos que especificar os conjuntos e dizer “sobrejetora em  $B$ ” e “bijetora entre  $A$  e  $B$ ”.

Cada abordagem tem suas vantagens e desvantagens. Constatamos inclusive que muitos livros textos são inconsistentes neste ponto, e adotam ora uma definição, ora outra, conforme as conveniências do momento. Debateremos muito qual destas duas abordagens deveríamos adotar para os capítulos seguintes (veja a figura 1.), e por fim resolvemos adotar a segunda (conjunto de pares, sem domínio e contra-domínio).

Enfrentamos um dilema semelhante na seção sobre relações de ordem, pois para esse conceito também há várias escolhas incompatíveis (ou mesmo ilógicas) de nomenclatura. Por exemplo, os termos “ordem parcial” e “ordem total” não são mutuamente exclusivos (como se esperaria pelo dicionário), mas um inclui o outro. E “relação de ordem estrita” não é um caso particular de relação de ordem, mas um conceito praticamente disjunto (uma é reflexiva e a outra é irreflexiva). Além disso, os termos “elemento mínimo” e “elemento máximo” são enganosos quando são aplicados à relação “ $\geq$ ” (ou a outras relações sobre números que não “ $\leq$ ”). Mas não cabe a este livro propor nomenclaturas mais consistentes; tudo o que podemos fazer é alertar o estudante para essas armadilhas.

**Somatórias e produtórias.** Dentro dos objetivos deste livro, nosso tratamento de somatórias e

produtórias (capítulo 9) dá mais ênfase à “linguagem” do que a resultados avançados da teoria. Assim, tomamos cuidado de expor o leitor às várias convenções da notação, e procuramos ensinar as principais técnicas de manipulação de somatórias (como troca de índices e mudança de ordem de soma). Por outro lado, também procuramos desenvolver a intuição dos estudantes, apontando as analogias entre somatórias e integrais (que eles supostamente conhecem de cálculos diferenciais e integrais anteriores).

**Sequências e recorrências.** Procuramos seguir a mesma filosofia no capítulo 10, que trata de sequências definidas por recorrências. Além de apresentar a linguagem, enfatizamos a técnica geral de resolução de recorrências lineares homogêneas, que resolve muitos dos problemas encontrados em computação.

**Contagem.** A análise combinatória é fundamental tanto para a análise de algoritmos quanto para inúmeras áreas práticas, e deveria merecer uma disciplina à parte. Neste livro nos limitamos a rever os conceitos de permutações, arranjos e combinações, e o teorema da inclusão e exclusão. Embora esses assuntos sejam oficialmente vistos no ensino fundamental e médio, consideramos oportuno rever as definições e fórmulas básicas, especialmente à luz dos conceitos de indução e recorrências vistos nos capítulos anteriores. Uma vez que problemas de contagem raramente admitem fórmulas simples e exatas, consideramos oportuno também apresentar a fórmula de aproximação de Stirling para a função fatorial.

**Cardinalidade de conjuntos infinitos.** A rigor, a teoria das cardinalidades infinitas tem pouca utilidade prática em computação. Porém, a distinção entre infinidades enumeráveis e não enumeráveis é relevante para a teoria da computação.

Por exemplo, a existência de funções não computáveis decorre trivialmente da observação de que o conjunto de funções de  $\mathbb{N}$  para  $\mathbb{N}$  (que tem a mesma cardinalidade que  $\mathbb{R}$ ) é maior que o conjunto de todos os algoritmos (que tem a mesma cardinalidade que  $\mathbb{N}$ ). Além disso, o argumento de diagonalização usado para provar que  $\mathbb{R}$  não é enumerável é usado, por exemplo, na demonstração do teorema de Turing.

Consideramos também que essa área é um capítulo importante da história da matemática, e portanto é “cultura geral” quase que obrigatória para quem tem curso superior em ciência ou tecnologia. Por outro lado, esse assunto nem sempre é visto nas outras disciplinas de matemática dos currículos de computação. Por essas razões, optamos por incluir um curto resumo desses conceitos neste livro (capítulo 13).

**Probabilidade.** Optamos por incluir neste livro um capítulo sobre noções elementares de estatística e probabilidade pois constatamos que eles são essenciais para várias disciplinas teóricas e aplicadas, como análise de algoritmos, criptografia, redes e serviços distribuídos, sistemas operacionais, compiladores, processamento de imagens, reconhecimento de padrões, e processamento de linguagens naturais. A teoria da probabilidade é também a fundação da teoria da informação (incluindo o conceito de bit!) e portanto para a análise de sistemas de comunicação, digitais ou não. Além disso, a teoria da probabilidade é parte da evolução da lógica matemática, o passo seguinte após o desenvolvimento do cálculo de predicados.

## **Agradecimentos**

Queremos agradecer aqui a todas as pessoas que contribuíram para este livro, com seus comentários e sugestões: nossos colegas André Vignatti, Arnaldo V. Moura, Cândida N. da Silva, Célia P. de Mello, Orlando Lee, Otília T. W. Paques e Pedro J. de Rezende, e os alunos Gustavo T. Vicentini, Luiz F. F. Pereira, e Vinícius N. G. Pereira. Queremos agradecer em especial a Mário San Felice, que revisou todo o texto, incluindo os exercícios, e fez inúmeras correções e sugestões que muito melhoraram o texto.

# Capítulo 1

## Introdução à lógica matemática

### 1.1 Como ter certeza?

Você escreveu um programa, ou inventou um algoritmo, para resolver um certo problema. Como pode você se convencer que ele funciona? Como pode você convencer os outros que ele funciona?

Uma maneira de adquirir confiança sobre um algoritmo é testá-lo. Porém, para a maioria dos algoritmos, é impossível montar testes que verifiquem absolutamente todos os casos possíveis que podem ocorrer durante sua execução. Todo programador experiente já viu um programa funcionar perfeitamente em todos os testes, mas falhar imediatamente quando usado na prática.

## 1.2 A invenção da lógica

Essa questão — como ter certeza que nosso raciocínio é correto, e como transmitir aos outros essa certeza — foi estudada pelos gregos séculos antes de Cristo. Eles observaram que uma maneira de conseguir esse tipo de certeza, e para passar essa certeza a outras pessoas, é começar por um conjunto de *axiomas*, fatos simples que todos concordam que são verdade; e desenvolver um raciocínio a partir desses axiomas, usando *regras de inferência*, maneiras de raciocinar que todos concordam que são válidas. Com isso eles inventaram a *lógica*, que eles consideravam um ramo da *retórica*, a arte de discursar e convencer pessoas.

O filósofo grego Aristóteles (384–322 A.C.), em particular, estudou os chamados *silogismos*, raciocínios em que, partindo de duas premissas cuja verdade é aceita, obtém-se uma conclusão nova que é necessariamente verdadeira. Por exemplo, se acreditamos nas premissas “todos os homens são mortais” e “Sócrates é um homem”, então temos que acreditar também que “Sócrates é mortal.”. Ou então, se acreditamos que “nenhum mamífero tem penas”, e que “morcegos são mamíferos”, então temos que acreditar que “morcegos não tem penas”.

## 1.3 Euclides e demonstrações geométricas

Enquanto isso, os arquitetos e engenheiros gregos tinham preocupações semelhantes em relação aos “algoritmos geométricos” — construções com régua e compasso — que eles usavam em seus projetos. Por exemplo, a receita da figura 1.1 supostamente constrói um pentágono com todos os lados e ângulos iguais.

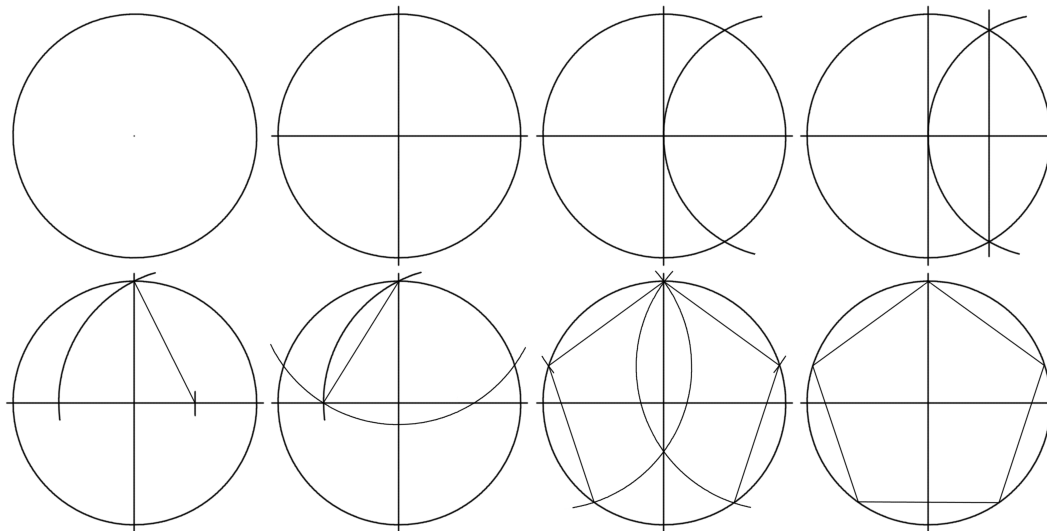


Figura 1.1: Construção de um pentágono regular.

Como podemos ter certeza de que essa construção realmente faz isso? Podemos efetuá-la numa folha de papel e medir os ângulos; mas tanto os passos da construção quanto a medida final tem sempre pequenos erros, e portanto esse teste não vai dizer se a construção é matematicamente correta ou apenas aproximada. Se as diferenças entre os ângulos são desprezíveis no papel, será que serão desprezíveis quando esse algoritmo for usado na construção de um anfiteatro?

O primeiro a descrever um sistema lógico completo para a geometria da época foi o geômetra grego Euclides (que viveu por volta do século III antes de Cristo), no seu livro *Elementos de Geometria* [?]. Euclides começou enumerando dez axiomas sobre conceitos geométricos (pontos, retas, círculos, distâncias, ângulos), 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.*

Em seguida Euclides mostrou centenas de outras afirmações (*teoremas*) que decorrem desses axiomas, como 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.*

Muitos desses teoremas são afirmações de que certas construções geométricas, como a da figura 1.1, produzem o resultado desejado. Principalmente, para cada teorema, ele também 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.

## 1.4 Álgebra

A lógica de Euclides e outros filósofos gregos foi extensamente usada por mais de dois mil anos. Entretanto, por muitos séculos o hábito de provar as afirmações foi limitado apenas à geometria. Embora os gregos conhecessem muitas propriedades de números (por exemplo, os conceitos de divisor comum e número primo), para demonstrar tais propriedades eles geralmente convertiam os números em comprimentos de retas. Esse é o caso, por exemplo, do *algoritmo de Euclides* para calcular o máximo divisor comum de dois números — que é considerado por muitos o mais antigo algoritmo não trivial. Na descrição original de Euclides, o problema era dividir dois segmentos de reta dados em partes iguais e de maior tamanho possível.

Na idade média, entretanto, o matemático 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. Na álgebra, os números são representados abstratamente por letras, e as operações ou afirmações sobre esses números são indicadas com símbolos como ‘+’ ou ‘>’. A álgebra também fornece algumas identidades e desigualdades, como  $A + B = B + A$  e  $A \times (B + C) = (A \times B) + (A \times C)$ , que são sempre verdadeiras, quaisquer que sejam os números representados pelas variáveis. A álgebra também fornece regras que permitem 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  $A > C$ .

A geometria e a álgebra foram enfim unidas pelo matemático René Descartes (1596–1650), que mostrou como usar pares de números reais para representar pontos do plano. Entre outras consequências, essa idéia revolucionária criou toda a área da geometria analítica e forneceu uma interpretação geométrica para álgebra linear.

## 1.5 As linguagens da lógica matemática

Em seguida à revolução de Descartes, outros matemáticos, principalmente no século 19, mostraram como aplicar a idéia geral da álgebra também à lógica. Esse trabalho produziu dois principais sistemas de notação, ou *linguagens formais*, para expressar raciocínios lógicos de maneira matematicamente clara, sucinta, e, principalmente, livre de ambiguidades. Estas linguagens são a *teoria de conjuntos* e o *cálculo de predicados*.

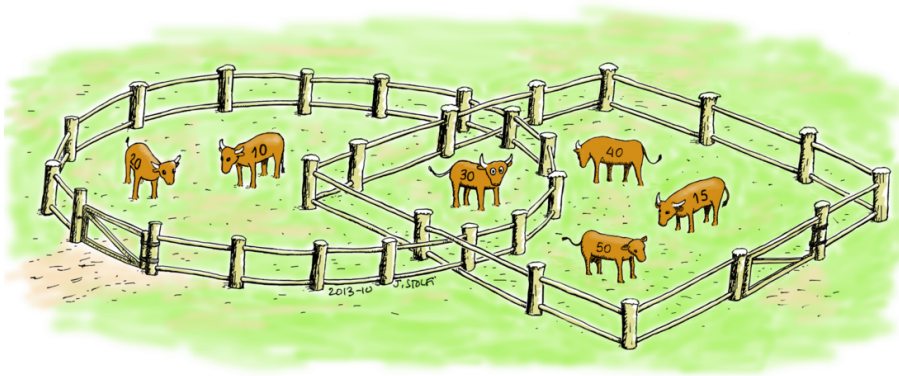
As duas linguagens são essencialmente equivalentes, mas continuam sendo usadas e misturadas, inclusive na mesma sentença, conforme a que for mais conveniente ou clara em cada momento.

A lógica clássica somente lida com afirmações que são verdadeiras ou falsas. Essa característica praticamente restringe o uso da lógica para afirmações matemáticas. Mas no século 16 e 17 matemáticos começaram a estudar o cálculo de chances em jogos de azar (dados, roletas, loteria, etc.). No início do século 20 estas investigações haviam evoluído para a *teoria da probabilidade*, que permite expressar nosso grau de confiança a respeito de afirmações incertas, e raciocinar com precisão sobre elas; e para a *estatística*, um conjunto de técnicas para analisar dados experimentais que supostamente confirmam ou refutam tais afirmações.

Em meados do século XX, motivada pela expansão do rádio, telefone e outros meios eletrônicos de comunicação, a teoria da probabilidade por sua vez deu origem à *teoria da informação*, que permite determinar, por exemplo, a capacidade real de canais de comunicação na presença de distúrbios aleatórios no sinal recebido. Finalmente, com o surgimento do computador digital, surgiram disciplinas matemáticas específicas para raciocinar precisamente com programas e estruturas de dados, incluindo *análise de algoritmos*, *teoria da computabilidade e complexidade de funções*, *criptografia digital*, e muitas outras.

# Capítulo 2

## Teoria dos Conjuntos



Acreditamos que o leitor já teve contato com os conceitos básicos da teoria dos conjuntos, como *elemento*, *união*, *interseção*, etc.. Nesta seção vamos revisar esses conceitos.

Embora seja possível desenvolver a teoria de conjuntos de maneira axiomática, como foi feito por Georg Cantor (1845–1918) e Ernest Zermelo (1871–1953), a abordagem informal apresentada é suficiente para nossos propósitos.

## 2.1 Conjuntos, elementos e pertinência

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  $x \notin A$ .

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  $A \not\ni x$ .

Por exemplo, se  $P$  representa o conjunto de todos os números primos, as afirmações  $7 \in P$ ,  $4 \notin P$ ,  $P \ni 7$ , e  $P \not\ni 4$  são verdadeiras; enquanto que  $4 \in P$ ,  $7 \notin P$ ,  $P \ni 4$ , e  $P \not\ni 7$  são falsas.

Não é correto ler  $x \in A$  ou  $A \ni x$  com a frase “ $A$  contém  $x$ ”, pois o termo ‘ontém’ é usado em matemática com um sentido bem diferente (veja a seção 2.2)

A notação  $x, y, z \in A$  é muito usada como uma abreviação de “ $x \in A$  e  $y \in A$  e  $z \in A$ .”

### 2.1.1 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  $A$ .

Por exemplo, o conjunto  $A$  de todos os inteiros maiores que 2 e menores que 6 é igual ao conjunto  $\{3, 4, 5\}$ ; mas é diferente do conjunto  $\{3, 4, 5, 6\}$ , porque 6 está neste mas não em  $A$ ; e diferente do conjunto  $\{3, 5\}$ , porque 4 está em  $A$  mas não está neste.

### 2.1.2 Especificando conjuntos explicitamente

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  $4 \notin \{2, 3, 5\}$ .

Considerando que os elementos de um conjunto são todos distintos e não tem nenhuma ordem especial, repetições e permutações dos elementos são ignoradas na notação '{ }'. Por exemplo,  $\{2, 3, 5\}$ ,  $\{5, 2, 3\}$ , e  $\{2, 5, 2, 3, 3, 3, 5\}$  são três maneiras equivalentes de descrever o mesmo conjunto, cujos elementos são 2, 3, e 5. Note que todo elemento que pertence a qualquer um destes conjuntos também pertence aos outros dois.

### 2.1.3 Especificando conjuntos por propriedades

Outra maneira de especificar um conjunto é pelas propriedades de seus elementos. Para tanto, usamos a notação  $\{x : P(x)\}$ , onde  $x$  é uma variável arbitrária, não definida pelo contexto, e  $P(x)$  uma afirmação matemática que depende do valor de  $x$ . Essa notação é lida “o conjunto de todos os  $x$  tais que  $P(x)$ ”. Por exemplo, o conjunto  $\{-4, -3, -2, -1, 0, +1, +2, +3, +4\}$  pode ser escrito

$$\{x : x \text{ é um número inteiro e } -5 < x < 5\} \quad (2.1)$$

Se  $A$  é um conjunto previamente definido, a notação  $\{x \in A : P(x)\}$  é abreviação de  $\{x : x \in A \text{ e } P(x)\}$ .

Mais geralmente, podemos escrever  $\{F(x) : P(x)\}$ , onde  $x$  e  $P(x)$  são como acima, e  $F(x)$  é uma fórmula matemática que envolve  $x$ . Essa notação é lida “o conjunto dos valores  $F(x)$ , para todos os  $x$  tais que  $P(x)$ ”.

Por exemplo, a notação  $\{x^2 : x \text{ é um inteiro e } -4 \leq x \leq +2\}$  significa o conjunto  $\{0, 1, 4, 9, 16\}$ . Note que o elemento 4 é obtido duas vezes, quando  $x = -2$  e quando  $x = +2$ ; mas mesmo assim pertence apenas uma vez ao conjunto.

Alguns livros e autores usam o símbolo ‘|’ em vez de ‘:’ para significar “tais que”.

**Exercício 2.1:** Escreva os elementos dos conjuntos abaixo:

- (a)  $\{x : x \text{ é raiz do polinômio } x^4 - 5x^2 + 6\}$
- (b)  $\{x^2 + 1 : x \text{ é raiz do polinômio } x^4 - 5x^2 + 6\}$
- (c)  $\{x \in \{1, 2, 3, 4\} : x \text{ é raiz do polinômio } x^4 - 5x^2 + 6\}$

### 2.1.4 Conjunto vazio

É possível definir conjuntos sem elementos. Dizemos que tal conjunto é *vazio*. Por exemplo, considere o conjunto  $A$  de todos os números inteiros  $x$  tais que  $x = x + 1$ . Não existe nenhum inteiro  $x$  com essa propriedade; portanto esse conjunto é vazio.

Todos os conjuntos vazios são iguais; ou seja existe um único conjunto vazio. Esse conjunto é geralmente denotado por  $\emptyset$ , mas pode ser escrito também  $\{\}$  — a notação que usaremos neste livro.

### 2.1.5 Conjuntos importantes

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

os *números inteiros*  $\mathbb{Z}$ ,

os *números naturais*  $\mathbb{N} = \{x : x \in \mathbb{Z} \text{ e } x \geq 0\}$ ,

os *números racionais*  $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ e } b \neq 0\right\}$ , e

os *números reais*  $\mathbb{R}$ .

os *números complexos*  $\mathbb{C} = \{x + y\mathbf{i} : x, y \in \mathbb{R}\}$ , onde  $\mathbf{i} = \sqrt{-1}$ .

os *números irracionais*, todos os números reais que não são racionais;

os *números algébricos*, as raízes de polinômios com coeficientes inteiros;

os *números transcendentais*, todos os números reais que não são algébricos.

**Zero é natural?** Alguns livros e autores, especialmente os mais antigos, definem os números naturais  $\mathbb{N}$  com ‘>’ em vez de ‘ $\geq$ ’; ou seja, consideram que zero não é um número natural. Essa escolha possivelmente se deve ao fato de que, em muitas línguas, a quantia zero é expressa de maneira bem diferente da usada para números positivos: em vez de “tenho zero bois”, diz-se “não tenho bois”. Em latim nem sequer existia uma palavra para esse número, que não pode ser escrito em algarismos romanos. (A palavra tem origem árabe, e foi introduzida na Europa apenas na Idade Média, junto com os algarismos “arábicos” inventados na Índia séculos antes.) Na alfabetização de crianças, o número zero era geralmente ensinado bem depois de 1, 2, 3, etc., como um conceito “avançado”.

Matematicamente, porém, não há nada errado com “zero bois” — e crianças podem aprender o número 0 até mais facilmente que o número 2. Hoje em dia, a definição de  $\mathbb{N}$  que inclui zero parece ser mais popular. É a recomendada pela ISO (padrão 80000-2) e, no geral, a mais útil em computação. Muitos matemáticos até definem  $\mathbb{N}$  como “o conjunto de todas as cardinalidades de conjuntos finitos” (veja a seção 2.1.6); e 0 é a cardinalidade do conjunto vazio.

**Exercício 2.2:** Escreva explicitamente os elementos dos seguintes conjuntos:

- (a)  $\{x \in \mathbb{Z} : x^2 - 2x + 1 \leq 0\}$ .
- (b)  $\{x \in \mathbb{Z} : 2 \leq x \leq 20 \text{ e } x \text{ é primo}\}$ .
- (c)  $\{x \in \mathbb{R} : x^2 - 2x = 0\}$ .

### 2.1.6 Conjuntos finitos e infinitos; 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  $A = \{\}$ .

**Exercício 2.3:** Determine a cardinalidade dos seguintes conjuntos:

- (a)  $\{x \in \mathbb{Z} : -2 \leq x \leq 4\}$
- (b)  $\{x \in \mathbb{Z} : 10 \leq x^2 \leq 100\}$
- (c)  $\{x \in \mathbb{R} : x^4 - 5x^2 + 6 = 0\}$
- (d)  $\{\sin(k\pi/7) : k \in \mathbb{N}\}$

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

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, +1, +2, +3, \dots\}$$

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

### 2.1.7 Definições circulares e contraditórias

A definição de um conjunto pode usar outros conjuntos, como por exemplo “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. Um exemplo clássico é a definição “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.

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*, pois foi exemplificado com uma anedota em 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 — deixando o barbeiro na dúvida sobre o que ele deveria fazer com a sua.

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 no capítulo 5.

## 2.2 Relações 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*  $B$ , ou que  $B$  *contém*  $A$ . Denotamos esta condição por  $A \subseteq B$  ou  $B \supseteq A$ .

Se existe um elemento de  $A$  que não pertence a  $B$ , então  $A$  não é subconjunto de  $B$ , e escrevemos  $A \not\subseteq B$ . De acordo com esta definição, todo conjunto está contido em si próprio e contém o conjunto vazio; ou seja,  $A \subseteq A$  e  $\{\} \subseteq A$ , para qualquer conjunto  $A$ .

Note que se  $A \subseteq B$  e  $B$  é finito, então  $|A| \leq |B|$ . Porém, a recíproca não vale. Por exemplo, seja  $A = \{2, 3\}$  e  $B = \{3, 4, 5\}$ : temos  $|A| \leq |B|$ , mas  $A \not\subseteq B$ .

Se  $A \subseteq B$  mas  $A \neq B$ , dizemos que  $A$  é um sub-conjunto *próprio* de  $B$ , que denotamos por  $A \subset B$  ou  $B \supset A$ . Analogamente,  $A \not\subset B$  significa que  $A$  não é um subconjunto próprio de  $B$ .

Note também que os *símbolos* das relações de conjuntos ' $\subseteq$ ' e ' $\subset$ ' são consistentes com os *símbolos* das relações de comparação de números ' $\leq$ ' e ' $<$ ': nos dois casos, o traço na parte inferior indica que os objetos podem ser iguais, e a ausência do traço significa que não podem. Porém, a *nomenclatura* é inconsistente: ' $\subseteq$ ' lê-se “contido” enquanto que “ $\leq$ ” lê-se “menor ou igual”, e “ $\subset$ ” lê-se “propriamente contido” enquanto que “ $<$ ” lê-se “menor”.

## 2.3 Operações com conjuntos

Para os próximos conceitos, vamos supor que  $A$  e  $B$  são dois conjuntos.

### 2.3.1 União e interseção

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  $B$ . Por exemplo, se  $A = \{1, 2, 3\}$  e  $B = \{2, 4, 5\}$  então  $A \cup B = \{1, 2, 3, 4, 5\}$ .

A *interseção* de  $A$  e  $B$ , denotada por  $A \cap B$ , é o conjunto de todos os elementos que estão em ambos os conjuntos,  $A$  e  $B$ . Por exemplo, se  $A = \{1, 2, 3\}$  e  $B = \{0, 1, 3, 5\}$  então  $A \cap B = \{1, 3\}$ . (Esta palavra também pode ser escrita “intersecção”, e neste caso a letra “c” pode ser pronunciada ou não.)

Se  $A \cap B = \{\}$  dizemos que os conjuntos  $A$  e  $B$  são *disjuntos*, ou *não tem interseção*, ou *não se intersectam*.

Diz-se também que três ou mais conjuntos são *disjuntos dois a dois* se todos os pares desses conjuntos são disjuntos. Por exemplo, os conjuntos  $A = \{1, 2\}$ ,  $B = \{3, 4, 5\}$  e  $C = \{6, 7\}$  são disjuntos dois a dois, pois  $A \cap B = A \cap C = B \cap C = \{\}$ . Por outro lado, os conjuntos  $X = \{1, 2\}$ ,  $Y = \{2, 3\}$ , e  $Z = \{4, 5\}$  *não* são disjuntos dois a dois, pois  $X \cap Y = \{2\} \neq \{\}$ ; embora a interseção  $X \cap Y \cap Z$  dos três seja o conjunto vazio.

### 2.3.2 Diagrama de Venn

A figura 2.1 mostra uma representação gráfica das operações de conjuntos:

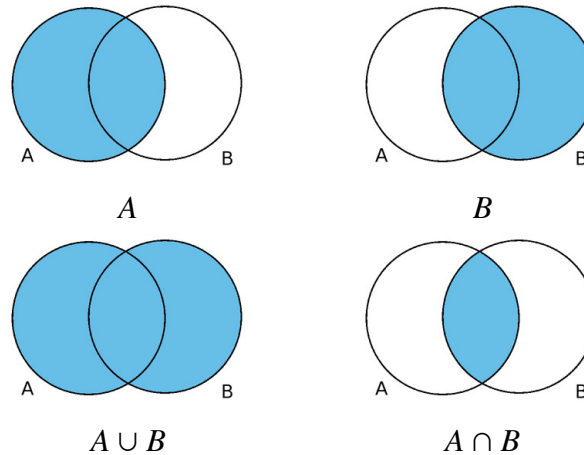


Figura 2.1: Diagrama de Venn da união e interseção.

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

**Exercício 2.4:** Sejam  $A$  e  $B$  dois conjuntos finitos quaisquer. Encontre uma fórmula matemática que relaciona  $|A|$ ,  $|B|$ ,  $|A \cap B|$  e  $|A \cup B|$ .

### 2.3.3 Diferença

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* ou *relativo a A*, e é denotado por  $A \setminus B$  (ou, para alguns autores, por  $A - B$ ). Por exemplo, se  $A = \{1, 2, 3, 4\}$  e  $B = \{2, 4, 6\}$ , então  $A \setminus B = \{1, 3\}$ , e  $B \setminus A = \{6\}$ .

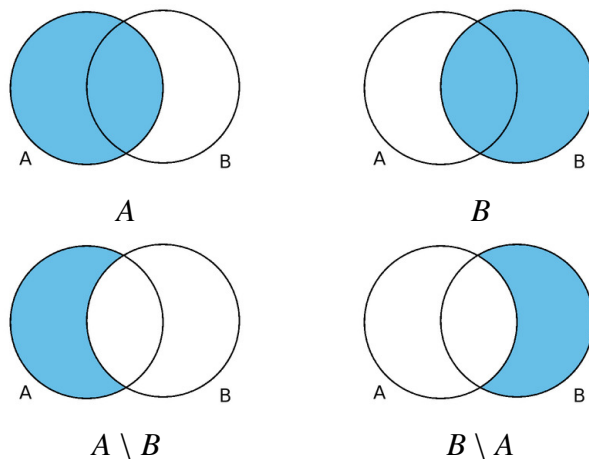


Figura 2.2: Diagrama de Venn da diferença de conjuntos.

**Exercício 2.5:** Sejam  $A = \{1, 2, 3, 4\}$ ,  $B = \{n \in \mathbb{N} : n \text{ é ímpar e } n \leq 5\}$  e  $C = \{x \in \mathbb{R} : (x^2 - 4)(x^2 - 3) = 0\}$ . Calcule todas as diferenças  $A \setminus B$ ,  $B \setminus A$ ,  $A \setminus C$ ,  $C \setminus A$ ,  $B \setminus C$ , e  $C \setminus B$ .

### 2.3.4 Conjunto universal e complemento

Em certas situações, é conveniente supor que todos os elementos de todos os conjuntos que nos interessam pertencem a um *conjunto universal* ou *universo*, que denotaremos por  $\mathbb{U}$ . Nesse caso, a diferença  $\mathbb{U} \setminus B$  é dita o *complemento de B* denotado por  $\overline{B}$  (ou, segundo alguns, por  $B^c$ ).

Observe que se  $A \subseteq B$  então  $A \cup B = B$ ,  $A \cap B = A$  e  $\overline{B} \subseteq \overline{A}$ .

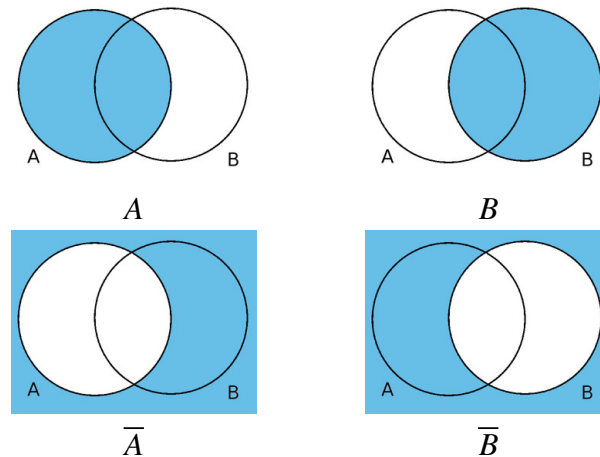


Figura 2.3: Diagrama de Venn do complemento.

**Exercício 2.6:** Seja  $\mathbb{U} = \{n \in \mathbb{N} : 0 \leq n \leq 9\}$  o conjunto universal, e sejam  $A = \{1, 2, 3, 4\}$  e  $B = \{n \in \mathbb{N} : n \text{ é ímpar}\}$ . Determine os conjuntos  $\overline{A}$  e  $\overline{B}$ .

### 2.3.5 Diferença simétrica

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

$$A \triangle B = (A \setminus B) \cup (B \setminus A) \quad (2.2)$$

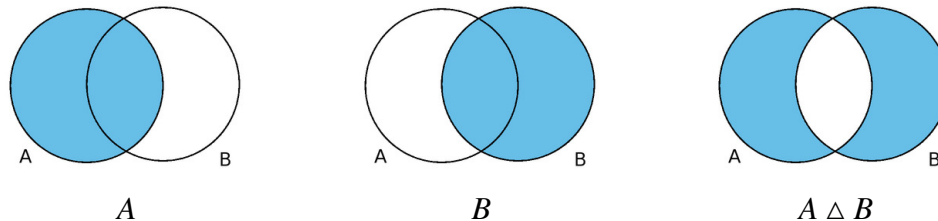


Figura 2.4: Diagrama de Venn da diferença simétrica.

**Exercício 2.7:** O que se pode dizer sobre os conjuntos  $A$  e  $B$  se:

- (a)  $A \triangle B = \{\}$
- (b)  $A \triangle B = A$
- (c)  $A \triangle B = A \cup B$
- (d)  $A \triangle B = A \setminus B$

### 2.3.6 Propriedades das operações com conjuntos

A seguir listaremos algumas propriedades que são satisfeitas pelas 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:*

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

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

- *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:*

$$\overline{\overline{A}} = A.$$

$$A \cup \overline{A} = \mathbb{U}.$$

$$A \cap \overline{A} = \{\}.$$

$$\overline{\mathbb{U}} = \{\}.$$

$$\overline{\{\}} = \mathbb{U}.$$

- *Propriedades do conjunto universal:*

$$A \cup \mathbb{U} = \mathbb{U}.$$

$$A \cap \mathbb{U} = A.$$

- *Propriedades do conjunto vazio:*

$$A \cup \{\} = A.$$

$$A \cap \{\} = \{\}.$$

**Exercício 2.8:** Encontre conjuntos  $A$  e  $B$  tais que (a)  $(A \cup B) \setminus B = A$  e (b)  $(A \cup B) \setminus B \neq A$

**Exercício 2.9:** 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 2.10:** Diagramas de Venn podem ser usados para três ou mais conjuntos. Um diagrama de Venn para três conjuntos  $A$ ,  $B$  e  $C$ , por exemplo, precisa dividir o plano em 8 regiões, correspondendo a todas as possíveis relações (pertence ou não pertence) entre um elemento e esses três conjuntos. Desenhe tal diagrama e use-o para mostrar as seguintes fórmulas:

- (a)  $A \cap B \cap C$ .
- (b)  $A \cup B \cup C$ .
- (c)  $(A \cup B) \setminus C$ .
- (d)  $(A \setminus B) \cup (B \setminus C) \cup (C \setminus A)$ .

**Exercício 2.11:** Use diagramas de Venn para verificar as seguintes identidades:

- (a)  $A \setminus (A \cap B) = A \setminus B$ .
- (b)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .
- (c)  $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ .
- (d)  $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$ .

**Exercício 2.12:** 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  $|A \cap B \cap C|$ .

## 2.4 Conjuntos de conjuntos

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

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

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  $A$  ( $B \not\subseteq A$ ). Note que  $\{\}$  é elemento de  $A$  e também subconjunto de  $A$ , enquanto que  $\{2\}$  não é nem uma coisa nem outra.

Em particular, o conjunto  $A = \{\{\}\}$  *não* é vazio, pois ele tem um elemento — o conjunto vazio. Observe que  $|\{\{\}\}| = 1$ , enquanto que  $|\{\}| = 0$ .

Os elementos de um conjunto também podem ser conjuntos de conjuntos, conjuntos de conjuntos de conjuntos, e assim por diante. Por exemplo, os conjuntos  $A = \{\{\}\}$ ,  $B = \{\{\}, A\}$ ,  $C = \{A, \{A\}\}$ ,  $\{A, \{A\}\}$  são todos distintos.

Na medida que os elementos de conjuntos de interesse podem ser conjuntos, é necessário supor que o conjunto universal  $\mathbb{U}$  possui também estes conjuntos como elementos. Assim, por exemplo, num contexto em que o conjunto  $\{1, 2, 3, \{10, 20\}\}$  pode ser relevante, devemos supor que  $\mathbb{U}$  possui não apenas 1, 2, 3, 10 e 20, mas também  $\{10, 20\}$ ; ou seja,  $\{10, 20\} \in \mathbb{U}$  (não apenas  $\{10, 20\} \subseteq \mathbb{U}$ ).

Porém, não se deve supor que  $\mathbb{U}$  possua *todos* os conjuntos como elementos. Nesse caso,  $\mathbb{U}$  também seria um elemento de  $\mathbb{U}$ ; e supor que um conjunto pode ser elemento de si mesmo pode levar a fórmulas e definições que não fazem sentido, como “seja  $X$  o conjunto de todos os elementos que não pertencem a  $X$ .”

**Exercício 2.13:** Considere os conjuntos  $A = \{\{\}\}$ ,  $B = \{\{\{\}\}, \{\}\}$  e  $C = \{\{\{\{\}\}\}, \{\{\}, \{\{\}\}\}, \{\{\}\}\}$ .

- (a) Determine as cardinalidades de  $A$ ,  $B$  e  $C$ .
- (b) Dentre esses três conjuntos, quais são elementos de quais?
- (c) Dentre esses três conjuntos, quais são subconjuntos de quais?
- (d) Quais são os elementos de  $\{|x| : x \in C\}$ ?

### 2.4.1 Conjunto potência

O conjunto de todos os subconjuntos de um conjunto  $A$  é chamado de *conjunto potência* de  $A$ , e denotado por  $\mathcal{P}(A)$ .

Por exemplo, se  $A = \{1, 2, 3\}$  então  $\mathcal{P}(A) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ .

Observe que se  $A = \{\}$  então  $\mathcal{P}(A) = \{\{\}\}$ , e se  $A = \{\{\}\}$  então  $\mathcal{P}(A) = \{\{\}, \{\{\}\}\}$ .

Se  $A$  é um conjunto finito, então  $|\mathcal{P}(A)| = 2^{|A|}$ . Este fato será demonstrado no capítulo 5. Por esta razão, muitos autores denotam o conjunto potência de  $A$  por  $2^A$ .

**Exercício 2.14:** Se  $A$  é um conjunto qualquer, e  $B$  é a união de todos os elementos de  $\mathcal{P}(A)$ , o que podemos dizer sobre  $A$  e  $B$ ?

**Exercício 2.15:** Sejam  $A$  e  $B$  dois conjuntos arbitrários. Qual a relação entre  $\mathcal{P}(A \cup B)$ ,  $\mathcal{P}(A \cap B)$ ,  $\mathcal{P}(A)$  e  $\mathcal{P}(B)$ ?

**Exercício 2.16:** Seja  $\mathcal{X}$  o conjunto de todos os conjuntos finitos de números naturais; de modo que, por exemplo,  $\{2, 3, 5\} \in \mathcal{X}$ , e  $\{235\} \in \mathcal{X}$ . Qual é a relação entre  $\mathcal{X}$  e  $\mathcal{P}(\mathbb{N})$ ?

## 2.5 Partição

Seja  $A$  um conjunto, e  $P$  um conjunto cujos elementos são sub-conjuntos de  $A$  (isto é,  $P \subseteq \mathcal{P}(A)$ ). 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.

Por 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  $A$  em quatro partes. Os conjuntos  $\{3\}$  e  $\{4, 8, 10\}$  são partes de  $P$  (e portanto subconjuntos de  $A$ , mas não partes de  $A$ ), enquanto que  $\{\}$ ,  $\{1, 2, 5\}$ , e  $\{3, 4, 8, 10\}$  não são partes de  $P$ , embora sejam subconjuntos de  $A$ .

Observe que, para qualquer conjunto não-vazio  $A$ , o conjunto  $\{A\}$  é sempre uma partição de  $A$ ; às vezes chamada de *partição trivial*. Além disso, se  $B$  é qualquer subconjunto próprio e não vazio de  $A$  ( $\{\} \subset B \subset A$ ), então o conjunto  $\{B, A \setminus B\}$  também é uma partição de  $A$ .

O conjunto vazio tem apenas uma partição, que é o próprio conjunto vazio (sem nenhuma parte).

**Exercício 2.17:** Determine todas as partições distintas dos seguintes conjuntos:

- (a)  $\{17\}$
- (b)  $\{17, 18\}$
- (c)  $\{\{17, 18\}\}$
- (d)  $\{1, 2, 3, 4\}$

**Exercício 2.18:** 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  $n$  tais que  $|n|$  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.
- (e)  $\{P_0, P_1, P_2, \dots, P_9\}$ , onde  $P_k$  é o conjunto de todos os inteiros cujo quadrado termina com o algarismo  $k$ . (Por exemplo,  $P_6 = \{4, -4, 6, -6, 14, \dots\}$ .)
- (f)  $\{\{0\}\} \cup \{P_k : k \in \mathbb{N}\}$ , onde  $P_k$  é o conjunto de todos os inteiros  $x$  cujo valor absoluto  $|x|$  está entre  $2^k$  (inclusive) e  $2^{k+1}$  (exclusive).

**Exercício 2.19:** Quais dos conjuntos abaixo são partições do conjunto  $\mathbb{R}$  dos números reais?

- (a)  $\{\mathbb{R}^+, \{0\}, \mathbb{R}^-\}$ , onde  $\mathbb{R}^+$  é o conjunto dos números reais positivos e  $\mathbb{R}^-$  é o conjunto dos números reais negativos.
- (b)  $\{\mathbb{I}, \mathbb{Q}\}$  onde  $\mathbb{I}$  é o conjunto dos números irracionais e  $\mathbb{Q}$  é o conjunto dos números racionais.
- (c)  $\{ \{x + n : n \in \mathbb{Z}\} : x \in [0, 1) \}$ .

## 2.6 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  $b = d$ .

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  $A = \{\}$  ou  $B = \{\}$ ).

**Exercício 2.20:** Quantos elementos tem o conjunto  $A \times B$  se o conjunto  $A$  tem  $p$  elementos, e o conjunto  $B$  tem  $q$  elementos?

**Exercício 2.21:** O produto cartesiano é distributivo sobre união, interseção, e diferença? Ou seja, se  $A$ ,  $B$  e  $C$  são três conjuntos quaisquer, as identidades abaixo valem?

(a)  $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(b)  $(A \cap B) \times C = (A \times C) \cap (B \times C)$

(c)  $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

### 2.6.1 Produto cartesiano de vários conjuntos

Definimos uma *ênupla ordenada*, ou simplesmente *ênupla*, como sendo uma sequência finita de  $m$  elementos  $(x_1, x_2, \dots, x_m)$ . (Sequências finitas são definidas formalmente na seção 8.13.) 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.

Em particular, uma 1-upla é uma sequência  $(a_1)$  com apenas um elemento, às vezes chamada de *sequência trivial*. Note que a 1-upla  $(10)$  não é a mesma coisa que o inteiro 10. Há uma única 0-upla, a *ênupla vazia* ou *sequência vazia*, denotada por  $()$ .

O *produto cartesiano* de  $m$  conjuntos  $A_1, A_2, \dots, A_m$ , denotado por  $A_1 \times A_2 \times \dots \times A_m$ , é o conjunto das  $m$ -uplas  $(a_1, a_2, \dots, a_m)$ , com  $a_i \in A_i$  para  $i = 1, 2, \dots, m$ .

Por exemplo, se  $A = \{1, 2\}$ ,  $B = \{30, 40, 50\}$ , e  $C = \{\pi\}$ , então  $A \times B \times C$  é o conjunto  $\{(1, 30, \pi), (1, 40, \pi), (1, 50, \pi), (2, 30, \pi), (2, 40, \pi), (2, 50, \pi)\}$ .

**Exercício 2.22:** Qual é a cardinalidade do produto  $A_1 \times A_2 \times \cdots \times A_m$ , em função das cardinalidades de  $A_1, A_2, \dots, A_m$ ? Quando é que o produto é vazio?

## 2.6.2 Produto cartesiano de conjunto consigo mesmo

Se todos os conjuntos  $A_1, A_2, \dots, A_m$  são o mesmo conjunto  $A$ , o produto cartesiano  $A_1 \times A_2 \times \cdots \times A_m$  é denotado por  $A^m$ . Por exemplo, se  $A = \{1, 2, 3\}$ , temos

$$A^3 = \{(1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 2, 1), (1, 2, 2), \dots, (3, 2, 3), (3, 3, 1), (3, 3, 2), (3, 3, 3)\}$$

$$A^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

$$A^1 = \{(1), (2), (3)\}$$

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

Note que, se  $A$  não é vazio,  $A^1$  é diferente de  $A$  (embora tenha o mesmo número de elementos).

Note também que  $A^0$ , para qualquer  $A$ , é o conjunto  $\{()\}$  cujo único elemento é a ênupla vazia, e portanto diferente de  $()$ ,  $\{\}$ , e  $\{\{\}\}$ . Em particular,  $\{\}^0 = \{()\}$

**Exercício 2.23:** Quanto elementos tem o conjunto  $A^3$  se o conjunto  $A$  tem  $n$  elementos? Se  $|A^3| \leq |A|$ , o que podemos dizer sobre  $A$ ?

**Exercício 2.24:** Seja  $A = \{20, 30\}$ . Descreva os conjuntos (a)  $(A^1)^1$ , (b)  $(A^2)^1$ , e (c)  $(A^2)^1$ .

**Exercício 2.25:** Se  $A$  é um conjunto tal que  $A \times A = \{(x, x) : x \in A\}$ , o que podemos dizer sobre  $A$ ?

**Exercício 2.26:** Se  $A$ ,  $B$  e  $C$  são conjuntos tais que  $A \times B \times C = B \times C \times A$ , o que podemos dizer sobre  $A$ ,  $B$  e  $C$ ?

**Exercício 2.27:** Se  $A$ ,  $B$  e  $C$  são conjuntos tais que  $A \times B \times C = B \times C \times A$ , o que podemos dizer sobre  $A$ ,  $B$  e  $C$ ?

**Origem do nome:** O nome “cartesiano” é referência ao matemático francês-holandês René Descartes (1596–1650), chamado Renatus Cartesius em latim, que unificou a álgebra e a geometria ao usar pares de números reais para representar os pontos de Euclides, e equações algébricas para definir curvas como retas e círculos. Nesta abordagem, o plano euclidiano é representado pelo conjunto  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ , dito o *plano cartesiano*; e o espaço tridimensional pelo conjunto  $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ , o *espaço cartesiano*. Estas representações são fundamentais para o uso de computadores em cálculos geométricos, especialmente nas áreas de computação gráfica e geometria computacional.

## 2.7 Intervalos reais

Em matemática, um *intervalo real* ou simplesmente *intervalo* geralmente significa o conjunto de todos os números reais  $\mathbb{R}$  compreendidos entre dois valores específicos. Há quatro variações principais deste conceito:

$$(a, b) = \{x : x \in \mathbb{R} \text{ e } a < x < b\} \text{ (intervalo aberto)}$$

$$[a, b] = \{x : x \in \mathbb{R} \text{ e } a \leq x \leq b\} \text{ (intervalo fechado)}$$

$$(a, b] = \{x : x \in \mathbb{R} \text{ e } a < x \leq b\} \text{ (intervalo fechado à direita)}$$

$$[a, b) = \{x : x \in \mathbb{R} \text{ e } a \leq x < b\} \text{ (intervalo fechado à esquerda)}$$

onde  $a$  e  $b$  são números reais, os *extremos*, *limites* ou *pontas* do intervalo. Os dois últimos tipos são ditos *semi-abertos* or *semi-fechados*.

**Exercício 2.28:** Adotando as definições acima, explique o significado das notações  $[a, b]$ ,  $(a, b)$ ,  $[a, b)$  e  $(a, b]$  (1) quando  $a = b$ , e (2) quando  $a > b$ .

Observe que a notação  $(a, b)$  é ambígua quando  $a$  e  $b$  são números: ela pode significar tanto um par ordenado, quanto um intervalo aberto. A interpretação correta depende inteiramente do contexto.

Alguns autores usam a notação  $]a, b[$  para intervalos abertos, e  $[a, b[$  ou  $]a, b]$  para semi-abertos. Esta escolha evita a ambiguidade acima, mas os colchetes “invertidos” podem gerar confusão em fórmulas, como por exemplo em  $[a, b[\cup]c, d]$ .

### 2.7.1 Intervalos ilimitados

Intervalos com as formas acima, com  $a$  e  $b$  reais, são ditos *limitados*. O termo *finito* também é usado, embora esses conjuntos em geral tenham infinitos elementos. São usados também intervalos *semi-infinitos* que são limitados em apenas um lado.

A notação para esses intervalos usa os símbolos  $-\infty$  e  $+\infty$  para indicar ausência de limite em cada lado. Estes valores *não* são elementos de  $\mathbb{R}$ , mas são considerados menor e maior, respectivamente, que todos os números reais. Assim, temos:

$$(-\infty, a) = \{ x : x \in \mathbb{R} \text{ e } x < a \},$$

$$(-\infty, a] = \{ x : x \in \mathbb{R} \text{ e } x \leq a \},$$

$$(a, +\infty) = \{ x : x \in \mathbb{R} \text{ e } a < x \},$$

$$[a, +\infty) = \{ x : x \in \mathbb{R} \text{ e } a \leq x \},$$

A notação  $(-\infty, +\infty)$  então seria a mesma coisa que  $\mathbb{R}$ . Observe que notações como  $[-\infty, a]$  ou  $[a, +\infty]$ , que implicariam que  $-\infty$  e/ou  $+\infty$  pertencem ao conjunto, não são intervalos reais.

**Exercício 2.29:** Descreva os conjuntos abaixo da maneira mais simples e explícita que puder:

- (a)  $[1, 3] \cap (2, 4)$ .
- (b)  $(-\infty, 2) \cap [-1, 0]$ .
- (c)  $(-\infty, 2) \cap [-1, 3]$ .
- (d)  $[0, 10] \cup [1, 11]$ .
- (e)  $(0, \infty) \cap (-\infty, 1)$ .
- (f)  $[-3, 0] \cup (0, 3]$ .
- (g)  $[-3, 0] \cup (0, 3]$ .
- (h)  $[-3, 0) \cup (0, 3]$ .
- (i)  $[-3, 0] \cap [0, 3]$ .
- (j)  $[-3, 0] \cap (0, 3]$ .
- (k)  $[-3, 0) \cap (0, 3]$ .
- (l)  $\overline{(0, 5]}$ .
- (m)  $\overline{(-\infty, 5]}$ .

**Exercício 2.30:** Suponha que  $a$ ,  $b$  e  $c$  são números reais tais que  $a < b$  e  $b < c$ . Quando é que as fórmulas abaixo produzem um único intervalo?

- (a)  $(a, b) \cup (b, c)$
- (b)  $[a, b] \cup [b, c]$
- (c)  $[a, b) \cup [b, c]$
- (d)  $[a, b) \cup (b, c]$

**Exercício 2.31:** Quais dos conjuntos de intervalos abaixo são partições do conjunto  $\mathbb{R}$  dos números reais?

- (a)  $\{[k, k + 1] : k \in \mathbb{Z}\}.$
- (b)  $\{(k, k + 1) : k \in \mathbb{Z}\}.$
- (c)  $\{(k, k + 1] : k \in \mathbb{Z}\}$
- (d)  $\{(-\infty, 0]\} \cup \{(k, k + 1] : k \in \mathbb{N}\}$

### 2.7.2 Caixas

O produto cartesiano  $[10, 20] \times [2, 4]$  é um retângulo no plano cartesiano  $\mathbb{R}^2$ , com lados paralelos aos eixos das coordenadas. Os pontos  $(10, 2)$  e  $(20, 4)$  são cantos opostos do mesmo. O produto cartesiano  $[10, 20] \times [2, 4] \times [60, 70]$  é um paralelepípedo no espaço cartesiano  $\mathbb{R}^3$ , com todas as arestas paralelas aos eixos; os pontos  $(10, 2, 60)$  e  $(20, 4, 70)$  são dois cantos opostos do mesmo.

Inspirado nestes exemplos, o nome *caixa* é as vezes usado para um subconjunto de  $\mathbb{R}^m$  que pode ser obtido pelo produto cartesiano de  $m$  intervalos  $I_1 \times I_2 \times \cdots \times I_m$ , especialmente quando os intervalos são finitos.

**Exercício 2.32:** Descreva precisamente os vários tipos de retângulo  $B = I_1 \times I_2$  considerando os quatro tipos principais de intervalo para  $I_1$  e  $I_2$ . Que cantos e que lados estão incluídos em  $B$ , em cada caso? Suponha que cada intervalo é limitado e não vazio, com extremos distintos.

**Exercício 2.33:** Seja  $B$  a caixa tridimensional  $[10, 20] \times [2, 4] \times [60, 70]$  no  $\mathbb{R}^3$ . Mostre que cada face, aresta, e canto da caixa é também uma caixa do  $\mathbb{R}^3$ .

## 2.8 Intervalos inteiros

Um conceito bastante usado em computação, e também em certos ramos da matemática, é o *intervalo de inteiros* ou *intervalo inteiro*, um conjunto de inteiros consecutivos. Não há uma notação padrão para estes intervalos, mas neste livro usaremos  $m .. n$ , onde  $m$  e  $n$  são inteiros, para significar o conjunto  $\{x : x \in \mathbb{Z} \text{ e } m \leq x \leq n\}$ . Por exemplo,

- $2 .. 5 = \{2, 3, 4, 5\}$ ;
- $-2 .. 2 = \{-2, -1, 0, +1, +2\}$ ;
- $7 .. 7 = \{7\}$ ,
- $5 .. 2 = \{\}$ .

Note que o intervalo inteiro  $m .. n$  é vazio se e somente se  $m > n$ , e tem apenas um elemento se  $m = n$ . Se  $m \leq n$ , os inteiros  $m$  e  $n$  são os *extremos*, *limites* ou *pontas* do intervalo.

**Exercício 2.34:** Qual é a cardinalidade  $|m .. n|$  de um intervalo inteiro  $m .. n$ ?

### 2.8.1 Intervalos inteiros ilimitados

Os intervalos definidos acima são ditos *limitados* ou *finitos*, pois tem um número finito de elementos. Em certos casos é útil ter o conceito de intervalo inteiro *semi-infinito* que são limitados em apenas um lado. Para esse fim, usam-se os símbolos  $-\infty$  e  $+\infty$  (que *não* são elementos de  $\mathbb{Z}$ ) para indicar ausência de limite em cada lado. Ou seja:

- $-\infty .. n = \{x : x \in \mathbb{Z} \text{ e } x \leq n\},$
- $m .. +\infty = \{x : x \in \mathbb{Z} \text{ e } m \leq x\},$
- $-\infty .. +\infty = \mathbb{Z}.$

Em álgebra linear, é praxe definir vetores do espaço  $\mathbb{R}^n$  de tal forma que os índices de suas coordenadas são o intervalo  $1 .. n$ . Essa também é a convenção da linguagem FORTRAN. Em muitas linguagens de programação, incluindo C e Python, o conjunto de índices válidos para um vetor de  $n$  elementos é o intervalo  $0 .. n - 1$ .

### 2.8.2 Grades inteiras

O produto cartesiano  $10 \dots 20 \times 3 \dots 7$  é um conjunto de pontos no plano cartesiano  $\mathbb{R}^2$ , que consiste de todos os pontos com coordenadas inteiras que estão dentro ou na borda da caixa  $[10, 20] \times [3, 7]$ . Esses pontos são os cruzamentos das linhas de uma grade com 11 linhas verticais e 5 linhas horizontais, igualmente espaçadas.

Analogamente, o produto cartesiano  $10 \dots 20 \times 3 \dots 7 \times 60 \dots 70$  consiste de todos os pontos de  $\mathbb{R}^3$  com coordenadas inteiras que estão dentro ou na superfície do paralelogramo  $[10, 20] \times [3, 7] \times [60, 70]$ .

Inspirado nestes exemplos, o nome *grade inteira* é às vezes usado para qualquer subconjunto de  $\mathbb{Z}^k$  que pode ser obtido pelo produto cartesiano de  $k$  intervalos inteiros  $m_1 \dots n_1 \times m_2 \dots n_2 \times \dots \times m_k \dots n_k$ , especialmente quando os intervalos são finitos.

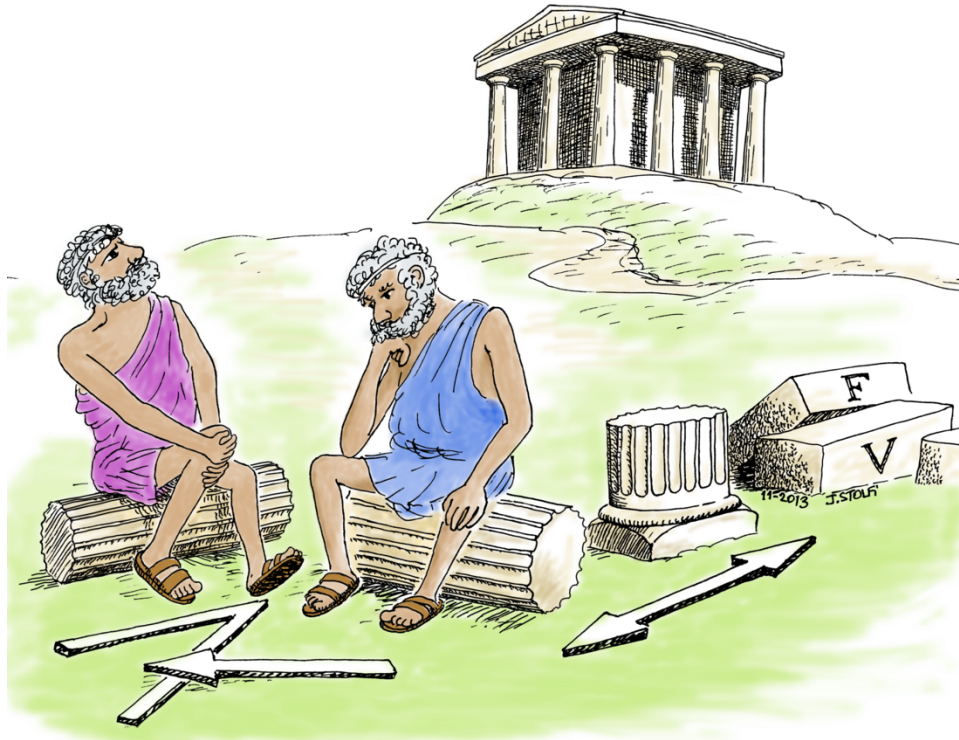
**Exercício 2.35:** Calcule as cardinalidades das grades inteiras  $|10 \dots 20 \times 3 \dots 7|$  e  $|10 \dots 20 \times 3 \dots 7 \times 60 \dots 70|$ .

Em álgebra linear, o conjunto dos índices dos elementos de uma matriz de  $m$  linhas e  $n$  colunas são a grade inteira  $1 \dots m \times 1 \dots n$ . Em computação, seriam  $0 \dots m - 1 \times 0 \dots n - 1$ .



# **Capítulo 3**

## **Lógica matemática**



## 3.1 Cálculo proposicional

### 3.1.1 Proposições e valores lógicos

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 quadrilionésimo algarismo decimal de  $\pi$  é 7.*

Observe que não é necessário que saibamos se a sentença é verdadeira ou falsa. Este fato pode depender de informações que não temos no momento (como no exemplo 3 acima), de eventos que ainda não aconteceram (como no exemplo 4), ou de cálculos que não temos recursos para realizar (como no exemplo 5).

Como exemplos de frases que *não* são proposições, podemos citar

- frases interrogativas, como “*O que é isto?*”,
- frases imperativas, como “*Leia com cuidado*”,
- certas sentenças auto referentes, como “*Esta frase é falsa*”.

**Exercício 3.1:** Quais das frases seguintes são proposições lógicas:

- (a)  $2 + 2 = 5$ .
- (b) O cientista perguntou: “Independência ou Marte?”
- (c) Não gosto de abacaxi.
- (d) Tomara que chova hoje.

Uma sentença declarativa que depende de variáveis pode ser considerada uma proposição em um contexto onde as variáveis tem valor determinado. Por exemplo, a sentença “ $x$  é menor que 3” isoladamente não é uma proposição. Porém, uma vez que o valor de  $x$  for definido, ela se torna uma proposição. Este ponto será tratado com mais detalhe na seção 3.6.

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

### 3.1.2 Conetivos lógicos e proposições compostas

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

1. [*Brasília é a capital do Brasil,*] e [*Montevidéu é a capital da Argentina*].
2. [*Brasília é a capital do Brasil,*] ou [*Montevidéu é a capital da Argentina*].
3. Se [*a taxa de juros cair amanhã*], então [*a inflação vai aumentar neste mês*].
4. Não [*haverá sessão da meia-noite hoje neste cinema*].

A palavra “conetivo” também pode ser escrita “conectivo”. Neste caso a letra “c” é geralmente pronunciada.

Uma proposição que não pode ser decomposta em proposições menores ligadas por conetivos lógicos é dita uma *proposição simples* ou *atômica*. Nos exemplos acima, os colchetes “[ ]” indicam as proposições simples.

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 conetivos. Assim, se sabemos que a proposição “*Brasília é a capital do Brasil*” é verdadeira, e “*Montevidéu é a capital da Argentina*” é falsa, podemos concluir que a proposição 1 acima é falsa, mas a proposição 2 é verdadeira.

### 3.1.3 Notação para cálculo proposicional

A linguagem natural é frequentemente ambígua, e os conectivos lógicos podem ter significados diferentes em sentenças diferentes. O *cálculo proposicional* é um formalismo algébrico que permite expressar uma proposições composta de maneira precisa e sem ambiguidades, e determinar seu valor lógico, dados os valores das proposições simples que a compõem. Nesse formalismo, cada proposição é representada por uma *fórmula lógica* composta de *variáveis lógicas* e *valores lógicos* combinados por *operadores lógicos*.

Uma variável lógica é uma letra que representa uma proposição, definida fora da fórmula. O *valor* de tal variável é o valor lógico dessa proposição, **V** (representando o valor lógico *verdadeiro*) ou **F** (*falso*). Neste livro, usaremos letras minúsculas ( $p, q, r, \dots$ ) para variáveis lógicas.

Um operador lógico é um símbolo que representa um conectivo lógico. Os operadores lógicos 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  $q$ ”.

*igualdade*:  $p \leftrightarrow q$ , significando “ $p$  se, e somente se,  $q$ ”.

*diferença*:  $p \oplus q$ , significando “ $p$  ou  $q$ , mas não ambos”.

Nas próximas seções, vamos explicar em detalhes estes operadores lógicos, e definir outros operadores menos usados.

### 3.1.4 Operador de conjunção

Se  $p, q$  são duas proposições, então “ $p$  e  $q$ ” também é uma proposição, chamada *conjunção* de  $p$  e  $q$ . Denotaremos essa proposição pela fórmula  $p \wedge q$ . Por definição, o valor lógico de  $p \wedge q$  é verdadeiro se  $p$  e  $q$  são ambos verdadeiros. Se qualquer uma das duas proposições for falsa, ou ambas forem falsas, o valor de  $p \wedge q$  é falso. Podemos resumir esta definição por uma tabela, a *tabela-verdade* do operador  $\wedge$ :

| $p$      | $q$      | $p \wedge q$ |
|----------|----------|--------------|
| <b>F</b> | <b>F</b> | <b>F</b>     |
| <b>F</b> | <b>V</b> | <b>F</b>     |
| <b>V</b> | <b>F</b> | <b>F</b>     |
| <b>V</b> | <b>V</b> | <b>V</b>     |

Em português e muitas outras línguas, frases semelhantes ligadas pelo conetivo de conjunção podem ter partes comuns fatoradas. Por exemplo, “José compra e vende casas” é na verdade uma conjunção de duas proposições atômicas, “[José compra casas]  $\wedge$  [José vende casas].”

Note que a palavra “e” em português tem vários sentidos, e nem todos correspondem à conjunção lógica. Por exemplo a frase “Maria gosta de arroz e feijão” não significa “Maria gosta de arroz e Maria gosta de feijão” (uma conjunção de duas proposições), mas sim “Maria gosta de arroz misturado com feijão” (uma proposição atômica).

Por outro lado, há outras maneiras de expressar a conjunção lógica de proposições em português; como, por exemplo. “tanto 17 quanto 31 são números primos”, “não só a estrada alagou, como a ponte ruiu,” “Batata é fruta, repolho é mamífero, sal é doce: é tudo verdade.”

### 3.1.5 Operador de disjunção

Se  $p, q$  são duas proposições, então “ $p$  ou  $q$ ” também é uma proposição, chamada de *disjunção* de  $p$  e  $q$ . Denotaremos essa proposição pela fórmula  $p \vee q$ . Por definição, o valor lógico de  $p \vee q$  é verdadeiro se pelo menos uma das duas proposições for verdadeira. Se ambas forem falsas, o valor de  $p \vee q$  é falso. A tabela-verdade do operador  $\vee$  é

| $p$ | $q$ | $p \vee q$ |
|-----|-----|------------|
| F   | F   | F          |
| F   | V   | V          |
| V   | F   | V          |
| V   | V   | V          |

Assim como a conjunção, a disjunção de proposições semelhantes pode ter as partes comuns fatoradas. Por exemplo, a “O cliente tem celular ou laptop na valise” é uma disjunção de duas proposições atômicas, “[O cliente tem celular na valise]  $\vee$  [O cliente tem laptop na valise]”.

Este conetivo é também chamado de “ou inclusivo”, pois a frase toda é verdadeira mesmo quando ambas as componentes são verdadeiras. A frase do exemplo acima é verdadeira se o cliente tem, na valise, apenas celular, apenas laptop, ou celular e laptop.

**Exercício 3.2:** Decomponha a seguinte frase em proposições elementares ligadas pelos conetivos ‘ $\vee$ ’ e ‘ $\wedge$ ’: “tendo chovido, a rua e o parque estavam molhados ou mesmo alagados” Delimite as proposições atômicas com colchetes ‘[ ]’.

### 3.1.6 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  $\neg p$ . A tabela-verdade desse operador é:

| $p$      | $\neg p$ |
|----------|----------|
| <b>F</b> | <b>V</b> |
| <b>V</b> | <b>F</b> |

Em português, a negação pode ser expressa de várias formas, por exemplo acrescentando a palavra “não” antes do verbo ou dizendo que “não é verdade que ...”. Podemos também dizer “casa é de qualquer cor menos branca” para significar a negação “ $\neg$ [A casa é branca].”

Em português (e algumas outras línguas) a gramática exige o uso da chamada *dupla negação* para expressar o que logicamente é uma negação simples. Por exemplo, a frase “não tenho nenhum lápis” significa “ $\neg$ [tenho lápis]”, em vez de “ $\neg$ [tenho nenhum lápis]”.

O conetivo de negação pode também interagir com outros conetivos de maneira não óbvia. Por exemplo, a proposição “[José não veio]  $\wedge$  [João não veio]” seria normalmente expressa como “nem José nem João vieram”. Para expressar “[José não cantou]  $\vee$  [José não dançou]” poderíamos dizer “José não cantou e dançou” (com ênfase no “e”). A proposição “[José não cantou]  $\wedge$  [João cantou]” seria “José não cantou, mas João sim,” enquanto que “[José cantou]  $\wedge$  [João não cantou]” seria “José cantou, mas João não.”

**Exercício 3.3:** Escreva fórmulas lógicas equivalentes às afirmações abaixo, identificando as proposições atômicas contidas nas mesmas e associando-as às variáveis lógicas  $p$ ,  $q$ ,  $r$  e  $s$ :

- (a) Nem encontrei José ou João, nem sei onde foi a festa, ou quando.
- (b) Encontrei José mas não João, e sei onde foi a festa mas não quando.
- (c) Encontrei tanto José quanto João, mas, embora saiba quando foi a festa, não sei onde.
- (d) José ou João? Encontrei ambos; além disso, sei quando foi a festa, bem como onde.

Em fórmulas com mais de um operador, pode ser necessário usar parênteses para indicar a quais são as sub-fórmulas combinadas por cada operador. Por exemplo, na fórmula  $(p \wedge q) \vee r$ , o operador ‘ $\vee$ ’ combina o valor de  $p \wedge q$  com o de  $r$ ; enquanto que em  $p \wedge (q \vee r)$  ele combina  $q$  e  $r$  apenas.

**Exercício 3.4:** Seja  $p$  a proposição “17 é um numero primo”,  $q$  a proposição “ $2+2 = 5$ ”, e  $r$  a proposição “Brasília é a capital do Brasil”. Determine o valor lógico das seguintes fórmulas:

- (a)  $\neg(\neg p \vee q) \vee (p \wedge \neg r)$ .
- (b)  $\neg(\neg p \wedge q) \vee (p \wedge \neg r)$ .
- (c)  $(p \wedge r) \vee (\neg r \wedge (p \vee q))$ .

**Exercício 3.5:** Encontre atribuições de valores verdades para as variáveis  $p$ ,  $q$ , e  $r$  que tornam a fórmula  $((\neg p) \wedge (q \vee p)) \wedge ((\neg p) \vee (r \wedge p))$  (a) verdadeira, (b) falsa.

**Exercício 3.6:** Sejam  $p$  e  $q$  as proposições “a eleição foi decidida” e “os votos foram contados”, respectivamente. Expresse cada uma das fórmulas lógicas a seguir como uma sentença em português.

- (a)  $\neg p \wedge q$
- (b)  $\neg q \rightarrow \neg p$
- (c)  $\neg q \vee (\neg p \wedge q)$

**Exercício 3.7:** Um grupo de pessoas está tentando planejar um passeio turístico. Porém:

- Alice só vai se Bento também for;
- Bento não vai se Carlos e Eunice forem;
- Somente Carlos, Dudu e Eunice conhecem o lugar, então um deles tem que ir;
- Dudu só vai se ou Carlos, ou Alice ou ambos forem;
- Carlos não pode ir se nem Alice nem Bento forem.

É possível realizar esse passeio? Em caso afirmativo, quais composições são viáveis?

### 3.1.7 Operador de implicação

O operador *condicional* ou *implicação*, que denotaremos por ' $\rightarrow$ ', é o conetivo lógico em frases da forma “se  $p$  então  $q$ ”. O valor lógico de  $p \rightarrow q$  é falso apenas se  $p$  for verdadeiro e  $q$  for falso. Nos demais casos, o valor de  $p \rightarrow q$  é verdadeiro. A tabela-verdade desse conetivo é portanto:

| $p$      | $q$      | $p \rightarrow q$ |
|----------|----------|-------------------|
| <b>F</b> | <b>F</b> | <b>V</b>          |
| <b>F</b> | <b>V</b> | <b>V</b>          |
| <b>V</b> | <b>F</b> | <b>F</b>          |
| <b>V</b> | <b>V</b> | <b>V</b>          |

Por exemplo, a afirmação “se José for para casa, ele vai perder a reunião” poderia ser escrita “[José vai para casa]  $\rightarrow$  [José vai perder a reunião].” A afirmação é falsa caso José vá para casa mas mesmo assim compareça à reunião. Caso José vá para casa e perca a reunião, a afirmação toda será obviamente verdadeira. Porém, caso José *não* vá para casa, a afirmação também será verdadeira, quer ele compareça ou não à reunião. Pois neste caso não se pode dizer que a afirmação seja falsa; portanto, ela deve ser verdadeira.

Mais geralmente, a proposição  $p \rightarrow q$  é sempre *verdadeira* caso  $p$  seja *falsa*, qualquer que seja a proposição  $q$ . Esta interpretação pode não ser intuitiva, mas é a que faz sentido em raciocínios lógicos envolvendo afirmações condicionais.

Note que, em lógica, este conetivo não pressupõe uma relação causal entre  $p$  e  $q$ . Por exemplo a sentença “se 2 é um inteiro par então Brasília é a capital do Brasil” é verdadeira apesar de não

haver nenhuma relação conhecida entre os dois fatos.

Alguns autores e livros denotam este operador por  $\Rightarrow$ ; porém, é melhor reservar este símbolo para o conceito de implicação lógica entre fórmulas. (seção 3.2.6).

Muitos teoremas em matemática são enunciados 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.

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  $p$ .

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

- $p$  é condição suficiente para  $q$ .
- $p$  somente se  $q$ .
- Uma condição suficiente para  $q$  é  $p$ .

- $p$  é uma condição mais forte que  $q$ .

**Exercício 3.8:** Suponha que  $p$ ,  $\neg q$  e  $r$  são proposições verdadeiras. Determine quais das afirmações são verdadeiras:

- (a)  $p \rightarrow q$ .
- (b)  $q \rightarrow p$ .
- (c)  $p \rightarrow (q \vee r)$ .
- (d)  $(p \vee q) \rightarrow p$ .
- (e)  $(p \wedge q) \rightarrow q$ .

**Exercício 3.9:** Em cada frase abaixo, determine as proposições atômicas, atribua variáveis lógicas às mesmas, e escreva a frase em notação lógica, usando o operador ' $\rightarrow$ ' sempre que possível.

- (a) O teatro fecha sempre que chove.
- (b) Para chegar a tempo ele precisaria vir de trem ou de avião.
- (c) Supondo que Marcos não vem, Maria só vem para a festa se João vier.
- (d) Se saber cantar é necessário para progredir, então quem é chefe pode cantar o hino.
- (e) Não é possível que João faz isso mas não sabe trocar a lâmpada quando estiver queimada.

A *contrapositiva* de  $p \rightarrow q$  é a implicação  $(\neg q) \rightarrow (\neg p)$ . Pode-se verificar que ela tem sempre o mesmo valor lógico que a implicação  $p \rightarrow q$ , quaisquer que sejam os valores lógicos de  $p$  e de  $q$  (vide exercício 3.10).

**Exercício 3.10:** Demonstre, pelas tabelas-verdade, que as fórmulas  $p \rightarrow q$  e  $(\neg q) \rightarrow (\neg p)$  tem sempre o mesmo valor lógico, 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  $q$ .

A *recíproca* da implicação  $p \rightarrow q$  é a implicação  $q \rightarrow p$ ; e a *inversa* é  $(\neg p) \rightarrow (\neg q)$ . Verifica-se que elas são distintas de  $p \rightarrow q$  (e portanto da contrapositiva), mas são a mesma operação; ou seja, elas tem o mesmo valor lógico, para quaisquer valores de  $p$  e  $q$ . Vide exercício 3.11.

**Exercício 3.11:** Demonstre, pelas tabelas-verdade, que a recíproca e a inversa de  $p \rightarrow q$  tem o mesmo valor lógico, para quaisquer valores de  $p$  e  $q$ . Compare com  $p \rightarrow q$ .

**Exercício 3.12:** Determine fórmulas equivalentes

- (a) à contrapositiva de  $\neg p \rightarrow q$ .
- (b) à recíproca de  $\neg q \rightarrow p$ .
- (c) à inversa da recíproca de  $q \rightarrow \neg p$ .
- (d) à negação de  $p \rightarrow \neg q$ .
- (e) à recíproca de  $\neg p \vee q$ .

### 3.1.8 Operador de igualdade lógica

O operador de *igualdade lógica*, denotado pelo símbolo ' $\leftrightarrow$ ', é definido pela tabela-verdade

| $p$ | $q$ | $p \leftrightarrow q$ |
|-----|-----|-----------------------|
| F   | F   | V                     |
| F   | V   | F                     |
| V   | F   | F                     |
| V   | V   | V                     |

Ou seja, a fórmula  $p \leftrightarrow q$  é verdade se  $p$  e  $q$  tem o mesmo valor lógico (ambos são verdade, ou ambos são falsos) e é falsa se  $p$  e  $q$  tem valores diferentes (um é verdade e o outro falso).

**Exemplo 3.1:** A proposição “a encomenda foi enviada se, e somente se, o cheque tinha fundo” pode ser escrita “[a encomenda foi enviada]  $\leftrightarrow$  [o cheque tinha fundo].” Esta afirmação é verdadeira se encomenda foi enviada e o cheque tinha fundo, ou se a encomenda não foi enviada e o cheque não tinha fundo. Essa afirmação é falsa nos outros casos: se a encomenda foi enviada mas o cheque não tinha fundo, ou a encomenda não foi enviada mas o cheque tinha fundo.

Como veremos mais adiante, a fórmula  $p \leftrightarrow q$  significa o mesmo que a fórmula  $(p \rightarrow q) \wedge (q \rightarrow p)$ , ou seja “ $p$  é verdade se, e somente se,  $q$  é verdade”. Por esta razão, o operador ' $\leftrightarrow$ ' é também chamado *bicondicional* ou *implicação dupla*.

Alguns autores usam a abreviação “ $p$  sse  $q$ ” (com dois “s”) em textos para significar “ $p$  se e somente se  $q$ ”. Porém, essa abreviação precisa ser lida “ $p$  se e somente se  $q$ ”, por extenso, para não confundir com “ $p$  se  $q$ ” (que significa  $p \rightarrow q$ ).

**Exercício 3.13:** Suponha que  $p = r = \mathbf{V}$  e  $q = \mathbf{F}$ . Verifique quais destas fórmulas são verdadeiras:

- (a)  $p \leftrightarrow q$ .
- (b)  $p \leftrightarrow r$ .
- (c)  $(p \leftrightarrow q) \leftrightarrow p$ .
- (d)  $(\neg(p \leftrightarrow r)) \leftrightarrow q$ .

Em matemática, o conetivo lógico “se e somente se” pode ser expresso de várias outras maneiras; como, por exemplo:

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

Alguns autores chamam este operador de *equivalência* e usam o símbolo “ $\Leftrightarrow$ ” ou “ $\equiv$ ” em vez de “ $\leftrightarrow$ ”. Porém, é melhor reservar o termo “equivalência” e esses símbolos para o conceito de equivalência lógica entre fórmulas (seção 3.2.3).

O operador de igualdade lógica “ $\leftrightarrow$ ” também pode ser indicado pelo símbolo geral de igualdade, “ $=$ ”. Este fato é usado em muitas linguagens de programação que não tem uma notação específica para este operador lógico.

### 3.1.9 Operador de diferença

O operador de diferença lógica, ou apenas *diferença*, denotado por ' $\oplus$ ', é definido por esta tabela-verdade:

| $p$ | $q$ | $p \oplus q$ |
|-----|-----|--------------|
| F   | F   | F            |
| F   | V   | V            |
| V   | F   | V            |
| V   | V   | F            |

Ou seja,  $p \oplus q$  é verdade se  $p$  é verdade ou  $q$  é verdade, mas não se ambos são verdade. Por esta razão, este operador é também chamado de *disjunção exclusiva*, enquanto que  $\vee$  seria a *disjunção inclusiva*.

É importante observar que, em português, o conetivo “ou” ‘as vezes significa ' $\oplus$ ', em vez de ' $\vee$ '. Por exemplo, na frase “o original foi enviado pelo correio ou pelo malote,” entende-se “[o original foi enviado pelo correio]  $\oplus$  [o original foi enviado pelo malote]”, pois o documento não pode ter sido enviado pelos dois meios. Por outro lado, na frase “a bateria está descarregada ou o tanque está vazio” o “ou” deve ser entendido como inclusivo ( $\vee$ ), pois pode ser que as duas proposições atômicas sejam verdadeiras. A interpretação correta geralmente depende do contexto, e em alguns casos pode ser impossível determinar qual dos dois sentidos é o que o autor da frase pretendia.

**Exercício 3.14:** Suponha que exatamente três das cinco proposições  $p$ ,  $q$ ,  $r$ ,  $s$  e  $t$  são verdadeiras. Qual o valor de  $((p \oplus q) \oplus r) \oplus s) \oplus t$ ?

### 3.1.10 Tabela-verdade de uma fórmula

O conceito de tabela-verdade aplica-se a qualquer proposição com uma ou mais proposições atômicas, ou a qualquer fórmula com uma ou mais variáveis lógicas. Se a fórmula tem  $n$  variáveis distintas, a tabela-verdade tem  $2^n$  linhas, uma para cada combinação de valores dessas variáveis.

Por exemplo, a fórmula  $((p \wedge q) \vee r) \vee (\neg q)$  tem a seguinte tabela da verdade:

| $p$ | $q$ | $r$ | $p \wedge q$ | $(p \wedge q) \vee r$ | $\neg q$ | $((p \wedge q) \vee r) \wedge (\neg q)$ |
|-----|-----|-----|--------------|-----------------------|----------|-----------------------------------------|
| F   | F   | F   | F            | F                     | V        | F                                       |
| F   | F   | V   | F            | V                     | V        | V                                       |
| F   | V   | F   | F            | F                     | F        | F                                       |
| F   | V   | V   | F            | V                     | F        | F                                       |
| V   | F   | F   | F            | F                     | V        | F                                       |
| V   | F   | V   | F            | V                     | V        | V                                       |
| V   | V   | F   | V            | V                     | F        | F                                       |
| V   | V   | V   | V            | V                     | F        | F                                       |

**Exercício 3.15:** Construa a tabela da verdade das seguintes fórmulas lógicas:

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

(b)  $((p \rightarrow q) \oplus (q \leftrightarrow r)) \wedge (p \oplus r)$

**Exercício 3.16:** Um conetivo muito importante para projeto de circuitos lógicos é o operador *não-e* ou (*nand*), que denotaremos por  $\overline{\wedge}$ , definido por  $p \overline{\wedge} q = \neg(p \wedge q)$ . De maneira análoga temos o operador *não-ou* ou (*nor*), denotado por  $\overline{\vee}$ , e definido por  $p \overline{\vee} q = \neg(p \vee q)$ . Construa as tabelas-verdade dos operadores  $\overline{\wedge}$  e  $\overline{\vee}$ .

**Exercício 3.17:** Construa a tabela-verdade de cada uma das fórmulas abaixo:

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

**Exercício 3.18:** Uma proposição composta é *satisfactível* ou *possível* se existe uma atribuição de valores verdades para as variáveis da proposição que a torna verdadeira. Verifique quais das fórmulas abaixo são viáveis.

- (a)  $(p \oplus q) \wedge ((p \leftrightarrow r) \wedge (q \leftrightarrow r))$ .
- (b)  $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$ .
- (c)  $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$ .

## 3.2 Manipulação de fórmulas lógicas

Nesta seção estudaremos transformações de fórmulas lógicas que não mudam seu valor lógico, independentemente do significado e valores lógicos das variáveis que ocorrem nelas.

### 3.2.1 Tautologias

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

A tautologia mais simples é **V**. Mais geralmente, uma fórmula lógica é uma tautologia se, e somente se, a coluna de resultado de sua tabela-verdade contém somente valores lógicos verdadeiros (**V**). Por exemplo, a fórmula  $p \vee (q \vee \neg p)$  tem a seguinte tabela-verdade:

| $p$      | $q$      | $\neg p$ | $q \vee \neg p$ | $p \vee (q \vee \neg p)$ |
|----------|----------|----------|-----------------|--------------------------|
| <b>F</b> | <b>F</b> | <b>V</b> | <b>V</b>        | <b>V</b>                 |
| <b>F</b> | <b>V</b> | <b>V</b> | <b>V</b>        | <b>V</b>                 |
| <b>V</b> | <b>F</b> | <b>F</b> | <b>F</b>        | <b>V</b>                 |
| <b>V</b> | <b>V</b> | <b>F</b> | <b>V</b>        | <b>V</b>                 |

Podemos concluir então que a fórmula  $p \vee (q \vee \neg p)$  é uma tautologia. Observe que esse fato independe dos significados das variáveis  $p$  e  $q$ .

### 3.2.2 Contradições

Uma *contradição* é uma proposição composta que é sempre falsa, quaisquer que sejam os valores lógicos das suas proposições atômicas.

A contradição mais simples é **F**. Mais geralmente, uma fórmula lógica é uma contradição se, e somente se, sua tabela-verdade contém somente **F** na sua coluna de resultado. Por exemplo, a fórmula  $(p \wedge q) \wedge \neg q$  é uma contradição.

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

**Exercício 3.19:** Construa as tabelas-verdade das fórmulas 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)  $((p \oplus q) \oplus (q \oplus p))$ .
- (h)  $((p \rightarrow q) \leftrightarrow r) \leftrightarrow (p \rightarrow (q \leftrightarrow r))$ .
- (i)  $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

### 3.2.3 Equivalência lógica de fórmulas

Duas fórmulas  $\mathcal{F}$  e  $\mathcal{G}$  do cálculo proposicional são ditas *equivalentes* se elas têm valores lógicos iguais, quaisquer que sejam os valores lógicos das variáveis que ocorrem nas mesmas. Em outras palavras,  $\mathcal{F}$  e  $\mathcal{G}$  são equivalentes se e somente se a fórmula  $(\mathcal{F}) \leftrightarrow (\mathcal{G})$  é uma tautologia.

Por exemplo, seja  $\mathcal{F}$  a fórmula  $p \wedge (\neg q)$ , e seja  $\mathcal{G}$  a fórmula  $\neg((\neg p) \vee q)$ . Podemos verificar que são equivalentes, calculando as tabelas-verdade de  $\mathcal{F}$ ,  $\mathcal{G}$ , e  $(\mathcal{F}) \leftrightarrow (\mathcal{G})$ :

| $p$      | $q$      | $\neg q$ | $\mathcal{F}$<br>$p \wedge (\neg q)$ | $\neg p$ | $(\neg p) \vee q$ | $\mathcal{G}$<br>$\neg((\neg p) \vee q)$ | $(\mathcal{F}) \leftrightarrow (\mathcal{G})$<br>$(p \wedge (\neg q)) \leftrightarrow \neg((\neg p) \vee q)$ |
|----------|----------|----------|--------------------------------------|----------|-------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>F</b> | <b>F</b> | <b>V</b> | <b>F</b>                             | <b>V</b> | <b>V</b>          | <b>F</b>                                 | <b>V</b>                                                                                                     |
| <b>F</b> | <b>V</b> | <b>F</b> | <b>F</b>                             | <b>V</b> | <b>V</b>          | <b>F</b>                                 | <b>V</b>                                                                                                     |
| <b>V</b> | <b>F</b> | <b>V</b> | <b>V</b>                             | <b>F</b> | <b>F</b>          | <b>V</b>                                 | <b>V</b>                                                                                                     |
| <b>V</b> | <b>V</b> | <b>F</b> | <b>F</b>                             | <b>F</b> | <b>V</b>          | <b>F</b>                                 | <b>V</b>                                                                                                     |

Note que as colunas “ $\mathcal{F}$ ” e “ $\mathcal{G}$ ” tem os mesmos valores em cada linha.

Uma vez estabelecido que a fórmula  $\mathcal{F}$  é logicamente equivalente a  $\mathcal{G}$ , Sempre que determinarmos que  $\mathcal{F}$  é verdadeira, podemos concluir imediatamente que  $\mathcal{G}$  também é verdadeira, e vice-versa; e sempre que determinarmos que  $\mathcal{F}$  é falsa, podemos concluir que  $\mathcal{G}$  é falsa, e vice-versa.

Assim como a propriedade de ser tautologia ou de ser contradição, a equivalência lógica de duas proposições não depende do significado das proposições atômicas que ocorrem nela.

A notação “ $\mathcal{F} \Leftrightarrow \mathcal{G}$ ” ou “ $\mathcal{F} \equiv \mathcal{G}$ ” é usada para significar “as fórmulas  $\mathcal{F}$  e  $\mathcal{G}$  são equivalentes”. Note que estes símbolos *não* são operadores lógicos. Em particular, não devem ser confundidos com o operador lógico “ $\leftrightarrow$ ”.

- A expressão “ $\mathcal{F} \leftrightarrow \mathcal{G}$ ” é uma proposição, que só tem um valor lógico se as variáveis que ocorrem nessas fórmulas estão definidas, e é verdade se e somente se  $\mathcal{F}$  e  $\mathcal{G}$  tem o mesmo valor lógico *para esses valores dessas variáveis*.
- A expressão “ $\mathcal{F} \Leftrightarrow \mathcal{G}$ ” supõe que as variáveis *não* estão definidas, e afirma que as fórmulas  $\mathcal{F}$  e  $\mathcal{G}$  tem os mesmos valores lógicos *quaisquer que sejam os valores dessas variáveis*.

**Exercício 3.20:** Verifique quais das afirmações abaixo são corretas

- (a)  $(\neg p \wedge (p \vee q)) \Leftrightarrow q$ .
- (b)  $((p \rightarrow q) \rightarrow r) \Leftrightarrow (p \rightarrow (q \rightarrow r))$ .
- (c)  $p \rightarrow (q \wedge r) \Leftrightarrow (p \rightarrow q) \wedge (p \rightarrow r)$ .
- (d)  $(p \vee q) \rightarrow r \Leftrightarrow (p \rightarrow r) \wedge (q \rightarrow r)$ .

Podemos dizer também que uma tautologia é uma proposição logicamente equivalente a **V**; e uma contradição é uma proposição logicamente equivalente a **F**.

### 3.2.4 Equivalências lógicas importantes

A seguir listaremos algumas equivalências lógicas importantes. O leitor pode se convencer da veracidade delas construindo as respectivas tabelas-verdade.

- *Leis de elemento identidade:*

$$p \wedge \mathbf{V} \text{ equivale a } p$$

$$p \vee \mathbf{F} \text{ equivale a } p$$

$$p \leftrightarrow \mathbf{V} \text{ equivale a } p$$

$$p \oplus \mathbf{F} \text{ equivale a } p$$

- *Lei da negação dupla:*

$$\neg(\neg p) \text{ equivale a } p$$

- *Leis da idempotência:*

$$p \wedge p \text{ equivale a } p$$

$$p \vee p \text{ equivale a } p$$

- *Leis de dominação:*

$$p \vee \mathbf{V} \text{ equivale a } \mathbf{V}$$

$$p \wedge \mathbf{F} \text{ equivale a } \mathbf{F}$$

- *Leis da comutatividade:*

$$p \vee q \text{ equivale a } q \vee p$$

$$p \wedge q \text{ equivale a } q \wedge p$$

$$p \leftrightarrow q \text{ equivale a } q \leftrightarrow p$$

$$p \oplus q \text{ equivale a } q \oplus p$$

- *Leis da associatividade:*

$$(p \vee q) \vee r \text{ equivale a } p \vee (q \vee r)$$

$$(p \wedge q) \wedge r \text{ equivale a } p \wedge (q \wedge r)$$

$$(p \leftrightarrow q) \leftrightarrow r \text{ equivale a } p \leftrightarrow (q \leftrightarrow r)$$

$$(p \oplus q) \oplus r \text{ equivale a } p \oplus (q \oplus r)$$

- *Leis da distributividade:*

$$p \vee (q \wedge r) \text{ equivale a } (p \vee q) \wedge (p \vee r)$$

$$p \wedge (q \vee r) \text{ equivale a } (p \wedge q) \vee (p \wedge r)$$

$$p \wedge (q \oplus r) \text{ equivale a } (p \wedge q) \oplus (p \wedge r)$$

- *Leis de De Morgan:*

$$\neg(p \wedge q) \text{ equivale a } \neg p \vee \neg q$$

$$\neg(p \vee q) \text{ equivale a } \neg p \wedge \neg q$$

- *Leis de absorção:*

$(p \vee (p \wedge q))$  equivale a  $p$ .

$(p \wedge (p \vee q))$  equivale a  $p$ .

- *Leis do operador implicação*

$p \rightarrow q$  equivale a  $\neg p \vee q$

$p \rightarrow q$  equivale a  $(\neg q) \rightarrow (\neg p)$  (*lei da contrapositiva*)

$\neg(p \rightarrow q)$  equivale a  $p \wedge \neg q$

$\mathbf{F} \rightarrow p$  equivale a  $\mathbf{V}$

$\mathbf{V} \rightarrow p$  equivale a  $p$

$p \rightarrow \mathbf{F}$  equivale a  $\neg p$  (*lei da redução ao absurdo*)

$p \rightarrow \mathbf{V}$  equivale a  $\mathbf{V}$

$p \rightarrow q$  equivale a  $(p \wedge \neg q) \rightarrow \mathbf{F}$

- *Leis do operador igualdade lógica*

$p \leftrightarrow q$  equivale a  $(p \rightarrow q) \wedge (q \rightarrow p)$

$p \leftrightarrow q$  equivale a  $\neg(p \oplus q)$

**Exercício 3.21:** Verifique cada uma das equivalências acima, construindo a tabela-verdade para as duas fórmulas.

**Exercício 3.22:** Quais das fórmulas abaixo são logicamente equivalentes?

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

**Exercício 3.23:** Use as leis de equivalência lógica vistas acima para encontrar fórmulas mais simples que sejam logicamente equivalentes às seguintes fórmulas:

- (a)  $\neg(\neg p \vee q) \vee (p \wedge \neg r)$ .
- (b)  $\neg(\neg p \wedge q) \vee (p \wedge \neg r)$ .
- (c)  $(p \wedge r) \vee (\neg r \wedge (p \vee q))$ .

**Exercício 3.24:** Encontre uma fórmula usando apenas os conectivos  $\wedge$  e  $\neg$  que seja logicamente equivalente a  $(r \wedge \neg p) \vee (q \wedge \neg r)$ . Justifique sua resposta com a tabela-verdade.

**Exercício 3.25:** Encontre uma fórmula usando apenas os conectivos  $\rightarrow$  e  $\neg$  que seja logicamente equivalente a  $p \wedge q$ . Justifique sua resposta com a tabela-verdade.

**Exercício 3.26:** Encontre uma fórmula usando os conectivos  $\rightarrow$  e  $\oplus$  que seja logicamente equivalente a  $p \vee q$ . Justifique sua resposta com a tabela-verdade.

**Exercício 3.27:** Considere a tabela-verdade abaixo de uma certa proposição composta  $\mathcal{F}$  formada a partir de proposições elementares  $x$ ,  $y$  e  $z$ :

| $x$ | $y$ | $z$ | $\mathcal{F}$ |
|-----|-----|-----|---------------|
| F   | F   | F   | F             |
| F   | F   | V   | F             |
| F   | V   | F   | F             |
| F   | V   | V   | F             |
| V   | F   | F   | V             |
| V   | F   | V   | V             |
| V   | V   | F   | F             |
| V   | V   | V   | F             |

Encontre uma fórmula lógica equivalente a  $\mathcal{F}$ , usando as variáveis  $x$ ,  $y$  e  $z$ , e:

- (a) apenas os operadores  $\wedge$ ,  $\vee$  e  $\neg$
- (b) apenas os operadores  $\neg$  e  $\rightarrow$

### 3.2.5 Substituição de variáveis em equivalências

Uma regra importante do cálculo proposicional é que a equivalência de duas fórmulas lógicas é preservada se as variáveis que ocorrem nas mesmas forem substituídas por outras fórmulas de maneira consistente.

Mas precisamente, sejam  $\mathcal{F}$  e  $\mathcal{G}$  duas fórmulas logicamente equivalentes que dependem de uma variável  $p$ . As fórmulas  $\mathcal{F}'$  e  $\mathcal{G}'$  obtidas de  $\mathcal{F}$  e  $\mathcal{G}$  substituindo todas as ocorrências de  $p$  por uma mesma fórmula arbitrária ( $\mathcal{E}$ ) também serão equivalentes, qualquer que seja  $\mathcal{E}$ .

**Exemplo 3.2:** Seja  $\mathcal{F}$  a fórmula  $p \rightarrow q$ , e  $\mathcal{G}$  a fórmula  $(\neg p) \vee q$ . Sejam  $\mathcal{F}'$  e  $\mathcal{G}'$  os resultados de substituir todas as ocorrências de  $p$  pela fórmula  $r \oplus s$ , ou seja  $(r \oplus s) \rightarrow q$  e  $(\neg(r \oplus s)) \vee q$ . Como  $\mathcal{F}$  e  $\mathcal{G}$  são equivalentes, podemos concluir que  $\mathcal{F}'$  e  $\mathcal{G}'$  também são equivalentes.

Outra regra semelhante é que a substituição de uma variável numa fórmula por duas fórmulas equivalentes também gera duas fórmulas equivalentes. Mais precisamente, suponha que  $\mathcal{F}$  é uma fórmula qualquer na qual a variável  $p$  aparece, e sejam  $\mathcal{E}'$  e  $\mathcal{E}''$  duas fórmulas equivalentes. Sejam  $\mathcal{F}'$  e  $\mathcal{F}''$  duas fórmulas que resultam de substituir  $p$  por  $\mathcal{E}'$  e  $p$  por  $\mathcal{E}''$ , respectivamente. então  $\mathcal{F}'$  e  $\mathcal{F}''$  serão euivalentes.

**Exemplo 3.3:** Seja  $\mathcal{F}$  a fórmula  $p \rightarrow q$ ,  $\mathcal{E}'$  a fórmula  $r \oplus (\neg s)$ , e  $\mathcal{E}''$  a fórmula  $(\neg r) \oplus s$ . Sejam  $\mathcal{F}'$  e  $\mathcal{F}''$  os resultados de substituir  $p$  por estas duas fórmulas; ou seja,  $(r \oplus (\neg s)) \rightarrow q$  e  $((\neg r) \oplus s) \rightarrow q$ . Como  $\mathcal{E}'$  e  $\mathcal{E}''$  são equivalentes, podemos concluir que  $\mathcal{F}'$  e  $\mathcal{F}''$  também são equivalentes.

### 3.2.6 Dominância de fórmulas lógicas

Sejam  $\mathcal{F}$  e  $\mathcal{G}$  duas fórmulas lógicas que dependem de uma certa coleção de variáveis lógicas. Dizemos que  $\mathcal{F}$  *domina*  $\mathcal{G}$  se a fórmula  $(\mathcal{F}) \rightarrow (\mathcal{G})$  é uma tautologia. Ou seja, se, 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.

Por exemplo, seja  $\mathcal{F}$  a fórmula  $p \wedge q$ , e  $\mathcal{G}$  a fórmula  $p \vee q$ . As tabelas-verdade são

|          |          | $\mathcal{F}$ | $\mathcal{G}$ | $(\mathcal{F}) \rightarrow (\mathcal{G})$ |
|----------|----------|---------------|---------------|-------------------------------------------|
| $p$      | $q$      | $p \wedge q$  | $p \vee q$    | $(p \wedge q) \rightarrow (p \vee q)$     |
| <b>F</b> | <b>F</b> | <b>F</b>      | <b>F</b>      | <b>V</b>                                  |
| <b>F</b> | <b>V</b> | <b>F</b>      | <b>V</b>      | <b>V</b>                                  |
| <b>V</b> | <b>F</b> | <b>F</b>      | <b>V</b>      | <b>V</b>                                  |
| <b>V</b> | <b>V</b> | <b>V</b>      | <b>V</b>      | <b>V</b>                                  |

Concluimos que  $\mathcal{F}$  domina  $\mathcal{G}$ , embora as duas fórmulas *não* sejam equivalentes.

Essa afirmação é denotada  $\mathcal{F} \Rightarrow \mathcal{G}$ , e pode ser lida também “ $\mathcal{G}$  é uma *consequência lógica* de  $\mathcal{F}$ ”. Nesse caso, sempre que conseguirmos provar, de alguma forma, que  $\mathcal{F}$  é verdadeira para alguma combinação de valores de variáveis, podemos concluir imediatamente que  $\mathcal{G}$  é verdadeira para essa combinação (mas não vice-versa). Pela contrapositiva, se determinarmos que  $\mathcal{G}$  é falsa, podemos concluir imediatamente que  $\mathcal{F}$  também é falsa (mas não vice-versa).

**Exemplo 3.4:** Pode-se verificar que a fórmula “ $(p \rightarrow q) \wedge p$ ” domina a fórmula “ $q$ ”. Isso significa que, se estabelecermos de alguma forma que  $p$  implica  $q$ , e que  $p$  é verdadeira, podemos concluir que  $q$  é verdadeira. Esta regra é chamada *lei do modus ponens* e é frequentemente usada nas demonstrações de teoremas em matemática.

**Exemplo 3.5:** Seja  $\mathcal{F}$  a fórmula “ $(p \vee q) \wedge ((\neg p) \vee (\neg q))$ ” e  $\mathcal{G}$  a fórmula “ $p \wedge (\neg q)$ ”. As tabelas-verdade de  $\mathcal{F}$ ,  $\mathcal{G}$  e  $(\mathcal{F}) \rightarrow (\mathcal{G})$  são

|          |          | $\mathcal{F}_1$ | $\mathcal{F}_2$          | $\mathcal{F}$                        | $\mathcal{G}$       | $(\mathcal{F}) \rightarrow (\mathcal{G})$ |
|----------|----------|-----------------|--------------------------|--------------------------------------|---------------------|-------------------------------------------|
| $p$      | $q$      | $p \vee q$      | $(\neg p) \vee (\neg q)$ | $\mathcal{F}_1 \wedge \mathcal{F}_2$ | $p \wedge (\neg q)$ |                                           |
| <b>F</b> | <b>F</b> | <b>F</b>        | <b>V</b>                 | <b>F</b>                             | <b>F</b>            | <b>V</b>                                  |
| <b>F</b> | <b>V</b> | <b>V</b>        | <b>V</b>                 | <b>V</b>                             | <b>F</b>            | <b>V</b>                                  |
| <b>V</b> | <b>F</b> | <b>V</b>        | <b>V</b>                 | <b>V</b>                             | <b>V</b>            | <b>V</b>                                  |
| <b>V</b> | <b>V</b> | <b>V</b>        | <b>F</b>                 | <b>F</b>                             | <b>F</b>            | <b>V</b>                                  |

Concluimos portanto que  $\mathcal{F}$  domina  $\mathcal{G}$ .

Seguem algumas dominações importantes.

- *Lei da adição:*

$$p \text{ domina } p \vee q$$

- *Lei da simplificação:*

$$p \wedge q \text{ domina } p$$

- *Lei do modus ponens:*

$$(p \rightarrow q) \wedge p \text{ domina } q$$

- *Lei do modus tollens:*

$$(p \rightarrow q) \wedge \neg q \text{ domina } \neg p$$

- *Silogismo hipotético:*

$$(p \rightarrow q) \wedge (q \rightarrow r) \text{ domina } p \rightarrow r$$

- *Silogismo disjuntivo:*

$$(p \vee q) \wedge \neg p \text{ domina } q$$

- *Demonstração por absurdo:*

$$p \rightarrow \mathbf{F} \text{ domina } \neg p$$

**Exercício 3.28:** Verifique cada uma das dominações acima, construindo a tabela-verdade para as duas fórmulas.

O símbolo “ $\Rightarrow$ ” é frequentemente usado para significar “domina”. Entretanto, assim como o símbolo “ $\Leftrightarrow$ ”, ele não é um operador lógico, e não deve ser confundido com ‘ $\rightarrow$ ’:

- “ $(\mathcal{F}) \rightarrow (\mathcal{G})$ ” é uma proposição que pode ser verdadeira ou falsa, *dependendo dos valores das variáveis* que aparecem nas fórmulas  $\mathcal{F}$  e  $\mathcal{G}$ ;
- “ $\mathcal{F} \Rightarrow \mathcal{G}$ ” é a afirmação de que  $\mathcal{F} \rightarrow \mathcal{G}$  é verdade *para quaisquer valores* dessas variáveis.

**Exercício 3.29:** Verifique quais das seguintes afirmações são corretas:

- (a)  $(p \rightarrow (q \vee r)) \Rightarrow (p \rightarrow q)$ .
- (b)  $(p \rightarrow q) \Rightarrow (r \wedge p \rightarrow q)$ .
- (c)  $((p \vee q) \rightarrow r) \Rightarrow (p \rightarrow r)$ .
- (d)  $((p \rightarrow q) \wedge \neg p) \Rightarrow \neg q$ .
- (e)  $(p \leftrightarrow q) \Rightarrow (p \rightarrow q)$ .
- (f)  $(p \rightarrow q) \Rightarrow (p \leftrightarrow q)$ .
- (g)  $(p \rightarrow q) \Rightarrow q$ .
- (h)  $(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$ .

### 3.2.7 Equivalência e dominância em contexto específico

Duas fórmulas lógicas que não são logicamente equivalentes por si mesmas podem ser equivalentes em um contexto que restringe as combinações de valores que as variáveis podem assumir.

Por exemplo as fórmulas “ $p \leftrightarrow q$ ” e “ $p \wedge q$ ” não são equivalentes, pois suas tabelas-verdade diferem na primeira linha:

| $p$      | $q$      | $p \vee q$ | $p \leftrightarrow q$ | $p \wedge q$ | $(p \leftrightarrow q) \leftrightarrow (p \wedge q)$ |
|----------|----------|------------|-----------------------|--------------|------------------------------------------------------|
| <b>F</b> | <b>F</b> | <b>F</b>   | <b>V</b>              | <b>F</b>     | <b>F</b>                                             |
| <b>F</b> | <b>V</b> | <b>V</b>   | <b>F</b>              | <b>F</b>     | <b>V</b>                                             |
| <b>V</b> | <b>F</b> | <b>V</b>   | <b>F</b>              | <b>F</b>     | <b>V</b>                                             |
| <b>V</b> | <b>V</b> | <b>V</b>   | <b>V</b>              | <b>V</b>     | <b>V</b>                                             |

Porém, se soubermos que a afirmação  $p \vee q$  é verdadeira, então a combinação  $p = q = \mathbf{F}$  não pode ocorrer, excluindo a primeira linha dessa tabela. Nas demais linhas, a fórmula “ $p \leftrightarrow q$ ” tem o mesmo valor lógico de que “ $p \wedge q$ ”. Portanto, *supondo que  $p \vee q$  é verdade*, elas são logicamente equivalentes.

Em geral, podemos dizer que duas fórmulas são equivalentes *em determinado contexto* se tiverem o mesmo valor lógico para todas as combinações de valores de suas variáveis *que forem permitidas pelos fatos conhecidos nesse contexto*.

Da mesma forma, podemos dizer que uma fórmula  $\mathcal{F}$  domina uma fórmula  $\mathcal{G}$  *em determinado contexto* se a fórmula  $(\mathcal{F}) \rightarrow (\mathcal{G})$  for verdade para todas as combinações de valores de suas variáveis *que forem permitidas pelos fatos conhecidos nesse contexto*.

### 3.2.8 Precedência dos operadores lógicos

Em fórmulas lógicas que usam dois ou mais operadores lógicos a ordem em que eles devem ser aplicados é muito importante. Observe que as duas fórmulas “ $(p \vee q) \wedge r$ ” e “ $p \vee (q \wedge r)$ ” não são equivalentes, pois tem valores lógicos diferentes se  $p = \mathbf{V}$  e  $q = r = \mathbf{F}$ .

Assim como na álgebra de números, a necessidade de parênteses pode ser reduzida estabelecendo-se *regras de precedência* entre os operadores. A ordem tradicional é:

| <i>Operador</i>                | <i>Precedência</i> |
|--------------------------------|--------------------|
| $\neg$                         | 1                  |
| $\wedge$                       | 2                  |
| $\vee, \oplus$                 | 3                  |
| $\rightarrow, \leftrightarrow$ | 4                  |

Por exemplo, a fórmula  $\neg p \wedge q \rightarrow r \oplus s \wedge u$  deve ser entendida como  $((\neg p) \wedge q) \rightarrow (r \oplus (s \wedge u))$ .

As prioridades relativas tradicionais de  $\wedge$  e  $\vee$  vem da álgebra original de Boole, onde  $\wedge$  correspondia à multiplicação de números, e  $\vee$  a uma soma modificada. Pelas convenções tradicionais da álgebra de números, a fórmula “ $p + qr$ ” de Boole seria entendida como “ $p + (qr)$ ” e não como “ $(p + q)r$ ”. Daí vem a convenção de que “ $p \vee q \wedge r$ ” significa “ $p \vee (q \wedge r)$ ” e não “ $(p \vee q) \wedge r$ ”.

É tradicional considerar  $\oplus$  como tendo menos prioridade que  $\wedge$ . (Em parte, isso se deve ao uso de “+” para denotar  $\oplus$  em certas áreas da matemática.) Por outro lado, não há uma tradição forte para interpretar combinações de  $\oplus$  com  $\vee$ , como  $p \oplus q \vee r$ .

### 3.2.9 Associatividade de operadores

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.

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  $p \rightarrow (q \rightarrow r)$ . (Veja o exercício 3.30.)

**Exercício 3.30:** Construa e compare as tabelas-verdade das fórmulas

- (a)  $(p \rightarrow q) \rightarrow r$  e  $p \rightarrow (q \rightarrow r)$ .
- (b)  $(p \oplus q) \oplus r$  e  $p \oplus (q \oplus r)$ .
- (c)  $(p \leftrightarrow q) \leftrightarrow r$  e  $p \leftrightarrow (q \leftrightarrow r)$ .

Alguns autores convencionam que fórmulas com dois ou mais operadores não associativos de mesma prioridade, como  $p \rightarrow q \rightarrow r$ , devem ser avaliadas da esquerda para a direita; ou seja  $(p \rightarrow q) \rightarrow r$ . 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 fórmulas como  $p \oplus q \vee r$  ou  $p \rightarrow q \leftrightarrow r$ . Porém, por via das dúvidas, é aconselhável usar parênteses nesses casos.

## 3.3 Síntese de fórmulas

### 3.3.1 Forma normal disjuntiva

Nesta seção veremos como construir uma fórmula lógica que tem uma dada tabela-verdade.

Uma maneira de obter tal fórmula é fazer a disjunção de várias fórmulas que correspondem às linhas da tabela em que o resultado desejado é verdadeiro. Cada uma dessas fórmulas é uma uma conjunção de variáveis ou de suas negações, que é verdade apenas para a combinação de valores correspondentes a essa linha.

Por exemplo, suponha que queremos construir uma fórmula  $\mathcal{F}(p, q)$  que tem esta tabela-verdade:

| $p$      | $q$      | $\mathcal{F}(p, q)$ |
|----------|----------|---------------------|
| <b>F</b> | <b>F</b> | <b>F</b>            |
| <b>F</b> | <b>V</b> | <b>V</b>            |
| <b>V</b> | <b>F</b> | <b>V</b>            |
| <b>V</b> | <b>V</b> | <b>F</b>            |

Para a segunda linha, precisamos de uma sub-fórmula que seja **V** apenas quando  $p = \mathbf{F}$  e  $q = \mathbf{V}$ ; ou seja,  $(\neg p) \wedge q$ . Para a terceira linha, a fórmula é  $p \wedge (\neg q)$ . A fórmula  $\mathcal{F}(p, q)$  desejada é então

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

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

### 3.3.2 Forma normal conjuntiva

Outra maneira de construir uma fórmula lógica a partir de sua tabela-verdade é considerar cada linha em que o resultado desejado é **F**, e escrever uma sub-fórmula que é falsa apenas para essa combinação de variáveis. Esta fórmula pode ser uma disjunção das variáveis e suas negações. A conjunção dessas sub-fórmulas é a fórmula desejada.

Por exemplo, considere a tabela

| $p$      | $q$      | $r$      | $\mathcal{F}(p, q, r)$ |
|----------|----------|----------|------------------------|
| <b>F</b> | <b>F</b> | <b>F</b> | <b>F</b>               |
| <b>F</b> | <b>F</b> | <b>V</b> | <b>V</b>               |
| <b>F</b> | <b>V</b> | <b>F</b> | <b>V</b>               |
| <b>F</b> | <b>V</b> | <b>V</b> | <b>F</b>               |
| <b>V</b> | <b>F</b> | <b>F</b> | <b>V</b>               |
| <b>V</b> | <b>F</b> | <b>V</b> | <b>F</b>               |
| <b>V</b> | <b>V</b> | <b>F</b> | <b>V</b>               |
| <b>V</b> | <b>V</b> | <b>V</b> | <b>V</b>               |

Para conseguir a primeira linha da tabela, precisamos de uma fórmula que tem valor **F** apenas quando  $p = q = r = \mathbf{F}$ , ou seja  $p \vee q \vee r$ . Para a quarta linha, a fórmula deve ser **F** apenas quando  $p = \mathbf{F}$  e  $q = r = \mathbf{V}$ ; ou seja  $p \vee (\neg q) \vee (\neg r)$ . Para a sexta linha a fórmula é  $(\neg p) \vee q \vee (\neg r)$ . Portanto,  $\mathcal{F}(p, q, r)$  será

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

A fórmula assim obtida — uma conjunção, cujos termos são disjunções das variáveis ou suas negações — é chamada de *forma normal conjuntiva*.

As construções acima nos permitem concluir que toda fórmula lógica, por mais complicada que seja, é equivalente a uma fórmula normal disjuntiva, e a uma fórmula normal conjuntiva.

Uma forma normal disjuntiva (ou conjuntiva) com  $n$  variáveis pode ter até  $n$  sub-fórmulas, cada uma com  $n$  variáveis ou negações de variáveis. Esta nem sempre é a fórmula mais simples com essa tabela-verdade. Simplificar uma fórmula lógica é, em geral, um problema muito difícil, que foge do escopo deste livro.

**Exercício 3.31:** Considere a tabela-verdade abaixo:

| $p$ | $q$ | $r$ | $\mathcal{F}(p, q, r)$ |
|-----|-----|-----|------------------------|
| F   | F   | F   | F                      |
| F   | F   | V   | V                      |
| F   | V   | F   | V                      |
| F   | V   | V   | F                      |
| V   | F   | F   | V                      |
| V   | F   | V   | F                      |
| V   | V   | F   | F                      |
| V   | V   | V   | F                      |

- Construa uma fórmula para  $\mathcal{F}(p, q, r)$  na forma normal disjuntiva com essa tabela-verdade.
- Idem, na forma normal conjuntiva.

**Exercício 3.32:** Determine as formas normais disjuntiva e conjuntiva de:

- (a)  $p \wedge q$ .
- (b)  $p \vee q$ .
- (c)  $p \rightarrow q$ .
- (d)  $p \leftrightarrow q$ .

**Exercício 3.33:** Quantos termos tem a forma normal disjuntiva de  $p \oplus q \oplus r \oplus s$ ? E a forma normal conjuntiva?

**Exercício 3.34:** Sejam  $x_1, x_2, \dots, x_5$  cinco variáveis lógicas. Escreva uma fórmula usando apenas essas variáveis e os operadores  $\wedge$ ,  $\vee$  e  $\neg$ , equivalente à afirmação “pelo menos duas e no máximo três dessas variáveis são verdadeiras.”

**Exercício 3.35:** Um inteiro  $n$  no intervalo  $0 \dots 31$  pode ser representado por cinco variáveis lógicas  $x_4, x_3, x_2, x_1, x_0$ , que são os dígitos (bits) de  $n$  na base 2; sendo que  $x_i$  representa a potência  $2^i$ . Escreva uma fórmula usando apenas essas variáveis e os operadores  $\wedge$ ,  $\vee$  e  $\neg$ , equivalente à afirmação “ $n$  é um inteiro primo”.

### 3.3.3 Sistemas completos de operadores

A construção da forma normal disjuntiva (ou conjuntiva) permite concluir que toda fórmula lógica, usando quaisquer conectivos, é logicamente equivalente a outra fórmula que usa apenas os conectivos  $\vee$ ,  $\wedge$  e  $\neg$ .

Este é um exemplo do que se chama um *sistema completo* de operadores lógicos: um conjunto de operadores que, sozinhos, permitem escrever uma fórmula que é equivalente a qualquer fórmula do cálculo proposicional dada.

Uma vez que  $\{\vee, \wedge, \neg\}$  é um sistema completo, para mostrar que outro conjunto  $S$  de operadores é completo basta mostrar que cada uma das fórmulas  $p \vee q$ ,  $p \wedge q$ , e  $\neg p$  pode ser escrita usando apenas operadores de  $S$ .

**Exercício 3.36:** Prove que os conectivos  $\wedge$  e  $\neg$ , sozinhos, constituem um sistema completo de operadores lógicos. Idem para  $\vee$  e  $\neg$ .

**Exercício 3.37:** Prove que os conectivos  $\oplus$  e  $\wedge$ , sozinhos, constituem um sistema completo de operadores lógicos. (Dica: prove que é possível obter o operador  $\neg$  combinando esses dois operadores.)

**Exercício 3.38:** Prove que o conectivo  $\overline{\wedge}$  (não-e), sozinho, constitui um sistema completo de operadores lógicos. Idem para  $\overline{\vee}$  (não-ou).

### 3.4 Dualidade lógica

Seja  $\mathcal{F}$  uma fórmula lógica que usa apenas os conectivos  $\vee$ ,  $\wedge$ , e  $\neg$ . A *fórmula dual* é obtida a partir de  $\mathcal{F}$  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 fórmula “ $(p \wedge \neg q) \vee r$ ” é “ $(p \vee \neg q) \wedge r$ ”.

A dual de uma fórmula  $\mathcal{F}$  é geralmente denotada por  $\mathcal{F}^*$ . Note que  $(\mathcal{F}^*)^*$ , a dual da dual, é a fórmula original  $\mathcal{F}$ .

Em geral, as fórmulas  $\mathcal{F}$  e  $\mathcal{F}^*$  *não* são logicamente equivalentes. Entretanto, se  $\mathcal{F}$  é uma tautologia,  $\mathcal{F}^*$  é uma contradição, e vice-versa. Além disso, prova-se que se duas fórmulas  $\mathcal{F}$  e  $\mathcal{G}$  são equivalentes, então seus duais  $\mathcal{F}^*$  e  $\mathcal{G}^*$  são equivalentes, e vice-versa. Esta segunda propriedade nos permite obter equivalências lógicas a partir de equivalências já demonstradas.

Por exemplo, considere as duas leis de distributividade, de  $\wedge$  sobre  $\vee$  e  $\vee$  sobre  $\wedge$ :

$$p \wedge (q \vee r) \text{ é equivalente a } (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \text{ é equivalente a } (p \vee q) \wedge (p \vee r)$$

Uma vez provada a primeira equivalência, não precisamos provar a segunda: basta observar que “ $p \vee (q \wedge r)$ ” é a fórmula dual de “ $p \wedge (q \vee r)$ ”, e “ $(p \vee q) \wedge (p \vee r)$ ” é a dual de “ $(p \wedge q) \vee (p \wedge r)$ ”.

**Exercício 3.39:** Escreva a fórmula dual de  $(p \wedge q) \vee \neg(p \vee r)$ .

**Exercício 3.40:** Qual é a relação entre as tabelas-verdade de uma fórmula  $\mathcal{F}$  e de sua dual  $\mathcal{F}^*$ ?

**Exercício 3.41:** Encontre uma fórmula  $\mathcal{F}$  com duas variáveis lógicas usando apenas os operadores  $\vee$ ,  $\wedge$  e  $\neg$ , que seja logicamente equivalente à sua fórmula dual  $\mathcal{F}^*$ .

**Exercício 3.42:** Para definir o dual de um operador lógico binário qualquer  $\odot$ , basta encontrar uma fórmula equivalente a  $p \odot q$  que use apenas os operadores  $\wedge$ ,  $\vee$ , e  $\neg$ , e definir um operador  $\otimes$  tal que  $p \otimes q$  seja equivalente à fórmula dual dessa fórmula. Use este processo para definir os operadores duais de  $\leftrightarrow$ ,  $\oplus$ ,  $\rightarrow$ ,  $\overline{\vee}$  e  $\overline{\wedge}$ . Em cada caso, determine se o dual é um operador conhecido.

### 3.5 Afirmações auto-referentes

Já mencionamos que as 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.

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. Um exemplo mais elaborado é o seguinte

**Exercício 3.43:** Considere uma lista de 9 proposições,  $p_0, p_1, \dots, p_9$ , onde cada proposição  $p_n$  diz “a proposição  $p_{n+1}$  é verdadeira”, exceto que  $p_9$  diz “a proposição  $p_0$  é falsa.”

- (a) É possível que essas 10 afirmações sejam todas falsas?
- (b) É possível que essas 10 afirmações sejam todas verdadeiras?
- (c) É possível que haja pelo menos uma afirmação verdadeira e pelo menos uma falsa?

**Exercício 3.44:** Resolva novamente o exercício 3.43, mas com  $p_9$  dizendo “a proposição  $p_0$  é verdadeira.”

## 3.6 Cálculo de Predicados

Uma *proposição aberta* é uma proposição que depende de uma ou mais variáveis, lógicas ou não. Por exemplo:

- “ $x + y$  é um número primo”.
- “ $x$  pertence à união de  $A$  e  $B$ ”.
- “se  $p$  então  $q$  mas não  $r$ ”.

Analogamente, uma *fórmula aberta* é uma fórmula, lógica ou não, que depende de uma ou mais variáveis, lógicas ou não.

- $(x^2 \geq xy) \wedge (y^2 \leq xy)$
- $x \in A \cup B$
- $p \rightarrow (q \wedge \neg r)$

Em geral, o valor lógico de uma proposição ou fórmula aberta depende dos valores das variáveis que nela ocorrem. Por exemplo, a frase “ $x$  é maior que  $y$ ” é verdadeira se os valores de  $x$  e  $y$  forem 7 e 4, mas é falsa se os valores forem 10 e 21.

Uma proposição ou fórmula aberta pode fazer sentido apenas para certos valores das suas variáveis. Por exemplo, “ $x$  é maior que  $y$ ” faz sentido se  $x$  e  $y$  forem números reais, mas não faz sentido se  $x$  e  $y$  forem números complexos, ou se  $x$  for uma matriz e  $y$  for um número real.

A substituição de variáveis de uma proposição (ou fórmula) aberta por valores explícitos resulta em uma *proposição fechada* (ou *fórmula fechada*) que não depende de nenhuma variável — e que portanto pode ser tratada como uma proposição atômica do cálculo proposicional.

Neste livro usaremos uma letra maiúscula seguida por uma lista de variáveis distintas entre parênteses, por exemplo  $Q(x, y)$ , para denotar uma proposição aberta que depende dessas variáveis. A letra  $Q$  é chamada de *predicado*, e pode ser entendido como uma função que, dados valores das variáveis, devolve um valor lógico (**F** ou **V**).

Em geral, para que uma fórmula tenha sentido, é preciso definir o significado de cada predicado que ela usa. Como na álgebra, depois de definido um predicado  $P(x_1, x_2, \dots, x_n)$ , usaremos a notação  $P(v_1, v_2, \dots, v_n)$  para indicar a substituição, na definição do predicado, de todas as ocorrências da variável  $x_1$  pelo valor ou fórmula  $v_1$ , das de  $x_2$  por  $v_2$ , etc.. Se a fórmula resultante for verdadeira, dizemos que esses valores *satisfazem* o predicado  $P$ .

Por exemplo, seja  $Q$  o predicado tal que  $Q(x, y)$  significa “ $y > x/y$ ”. Então a fórmula  $Q(a^3, z + 1)$  representa a afirmação “ $z + 1 > a^3/(z + 1)$ ”, e  $Q(10, 5)$  significa “ $5 > 10/5$ ”. Como esta última afirmação é verdade, o par  $(10, 5)$  satisfaz o predicado  $Q$ .

**Exercício 3.45:** Seja  $P$  o predicado tal que  $P(x, A, B)$  significa “ $x + 1$  pertence a  $A$  e  $x - 1$  pertence a  $B$ ”. Determine o valor lógico da fórmula  $P(2, \{3, 4\}, \{\}) \oplus P(1, \{1, 2\}, \mathbb{N})$ .

O *cálculo de predicados* é a parte da lógica que estuda a interpretação e manipulação de fórmulas envolvendo predicados, independentemente de seu significado.

### 3.6.1 Quantificação universal

A substituição de variáveis por valores explícitos não é a única maneira de transformar uma proposição aberta em uma proposição atômica. Outra maneira é a chamada *quantificação universal*, que é uma afirmação do tipo “para todo  $x$  no conjunto  $D$ ,  $P(x)$ ”.

Denotaremos esta frase por  $(\forall x \in D) P(x)$ . Note que o primeiro par de parênteses é obrigatório. Nesta frase,  $D$  (o *domínio* da quantificação) pode ser qualquer conjunto previamente definido,  $x$  pode ser qualquer variável sem valor definido, e  $P(x)$  qualquer fórmula 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 fórmula  $P(x)$  for sempre verdadeira quando substituirmos 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  $P(x)$  significa “ $x$  é um número primo”, então a frase “ $(\forall x \in \mathbb{N}) P(x)$ ” é falsa; pois, embora as afirmações  $P(3)$  e  $P(17)$  sejam verdadeiras, a afirmação  $P(6)$  (por exemplo) é falsa.

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

**Exercício 3.46:** Sejam  $\mathbb{N}$  o conjunto dos números naturais, e suponha que  $P(x)$  significa “ $x$  é par”,  $Q(x)$  significa “ $x$  é divisível por 3” e  $R(x)$  significa “ $x$  é divisível por 4”. Escreva em linguagem natural (português) cada uma das fórmulas a seguir, e determine seu valor-verdade:

- (a)  $(\forall x \in \mathbb{N}) P(x)$ .
- (b)  $(\forall x \in \mathbb{N}) P(x) \vee Q(x)$ .
- (c)  $(\forall x \in \mathbb{N}) P(x) \rightarrow Q(x)$ .
- (d)  $(\forall x \in \mathbb{N}) P(x) \vee R(x)$ .
- (e)  $(\forall x \in \mathbb{N}) P(x) \wedge R(x)$ .
- (f)  $(\forall x \in \mathbb{N}) R(x) \rightarrow P(x)$ .
- (g)  $(\forall x \in \mathbb{N}) P(x) \rightarrow \neg Q(x)$ .
- (h)  $(\forall x \in \mathbb{N}) P(x) \rightarrow P(x + 2)$ .
- (i)  $(\forall x \in \mathbb{N}) R(x) \rightarrow R(x + 4)$ .
- (j)  $(\forall x \in \mathbb{N}) Q(x) \rightarrow Q(x + 1)$ .

### 3.6.2 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  $(\exists x \in D) P(x)$ . Note que o primeiro par de parênteses é obrigatório, e não há nenhum símbolo correspondente às palavras “tal que”. Aqui também, o domínio  $D$  da quantificação pode ser qualquer conjunto já definido;  $x$  pode ser qualquer variável; e  $P(x)$  qualquer fórmula 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.

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

Como exemplo, denotemos por  $P(x)$  o predicado “ $x$  é um número primo”. A fórmula  $(\exists x \in \mathbb{N}) P(x)$  é verdadeira, pois, por exemplo, a afirmação  $P(7)$  (“7 é um número primo”) é verdadeira, e 7 é um elemento de  $\mathbb{N}$ . Por outro lado, se  $Q(y)$  representa a proposição “ $y$  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.

**Exercício 3.47:** Sejam  $\mathbb{N}$  o conjunto dos números naturais, e suponha que  $P(x)$  significa “ $x$  é par”,  $Q(x)$  significa “ $x$  é divisível por 3” e  $R(x)$  significa “ $x$  é divisível por 4”. Escreva em linguagem natural (português) cada uma das fórmulas a seguir, e determine seu valor-verdade:

- (a)  $(\exists x \in \mathbb{N}) R(x)$
- (b)  $(\exists x \in \mathbb{N}) P(x) \vee Q(x)$ .
- (c)  $(\exists x \in \mathbb{N}) P(x) \rightarrow Q(x)$ .
- (d)  $(\exists x \in \mathbb{N}) Q(x) \rightarrow Q(x + 1)$ .
- (e)  $(\exists x \in \mathbb{N}) P(x) \rightarrow Q(x + 1)$ .

**Exercício 3.48:** Sejam  $\mathbb{N}$  o conjunto dos números naturais, e suponha que  $P(x, y)$  significa “ $x + 2 > y$ ”. Escreva as fórmulas listadas abaixo em linguagem natural (português) e atribua o valor-verdade correspondente a cada uma delas:

- (a)  $(\exists x \in \mathbb{N}) (\forall y \in \mathbb{N}) P(x, y)$ .
- (b)  $(\exists x \in \mathbb{N}) (\exists y \in \mathbb{N}) P(x, y)$ .
- (c)  $(\forall x \in \mathbb{N}) (\forall y \in \mathbb{N}) P(x, y)$ .
- (d)  $(\forall x \in \mathbb{N}) (\exists y \in \mathbb{N}) P(x, y)$ .

### 3.6.3 Quantificador de existência e unicidade

Na matemática são comuns afirmações do tipo “existe um *único*  $x$  no conjunto  $D$  tal que  $P(x)$ .” Esta afirmação é frequentemente denotada por  $(\exists!x \in D) P(x)$ .

Se o domínio  $D$  é finito, por exemplo  $D = \{x_1, x_2, \dots, x_n\}$ , a fórmula  $(\exists!x \in D) P(x)$  significa que uma, e apenas uma, das afirmações  $P(x_1), P(x_2), \dots, P(x_n)$  é verdadeira.

Esta fórmula pode ser escrita em termos dos quantificadores já definidos:

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

Ou seja, existe pelo menos um elemento  $x$  de  $D$  que satisfaz  $P$ , e qualquer elemento de  $D$  que satisfaz  $P$  deve ser igual a esse  $x$ . Outra definição equivalente é

$$[(\exists x \in D) P(x)] \wedge [(\forall y \in D) (\forall z \in D) ((P(y) \wedge P(z)) \rightarrow (y = z))]$$

A primeira parte desta fórmula diz que existe pelo menos um elemento de  $D$  que satisfaz  $P$ . A segunda parte diz que há no máximo um elemento em  $D$  que satisfaz  $P$ .

**Exercício 3.49:** Escreva uma fórmula lógica que expressa a proposição “Há no máximo dois elementos distintos de  $D$  que satisfazem o predicado  $P$ .”

**Exercício 3.50:** Seja  $D = \{x_1, x_2, \dots, x_n\}$  para algum  $n \geq 3$ . A afirmação  $(\exists!x \in D) P(x)$  equivale a  $P(x_1) \oplus P(x_2) \oplus \dots \oplus P(x_n)$ ? E se  $n = 2$ ? Justifique suas respostas.

### 3.6.4 Quantificação sobre o conjunto vazio

A afirmação “existe um estudante com mais de duzentos anos que gosta de física” é obviamente falsa; pois nem sequer existem estudantes com essa idade, muito menos que gostem 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? Mais geralmente: qual o valor lógico da afirmação “ $(\forall x \in D) P(x)$ ”, ou seja, “ $P(x)$  é verdadeira, para qualquer elemento  $x$  de  $D$ ”, se  $D$  não tem nenhum elemento?

Verifica-se que, neste caso, a interpretação mais consistente é considerar a frase “ $(\forall x \in D) P(x)$ ” *verdadeira, qualquer que seja o predicado  $P$* . Dizemos que tais afirmações são *verdadeiras por vacuidade*. Em particular, é verdade que “todos os estudantes com mais de duzentos anos de idade gostam de física”.

**Exercício 3.51:** Sejam  $A = \{0, 1, 2\}$ ,  $B = \{2, 3, 4\}$ ,  $C = \{4, 5, 6\}$ , e  $Q$  o predicado tal que  $(\forall z \in \mathbb{N}) Q(x) \leftrightarrow (\sqrt{x} \in \mathbb{N})$ . Determine o valor lógico das seguintes afirmações:

- (a)  $(\forall x \in A \cap B) Q(x)$
- (b)  $(\forall x \in B \cap C) Q(x)$
- (c)  $(\forall x \in A \cap C) Q(x)$

### 3.6.5 Quantificação sobre o conjunto universo

O domínio de um quantificador pode ser omitido da notação se for o conjunto universo  $\mathbb{U}$ :

$(\forall x) P(x)$  significa  $(\forall x \in \mathbb{U}) P(x)$

$(\exists x) P(x)$  significa  $(\exists x \in \mathbb{U}) P(x)$

Por exemplo, uma vez dito que “todas as variáveis a seguir representam números reais”, podemos escrever  $(\forall x) P(x)$  em vez de  $(\forall x \in \mathbb{R}) P(x)$ , ou  $(\exists x) Q(x)$  em vez de  $(\exists x \in \mathbb{R}) Q(x)$ .

Na verdade, todo quantificador com domínio explícito equivale a um quantificador sobre o conjunto universo onde o domínio é indicado no predicado. Especificamente:

$(\forall x \in D) P(x)$  equivale logicamente a  $(\forall x) (x \in D) \rightarrow P(x)$

$(\exists x \in D) P(x)$  equivale logicamente a  $(\exists x) (x \in D) \wedge P(x)$

Estas equivalências pressupõem que  $\mathbf{F} \rightarrow p$  equivale a  $\mathbf{V}$ , e  $\mathbf{F} \wedge p$  equivale a  $\mathbf{F}$ , *mesmo que o valor lógico da proposição  $p$  não esteja definido no contexto*. Por exemplo, suponha que o predicado  $Q$  é definido apenas para inteiros. A fórmula  $(\forall x \in \mathbb{Z}) Q(x)$  equivale a  $(\forall x) (x \in \mathbb{Z}) \rightarrow Q(x)$ , embora nesta fórmula a variável  $x$  em princípio assume valores não inteiros. Para estes valores a fórmula  $(x \in \mathbb{Z}) \rightarrow Q(x)$  é verdadeira, porque  $x \in \mathbb{Z}$  é  $\mathbf{F}$ , embora  $Q(x)$  não esteja definido.

**Exercício 3.52:** Sejam  $A = \{0, 1, 2\}$ ,  $B = \{2, 3, 4\}$  e  $C = \{4, 5, 6\}$ . Elimine o domínio explícito das seguintes fórmulas, e determine seu valor lógico:

- (a)  $(\forall x \in A \cap B) x \notin A$
- (b)  $(\exists x \in B \cap C) x \in C$
- (c)  $(\forall x \in A \cap C) x \in B$

**Exercício 3.53:** Escreva, em português, as seguintes fórmulas, supondo que  $R(x)$  significa “ $x$  é um rato,”  $Q(x)$  significa “ $x$  come queijo,” e o domínio consiste de todos os animais.

- (a)  $(\forall x) R(x) \rightarrow Q(x)$ .
- (b)  $(\forall x) R(x) \wedge Q(x)$ .
- (c)  $(\exists x) R(x) \rightarrow Q(x)$ .
- (d)  $(\exists x) R(x) \wedge Q(x)$ .

### 3.6.6 Escopo de um quantificador

Quando um quantificador sobre uma variável é aplicado a uma proposição aberta que depende dessa variável, dizemos que cada ocorrência dessa variável na proposição está *amarrada* ao quantificador. Todas as demais variáveis e predicados que ocorrem na proposição (inclusive no domínio

do quantificador) continuam *livres*. Por exemplo, na fórmula  $(\forall x \in D) P(x) \wedge x^2 + x - y > z/(x + y)$ , as quatro ocorrências de  $x$  estão amarradas, enquanto que as ocorrências de  $D$ ,  $P$ ,  $y$  e  $z$  estão livres.

A parte da fórmula onde a variável de um quantificador é amarrada por ele é chamada de *escopo* do quantificador. Por convenção, o escopo é toda a parte da fórmula que segue ao quantificador; mas podemos usar parênteses para limitar esse escopo. Por exemplo, na fórmula  $((\forall x \in D) P(x)) \wedge ((\exists x \in E) Q(x)) \vee R(x)$ , 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.

Assim, por exemplo, a fórmula  $[(\exists x \in \mathbb{Z}) x + 1 = 3] \wedge [(\exists x \in \mathbb{Z}) x + 1 = 5]$  é verdadeira, pois o escopo do primeiro “ $\exists x$ ” inclui apenas “ $x + 1 = 3$ ”, enquanto que “ $x + 1 = 5$ ” está no escopo do segundo “ $\exists x$ ”. Portanto a primeira parte é verdade para (um)  $x = 2$ , e a segunda para (outro)  $x = 4$ . Já a fórmula  $(\exists x \in \mathbb{Z})(x + 1 = 3) \wedge (x + 1 = 5)$  é falsa, pois as duas ocorrências de  $x$  no predicado são o mesmo valor.

Duas amarrações da mesma variável podem ter escopos encaixados. Por exemplo, na fórmula

$$(\forall x \in \mathbb{Z}) (\exists y \in \mathbb{Z}) (y = x + 1) \wedge (\forall x \in \mathbb{N}) (y - x \leq y) \wedge (y > x]$$

o escopo do segundo “ $\forall x$ ” vai até o fim da fórmula, e portanto a fórmula toda é falsa. Já na fórmula

$$(\forall x \in \mathbb{Z}) (\exists y \in \mathbb{Z}) (y = x + 1) \wedge [(\forall x \in \mathbb{N}) (y - x \leq y)] \wedge (y > x]$$

o escopo do segundo “ $\forall x$ ” é apenas “ $y - x \leq y$ ”, o que torna a fórmula entre colchetes verdadeira. O último  $x$  está amarrado no primeiro “ $\forall x$ ”, e portanto essa afirmação também é verdadeira, assim como a fórmula toda.

### 3.6.7 Equivalência e dominância com quantificadores

Os conceitos de tautologia, contradição, equivalência e dominância também se aplicam a fórmulas com quantificadores.

Assim como no cálculo proposicional, definimos uma *tautologia* do cálculo de predicados como sendo uma proposição que é verdadeira quaisquer que sejam os valores das variáveis livres e as definições dos predicados que aparecem nas mesmas. Um exemplo trivial é a fórmula “ $(\forall x \in D) P(x) \vee \neg P(x)$ ”. Esta afirmação é verdade quaisquer que sejam of domínio  $D$  e o predicado  $P$ .

Por outro lado, uma *contradição* é uma proposição que é falsa quaisquer que sejam as definições adotadas para seus predicados; como, por exemplo, “ $(\exists x \in D) P(x) \wedge \neg P(x)$ ”.

Como no cálculo proposicional, dizemos também que duas fórmulas  $\mathcal{F}$  e  $\mathcal{G}$  são *equivalentes* se  $(\mathcal{F}) \leftrightarrow (\mathcal{G})$  é uma tautologia, e que  $\mathcal{F}$  *domina*  $\mathcal{G}$  se  $(\mathcal{F}) \rightarrow (\mathcal{G})$  é uma tautologia.

### 3.6.8 Negação de quantificadores

Um exemplo importante de equivalência lógica no cálculo de predicados são as regras para *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  $(\forall x \in D) \neg P(x)$

Ou seja, podemos trocar as posições do operador de negação e do quantificador, *desde que também troquemos o tipo de quantificador* ( $\forall$  por  $\exists$ , e vice-versa). Ressaltamos que estas equivalências

valem para qualquer predicado  $P$  e qualquer domínio  $D$ , e, naturalmente, qualquer que seja a variável usada nos quantificadores.

Por exemplo, considere a afirmação  $(\forall n \in \mathbb{N}) n + 1 > 2$ . O valor lógico dessa afirmação é falso, pois a fórmula aberta “ $n + 1 > 2$ ” não vale quando  $n = 0$  ( $(0 + 1) = 1$  e 1 não é maior que 2). Por outro lado, este mesmo exemplo mostra que existe um  $n$  tal que a afirmação contrária “ $n + 1 \leq 2$ ” é verdadeira; isto é, que  $(\exists n \in D) n + 1 \leq 2$  é verdadeira.

Lembramos que  $\forall$ , de certa forma, representa várias conjunções ( $\wedge$ ); no mesmo sentido que  $\exists$  representa várias disjunções ( $\vee$ ). Observe portanto que as regras para disjunção de quantificadores são análogas às leis de De Morgan para negação de  $\wedge$  e  $\vee$ .

Estas regras valem também quando o domínio  $D$  é vazio. Aliás, a principal justificativa para a regra da seção 3.6.4 é justamente fazer com que as regras de negação de quantificadores sejam válidas em todos os casos. Por exemplo, considere a afirmação “existe um estudante com mais de duzentos anos de idade que não gosta de física”, ou seja  $(\exists x \in D) \neg P(x)$  onde  $D$  é o conjunto (vazio) dos “estudantes com mais de duzentos anos”, e  $P(x)$  é a frase “ $x$  gosta de física”. Esta afirmação é obviamente falsa; e portanto sua negação,  $\neg((\exists x \in D) \neg P(x))$ , deveria ser verdadeira. De fato, pelas regras acima, a negação desta frase  $\neg((\exists x \in D) \neg P(x))$  é  $(\forall x \in D) \neg \neg P(x)$ , ou seja  $(\forall x \in D) P(x)$ ; e, conforme definimos na seção 3.6.4, esta afirmação tem valor lógico verdadeiro.

### 3.6.9 Distributividade de quantificadores

Em alguns casos, é possível trocar a ordem de quantificadores com outros conectivos lógicos. Por exemplo, lembrando que  $\forall$  representa uma série de conjunções  $\wedge$ , e que  $\exists$  representa uma série de

disjunções  $\vee$ , podemos concluir que

- $(\forall x \in D) (P(x) \wedge Q(x))$  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  $((\exists x \in D) P(x)) \vee ((\exists x \in D) Q(x))$ .

### 3.6.10 Traduzindo linguagem natural para fórmulas quantificadas

A codificação de proposições da linguagem natural em fórmulas com quantificadores nem sempre é fácil. Na linguagem natural, muitas vezes os quantificadores e/ou o domínio estão implícitos.

Por exemplo, considere a seguinte afirmação: “macacos gostam de bananas.” Nesta afirmação, há um quantificador universal implícito: “*todos* os macacos gostam de bananas.” Sua formalização é portanto  $(\forall x \in M) B(x)$  onde  $M$  é o conjunto dos macacos, e  $B(x)$  é o predicado “ $x$  gosta de banana.”

Outro exemplo é a afirmação “existe um  $x$  tal que  $x^2 = 5$ ”. O valor lógico dessa afirmação depende do domínio; se escrevermos  $(\exists x \in \mathbb{N}) x^2 = 5$ , a afirmação é falsa; se escrevermos  $(\exists x \in \mathbb{R}) x^2 = 5$ , ela é verdadeira. Neste caso, o domínio correto só pode ser determinado pelo contexto da afirmação.

Várias expressões podem ser usadas na língua portuguesa para expressar os quantificadores:

- “para qualquer  $x$  em  $D$ ,  $P(x)$ ”,
- “se  $x$  é um elemento genérico de  $D$ , então  $P(x)$ ”,

- “um elemento que está em  $D$  sempre satisfaz  $P(x)$ ”,
- “para quem está em  $D$ , vale  $P(x)$ ”,
- “algum elemento de  $D$  satisfaz  $P(x)$ ”,
- “há elementos em  $D$  para os quais  $P(x)$  vale”.

Há também muitas expressões para a negação dos quantificadores:

- “nenhum  $x$  em  $D$  satisfaz  $P(x)$ ”,
- “nem todo  $x$  em  $D$  satisfaz  $P(x)$ ”,
- “não há elemento  $x$  em  $D$  que satisfaça  $P(x)$ ”,
- “ninguém em  $D$  satisfaz  $P(x)$ ”,
- “para nenhum  $x$  em  $D$  vale  $P(x)$ ”,
- “quando  $x$  está em  $D$ , a afirmação  $P(x)$  nem sempre é verdadeira.”

Na linguagem natural, muitas vezes o quantificador está no meio ou no fim da sentença:

- “ $P(x)$  vale para todo  $x$  em  $D$ ”,
- “ $P(x)$  é verdade para algum  $x$  em  $D$ ”,
- “ $P(x)$  vale sempre que  $x$  está em  $D$ ”,
- “ $P(x)$  não é verdade para alguns elementos  $x$  de  $D$ ”.

Uma maneira de verificar se uma fórmula com quantificadores representa corretamente uma afirmação em linguagem natural é trocar os quantificadores por meio das regras de negação, traduzir o resultado novamente para a linguagem natural, e conferir se o sentido é o mesmo que o original. Por exemplo, suponha que representemos a frase “nenhum gorila é bonito” por  $\neg(\exists x \in F) B(x)$ , onde  $F$  é o conjunto de gorilas, e  $B(x)$  significa “ $x$  é bonito”. Pelas regras de negação, esta frase é equivalente a  $(\forall x \in F) \neg B(x)$ , ou seja, “todos os gorilas são feios”.

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 3.54:** 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.
- (f) Entre todos os inteiros existem alguns que são primos.
- (g) Um dia do próximo mês é domingo.
- (h) Alguns inteiros são pares e divisíveis por 3.
- (i) Alguns inteiros são pares ou divisíveis por 3.
- (j)  $x^2 - 14 = 0$  tem uma solução positiva.
- (k) Toda solução de  $x^2 - 14 = 0$  é positiva.
- (l) Nenhuma solução de  $x^2 - 14 = 0$  é positiva.
- (m) Existe algum estudante de direito que não é brasileiro.
- (n) Todo estudante de direito tem um celular.
- (o) Ninguém é perfeito.
- (p) Alguém é perfeito.
- (q) Todos os nossos amigos são perfeitos.
- (r) Algum de nossos amigos é perfeito.
- (s) Todos são nossos amigos e são perfeitos.
- (t) Ninguém é nosso amigo ou alguém não é perfeito.

**Exercício 3.55:** Expresse, em português, a negação de cada uma das proposições do exercício 3.54.

**Exercício 3.56:** Se  $D$  é o conjunto de estudantes de uma escola, e  $P(x)$  é o predicado “ $x$  fala francês”, como poderíamos escrever a afirmação “existem pelo menos dois estudantes dessa escola que falam francês,” na notação do cálculo proposicional?

**Exercício 3.57:** Expresse a negação de cada uma das proposições do exercício 3.47 em forma simbólica e em linguagem natural (português).

### 3.6.11 Mudança de domínio

A regra abaixo permite restringir o domínio das quantificações universais:

- A afirmação  $(D \subseteq E) \wedge (\forall x \in E) P(x)$  domina  $(\forall x \in D) P(x)$ .

Ou seja, uma quantificação universal verdadeira continua verdadeira se restringirmos o domínio a qualquer subconjunto do mesmo. Por exemplo, se sabemos que as zebras são um subconjunto dos ruminantes, e que “todo ruminante tem quatro patas”, podemos concluir que “todas as zebras tem quatro patas”.

Reciprocamente, a regra abaixo permite ampliar o domínio de quantificações existenciais:

- A afirmação  $(D \subseteq E) \wedge (\exists x \in D) P(x)$  domina  $(\exists x \in E) P(x)$ .

Ou seja, uma quantificação existencial verdadeira continua verdadeira se ampliarmos o domínio. Por exemplo, se sabemos que “existe um boi preto”, e que os bois são um subconjunto dos ruminantes, podemos concluir que “existe um ruminante preto”.

Outras regras permitem mudar o domínio no sentido contrário, com ressalvas na fórmula quantificada:

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

Por exemplo, se aceitarmos que os papagaios são um subconjunto dos animais, a afirmação “todo papagaio tem um bico” equivale a dizer “todo animal, se for um papagaio, tem um bico;” E a afirmação “existe um papagaio amarelo” equivale a dizer que “existe um animal que é papagaio e é amarelo.”

Um erro comum é confundir as duas regras, e mudar o domínio do quantificador universal com  $\wedge$  ao invés de  $\rightarrow$ . Por exemplo, suponha que  $A$  é o conjunto dos animais,  $M$  é o conjunto dos macacos, e  $B(x)$  significa “ $x$  gosta de banana”. É errado traduzir a afirmação “todo macaco gosta de banana” pela fórmula  $(\forall x \in A) (x \in M) \wedge B(x)$ . Esta fórmula na verdade significa “todo animal é macaco e gosta de banana”, que é bem diferente do sentido original. A fórmula correta seria  $(\forall x \in A) (x \in M) \rightarrow B(x)$ , que, pelas regras acima, equivale a  $(\forall x \in M) B(x)$ .

O erro simétrico é usar  $\rightarrow$  ao mudar o domínio do quantificador existencial. Por exemplo, representar a afirmação (falsa) “existe um macaco que voa” por  $(\exists x \in A) (x \in M) \rightarrow V(x)$ , onde  $A$  é

o conjunto dos animais,  $M$  o conjunto dos macacos, e  $V(x)$  significa “ $x$  voa”. Esta fórmula na verdade significa “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  $(x \in M) \rightarrow V(x)$  fica  $\mathbf{F} \rightarrow V(x)$  e portanto verdadeira. A fórmula correta seria  $(\exists x \in A)(x \in M) \wedge V(x)$ , que é falsa como a original.

**Exercício 3.58:** Em cada um dos casos abaixo, procure determinar se as duas fórmulas são logicamente equivalentes:

- (a)  $((\forall x \in A) P(x)) \wedge ((\forall x \in B) P(x))$  equivale a  $(\forall x \in A \cup B) P(x)$ ?
- (b)  $((\exists x \in A) P(x)) \vee ((\exists x \in B) Q(x))$  equivale a  $(\exists x \in A \cup B) (P(x) \vee Q(x))$ ?
- (c)  $((\forall x \in A) P(x)) \vee ((\forall x \in B) P(x))$  equivale a  $(\forall x \in A \cup B) P(x)$ ?
- (d)  $((\exists x \in A) P(x)) \wedge ((\exists x \in B) Q(x))$  equivale a  $(\exists x \in A \cup B) (P(x) \vee Q(x))$ ?

### 3.6.12 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 fórmula fechada:

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

A ordem dos quantificadores pode ser muito importante. Por exemplo, a fórmula  $(\forall x \in \mathbb{Z}) (\exists y \in \mathbb{Z}) x + y = 2x$  significa “para todo inteiro  $x$ , existe um inteiro  $y$  (que pode ser diferente para cada  $x$ !) tal que  $x + y = 2x$ ”. Esta afirmação é verdadeira, pois, para cada  $x$ , basta tomar  $y = x$  para satisfazer a condição. Por outro lado, a fórmula  $(\exists y \in \mathbb{Z}) (\forall x \in \mathbb{Z}) x + y = 2x$  significa “existe um inteiro  $y$  tal que, para todo inteiro  $x$  (e esse mesmo  $y$ !),  $x + y = 2x$ ”. Esta frase é falsa, pois, 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 quaisquer 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  $(\exists y \in E) (\exists x \in D) P(x, y)$

Dois ou mais quantificadores do mesmo tipo com mesmo domínio podem ser combinados:

- A fórmula  $(\forall x, y, z \in D) P(x, y, z)$  é uma abreviação de  $(\forall x \in D) (\forall y \in D) (\forall z \in D) P(x, y, z)$
- A fórmula  $(\exists x, y, z \in D) P(x, y, z)$  é uma abreviação de  $(\exists x \in D) (\exists y \in D) (\exists z \in D) P(x, y, z)$

Este tipo de abreviação obviamente não se aplicam se os quantificadores tiverem tipos ou domínios diferentes.

Enquanto houver variáveis livres, a proposição ou fórmula continua sendo aberta. Ela só é fechada quando todas as variáveis estiverem amarradas.

Por influência da linguagem natural, alguns autores às vezes escrevem o símbolo quantificador (especialmente ‘ $\forall$ ’) *depois* da fórmula lógica quantificada, como por exemplo em “ $P(x), \forall x \in D$ .” Entretanto, este estilo deve ser evitado, pois pode gerar ambiguidade — especialmente quando há vários quantificadores envolvidos. Considere, por exemplo “ $(\exists x \in \mathbb{Z}) x + y = 0, \forall y \in \mathbb{Z}$ .”

**Exercício 3.59:** Sejam  $\mathbb{N}$  o conjunto dos números naturais,  $P(x, y)$  é “ $x + 2 > y$ ”. Escreva as fórmulas listadas abaixo em linguagem natural (português) e atribua o valor-verdade correspondente a cada uma delas:

- (a)  $(\forall x \in \mathbb{N}) (\exists y \in \mathbb{N}) P(x, y)$ .
- (b)  $(\forall x \in \mathbb{N}) (\forall y \in \mathbb{N}) P(x, y)$ .
- (c)  $(\forall y \in \mathbb{N}) (\exists x \in \mathbb{N}) P(x, y)$ .

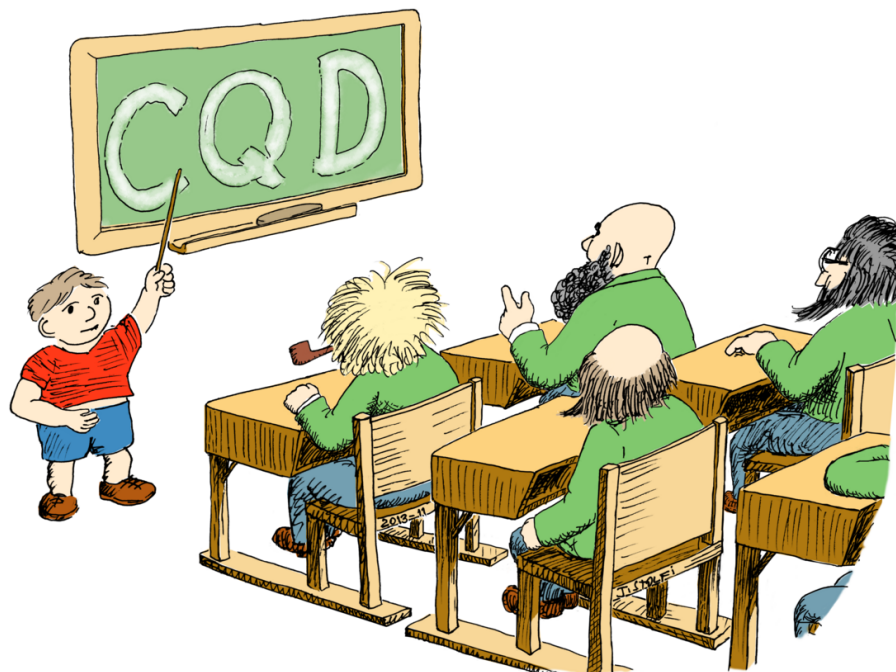
**Exercício 3.60:** Determine o valor verdade de cada uma das fórmulas:

- (a)  $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 < m)$ .
- (b)  $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n < m^2)$ .
- (c)  $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(nm = m)$ .
- (d)  $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 0)$ .
- (e)  $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n \cdot m = m)$ .
- (f)  $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 + m^2 = 5)$ .
- (g)  $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 + m^2 = 25)$ .
- (h)  $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 4 \wedge n - m = 1)$ .
- (i)  $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 4 \wedge n - m = 2)$ .
- (j)  $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\exists p \in \mathbb{N})(p = (n + m)/2)$ .
- (k)  $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x^2 = y)$ .
- (l)  $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x = y^2)$ .
- (m)  $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x \cdot y = 0)$ .
- (n)  $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y \neq y + x)$ .
- (o)  $(\forall x \in \mathbb{R}) x \neq 0 \rightarrow (\exists y \in \mathbb{R})(x \cdot y = 1)$ .
- (p)  $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(y \neq 0 \rightarrow (x \cdot y = 1))$ .
- (q)  $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 1)$ .
- (r)  $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(x + 2y = 2 \wedge 2x + 4y = 5)$ .
- (s)  $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 2 \wedge 2x - y = 1)$ .
- (t)  $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\exists z \in \mathbb{R})(z = (x + y)/2)$ .

**Exercício 3.61:** Encontre a negação e o valor-verdade de cada uma das fórmulas do exercício 3.60.

# **Capítulo 4**

## **Métodos de Demonstração**



## 4.1 Introdução

Como vimos no capítulo 1, 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 algumas definições e/ou afirmações básicas — chamadas *axiomas* ou *postulados* — que ambas as partes aceitam como verdadeiras, e/ou afirmações que foram previamente demonstradas.

Para ser convincente, uma demonstração somente pode usar afirmações e regras de raciocínio que as duas partes consideram válidas. Portanto, o nível de detalhe da demonstração depende do conhecimento do leitor, e de sua familiaridade com demonstrações.

Neste livro, por exemplo, vamos supor que o leitor conhece o conteúdo dos capítulos anteriores, e está em um curso superior de ciência ou engenharia, de modo que deve estar familiarizado com as regras da álgebra de números e da teoria de conjuntos.

Uma afirmação devidamente demonstrada é chamada de *teorema* (palavra derivada de uma 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.

### 4.1.1 Definições

Uma demonstração também pode usar *definições* que tenham sido feitas previamente. De modo geral, uma definição introduz no escopo da discussão um novo predicado, e uma fórmula lógica equivalente ao mesmo. Por convenção, as palavras que representam o novo predicado são enfati-

zadas na 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  $n = pq$ .

Esta definição introduz um novo predicado “é múltiplo de”, que, na notação formal, podemos denotar (por exemplo) por  $M$ . Neste caso,  $M(n, p)$  é lido “ $n$  é múltiplo de  $p$ ”. A parte que vem depois do “se, e somente se” seria escrita formalmente “ $(\exists q \in \mathbb{Z}) n = pq$ ”. Assim, depois de enunciarmos esta definição, podemos tratar a fórmula

$$(\forall n, p \in \mathbb{Z}) M(n, p) \leftrightarrow (\exists q \in \mathbb{Z}) n = pq \quad (4.1)$$

como um axioma, ou supor que  $M(n, p)$  é logicamente equivalente a  $(\exists q \in \mathbb{Z}) n = pq$ . Em particular, podemos trocar qualquer sub-fórmula  $M(\mathcal{E}, \mathcal{F})$ , onde  $\mathcal{E}$  e  $\mathcal{F}$  são fórmulas com valores inteiros, por  $(\exists q \in \mathbb{Z}) (\mathcal{E}) = (\mathcal{F}) q$ , ou vice-versa; sem que isso quebre a equivalência lógica.

Mesmo quando escrita em linguagem natural, uma definição precisa ser *completa*, isto é, deve especificar todas as propriedades que identificam exatamente o predicado em questão. Deve ser também *precisa*, de modo que o leitor não tenha dúvidas sobre o valor lógico do predicado, quando ele se aplica.

Observe que para quaisquer inteiros  $n$  e  $p$ , tanto a definição 4.1 quanto o axioma (4.1) determinam, sem ambiguidade, se  $n$  é ou não múltiplo de  $p$ .

Por outro lado, da maneira como está escrita, a definição 4.1 só vale no domínio dos inteiros. Será o número  $\pi$  um múltiplo de  $\sqrt{17}$ ? A definição 4.1 não diz nem que sim, nem que não. Enquanto o conceito de “múltiplo” não for definido para esses números, essa frase (ou a fórmula  $M(\pi, \sqrt{17})$ ) não tem sentido: ela não é nem verdadeira nem falsa, e portanto não é uma proposição lógica.

Observe também que, na parte da definição 4.1 que descreve o sentido do predicado, as variáveis  $n$  e  $p$  são livres, enquanto que  $q$  está amarrada no quantificador “existe”.

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 múltiplo de”. Formalmente, se denotarmos esse predicado por  $D$ , ela introduz o axioma

$$(\forall p, n \in \mathbb{Z}) D(p, n) \leftrightarrow M(n, p) \quad (4.2)$$

Observe o uso do conetivo lógico “se e somente se” ( $\leftrightarrow$ ) nestas definições. Este conetivo permite ao leitor decidir se uma entidade qualquer do domínio se enquadra *ou não* na definição. Portanto toda definição deve ser uma afirmação da forma “se e somente se”.

Entretanto, em textos matemáticos e técnicos é comum encontrar definições que usam apenas a palavra “se” quando o autor na verdade quer dizer “se e somente se.” Por exemplo:

**Definição 4.3:** Um inteiro é *par* se ele é múltiplo de 2.

Esta definição deve ser entendida como “um inteiro é par se, e somente se, ele é múltiplo de 2”. Formalmente, ela introduz um predicado  $P$ , tal que  $P(n)$  é lido “ $n$  é um inteiro par”, e o axioma  $(\forall n \in \mathbb{Z}) P(n) \leftrightarrow M(n, 2)$ . Eis outro exemplo:

**Definição 4.4:** Se um inteiro não é par, dizemos que ele é *ímpar*.

Formalmente, esta definição introduz um predicado  $I$ , tal que  $I(n)$  é lido “ $n$  é ímpar”, e o axioma  $(\forall n \in \mathbb{Z}) I(n) \leftrightarrow \neg P(n)$

Há outros formatos de definição que não usam nem “se” nem “se e somente se”. Por exemplo:

**Definição 4.5:** Um *número primo* é um número inteiro maior que 1, que não tem nenhum divisor exceto 1 e ele mesmo.

Esta definição deve ser lida “ $n$  é um *número primo* se, e somente se,  $n$  é um número inteiro,  $n$  é maior que 1, e não existe nenhum  $d$  que seja divisor de  $n$  e diferente de 1 e de  $n$ .” Formalmente, se  $R$  representa o predicado “é primo”, esta definição introduz o axioma

$$(\forall n) R(n) \leftrightarrow (n \in \mathbb{Z} \wedge n > 1 \wedge \neg((\exists d) D(d, n) \wedge d \neq 1 \wedge d \neq n))$$

### Definições equivalentes

Em geral há muitas maneiras diferentes de definir o mesmo conceito. Por exemplo, em vez da definição 4.4 podemos dizer

**Definição 4.6:** Um inteiro  $n$  é *ímpar* se existe um inteiro  $k$  tal que  $n = 2k + 1$ .

Ou então

**Definição 4.7:** Um inteiro  $n$  é *ímpar* se existe um inteiro par  $m$  tal que  $n = m + 1$ .

Formalmente, os predicados  $I$ ,  $I_2$ , e  $I_3$  introduzidos pelas definições 4.4, 4.6 e 4.7 são o mesmo predicado; isto é,  $(\forall n) I(n) \leftrightarrow I_2(n)$ , e  $(\forall n) I_2(n) \leftrightarrow I_3(n)$ . Porém, estas equivalências não são inteiramente óbvias, e podem precisar de demonstrações.

### 4.1.2 Conjecturas

Uma *conjetura* (ou *conjectura*) 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*.

Um exemplo famoso é a *conjetura de Fermat*: “se  $n > 2$ , a equação  $x^n + y^n = z^n$  não tem soluções inteiras positivas.” Esta conjetura foi encontrada em um livro que pertenceu ao matemático Pierre de Fermat (1601–1665), que 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*.

Outro exemplo famoso é a *conjetura das quatro cores*: “todo mapa pode ser pintado com no máximo quatro cores, de modo que países vizinhos tenham cores diferentes.” Esta conjetura foi enunciada em 1852 por Francis Guthrie (1831–1899), mas somente foi provada em 1976 por Ken-

neth 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 continua sendo impossível demonstrar o teorema sem recorrer a um computador.

Há várias conjecturas famosas que ainda estão abertas. A *conjetura de Goldbach*, formulada pelo matemático alemão Christian Goldbach em 1742, afirma que *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  $4 \times 10^{14}$  (400 trilhões); 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. Estes números, hoje, são chamados *números de Mersenne*. 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 ( $2047 = 23 \times 89$ ). Depois de verificar mais alguns casos, ele conjecturou que  $M_n$  é primo para todo  $n$  em  $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$ . Porém, em 1876 Edouard Lucas (1842–1891) provou que  $M_{67} = 2^{67} - 1$  não era primo, e portanto a conjectura 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 palestra 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. A platéia aplaudiu em pé. Depois ele contou que tinha levado três anos, trabalhando todos os domingos, para encontrar essa fatoração.

### 4.1.3 Métodos de demonstração

Existem teoremas que tem muitas demonstrações diferentes. Qual delas 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.. De modo geral, quando não sabemos se uma afirmação é verdadeira, nossa primeira preocupação é encontrar uma demonstração que nos convença. Para convencer outras pessoas, entretanto, devemos cuidar para que a demonstração seja, além de correta, também simples, clara e objetiva, tanto quanto possível.

Há vários *métodos de demonstração* (*estilos, estratégias, esquemas*, etc.) que são frequentemente usados em matemática. Em geral, a mesma demonstração pode ser reformulada e rearranjada de modo a se enquadrar em vários esquemas distintos. Dependendo do caso, algumas dessas versões podem ser mais fáceis de encontrar, escrever e entender do que outras. No restante deste capítulo vamos descrever algumas técnicas frequentemente utilizadas em provas.

## 4.2 Demonstração de implicações

No decorrer de muitas demonstrações, temos que provar implicações da forma  $p \rightarrow q$ , isto é *se  $p$  é verdadeira, então  $q$  também é*. A afirmação  $p$  é chamada de *hipótese*, *premissa* ou *condição*, e a afirmação  $q$  é chamada de *tese* ou *conclusão*.

### 4.2.1 Método direto

No *método direto* de demonstração, supomos que a hipótese  $p$  é verdadeira, e usamos uma sequência de proposições que são consequências lógicas das anteriores, até obter a tese  $q$ . Esta sequência de passos prova a implicação  $p \rightarrow q$ . Por exemplo, digamos que, num contexto em que  $m$  e  $n$  são números inteiros, é preciso provar a afirmação

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

Podemos escrever a seguinte demonstração:

**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. (De 7 e definição de “par”. Tese.)

**Fim.**

Usando símbolos lógicos e o predicado  $P$  da definição 4.3, a afirmação que queremos demonstrar é  $P(m) \wedge P(n) \rightarrow P(m + n)$ . A demonstração direta, com alguns passos mais detalhados, seria:

**Prova:**

1. Suponha  $P(m)$ . (Hipótese.)
2. Suponha  $P(n)$ . (Hipótese.)
3.  $(\exists r \in \mathbb{Z}) m = 2r$ . (Definição de  $P$ .)
4.  $(\exists s \in \mathbb{Z}) n = 2s$ . (Definição de  $P$ .)
5.  $(\exists r, s \in \mathbb{Z}) m = 2r \wedge n = 2s$ . (De 3 e 4.)
6.  $(\exists r, s \in \mathbb{Z}) m + n = 2(r + s)$ . (De 5, por álgebra.)
7.  $(\forall r, s \in \mathbb{Z}) (\exists t \in \mathbb{Z}) r + s = t$ . (Propriedade da soma.)
8.  $(\exists t \in \mathbb{Z}) m + n = 2t$ . (De 6 e 7.)
9.  $P(m + n)$ . (De 8 e definição de  $P$ . Tese.)
10.  $P(m) \wedge P(n) \rightarrow P(m + n)$ . (De 3, 4 e 9.)

**Fim.**

Supõe-se que cada um dos passos acima é um raciocínio simples o bastante para ser aceito como válido pelo leitor.

Estritamente falando, cada passo de uma demonstração deveria ser uma aplicação de uma *regra de inferência*, tirada de uma lista fixa de regras que todos os matemáticos 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  $p \rightarrow q$ , então podemos considerar a proposição  $q$  demonstrada. Mais geralmente, qualquer das equivalências e dominâncias vistas na seção 3.2.6 pode ser um passo de uma demonstração. Outras regras são necessárias para lidar com quantificadores, como passagem das afirmações 3 e 4 para 5 da prova acima (veja seções 4.4–4.5).

Na prática, os passos são escritos de maneira muito abreviada, na suposição de que o leitor consegue perceber as regras de inferência usadas nas entrelinhas, e explicitá-las se for preciso. Por exemplo, a demonstração acima normalmente seria escrita da seguinte maneira:

**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.

**Fim.**

**Exercício 4.1:** Demonstre que o produto de um inteiro par por um inteiro ímpar é par.

**Exercício 4.2:** Demonstre que se  $r$  é um número racional diferente de zero, então  $\frac{1}{r}$  é racional.

**Exercício 4.3:** Demonstre que, para quaisquer conjuntos  $A$ ,  $B$ ,  $C$  e  $D$ , as seguintes afirmações são sempre verdadeiras

- (a) Se  $x \in A$ ,  $(A \setminus B) \subseteq (C \cap D)$  e  $x \notin D$ , então  $x \in B$ .
- (b) Se  $B$  e  $C$  são disjuntos,  $A \subseteq C$  e  $x \in A$ , então  $x \notin B$ .
- (c) Se  $x \in C$  e  $(A \cap C) \subseteq B$ , então  $x \notin (A \setminus B)$ .

**Exercício 4.4:** Sejam  $X_1$ ,  $X_2$ ,  $Y_1$ ,  $Y_2$  subconjuntos de um conjunto  $U$ . Suponha que  $X_1 \cup X_2 = U$  e  $Y_1 \cap Y_2 = \{\}$ , que  $X_1 \subset Y_1$  e que  $X_2 \subset Y_2$ . Prove que  $X_1 = Y_1$  e  $X_2 = Y_2$ .

## 4.2.2 Método da contrapositiva

No *método da contrapositiva*, para provar a afirmação  $p \rightarrow q$ , supomos que a negação da tese  $\neg q$  é verdadeira, e procuramos uma sequência de deduções lógicas que termina com a negação da hipótese  $\neg p$ . Esta sequência de passos prova que  $(\neg q) \rightarrow (\neg p)$ . Como vimos na seção 3.2.3, esta afirmação é logicamente equivalente a  $p \rightarrow q$ , que portanto também está provada.

Por exemplo, digamos que é necessário provar a afirmação, num contexto em que sabemos que  $n$  é um inteiro:

**Teorema 4.2:** Se  $n^2$  é par, então  $n$  é par.

**Prova:**

Vamos demonstrar a contrapositiva dessa afirmação, ou seja, se  $n$  é ímpar,  $n^2$  é ímpar. Suponha que  $n$  é ímpar. Pela definição de “ímpar”, existe um inteiro  $k$  tal que  $n = 2k + 1$ . Portanto  $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2t + 1$ , onde  $t$  é  $2k^2 + 2k$ . Como  $t$  é um inteiro,  $2t + 1$  é ímpar. Concluimos que  $n^2$  é ímpar.

**Fim.**

Usando a notação formal, queremos provar que  $P(n^2) \rightarrow P(n)$ , onde  $P$  é o predicado “é par”. Vamos usar o predicado  $I$  (“é ímpar”) da definição 4.4, supondo já provado que ela equivale à definição 4.6:

**Prova:**

1. Suponha  $\neg P(n)$ . (Negação da tese.)
2.  $I(n)$ . (Definição 4.4.)
3.  $(\exists k \in \mathbb{Z}) n = 2k + 1$ . (De 2 e definição 4.6.)
4.  $(\exists k \in \mathbb{Z}) n^2 = (2k + 1)^2 = 4k^2 + 2k + 1 = 2(2k^2 + k) + 1$ . (De 3 e álgebra.)
5.  $(\forall k \in \mathbb{Z})(\exists t \in \mathbb{Z}) 2k^2 + k = t$ . (Props. da mult. e soma.)
6.  $(\exists t \in \mathbb{Z}) n^2 = 2t + 1$ . (De 4 e 5.)
7.  $I(n^2)$ . (De 6 e definição 4.6.)
8.  $\neg P(n^2)$ . (De 7 e definição 4.4. Negação da hipótese.)

9.  $\neg P(n) \rightarrow \neg P(n^2)$ . (De 1 e 8.)  
10.  $P(n^2) \rightarrow P(n)$ . (Equivalência lógica com 9.)

**Fim.**

**Exercício 4.5:** Demonstre que, para todo inteiro  $n$ , se  $n^3 + 5$  é ímpar, então  $n$  é par.

**Exercício 4.6:** Seja  $n$  um número inteiro da forma  $4k + 3$ ,  $k \geq 0$ . Demonstre que não existem inteiros  $x, y$  tais que  $x^2 + y^2 = n$ .

### 4.2.3 Método de redução ao absurdo

O *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  $(p \wedge \neg q) \rightarrow \mathbf{F}$ , vista na seção 3.2.3. Neste método, para provar a afirmação  $p \rightarrow q$ , supomos que tanto a hipótese  $p$  quanto a negação da tese  $\neg q$  são verdadeiras, e procuramos uma sequência de deduções lógicas que termina com uma contradição (uma afirmação com valor lógico  $\mathbf{F}$ ). Isto prova a afirmação  $(p \wedge \neg q) \rightarrow \mathbf{F}$ , e portanto também a afirmação equivalente a  $p \rightarrow q$ .

Por exemplo, suponha que, num contexto em que  $m$  e  $n$  são números inteiros, queremos provar a afirmação

**Teorema 4.3:** Se  $m$  e  $n$  são pares, então  $m + n$  é par

Uma prova por contradição seria:

**Prova:**

Suponha que  $m$  e  $n$  são pares e  $m + n$  é ímpar; vamos mostrar que estas suposições levam a uma contradição.

Pela definição de “par”, existem  $r$  e  $s$  inteiros tais que  $m = 2r$  e  $n = 2s$ . Pela definição de “ímpar”, existe um inteiro  $t$  tal que  $m + n = 2t + 1$ . Logo  $2r + 2s = 2t + 1$ , ou seja,  $r + s - t = 1/2$ . Isto é falso pois  $r + s - t$  é um inteiro.

Concluímos que, se  $m$  e  $n$  são pares,  $m + n$  não pode ser ímpar.

**Fim.**

Em notação formal, queremos provar que  $P(m) \wedge P(n) \rightarrow P(m + n)$ . Usando os predicados  $P$  e  $I$  definidos anteriormente, e supondo que as definições 4.4 e 4.6 são equivalentes, uma demonstração por contradição seria:

**Prova:**

1. Suponha  $P(m) \wedge P(n)$ . (Hipótese.)
2. Suponha  $\neg P(m + n)$ . (Negação da tese.)
3.  $P(m)$ . (De 1 por dominância.)

4.  $P(n)$ . (De 1 por dominância.)
5.  $(\exists r \in \mathbb{Z}) m = 2r$ . (De 3 e definição 4.3.)
6.  $(\exists s \in \mathbb{Z}) n = 2s$ . (De 4 e definição 4.3.)
7.  $(\exists r, s \in \mathbb{Z}) m = 2r \wedge n = 2s$ . (De 5 e 6.)
8.  $(\exists r, s \in \mathbb{Z}) m + n = 2(r + s)$ . (De 7 e álgebra.)
9.  $I(m + n)$ . (De 2 e definição 4.4.)
10.  $(\exists t \in \mathbb{Z}) m + n = 2t + 1$ . (De 9 e definição 4.6.)
11.  $(\exists r, s, t \in \mathbb{Z}) (m + n = 2(r + s) \wedge (m + n = 2t + 1))$ . (De 8 e 10.)
12.  $(\exists r, s, t \in \mathbb{Z}) 2(r + s) = 2t + 1$ . (De 11 e álgebra.)
13.  $(\exists r, s, t \in \mathbb{Z}) r + s - t = 1/2$ . (De 13 e álgebra.)
14.  $(\forall r, s, t \in \mathbb{Z}) (\exists k \in \mathbb{Z}) r + s - t = k$ . (Prop. da soma.)
15.  $(\exists k \in \mathbb{Z}) k = 1/2$ . (De 13 e 14.)
16.  $1/2 \in \mathbb{Z}$ . (De 15.)
17. **F**. (De 16 e definição de  $\mathbb{Z}$ .)
18.  $P(m) \wedge P(n) \wedge \neg P(m + n) \rightarrow \mathbf{F}$ . (De 1, 2 e 17.)
19.  $P(m) \wedge P(n) \rightarrow P(m + n)$ . (De 18 e equiv. lógica.)

**Fim.**

**Exercício 4.7:** Seja  $n$  um número inteiro da forma  $4k + 3$ ,  $k \geq 0$ . Escreva uma demonstração detalhada de não existem inteiros  $x, y$  tais que  $x^2 + y^2 = n$ .

**Exercício 4.8:** Demonstre que a soma de um número racional com um número irracional é um número irracional.

**Exercício 4.9:** Demonstre que o número  $\sqrt{2}$  é irracional.

**Exercício 4.10:** Sejam  $x, y, z$  números reais. Demonstre que pelo menos um deles é maior ou igual à média aritmética dos três.

**Exercício 4.11:** Demonstre que, se  $p$  é um inteiro ímpar, então a equação  $x^2 + x - p = 0$  não tem solução inteira.

**Exercício 4.12:** Demonstre que, se  $r$  é um número irracional, então  $\frac{1}{r}$  é irracional.

### 4.2.4 Implicação com tese conjuntiva

Para provar uma conjunção de duas afirmações  $p \wedge q$ , basta provar cada uma das afirmações separadamente.

Em particular, para provar uma implicação da forma  $p \rightarrow (q \wedge r)$ , podemos observar que ela equivale logicamente à afirmação “ $(p \rightarrow q) \wedge (p \rightarrow r)$ ”. Portanto, basta provar cada uma destas duas implicações separadamente. Se usarmos o método direto para provar cada implicação, supomos que  $p$  é verdadeira; provamos então  $q$ ; e provamos em seguida  $r$ .

Por exemplo, considere o teorema abaixo:

**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.**

Depois de provar a parte  $p \rightarrow q$ , podemos supor que  $q$  também é verdadeira, o que pode facilitar a prova de  $r$ . Ou seja, para provar  $p \rightarrow (q \wedge r)$ , podemos provar “ $p \rightarrow q$ ” e em seguida “ $(p \wedge q) \rightarrow r$ ”.

Essa análise pode ser estendida para tese com três ou mais termos, isto é,  $p \rightarrow (q_1 \wedge q_2 \wedge q_3 \cdots \wedge q_n)$  é equivalente a  $(p \rightarrow q_1) \wedge (p \rightarrow q_2) \wedge \cdots \wedge (p \rightarrow q_n)$ .

### 4.2.5 Implicação com hipótese disjuntiva

Suponha que é necessário provar uma implicação da forma  $(p \vee q) \rightarrow r$ , onde a hipótese é uma disjunção de duas afirmações. Pode-se verificar que esta implicação equivale a  $(p \rightarrow r) \wedge (q \rightarrow r)$ . (Note a troca de ‘ $\vee$ ’ por ‘ $\wedge$ ’.) Portanto, basta provar cada uma destas duas implicações separadamente.

Assim como na seção 4.2.4 podemos estender essa técnica para hipóteses com três ou mais termos. Observamos que  $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$  equivale a  $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$  e se cada uma das implicações for provada pelo método direto, a demonstração consistirá de uma lista de casos:

- Caso 1: Supomos que  $p_1$  vale. Provamos  $q$ .
- Caso 2: Supomos que  $p_2$  vale. provamos  $q$ .
- ...
- Caso  $n$ : Supomos que  $p_n$  vale. Provamos  $q$ .

Note que os casos não precisam ser mutuamente exclusivos. Por exemplo:

**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 (não exclusivos):

- 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.**

Muitas vezes os casos não são óbvios no enunciado, e tem que ser intuitivos. Por exemplo, considere este teorema:

**Teorema 4.6:** Se o número inteiro  $n$  não é divisível por 3, então seu quadrado tem resto 1 quando divisível por 3.

**Prova:**

Seja  $n$  um inteiro não divisível por 3. Podemos escrever  $n = 3p + r$ , onde  $p$  e  $r$  são inteiros e  $r$  é 1 ou 2. Então  $n^2 = (3p + r)^2 = 9p^2 + 6pr + r^2$ . Note que  $9p^2 + 6pr$  é um múltiplo de 3, portanto  $n^2 \equiv r^2$ . Temos dois casos:

- Caso 1:  $r = 1$ , então  $r^2 = 1$ , cujo resto na divisão por 3 é 1.
- Caso 2:  $r = 2$ , então  $r^2 = 4$ , cujo resto na divisão por 3 é 1.

Portanto, o resto de  $n^2$  é 1.

**Fim.**

**Exercício 4.13:** Demonstre que não existem soluções inteiras  $x$  e  $y$  para a equação  $x^2 + 3y^2 = 8$ .

**Exercício 4.14:** Demonstre que, se  $x$  e  $y$  são números reais, então  $\max(x, y) + \min(x, y) = x + y$

**Exercício 4.15:** Demonstre que o quadrado de um número inteiro, não divisível por 5, tem resto 1 ou 4 quando dividido por 5.

**Exercício 4.16:** Demonstre que o algarismo das unidades do quadrado de qualquer inteiro  $n$  é 0, 1, 4, 5, 6 ou 9.

**Exercício 4.17:** Demonstre que o algarismo das unidades da quarta potência de qualquer inteiro  $n$  é 0, 1, 5 ou 6.

**Exercício 4.18:** Demonstre que, para todo inteiro  $n$ , se  $n$  não é divisível nem por 2 nem por 3, então  $n^2 - 1$  é divisível por 24.

## 4.3 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.”

Para demonstrar este tipo de teorema, podemos usar a equivalência lógica entre as afirmações  $p \leftrightarrow q$  e  $(p \rightarrow q) \wedge (q \rightarrow p)$ . Ou seja, dividimos a demonstração em duas partes: (1) prova que  $p \rightarrow q$ ; (2) prova que  $q \rightarrow p$ . Por exemplo:

**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): 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): 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.**

Observe que neste exemplo usamos o método da contrapositiva na segunda parte. Com essa escolha, que é bastante comum, a prova de  $p \leftrightarrow q$  passa a ser (1) prova de que  $p \rightarrow q$ ; (2) prova de que  $(\neg p) \rightarrow (\neg q)$ .

**Exercício 4.19:** Prove que um número inteiro positivo  $n$  é ímpar se, e somente se,  $5n + 6$  é ímpar.

Este método pode ser generalizado para afirmações com três ou mais termos, como  $(p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge \cdots \wedge (p_{n-1} \leftrightarrow p_n)$ . Observe que esta afirmação significa que, no contexto corrente, todas as afirmações  $p_1, p_2, \dots, p_n$  são equivalentes. Esta afirmação é logicamente equivalente a  $(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)$ . Por exemplo:

**Teorema 4.8:** Para todo inteiro  $n$ , as seguintes afirmações são equivalentes:

1.  $n$  é um número par
2.  $n - 1$  é um número ímpar
3.  $n^2$  é um número par.

**Prova:**

Parte (1): vamos provar que se  $n$  é par então  $n - 1$  é ímpar. Como  $n$  é par, por definição existe um inteiro  $r$  tal que  $n = 2r$ . Logo,  $n - 1 = 2r - 1 = 2(r - 1) + 1$ . Como  $r - 1$  é inteiro, concluímos que  $n - 1$  é ímpar.

Parte (2) vamos provar que, se  $n - 1$  é ímpar, então  $n^2$  é par. Como  $n - 1$  é ímpar, existe um inteiro  $s$  tal que  $n - 1 = 2s + 1$ . Logo  $n = (2s + 1) + 1 = 2(s + 1)$ , e  $n^2 = (2(s + 1))^2 = 2(2(s + 1)^2)$ . Como  $2(s + 1)^2$  é inteiro, concluímos que  $n^2$  é par. Portanto  $n^2 = 4(k + 1)^2 = 2(2(k + 1)^2)$  é par.

Parte (3) vamos provar que, se  $n^2$  é par, então  $n$  é par. Esta afirmação é verdadeira pelo teorema 4.2.

**Fim.**

**Exercício 4.20:** Demonstre que as seguintes afirmações são equivalentes:

- (a)  $(\exists x) P(x) \wedge (\forall y) (P(y) \rightarrow y = x)$ .
- (b)  $(\exists x) (\forall y) P(y) \leftrightarrow y = x$ .
- (c)  $(\exists x) P(x) \wedge (\forall y) (\forall z) ((P(y) \wedge P(z)) \rightarrow y = z)$

**Exercício 4.21:** Demonstre que, se  $x$  e  $y$  são números reais, as seguintes afirmações são equivalentes:

- (a)  $x$  é menor que  $y$ .
- (b) A média aritmética de  $x$  e  $y$  é maior que  $x$ .
- (c) A média aritmética de  $x$  e  $y$  é menor que  $y$ .

Algumas vezes é possível demonstrar afirmações do tipo  $p \leftrightarrow q$  sem dividir as duas implicações. Por exemplo, em alguns casos é possível obter  $q$  a partir de  $p$  (ou vice-versa) através de uma cadeia de equivalências lógicas. Essa cadeia então é uma prova de que  $p \leftrightarrow q$ .

**Teorema 4.9:** Sejam  $A$  e  $B$  conjuntos. Prove que  $(A \subseteq \overline{B}) \leftrightarrow (A \cap B = \{\})$ .

**Prova:**

$A \subseteq \overline{B}$  é equivalente a  $(\forall x \in A) x \in \overline{B}$ ; que é equivalente a  $(\forall x \in A) x \notin B$ . Esta afirmação é equivalente a  $(\forall x)(x \in A) \rightarrow (x \notin B)$ , que é equivalente a  $(\forall x), \neg((x \in A) \wedge (x \in B))$ . Pela definição de interseção, esta afirmação equivale a  $A \cap B = \{\}$ .

**Fim.**

**Exercício 4.22:** Em cada item abaixo, encontre e prove uma condição necessária e suficiente sobre dois conjuntos  $A$  e  $B$  para que a fórmula seja verdadeira, qualquer que seja o conjunto  $X$ .

(a)  $A \cup (X \cap B) = (A \cup X) \cap B$ .

(b)  $A \setminus (X \setminus B) = (A \setminus X) \setminus B$

## 4.4 Regras para quantificadores universais

### 4.4.1 Instanciação universal

No decorrer de uma prova, uma vez que tivermos estabelecido a veracidade de uma afirmação do tipo  $(\forall x \in D) P(x)$ , podemos afirmar  $P(c)$  para qualquer elemento  $c$  do domínio  $D$ . Por exemplo, se tivermos provado que “para todo inteiro  $x$ ,  $2^x > x^2$ ”, podemos imediatamente concluir que  $2^{418} > 418^2$ . Esta regra é chamada de *instanciação universal*.

### 4.4.2 Generalização universal

Por outro lado, se o objetivo é provar uma afirmação do tipo  $(\forall x \in D) P(x)$ , podemos começar supondo que  $x$  é um elemento de  $D$  escolhido arbitrariamente, e omitir o quantificador no restante da prova. Se, com essa suposição, conseguirmos provar a afirmação  $P(x)$ , podemos concluir que o teorema original (com o quantificador) é verdadeiro. Este último passo é chamado de *generalização universal* ou *suspensão do quantificador universal*.

O mesmo método pode ser usado para vários quantificadores universais encaixados. Por exemplo:

**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.**

Ao usar este método, deve-se tomar cuidado para usar variáveis que não tenham significado já definido anteriormente.

**Exercício 4.23:** Prove a seguinte proposição:

$$(\forall x \in \mathbb{Z}) (\forall y \in \mathbb{Z}) (\forall k \in \mathbb{Z}) x + y = 7k \leftrightarrow 4x - 3y = 7(4k - y)$$

### 4.4.3 Demonstração por vacuidade

Lembramos que, se  $E$  é o conjunto vazio, a afirmação  $(\forall x \in E) Q(x)$  é verdadeira, qualquer que seja o predicado  $Q$ . Como vimos na seção 3.6.4 esta afirmação é verdadeira *por vacuidade*.

**Exemplo 4.1:** Todos os pares primos maiores que dois são quadrados perfeitos.

Esta afirmação é verdadeira por vacuidade pois não existem primos pares maiores que dois.

Uma maneira de provar uma afirmação da forma  $(\forall x \in D) P(x)$ , para um domínio arbitrário  $D$ , é mostrar que ela é equivalente a outra afirmação  $(\forall x \in E) Q(x)$ , para um certo domínio  $E$  e algum predicado  $Q$ ; e então mostrar que  $E$  é vazio.

Por exemplo, a afirmação  $(\forall x \in D) A(x) \rightarrow B(x)$  equivale a  $(\forall x \in E) B(x)$  onde  $E = \{x \in D : A(x)\}$ . Portanto, se mostrarmos que  $A(x)$  é falsa para todo  $x$  em  $D$ , a afirmação  $(\forall x \in D) A(x) \rightarrow B(x)$  estará provada por vacuidade — qualquer que seja o predicado  $B$ .

**Exemplo 4.2:** Para todo número inteiro  $x$ , se  $x^2 = 5$  então  $x$  é par.

Esta afirmação pode ser escrita  $(\forall x \in D) Q(x) \rightarrow P(x)$  onde  $D = \mathbb{Z}$ ,  $Q(x)$  significa “ $x^2 = 5$ ”, e  $P(x)$  é “ $x$  é par”. Ela é equivalente a “Para todo número inteiro  $x$  cujo quadrado é 5,  $x$  é par”, ou seja  $(\forall x \in E) P(x)$  onde  $E$  é o conjunto dos inteiros cujo quadrado é 5. Como  $E$  é vazio, a afirmação é verdadeira por vacuidade.

## 4.5 Regras para quantificadores existenciais

### 4.5.1 Instanciação existencial

Uma vez que estabelecemos a veracidade de uma proposição do tipo  $(\exists x \in D) P(x)$ , podemos supor, dali em diante, que a variável  $x$  é um dos elementos cuja existência é afirmada, e portanto que  $P(x)$  é verdadeira. Desse ponto em diante, a variável  $x$  passa a ser livre (veja seção 3.6.12). Esta regra é chamada de *instanciação existencial*.

Para evitar confusão, a variável  $x$  deve ser distinta de todas as outras variáveis livres criadas em passos anteriores da demonstração. Se necessário, pode-se trocar a variável do quantificador.

### 4.5.2 Demonstrações construtivas

Por outro lado, em muitas demonstrações é necessário provar a existência de objetos com uma propriedade particular, ou seja, são da forma  $(\exists x \in D) P(x)$ . Uma maneira de chegar a essa conclusão é através de uma *demonstração construtiva*, em que se exhibe um elemento específico  $a$  do domínio  $D$  (explicitamente, ou através de uma construção algorítmica) e prova-se que  $P(a)$  é verdadeira, para esse elemento. Por exemplo:

**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.**

(Três números  $x, y, z$  que satisfazem o teorema 4.11 são chamados de *tripla de inteiros pitagóricos* ou *tripla pitagórica*. Essas triplas correspondem a triângulos retângulos cujos lados têm comprimentos inteiros.)

Naturalmente, este método pode ser usado como parte de uma demonstração mais longa. Por exemplo:

**Teorema 4.12:** Para todo número natural  $n$ , se  $2^n - 1$  é primo, então  $n$  é primo.

**Prova:**

Seja  $n$  um número natural. Vamos provar a contrapositiva, ou seja, que se  $n$  não é um número primo, então  $2^n - 1$  não é primo. Se  $n = 0$  ou  $n = 1$ , nenhum dos dois é primo, e a afirmação é trivialmente verdadeira. Suponhamos então que  $n$  é maior que 1 e não é primo. Por definição, existem inteiros  $r$  e  $s$  maiores que 1 e menores que  $n$  tais que  $n = rs$ .

Vamos agora mostrar que existe um inteiro  $x$  que é divisor próprio de  $2^n - 1$ . Seja  $x = 2^s - 1$  e  $y = 1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}$ . Então

$$\begin{aligned} xy &= (2^s - 1)(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= 2^s(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= (2^s + 2^{2s} + \dots + 2^{rs}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= 2^{rs} - 1 \\ &= 2^n - 1. \end{aligned}$$

Uma vez que  $s$  é maior que 1 e menor que  $n$ , temos que  $x = 2^s - 1$  é maior que  $2^1 - 1 = 1$  e menor que  $2^n - 1$ . Ou seja,  $x$  é um divisor próprio de  $2^n - 1$ .

Concluimos portanto  $2^n - 1$  não é primo.

**Fim.**

Observe na demonstração acima, que a existência do divisor próprio de  $2^n - 1$  foi provada exibindo um  $x$  e provando que ele tem essa propriedade. Esta regra de inferência é também chamada de *generalização existencial*.

Outro exemplo de demonstração construtiva é a seguinte afirmação, conhecida como *teorema do deserto de primos*:

**Teorema 4.13:** 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

$$2 \text{ divide } x = (n + 1)! + 2, \quad (4.3)$$

$$3 \text{ divide } x + 1 = (n + 1)! + 3, \quad (4.4)$$

$$\dots \quad (4.5)$$

$$n + 1 \text{ divide } x + (n - 1) = (n + 1)! + n + 1. \quad (4.6)$$

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 4.24:** Existem 100 inteiros consecutivos que não são quadrados perfeitos.

**Exercício 4.25:** Demonstre que existem dois inteiros positivos consecutivos, tal que um é um cubo perfeito e o outro é um quadrado perfeito.

### 4.5.3 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*. Por exemplo:

**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  $x = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}}$  e  $y = \sqrt{2}$ . Então  $x^y = (((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}})^{\sqrt{2}} = ((\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}})^{\sqrt{2}} = ((\sqrt{2})^2)^{\sqrt{2}} = 2^{\sqrt{2}}$  que é racional.

**Fim.**

Observe que esta demonstração prova que existem valores de  $x$  e  $y$  que satisfazem a condição, mas deixa em suspenso o valor de  $x$  ( $\sqrt{2}$  ou  $(\sqrt{2})^{\sqrt{2}}$ ). Para tornar esta demonstração construtiva, teríamos que determinar se  $(\sqrt{2})^{\sqrt{2}}$  é racional ou não; mas este é um problema muito difícil.

Outro exemplo clássico de demonstração não construtiva de existência é o seguinte teorema, atribuído a Euclides (360 AC – 295 AC).

**Teorema 4.15:** Existem infinitos números primos.

**Prova:**

Vamos usar o método da demonstração por absurdo. Suponhamos que existem finitos números primos, a saber  $2, 3, 5, \dots, p$ . Seja  $n$  o inteiro  $(2 \times 3 \times 5 \times \dots \times p) + 1$ . Como  $n$  é maior que 1, ele tem algum fator primo  $r$ . Observe que  $n$  não é divisível por  $2, 3, 5, \dots, p$ , pois tem resto 1 quando dividido por qualquer desses números. Portanto,  $r$ , que é divisor de  $n$ , não pode ser nenhum dos primos listados acima. Isso contradiz a suposição de que essa lista contém todos os primos.

**Fim.**

#### 4.5.4 Demonstração de existência e unicidade

Lembramos que uma afirmação do tipo  $(\exists! x \in D) P(x)$  equivale logicamente a

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

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

- *Existência:* prova-se-se (construtivamente ou não) 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  $x$  cuja existência foi mostrada na primeira parte.

**Teorema 4.16:** Para todo número complexo  $z$  diferente de zero, existe um único número complexo  $x$  tal que  $zx = 1$ .

**Prova:**

Seja  $z$  um número complexo qualquer, diferente de zero. Por definição, existem  $a$  e  $b$  em  $\mathbb{R}$  tais que  $z = a + b\mathbf{i}$ , onde  $\mathbf{i}$  é um elemento de  $\mathbb{C}$  tal que  $\mathbf{i}^2 = -1$ .

Vamos primeiro mostrar que existe pelo menos um  $x$  em  $\mathbb{C}$  tal que  $zx = 1$ . Como  $z$  é diferente de zero, pelo menos um dos números  $a$  e  $b$  é diferente de zero. Isso implica que  $a^2 + b^2$  é positivo. Seja então  $x = (a - b\mathbf{i})/(a^2 + b^2)$ . Temos que

$$\begin{aligned}zx &= (a + b\mathbf{i})((a - b\mathbf{i})/(a^2 + b^2)) \\&= (a^2 - ab\mathbf{i} + ab\mathbf{i} - b^2\mathbf{i}^2)/(a^2 + b^2) \\&= (a^2 + b^2)/(a^2 + b^2) \\&= 1.\end{aligned}$$

Suponha agora que  $y$  é um número complexo qualquer tal que  $zy = 1$ ; vamos mostrar que ele é igual a  $x$ . Multiplicando os dois lados da equação  $zy = 1$  por  $x$  temos  $(zy)x = x$ . Como a multiplicação de números complexos é associativa e comutativa, esta afirmação equivale a  $(zx)y = x$ . Como  $zx = 1$ , concluímos que  $y = x$ .

**Fim.**

**Exercício 4.26:** Demonstre que, se  $m$  e  $n$  são inteiros distintos e  $m - n$  é par, então existe um único inteiro  $r$  tal que  $|m - r| = |n - r|$

**Exercício 4.27:** Demonstre que, se  $r$  é um número irracional, então existe um único inteiro  $n$  tal que a distância entre  $r$  e  $n$  é menor do que  $1/2$ .

**Exercício 4.28:** Prove que para qualquer matriz  $A 2 \times 2$  de números reais com determinante  $|a|$  não nulo existe uma única matriz  $B 2 \times 2$  de números reais tal que

$$AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

### 4.5.5 Demonstração de falsidade por contra-exemplo

Demonstrações de existência são usadas, em particular, para refutar conjecturas 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  $P(x)$ , e que portanto mostra a falsidade da conjectura, é um *contra-exemplo* para a mesma.

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  $P(11) = 2^{11} - 1 = 2047 = 23 \times 89$ .

**Exercício 4.29:** Demonstre (por meio de contra-exemplos) que as seguintes conjecturas são falsas:

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

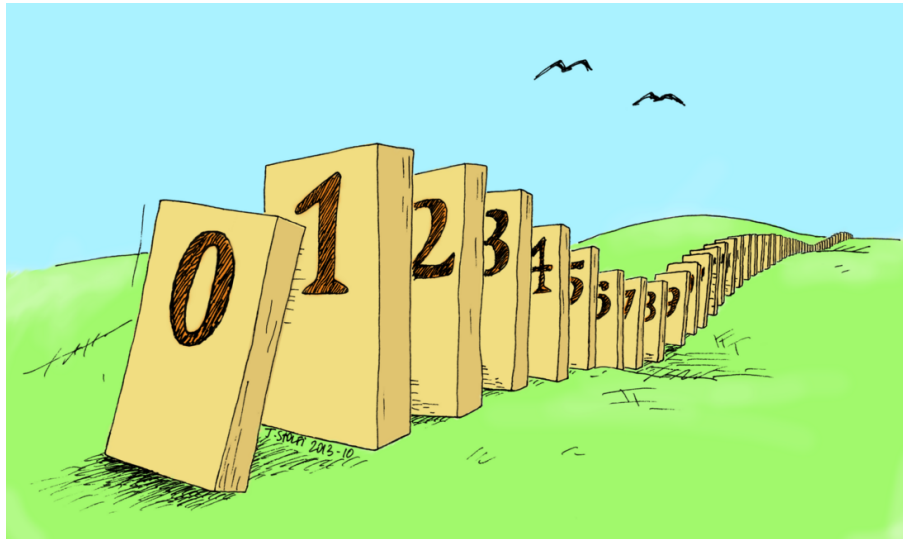
**Exercício 4.30:** Em cada caso abaixo, demonstre (por meio de contra-exemplo) que as duas fórmulas *não* são equivalentes:

- (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  $((\exists x \in D) P(x)) \wedge (\exists x \in D) Q(x)$ .



# Capítulo 5

## Indução Matemática



## 5.1 Introdução

Seja  $P$  um predicado definido sobre os números naturais; ou seja,  $P(n)$  é uma proposição envolvendo uma variável  $n$ , que é verdadeira ou falsa quando substituímos  $n$  por um número natural dado qualquer. Exemplos:

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  $P(1), P(2), \dots, P(40)$  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.  $P(n)$ : “ $1 + 3 + 5 + \dots + (2n + 1) = (n + 1)^2$ .” Será que conseguiremos encontrar algum  $m$  tal que  $P(m)$  seja falso?

Depois de algumas tentativas começamos a desconfiar que a sentença  $P(n)$  do exemplo 4 é verdadeira para todo  $n \in \mathbb{N}$ . Como poderíamos provar isso? Obviamente não podemos testar, um por um, todos os valores de  $n$ , pois há infinitos números naturais. Algumas proposições  $P(n)$ , como no exemplo 3, podem ser demonstradas usando álgebra e as técnicas estudadas anteriormente. No exemplo 4, como o lado esquerdo da igualdade não é uma forma fechada, ela não pode ser tratada algebricamente. Para estes casos, vamos precisar de uma nova técnica, a *demonstração por indução matemática*.

## 5.2 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 5.1:** Seja  $P$  um predicado definido 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  $n \in \mathbb{N}$ .

Ou, em notação formal, podemos tomar a afirmação abaixo como um axioma, para qualquer predicado  $P$ :

$$(P(0) \wedge (\forall k \in \mathbb{N}) P(k) \rightarrow P(k + 1)) \rightarrow (\forall n \in \mathbb{N}) P(n) \quad (5.1)$$

Este princípio pode ser visto como uma propriedade fundamental dos números naturais. Estes podem ser definidos por um conjunto de axiomas enunciados pelo matemático Giuseppe Peano em 1889; e um dos postulados de Peano é equivalente ao PIM.

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

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

3. *Passo da Indução:* Com essa suposição, provar que  $P(k + 1)$  é verdade.

**Exemplo 5.1:** Provar que, para todo  $n \geq 0$ , a soma dos primeiros  $n$  números naturais ímpares é  $n^2$ . Isto é, que:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \quad (5.2)$$

**Prova:**

Seja  $P$  o predicado tal que  $P(n)$  representa a equação (5.2), ou seja, a afirmação “a soma dos  $n$  primeiros números ímpares é  $n^2$ ”.

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

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

3. *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

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

Mas o lado direito é  $k^2 + 2k + 1$  que é  $(k + 1)^2$  Isto mostra que  $P(k + 1)$  é verdade, toda vez que  $P(k)$  é verdade.

Portanto, pelo princípio da indução matemática, concluímos que  $P(n)$ , a fórmula (5.2), é verdade para todo natural  $n$ .

**Fim.**

**Exemplo 5.2:** Dizemos que um conjunto de  $n$  retas no plano *estão em posição geral* (PG) se não possui duas retas paralelas e nem três retas se interceptando num mesmo ponto. Vamos provar por indução que um conjunto de  $n$  retas em PG divide o plano em  $n(n+1)/2 + 1$  regiões.

**Prova:**

Seja  $R$  a função definida sobre  $\mathbb{N}$  tal que  $R(n) = n(n+1)/2 + 1$ , e seja  $P$  o predicado tal que  $P(n)$  significa “todo conjunto de  $n$  retas em PG no plano divide o mesmo em  $R(n)$  regiões.”

1. *Base:* Se não há nenhuma reta ( $n = 0$ ), há apenas uma região. Como  $R(0) = 0(0+1)/2 + 1 = 1$ , a fórmula é válida neste caso.
2. *Hipótese de indução:* Suponhamos que  $P(k)$  é verdade para algum natural  $k$ , isto é, quaisquer  $k$  retas em PG dividem o plano em  $R(k) = k(k+1)/2 + 1$  regiões.
3. *Passo da indução:* temos que provar  $P(k+1)$ , isto é, quaisquer  $k+1$  retas em PG definem  $R(k+1) = (k+1)(k+2)/2 + 1$  regiões.

Sejam  $L_1, L_2, \dots, L_{k+1}$  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  $L_1, L_2, \dots, L_k$  estão em posição geral, podemos usar a hipótese de indução. Obtemos

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

**Fim.**

### 5.2.1 Formulação do PIM usando conjuntos

O Princípio da Indução Matemática também pode ser enunciando usando a linguagem da teoria de conjuntos:

**Teorema 5.1:** Seja  $S$  um subconjunto de  $\mathbb{N}$  tal que

1.  $0 \in S$ , e
2. sempre que  $k \in S$ , para algum  $k \in \mathbb{N}$ , temos que  $k + 1 \in S$ .

Então  $S = \mathbb{N}$ .

Este teorema pode ser facilmente mostrado usando o PIM. Por outro lado, podemos demonstrar o PIM supondo que o teorema acima é verdade, e considerando o conjunto  $S$  de todos os naturais  $n$  para os quais  $P(n)$  é verdadeira.

**Exercício 5.1:** Prove que  $(\forall n \in \mathbb{N}) 2^0 + 2^{-1} + 2^{-2} + 2^{-3} + \cdots + 2^{-n} \leq 2$ .

**Exercício 5.2:** Prove que  $(\forall n \in \mathbb{N}) 1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} = 1 + (n-1)2^n$

**Exercício 5.3:** Prove que  $(\forall n \in \mathbb{N}) 2^n > n$ .

**Exercício 5.4:** Prove que  $(\forall n \in \mathbb{N} \setminus \{0\}) n^n \geq n!$  (onde  $n!$  denota o fatorial de um inteiro  $n$ ; veja seção 8.10).

**Exercício 5.5:** Prove que, para todo  $n \in \mathbb{N}$ ,  $9^n - 1$  é divisível por 8.

**Exercício 5.6:** Prove que, para todo  $n \in \mathbb{N}$ ,  $a^n - 1$  é divisível por  $a - 1$  para todo número inteiro  $a > 1$ .

**Exercício 5.7:** Prove que, para todo  $n \in \mathbb{N}$ ,  $11^{n+2} + 12^{2n+1}$  é divisível por 133.

**Exercício 5.8:** Prove que, para todo  $n \in \mathbb{N}$ ,  $\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$  é um número inteiro.

**Exercício 5.9:** Suponha que uma caixa contém  $p$  bolas vermelhas e  $q$  bolas amarelas, e que o seguinte procedimento é repetido até sobrar uma única bola na caixa: “Retire duas bolas da caixa; se elas tiverem a mesma cor, coloque uma bola vermelha na caixa; se elas tiverem cores diferentes, coloque uma bola amarela na caixa. Em ambos os casos, não devolva à caixa as bolas retiradas.” Descubra qual é a cor da bola que ficará na caixa, em função de  $p$  e  $q$ . Demonstre, por indução no número de bolas  $p + q$ , que a sua resposta está correta.

**Exercício 5.10:** Prove que, para todo  $n \in \mathbb{N}$ ,  $2^{2n} - 1$  é um múltiplo de 3.

### 5.3 Generalizações da Indução Matemática

Há muitas variações do princípio da indução matemática, que são no fundo equivalentes, mas podem tornar algumas demonstrações mais simples.

### 5.3.1 Base genérica

Muitas vezes precisamos provar que um predicado  $P$  é verdadeiro 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  $Q$  tal que  $Q(m)$  é 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 justifica o teorema geral abaixo, que nos permite provar tais afirmações por indução matemática de maneira mais direta, usando  $n_0$  como base em vez de 0:

**Teorema 5.2:** Seja  $n_0$  um número natural, e  $P$  um predicado definido sobre o conjunto dos naturais maiores ou iguais a  $n_0$ . 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 5.3:** Prove que  $n^2 > 3n$  para todo  $n \in \mathbb{N}$  com  $n \geq 4$ .

**Prova:**

Seja  $P$  o predicado tal que  $P(n)$  significa “ $n^2 > 3n$ ”.

1. *Base*: Para  $n = 4$ ,  $P(n)$  é verdade, pois  $n^2 = 16$ ,  $3n = 12$ , e  $16 > 12$ .
2. *Hipótese de indução*: Suponhamos que para algum  $k \geq 4$ ,  $P(k)$  é verdade; isto é,  $k^2 > 3k$ .
3. *Passo da indução*: Vamos provar que  $P(k + 1)$  é verdade isto é,  $(k + 1)^2 > 3(k + 1)$ .  
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.**

### 5.3.2 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  $P(k) \rightarrow P(k + 1)$ . Nesse caso, o roteiro é dado pelo seguinte teorema geral:

**Teorema 5.3:** Seja  $n_0$  um número natural,  $p$  um inteiro positivo, e  $P$  um predicado definido para todos os naturais maiores ou iguais a  $n_0$ . Se

1.  $P(n_0), P(n_0 + 1), \dots, P(n_0 + p - 1)$  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  $n \geq n_0$ .

Observe que, neste caso, a prova da base da indução deve valer para  $p$  inteiros consecutivos,  $(n_0, n_0 + 1, \dots, n_0 + p - 1)$ , e não apenas  $n_0$ .

**Exemplo 5.4:** Prove que qualquer valor postal inteiro  $n \geq 8$  pode ser obtido utilizando apenas selos com valores 3 e/ou 5.

Podemos provar esta afirmação usando o teorema da indução geral 5.3, com incremento  $p = 3$ :

**Prova:**

Seja  $P$  o predicado tal que  $P(n)$  significa “o valor postal inteiro  $n$  pode ser obtido com selos de valores 3 e/ou 5”.

1. *Bases:* Como  $8 = 5 + 3$ ,  $9 = 3 + 3 + 3$  e  $10 = 5 + 5$  temos que  $P(8)$ ,  $P(9)$  e  $P(10)$  são verdade.
2. *Hipótese de indução:* Suponhamos que  $P(k)$  é verdade para algum valor  $k \geq 8$ .
3. *Passo:* Vamos provar que  $P(k + 3)$  é verdade. Pela hipótese de indução, o valor  $k$  pode ser obtido com selos de valor 3 e/ou 5. Então podemos obter o valor  $k + 3$  acrescentando um selo de valor 3 a esses selos.

**Fim.**

### 5.3.3 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:

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

### 5.3.4 Exercícios

**Exercício 5.11:** Prove que a soma dos ângulos internos de um polígono convexo de  $n$  vértices,  $n \geq 3$ , é  $180(n - 2)$ .

**Exercício 5.12:** Prove que o número de diagonais de um polígono convexo de  $n$  lados,  $n \geq 3$ , é dado por  $d_n = \frac{n(n-3)}{2}$ .

**Exercício 5.13:** Seja  $C$  um conjunto com  $n \geq 2$  elementos. Prove que  $C$  tem  $n(n - 1)/2$  subconjuntos com exatamente dois elementos.

**Exercício 5.14:** Prove que a soma dos cubos de três números naturais consecutivos é sempre divisível por 9.

**Exercício 5.15:** Prove que  $(\forall n \in \mathbb{N}) n \geq 13 \rightarrow n^2 < (3/2)^n$ .

**Exercício 5.16:** Prove que todo valor inteiro  $n \geq 5$ , em dinheiro, pode ser obtido usando somente notas de 2 ou de 5 reais.

**Exercício 5.17:** Prove que, para todo inteiro  $n \geq 2$ ,  $\frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} \cdots \frac{1}{2n} > \frac{13}{24}$ .

**Exercício 5.18:** Prove que, para todo inteiro  $n \geq 3$ ,  $n^2 - 7n + 12 \geq 0$ .

**Exercício 5.19:** Prove que, para todo inteiro  $n > 1$ ,  $2^{n+1} < 3^n$ .

**Exercício 5.20:** Prove que,  $(\forall n \in \mathbb{N} - \{0\}) \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots \frac{1}{n(n+1)} = \frac{n}{n+1}$ .

## 5.4 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.

**Exemplo 5.5:** Todos os cavalos têm a mesma cor.

**Prova:**

Seja  $P$  o predicado tal que  $P(n)$  significa “em qualquer conjunto de  $n$  cavalos, todos os cavalos têm a mesma cor.” Vamos provar que  $P(n)$  é verdadeira para todo  $n \geq 1$ , por indução.

1. *Base:* Para  $n = 1$  a sentença  $P(n)$  é verdadeira.
2. *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.
3. *Passo de indução:* Vamos provar que, em todo conjunto com  $k + 1$  cavalos, todos têm a mesma cor. Considere um conjunto  $C = \{c_1, c_2, \dots, c_k, c_{k+1}\}$  com  $k + 1$  cavalos. Podemos escrever o conjunto  $C$  como união de dois conjuntos, cada um com  $k$  cavalos, da seguinte forma:

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

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.

**Fim.**

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:

**Exemplo 5.6:** Todos os números naturais são iguais.

**Prova:**

Seja  $P$  o predicado tal que  $P(n)$  significa “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.

1. *Base:*  $P(0)$  é obviamente verdadeira.
2. *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.
3. *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 igualdade temos  $k = k + 1$ . Portanto  $P(k + 1)$  também é verdadeira.

**Fim.**

O próximo exemplo mostra a necessidade de provar a base da indução:

**Exemplo 5.7:** Para todo número natural  $n \geq 1$ , o número  $n^2 + n$  é ímpar.

**Prova:**

1. *Hipótese de indução*: Suponha que  $k^2 + k$  é ímpar para algum  $k \geq 1$ .
2. *Passo de indução*: Vamos provar que  $(k + 1)^2 + (k + 1)$  é ímpar. Observe que

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

Este resultado é ímpar, pois  $(k^2 + k)$  é ímpar pela hipótese de indução,  $2(k + 1)$  é par, e um número ímpar somado com um número par é ímpar.

**Fim.**

O leitor pode verificar que a afirmação “provada” acima não é verdadeira.

Outro erro comum é ilustrado pelo exemplo seguinte:

**Exemplo 5.8:** Todo polinômio de grau  $n \geq 1$  tem exatamente  $n$  raízes reais distintas.

**Prova:**

1. *Base da indução*:  $P(1)$  diz que todo polinômio de grau 1 tem exatamente uma raiz real. De fato, todo polinômio de grau 1 tem a forma  $ax + b$  com  $a \neq 0$ , e o número real  $-b/a$  é sua única raiz.
2. *Hipótese de indução*: Suponha que, para algum inteiro  $k \geq 1$ ,  $P(k)$  é verdadeira; isto é, todo polinômio de grau  $k$  tem exatamente  $k$  raízes reais distintas.
3. *Passo de indução*: Vamos provar que  $P(k + 1)$  é verdade. Seja  $F$  um polinômio de grau  $k$ , com variável  $x$ . Pela hipótese da indução,  $F$  tem exatamente  $k$  raízes reais distintas. Seja  $r$  a maior dessas raízes, e seja  $G = (x - (r + 1))F$ . Pode-se ver que  $G$  é um polinômio de grau  $k + 1$ . Toda raiz de  $F$  é raiz de  $G$ , e  $r + 1$  (que é distinta de todas essas) também é. Por outro lado, toda raiz de  $G$  deve ser raiz de  $(x - (r + 1))$  ou de  $F$ . Portanto todo polinômio de grau  $k + 1$  tem exatamente  $k + 1$  raízes distintas;

**Fim.**

Obviamente essa afirmação é falsa, pois o polinômio  $x^2 + 1$ , por exemplo, não tem nenhuma raiz real. Onde está o erro da demonstração? Observe que no passo da indução precisaríamos provar a afirmação para *qualquer* polinômio de grau  $k + 1$ , mas em vez disso só provamos para os polinômios que podem ser obtidos pelo produto de qualquer polinômio de grau  $k$  por um certo fator de grau 1. Acontece que existem polinômios de grau  $k + 1$  (como  $x^2 + 1$ ) que não podem ser obtidos desta forma.

Mais formalmente, a afirmação que queremos provar pode ser escrita como  $(\forall n \in \mathbb{N})(\forall F \in \mathcal{P}_n) Q(F, n)$ , onde  $\mathcal{P}_n$  é o conjunto de todos os polinômios de grau  $n$ , e  $Q(F, n)$  é o predicado “ $F$  tem  $n$  raízes reais distintas.” A indução se aplica ao primeiro quantificador, mas não ao segundo. Na demonstração (incorreta) acima, a hipótese de indução é “suponha que, para algum inteiro  $k \geq 1$ ,  $(\forall F \in \mathcal{P}_k) Q(F, k)$ . No passo de indução, usamos instanciação universal para dizer que “seja um  $F$  qualquer em  $\mathcal{P}_k$ , pela hipótese de indução temos  $Q(F, k)$ ”. Construímos então *um* polinômio  $G$  de  $\mathcal{P}_{k+1}$  tal que  $Q(G, k+1)$ . Entretanto, como este  $G$  não foi escolhido *arbitrariamente* em  $\mathcal{P}_{k+1}$ , não podemos usar a generalização universal para concluir  $(\forall G \in \mathcal{P}_{k+1}) Q(G, k + 1)$ .

## 5.5 Mais exemplos de indução matemática

**Exemplo 5.9:** [Desigualdade de Bernoulli] Se  $c$  é um número real tal que  $c > -1$  e  $c \neq 0$ , então para todo número natural  $n \geq 2$  vale a desigualdade

$$(1 + c)^n > 1 + nc$$

**Prova:**

1. *Base:* Para  $n = 2$  a proposição é verdadeira pois

$$(1 + c)^2 = 1 + 2c + c^2 > 1 + 2c.$$

2. *Hipótese de indução:* Para um dado  $k \geq 2$ ,  $(1 + c)^k > 1 + kc$ .

3. *Passo:* Provar que  $(1 + c)^{k+1} > 1 + (k + 1)c$ .

Como  $(1 + c)^{k+1} = (1 + c)^k(1 + c)$ , pela hipótese de indução temos que

$$(1 + c)^{k+1} > (1 + kc)(1 + c) = 1 + (k + 1)c + kc^2 > 1 + (k + 1)c.$$

Logo a desigualdade é válida para  $k + 1$ . Portanto a desigualdade vale para todo  $n \geq 2$

**Fim.**

**Exemplo 5.10:** [Conjunto Potência] Seja  $A$  um conjunto com  $n$  elementos. Prove que o conjunto potência  $\mathcal{P}(A)$  tem  $2^n$  elementos.

**Prova:**

1. *Base:* Se  $n = 0$  temos que o conjunto  $A$  é vazio e portanto  $\mathcal{P}(A) = \{\{\}\}$ . Logo o número de elementos de  $\mathcal{P}(A)$  é igual a  $1 = 2^0$ .
2. *Hipótese de indução:* Para um dado conjunto  $A$  com  $k \geq 0$  elementos temos que o conjunto potência  $\mathcal{P}(A)$  tem  $2^k$  elementos.

3. *Passo*: Provar que para um conjunto  $A$  com  $k + 1$  elementos o conjunto  $\mathcal{P}(A)$  tem  $2^{k+1}$  elementos. Seja  $A$  um conjunto com  $k + 1$  elementos. Como  $k \geq 0$ ,  $A$  tem pelo menos um elemento. Seja  $a$  este elemento. Considere o conjunto  $B = A \setminus \{a\}$ . Logo  $B$  tem  $k$  elementos, o que, pela hipótese de indução, implica que  $\mathcal{P}(B)$  tem  $2^k$  elementos. O conjunto  $\mathcal{P}(A)$  pode ser dividido em dois sub-conjuntos, ou seja

$$\mathcal{P}(A) = \mathcal{P}(B) \cup \{ C \cup \{a\} : C \in \mathcal{P}(B) \}.$$

Como  $\mathcal{P}(B) \cap \{ C \cup \{a\} : C \in \mathcal{P}(B) \} = \{ \}$  e

$$|\mathcal{P}(B)| = |\{ C \cup \{a\} : C \in \mathcal{P}(B) \}| = 2^k$$

concluimos que o número de elementos de  $\mathcal{P}(A)$  é  $2^{k+1}$ , ou seja  $|\mathcal{P}(A)| = 2^{k+1}$ .

**Fim.**

**Exemplo 5.11:**[Descobrimo 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:**

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

3. *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.**

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

Vamos provar este princípio usando indução matemática no número  $n$  de caixas.

**Prova:**

1. *Base*: Para  $n = 1$  o resultado é trivial pois, se há mais de um objeto, essa caixa terá mais de um objeto.
2. *Hipótese de indução*: Suponhamos que o resultado é válido para algum número  $k \geq 1$  de caixas, contendo mais do que  $k$  objetos.
3. *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.**

## 5.6 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. Na seção 5.9 provaremos a equivalência desses dois princípios.

**Teorema 5.5:** Seja  $P$  um predicado definido sobre  $\mathbb{N}$ . Suponha que

1.  $P(0)$  é verdade; e
2. para todo  $k \in \mathbb{N}$ ,  $((\forall i \in \mathbb{N}) i \leq k \rightarrow P(i)) \rightarrow P(k + 1)$ ,

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

Ou seja, ao provar o caso geral  $P(k + 1)$ , podemos supor já provados *todos* os casos anteriores, desde a base  $P(0)$  até  $P(k)$ . Mais precisamente, para provar que “ $(\forall n \in \mathbb{N}) P(n)$ ” é verdadeiro, usando indução completa, devemos proceder da seguinte forma:

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

### Exemplo 5.12:

**Teorema 5.6:** Todo número natural  $m > 0$  pode ser escrito como soma de distintas potências de 2, isto é, existem números inteiros  $n_1, n_2, \dots, n_r$ , com  $0 \leq n_1 < n_2 < \dots < n_r$ , tais que

$$m = 2^{n_1} + 2^{n_2} + \dots + 2^{n_r}$$

Isto equivale a dizer que todo número natural pode ser representado na base 2 com algarismos 0 e 1.

### Prova:

Seja  $P$  o predicado sobre números naturais tal que  $P(n)$  significa “ $n$  pode ser escrito como soma de potências distintas de 2”. Vamos provar  $(\forall n \in \mathbb{N}) P(n)$  por indução completa.

1. *Base*: A afirmação  $P(0)$  significa “zero é soma de potências distintas de 2”. De fato, a soma de um conjunto vazio de tais potências é zero. Portanto  $P(0)$  é verdade.

2. *Hipótese de indução:* Suponha que, para um natural  $k \geq 0$ , as afirmações  $P(0)$ ,  $P(1)$ ,  $\dots$ ,  $P(k)$  são todas verdadeiras.
3. *Passo da indução:* Vamos provar que, nesse caso,  $P(k+1)$  também é verdadeiro. Seja  $A$  o conjunto de todas as potências de 2 menores ou iguais a  $k+1$ . Como  $k+1 \geq 1$ , a potência  $2^0 = 1$  está em  $A$ , portanto  $A$  não é vazio. Seja  $2^t$  a maior das potências em  $A$ , e seja  $m = k+1 - 2^t$ . Note que  $m$  é natural e  $m \leq k$  pois  $2^t \geq 1$ . Pela hipótese de indução,  $m$  é soma de um certo conjunto  $B$  de potências distintas de 2. Portanto  $k+1$  é a soma das potências em  $B$ , mais  $2^t$ . Precisamos porém demonstrar que  $2^t$  é distinta de todas as potências em  $B$ . Para ver isso, note que  $2^{t+1} = 2^t + 2^t$  deve ser maior que  $k+1 = 2^t + m$ , o que implica  $m < 2^t$ . Mas todos elementos de  $B$  são menores ou iguais a  $m$ , portanto são menores que  $2^t$ .

**Fim.**

### 5.6.1 Indução completa sem prova da base

Formalmente, numa prova usando o princípio da indução completa, é possível omitir prova da base da indução. Para isso seguimos o roteiro

1. *Hipótese de indução:* Supor que, para algum  $k \in \mathbb{N}$ ,  $P(i)$  é verdade para todo inteiro  $i$  com  $0 \leq i < k$ .
2. *Passo da indução:* Provar que  $P(k)$  é verdade.

Note que a hipótese de indução diz “ $0 \leq i < k$ ” em vez de “ $0 \leq i \leq k$ ”, e o objetivo é provar  $P(k)$  em vez de  $P(k + 1)$  (como na seção 5.3.3). Este roteiro fornece uma prova válida porque, quando  $k = 0$ , o conjunto dos inteiros  $i$  com  $0 \leq i < k$  é vazio, portanto a hipótese de indução é verdadeira por vacuidade. Porém, na prova do passo de indução, temos que lembrar que  $k$  pode ser zero, o que pode exigir um tratamento especial para esse caso. Ou seja, a demonstração de  $P(0)$ , que seria tratada na base, passa a ser tratada como um caso particular do passo. Portanto esta alternativa nem sempre é mais simples e fácil do que tratar o caso base separadamente.

## 5.6.2 Indução completa com base genérica

Como no *PIM*, podemos generalizar este princípio para provar afirmações do tipo “ $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow P(n)$ ”. Neste caso, a base da indução é  $P(n_0)$  em vez de  $P(0)$ , e na hipótese de indução supomos provados  $P(n_0), P(n_0 + 1), \dots, P(k)$  para algum  $k \in \mathbb{N}$ . Isto equivale a definir um predicado  $Q$  tal que  $Q(n) = P(n + n_0)$ , para todo  $n \in \mathbb{N}$ ; e então provar “ $(\forall n \in \mathbb{N}) Q(n)$ ” pelo PIC.

**Exemplo 5.13:** 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  $P$  o predicado tal que  $P(n)$  significa “ $n$  é primo ou é um produto de primos.” Vamos provar que  $(\forall n \in \mathbb{N}) n \geq 2 \rightarrow P(n)$ , por indução completa.

1. *Base:*  $P(2)$  é verdade pois 2 é primo.

2. *Hipótese de indução*: Suponha que, para algum  $k \geq 2$ ,  $P(i)$  é verdade para todo  $i \in \mathbb{N}$  com  $2 \leq i \leq k$ .
3. *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.**

### 5.6.3 Indução completa com vários casos na base

Na demonstração pelo PIC, pode ser conveniente tratar vários valores consecutivos no caso base. Ou seja, para provar “ $(\forall n \in \mathbb{N}) P(n)$ ”, podemos proceder como segue:

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

Observe que, neste caso, na demonstração do passo de indução podemos supor que  $k \geq p$ .

Esta variante da prova pelo PIC pode ser usada também com base genérica  $n_0$  (seção 5.6.2). Nesse caso, provamos primeiro as afirmações  $P(n_0)$ ,  $P(n_0 + 1)$ ,  $\dots$ ,  $P(n_0 + p)$ , para algum  $p \in \mathbb{N}$ ; e na hipótese de indução, supomos que  $P(i)$  é verdade para todo  $i \in \mathbb{N}$  entre  $n_0$  e algum inteiro  $k \geq n_0 + p$ .

**Exemplo 5.14:** Os números de Lucas  $A_1, A_2, \dots$  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  $A_n < \left(\frac{7}{4}\right)^n$  para todo inteiro  $n \geq 1$ , por indução completa.

**Prova:**

Seja  $P$  o predicado tal que  $P(n)$  significa “ $A_n < \left(\frac{7}{4}\right)^n$ .”

1. *Base:*

(a)  $P(1)$  é verdade pois  $A_1 = 1 < \frac{7}{4}$ .

(b)  $P(2)$  é verdade pois  $A_2 = 3 < \left(\frac{7}{4}\right)^2 = \frac{49}{16}$ .

2. *Hipótese de indução:* Suponha que, para algum inteiro  $k \geq 2$ ,  $P(i)$  é verdade para todo  $i \in \mathbb{N}$  com  $1 \leq i \leq k$ .

3. *Passo da indução:* Vamos provar que  $P(k + 1)$  também é verdade, ou seja  $A_{k+1} < \left(\frac{7}{4}\right)^{k+1}$ . 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,

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

Fim.

### 5.6.4 Formulação do PIC usando conjuntos

O princípio da indução completa também pode ser enunciando usando a linguagem da teoria de conjuntos:

**Teorema 5.7:** Seja  $S$  um subconjunto de  $\mathbb{N}$  tal que

1.  $0 \in S$ , e
2. para todo  $k \in \mathbb{N}$ ,  $\{0, 1, 2, \dots, k\} \subseteq S \rightarrow k + 1 \in S$ .

Então  $S = \mathbb{N}$ .

## 5.7 Exercícios

**Exercício 5.21:** 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  $10 = 3 + 7$ .

**Exercício 5.22:** Sejam  $m$  moedas, uma das quais é falsa e tem peso diferente das demais (mais leve). Use o exercício anterior para provar, por indução, que bastam  $n_r$  pesagens com uma balança de pratos para descobrir a moeda falsa.

**Exercício 5.23:** Os números de Fibonacci  $F_0, F_1, F_2, \dots$  são definidos pelas seguintes regras:  $F_0 = 0$ ,  $F_1 = 1$ , e  $F_n = F_{n-1} + F_{n-2}$  para todo número natural  $n$  maior ou igual a 2. Prove, por indução, que

(a)  $(\forall n \in \mathbb{N}) F_n < (\frac{13}{8})^n$ .

(b)  $(\forall n \in \mathbb{N}) S_n = F_{n+1} - 1$  onde  $S_n$  é o número de somas realizadas ao se calcular  $F_n$ .

**Exercício 5.24:** Sejam  $\alpha$  e  $\beta$  as duas soluções da equação  $x^2 - x - 1 = 0$ , com  $\alpha > 0$ . Prove que  $F_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ , para todo  $n$  em  $\mathbb{N}$ .

**Exercício 5.25:** Prove que os números de Fibonacci satisfazem as seguintes identidades:

- (a)  $F_0 + F_1 + F_2 + \cdots + F_n = F_{n+2} - 1.$
- (b)  $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}.$
- (c)  $F_0 + F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1.$
- (d)  $F_0^2 + F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}.$
- (e)  $F_0 + F_3 + F_6 + \cdots + F_{3n} = \frac{1}{2}(F_{3n+2} - 1).$
- (f)  $F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3.$

**Exercício 5.26:** Prove que, para quaisquer números naturais  $m$  e  $n$ ,  $F_m F_n + F_{m+1} F_{n+1} = F_{m+n+1}$ .  
(Dica: fixe um  $m$  arbitrário e prove por indução em  $n$ .)

**Exercício 5.27:** 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.

**Exercício 5.28:** Considere a afirmação (obviamente falsa)  $P(n)$ : “Para todo número real  $a > 0$  e todo natural  $n$ ,  $a^n = 1$ ”. Encontre o erro na demonstração por indução abaixo.

**Prova:**

- *Base:*  $P(0)$  é obviamente verdadeira uma vez que  $a^0 = 1$ .
- *Hipótese de indução:* Suponha que, para algum  $k \geq 0$ ,  $P(i)$  é verdade para todo  $i \in \mathbb{N}$  com  $0 \leq i \leq k$ . ou seja,  $a^i = 1$  para todo  $i$  com  $0 \leq i \leq k$ .
- *Passo de indução:* Vamos provar que  $P(k+1)$  é verdadeira, isto é  $a^{k+1} = 1$ . Observe que

$$a^{k+1} = a^k \cdot a = a^k \cdot \frac{a^k}{a^{k-1}} = 1 \cdot \frac{1}{1} = 1.$$

Portanto  $P(k+1)$  também é verdadeira.

**Fim.**

## 5.8 Princípio da Boa Ordenação

Uma outra maneira de provar que um predicado é verdadeiro para todos os 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 5.8:** 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 5.9:** 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

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

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

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  $r < b$ .

**Fim.**

## 5.9 Formas equivalentes do princípio da indução

Nesta seção vamos provar as equivalências do princípio da indução matemática, do princípio da indução completa e do princípio da boa ordenação (PBO). Mais precisamente, vamos provar que

$$PIM \rightarrow PBO \rightarrow PIC \rightarrow PIM.$$

### 5.9.1 PIM implica PBO

Vamos supor que o princípio da indução matemática é válido, e provar o princípio da boa ordenação.

**Prova:**

Seja  $S$  um subconjunto de  $\mathbb{N}$  que não possui elemento mínimo; vamos provar que ele só pode ser o conjunto vazio. Considere o predicado  $P$  tal que  $P(n)$  significa “todo elemento de  $S$  é maior que  $n$ ”. Vamos provar  $(\forall n \in \mathbb{N}) P(n)$  por indução matemática.

- *Base:* como  $0 \leq x$  para todo  $x \in \mathbb{N}$ , 0 não pertence a  $S$ , pois caso contrário seria um elemento mínimo. Logo,  $P(0)$  é verdadeira.
- *Hipótese de indução:* Vamos supor que  $P(k)$  é verdadeira para algum  $k$ ; isto é, todo elemento de  $S$  é maior que  $k$ .
- *Passo da indução:* Vamos provar que  $P(k + 1)$  é verdadeira. Todo elemento  $x$  de  $S$  é maior que  $k$ , portanto é maior ou igual a  $k + 1$ . Segue daí que o número  $k + 1$  não pode pertencer a  $S$ , pois nesse caso seria um elemento mínimo. Portanto, todo

elemento de  $S$  é maior que  $k + 1$ . Ou seja,  $P(k + 1)$  é verdadeira. Logo  $(\forall n \in \mathbb{N}) P(n)$  é verdadeira.

Por outro lado, se  $x$  é um elemento qualquer de  $S$ , a afirmação  $P(x)$  é falsa. Portanto, a afirmação  $(\forall n \in \mathbb{N}) P(n)$  implica que  $S$  é vazio.

**Fim.**

### 5.9.2 PBO implica PIC

Vamos supor agora que o princípio da boa ordenação é válido, e provar o princípio da indução completa.

**Prova:**

Suponha que  $P$  é um predicado que satisfaz as condições do PIC, isto é

1.  $P(0)$  é verdade; e
2. para todo  $k \in \mathbb{N}$ ,  $((\forall i \in \mathbb{N}) i \leq k \rightarrow P(i)) \rightarrow P(k + 1)$ .

Considere o conjunto  $S = \{n \in \mathbb{N} : P(n) \text{ é falsa} \}$ . Se  $S$  não for vazio, pelo PBO ele possui um elemento mínimo. Pela condição 1 acima, este elemento é positivo, ou seja é igual a  $k + 1$  para algum  $k \in \mathbb{N}$ . Como  $k + 1$  é mínimo,  $P(i)$  deve ser verdadeira para todo natural  $i \leq k$ . Mas pela condição 2,  $P(k + 1)$  deve ser verdadeira, ou seja  $k + 1 \notin S$ . Esta contradição significa que  $S$  é vazio, ou seja  $P(n)$  é verdadeira para todo  $n$ .

**Fim.**

### 5.9.3 PIC implica PIM

Para concluir, vamos supor que o PIC é verdade, e provar o PIM.

**Prova:**

Seja  $P$  um predicado que satisfaz as condições do PIM, isto é,

1.  $P(0)$  é verdade; e
2. para todo  $k \in \mathbb{N}$ ,  $P(k) \rightarrow P(k + 1)$ .

A segunda afirmação implica que

- 2'. para todo  $k \in \mathbb{N}$ ,  $((\forall i \leq k) P(i)) \rightarrow P(k + 1)$ .

Nesta passagem usamos o fato que  $(\forall i \leq k) P(i)$  equivale a

$$((\forall i < k) P(i)) \wedge P(k)$$

e o teorema da lógica proposicional (exercício 3.29 item b))

$$(p \rightarrow q) \rightarrow (r \wedge p \rightarrow q)$$

onde  $p = P(k)$ ,  $q = P(k + 1)$ , e  $r = ((\forall i < k) P(i))$  As condições 1 e 2 são as hipóteses do PIC, portanto concluímos que  $P(n)$  é verdadeira para todo  $n$ .

**Fim.**

## **5.10 Exercícios adicionais**

**Exercício 5.29:** Demonstre a validade das seguintes fórmulas:

- $(\forall n \in \mathbb{N}) 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$
- $(\forall n \in \mathbb{N}) 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$
- $(\forall n \in \mathbb{N} - \{0\}) 1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}.$
- $(\forall n \in \mathbb{N}) 1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2.$
- $(\forall n \in \mathbb{N}) 2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$
- $(\forall n \in \mathbb{N}) 1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}.$
- $(\forall n \in \mathbb{N} - \{0\}) \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}.$
- $(\forall n \in \mathbb{N}) 1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} = 1 + (n-1)2^n.$

**Exercício 5.30:** Prove que as regiões do plano determinadas por  $n$  retas, em posição geral, podem ser coloridas utilizando duas cores de modo que regiões adjacentes recebam cores diferentes.

**Exercício 5.31:** Encontre o menor natural  $n_0 \in \mathbb{N}$  que torna as seguintes afirmações verdadeiras, e prove-as por indução em  $n$ :

- $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow 2^n > n^2$ .
- $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow n^2 < (\frac{5}{4})^n$ .
- $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow n! > 2^n$ .
- $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow n! > 4^n$ .

**Exercício 5.32:** Seja  $C$  um conjunto com  $n \geq 2$  elementos. Prove, usando indução em  $n$ , que  $C$  tem  $n(n-1)/2$  subconjuntos com exatamente dois elementos.

**Exercício 5.33:** Seja  $P$  um polígono no plano. *Triangular* um polígono significa dividir seu interior traçando diagonais que não se cruzam até que todas as regiões obtidas sejam triângulos. Neste caso, dizemos que o polígono  $P$  é *triangulado*. Um triângulo  $T$  de um polígono triangulado  $P$  é *exterior* se dois dos lados de  $T$  são lados do polígono  $P$ . Na figura 5.1, os triângulos  $T_1$  e  $T_2$  são exteriores.

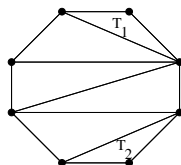


Figura 5.1: Polígono triangulado.

Prove, usando indução matemática, que um polígono triangulado  $P$  com quatro ou mais lados possui pelo menos dois triângulos exteriores.

**Exercício 5.34:** Prove que, para todo  $n, m \in \mathbb{N}$ ,

$$1 \cdot 2 \dots m + 2 \cdot 3 \dots m(m+1) + \dots + n(n+1) \dots (n+m-1) = \frac{n(n+1) \dots (n+m)}{m+1}$$

Sugestão: Fixe  $m$  arbitrário e prove por indução sobre  $n$ .

**Exercício 5.35:** Para todo inteiro positivo  $i$ , seja  $d_i$  o dígito das unidades de  $7^i$ . Prove que  $d_i = d_{i+4}$  para todo  $i$  positivo.

**Exercício 5.36:** 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.

**Exercício 5.37:** Prove que os conetivos  $\oplus$ ,  $\leftrightarrow$  e  $\neg$  não constituem um sistema completo de operadores lógicos. (Dica: prove que toda fórmula que usa apenas esses operadores e duas variáveis  $p$ ,  $q$  pode ser re-escrita na forma  $p \oplus q \oplus b$ ,  $p \oplus b$ ,  $q \oplus b$ , ou apenas  $b$ , onde  $b$  é uma constante **V** ou **F**. Use indução sobre o número de operações da fórmula e as equivalências básicas desses operadores (seção 3.2.3). Em seguida, encontre uma fórmula com operadores  $\vee$ ,  $\wedge$  e  $\neg$  que não seja equivalente a nenhuma dessas 8 fórmulas.)



# Capítulo 6

## Relações

Funções como seno e logaritmo, e os sinais de comparação ' $>$ ', ' $=$ ', etc., são casos particulares de *relações*, um conceito fundamental da matemática.

## 6.1 Conceitos básicos

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  $b \in B$ .

Dizemos que um elemento  $a$  *está relacionado com* um elemento  $b$  *por*  $\mathcal{R}$  se e somente se  $(a, b) \in \mathcal{R}$ . Este fato é frequentemente denotado por  $a \mathcal{R} b$ . Usa-se também a notação  $a \not\mathcal{R} b$  para dizer que  $(a, b) \notin \mathcal{R}$ .

**Exemplo 6.1:** O conjunto de pares  $\mathcal{R} = \{(1, 20), (1, 30), (2, 20), (2, 50), (9, 50)\}$  é uma relação do conjunto  $A = \{1, 2, 5, 9\}$  para o conjunto  $B = \{20, 30, 40, 50, 60\}$ . Temos  $2 \mathcal{R} 50$  (ou seja, 2 está relacionado com 50 por  $\mathcal{R}$ ) e  $9 \mathcal{R} 50$ , mas  $2 \not\mathcal{R} 40$  (2 não está relacionado com 40) e  $5 \not\mathcal{R} 20$ .

**Exemplo 6.2:** Sejam  $C = \{0, 1, 2, 3, 9\}$  e  $D = \{10, 20, 40, 60, 70\}$ . Observe que o conjunto de pares  $\mathcal{R}$  do exemplo 6.1 também é uma relação de  $C$  para  $D$ .

**Exemplo 6.3:** O conjunto de pares  $\mathcal{S} = \{(x, \sqrt{x}) : x \in \mathbb{N}\}$  é um exemplo de uma relação de  $\mathbb{N}$  para  $\mathbb{R}$ . Note que **não** é uma relação de  $\mathbb{N}$  para  $\mathbb{N}$ , pois  $\mathcal{R}$  possui (por exemplo) o par  $(3, \sqrt{3})$ , que não está em  $\mathbb{N} \times \mathbb{N}$ .

Se  $\mathcal{R}$  é uma relação de  $A$  para  $A$ , dizemos que  $\mathcal{R}$  é uma relação *em*  $A$  ou *sobre*  $A$ .

**Exemplo 6.4:** Os sinais de comparação da álgebra (“<”, “>”, “≤”, etc.) são relações sobre os números reais. Ou seja, o símbolo “<” (por exemplo) pode ser definido formalmente como o conjunto dos pares  $(x, y) \in \mathbb{R} \times \mathbb{R}$  tais que  $x$  é estritamente menor que  $y$ .

Note que toda relação de  $A$  para  $B$  é uma relação sobre o conjunto  $A \cup B$ .

Observe também que “ $\in$ ” é uma relação binária entre o conjunto  $\mathbb{U}$  de todos os elementos, e o conjunto  $\mathcal{P}(\mathbb{U})$  de todos os conjuntos; e que “ $\subseteq$ ” é uma relação binária sobre o conjunto  $\mathcal{P}(\mathbb{U})$ .

### 6.1.1 Especificando uma relação

Como uma relação é um conjunto de pares, ela pode ser especificada precisamente pelas mesmas maneiras que um conjunto pode ser. Por exemplo, uma relação que tem um número finito e pequeno de pares pode em princípio ser especificada precisamente listando todos esses pares.

Se os conjuntos  $A$  e  $B$  são finitos e suficientemente pequenos, uma relação binária de  $A$  para  $B$  pode ser representada por um diagrama, em que cada elemento de  $A$  ou  $B$  é representado por um ponto, e cada par ordenado  $(a, b)$  por uma seta de  $a$  para  $b$ . Veja a figura 6.1.

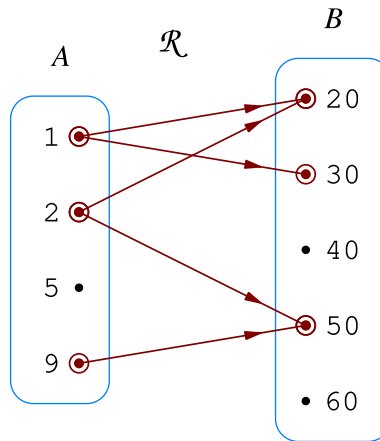


Figura 6.1: Diagrama da relação  $\mathcal{R} = \{(1, 20), (1, 30), (2, 20), (2, 50), (9, 50)\}$  do conjunto  $A = \{1, 2, 5, 9\}$  para o conjunto  $B = \{20, 30, 40, 50, 60\}$  (exemplo 6.1).

Outra maneira de representar graficamente uma relação entre conjuntos  $A$  e  $B$ , finitos e suficientemente pequenos, é representar cada elemento  $a$  de  $A$  por uma linha vertical, cada elemento  $b$  de  $B$  por uma linha horizontal, e marcar o cruzamento dessas linhas se, e somente se, o par  $(a, b)$  está na relação. Veja a figura 6.2.

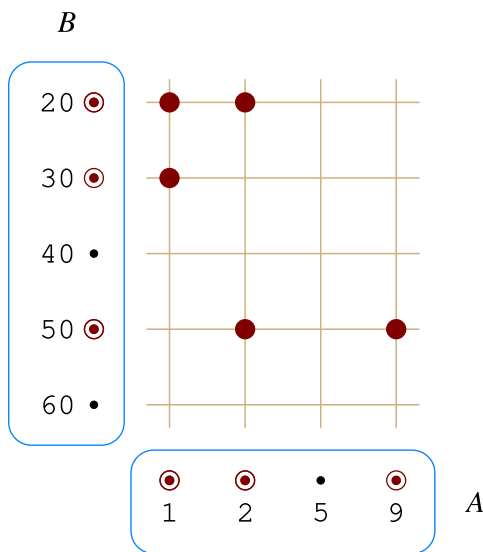


Figura 6.2: Diagrama alternativo da relação  $\mathcal{R} = \{(1, 30), (1, 40), (2, 30), (2, 50), (4, 50)\}$  do conjunto  $A = \{1, 2, 3, 4\}$  para o conjunto  $B = \{30, 40, 50, 60\}$  (exemplo 6.1).

Outra maneira é especificar um predicado  $P(a, b)$  de duas variáveis  $a, b$  tal que  $(a, b)$  está na relação se e somente se  $P(a, b)$  é verdadeiro. Podemos ainda fornecer um algoritmo que, dados  $a$  e  $b$ , determina se o par  $(a, b)$  está na sequência. Estas técnicas permitem especificar relações infinitas (ou finitas, mas grandes demais para listar explicitamente).

**Exercício 6.1:** Desenhe o diagrama da relação  $\mathcal{R}$  entre o conjunto  $A$  dos inteiros entre 1 e 10 (inclusive ambos) e o conjunto  $B$  dos números de 11 a 20 (inclusive ambos) tal que  $a \mathcal{R} b$  se e somente se  $a$  é divisor de  $b$ .

**Exercício 6.2:** Seja  $A$  o conjunto dos nomes dos dias da semana, {domingo, segunda, ..., sábado}; e seja  $B$  o conjunto dos nomes dos meses, {janeiro, fevereiro, março, ..., dezembro}. Seja  $\mathcal{R}$  a relação entre  $A$  e  $B$  tal que  $x \mathcal{R} y$  se e somente se os nomes  $x$  e  $y$  tem pelo menos duas letras distintas em comum. Desenhe o diagrama da relação  $\mathcal{R}$ .

Podemos também definir uma relação por um predicado que se aplica a toda a relação, não apenas a cada par individualmente. Veja o exemplo 6.5 abaixo. Porém, para usar este tipo de definição, é preciso garantir que de fato existe uma relação com as propriedades indicadas, e apenas uma.

**Exemplo 6.5:** Seja  $\mathcal{R}$  uma relação de  $\mathbb{N}$  para  $\mathbb{N}$  com as seguintes propriedades (1) para qualquer natural  $n$ ,  $n \mathcal{R} n + 1$ ; (2) para quaisquer naturais  $k, m, n$ ,  $(k \mathcal{R} m) \wedge (m \mathcal{R} n) \rightarrow (k \mathcal{R} n)$ ; e (3)  $\mathcal{R} \subseteq \mathcal{S}$  para qualquer outra relação com as propriedades (1) e (2). Pode-se verificar que existe uma, e apenas uma, relação de  $\mathbb{N}$  para  $\mathbb{N}$  com estas propriedades.

**Exercício 6.3:** Encontre um predicado explícito  $P(a, b)$  que é verdade se e somente se o par  $(a, b)$  está na relação  $\mathcal{R}$  do exemplo 6.5.

Assim como no caso de conjuntos, pode ser muito difícil, ou mesmo matematicamente impossível, determinar se uma definição algorítmica ou implícita faz sentido e descreve uma e apenas uma relação.

### 6.1.2 Domínio e imagem

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

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

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

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

Na figura reffig.rela, o domínio de  $\mathcal{R}$  são os pontos destacados de  $A$ , e a imagem são os pontos destacados de  $B$ . Observe que um conjunto de pares ordenados  $\mathcal{R}$  é uma relação de  $A$  para  $B$  se, e somente se,  $\text{Dom}(\mathcal{R}) \subseteq A$  e  $\text{Img}(\mathcal{R}) \subseteq B$ .

**Exemplo 6.6:** Seja  $\mathcal{R}$  a relação  $\{(1, 4), (2, 5), (3, 5), (3, 6)\}$ . Temos que  $\text{Dom}(\mathcal{R}) = \{1, 2, 3\}$  e  $\text{Img}(\mathcal{R}) = \{4, 5, 6\}$ .

**Exemplo 6.7:** Seja  $\mathcal{R}$  a relação  $\{(x, x^2) : x \in \mathbb{Z}\}$ . Observe que  $\text{Dom}(\mathcal{R})$  é o conjunto de todos os inteiros  $\mathbb{Z}$ , mas  $\text{Img}(\mathcal{R})$  é o conjunto dos quadrados perfeitos  $\{0, 1, 4, 9, \dots\}$ .

**Exemplo 6.8:** 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.

**Exemplo 6.9:** Seja  $A = \{1, 2, 3\}$ , e  $\mathcal{R}$  o conjunto dos pares  $(a, b)$  de  $A \times A$  tais que  $a < b$ . Ou seja,  $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$ . Neste caso,  $\text{Dom}(\mathcal{R}) = \{1, 2\}$  e  $\text{Img}(\mathcal{R}) = \{2, 3\}$ .

**Exemplo 6.10:** Seja  $\mathcal{R} = \{(a, b) : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge a = 2b\}$ . Note que  $\text{Dom}(\mathcal{R})$  é o conjunto dos inteiros pares e  $\text{Img}(\mathcal{R}) = \mathbb{Z}$ .

**Exemplo 6.11:** Seja  $\mathcal{R} = \{(a, b) : a \in \mathbb{R} \wedge b \in \mathbb{R} \wedge a^2 + b^2 = 25\}$ . Neste caso  $\text{Dom}(\mathcal{R}) = \text{Img}(\mathcal{R}) = \{a : a \in \mathbb{R} \wedge -5 \leq a \leq 5\} = [-5, +5]$ .

**Exercício 6.4:** Seja  $A$  o conjunto de todas as pessoas vivas hoje. Seja  $\mathcal{R}$  o conjunto de todos os pares  $(p, q) \in A \times A$  tais que a pessoa  $p$  é filha ou filho da pessoa  $q$ . Descreva os conjuntos  $\text{Dom}(\mathcal{R})$  e  $\text{Img}(\mathcal{R})$ , sua interseção  $\text{Dom}(\mathcal{R}) \cap \text{Img}(\mathcal{R})$  e sua união  $\text{Dom}(\mathcal{R}) \cup \text{Img}(\mathcal{R})$ .

**Exercício 6.5:** Seja  $\mathcal{R}$  a relação que consiste de todos os pares  $(x, y)$  de números reais tais que  $(x^2 - 2)^2 + y^2 = 1$ . Determine  $\text{Dom}(\mathcal{R})$  e  $\text{Img}(\mathcal{R})$ .

**Exercício 6.6:** Seja  $A$  o conjunto dos inteiros entre 0 e 10, inclusive. Seja  $\mathcal{R}$  o conjunto de todos os pares da forma  $(x, x^2 - 5)$  que estão em  $A \times A$ . Determine  $\text{Dom}(\mathcal{R})$  e  $\text{Img}(\mathcal{R})$ .

**Exercício 6.7:** Prove que uma relação  $\mathcal{R}$  é vazia se e somente se imagem  $\text{Img}(\mathcal{R})$  é vazia ou o domínio  $\text{Dom}(\mathcal{R})$  é vazio.

### 6.1.3 Restrição de relações

Seja  $\mathcal{R}$  uma relação, e sejam  $A'$  e  $B'$  conjuntos quaisquer. 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 6.12:** 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  $V = \{0, 1, 2, \dots, 9\}$  é o conjunto de pares

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

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

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

É comum se usar uma relação  $\mathcal{R}$  que foi definida sobre um conjunto  $A$  como se fosse uma relação sobre qualquer subconjunto  $A' \subset A$ , quando na realidade se deveria usar a restrição de  $\mathcal{R}$  a  $A'$ . Por exemplo, a relação ' $\leq$ ' é definida sobre os reais  $\mathbb{R}$ , mas ela é frequentemente usada como se fosse também uma relação sobre os inteiros  $\mathbb{Z}$ , os naturais  $\mathbb{N}$ , ou qualquer outro subconjunto de  $\mathbb{R}$ . Nestes casos entende-se que a relação desejada é a restrição de ' $\leq$ ' a estes subconjuntos.

### 6.1.4 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 6.13:** Se  $A = \{1, 2, 3\}$  então  $\mathcal{I}_A = \{(1, 1), (2, 2), (3, 3)\}$ .

### 6.1.5 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  $b$ . Veja a figura 6.3. Observe que  $\text{Dom}(\mathcal{R}^{-1}) = \text{Img}(\mathcal{R})$  e  $\text{Img}(\mathcal{R}^{-1}) = \text{Dom}(\mathcal{R})$ .

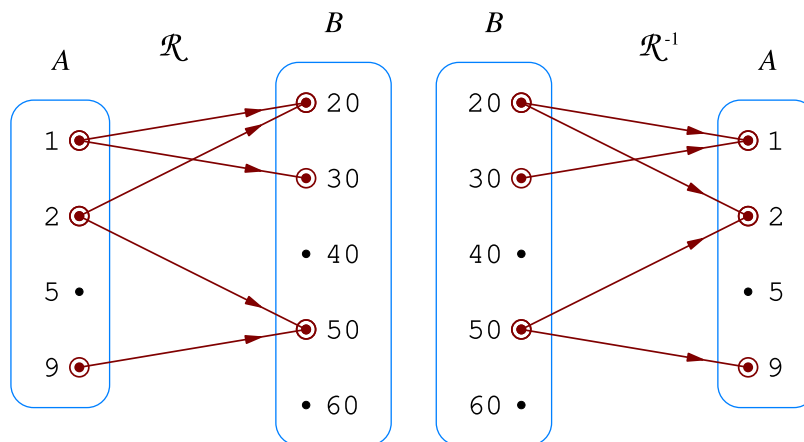


Figura 6.3: Diagrama da relação  $R$  da figura 6.1 e de sua inversa

**Exemplo 6.14:** Seja  $A = \{1, 2, 3\}$  e  $R$  a relação sobre  $A$  do exemplo 6.9. A relação inversa é  $R^{-1} = \{(a, b) : b R a\} = \{(a, b) : a \in A \wedge b \in A \wedge b < a\} = \{(2, 1), (3, 1), (3, 2)\}$ . Veja que  $\text{Dom}(R^{-1}) = \{2, 3\}$  e  $\text{Img}(R^{-1}) = \{1, 2\}$ .

**Exemplo 6.15:** A inversa de “ $\in$ ”, denotada por “ $\ni$ ”, é uma relação do conjunto  $\mathcal{P}(\mathbb{U})$  de todos os conjuntos para o conjunto  $\mathbb{U}$  de todos os elementos. A fórmula  $A \ni x$  (lê-se “ $A$  possui  $x$ ”, ou “ $A$  tem  $x$ ”) significa a mesma coisa que  $x \in A$ . (Note a diferença entre “ $\ni$ ”, “ $\supseteq$ ”, e  $\supset$ .)

**Exercício 6.8:** Seja  $R$  a relação  $\{(1, 4), (1, 5), (2, 5), (3, 4), (5, 5)\}$ . Escreva a relação inversa  $R^{-1}$ .

**Exercício 6.9:** Qual é inversa da relação “<”? E da relação “=”? E da relação “⊆”?

### 6.1.6 Imagem e imagem inversa de conjuntos sob uma relação

**Definição 6.1:** 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

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

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  $\mathcal{R}^{-1}(X)$ .

## 6.2 Composição de relações

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

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

Veja o exemplo 6.16 e a figura 6.4.

**Exemplo 6.16:** Sejam  $A = \{1, 2, 5, 9\}$ ,  $B = \{20, 30, 40, 50, 60\}$  e  $\mathcal{S}$  de  $B$  para  $C = \{200, 300, 400, 500\}$ . Considere as relações

$$\mathcal{R} = \{(1, 20), (1, 30), (2, 20), (2, 50), (9, 50)\}$$

$$\mathcal{S} = \{(20, 300), (20, 400), (30, 200), (40, 500)\}$$

A composição delas é

$$\mathcal{R}\mathcal{S} = \mathcal{S} \circ \mathcal{R} = \{(1, 200), (1, 300), (1, 400), (2, 300), (2, 400)\}$$

Observe que

- $(1, 200) \in \mathcal{S} \circ \mathcal{R}$  porque  $(1, 30) \in \mathcal{R}$  e  $(30, 200) \in \mathcal{S}$ ,
- $(1, 300) \in \mathcal{S} \circ \mathcal{R}$  porque  $(1, 20) \in \mathcal{R}$  e  $(20, 300) \in \mathcal{S}$ ,
- $(1, 400) \in \mathcal{S} \circ \mathcal{R}$  porque  $(1, 20) \in \mathcal{R}$  e  $(20, 400) \in \mathcal{S}$ ,
- $(2, 300) \in \mathcal{S} \circ \mathcal{R}$  porque  $(2, 20) \in \mathcal{R}$  e  $(20, 300) \in \mathcal{S}$ ,
- $(2, 400) \in \mathcal{S} \circ \mathcal{R}$  porque  $(2, 20) \in \mathcal{R}$  e  $(20, 400) \in \mathcal{S}$ .

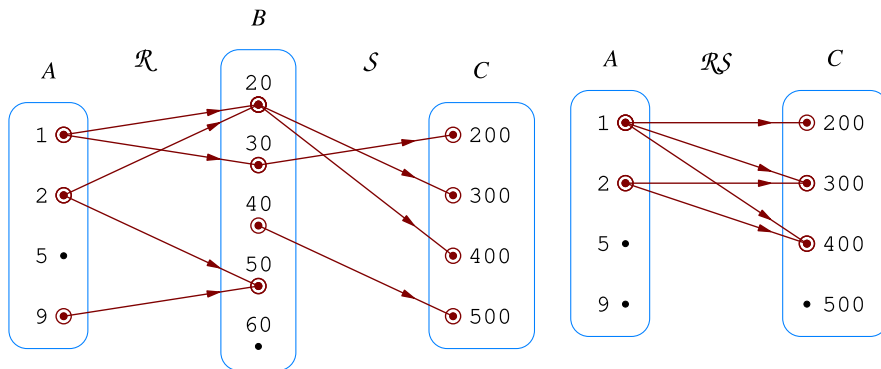


Figura 6.4: Composição das duas relações  $\mathcal{R}$  e  $\mathcal{S}$  do exemplo 6.16.

**Exemplo 6.17:** 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  $(5, 2) \notin \mathcal{S}$ .

**Exemplo 6.18:** Sejam  $\mathcal{R}$  e  $\mathcal{S}$  as mesmas relações do exemplo 6.17. 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  $(6, 2) \in \mathcal{R} \circ \mathcal{S}$ .

Os exemplos 6.17 e 6.18 mostram que há casos em que  $\mathcal{S} \circ \mathcal{R} \neq \mathcal{R} \circ \mathcal{S}$ ; isto é, a composição de relações não é comutativa.

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

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

e

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

**Exercício 6.10:** 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  $\mathcal{S} \circ \mathcal{R}$ .

**Exercício 6.11:** Sejam  $\mathcal{R}, \mathcal{S}, \mathcal{T}$  três relações. Para cada uma das afirmações abaixo, apresente uma prova ou um contra-exemplo.

- (a)  $(\mathcal{R} \circ \mathcal{T}) \setminus (\mathcal{S} \circ \mathcal{T}) \subseteq (\mathcal{R} \setminus \mathcal{S}) \circ \mathcal{T}$ .
- (b)  $(\mathcal{R} \setminus \mathcal{S}) \circ \mathcal{T} \subseteq (\mathcal{R} \circ \mathcal{T}) \setminus (\mathcal{S} \circ \mathcal{T})$ .
- (c)  $(\mathcal{R} \circ \mathcal{T}) \cap (\mathcal{S} \circ \mathcal{T}) \subseteq (\mathcal{R} \cap \mathcal{S}) \circ \mathcal{T}$ .
- (d)  $(\mathcal{R} \cap \mathcal{S}) \circ \mathcal{T} \subseteq (\mathcal{R} \circ \mathcal{T}) \cap (\mathcal{S} \circ \mathcal{T})$ .
- (e)  $(\mathcal{R} \circ \mathcal{T}) \cup (\mathcal{S} \circ \mathcal{T}) \subseteq (\mathcal{R} \cup \mathcal{S}) \circ \mathcal{T}$ .
- (f)  $(\mathcal{R} \cup \mathcal{S}) \circ \mathcal{T} \subseteq (\mathcal{R} \circ \mathcal{T}) \cup (\mathcal{S} \circ \mathcal{T})$ .

**Exercício 6.12:** Seja  $n$  um número natural, e  $A$  o conjunto dos inteiros entre 1 e  $n$ , inclusive. Note que o conjunto  $A \times A$  tem  $n^2$  pares. Encontre duas relações  $\mathcal{R}$  e  $\mathcal{S}$  sobre  $A$ , cada uma com no máximo  $2n$  pares, tal que  $\mathcal{R} \circ \mathcal{S}$  seja o conjunto  $A \times A$ .

### 6.2.1 Notação alternativa

A notação  $\mathcal{S} \circ \mathcal{R}$  para composição de  $\mathcal{R}$  com  $\mathcal{S}$  é muito comum, especialmente para funções (vide capítulo 8.1). Em algumas áreas da matemática, entretanto, a composição de uma relação  $\mathcal{R}$  com uma relação  $\mathcal{S}$  é denotada pela justaposição  $\mathcal{R}\mathcal{S}$ .

Observe que, nesta notação, a ordem das relações é oposta à da notação tradicional. Ela indica a ordem em que as relações devem ser aplicadas ao determinar a imagem de um conjunto sob a relação composta: primeiro aplica-se  $\mathcal{R}$  ao conjunto, depois aplica-se  $\mathcal{S}$  ao conjunto resultante.

### 6.2.2 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  $\mathcal{R}$ .

**Exemplo 6.19:** Seja  $A = \{1, 2, 3\}$ ,  $B = \{10, 20, 30, 40\}$  e  $\mathcal{R} = \{(1, 20), (1, 30), (2, 30)\}$ . Lembramos que  $\mathcal{I}_A = \{(1, 1), (2, 2), (3, 3)\}$  e  $\mathcal{I}_B = \{(10, 10), (20, 20), (30, 30), (40, 40)\}$ . Pode-se verificar que  $\mathcal{R} \circ \mathcal{I}_A = \mathcal{I}_B \circ \mathcal{R} = \{(1, 20), (1, 30), (2, 30)\}$ .

### 6.2.3 Composição com a relação inversa

Considere o seguinte exemplo:

**Exemplo 6.20:** Seja  $A = \{1, 2, 3\}$  e seja  $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$ , uma relação sobre  $A$ . Lembremos 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  $\mathcal{I}_A$ .

**Exercício 6.13:** Prove que, para toda relação  $\mathcal{R}$ , a composição  $\mathcal{R}^{-1} \circ \mathcal{R}$  contém a relação de identidade sobre  $\text{Dom}(\mathcal{R})$ ; e que  $\mathcal{R} \circ \mathcal{R}^{-1}$  contém a identidade sobre  $\text{Img}(\mathcal{R})$ .

### 6.2.4 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*. Veja o exemplo 6.21 e a figura 6.5

**Exemplo 6.21:** Sejam as relações do exemplo 6.16,

$$\mathcal{R} = \{(1, 20), (1, 30), (2, 20), (2, 50), (9, 50)\}$$

$$\mathcal{S} = \{(20, 300), (20, 400), (30, 200), (40, 500)\}$$

Observe que

- $\mathcal{R}\mathcal{S} = \mathcal{S} \circ \mathcal{R} = \{(1, 200), (1, 300), (1, 400), (2, 300), (2, 400)\}.$
- $\mathcal{R}^{-1} = \{(20, 1), (30, 1), (20, 2), (50, 2), (50, 9)\}.$
- $\mathcal{S}^{-1} = \{(300, 20), (400, 20), (200, 20), (500, 40)\}.$
- $\mathcal{S}^{-1}\mathcal{R}^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1} = \{(200, 2), (300, 1), (300, 2), (400, 1), (400, 2)\} = (\mathcal{R}\mathcal{S})^{-1} = (\mathcal{S} \circ \mathcal{R})^{-1}.$

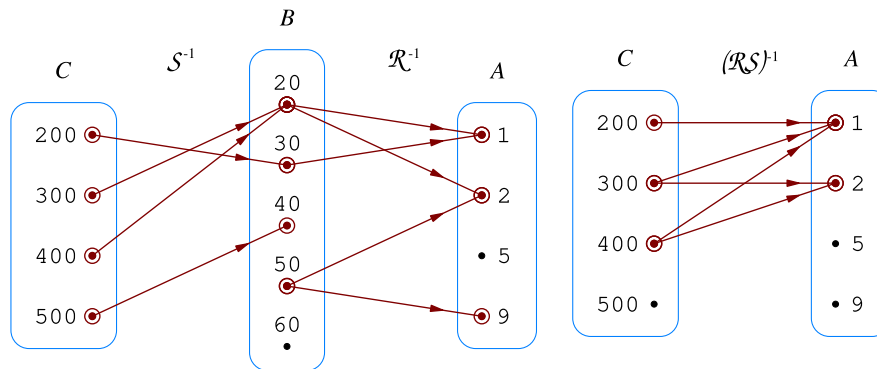


Figura 6.5: Composição das inversas  $\mathcal{R}^{-1}$  e  $\mathcal{S}^{-1}$  das duas relações  $\mathcal{R}$  e  $\mathcal{S}$  do exemplo 6.16, e a inversa  $(\mathcal{R}\mathcal{S})^{-1}$  da composição  $\mathcal{R}\mathcal{S} = \mathcal{S} \circ \mathcal{R}$ .

### 6.2.5 Composição e inclusão

O seguinte teorema decorre imediatamente das definições:

**Teorema 6.1:** 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  $\mathcal{R}_1 \circ \mathcal{S}_1 \subseteq \mathcal{R}_2 \circ \mathcal{S}_2$ .

### 6.2.6 Potências de uma relação

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

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

**Teorema 6.2:** Para quaisquer relações  $\mathcal{R}$  e  $\mathcal{S}$ , e qualquer inteiro  $n \geq 1$ , se  $\mathcal{R} \subseteq \mathcal{S}$  então  $\mathcal{R}^n \subseteq \mathcal{S}^n$ .

**Prova:**

Vamos provar este teorema por indução em  $n$ .

1. *Base:* para  $n = 1$ , o resultado é verdadeiro, pois  $\mathcal{R}^1 = \mathcal{R} \subseteq \mathcal{S} = \mathcal{S}^1$ .
2. *Hipótese de indução:* vamos supor que, para algum  $k \geq 1$ ,  $\mathcal{R}^k \subseteq \mathcal{S}^k$ .
3. *Passo da indução:* vamos provar que  $\mathcal{R}^{k+1} \subseteq \mathcal{S}^{k+1}$ . Pelo teorema 6.1, concluímos que  $\mathcal{R}^k \circ \mathcal{R} \subseteq \mathcal{S}^k \circ \mathcal{S}$ . Pela definição de potência,  $\mathcal{R}^{k+1} \subseteq \mathcal{S}^{k+1}$ .

**Fim.**

**Exercício 6.14:** Demonstre que, se  $\mathcal{R}$  é uma relação de  $A$  para  $B$ , então  $\mathcal{R} \circ \mathcal{I}_A = \mathcal{I}_B \circ \mathcal{R} = \mathcal{R}$ .

**Exercício 6.15:** Demonstre que, para quaisquer relações  $\mathcal{R}$  e  $\mathcal{S}$ , vale  $\mathcal{R}^{-1} \circ \mathcal{S}^{-1} = (\mathcal{S} \circ \mathcal{R})^{-1}$ .

**Exercício 6.16:** Demonstre que a composição de relações é associativa; isto é, que, para quaisquer três relações  $\mathcal{R}$ ,  $\mathcal{S}$  e  $\mathcal{T}$ , vale  $\mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) = (\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R}$ .

**Exercício 6.17:** Demonstre que a composição de relações distribui sobre união de relações; isto é, que, para quaisquer três relações  $\mathcal{R}$ ,  $\mathcal{S}$  e  $\mathcal{T}$ , vale  $\mathcal{T} \circ (\mathcal{R} \cup \mathcal{S}) = (\mathcal{T} \circ \mathcal{R}) \cup (\mathcal{T} \circ \mathcal{S})$ , e  $(\mathcal{R} \cup \mathcal{S}) \circ \mathcal{T} = (\mathcal{R} \circ \mathcal{T}) \cup (\mathcal{S} \circ \mathcal{T})$ .

**Exercício 6.18:** Demonstre que para quaisquer três relações  $\mathcal{R}$ ,  $\mathcal{S}$  e  $\mathcal{T}$ , vale  $\mathcal{T} \circ (\mathcal{R} \cap \mathcal{S}) \subseteq (\mathcal{T} \circ \mathcal{R}) \cap (\mathcal{T} \circ \mathcal{S})$ . Encontre um exemplo em que não vale a igualdade; isto é,  $\mathcal{T} \circ (\mathcal{R} \cap \mathcal{S}) \neq (\mathcal{T} \circ \mathcal{R}) \cap (\mathcal{T} \circ \mathcal{S})$ .

**Exercício 6.19:** Prove que, para toda relação  $\mathcal{R}$  e quaisquer inteiros positivos  $m$  e  $n$ ,  $\mathcal{R}^m \circ \mathcal{R}^n = \mathcal{R}^{m+n}$ .

### 6.2.7 Potências negativas de uma relação

Se  $\mathcal{R}$  é uma relação, e  $n$  um inteiro positivo, costuma-se definir  $\mathcal{R}^{-n}$  como sendo a potência  $n$  da relação inversa  $\mathcal{R}^{-1}$ . Isto é

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

### 6.2.8 Potência nula de uma relação

A potência nula  $\mathcal{R}^0$  de uma relação  $\mathcal{R}$  pode ser definida como a relação de identidade sobre o conjunto  $\text{Dom}(\mathcal{R}) \cup \text{Img}(\mathcal{R})$ . Com esta definição, pode-se verificar que, para todos os números naturais  $m$  e  $n$ ,

$$\mathcal{R}^m \circ \mathcal{R}^n = \mathcal{R}^{m+n} \quad (6.1)$$

e, portanto,

$$\mathcal{R}^{-m} \circ \mathcal{R}^{-n} = \mathcal{R}^{-(m+n)}$$

Entretanto, a fórmula (6.1) **não** vale se  $m$  for um inteiro positivo e  $n$  for um inteiro negativo, ou vice-versa.

## 6.3 Tipos de relações

Nesta seção daremos algumas propriedades de relações que são importantes em muitos contextos. Seja  $\mathcal{R}$  uma relação sobre um conjunto  $A$ . Dizemos que:

- $\mathcal{R}$  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,  $(\forall a, b) a \mathcal{R} b \rightarrow b \mathcal{R} a$ . 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,  $(\forall a, b) (a \mathcal{R} b) \wedge (b \mathcal{R} a) \rightarrow a = b$ . Ou seja, para quaisquer elementos distintos  $a$  e  $b$ , no máximo um dos pares  $(a, b)$  e  $(b, a)$  está em  $\mathcal{R}$ .
- $\mathcal{R}$  é *transitiva* se, e somente se,  $(\forall a, b, c) (a \mathcal{R} b) \wedge (b \mathcal{R} c) \rightarrow a \mathcal{R} c$ . 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  $\mathcal{I}_A \subseteq \mathcal{R}$ ; e dizer que  $\mathcal{R}$  é irreflexiva equivale a dizer que  $\mathcal{R} \cap \mathcal{I}_A = \{\}$ . (Quando  $A$  não é especificado, “ $\mathcal{R}$  é reflexiva” geralmente significa que é reflexiva sobre  $\text{Dom}(\mathcal{R})$ .) 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  $\mathcal{R}_1$  acima 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 acima por vacuidade, se não existirem elementos em  $A$  que satisfaçam as condições no lado esquerdo do

conetivo ‘ $\rightarrow$ ’. Por exemplo, a relação  $\mathcal{R}_3 = \{(1, 2)\}$  é transitiva, porque não existem  $a, b$  e  $c$  tais que  $(a \mathcal{R}_3 b) \wedge (b \mathcal{R}_3 c)$ .

**Exemplo 6.22:** Considere o conjunto  $A = \{1, 2, 3, 4\}$  e as seguintes relações sobre  $A$ :

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

**Exercício 6.20:** Prove que uma relação  $\mathcal{R}$  é irreflexiva se, e somente se, ela é disjunta de  $\mathcal{I}_A$  onde  $A = \text{Dom}(\mathcal{R})$ .

**Exercício 6.21:** Prove que uma relação  $\mathcal{R}$  é simétrica se, e somente se, ela é igual à sua inversa.

**Exercício 6.22:** Prove que uma relação  $\mathcal{R}$  é anti-simétrica se, e somente se, ela é disjunta de sua inversa.

**Exercício 6.23:** Seja  $\mathcal{R}$  uma relação simétrica e transitiva sobre  $\mathbb{A}$ . Prove que se para todo  $x \in \mathbb{A}$  existe um  $y \in \mathbb{A}$  tal que  $x \mathcal{R} y$ , então  $\mathcal{R}$  é reflexiva.

### 6.3.1 Composição e transitividade

O próximo teorema mostra como a operação de composição se relaciona com a propriedade transitiva de uma relação.

**Teorema 6.3:** 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, concluímos 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.

**Fim.**

O teorema 6.3 pode ser generalizado:

**Teorema 6.4:** Uma relação  $\mathcal{R}$  é transitiva se e somente se  $\mathcal{R}^n \subseteq \mathcal{R}$  para todo  $n \geq 1$ .

**Prova:**

Para provar a parte “somente se”, basta tomar  $n = 2$  e usar o teorema 6.3. Para provar a segunda parte, vamos supor que  $\mathcal{R}$  é uma relação transitiva sobre um conjunto  $A$ , e provar que  $\mathcal{R}^n \subseteq \mathcal{R}$ , para todo  $n \geq 1$ , usando indução em  $n$ .

1. *Base:* Para  $n = 1$  a afirmação é verdadeira, pois  $\mathcal{R}^1 = \mathcal{R} \subseteq \mathcal{R}$ .
2. *Hipótese de indução:* Vamos supor que  $\mathcal{R}^k \subseteq \mathcal{R}$  para algum  $k \geq 1$ .
3. *Passo:* Vamos demonstrar que  $\mathcal{R}^{k+1} \subseteq \mathcal{R}$ . Seja  $(a, b) \in \mathcal{R}^{k+1}$ ; pela definição de potência,  $(a, b) \in \mathcal{R}^k \circ \mathcal{R}$ . Pela definição de composição, temos que  $(\exists x \in A) (a, x) \in \mathcal{R} \wedge (x, b) \in \mathcal{R}^k$ . Pela hipótese de indução,  $\mathcal{R}^k \subseteq \mathcal{R}$ , portanto  $(x, b) \in \mathcal{R}$ . Como  $\mathcal{R}$  é transitiva, temos que  $(a, b) \in \mathcal{R}$ .

**Fim.**

O que este teorema nos diz é que as potências de uma relação transitiva são subconjuntos da relação. Portanto se verificarmos que  $\mathcal{R}^n \not\subseteq \mathcal{R}$ , para algum  $n \geq 1$ , podemos concluir que a relação não é transitiva.

**Exercício 6.24:** Demonstre a afirmação, ou encontre um contra-exemplo: “Se  $\mathcal{R}^4 \subseteq \mathcal{R}$ , então  $\mathcal{R}$  é transitiva.”

## 6.4 Representação de relações usando matrizes

### 6.4.1 Matriz booleana de uma relação

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  $A = \{a_1, a_2, \dots, a_m\}$  e  $B = \{b_1, b_2, \dots, b_n\}$  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:

$$M_{i,j} = \begin{cases} 1 & \text{se } a_i \mathcal{R} b_j \\ 0 & \text{se } a_i \not\mathcal{R} b_j \end{cases}$$

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

**Exemplo 6.23:** 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

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

**Composição de relações.** A composição de relações também pode ser entendida em termos de matrizes. Sejam  $\mathcal{R}$  uma relação de  $A = \{a_1, a_2, \dots, a_m\}$  para  $B = \{b_1, b_2, \dots, b_n\}$ , e  $\mathcal{S}$  uma relação de  $B = \{b_1, b_2, \dots, b_n\}$  para  $C = \{c_1, c_2, \dots, c_p\}$ , com matrizes booleanas  $M$  ( $m \times n$ ) e  $N$  ( $n \times p$ ), respectivamente. 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  $k \in \{1, 2, \dots, n\}$  tal que  $M_{i,k} = 1$  e  $N_{k,j} = 1$ . Ou seja,

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

que como veremos na seção 9.8, pode ser escrita mais sucintamente como

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

Note a semelhança entre esta fórmula e a fórmula do produto de duas matrizes ordinárias,

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

Concluimos que a composição de uma relação  $\mathcal{R}$  com uma relação  $\mathcal{S}$  corresponde ao produto  $MN$  das respectivas matrizes booleanas  $M$  e  $N$ , no sentido da álgebra de matrizes; exceto que o produto “.” de dois números é substituído pela conjunção “ $\wedge$ ”, e a soma de números “+” é substituída pela disjunção “ $\vee$ ”. Observe que a ordem em que as matrizes devem ser multiplicadas é oposta à ordem usada na notação  $\mathcal{S} \circ \mathcal{R}$ .

**Exemplo 6.24:** 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

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

### 6.4.2 Operações com relações usando matrizes

A representação por matrizes também pode ser usada para visualizar operações entre relações.

**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 intersecção  $\mathcal{R} \cap \mathcal{S}$  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  $M \wedge N$ .

**Exemplo 6.25:** 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

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

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

### 6.4.3 Propriedades de relações usando matrizes

Seja  $\mathcal{R}$  uma relação sobre um conjunto finito  $A$ . Se matriz quadrada  $M$  que representa essa relação tem a mesma ordem para linhas e colunas, várias propriedades da relação  $\mathcal{R}$  podem ser facilmente verificadas na matriz  $M$ :

1. Uma relação  $\mathcal{R}$  é reflexiva sobre  $A$  se, e somente se  $(\forall i \in \{1, 2, \dots, n\}) a_i \mathcal{R} a_i$ . Portanto  $\mathcal{R}$  é reflexiva sobre  $A$  e somente se  $(\forall i \in \{1, 2, \dots, n\}) M_{i,i} = 1$ ; isto é, os elementos da diagonal de  $M$  são todos 1.
2. Uma relação  $\mathcal{R}$  é irreflexiva sobre  $A$  se, e somente se  $(\forall i \in \{1, 2, \dots, n\}) a_i \not\mathcal{R} a_i$ . Portanto  $\mathcal{R}$  é irreflexiva sobre  $A$  e somente se os elementos da diagonal de  $M$  são todos 0.
3. Uma relação  $\mathcal{R}$  é simétrica se, e somente se  $(\forall i, j \in \{1, 2, \dots, n\}) a_i \mathcal{R} a_j \leftrightarrow a_j \mathcal{R} a_i$ . Portanto  $\mathcal{R}$  é simétrica se, e somente se, a matriz  $M$  é simétrica, ou seja, ela é igual à sua transposta.
4. Uma relação  $\mathcal{R}$  é anti-simétrica se, e somente se  $(\forall i, j \in \{1, 2, \dots, n\}) (a_i \mathcal{R} a_j \wedge a_j \mathcal{R} a_i) \rightarrow a_i = a_j$ . 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.

Note que, no caso de uma relação anti-simétrica os elementos da diagonal são arbitrários. Note também que esta definição não corresponde ao conceito de “matriz anti-simétrica” da álgebra linear. Essa definição exige  $M_{i,j} = -M_{j,i}$  o que implica que a diagonal é nula ( $M_{i,i} = 0$ ).

**Exemplo 6.26:** 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  $m_{1,2} = m_{2,1} = 1$ .

## 6.5 Fechos de uma relação

### 6.5.1 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 6.27:** 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  $A$ .

**Exemplo 6.28:** Seja a relação  $\mathcal{R} = \{(a, b) : a, b \in \mathbb{Z} \wedge a < b\}$  sobre o conjunto dos números inteiros  $\mathbb{Z}$ . O fecho reflexivo  $\mathcal{S}$  é obtido incluindo na relação  $\mathcal{R}$  todos os pares  $\{(a, a) : a \in \mathbb{Z}\}$ . Ou seja, o fecho reflexivo de  $\mathcal{R}$  sobre  $\mathbb{Z}$  é

$$\mathcal{S} = \{(a, b) : a, b \in \mathbb{Z} \wedge a \leq b\}$$

Observe que o fecho reflexivo pode ser escrito como  $\mathcal{R} \cup \mathcal{I}_A$ . Observe também que qualquer outra relação  $\mathcal{T}$  que é reflexiva sobre  $A$  e contém  $\mathcal{R}$  deve conter  $\mathcal{I}_A$ , e portanto contém  $\mathcal{I}_A \cup \mathcal{R} = \mathcal{S}$ .

## 6.5.2 Fecho simétrico

De maneira análoga, 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 6.29:** 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  $\mathcal{R}$ .

**Exemplo 6.30:** Seja a relação  $\mathcal{R} = \{(a, b) : a, b \in \mathbb{Z} \wedge a < b\}$  sobre o conjunto dos números inteiros  $\mathbb{Z}$ . O fecho simétrico  $\mathcal{S}$  é obtido incluindo na relação  $\mathcal{R}$  todos os pares

$$\{(b, a) : a, b \in \mathbb{Z} \wedge a > b\}$$

. Ou seja, o fecho simétrico de  $\mathcal{R}$  é

$$\mathcal{S} = \{(a, b) : a, b \in \mathbb{Z} \wedge a \neq b\}$$

Observe que o fecho simétrico é simplesmente  $\mathcal{R} \cup \mathcal{R}^{-1}$ . Observe também que, como no caso do fecho reflexivo, qualquer outra relação simétrica  $\mathcal{T}$  que contém  $\mathcal{R}$  deve conter  $\mathcal{R}^{-1}$ , e portanto contém seu fecho simétrico  $\mathcal{R} \cup \mathcal{R}^{-1}$ .

### 6.5.3 Fecho transitivo

Vamos agora considerar o problema análogo 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.

Podemos pensar que basta examinar todos os pares  $(a, c)$  e  $(b, c)$  que estão na relação dada  $\mathcal{R}$ . Entretanto, isso não é suficiente. Por exemplo, considere a relação

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

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

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

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

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

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.

Os pares que faltam em  $\mathcal{R}$  são da forma  $(a, c)$  tais que existe algum  $b$  com  $(a, b) \in \mathcal{R}$  e  $(b, c) \in \mathcal{R}$ . Ou seja, são os pares de  $\mathcal{R} \circ \mathcal{R} = \mathcal{R}^2$ . Portanto, ao acrescentarmos esses pares estamos construindo a relação  $\mathcal{R}' = \mathcal{R} \cup \mathcal{R}^2$ . Pela mesma razão, os pares que ainda faltam em  $\mathcal{R}'$  estão na relação  $\mathcal{R}' \circ \mathcal{R}' = (\mathcal{R} \cup \mathcal{R}^2)^2$ , que (pelo exercício 6.17) é a relação  $\mathcal{R}^2 \cup \mathcal{R}^3 \cup \mathcal{R}^4$ . Portanto, acrescentando esses pares obtemos  $\mathcal{R}'' = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \mathcal{R}^4$ . No próximo passo, obtemos  $\mathcal{R} \cup \mathcal{R}^2 \cup \dots \cup \mathcal{R}^7 \cup \mathcal{R}^8$ . E assim por diante.

Por estas considerações, 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

$$\mathcal{R}^* = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \dots \quad (6.2)$$

Como veremos na seção 9.8, esta fórmula pode ser escrita mais sucintamente da seguinte maneira

$$\mathcal{R}^* = \bigcup_{k=1}^{\infty} \mathcal{R}^k \quad (6.3)$$

Ou seja, um par  $(a, b)$  está em  $\mathcal{R}^*$  se, e somente se, existe um inteiro  $k \geq 1$  tal que  $(a, b) \in \mathcal{R}^k$ .

Se  $\mathcal{R}$  é uma relação sobre um conjunto *finito*  $A$ , a união eventualmente deixa de crescer após um número finito de termos; pois os pares que podem ser acrescentados pertencem ao conjunto  $A \times A$ ,

que é finito. Pode-se mostrar que, se  $A$  tem  $n$  elementos, o processo termina com o termo  $\mathcal{R}^n$ , no máximo. Nesse caso, a relação  $\mathcal{R}^*$  assim obtida é uma relação transitiva, por construção.

No caso de  $A$  ser finito, também podemos escrever a fórmula (6.3) em termos das matrizes booleanas. Se  $M$  é a matriz de  $\mathcal{R}$ , a matriz  $M^*$  de  $\mathcal{R}^*$  é dada pela fórmula

$$M^* = \bigvee_{k=1}^n M^k = M \vee M^2 \vee M^3 \vee \dots \vee M^n \quad (6.4)$$

Caso o conjunto  $A$  seja infinito, o processo pode nunca terminar: após cada acréscimo de pares que faltam podem surgir novos casos de falha de transitividade. Nesse caso, a união (6.3) precisa incluir todas as potências de  $\mathcal{R}$ . Precisamos então provar o seguinte resultado:

**Teorema 6.5:** Para qualquer relação  $\mathcal{R}$ , a relação  $\mathcal{R}^*$  é transitiva.

**Prova:**

Sejam  $a, b, c$  elementos tais que  $(a, b)$  e  $(b, c)$  estão em  $\mathcal{R}^*$ . Precisamos provar que  $(a, c)$  também está em  $\mathcal{R}^*$ .

Pela definição de  $\mathcal{R}^*$ , existem inteiros  $i \geq 1$  e  $j \geq 1$  tais que  $(a, b) \in \mathcal{R}^i$  e  $(b, c) \in \mathcal{R}^j$ . Portanto  $(a, c)$  está na composição  $\mathcal{R}^j \circ \mathcal{R}^i$ , que, pelo exercício 6.19, é igual a  $\mathcal{R}^{i+j}$ . Portanto o par  $(a, c)$  também está em  $\mathcal{R}^*$ .

**Fim.**

Por outro lado, o teorema a seguir mostra que o fecho transitivo  $\mathcal{R}^*$  calculado pela fórmula (6.3) não tem nenhum par supérfluo:

**Teorema 6.6:** Para qualquer relação  $\mathcal{R}$ , qualquer relação transitiva que contém  $\mathcal{R}$  contém o fecho transitivo  $\mathcal{R}^*$  de  $\mathcal{R}$ .

**Prova:**

Seja  $\mathcal{R}$  uma relação qualquer, e seja  $\mathcal{S}$  uma relação que contém  $\mathcal{R}$ . Pelo teorema 6.2, para todo  $n \geq 1$ , temos que  $\mathcal{R}^n \subseteq \mathcal{S}^n$ . Pelo teorema 6.4, temos que  $\mathcal{S}^n = \mathcal{S}$ ; logo  $\mathcal{R}^n \subseteq \mathcal{S}$ . Uma vez que todos os termos da fórmula (6.3) estão contidos em  $\mathcal{S}$ , então a união de todos esses termos  $\mathcal{R}^*$  também está.

**Fim.**

Os dois teoremas acima implicam que o fecho transitivo  $\mathcal{R}^*$  definido pela fórmula (6.3) é a *única* relação transitiva que contém  $\mathcal{R}$  e está contida em qualquer relação transitiva que contém  $\mathcal{R}$ . Portanto ela é também a menor relação transitiva que contém  $\mathcal{R}$ .

### 6.5.4 Fecho em geral

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

Em outras palavras,  $\mathcal{S}$  é o fecho de  $\mathcal{R}$  com respeito à propriedade  $\mathbf{P}$  se

- $\mathcal{R} \subseteq \mathcal{S}$ .

- $\mathcal{S}$  satisfaz a propriedade **P**.
- Para toda relação  $\mathcal{T}$  em  $A$ , se  $\mathcal{R} \subseteq \mathcal{T}$  e  $\mathcal{T}$  satisfaz a propriedade **P**, então  $\mathcal{S} \subseteq \mathcal{T}$ .

A relação  $\mathcal{R}$  pode ter ou não ter a propriedade **P**. Se  $\mathcal{R}$  tiver a propriedade **P** então  $\mathcal{R} = \mathcal{S}$ .

O fecho de uma relação com respeito a uma determinada propriedade pode ou não existir. Veja o exemplo a seguir:

**Exemplo 6.31:** Sejam  $A = \{1, 2, 3\}$ ,  $\mathcal{R} = \{(1, 1), (1, 2), (2, 2), (3, 3)\}$  e  $\mathbf{P}(\mathcal{R}) = “\mathcal{R}$  não é reflexiva sobre  $A”$ . Observe que qualquer relação contendo  $\mathcal{R}$  conterá  $\{(1, 1), (2, 2), (3, 3)\}$ , portanto não existe nenhuma relação, que não seja reflexiva sobre  $A$ , e contenha  $\mathcal{R}$ .

Neste exemplo, o fecho não existe porque é impossível completar  $\mathcal{R}$  de modo a satisfazer **P**. No exemplo abaixo, o fecho não existe porque há duas ou mais maneiras de fazer isso, mas elas são incompatíveis:

**Exemplo 6.32:** Sejam  $A = \{1, 2\}$ ,  $\mathcal{R} = \{(1, 1), (2, 2)\}$  e  $\mathbf{P}(\mathcal{R}) = “\mathcal{R}$  tem 3 pares”.

As duas relações  $\mathcal{S}_1 = \{(1, 1), (1, 2), (2, 2)\}$  e  $\mathcal{S}_2 = \{(1, 1), (2, 1), (2, 2)\}$  são relações que satisfazem a propriedade **P** e contêm  $\mathcal{R}$ ; porém, a única relação  $\mathcal{S}$  que está contida em  $\mathcal{S}_1$  e em  $\mathcal{S}_2$  e contém  $\mathcal{R}$  é a própria relação  $\mathcal{R}$ , que não satisfaz **P**.

**Exercício 6.25:** Encontre os fechos reflexivo, simétrico e transitivo das seguintes relações:

- $A = \{a, b, c\}$  e  $\mathcal{R} = \{(a, a), (a, b), (b, c), (c, b)\}$ .
- $A = \{0, 1, 2, 3\}$  e  $\mathcal{R} = \{(0, 1), (1, 1), (1, 2), (2, 0), (2, 2), (3, 0)\}$ .

**Exercício 6.26:** Sejam  $A = \{1, 2, 3, 4, 5\}$  e  $\mathcal{R} = \{(1, 3), (2, 4), (3, 1), (3, 5), (4, 3), (5, 1), (5, 2), (5, 4)\}$ . Encontre as potências  $\mathcal{R}^2$ ,  $\mathcal{R}^3$ ,  $\mathcal{R}^4$ ,  $\mathcal{R}^5$ ,  $\mathcal{R}^6$  e o fecho transitivo  $\mathcal{R}^*$ .

**Exercício 6.27:** Seja  $A = \{0, 1, 2, 3, 4, 5\}$ . Encontre a menor relação contendo a relação  $\mathcal{R} = \{(1, 2), (1, 4), (3, 3), (4, 1)\}$  que é:

- (a) Simétrica e reflexiva sobre  $A$ .
- (b) Reflexiva sobre  $A$  e transitiva.
- (c) Simétrica e transitiva.
- (d) Reflexiva sobre  $A$ , simétrica e transitiva.

**Exercício 6.28:** Sejam  $\mathcal{R}_1$  e  $\mathcal{R}_2$  relações sobre o conjunto  $A$ , tais que  $\mathcal{R}_1 \subseteq \mathcal{R}_2$ .

- (a) Sejam  $\mathcal{S}_1$  e  $\mathcal{S}_2$  os fechos reflexivos de  $\mathcal{R}_1$  e  $\mathcal{R}_2$ , respectivamente. Prove que  $\mathcal{S}_1 \subseteq \mathcal{S}_2$ .
- (b) Enuncie os teoremas análogos para os fechos simétricos e transitivos. Prove esses teoremas, ou encontre contra-exemplos.

**Exercício 6.29:** Sejam  $\mathcal{R}_1$  e  $\mathcal{R}_2$  relações sobre o conjunto  $A$ , e  $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$ .

- (a) Sejam  $\mathcal{S}_1, \mathcal{S}_2$  e  $\mathcal{S}$  os fechos reflexivos de  $\mathcal{R}_1, \mathcal{R}_2$  e  $\mathcal{R}$ , respectivamente. Prove que  $\mathcal{S}_1 \cup \mathcal{S}_2 = \mathcal{S}$ .
- (b) Sejam  $\mathcal{S}_1, \mathcal{S}_2$  e  $\mathcal{S}$  os fechos simétricos de  $\mathcal{R}_1, \mathcal{R}_2$  e  $\mathcal{R}$ , respectivamente. Prove que  $\mathcal{S}_1 \cup \mathcal{S}_2 = \mathcal{S}$ .
- (c) Sejam  $\mathcal{S}_1, \mathcal{S}_2$  e  $\mathcal{S}$  os fechos transitivos de  $\mathcal{R}_1, \mathcal{R}_2$  e  $\mathcal{R}$ , respectivamente. Prove que  $\mathcal{S}_1 \cup \mathcal{S}_2 \subseteq \mathcal{S}$ , e encontre um exemplo em que a inclusão é própria.

**Exercício 6.30:** Sejam  $\mathcal{R}_1$  e  $\mathcal{R}_2$  relações sobre o conjunto  $A$ , e  $\mathcal{R} = \mathcal{R}_1 \cap \mathcal{R}_2$ .

- (a) Sejam  $\mathcal{S}_1, \mathcal{S}_2$  e  $\mathcal{S}$  os fechos reflexivos de  $\mathcal{R}_1, \mathcal{R}_2$  e  $\mathcal{R}$ , respectivamente. Prove que  $\mathcal{S} = \mathcal{S}_1 \cap \mathcal{S}_2$ .
- (b) Sejam  $\mathcal{S}_1, \mathcal{S}_2$  e  $\mathcal{S}$  os fechos simétricos de  $\mathcal{R}_1, \mathcal{R}_2$  e  $\mathcal{R}$ , respectivamente. Prove que  $\mathcal{S} \subseteq \mathcal{S}_1 \cap \mathcal{S}_2$ , e mostre com um exemplo que a inclusão pode ser própria.
- (c) Sejam  $\mathcal{S}_1, \mathcal{S}_2$  e  $\mathcal{S}$  os fechos transitivos de  $\mathcal{R}_1, \mathcal{R}_2$  e  $\mathcal{R}$ , respectivamente. Prove que  $\mathcal{S} \subseteq \mathcal{S}_1 \cap \mathcal{S}_2$ , e mostre com um exemplo que a inclusão pode ser própria.

**Exercício 6.31:** Seja  $\mathcal{R}$  a relação sobre o conjunto dos números inteiros positivos tal que  $a \mathcal{R} b$  se e somente se existe um número primo  $p$  tal que  $a = pb$ . Qual é o fecho reflexivo de  $\mathcal{R}$ ? Qual é o fecho transitivo de  $\mathcal{R}$ ? Qual é o fecho transitivo e reflexivo?

## 6.6 Relações $n$ -árias

### 6.6.1 Definição

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

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  $\text{Dom}_i(\mathcal{R})$  de todos os elementos de  $A_i$  que ocorrem na posição  $i$  das suas  $n$ -uplas. Ou seja, um elemento  $x$  pertence a  $\text{Dom}_i(\mathcal{R})$  se, e somente se, existe uma  $n$ -upla  $(a_1, a_2, \dots, a_n)$  em  $\mathcal{R}$  com  $a_i = x$ .

**Exemplo 6.33:** Seja  $\mathcal{R}$  a relação em  $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$  definida pelo conjunto das triplas  $(a, b, c)$  tais que  $a = b = c$ . Observe que a tripla  $(2, 2, 2) \in \mathcal{R}$ , mas a tripla  $(-2, 3, 3) \notin \mathcal{R}$ . Os domínios  $\text{Dom}_1(\mathcal{R})$ ,  $\text{Dom}_2(\mathcal{R})$  e  $\text{Dom}_3(\mathcal{R})$  são o conjunto dos números reais, e o grau de  $\mathcal{R}$  é 3.

**Exemplo 6.34:** Seja  $\mathcal{R}$  a relação em  $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$  definida pelo conjunto das triplas  $(a, b, c)$  tais que  $a^2 + b^2 = c^2$ ,  $a > 0$  e  $b > 0$ . Observe que a tripla  $(3, 4, 5) \in \mathcal{R}$  mas a tripla  $(2, 2, 3) \notin \mathcal{R}$ . Pode-se verificar que  $\text{Dom}_1(\mathcal{R}) = \text{Dom}_2(\mathcal{R}) = \mathbb{N} \setminus \{1, 2\}$ , e que os menores elementos de  $\text{Dom}_3(\mathcal{R})$  são  $\{5, 10, 13, 17, 20, 25, 26, 29, \dots\}$ .

**Exemplo 6.35:** Seja  $\mathcal{R}$  a relação em  $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  definida pelo conjunto das quádruplas  $(a, b, q, r)$  tais que  $a = b * q + r$ . Observe que a quádrupla  $(7, 3, 2, 1)$  está em  $\mathcal{R}$  mas a quádrupla  $(3, 7, 2, 1)$  não está.

### 6.6.2 Projecção

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

**Exemplo 6.36:** 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 projecções 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 1 e 2:  $\{(1, 10), (1, 20), (2, 20), (2, 30), (3, 30)\}$
- Sobre 2 e 1:  $\{(10, 1), (20, 1), (20, 2), (30, 2), (30, 3)\}$
- Sobre 1, 2 e 3:  $\{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 300)\} = \mathcal{R}$

**Exemplo 6.37:** Seja  $\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R} \times \mathbb{R}$  a relação ternária que consiste de todas as triplas  $(a, b, c)$  tais que  $a^2 + b^2 + c^2 = 1$  — isto é, todos os pontos da superfície da esfera de raio 1 e centro na origem do  $\mathbb{R}^3$ . A projecção de  $\mathcal{R}$  sobre as componentes 1 e 3 é o conjunto  $\mathcal{S}$  de todos os pares  $(a, c) \in \mathbb{R} \times \mathbb{R}$  tais que  $(\exists b \in \mathbb{R}) a^2 + b^2 + c^2 = 1$ . Pode-se verificar que  $\mathcal{S} = \{(a, c) \in \mathbb{R} \times \mathbb{R} : a^2 + c^2 \leq 1\}$ , ou seja, o disco de raio 1 e centro na origem do plano  $\mathbb{R}^2$ .

Observe que a ordem dos índices  $i_1, i_2, \dots, i_m$  é importante. Observe também que, se  $m = n$  e os índices forem  $1, 2, \dots, n$ , a operação não tem efeito — o resultado é a própria relação  $\mathcal{R}$ .

Um caso muito comum é a eliminação de uma determinada componente  $j$  mantendo a ordem das demais, como no exemplo 6.37. Nesse caso,  $m = n - 1$  e os índices  $i_1, i_2, \dots, i_m$  são  $1, 2, \dots, j - 1, j + 1, \dots, n$ .

### 6.6.3 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  $i_1, i_2, \dots, i_n$  dos inteiros  $1, 2, \dots, n$ , esta operação produz a relação  $n$ -ária  $\mathcal{S}$  que consiste de todas as  $n$ -uplas  $(a_{i_1}, a_{i_2}, \dots, a_{i_n})$  tais que  $(a_1, a_2, \dots, a_n)$  está em  $\mathcal{R}$ .

Por exemplo, dada a relação ternária  $\{(1, 20, 350), (2, 20, 300), (4, 40, 400)\}$ , podemos formar a relação ternária  $\{(20, 350, 1), (20, 300, 2), (40, 400, 4)\}$  substituindo cada tripla  $(a_1, a_2, a_3)$  pela tripla rearranjada  $(a_2, a_3, a_1)$ .

Note que esta operação é um caso particular da projeção generalizada com índices  $i_1, i_2, \dots, i_m$ , em que  $m = n$  e os índices são uma permutação dos inteiros  $1, 2, \dots, n$ . Note também que cada  $n$ -upla de  $\mathcal{R}$  corresponde a uma única  $n$ -upla de  $\mathcal{S}$ , e vice-versa.

### 6.6.4 Restrição

Sejam  $\mathcal{R}$  uma relação  $n$ -ária, e  $X_1, X_2, \dots, X_n$  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  $(a_1, a_2, \dots, a_n)$  de  $\mathcal{R}$  que tem  $a_j \in X_j$ , para cada  $j$ ; ou seja

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

**Exemplo 6.38:** 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

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

### 6.6.5 Junção

As tabelas abaixo descrevem duas relações  $\mathcal{R}$  (quaternária) e  $\mathcal{S}$  (ternárias). A relação  $\mathcal{R}$  é uma relação que associa empregados, salas, funções e chefe imediato. A segunda relação associa salas,

departamentos e ramais de telefone.

| $\mathcal{R}$ |            |        |       |
|---------------|------------|--------|-------|
| 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  $\mathcal{T}$  abaixo:

| $\mathcal{T}$ |            |        |       |       |            |
|---------------|------------|--------|-------|-------|------------|
| 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  $\mathcal{S}$ . A construção da tabela acima é um exemplo de *junção* de duas relações  $n$ -árias para produzir uma terceira relação  $n$ -árias.

Mais 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  $(a_1, a_2, \dots, a_{m-1}, c, b_1, b_2, \dots)$  tais que  $(a_1, a_2, \dots, a_{m-1}, c) \in \mathcal{R}$  e  $(c, b_1, b_2, \dots, b_{n-1}) \in \mathcal{S}$ .

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  $(a_1, a_2, \dots, a_{m-p}, c_1, c_2, \dots, c_p, b_1, b_2, \dots, b_{n-p})$ , tais que  $(a_1, a_2, \dots, a_{m-p}, c_1, c_2, \dots, c_p) \in \mathcal{R}$ , e  $(c_1, c_2, \dots, c_p, b_1, b_2, \dots, b_{n-p}) \in \mathcal{S}$ .

Observe que a junção, tal como definida acima, pode ser combinada com operações de permutação e projeção para casar quaisquer campos de duas relações (e não apenas os últimos campos de  $\mathcal{R}$  com os primeiros de  $\mathcal{S}$ ), e eliminar campos desnecessários no resultado.

Relações  $n$ -árias e as operações vistas acima são conceitos fundamentais em bancos de dados, especificamente nos *bancos de dados relacionais*.

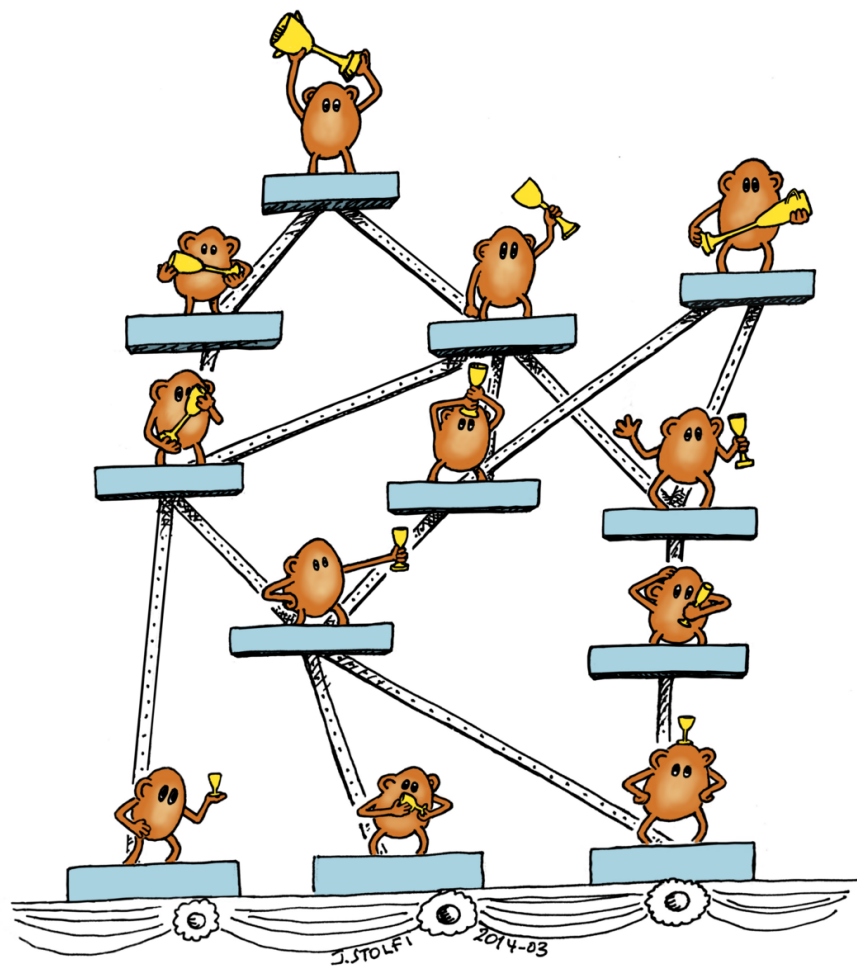
**Exercício 6.32:** Prove que a composição  $\mathcal{S} \circ \mathcal{R}$  de duas relações binárias  $\mathcal{R}$  e  $\mathcal{S}$  pode ser obtida por uma junção seguida de uma projeção.



# **Capítulo 7**

## **Relações de ordem e equivalência**





## 7.1 Relações de ordem

**Definição 7.1:** Uma relação  $\mathcal{R}$  sobre um conjunto  $A$  é uma *relação de ordem* se ela é reflexiva sobre  $A$ , anti-simétrica e transitiva.

**Exemplo 7.1:** 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  $(\forall x \in \mathbb{R}) x \mathcal{R} x$ .
- $\mathcal{R}$  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

$$(\forall x, y \in \mathbb{R}) (x \mathcal{R} y \wedge y \mathcal{R} x) \rightarrow x = y$$

**Exemplo 7.2:** Sejam  $\mathcal{P}(A)$  o conjunto potência de um conjunto  $A$  e

$$\mathcal{S} = \{ (X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) : X \subseteq Y \}$$

- $\mathcal{R}$  é reflexiva sobre  $\mathcal{P}(A)$  pois  $(\forall X \in \mathcal{P}(A)) X \subseteq X$  logo  $(\forall X \in \mathcal{P}(A)) X \mathcal{R} X$ .

- $\mathcal{R}$  é transitiva pois  $(\forall X, Y, Z \in \mathcal{P}(A))(X \subseteq Y \wedge Y \subseteq Z) \rightarrow X \subseteq Z$ . Portanto  $(\forall X, Y, Z \in \mathcal{P}(A))(X \mathcal{R} Y \wedge Y \mathcal{R} Z) \rightarrow X \mathcal{R} Z$ .
- $\mathcal{R}$  é anti-simétrica pois  $(\forall X, Y \in \mathcal{P}(A))(X \subseteq Y \wedge Y \subseteq X) \rightarrow X = Y$ . Portanto  $(\forall X, Y \in \mathcal{P}(A))(X \mathcal{R} Y \wedge Y \mathcal{R} X) \rightarrow X = Y$ .

Observe que se  $\mathcal{R}$  é uma relação de ordem sobre um conjunto  $A$ , e  $A' \subseteq A$ , a restrição de  $\mathcal{R}$  a  $A'$  é uma relação de ordem sobre  $A'$ . (Veja o exercício 7.4.)

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  $(\mathcal{P}(A), \subseteq)$ , para qualquer conjunto  $A$ .

**Exercício 7.1:** Seja  $\mathcal{R}$  a relação sobre o conjunto dos números inteiros positivos tal que  $a \mathcal{R} b$  se e somente se existe um inteiro positivo  $k$  tal que  $a = kb$ . Prove que  $\mathcal{R}$  é uma relação de ordem.

**Exercício 7.2:** Seja  $A$  o conjunto dos inteiros de 0 a 9, e  $\mathcal{R}$  a relação sobre  $A$  tal que  $a \mathcal{R} b$  se e somente se  $a$  é par e  $b$  é ímpar, ou ambos são pares e  $a \leq b$ , ou ambos são ímpares e  $a \geq b$ . Esta é uma relação de ordem?

**Exercício 7.3:** Considere a relação  $\mathcal{R}$  sobre os pares ordenados de inteiros  $\mathbb{Z} \times \mathbb{Z}$  tal que

$$(a, b) \mathcal{R} (c, d) \leftrightarrow (a \leq c) \vee (b \leq d)$$

para quaisquer inteiros  $a, b, c$  e  $d$ . Esta é uma relação de ordem?

**Exercício 7.4:** Seja  $\mathcal{R}$  uma relação de ordem sobre um conjunto  $A$ . Prove que, para todo subconjunto  $A'$  de  $A$ , a restrição  $\mathcal{R}'$  de  $\mathcal{R}$  a  $A'$  é uma relação de ordem sobre  $A'$ .

**Exercício 7.5:** Para quaisquer relações de ordem  $\mathcal{R}$  e  $\mathcal{S}$  sobre um conjunto  $A$ , a relação  $\mathcal{R} \cup \mathcal{S}$  é sempre uma relação de ordem sobre  $A$ ? E a relação  $\mathcal{R} \cap \mathcal{S}$ ? Prove suas respostas.

**Exercício 7.6:** Seja  $S$  o conjunto de todos os arquivos em um sistema de arquivos, e  $\mathcal{R}$  a relação sobre  $S$  tal que  $a\mathcal{R}b$  se e somente se o arquivo  $a$  contém uma cópia do conteúdo do arquivo  $b$ , possivelmente com informações adicionais antes do início de  $b$  ou depois do fim. A relação  $\mathcal{R}$  é uma relação de ordem?

### 7.1.1 Relações de ordem estrita

**Definição 7.2:** 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 7.3:** 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  $(\forall x \in \mathbb{R}) x \not\mathcal{R} x$ .
- $\mathcal{R}$  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  $A$ . 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.

**Exercício 7.7:** Seja  $A$  um conjunto de caixas, e  $\mathcal{R}$  a relação sobre  $A$  tal que  $a \mathcal{R} b$  se e somente se a caixa  $a$  cabe dentro da caixa  $b$ . Prove que esta é uma relação de ordem estrita.

### 7.1.2 Ordem total

Dizemos que dois elementos  $a, b$  são *comparáveis* por uma relação  $\mathcal{R}$  se  $a \mathcal{R} b$  ou  $b \mathcal{R} a$ .

**Definição 7.3:** 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*.

Observe que a relação  $\leq$  (exemplo 7.1) é uma ordem total sobre  $\mathbb{R}$ , pois  $(\forall a, b \in \mathbb{R}) a \leq b \vee b \leq a$ . Por outro lado, a relação  $\subseteq$  (exemplo 7.2) não é uma ordem total quando  $A$  tem pelo menos dois elementos, pois nesse caso existem subconjuntos distintos  $X$  e  $Y$  em  $\mathcal{P}(A)$  tais que nem  $X \subseteq Y$  nem  $Y \subseteq X$ . Por exemplo, se  $A = \{1, 2\}$ , podemos tomar  $X = \{1\}$  e  $Y = \{2\}$ .

Analogamente, dizemos que uma ordem estrita  $\mathcal{R}$  sobre um conjunto  $A$  é *total* se e somente se quaisquer dois elementos *distintos* de  $A$  são comparáveis por  $\mathcal{R}$ .

**Exercício 7.8:** A ordem estrita sobre um conjunto de caixas definida no exercício 7.7 é uma ordem total?

**Exercício 7.9:** Seja  $\mathcal{R}$  uma relação de ordem total sobre um conjunto  $A$ , Prove que, para todo subconjunto  $B$  de  $A$ , a restrição  $\mathcal{R}$  a  $B$  também é uma relação de ordem total. (Veja o exercício 7.4.)

**Exercício 7.10:** Seja  $\mathcal{R}$  uma relação sobre um conjunto  $A$ , e seja  $\mathcal{S}$  a relação complementar,  $(A \times A) \setminus \mathcal{R}$ .

- (a) Prove que  $\mathcal{R}$  é uma relação de ordem total sobre  $A$  se e somente se  $\mathcal{S}$  é uma relação de ordem estrita total sobre  $A$ .
- (b) Mostre um exemplo em que  $\mathcal{R}$  é uma relação de ordem mas  $\mathcal{S}$  não é uma relação de ordem estrita.

### 7.1.3 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. A regra é: para decidir se uma palavra vem antes da outra, 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”), convencionam-se que a palavra que termina primeiro vem antes da outra.

Uma idéia semelhante pode ser utilizada para ordenar pares de reais. Seja a relação  $\leq_2$  definida

sobre os pares  $\mathbb{R} \times \mathbb{R}$ , pela fórmula

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

Note a semelhança entre a relação  $\leq_2$  e a ordem alfabética de palavras.

Este conceito pode ser generalizado para sequências de “letras” arbitrárias e ordenações arbitrárias dessas “letras”. Seja  $\mathcal{R}$  uma relação de ordem sobre um conjunto  $A$ . Vamos denotar por  $A^*$  o conjunto de todas as sequências de elementos de  $A$ , e  $()$  a sequência vazia. Considere a relação  $\mathcal{R}^*$  definida recursivamente sobre  $A^*$ , da seguinte maneira:

1.  $() \mathcal{R}^* b$  para qualquer sequência  $b \in A^*$ .
2.  $b \mathcal{R}^* ()$  para qualquer sequência não vazia  $a$  em  $A^*$ .
3. Se  $a$  e  $b$  são sequências não vazias em  $A^*$ , sejam  $a_1$  e  $b_1$  os elementos iniciais de  $a$  e  $b$ , e  $a', b'$  o que resta de  $a$  e  $b$  retirando-se estes elementos iniciais. Então temos que  $a \mathcal{R}^* b$  se, e somente se,

$$(a_1 \neq b_1 \wedge a_1 \mathcal{R} b_1) \vee (a_1 = b_1 \wedge a' \mathcal{R}^* b')$$

Observe que esta definição recursiva permite determinar, em um número finito de passos, se qualquer par  $(a, b)$  de sequências de  $A^*$  está na relação  $\mathcal{R}^*$  ou não. Prova-se (veja exercícios 7.11, 7.12 e 7.13) que a relação  $\mathcal{R}^*$  definida desta forma é uma relação de ordem. Prova-se também que  $\mathcal{R}^*$  é uma ordem total se e somente se  $\mathcal{R}$  é total (veja exercício 7.14).

A relação  $\mathcal{R}^*$  acima é chamada de *ordem lexicográfica induzida por  $\mathcal{R}$* .

**Exercício 7.11:** Prove que a relação  $\mathcal{R}^*$  definida acima é reflexiva. (Dica: use indução no número  $n$  de elementos da mais curta entre as duas sequências.)

**Exercício 7.12:** Prove que a relação  $\mathcal{R}^*$  definida acima é anti-simétrica.

**Exercício 7.13:** Prove que a relação  $\mathcal{R}^*$  definida acima é transitiva.

**Exercício 7.14:** Prove que a relação de ordem  $\mathcal{R}^*$  definida acima é total se e somente se  $\mathcal{R}$  é total.

### 7.1.4 Ordens “parciais”

Fora de contextos matemáticos, a palavra “parcial” geralmente significa “incompleto”, e portanto o oposto de “total”. Em matemática, entretanto, muitos autores usam “relação de ordem parcial” como sinônimo de “relação de ordem”. Para esses autores, as ordens totais são casos particulares de ordens parciais.

Esses autores também se referem a um conjunto ordenado  $(A, \mathcal{R})$  como “conjunto parcialmente ordenado”, (em inglês, *partially ordered set* ou *poset*) — mesmo que a relação  $\mathcal{R}$  seja uma ordem total.

Para outros autores, entretanto, “ordem parcial” pode significar uma ordem que não é total. O leitor deve ficar atento para esses dois sentidos da palavra “parcial”. Para evitar ambiguidades, sugerimos evitar essa palavra, usando “relação de ordem” para o caso geral, e “ordem total” ou “ordem não total” para os dois tipos.

### 7.1.5 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).

Neste diagrama, 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 deste diagrama, vamos usar o conjunto  $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ , e a

seguinte relação sobre  $A$ :

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

Podemos representar o conjunto  $A$  e os pares de  $\mathcal{R}$  pelo diagrama de pontos e setas da figura 7.1 (à esquerda). Observe que, da maneira como os pontos foram dispostos, todas as setas apontam de baixo para cima; portanto não é necessário indicar sua direção. Sabendo que  $\mathcal{R}$  é uma relação de ordem, podemos também omitir todos os laços, e todas as linhas que podem ser deduzidas pela transitividade; como  $(1, 3)$ , por exemplo, que pode ser deduzida pelos pares  $(1, 2)$  e  $(2, 3)$ . O resultado dessas simplificações é o diagrama de Hasse (à direita).

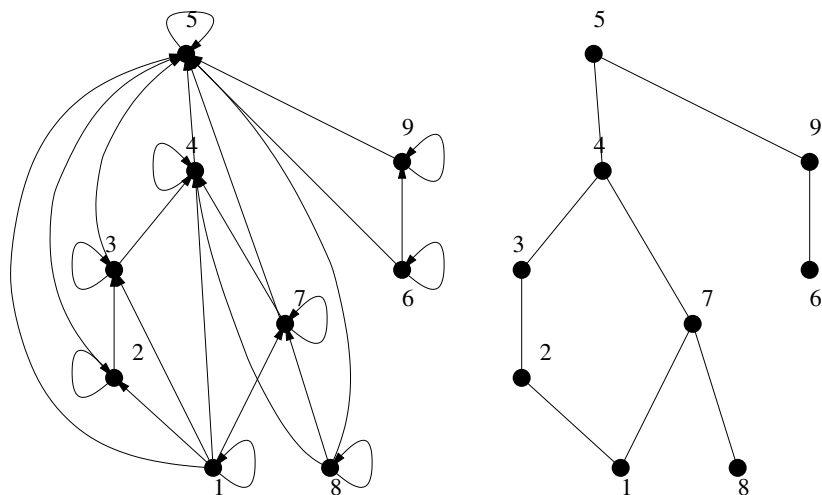


Figura 7.1: Diagrama de pontos e setas do conjunto ordenado  $(A, \mathcal{R})$  (à esquerda) e o diagrama de Hasse (à direita).

Observe que o diagrama de Hasse contém toda a informação necessária para determinar exatamente a relação de ordem  $\mathcal{R}$ .

O diagrama de Hasse pode ser construído também a partir de uma ordem estrita, e é igual ao diagrama da relação de ordem associada.

**Exercício 7.15:** Seja  $A$  o conjunto dos inteiros entre 1 e 20, inclusive. Seja  $\mathcal{R}$  a relação sobre  $A$  tal que  $x \mathcal{R} y$  se, e somente se,  $x$  divide  $y$ . Construa o diagrama de Hasse de  $\mathcal{R}$ .

**Exercício 7.16:** Uma *sub-palavra* de uma palavra  $x$  é uma sequência de letras que aparecem em posições consecutivas em  $x$ , na mesma ordem. Por exemplo, ‘nan’ é uma sub-palavra de ‘banana’, mas ‘bn’ e ‘nab’ não são. Seja  $A$  o conjunto de todas as sub-palavras de ‘banana’, e ‘ $\sqsubset$ ’ a relação sobre  $A$  tal que  $x \sqsubset y$  se e somente se,  $x$  é sub-palavra de  $y$ .

- (a) Prove que ‘ $\sqsubset$ ’ é uma relação de ordem.
- (b) Construa o diagrama de Hasse de ‘ $\sqsubset$ ’.

**Exercício 7.17:** Descreva o diagrama de Hasse de uma ordem total sobre um conjunto finito  $A$ .

### 7.1.6 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 7.4:** Seja  $A = \{2, 4, 6, 8\} \subseteq \mathbb{Z}$ , e seja  $\mathcal{R}$  a relação ‘ $\leq$ ’ (“menor ou igual”) sobre  $\mathbb{Z}$ . O inteiro 2 é um mínimo de  $A$  sob  $\mathcal{R}$ , pois  $(2, a) \in \mathcal{R}$  (ou seja  $2 \leq a$ ) para todo  $a \in A$ .

**Exemplo 7.5:** 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  $b \in A$ .

O conceito de *elemento máximo de  $A$  sob  $\mathcal{R}$*  é inteiramente simétrico. Ou seja, 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.

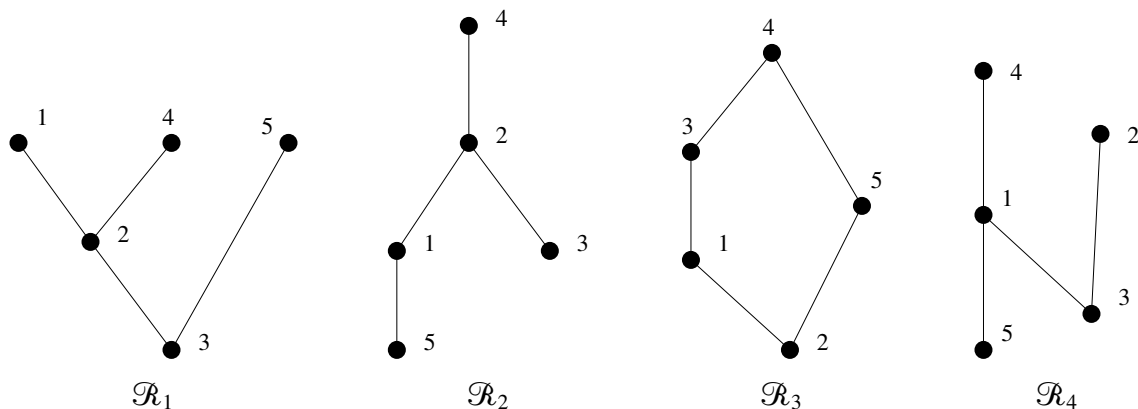


Figura 7.2: Diagramas de Hasse de quatro relações de ordem sobre o conjunto  $\{1, 2, 3, 4, 5\}$ . Na relação  $\mathcal{R}_1$ , o elemento 3 é mínimo e não existe elemento máximo. Na relação  $\mathcal{R}_2$ , o elemento 4 é máximo, e não há elemento mínimo. Na relação  $\mathcal{R}_3$ , o elemento 2 é mínimo e 4 é máximo. Na relação  $\mathcal{R}_4$  não existe nem mínimo nem máximo.

Se  $\mathcal{R}$  é uma relação de ordem total, e o conjunto  $A$  é finito, sempre existe um elemento mínimo. Se  $\mathcal{R}$  não é uma ordem total, ou se  $A$  é infinito, o mínimo pode existir ou não. Em qualquer caso, se existe um elemento mínimo, ele é único. As mesmas observações são válidas para o máximo.

**Exemplo 7.6:** Seja  $A$  o conjunto dos inteiros pares, e  $\mathcal{R}$  a relação “ $\leq$ ” (menor ou igual) sobre  $\mathbb{Z}$ . Não existe nenhum elemento mínimo de  $A$  sob  $\mathcal{R}$ , pois para qualquer inteiro  $m \in A$  o par  $(m - 2, m)$ , por exemplo, está em  $\mathcal{R}$ .

É importante observar que o fato de um elemento ser mínimo depende tanto do conjunto  $A$  quanto da relação  $\mathcal{R}$ . Um elemento que é mínimo sob  $\mathcal{R}$  pode não ser mínimo sob outra relação  $\mathcal{S}$ . Em particular, um elemento mínimo sob  $\mathcal{R}$  é um elemento máximo sob  $\mathcal{R}^{-1}$ , e vice-versa.

Este fato pode gerar confusões se existe uma ordem “usual” para os elementos de  $A$ , distinta da ordem  $\mathcal{R}$ . Por exemplo, no conjunto  $A$  acima do exemplo 7.4, o elemento 8 é mínimo, e 2 é máximo, sob a ordem “ $\geq$ ”.

**Exercício 7.18:** Seja  $A$  o conjunto das palavras de 3 letras da língua portuguesa, e  $\mathcal{R}$  a relação tal que  $a \mathcal{R} b$  se e somente se a palavra  $a$  vem antes da palavra  $b$  no dicionário. Quais são os elementos mínimo e máximo de  $A$  sob  $\mathcal{R}$ ?

**Exercício 7.19:** Seja  $A$  o conjunto das sequências de 4 bits (algarismos 0 ou 1), e  $\mathcal{R}$  a relação tal que  $a \mathcal{R} b$  se e somente se cada bit de  $a$  é menor ou igual ao bit correspondente de  $b$ . Assim, por exemplo,  $0100 \mathcal{R} 1100$ , mas  $1001 \not\mathcal{R} 0101$ . Quais são os elementos mínimo e máximo de  $A$  sob  $\mathcal{R}$ ?

**Exercício 7.20:** Prove que todo conjunto ordenado tem no máximo um elemento mínimo e um elemento máximo.

**Exercício 7.21:** Prove que um conjunto finito não vazio totalmente ordenado tem exatamente um elemento mínimo e um elemento máximo.

### 7.1.7 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  $(a, m) \in \mathcal{R}$ .

**Exemplo 7.7:** 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.

**Exemplo 7.8:** Seja  $A = \mathbb{N} \setminus \{0, 1\}$  e  $\mathcal{R}$  a relação “é divisor próprio de”; isto é,

$$\mathcal{R} = \{(x, y) : x \in A \wedge y \in A \wedge x < y \wedge (\exists k \in \mathbb{N}) y = kx\}.$$

O número 21 não é minimal sob  $\mathcal{R}$  pois existem pares  $(a, 21)$  em  $\mathcal{R}$ , por exemplo  $(3, 21)$ . O número 17 é minimal sob  $\mathcal{R}$  pois não existe nenhum par  $(a, 17)$  em  $\mathcal{R}$ . Note que os elementos minimais de  $A$  sob  $\mathcal{R}$  são os números primos.

Como estes exemplos mostram, uma relação pode não ter elementos minimais, ou pode ter mais de um elemento minimal. É fácil mostrar que um elemento mínimo de  $A$  sob  $\mathcal{R}$ , se existir, é também um elemento minimal (e o único elemento minimal em  $A$ ). O contrário não é verdadeiro: um elemento minimal pode não ser mínimo.

Da mesma forma definimos um *elemento maximal de  $A$  sob  $\mathcal{R}$*  como um elemento  $m$  de  $A$  tal que não existe nenhum  $a$  em  $A$ , diferente de  $m$ , tal que  $(m, a) \in \mathcal{R}$ .

No diagrama de Hasse de  $\mathcal{R}$ , um elemento minimal é qualquer ponto do qual não sai nenhuma linha descendente. Um elemento maximal é um elemento do qual não sai nenhuma linha ascendente. Veja a figura 7.3

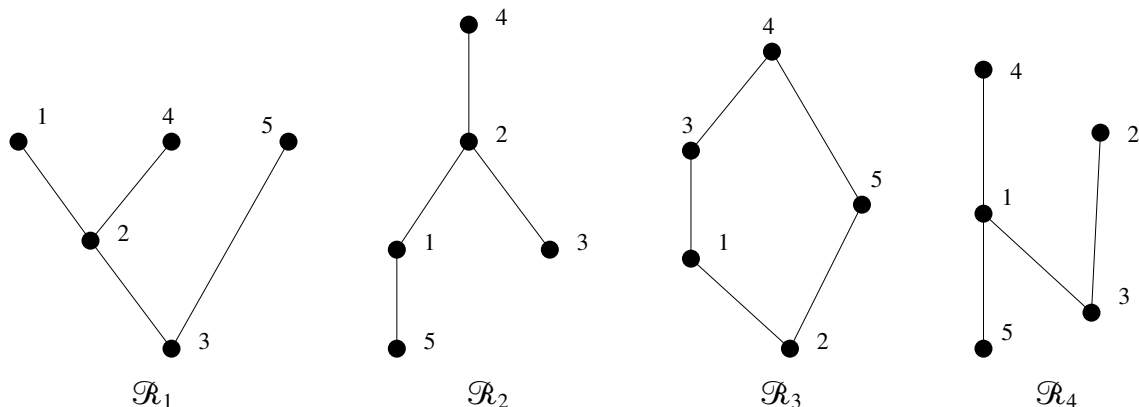


Figura 7.3: Diagramas de Hasse de quatro relações de ordem sobre o conjunto  $\{1, 2, 3, 4, 5\}$ . Na relação  $\mathcal{R}_1$ , o único elemento minimal é 3, e os elementos maximais são 1, 4 e 5. Na relação  $\mathcal{R}_2$ , os elementos minimais são 3 e 5, e o único maximal é 4. Na relação  $\mathcal{R}_3$ , o único minimal é 2 e o único maximal é 4. Na relação  $\mathcal{R}_4$  os minimais são 3 e 5, e os maximais são 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

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

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  $\{3, 4, 5\}$ .

**Exercício 7.22:** Encontre um conjunto  $A$  e uma relação de ordem  $\mathcal{R}$  sobre  $A$  tal que existe um único elemento minimal em  $A$  sob  $\mathcal{R}$ , mas que não é mínimo.

**Exercício 7.23:** Prove que um conjunto finito ordenado tem pelo menos um elemento minimal e um elemento maximal.

**Exercício 7.24:** Seja  $A = \{3, 6, 9, \dots\}$  o conjunto dos múltiplos positivos de 3, e  $\mathcal{R}$  a relação sobre  $A$  tal que  $(x, y)$  está em  $\mathcal{R}$  se e somente se todos os algarismos decimais de  $x$  aparecem em  $y$ , na mesma sequência. Assim, por exemplo, **(262, 12682)** está em  $\mathcal{R}$ , mas **(262, 12268)** não está. Determine os elementos minimais de  $A$  sob  $\mathcal{R}$ .

**Exercício 7.25:** Seja  $A = \{X \subseteq \mathbb{N} : X \neq \{\} \wedge |X| \text{ é par}\}$ . Note que  $A$  não é um conjunto de inteiros, mas sim um conjunto de conjuntos:  $\{1, 2, 3, 4\}$  e  $\{10, 20\}$  são elementos de  $A$ , enquanto que  $20$  e  $\{20, 40, 60\}$  não são. Seja  $\mathcal{R}$  a relação “ $\subseteq$ ” de continência de conjuntos. Encontre os elementos minimais de  $A$  sob  $\mathcal{R}$ . Existe algum elemento maximal de  $A$  sob  $\mathcal{R}$ ?

**Exercício 7.26:** Seja  $\mathcal{R} = \{(x, y) \in N - \{0\} \times N - \{0\} : x \text{ divide } y\}$ .

1. Prove que  $\mathcal{R}$  é uma relação de ordem definida sobre  $N - \{0\}$ .
2. A relação de ordem  $\mathcal{R}$  é total? Prove ou dê um contra-exemplo.
3. Quais são os elementos minimais de  $N - \{0\}$  sob  $\mathcal{R}$ ?
4. O conjunto  $N - \{0\}$  tem um elemento mínimo sob  $\mathcal{R}$ ?

**Exercício 7.27:** Seja  $A$  o conjunto das sequências de 4 bits (algarismos 0 ou 1), exceto a sequência 0000; e seja  $\mathcal{R}$  a relação tal que  $a \mathcal{R} b$  se e somente se cada bit de  $a$  é menor ou igual ao bit correspondente de  $b$ . Assim, por exemplo, 0100  $\mathcal{R}$  1100, mas 1001  $\mathcal{R}$  0101. Quais são os elementos mínimos, máximos, minimais e maximais de  $A$  sob  $\mathcal{R}$ ?

## 7.2 Relações de equivalência

**Definição 7.4:** Uma *relação de equivalência sobre* um conjunto  $A$  é uma relação  $\mathcal{R}$  sobre  $A$  que é reflexiva sobre  $A$ , simétrica e transitiva.

**Exemplo 7.9:** 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  $X \cap Y = \{\}$ . 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.

**Exemplo 7.10:** Sejam  $\mathbb{Z}$  o conjunto dos números inteiros. A relação

$$\mathcal{R} = \{(a, b) : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge (a - b) \text{ é múltiplo de } 5\}$$

é uma relação de equivalência. Verificando:

- $\mathcal{R}$  é reflexiva sobre  $\mathbb{Z}$ : para todo  $a \in \mathbb{Z}$ , temos  $(a, a) \in \mathcal{R}$ , pois  $a - a = 0 \cdot 5$ .
- $\mathcal{R}$  é simétrica: para todo  $(a, b) \in \mathcal{R}$ , temos  $a - b = 5r$  para algum  $r \in \mathbb{Z}$ ; logo  $b - a = 5(-r)$ , portanto  $(b, a) \in \mathcal{R}$ .
- $\mathcal{R}$  é transitiva: para todo  $(a, b) \in \mathcal{R}$  e todo  $(b, c) \in \mathcal{R}$ , temos  $a - b = 5r$  para algum  $r \in \mathbb{Z}$ , e  $b - c = 5s$  para algum  $s \in \mathbb{Z}$ ; logo  $c = b - 5s$ ,  $a - c = a - b + 5s = 5r + 5s = 5(r + s)$ ; portanto  $(a, c) \in \mathcal{R}$ .

No exemplo 7.10 o número 5 pode ser substituído por qualquer inteiro  $m$ . Esta relação é denominada *congruência módulo  $m$* .

**Exemplo 7.11:** Para todo conjunto  $A$ , a relação de identidade  $\mathcal{I}_A$  é uma relação de equivalência sobre  $A$ .

**Exemplo 7.12:** Para todo conjunto  $A$ , o produto cartesiano  $A \times A$  é uma relação de equivalência sobre  $A$  (onde quaisquer dois elementos estão relacionados entre si).

**Exemplo 7.13:** Seja  $A$  um conjunto não vazio. A relação  $\subseteq$  entre os conjuntos de  $\mathcal{P}(A)$  é reflexiva sobre  $\mathcal{P}(A)$  e transitiva, mas não é uma relação de equivalência sobre  $\mathcal{P}(A)$ , pois ela não é simétrica (por exemplo,  $\{\} \subseteq A$  mas  $A \not\subseteq \{\}$ ).

Se  $\mathcal{R}$  é uma relação de equivalência, a notação  $a \mathcal{R} b$  também pode ser lida “ $a$  é equivalente a  $b$  módulo  $\mathcal{R}$ ,” e denotada por  $a \equiv b \bmod \mathcal{R}$ . Analogamente,  $a \not\mathcal{R} b$  pode ser lida “ $a$  não é equivalente a  $b$  módulo  $\mathcal{R}$ ,” e denotada por  $a \not\equiv b \bmod \mathcal{R}$ .

### 7.2.1 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 7.14:** Vamos construir as classes de equivalência da relação  $\mathcal{R}$  de congruência módulo 5 (exemplo 7.10). 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  $r \in \mathbb{Z}$ ; 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:

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

- $[4]_{\mathcal{R}} = \{\dots, -6, -1, 4, 9, 14, \dots\}$ .

**Teorema 7.1:** Seja  $\mathcal{R}$  uma relação de equivalência sobre um conjunto  $A$ . As seguintes afirmações são equivalentes.

- $a \mathcal{R} b$ .
- $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ .
- $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \{\}$

**Prova:**

- Vamos provar que  $a \mathcal{R} b \rightarrow [a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ . Seja  $c$  um elemento qualquer de  $[a]_{\mathcal{R}}$ . Por definição,  $c \mathcal{R} a$ . Como  $\mathcal{R}$  é uma relação de equivalência, se  $a \mathcal{R} b$  então  $c \mathcal{R} b$  (por transitividade), e portanto  $c \in [b]_{\mathcal{R}}$ . Concluimos assim que  $[a]_{\mathcal{R}} \subseteq [b]_{\mathcal{R}}$ . Analogamente prova-se que  $[b]_{\mathcal{R}} \subseteq [a]_{\mathcal{R}}$ . Portanto  $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ .
- Vamos provar que  $[a]_{\mathcal{R}} = [b]_{\mathcal{R}} \rightarrow [a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \{\}$ . Se  $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ , então  $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = [a]_{\mathcal{R}} \cap [a]_{\mathcal{R}} = [a]_{\mathcal{R}}$ . Como  $\mathcal{R}$  é reflexiva sobre  $A$ , temos  $a \in [a]_{\mathcal{R}}$ , logo  $[a]_{\mathcal{R}} \neq \{\}$ . Concluimos que  $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \{\}$ .
- Vamos provar que  $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \{\} \rightarrow a \mathcal{R} b$ . Como  $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \{\}$  então existe um  $c \in A$  tal que  $c \in [a]_{\mathcal{R}}$  e  $c \in [b]_{\mathcal{R}}$ . Por definição,  $c \mathcal{R} a$  e  $c \mathcal{R} b$ . Por simetria e transitividade de  $\mathcal{R}$ , concluimos que  $a \mathcal{R} b$ .

**Fim.**

Cada elemento de uma classe de equivalência é chamado de um *representante* dessa classe.

### 7.2.2 Relações de equivalência e partições

O que o teorema 7.1 nos mostra é as que 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  $A$ . (Veja a seção 2.5.)

Vamos mostrar agora que toda partição de um conjunto pode ser usada para construir uma relação de equivalência sobre esse conjunto. Dizemos que dois elementos estão relacionados se e somente se eles estão no mesmo bloco da partição. Mais precisamente:

**Teorema 7.2:** Sejam  $P$  uma partição do conjunto  $A$ , e  $\mathcal{S}_P$  a relação

$$\mathcal{S}_P = \{(x, y) : (\exists C \in P) x \in C \wedge y \in C\}.$$

Então  $\mathcal{S}_P$  é uma relação de equivalência, e suas classes são os blocos da partição  $P$ .

**Prova:**

Para mostrar que  $\mathcal{S}_P$  é uma relação de equivalência, precisamos mostrar que ela é reflexiva sobre  $A$ , simétrica e transitiva.

- A relação é reflexiva sobre  $A$ : para todo  $a \in A$ , temos  $a \mathcal{S}_P a$ ; pois, pela definição de partição, todo elemento de  $A$  pertence a algum bloco  $C$  da partição  $P$ .
- A relação é simétrica: para todo  $(a, b) \in \mathcal{S}_P$ , por definição  $a$  e  $b$  pertencem a algum sub-conjunto  $C \in P$ ; logo  $b \mathcal{S}_P a$ .

- A relação é transitiva: para quaisquer  $(a, b)$  e  $(b, c)$  em  $\mathcal{S}_P$ , existem blocos  $C$  e  $D$  de  $P$  tais que  $a, b \in C$  e  $b, c \in D$ ; logo  $b \in C \cap D$ . Como os blocos de uma partição são disjuntos dois a dois, concluímos que  $C$  e  $D$  são o mesmo bloco. Portanto  $a$  e  $c$  pertencem ao mesmo bloco, logo  $a \mathcal{S}_P c$ .

**Fim.**

**Exercício 7.28:** Seja  $\mathcal{S} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Q}\}$ . Prove que  $\mathcal{S}$  é uma relação de equivalência.

**Exercício 7.29:** Seja  $\mathcal{R}$  uma relação sobre o conjunto dos pares ordenados de inteiros positivos definida por  $((a, b) \mathcal{R} (c, d))$  se, e somente se,  $ad = bc$ .

- (a) Prove que  $\mathcal{R}$  é uma relação de equivalência.
- (b) Descreva a classe de equivalência de  $(1, 2)$  segundo a relação  $\mathcal{R}$ .

**Exercício 7.30:** Seja  $\mathcal{R}$  uma relação sobre o conjunto dos pares ordenados de inteiros positivos definida por  $((a, b) \mathcal{R} (c, d))$  se, e somente se,  $a + d = b + c$ .

- (a) Prove que  $\mathcal{R}$  é uma relação de equivalência.
- (b) Descreva a classe de equivalência de  $(3, 1)$  segundo a relação  $\mathcal{R}$ .
- (c) Descreva as classes de equivalência de  $\mathcal{R}$ .

**Exercício 7.31:** Prove que as relações descritas a seguir são relações de equivalência. Descreva as classes de equivalência de cada uma das relações.

- (a) Seja  $\mathcal{R}$  a relação sobre  $\mathbb{Z}$  definida por  $m \mathcal{R} n$  se, e somente se, 2 divide  $m - n$ .
- (b) Seja  $\mathcal{S}$  a relação sobre  $\mathbb{R}$  definida por  $x \mathcal{R} y$  se, e somente se,  $|x| = |y|$ .
- (c) Seja  $\mathcal{F}$  a relação sobre inteiros positivos definida por  $x \mathcal{F} y$  se, e somente se, todo número primo que divide  $x$  divide  $y$ , e vice-versa.

**Exercício 7.32:** Seja  $\mathbb{A}$  o conjunto de todas as fórmulas lógicas abertas que dependem apenas das variáveis lógicas  $x$ ,  $y$  e  $z$ . Seja  $\mathcal{L}$  uma relação sobre  $\mathbb{A}$  definida por  $P \mathcal{L} Q$  se, e somente se,  $P$  e  $Q$  tem a mesma tabela verdade. Prove que  $\mathcal{L}$  é uma relação de equivalência.

**Exercício 7.33:** Seja  $\varepsilon$  um número real positivo, e considere a relação  $\approx_\varepsilon$  sobre  $\mathbb{R}$  tal que

$$x \approx_\varepsilon y \leftrightarrow |x - y| \leq \varepsilon$$

para quaisquer  $x$  e  $y$  em  $\mathbb{R}$ . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

**Exercício 7.34:** Considere a relação  $\mathcal{R}$  sobre os pares ordenados de inteiros  $\mathbb{Z} \times \mathbb{Z}$  tal que

$$(a, b) \mathcal{R} (c, d) \leftrightarrow ((a = c) \wedge (b = d)) \vee ((a = d) \wedge (b = c))$$

para quaisquer inteiros  $a, b, c$  e  $d$ . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

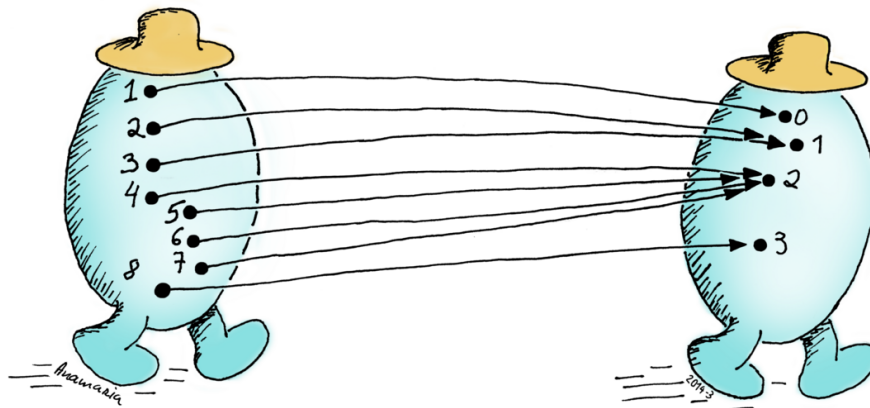
**Exercício 7.35:**

- (a) Prove que, se  $\mathcal{R}$  é uma relação simétrica, então  $\mathcal{R}^k$  é simétrica para qualquer inteiro positivo  $k$ .
- (b) Seja  $\mathcal{R}$  uma relação qualquer sobre um conjunto  $A$ , e  $\mathcal{I}_A$  a identidade sobre  $A$ . Seja  $\mathcal{S}$  a relação  $\mathcal{R} \cup \mathcal{R}^{-1} \cup \mathcal{I}_A$ . Prove que o fecho transitivo  $\mathcal{T}$  de  $\mathcal{S}$  é uma relação de equivalência sobre  $A$ .



# Capítulo 8

## Funções



## 8.1 Conceito

Dizemos que 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  $(a, b) \in \mathcal{F}$ .

**Exemplo 8.1:** O conjunto de pares  $f = \{(1, 20), (2, 50), (5, 50), (9, 40)\}$  é uma função do conjunto  $A = \{1, 2, 5, 9\}$  para o conjunto  $B = \{20, 30, 40, 50, 60\}$ . Note que, para cada elemento  $a$  de  $A$ , existe um, e apenas um, elemento  $b$  tal que  $(a, b) \in f$ .

Pelo fato de ser uma relação, uma função  $\mathcal{F}$  de  $A$  para  $B$  é um subconjunto do produto cartesiano  $A \times B$ , ou seja um conjunto de pares  $(a, b)$  com  $a \in A$  e  $b \in B$ , com a propriedade acima. (Veja seção 6.1).

Para indicar que  $\mathcal{F}$  é uma função de  $A$  para  $B$ , usa-se geralmente a notação  $\mathcal{F} : A \rightarrow B$ . 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 8.2:** 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 8.3:** 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 8.4:** A relação  $\mathcal{F} = \{(x, x^2) : x \in \mathbb{Z}\}$  é uma função do conjunto  $\mathbb{Z}$  para o conjunto  $\mathbb{N}$ , isto é  $\mathcal{F} : \mathbb{Z} \rightarrow \mathbb{N}$ .

**Exemplo 8.5:** A relação  $\mathcal{F} = \{(x^2, x) : x \in \mathbb{Z}\}$  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.

### 8.1.1 Especificando uma função

Todas as maneiras de especificar relações mencionadas na seção 6.1.1 também podem ser usadas para especificar funções — desde que a propriedade básica (seção 8.1) seja satisfeita. Por exemplo, uma função de  $A$  para  $B$  pode ser descrita por um diagrama de setas, tal que existe uma e apenas uma seta saindo de cada elemento de  $A$ . Veja a figura 8.1 (esquerda). Ou por um diagrama de pontos onde há apenas um ponto marcado em cada linha vertical. Veja a figura 8.1 (direita). Se  $A$  e  $B$  são conjuntos de números, e as linhas são rotuladas em ordem crescente de valor, o diagrama de pontos é dito o *gráfico* da função.

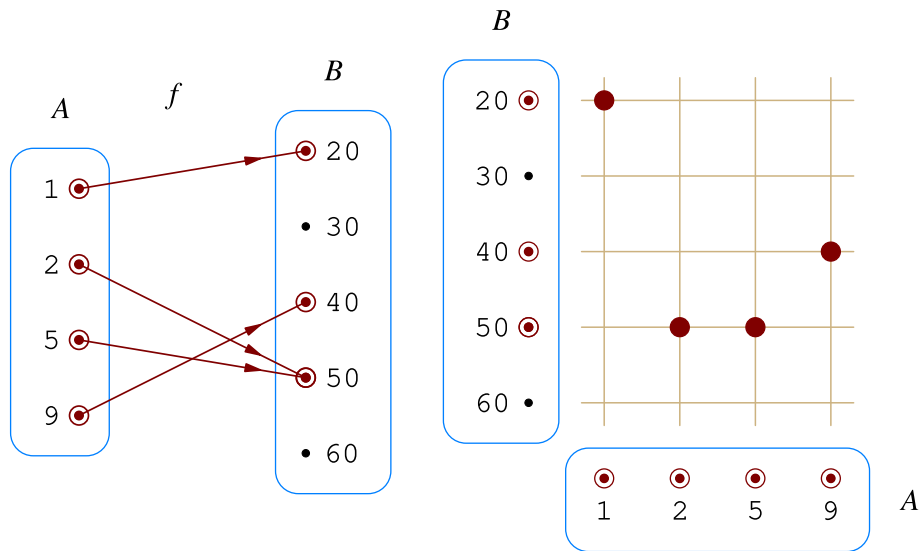


Figura 8.1: Diagrama de setas (à esquerda) e gráfico (à direita) da função  $f$  do exemplo 8.1. Nos dois diagramas, os elementos destacados de  $A$  e  $B$  são o domínio e a imagem de  $f$ , respectivamente.

Como discutido na seção 6.1.1, uma função ser especificada também por fórmula algébrica ou algoritmo que diz se um par de elementos  $(a, b)$  está em  $f$ ; ou seja, se  $f(a) = b$ .

Além disso, uma função de  $A$  para  $B$  também pode ser especificada por uma fórmula algébrica ou algoritmo que, dado um elemento qualquer  $a$  de  $A$ , sempre devolve um e um único elemento  $b$  de

$B$ , tal que  $f(a) = b$ . Veja os exemplos 8.4 acima e 8.6 e 8.7 abaixo.

**Exemplo 8.6:** Seja  $d$  a função de  $\mathcal{Q} = \mathbb{N} \setminus \{0, 1\}$  para  $\mathbb{N}$  tal que  $d(n)$  é o menor divisor primo de  $n$ . Alguns pares de  $d$  são

$$(2, 2), (3, 2), (4, 2), (5, 5), (6, 2), (7, 7), (8, 2), (9, 3), \dots$$

Até hoje não se conhece nenhuma fórmula algébrica explícita que calcule  $d(n)$  diretamente a partir de  $n$ . Mas esta função pode ser definida dizendo que  $d(n) = v$  (ou seja,  $(n, v) \in d$ ) se e somente se  $n$  e  $v$  satisfazem o predicado

$$(n, v \in \mathcal{Q}) \wedge (v|n) \wedge (\forall u \in \mathcal{Q})(u|n) \rightarrow (u \geq v)$$

Verifica-se que, para cada  $n$ , existe um único  $v$  que satisfaz este predicado, e portanto  $d$  é uma função.

**Exemplo 8.7:** Seja  $p$  a função de  $\mathbb{N}$  para  $\mathbb{N}$  tal que  $p(n)$  é o elemento  $n$  na lista dos primos em ordem crescente, contando a partir de zero. Os primeiros pares são função são

$$(0, 2), (1, 3), (2, 5), (3, 7), (4, 11), (5, 13), (6, 17), (7, 19), \dots$$

Esta função tampouco tem uma fórmula algébrica explícita para o termo geral. Porém a função pode ser definida precisamente por um algoritmo que produz o valor  $p(n)$  dado  $n$ .

Uma função, finita ou infinita, também pode ser definida por um predicado que se aplica a toda a função. Naturalmente uma definição deste tipo é válida se e somente se existe uma função, e apenas uma, com as propriedades dadas.

### 8.1.2 Domínio e imagem de uma função

Uma vez que funções são um tipo particular de relações, 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  $\text{Dom}(f)$  de  $f$  é sempre o conjunto  $A$ . veja a figura 8.1.

A imagem ou contra-domínio  $\text{Img}(f)$  de  $f$  é o conjunto

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

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

Podemos portanto dizer que duas funções  $f : A \rightarrow B$  e  $g : C \rightarrow D$  são a mesma função se, e somente se,  $A = C$  e  $(\forall a \in A) f(a) = g(a)$ .

Como observamos no caso de relações em geral, se  $f$  é uma função de  $A$  para  $B$  e  $B \subseteq C$ , então  $f$  também é uma função de  $A$  para  $C$ . Por exemplo, a função *seno* é uma função do conjunto dos números reais  $\mathbb{R}$  para o intervalo  $B = [-1, +1]$ . Como  $B$  é um subconjunto de  $\mathbb{R}$ , então *seno* também é uma função de  $\mathbb{R}$  para  $\mathbb{R}$ .

Porém, precisamos observar que alguns autores consideram que o conjunto  $B$  é parte da definição da função. Nesta abordagem, se  $f$  for definida como função de  $A$  para  $B$ , e  $C$  for um conjunto diferente de  $B$ , então  $f$  *não* é uma função de  $A$  para  $C$ . Para esses autores, por exemplo, *seno* pode ser definida como função de  $\mathbb{R}$  para  $\mathbb{R}$ , ou de  $\mathbb{R}$  para  $[-1, +1]$ ; mas estas duas escolhas resultam em funções distintas. Neste livro não seguimos essa abordagem: para nós, uma função, assim como uma relação, é apenas o conjunto dos seus pares.

**Exercício 8.1:** Seja  $f$  uma função e  $\mathcal{R}$  uma relação sobre  $\text{Dom}(f)$  tal que para todo  $x$  e  $y$   $x\mathcal{R}y \leftrightarrow f(x) = f(y)$  para todo  $x, y \in \text{Dom}(f)$ .

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

## 8.2 Inversa de função

A inversa de uma função  $f$  é definida como na seção 6.1.5, ou seja, é a relação

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

Note que a inversa de uma função nem sempre é uma função. Veja a figura 8.2.

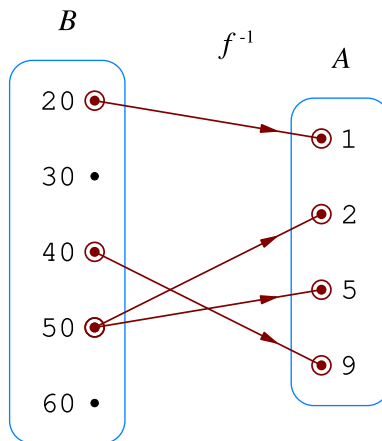


Figura 8.2: Relação  $f^{-1}$  que é a inversa da função  $f$  do exemplo 8.1 e da figura 8.1.

**Exemplo 8.8:** Seja  $f$  a função de  $\mathbb{R}$  para  $\mathbb{R}$  tal que  $f(x) = x^2$ . Sua inversa é a relação

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

que associa a cada número real  $y \geq 0$  suas duas raízes quadradas  $-\sqrt{y}$  e  $+\sqrt{y}$ . Esta relação não é uma função.

**Exercício 8.2:** Para cada uma das seguintes funções de  $\mathbb{R}$  para  $\mathbb{R}$ , determine se a inversa é uma função:

- (a)  $f_1(x) = x^3$ .
- (b)  $f_2(x) = e^x$ .
- (c)  $f_3(x) = \sin x$ .
- (d)  $f_4(x) = x^5 + x$ .
- (e)  $f_5(x) = x^5 - x$ .

## 8.3 Imagem e imagem inversa de um conjunto

Para qualquer função  $f$  e qualquer conjunto  $X$ , verifica-se que a imagem de  $X$  sob  $f$ , definida na seção 6.1.6, é

$$f(X) = \{f(x) : x \in (X \cap \text{Dom}(f))\} = \{y \in \text{Img}(f) : (\exists x \in X) f(x) = y\}$$

Note que os elementos de  $X$  que não estão em  $\text{Dom}(f)$  não contribuem para a imagem. Este conceito é geralmente usado quando  $X \subseteq \text{Dom}(f)$ . A imagem inversa de um conjunto  $Y$  qualquer sob  $f$ , também definida na seção 6.1.6, é a imagem de  $Y$  sob a relação inversa  $f^{-1}$ , ou seja

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

Observe que a relação  $f^{-1}$  pode não ser uma função. Isto não é um problema uma vez que os conceitos de imagem e imagem inversa são definidos para relações em geral.

## 8.4 Restrição

O conceito de restrição de relações pode ser aplicado também a funções. Se  $f$  é uma função e  $X$  é um conjunto, a notação  $f|X$  ou  $f|_X$  é frequentemente usada para indicar a restrição de  $f$  (vista como relação) aos conjuntos  $X$  e  $\text{Img}(f)$ . Isto é,

$$f|X = f \cap (X \times \text{Img}(f)) = \{(x, y) : (x, y) \in f \wedge x \in X\}$$

Este conceito também é geralmente usado quando  $X$  é um subconjunto de  $\text{Dom}(f)$ .

**Exercício 8.3:** Sejam  $f$  uma função,  $A, B$  subconjuntos de  $\text{Dom}(f)$  e  $U, V$  subconjuntos de  $\text{Img}(f)$ . Prove ou encontre contra-exemplos para cada uma destas afirmações:

- (a)  $f(A \cup B) = f(A) \cup f(B)$ .
- (b)  $f(A \setminus B) = f(A) \setminus f(B)$ .
- (c)  $B \subseteq A \leftrightarrow f(B) \subseteq f(A)$ .
- (d)  $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$ .
- (e)  $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$ .
- (f)  $f^{-1}(U \setminus V) = f^{-1}(U) \setminus f^{-1}(V)$ .
- (g)  $U \subseteq V \leftrightarrow f^{-1}(U) \subseteq f^{-1}(V)$ .
- (h)  $f^{-1}(f(A)) = A$ .
- (i)  $f(f^{-1}(U)) = U$ .

**Exercício 8.4:** Seja  $f$  uma função de um conjunto  $A$  para um conjunto  $B$ . Considere a relação  $\mathcal{R}$  sobre  $A$  tal que

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

para quaisquer elementos  $a$  e  $b$  de  $A$ . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

## 8.5 Composição de funções

Uma vez que funções são relações, a composição de duas funções  $f$  e  $g$  é definida da mesma forma que para relações, ou seja, é a relação

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

Em particular, se  $f : A \rightarrow B$  e  $g : B \rightarrow C$ , 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:

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

Veja o exemplo 8.9 e a figura 8.3.

**Exemplo 8.9:** Sejam  $A = \{1, 2, 5, 9\}$ ,  $B = \{20, 30, 40, 50, 60\}$ , e  $C = \{200, 300, 400, 500\}$ . Considere as funções  $f = \{ \}$  de  $A$  para  $B$  (como no exemplo 8.1) e  $g = \{ \}$  de  $B$  para  $C$ . A composição de  $f$  com  $g$  é a função  $g \circ f = \{ \}$  de  $A$  para  $C$ .

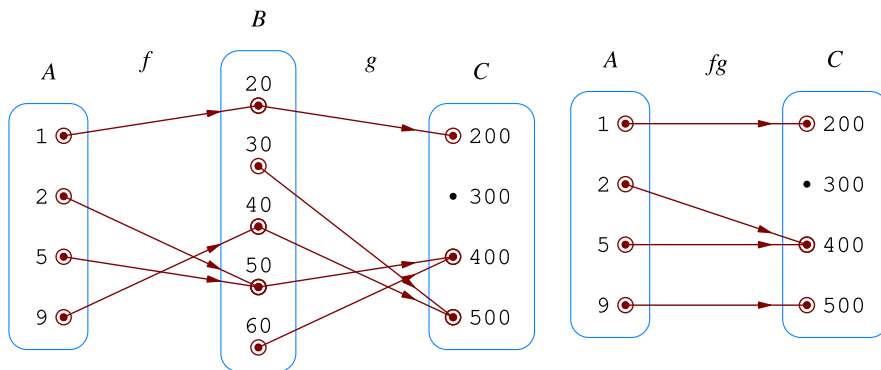


Figura 8.3: Composição das funções  $f$  e  $g$  do exemplo 8.9.

**Exemplo 8.10:** Por exemplo, sejam  $f : \mathbb{R} \rightarrow \mathbb{R}$  com  $f(x) = 2x + 3$ , e  $g : \mathbb{R} \rightarrow \mathbb{R}$  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.

Na verdade, demonstra-se que a composição de duas funções quaisquer é sempre uma função. Como vimos na seção 6.2 é também verdade que

$$\text{Dom}(g \circ f) \subseteq \text{Dom}(f)$$

e

$$\text{Img}(g \circ f) \subseteq \text{Img}(g)$$

Além disso, no caso de funções, temos que

$$\text{Img}(f) \subseteq \text{Dom}(g) \Leftrightarrow \text{Dom}(g \circ f) = \text{Dom}(f)$$

e

$$\text{Dom}(g) \subseteq \text{Img}(f) \Leftrightarrow \text{Img}(g \circ f) = \text{Img}(g)$$

As potências de uma função  $f$  são definidas da mesma forma que as potências de uma relação. Isto é,  $f^1 = f$ , e, para todo inteiro  $n > 1$ ,

$$\begin{aligned} f^{n+1} &= f^n \circ f \\ f^{-(n+1)} &= f^{-n} \circ f^{-1} \end{aligned}$$

Todas as potências positivas são funções, com mesmo domínio que  $f$ . Se a inversa  $f^{-1}$  é uma função, então todas as potências negativas são funções, com mesmo domínio que  $f^{-1}$ .

**Exemplo 8.11:** Seja  $f$  a função logaritmo,  $f(x) = \log x$ ,  $g$  a função raiz quadrada,  $g(y) = \sqrt{y}$ . Seja  $\mathbb{R}^+$  o conjunto de todos os reais não negativos.

$$\begin{aligned} \text{Dom}(f) &= \mathbb{R}^+ \setminus \{0\} & \text{Dom}(g) &= \mathbb{R}^+ \\ \text{Img}(f) &= \mathbb{R} & \text{Img}(g) &= \mathbb{R}^+ \end{aligned}$$

Observe que a imagem de  $f$  não está contida no domínio de  $g$ . A composição  $g \circ f$  é a raiz quadrada do logaritmo,  $(g \circ f)(x) = \sqrt{\log x}$ . O domínio desta função não é  $\text{Dom}(f)$ , mas o conjunto dos números reais maiores ou iguais a 1, que é subconjunto próprio de  $\text{Dom}(f)$ . Por outro lado, a imagem de  $g \circ f$  é  $\mathbb{R}^+$ , que neste exemplo é igual a  $\text{Img}(g)$ .

**Exemplo 8.12:** Sejam  $f$  e  $g$  as funções logaritmo e raiz quadrada, como no exemplo 8.11. A composição  $f \circ g$  é o logaritmo da raiz quadrada,  $(f \circ g)(y) = \log \sqrt{y}$ ; como  $\text{Img}(g) \subseteq \text{Dom}(f)$ , então  $\text{Dom}(f \circ g) = \text{Dom}(g) = \mathbb{R}^+$ ; e como  $\text{Dom}(g) \subseteq \text{Img}(f)$ ,  $\text{Img}(f \circ g) = \text{Img}(f) = \mathbb{R}$ .

### 8.5.1 Função idempotente

Uma função  $f$  é dita *idempotente* se a composição  $f \circ f$  é igual a  $f$ . Ou seja, se  $f(f(x)) = f(x)$  para todo  $x \in \text{Dom}(f)$ . Esta condição também equivale a dizer que  $f$  restrita a  $\text{Img}(f)$  é a função identidade sobre  $\text{Img}(f)$ . Um exemplo é a função  $f$  com domínio  $\mathbb{N} \setminus \{0, 1\}$  tal que  $f(z)$  é o menor fator primo de  $z$ .

**Exercício 8.5:** Prove, ou encontre um contra-exemplo, que a composição de duas funções idempotentes é uma função idempotente.

Em álgebra linear, uma transformação linear idempotente é chamada de *projecção*.

## 8.6 Tipos de funções

### 8.6.1 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 8.6:** 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.

**Exercício 8.7:** Seja  $f$  uma função. Prove que a relação inversa  $f^{-1}$  também é uma função se e somente se  $f$  é injetora.

**Exercício 8.8:** Sejam  $f : A \rightarrow C$  e  $g : B \rightarrow D$  duas funções injetoras. Considere a função  $h : A \times B \rightarrow C \times D$  tal que

$$h(a, b) = (f(a), g(b))$$

Prove que  $h$  é uma função injetora.

**Exercício 8.9:** Sejam  $f$  uma função e  $A, B$  subconjuntos de  $\text{Dom}(f)$ . Prove que  $f(A \cap B) \subseteq f(A) \cap f(B)$ . Mais ainda, se  $f$  é injetora então  $f(A \cap B) = f(A) \cap f(B)$ .

**Exercício 8.10:** Sejam  $f : A \rightarrow B$ ,  $g : B \rightarrow C$ . Prove que se  $f$  e  $g$  são injetoras então  $g \circ f$  é injetora.

**Exercício 8.11:** Seja  $\mathcal{R}$  uma relação de  $A$  para  $B$ . Escreva expressões lógicas formais (sem palavras, apenas variáveis e símbolos), com todos os quantificadores necessários, que expresse as afirmações

- (a) “A relação  $\mathcal{R}$  é transitiva.”
- (b) “A relação  $\mathcal{R}$  é uma função injetora.”

### 8.6.2 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  $B = \text{Img}(f)$ . 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 8.12:** Sejam  $f : A \rightarrow B$ ,  $g : B \rightarrow C$ . Prove que se  $f$  é sobrejetora em  $B$ , e  $g$  é sobrejetora em  $C$ , então  $g \circ f$  é sobrejetora em  $C$ .

### 8.6.3 Função bijetora

**Definição 8.1:** 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  $B$ .

Dito de outra forma, uma relação  $f$  é uma bijeção de  $A$  para  $B$  se, e somente se,  $(\forall a \in A)(\exists! b \in B)(f(a) = b)$  (isto é,  $f$  é uma função de  $A$  para  $B$  e  $(\forall b \in B)(\exists! x \in A)(f(x) = b)$ ). Observe que a inversa de uma bijeção de  $A$  para  $B$  também é uma bijeção de  $B$  para  $A$ .

Se  $f$  é uma bijeção do conjunto  $A$  para o conjunto  $B$ , então verifica-se que a inversa  $f^{-1}$  também é uma bijeção do conjunto  $B$  para o conjunto  $A$ . Nesse caso, para todo  $a$  em  $A$  e todo  $b$  em  $B$  temos  $(f^{-1}(b) = a) \leftrightarrow (f(a) = b)$ . Portanto,

$$(\forall a \in A) f^{-1}(f(a)) = a$$

e

$$(\forall b \in B) f(f^{-1}(b)) = b$$

Por outro lado, se estas propriedades valem, então  $f$  é uma bijeção de  $A$  para  $B$ . Ou seja,  $f$  é uma bijeção de  $A$  para  $B$  se, e somente se,  $f^{-1} \circ f = \mathcal{I}_A$  e  $f \circ f^{-1} = \mathcal{I}_B$ .

Funções bijetoras são muito importantes em matemática e computação. Entre outras coisas, elas permitem definir o “tamanho” de conjuntos infinitos, como veremos no capítulo 13.

**Exercício 8.13:** Sejam  $A$  e  $B$  dois conjuntos não vazios. Considere a função  $p : A \times B \rightarrow A$  onde  $p((a, b)) = a$ . Prove as afirmações abaixo ou dê um contra-exemplo.

- (a) A função  $p$  é uma função sobrejetora.
- (b) A função  $p$  é uma função bijetora.

## 8.7 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 8.13:** 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 8.14:** Sejam  $m, n$  inteiros positivos quaisquer, e seja  $A = \{x \in \mathbb{N} : x < n\}$ . Seja  $f : A \rightarrow A$  tal que  $f(x)$  é o resto da divisão de  $x + m$  por  $n$ . Verifica-se que  $f$  é uma permutação de  $A$

**Exercício 8.14:** Liste todas as permutações do conjunto  $A = \{10, 20, 30\}$ .

**Exercício 8.15:** Liste todas as permutações do conjunto  $A = \{10, 20, 30, 40\}$ .

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  $f(x)$ .

Uma permutação  $f$  também pode ser entendida como uma maneira de trocar o conteúdo de uma coleção de caixas rotuladas com elementos de  $A$ . Nesse caso, para cada  $x$  em  $A$ , o elemento na caixa de rótulo  $x$  deve ser transferido para a caixa de rótulo  $f(x)$ . Ou então, a caixa de rótulo  $x$  deve receber o conteúdo da caixa de rótulo  $f(x)$ . Nas duas interpretações, entende-se que todas as trocas são realizadas simultaneamente.

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  $\{0 \dots n - 1\}$ .

Um *elemento fixo* de uma função  $f : A \rightarrow A$  é um elemento  $x \in \text{Dom}(f)$  tal que  $f(x) = x$ . No exemplo 8.13 o inteiro 10 é um elemento fixo de  $f$ . Em uma função identidade, todos os elementos do domínio são fixos. Uma permutação que não é a identidade ainda pode ter um ou mais elementos fixos. Os nomes *permutação caótica* ou *desarranjo* são usados para permutações que não tem nenhum elemento fixo.

**Exercício 8.16:** Considere uma caixa quadrada de papelão com tampa. Suponha que os lados da caixa e da tampa são rotulados em ordem anti-horária com inteiros de 0 a 3. Cada maneira de fechar a caixa com a tampa corresponde a uma permutação  $f$  do conjunto  $A = \{0, 1, 2, 3\}$ , tal que  $f(k)$  é o lado da tampa que é encaixado sobre o lado  $k$  da caixa, para cada  $k$  em  $A$ . Escreva as permutações de  $A$  que correspondem a todos os jeitos possíveis de tampar a caixa.

**Exercício 8.17:** Um dado de jogar tem as faces numeradas de 1 a 6, de tal modo tal que faces opostas somam 7. Suponha que o dado é rolado de modo que ele termina na mesma posição onde começou, exceto que algumas faces podem ficar trocadas entre si. A rotação pode ser descrita por uma permutação  $f$  do conjunto  $A = \{1, 2, 3, 4, 5, 6\}$ , tal que a face  $k$  termina onde estava a face  $f(k)$ .

- (a) Liste todas as permutações de  $A$  que podem ser obtidas desta forma.
- (b) Se  $f$  e  $g$  são duas dessas permutações, qual é o significado da composição  $f \circ g$ ? Ela também é uma dessas permutações?

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  $A$ .

Seja  $f$  uma função permutação sobre  $A$  e  $a$  um elemento de  $A$ . A *órbita* ou *ciclo de  $a$  sob  $f$*  é o subconjunto de  $A$  obtido por aplicações repetidas de  $f$  ou  $f^{-1}$  a esse elemento, ou seja,  $\{f^n(a) : n \in \mathbb{Z}\}$ . No exemplo 8.13, o ciclo do elemento 11 é  $\{11, 12, 13\}$ , que também é o ciclo de 13. O ciclo do elemento 10 é  $\{10\}$  e o ciclo de 14 é  $\{14, 15\}$ .

**Exercício 8.18:** Seja  $f$  uma permutação de um conjunto finito  $A$ , e sejam  $x, y$  dois elementos de  $A$ . Prove que os ciclos de  $x$  e de  $y$  sob  $f$  ou são o mesmo conjunto, ou são conjuntos disjuntos.

**Exercício 8.19:** Prove que o fecho transitivo e o fecho reflexivo de uma permutação, sobre um conjunto finito, é uma relação de equivalência. Quem são as classes de equivalência?

Uma *involução* de um conjunto  $A$  é uma permutação  $f$  sobre  $A$  que é sua própria inversa, ou seja  $f^{-1} = f$ .

**Exercício 8.20:** Seja  $f$  uma permutação sobre um conjunto  $A$ . Prove que as seguintes afirmações são equivalentes:

- (a)  $f$  é uma involução.
- (b)  $f^2 = \mathcal{I}_A$ .
- (c) Todo ciclo de  $f$  tem 1 ou 2 elementos.

## 8.8 Funções piso e teto

Há várias funções que são bem conhecidas pelo seu papel em álgebra e cálculo diferencial e integral, como raiz quadrada, seno, cosseno, logaritmo, etc. Duas funções menos conhecidas são especialmente importantes em computação:

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

Ou seja, ambas arredondam para um inteiro: o piso sempre para baixo, e o teto sempre para cima.  
Por exemplo:

$$\lfloor 7/3 \rfloor = \lfloor 8/3 \rfloor = 2$$

$$\lfloor -1/3 \rfloor = \lfloor -3/4 \rfloor = -1$$

$$\lfloor 5 \rfloor = 5$$

$$\lceil 7/3 \rceil = \lceil 8/3 \rceil = 3$$

$$\lceil -1/3 \rceil = \lceil -3/4 \rceil = 0$$

$$\lceil 5 \rceil = 5$$

Veja a figura 8.4.

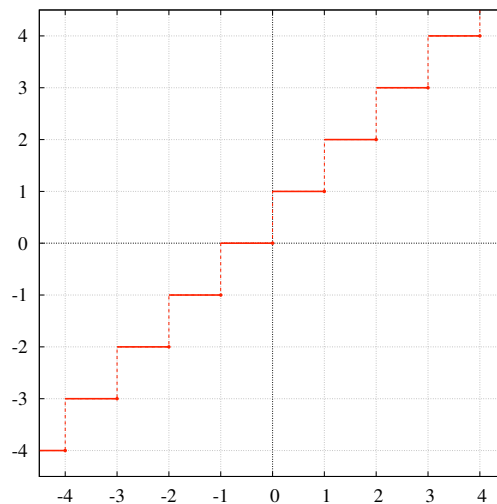
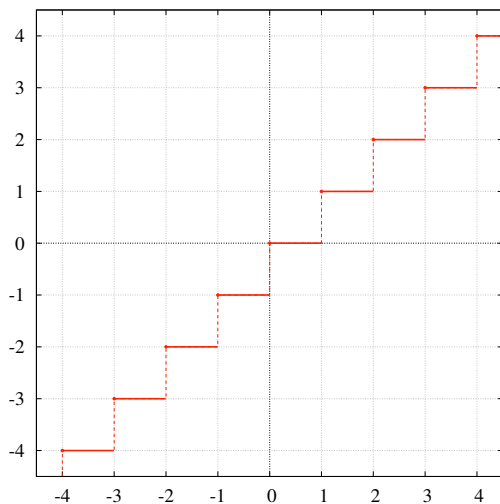


Figura 8.4: Gráficos da função piso  $\lfloor x \rfloor$  (à esquerda) e da função teto  $\lceil x \rceil$  (à direita).

Piso e teto são funções do conjunto  $\mathbb{R}$  para o conjunto  $\mathbb{Z}$ . Algumas de suas propriedades são:

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

**Exercício 8.21:** Prove que  $\lceil x + n \rceil = \lceil x \rceil + n$  e  $\lfloor x + n \rfloor = \lfloor x \rfloor + n$  para todo  $x \in \mathbb{R}$  e todo  $n \in \mathbb{N}$

**Exercício 8.22:** Prove que as funções piso e teto são idempotentes.

**Exercício 8.23:** Prove, ou dê um contra exemplo, que  $\lceil x + y \rceil = \lceil x \rceil + y$  e  $\lfloor x + y \rfloor = \lfloor x \rfloor + y$ .

**Exercício 8.24:** Escreva uma fórmula, usando a função piso, que devolve a parte fracionária de um número real positivo  $x$ . Ou seja, se  $x = 3.1416$ , devolve 0.1416.

**Exercício 8.25:** Seja  $\varepsilon$  um número real positivo. Considere a relação  $\sim_\varepsilon$  sobre  $\mathbb{R}$  tal que

$$x \sim_\varepsilon y \leftrightarrow \left\lfloor \frac{x}{\varepsilon} \right\rfloor = \left\lfloor \frac{y}{\varepsilon} \right\rfloor$$

para quaisquer  $x$  e  $y$  em  $\mathbb{R}$ . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

## 8.9 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  $d$ ”. Note a diferença entre este uso do termo e os usos para valor absoluto  $|x|$  de um número real, a norma  $\sqrt{x^2 + y^2}$  de um número complexo  $x + yi$ , ou norma de um vetor em álgebra linear.

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

Estas operações podem ser definidas usando a função piso:

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

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

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  $(-17) \bmod 3 = (-17) - 3(-6) = 1$ .

Mais geralmente, estas fórmulas também são usadas quando  $x$  é um número real, inclusive negativo, e  $d$  é um número real positivo. Assim, por exemplo,  $3.1416 \div 0.001 = 3141$ , e  $3.1416 \bmod 0.001 = 0.0006$ . Veja a figura 8.5 (alto).

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  $x$ . Nessas linguagens, por exemplo,  $(-17) \div 3 = -5$  (em vez de  $-6$ ) e  $(-17) \bmod 3 = -2$  (em vez de  $1$ ). Veja a figura 8.5 (baixo). Embora pareçam menos naturais, as definições matemáticas são geralmente mais úteis, em matemática e programação, do que estas definições antigas.

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.

Diz-se que dois números  $x$  e  $y$  são *congruentes módulo  $d$*  se  $(x \bmod d) = (y \bmod d)$ , ou seja se  $(x - y) \bmod d = 0$ .

**Exercício 8.26:** Mostre como usar as operações de quociente inteiro e/ou resto para arredondar uma quantia arbitrária  $x$  de dinheiro obtendo um valor em reais e centavos exatos. Por exemplo, dado  $x = \text{R\$ } 2.71828$ , retornar  $\text{R\$ } 2.71$ .

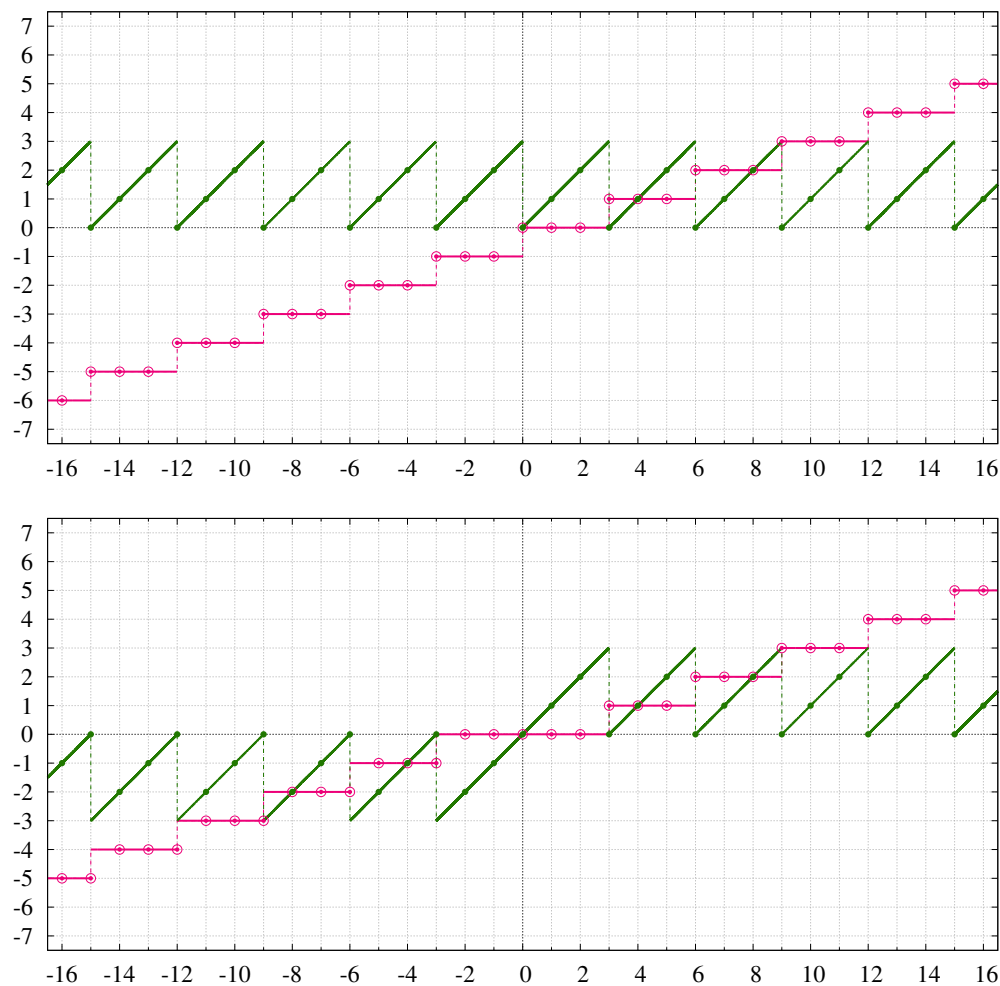


Figura 8.5: No alto, gráficos da função  $x \div 3$  (vermelho) e  $x \bmod 3$  (verde) para valores inteiros

**Exercício 8.27:** O dia da semana do dia primeiro de janeiro de um ano  $n \geq 1582$  pode ser determinado pela fórmula:

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

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

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

**Exercício 8.28:** Prove que, para qualquer número positivo  $d$ , quaisquer números reais  $x, y$ , e qualquer inteiro  $k$ :

- (a)  $(x + kd) \div d = x \div d$ .
- (b)  $(x + kd) \bmod d = x \bmod d$ .
- (c)  $(x + y) \bmod d = ((x \bmod d) + y) \bmod d$ .
- (d)  $(x \bmod (kd)) \bmod d = x \bmod d$  (supondo  $k > 0$ ).
- (e)  $\sin x = \sin(x \bmod (2\pi))$ .

## 8.10 Fatorial e função gama

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

$$n! = \prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n \quad (8.1)$$

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  $0! = 1$ .

A *função gama*, denotada por  $\Gamma$ , é uma variante do fatorial; mais precisamente,

$$\Gamma(n) = (n-1)! \quad (8.2)$$

para todo inteiro *positivo*  $n$ . Portanto,

$$n! = \Gamma(n+1) \quad (8.3)$$

para todo número natural  $n$ . Por exemplo,  $\Gamma(1) = 1$ ,  $\Gamma(2) = 1$ ,  $\Gamma(5) = 24$ , etc.. Observe que  $\Gamma(0)$  não é definido.

A função gama é na verdade definida para qualquer número real (ou complexo), exceto 0 e inteiros negativos, pela fórmula

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt \quad (8.4)$$

Por exemplo,  $\Gamma(1/2)$  é definido como  $\sqrt{\pi}$ . A função gama é muito usada em análise combinatória, na teoria da probabilidade e na estatística.

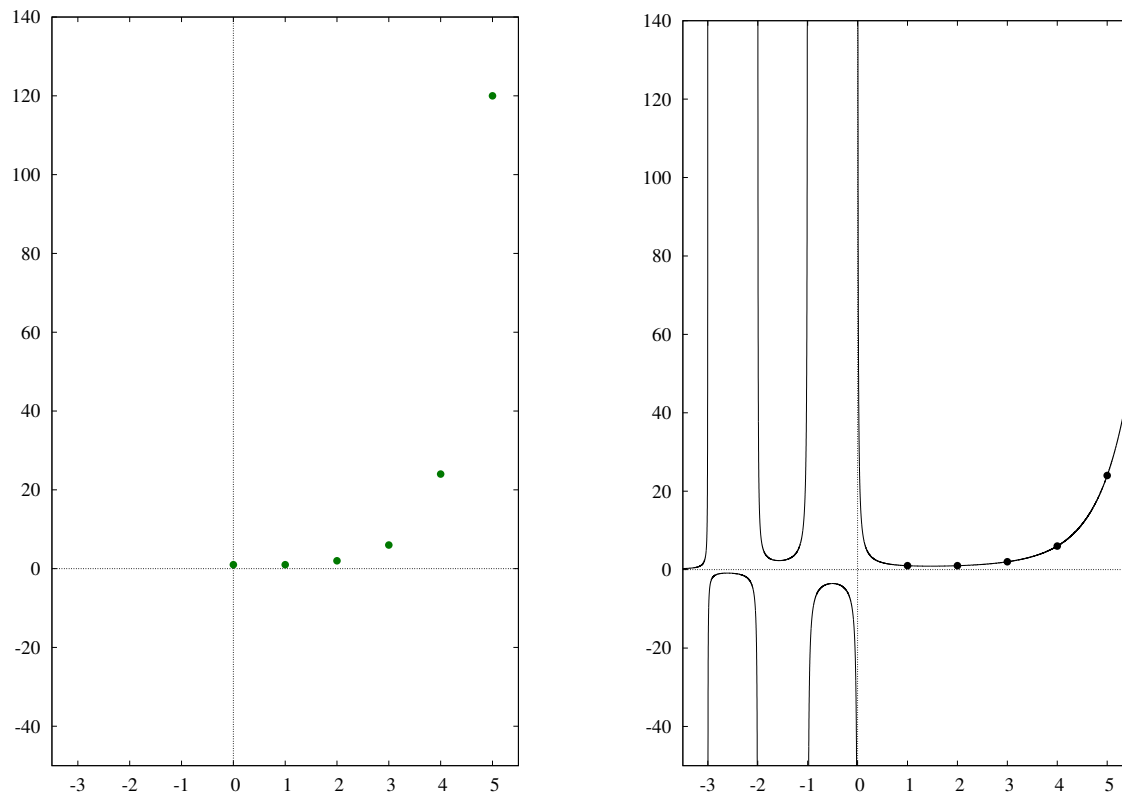


Figura 8.6: À esquerda, um gráfico da função fatorial, que dado  $n$  devolve  $n!$ , para  $n \in \{0, 1, \dots, 5\}$ . À direita, um gráfico da função  $\Gamma$  (linha contínua) e de  $(n-1)!$  (pontos).

## 8.11 Função característica

A *função característica* de um conjunto  $A$  qualquer é uma função  $f$  cujo domínio é o conjunto universal  $\mathbb{U}$ , 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  $\chi_A$ .

Ou seja  $\chi_A(z)$  tem o mesmo valor lógico que a fórmula “ $z \in A$ ”. Podemos ver a função  $\chi_A$  como uma representação do conjunto  $A$ .

Em alguns contextos é mais conveniente definir a função característica como tendo valores 1 e 0, em vez de **V** e **F**, respetivamente. Além disso, se todos os conjuntos de interesse são subconjuntos de um conjunto principal  $V$ , pode ser preferível usar  $V$  como domínio das funções características, em vez de  $\mathbb{U}$ .

**Exercício 8.29:** Qual é a função característica do conjunto vazio?

## 8.12 Multiconjunto

Em certos contextos é desejável trabalhar com uma coleção de elementos onde pode haver elementos repetidos; sendo que a ordem dos elementos não importa, mas importa o número de vezes que cada elemento ocorre.

Por exemplo, considere um polinômio  $p$  cujo monômio de grau mais alto tem coeficiente 1; ou seja,  $p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$ , onde cada  $a_i$  é um número complexo. Um

teorema fundamental da álgebra diz que tal polinômio pode ser escrito como o produto de  $n$  fatores lineares

$$p(x) = (x - z_1)(x - z_2) \cdots (x - z_n) \quad (8.5)$$

onde cada  $z_i$  é um número complexo (possivelmente real). Portanto o polinômio  $p$  é determinado unicamente pela coleção de suas raízes  $z_1, z_2, \dots, z_n$ . Observe que a ordem destas raízes não importa, mas a mesma raiz pode ocorrer mais de uma vez no produto acima, e o número de vezes é importante. Por exemplo, o polinômio com raízes 1, 2, 2, 3 é

$$(x - 1)(x - 2)(x - 2)(x - 3) = x^4 - 8x^3 + 23x^2 - 28x + 12 \quad (8.6)$$

enquanto que o polinômio com raízes 1, 1, 2, 3 é

$$(x - 1)(x - 1)(x - 2)(x - 3) = x^4 - 7x^3 + 17x^2 - 17x + 6 \quad (8.7)$$

O nome *multiconjunto* é usado para descrever este tipo de estrutura matemática: uma coleção de elementos que podem ser repetidos, sendo que a ordem não importa, mas o número de repetições de cada elemento importa. Outros nomes, menos comuns, são *conjunto com multiplicidade*, *conjunto com repetição*, ou *coleção*. O número de vezes que um elemento  $z$  ocorre é dito a *multiplicidade de  $z$  em  $A$* .

Na verdade, o conceito de multiconjunto é supérfluo, pois é apenas uma generalização do conceito de função característica. Ou seja, um multiconjunto  $A$  pode ser visto como uma função que associa a cada elemento  $z$  do conjunto universo  $\mathbb{U}$  um número natural — a multiplicidade de  $z$  em  $A$  — em vez de apenas 0 ou 1. Em vista desta interpretação, a multiplicidade pode ser denotada por  $A(z)$ .

## 8.13 Sequências finitas

Uma *sequência finita* é uma função  $x$  cujo domínio é um intervalo de inteiros  $\{n \in \mathbb{Z} : r \leq n \leq s\}$ , 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* (vide seção 2.6.1).

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

A expressão “*elemento da sequência*” é bastante usada, mas é ambígua: pode se referir a um termo  $(i, x_i)$  da mesma, ou apenas ao valor  $x_i$  de um termo, dependendo do contexto.

**Exemplo 8.15:** Seja  $x : \{2 .. 6\} \rightarrow \mathbb{R}$  cujos termos são  $\{(2, 4), (3, 9), (4, 16), (5, 25), (6, 36)\}$ . Podemos então escrever que  $x_2 = 4$ ,  $x_3 = 9$ , e  $x_i = i^2$  para todo  $i \in \{2 .. 6\}$ .

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.

### 8.13.1 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  $\{(0, 1), (1, 2), (2, 2), (3, 5)\}$ .

Como observamos na seção 2.6.1, 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  $\langle \dots \rangle$ , ou colchetes comuns  $[ \dots ]$ , no lugar de parênteses para denotar sequências.

Note que há também uma diferença entre a sequência  $(2, 3)$  e o conjunto  $\{2, 3\}$ .

### 8.13.2 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 segundo termo de uma sequência  $x$  é  $x_2$ , o terceiro é  $x_3$ , etc.; ou seja, o  $k$ -ésimo elemento é  $x_k$ .

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 segundo elemento é  $x_1$  e não  $x_2$ , o terceiro é  $x_2$ , e o  $k$ -ésimo é  $x_{k-1}$ . Apesar destas incongruências, 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.

### 8.13.3 Comprimento

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

**Exercício 8.30:** 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 inteiro  $\{r .. s\}$  é vazio para quaisquer  $r$  e  $s$  com  $r > s$ .

### 8.13.4 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

$$z_k = \begin{cases} x_k, & \text{se } 0 \leq k < p \\ y_{k-p}, & \text{se } p \leq k < p + q \end{cases} \quad (8.8)$$

para todo  $k$  em  $\{0 \dots p + q - 1\}$ , onde  $p = |x|$  e  $q = |y|$ .

**Exercício 8.31:** Adapte a fórmula da concatenação (8.8) para a convenção em que todas as sequências tem índice inicial 1.

**Exercício 8.32:** Escreva a fórmula geral da concatenação (8.8) para o caso em que os domínios de  $x$  e  $y$  são  $\{r' \dots s'\}$  e  $\{r'' \dots s''\}$ , 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  $x$ .

### 8.13.5 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  $y =$

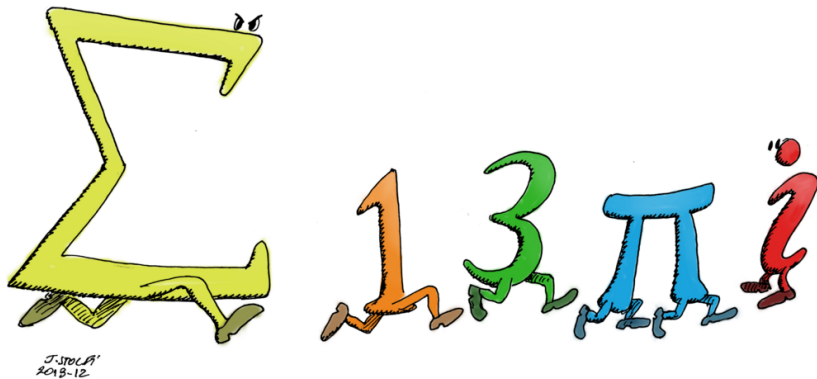
$\{(3, 30), (5, 20)\}$  é a subsequência de  $x = \{(2, 20), (3, 30), (4, 30), (5, 20)\}$  determinada pelo conjunto  $R = \{3, 5\}$ .

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.

# Capítulo 9

## Somatórias e produtórias



## 9.1 Introdução

Muitas quantidades importantes em matemática são definidas como a soma de uma quantidade variável de parcelas também variáveis, por exemplo a soma  $2^1 + 2^2 + \dots + 2^n$ , 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

$$\sum_{k=1}^n 2^k \quad \text{ou} \quad \sum_{k=1}^n 2^k \quad (9.1)$$

Em geral, a notação sigma tem a forma

$$\sum_{k=m}^n f(k) \quad \text{ou} \quad \sum_{k=m}^n f(k) \quad (9.2)$$

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 notação nos diz para incluirmos na soma precisamente aqueles termos  $f(k)$  onde  $k$  é um inteiro maior ou igual a  $m$  e menor ou igual a  $n$ , ou seja  $m \leq k \leq n$ .

Observe que se  $f(k)$  tem o mesmo valor para dois (ou mais) índices  $k$  diferentes entre  $m$  e  $n$ , esse valor deve ser somado duas (ou mais) vezes. Por exemplo, na somatória  $\sum_{k=1}^4 k(5-k)$ , as parcelas são 4, 6, 6, 4; portanto a soma é 20.

Uma variante mais geral da notação  $\Sigma$  é

$$\sum_{\substack{k \\ P(k)}} f(k) \quad (9.3)$$

onde  $k$  é a variável índice, e  $P$  é algum predicado sobre inteiros. Ela representa a soma de todos os valores  $f(k)$  para todos os inteiros  $k$  tais que  $P(k)$  é verdadeiro. Portanto, a fórmula (9.2) também pode ser escrita

$$\sum_{\substack{k \\ m \leq k \leq n}} f(k) \quad (9.4)$$

Costuma-se simplificar esta notação para

$$\sum_{P(k)} f(k) \quad (9.5)$$

quando a variável índice  $k$  é óbvia pelo contexto. Esta forma é mais comum quando temos restrições mais complicadas sobre os índices, como por exemplo

$$\sum_{\substack{1 \leq k \leq 10 \\ k \text{ ímpar}}} k^2 = 1^2 + 3^2 + 5^2 + 7^2 + 9^2 \quad (9.6)$$

$$\sum_{\substack{p \text{ primo} \\ p \text{ divide } 140}} \frac{1}{p} = \frac{1}{2} + \frac{1}{5} + \frac{1}{7} \quad (9.7)$$

Outra variante similar desta notação é

$$\sum_{k \in M} f(k) \quad (9.8)$$

onde  $M$  é um conjunto qualquer. Esta notação significa a soma dos valores de  $f(k)$  para todos os elementos de  $M$ , sendo cada elemento considerado exatamente uma vez. Por exemplo, se  $M =$

1, 2, 7, 8,

$$\sum_{k \in M} k(9 - k) = 1 \cdot 8 + 2 \cdot 7 + 7 \cdot 2 + 8 \cdot 1 = 44 \quad (9.9)$$

Em qualquer caso, chamaremos de *domínio* da somatória o conjunto dos índices dos seus termos.

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  $m > n$ .

Outra forma da notação é simplesmente  $\sum f$ , onde  $f$  é uma função de um conjunto finito com valores numéricos. Por exemplo,  $f$  pode ser uma sequência de números. Essa notação significa  $\sum_{x \in \text{Dom}(f)} f(x)$ . Se  $f$  é a função vazia, o valor é zero.

Finalmente, se  $A$  é um conjunto de números, a notação  $\sum A$  significa  $\sum_{x \in A} x$ . Se  $A$  é vazio, o valor é zero.

**Exercício 9.1:** Qual é a diferença entre  $\sum_{k \in M} f(k)$  e  $\sum \{ f(k) : k \in M \}$ ? Ilustre com um exemplo.

Todas estas notações também pode ser usadas quando os valores a somar são outros tipos de elementos que podem ser somados, como vetores, matrizes, ou funções. Nesse caso, se a somatória for vazia, o resultado é definido como o elemento nulo para o tipo de elemento esperado no contexto.

## 9.2 Somatórias básicas

Algumas somatórias simples tem fórmulas explícitas. Por exemplo:

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

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

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

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

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

Estas fórmulas podem ser demonstradas facilmente por indução sobre o valor de  $n$  (veja exercício 5.29).

### 9.3 Manipulação de somatórias

A notação  $\Sigma$  pode ser manipulada de várias maneiras. Em primeiro lugar, observe que a variável índice  $k$  pode ser substituída por qualquer outra letra  $i, j, l, \dots$  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 9.1:** 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 9.2:** Podemos simplificar a somatória (9.6) trocando a variável  $k$  por  $2i + 1$  (ou seja  $i = (k - 1)/2$ ):

$$\sum_{\substack{1 \leq k \leq 10 \\ k \text{ ímpar}}} k^2 = 1^2 + 3^2 + 5^2 + 7^2 + 9^2 = \sum_{i=0}^4 (2i + 1)^2$$

Note que a equação (9.7) não pode ser simplificada desta maneira, pois não se conhece uma fórmula explícita para os números primos.

Damos a seguir mais algumas regras básicas. Nestas somatórias, o domínio  $M$  é um conjunto qualquer de inteiros, e  $f, g$  são funções de inteiros para números reais.

- *Distributividade*: Para qualquer número  $c$

$$\sum_{k \in M} c f(k) = c \left( \sum_{k \in M} f(k) \right) \quad (9.10)$$

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

- *Associatividade*:

$$\sum_{k \in M} (f(k) + g(k)) = \left( \sum_{k \in M} f(k) \right) + \left( \sum_{k \in M} g(k) \right) \quad (9.11)$$

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

- *Decomposição do domínio*: Se  $\{M_1, M_2\}$  é uma partição de  $M$ , então

$$\sum_{k \in M} f(k) = \left( \sum_{k \in M_1} f(k) \right) + \left( \sum_{k \in M_2} f(k) \right) \quad (9.12)$$

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  $M$  em qualquer número de partes.

- *Comutatividade*: Se  $p$  é uma permutação qualquer de  $M$ ,

$$\sum_{k \in M} f(k) = \sum_{k \in M} f(p(k)) \quad (9.13)$$

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  $M$  para um conjunto  $J \subseteq \mathbb{Z}$ ,

$$\sum_{k \in M} f(p(k)) = \sum_{j \in J} f(j) \quad (9.14)$$

Note que troca de variável indexadora, como as dos exemplos 9.1 e 9.2, são casos particulares desta regra.

**Exemplo 9.3:** Calcular a soma  $\sum_{k=1}^n k(k+1)$ .

$$\begin{aligned} \sum_{k=1}^n k(k+1) &= \sum_{k=1}^n k^2 + \sum_{k=1}^n k \\ &= (1^2 + 2^2 + 3^2 + \cdots + n^2) + (1 + 2 + 3 + \cdots + n) \\ &= n(n+1)(2n+1)/6 + n(n+1)/2 \\ &= n(n+1)(n+2)/3 \end{aligned}$$

**Exemplo 9.4:** Seja  $x$  uma sequência qualquer de números reais, e considere a somatória  $\sum_{k=1}^n (x_{k+1} -$

$x_k$ ). Usando as regras acima, 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 9.4 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. Podemos usar esta identidade para provar as fórmulas das somatórias de quadrados e cubos da seção 9.2.

**Exemplo 9.5:** 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

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

**Exemplo 9.6:** Calcular a somatória  $\sum_{k=0}^{n-1} 2^k$ . Observe que  $2^k = 2^{k+1} - 2^k$ .

$$\begin{aligned}
 \sum_{k=0}^{n-1} 2^k &= \sum_{k=0}^{n-1} (2^{k+1} - 2^k) \\
 &= 2^n - 2^0 \\
 &= 2^n - 1
 \end{aligned}$$

**Exemplo 9.7:** Calcular a somatória  $\sum_{k=1}^n k2^{k-1}$ . Observe que  $2^{k-1} = 2^k - 2^{k-1}$ .

$$\begin{aligned}
 \sum_{k=1}^n k2^{k-1} &= \sum_{k=1}^n k(2^k - 2^{k-1}) \\
 &= \sum_{k=1}^n k2^k - k2^{k-1} \\
 &= \sum_{k=1}^n k2^k - ((k-1)2^{k-1} + 2^{k-1}) \\
 &= \left( \sum_{k=1}^n k2^k - (k-1)2^{k-1} \right) - \sum_{k=1}^n 2^{k-1}
 \end{aligned}$$

Substituindo  $k = i + 1$ ,  $i = k - 1$  nas duas somatórias, temos:

$$\begin{aligned}
 &= \left( \sum_{i+1=1}^{i+1=n} (i+1)2^{i+1} - (i+1-1)2^{i+1-1} \right) - \sum_{i+1=1}^{i+1=n} 2^{i+1-1} \\
 &= \left( \sum_{i=0}^{n-1} (i+1)2^{i+1} - i2^i \right) - \sum_{i=0}^{n-1} 2^i
 \end{aligned} \tag{9.15}$$

Uma soma é telescópica, a outra é conhecida, portanto:

$$\begin{aligned}
 &= (n2^n - 02^0) - (2^n - 1) \\
 &= (n-1)2^n + 1
 \end{aligned} \tag{9.16}$$

**Exercício 9.2:**[Soma de PA] Calcule a somatória  $\sum_{k=0}^{n-1}(a + rk)$ , cujas  $n$  parcelas são parte de uma progressão aritmética com termo inicial  $a$  e passo  $r$  arbitrários.

**Exercício 9.3:** Calcule a somatória  $\sum_{k=0}^{n-1} b^k$  para um número real  $b$  arbitrário diferente de 1 e 0. Observe que  $b^k = (b^{k+1} - b^k)/(b - 1)$ .

**Exercício 9.4:**[Soma de PG] Calcule a somatória  $\sum_{k=0}^{n-1} ar^k$ , cujas  $n$  parcelas são parte de uma progressão geométrica com termo inicial  $a$  e razão  $r$  arbitrários.

**Exercício 9.5:** Calcule a somatória  $\sum_{k=1}^n 1/k(k + 1)$ .

**Exercício 9.6:** Prove, por indução em  $n$ , que

$$\sum_{k=1}^n \sin k\alpha = \frac{\left(\sin \frac{n}{2}\alpha\right)\left(\sin \frac{n+1}{2}\alpha\right)}{\sin \frac{1}{2}\alpha} \quad (9.17)$$

para todo  $n \in \mathbb{N}$ , e todo ângulo  $\alpha$  que não é um múltiplo inteiro de  $2\pi$ .

**Exercício 9.7:** Sejam  $F_0, F_1, F_2, \dots$  os números de Fibonacci, definidos recursivamente por  $F_0 = 0, F_1 = 1$ , e  $F_n = F_{n-1} + F_{n-2}$  para todo número natural  $n$ . Prove, por indução em  $n$ , que

(a)  $(\forall n \in \mathbb{N}) \sum_{i=1}^n F_i = F_{n+2} - 1$

(b)  $(\forall n \in \mathbb{N}) \sum_{i=1}^n F_i^2 = F_n F_{n+1}$

**Exercício 9.8:** Sejam  $a$  e  $b$  número reais distintos. Prove que, para todo  $n$  em  $\mathbb{N}$ , vale a igualdade:

$$\sum_{i=0}^n a^i b^{n-i} = \frac{b^{n+1} - a^{n+1}}{b - a} \quad (9.18)$$

## 9.4 Somatórias múltiplas

Os termos de uma somatória podem ser especificados por dois ou mais índices, como no exemplo abaixo:

$$\sum_{\substack{j,k \\ 1 \leq j \leq 3 \\ 2 \leq k \leq 4}} f(j, k) = f(1, 2) + f(1, 3) + f(1, 4) + f(2, 2) + f(2, 3) + f(2, 4) + f(3, 2) + f(3, 3) + f(3, 4) \quad (9.19)$$

Este mesmo exemplo pode ser também escrito usando duas vezes a notação  $\Sigma$ , isto é, como uma somatória de somatórias:

$$\sum_{\substack{j,k \\ 1 \leq j \leq 3 \\ 2 \leq k \leq 4}} f(j,k) = \sum_{1 \leq j \leq 3} \sum_{2 \leq k \leq 4} f(j,k) = \begin{aligned} &(f(1,2) + f(1,3) + f(1,4)) + \\ &(f(2,2) + f(2,3) + f(3,4)) + \\ &(f(3,2) + f(3,3) + f(3,4)) \end{aligned} \quad (9.20)$$

ou então

$$\sum_{\substack{j,k \\ 1 \leq j \leq 3 \\ 2 \leq k \leq 4}} f(j,k) = \sum_{2 \leq k \leq 4} \sum_{1 \leq j \leq 3} f(j,k) = \begin{aligned} &(f(1,2) + f(2,2) + f(3,2)) + \\ &(f(1,3) + f(2,3) + f(3,3)) + \\ &(f(1,4) + f(2,4) + f(3,4)) \end{aligned} \quad (9.21)$$

Podemos entender as fórmulas (9.20) e (9.21) como duas maneiras de somar todos os elementos de uma matriz: coluna por coluna ou linha por linha.

### 9.4.1 Mudança de ordem de somatórias

As fórmulas (9.20) e (9.21) dizem que podemos trocar a ordem de duas somatórias, quando o domínio de cada variável é independente da outra variável:

$$\sum_{j \in J} \sum_{k \in K} f(j,k) = \sum_{\substack{j \in J \\ k \in K}} f(j,k) = \sum_{k \in K} \sum_{j \in J} f(j,k). \quad (9.22)$$

Quando o domínio da soma interna depende da variável índice da somatória externa, a troca exige mais cuidado. Por exemplo,

$$\sum_{j=1}^n \sum_{k=j}^n a_{j,k} = \sum_{1 \leq j \leq k \leq n} a_{j,k} = \sum_{k=1}^n \sum_{j=1}^k a_{j,k}. \quad (9.23)$$

Para entender esta transformação, veja a figura 9.1. Os pontos representam todos os pares  $(j, k)$  considerados na somatória central. As setas sólidas indicam a ordem descrita pela somatória dupla da esquerda (por linhas), e as setas tracejadas indicam a da direita (por colunas).

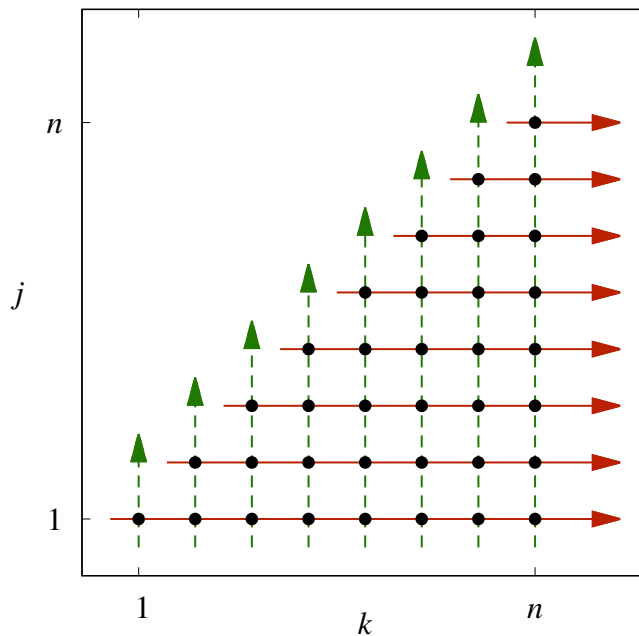


Figura 9.1: Duas maneiras de calcular uma soma dupla:  $\sum_{j=1}^n \sum_{k=j}^n f(j, k)$  (setas horizontais) e  $\sum_{k=1}^n \sum_{j=k}^n f(j, k)$  (setas verticais).

**Exercício 9.9:** Para todo número inteiro positivo  $n$ , o  $n$ -ésimo número hamônico é

$$H_n = \sum_{k=1}^n \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} \cdots \frac{1}{n}. \quad (9.24)$$

Prove que, para todo inteiro  $n$  maior ou igual a 2,

$$\sum_{k=1}^n H_k = (n+1)H_n - n. \quad (9.25)$$

### 9.4.2 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  $f : J \rightarrow \mathbb{R}$ ,  $g : K \rightarrow \mathbb{R}$

$$\left( \sum_{j \in J} f(j) \right) \left( \sum_{k \in K} g(k) \right) = \sum_{\substack{j \in J \\ k \in K}} f(j)g(k) = \sum_{j \in J} \sum_{k \in K} f(j)g(k) \quad (9.26)$$

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.

## 9.5 Majoração de somatórias

Muitas vezes não precisamos saber o valor exato de uma somatória, basta saber um limitante superior ou inferior.

### 9.5.1 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

$$\frac{k}{k+1} 2^k < 2^k \tag{9.27}$$

Podemos então concluir que

$$\begin{aligned}\sum_{k=0}^n \frac{k}{k+1} 2^k &< \sum_{k=0}^n 2^k \\ &= 2^{n+1} - 1.\end{aligned} \tag{9.28}$$

**Exercício 9.10:** Prove que, para todo  $n \in \mathbb{N}$ ,

$$H_{2^n} \geq 1 + \frac{n}{2}. \quad (9.29)$$

### 9.5.2 Majoração por indução matemática

No capítulo 5 discutimos a técnica de prova por indução matemática e vimos como usá-la para verificar uma fórmula explícita exata para o resultado de uma somatória. Esta técnica pode ser usada também para provar um limitante superior ou inferior para uma somatória.

**Exemplo 9.8:** Prove que existe uma constante  $c > 0$  tal que

$$\sum_{i=0}^n 3^i \leq c3^n$$

para todo  $n \in \mathbb{N}$ .

Embora esta somatória tenha uma fórmula conhecida (soma de progressão geométrica), vamos tentar mostrar a desigualdade sem usar essa fórmula.

**Prova:**

A tese a ser provada tem a forma  $(\exists c > 0)(\forall n \in \mathbb{N}) P(n)$ , portanto somente pode ser provada por indução se escolhermos um valor adequado para  $c$ . Para isso, podemos escrever um rascunho da demonstração da parte  $(\forall n \in \mathbb{N}) P(n)$ , por indução em  $n$ , deixando

o valor de  $c$  em aberto; e depois escolher um valor de  $c$  que torna todas as partes dessa demonstração válidas.

1. *Base*: para  $n = 0$ , a afirmação  $P(n)$  é

$$\sum_{i=0}^0 3^i = 3^0 = 1 \leq c \cdot 1 \quad (9.30)$$

Esta desigualdade será válida se  $c$  for maior ou igual a 1.

2. *Hipótese de indução*: suponhamos que a desigualdade é verdadeira para algum  $k$ , ou seja

$$\sum_{i=0}^k 3^i \leq c3^k \quad (9.31)$$

3. *Passo de indução*: temos de provar que a desigualdade é verdadeira para  $k + 1$ , isto é temos que mostrar que:

$$\sum_{i=0}^{k+1} 3^i \leq c3^{k+1} \quad (9.32)$$

Temos que

$$\sum_{i=0}^{k+1} 3^i = \sum_{i=0}^k 3^i + 3^{k+1} \quad (9.33)$$

Usando a hipótese de indução, temos

$$\begin{aligned} \sum_{i=0}^{k+1} 3^i &\leq c3^k + 3^{k+1} \\ &= \left(\frac{1}{3} + \frac{1}{c}\right)c3^{k+1} \end{aligned} \quad (9.34)$$

Precisamos agora concluir que

$$\left(\frac{1}{3} + \frac{1}{c}\right)c3^{k+1} \leq c3^{k+1} \quad (9.35)$$

Isto é verdade se  $c \geq 3/2$ .

Portanto se escolhermos  $c = 3/2$ , tanto a base quanto o passo da indução estarão corretos, e a afirmação  $(\forall n \in \mathbb{N}) P(n)$  ficará provada.

**Fim.**

### 9.5.3 Majoração por integrais

Uma somatória pode ser vista como uma versão discreta de uma integral. Algumas propriedades são de fato comuns aos dois conceitos: por exemplo, se  $f$  é um polinômio de grau  $g$ , tanto a somatória  $\sum_{k=0}^n f(k)$  quanto a integral  $\int_0^n f(x) dx$  são polinômios (diferentes) de grau  $g + 1$  na

variável  $n$ . Se  $f$  é uma função exponencial,  $f(x) = Ar^x$ , tanto a somatória quanto a integral são funções exponenciais  $ABr^n + C$  (com valores diferentes de  $B$  e  $C$ ). Muitas das regras para manipulação de somatórias (troca de variável, decomposição do domínio, associatividade, etc.) correspondem a regras para manipulação de integrais.

Embora não exista uma relação simples entre a integral de uma função e sua somatória, a primeira pode fornecer um limitante superior para a segunda. Suponha que  $f$  é uma função crescente de  $\mathbb{R}$  para  $\mathbb{R}$ . Considere a função

$$f^*(x) = f(\lfloor x \rfloor) \tag{9.36}$$

A figura 9.2 ilustra a relação entre  $f$  e  $f^*$ .

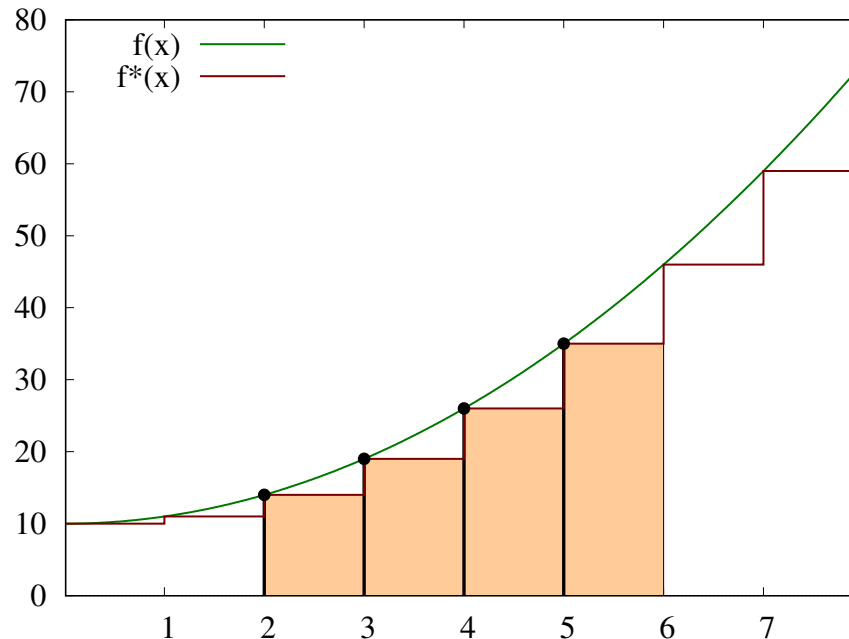


Figura 9.2: Limitante superior por integral.

Observe que o gráfico da função  $f^*$  é uma escada, pois ela é constante em cada intervalo entre inteiros consecutivos. Portanto a integral de  $f^*$  entre dois inteiros quaisquer pode ser decomposta na soma de áreas de retângulos de largura 1. Mais exatamente,  $f^*(x) = f(k)$  para todo inteiro  $k$  e

todo  $x$  entre  $k$  (inclusive) e  $k + 1$  (exclusive); portanto,  $\int_k^{k+1} f^*(x) dx = f(k)$ , e

$$\int_m^n f^*(x) dx = \sum_{k=m}^{n-1} f(k) \quad (9.37)$$

Por outro lado, como  $\lfloor x \rfloor \leq x$  para todo  $x$ , e  $f$  é uma função crescente de  $x$ , podemos concluir que

$$f^*(x) \leq f(x) \quad (9.38)$$

para todo  $x$ . Veja a figura 9.2. Temos portanto que

$$\int_m^n f^*(x) dx \leq \int_m^n f(x) dx \quad (9.39)$$

Ou seja

$$\sum_{k=m}^{n-1} f(k) \leq \int_m^n f(x) dx \quad (9.40)$$

Como exemplo, considere a somatória  $\sum_{k=1}^{n-1} k \log k$ , que ocorre na análise da eficiência de algoritmos importantes mas não tem uma fórmula explícita simples. Neste exemplo, a função  $f$  é  $f(x) = x \log x$ , que é crescente para  $x \geq 1$ . A integral de  $f$  pode ser facilmente calculada (por integração por partes):

$$\int_a^b x \log x dx = \frac{b^2}{2} \left( \log b - \frac{1}{2} \right) - \frac{a^2}{2} \left( \log a - \frac{1}{2} \right) \quad (9.41)$$

para quaisquer  $a, b$  maiores ou iguais a 1. Temos portanto que

$$\sum_{k=1}^{n-1} k \log k \leq \frac{n^2}{2} \left( \log n - \frac{1}{2} \right) + \frac{1}{4} \quad (9.42)$$

Como  $\log n - \frac{1}{2} < \log n$ , podemos escrever também que

$$\sum_{k=1}^{n-1} k \log k \leq \frac{n^2}{2} \log n + \frac{1}{4} \quad (9.43)$$

**Exercício 9.11:** Para todo número inteiro positivo  $n$ , o  $n$ -ésimo número hamônico é

$$H_n = \sum_{k=1}^n \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} \dots \frac{1}{n}. \quad (9.44)$$

Prove que  $H_n \leq 1 + \ln n$ .

**Exercício 9.12:** Prove que, para todo inteiro positivo  $n$ ,

$$\sum_{k=1}^n \frac{1}{2k-1} \leq 2 + \ln \sqrt{n}. \quad (9.45)$$

**Exercício 9.13:** Prove que a somatória  $\sum_{k=1}^n \frac{1}{k^2}$  tem um limitante superior que não depende de  $n$ .

**Exercício 9.14:** Encontre e prove um limitante superior para  $\sum_{k=1}^n k^{5/2}$ .

**Exercício 9.15:** Encontre um limitante superior para a somatória  $\sum_{k=m}^n k^{3/2}$ .

### 9.5.4 Minoração por integrais

De maneira análoga, podemos usar integração para obter um limitante inferior para uma somatória. Seja novamente  $f$  uma função crescente de  $\mathbb{R}$  para  $\mathbb{R}$ , e considere a função  $f^\#$  definida por  $f^\#(x) = f(\lceil x \rceil)$ . A figura 9.3 ilustra a relação entre estas duas funções:

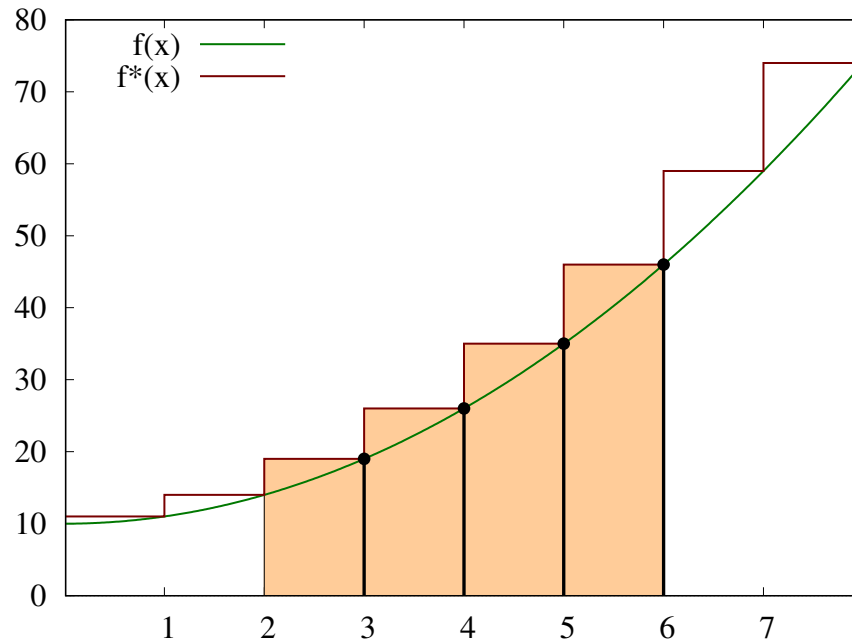


Figura 9.3: Limitante inferior por integral.

Observe que o gráfico da função  $f^\#$  está sempre acima do gráfico de  $f$ , pois  $\lceil x \rceil \geq x$  e portanto  $f^\#(x) \geq f(x)$ . Como na seção anterior, concluímos que a integral de  $f^\#$  entre dois inteiros é uma

somatória,

$$\int_m^n f^{\#}(x) dx = \sum_{k=m+1}^n f(k) \quad (9.46)$$

e portanto

$$\sum_{k=m+1}^n f(k) \geq \int_m^n f(x) dx \quad (9.47)$$

Para o exemplo da seção anterior,  $f(x) = x \log x$ , temos

$$\sum_{k=2}^n k \log k \geq \int_1^n x \log x dx = \frac{n^2}{2}(\log n - \frac{1}{2}) + \frac{1}{4} \quad (9.48)$$

Para melhor comparar este limitante inferior com o limitante superior (9.42), podemos passar o último termo da somatória ( $k = n$ ) para o lado direito, e observar que  $k \log k$  é zero quando  $k = 1$ . Obtemos então

$$\begin{aligned} \sum_{k=1}^{n-1} k \log k &\geq \frac{n^2}{2}(\log n - \frac{1}{2}) + \frac{1}{4} - n \log n \\ &= \frac{n^2}{2} \log n - \frac{n^2}{4} - n \log n + \frac{1}{4} \end{aligned} \quad (9.49)$$

A diferença entre os limitantes, que mede nossa incerteza sobre o valor da somatória, é

$$\Delta = (\frac{n^2}{2} \log n - \frac{n^2}{4} + \frac{1}{4}) - (\frac{n^2}{2} \log n - \frac{n^2}{4} - n \log n + \frac{1}{4}) \quad (9.50)$$

$$= n \log n \quad (9.51)$$

Por exemplo, para  $n = 100$ , os dois limitantes (9.42) e (9.49) permitem dizer que

$$20065.5 \leq \sum_{k=1}^{99} k \log k \leq 20526.2 \quad (9.52)$$

A largura desse intervalo é aproximadamente 460.5. O valor real da somatória é 20296.2 . . .

**Exercício 9.16:** Usando a minoração por integral, prove que  $H_n \geq \ln(n + 1)$ .

## 9.6 Somas infinitas

A notação  $\Sigma$  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,

$$\sum_{k=0}^{\infty} f(k) = \lim_{n \rightarrow \infty} \sum_{k=0}^n f(k) \quad (9.53)$$

**Exemplo 9.9:** Se  $x$  é um número real positivo, então

$$\sum_{k=0}^{\infty} x^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n x^k = \lim_{n \rightarrow \infty} \frac{1 - x^{n+1}}{1 - x} = \begin{cases} 1/(1 - x), & \text{se } 0 \leq x < 1 \\ +\infty, & \text{se } x \geq 1 \end{cases} \quad (9.54)$$

Em particular,

$$\sum_{k=0}^{\infty} \frac{1}{2^k} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 2 \quad (9.55)$$

e

$$\sum_{k=0}^{\infty} 2^k = 1 + 2 + 4 + 8 + \dots = +\infty \quad (9.56)$$

Observe que o limite pode não existir, ou pode ser infinito. Um exemplo clássico é a soma dos inversos dos inteiros positivos,

$$\sum_{k=1}^{\infty} \frac{1}{k} \quad (9.57)$$

A soma dos  $n$  primeiros termos é o número harmônico  $H_n$  que é maior ou igual a  $\ln(n+1)$  (veja o exercício 9.16), e portanto tende a infinito quando  $n$  tende a infinito.

Séries são muito importantes no cálculo diferencial e integral, e são exaustivamente estudadas nessa disciplina. Em computação, somatórias finitas são mais comuns, mas as infinitas também ocorrem ocasionalmente. Por exemplo, se  $f(k) \geq 0$  para todo  $k \in \mathbb{N}$ , temos que

$$\sum_{k=0}^n f(k) \leq \sum_{k=0}^{\infty} f(k) \quad (9.58)$$

desde que a somatória infinita esteja definida. Esta desigualdade pode oferecer um limitante superior simples para uma somatória finita que não possui uma fórmula fechada simples. Por exemplo,

$$\sum_{k=0}^n \frac{z^k}{k!} \leq \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z \quad (9.59)$$

**Exercício 9.17:** Prove que

$$\sum_{k=0}^{\infty} \frac{(k-1)}{2^k} = 0.$$

**Exercício 9.18:** Encontre um limitante superior para a somatória:

$$\sum_{k=0}^n \frac{k}{3^k}.$$

**Exercício 9.19:** Obtenha uma fórmula para  $\sum_{k=1}^{\infty} kx^k$ , supondo que a soma converge. (Dica: calcule a derivada de  $\sum_{k=0}^{\infty} x^k$  em relação a  $x$ .)

## 9.7 Produtórias

Sejam  $m, n$  números inteiros e  $f$  uma função definida sobre os inteiros. A notação

$$\prod_{k=m}^n f(k) \tag{9.60}$$

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 9.20:** Calcule o valor da produtória  $\prod_{k=-2}^{+2} k^2 + 1$ .

**Exercício 9.21:** Dê fórmulas explícitas (sem  $\prod$  nem ‘...’) para o valor das produtórias abaixo:

- |                      |                       |                        |                          |
|----------------------|-----------------------|------------------------|--------------------------|
| 1. $\prod_{k=1}^n 3$ | 2. $\prod_{k=0}^n 3$  | 3. $\prod_{k=m}^n 3$   | 4. $\prod_{k=m}^{m+2} 3$ |
| 5. $\prod_{k=1}^n k$ | 6. $\prod_{k=-n}^n k$ | 7. $\prod_{k=1}^n k^2$ | 8. $\prod_{k=0}^n 2^k$   |

**Exercício 9.22:** Dê fórmulas explícitas (sem  $\prod$  nem ‘...’) para o valor das produtórias abaixo:

- |                      |                                  |                                      |
|----------------------|----------------------------------|--------------------------------------|
| 1. $\prod_{k=m}^n k$ | 2. $\prod_{k=1}^n \frac{k+1}{k}$ | 3. $\prod_{k=1}^n \prod_{i=1}^m 3^i$ |
|----------------------|----------------------------------|--------------------------------------|

Uma produtória também pode ser transformada em somatória usando a função logaritmo  $\ln x = \log_e x$  e a função exponencial  $\exp x = e^x$ , onde  $e$  é a constante neperiana 2.718281828.... Lembramos que  $ab = \exp((\ln a) + (\ln b))$  para quaisquer reais positivos  $a, b$ . Podemos então concluir que

$$\prod_{k=m}^n f(k) = \exp \left( \sum_{k=m}^n \ln f(k) \right) \quad (9.61)$$

Esta identidade pode ser usada, por exemplo para majorar produtórias por integrais.

**Exercício 9.23:** Determine fórmulas explícitas para as produtórias

$$1. \prod_{k=1}^n 2 \cdot 4^k \quad 2. \prod_{k=0}^n \sqrt{k+1} \quad 3. \prod_{k=2}^n \left(1 - \frac{1}{k^2}\right)$$

## 9.8 Iteração de outras operações

Notações análogas a somatórias e produtórias podem ser usada para indicar a iteração (repetição) de outras operações associativas. Por exemplo, se  $P$  é um predicado que depende de um inteiro  $i$ , podemos escrever

$$\begin{aligned} \bigvee_{i=1}^n P(i) &= \mathbf{F} \vee P(1) \vee P(2) \vee \cdots \vee P(n) \\ \bigwedge_{i=1}^n P(i) &= \mathbf{V} \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(n) \\ \bigoplus_{i=1}^n P(i) &= \mathbf{F} \oplus P(1) \oplus P(2) \oplus \cdots \oplus P(n) \end{aligned} \tag{9.62}$$

De maneira análoga, se  $X$  é uma função que a cada inteiro  $i$  associa um conjunto, podemos escrever

$$\begin{aligned} \bigcup_{i=1}^n X(i) &= \{\} \cup X(1) \cup X(2) \cup \cdots \cup X(n) \\ \bigcap_{i=1}^n X(i) &= \mathbb{U} \cap X(1) \cap X(2) \cap \cdots \cap X(n) \end{aligned} \tag{9.63}$$

Note que, quando o conjunto de termos é vazio, o resultado é o elemento neutro da operação:  $\mathbf{F}$  para  $\vee$  e  $\oplus$ ,  $\mathbf{V}$  para  $\wedge$ ,  $\{\}$  para  $\cup$ , e o conjunto universal  $\mathbb{U}$  para  $\cap$ .

Assim como no caso de somatórias, muitas das variações, propriedades e fórmulas de somatórias podem ser adaptadas para estas operações iteradas. Porém, identidades e fórmulas que alteram a ordem dos termos somente valem se a operação for comutativa.

# Capítulo 10

## Sequências infinitas e recorrências

### 10.1 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  $r$ . Assim como no caso das sequências finitas, a escolha do índice inicial  $r$  varia de autor para autor. A escolha  $r = 1$  é tradicional e muito comum em matemática e outras ciências; nesse caso o domínio é o conjunto dos inteiros positivos  $\mathbb{P} = \mathbb{N} \setminus \{0\}$ . Entretanto, em alguns contextos (especialmente em computação), é conveniente adotar  $r = 0$ , e definir sequências infinitas como funções com domínio  $\mathbb{N}$ .

**Exemplo 10.1:** Seja  $x : \mathbb{N} \rightarrow \mathbb{R}$  onde  $x_n = \sqrt{n}$ , para todo  $n \in \mathbb{N}$ . A sequência é o conjunto de pares (termos)  $x = \{(n, \sqrt{n}) : n \in \mathbb{N}\} = \{(0, 0), (1, 1), (2, \sqrt{2}), (3, \sqrt{3}), (4, 2), \dots\}$ .

Outros exemplos de sequências infinitas com domínio  $\mathbb{N}$  são a função identidade  $x_n = n$ , a função fatorial  $x_n = n!$ , os números harmônicos  $H_n = \sum_{k=1}^n 1/k$ , e a sequência  $p$  dos números primos do exemplo ???. A função “menor divisor primo”  $d$  do exemplo 8.6, cujo domínio é  $Q = \mathbb{N} \setminus \{0, 1\}$ , é uma sequência infinita com índice inicial 2.

Para sequências infinitas valem os mesmos conceitos de termo, índice e valor vistos para sequências finitas, bem como a notação  $x_n$  em vez de  $x(n)$ .

Ocasionalmente a palavra “sequência” também é usada quando o domínio é o conjunto de todos os inteiros  $\mathbb{Z}$ ; nesse caso pode-se dizer que a sequência é *bi-infinita*.

O conceito de subsequência (definido na seção 8.13.5) também vale para sequências infinitas e bi-infinitas. Por exemplo, se  $x$  é a sequência com domínio  $\mathbb{N}$  tal que  $x_n = n^2$ , e  $R$  é o conjunto dos números naturais pares, a subsequência  $y$  de  $x$  determinada por  $R$  seria a restrição de  $x$  a  $R$ , ou seja, a função

$$y = \{(2k, 4k^2) : k \in \mathbb{N}\} = \{(0, 0), (2, 4), (4, 16), \dots\}$$

Como no caso finito, é conveniente supor que os termos de uma subsequência são re-indexados a partir do índice inicial convencional. No exemplo acima, a subsequência de  $x$  determinada por  $R$ , re-indexada a partir de 0, seria a função

$$y = \{(k, 4k^2) : k \in \mathbb{N}\} = \{(0, 0), (1, 4), (2, 16), \dots\}$$

## 10.2 Especificando sequências infinitas

Uma sequência infinita obviamente não pode ser especificada listando todos seus termos. Como discutido na seção ??, essas sequências podem ser definidas por fórmulas ou algoritmos.

Uma maneira que *não* é válida é listar alguns termos iniciais da sequência e escrever “e assim por diante” ou reticências. Na prática, é às vezes necessário deduzir uma fórmula para o termo geral de uma sequência da qual se conhecem apenas alguns termos, como 0, 1, 8, 27, 64, ... (que poderia ser  $x_n = n^3$ ), ou 1, 4, 10, 28, 82, 244, 730, ... (que poderia ser  $x_n = 3^n + 1$ ). Porém, este é um problema “mal posto,” pois sempre existem infinitas fórmulas distintas que fornecem os valores dados, mas diferem em outros índices. Por exemplo, outra sequência que também começa com 0, 1, 8, 27, 64, ... é  $y_n = n^3 + n(n-1)(n-2)(n-3)(n-4)$ . Esta fórmula é diferente de  $x_n = n^3$ , pois  $x_5 = 125$  mas  $y_5 = 245$ .

## 10.3 Recorrência

Muitas sequências importantes são definidas recursivamente, fornecendo-se um ou mais termos iniciais e uma fórmula que determina os demais termos a partir dos termos que os precedem. Essa fórmula é chamada de *recorrência*.

**Exemplo 10.2:** 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.

Pode-se provar facilmente por indução que o termo geral da progressão aritmética do exemplo 10.2 é  $x_n = a + nr$ , para todo  $n \geq 0$ ; ou seja, uma função linear do índice  $n$ .

**Exemplo 10.3:** 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.

O termo geral de uma progressão geométrica é  $x_n = ar^n$ , para todo  $n \geq 0$ ; ou seja, uma função exponencial do índice  $n$ .

**Exemplo 10.4:** A sequência dos *números de Fibonacci* é definida por

$$\begin{aligned}f_0 &= 0 \\f_1 &= 1 \\f_n &= f_{n-2} + f_{n-1} \quad \text{para todo } n \geq 2\end{aligned}$$

Os primeiros termos dessa sequência são 0, 1, 1, 2, 3, 5, 8, 13, ...

**Exemplo 10.5:** No capítulo 5 mostramos que um conjunto de  $n$  retas em posição geral divide o plano em  $R_n = n(n+1)/2 + 1$  regiões. Estas regiões também podem ser descritas pela recorrência abaixo:

$$\begin{aligned}R_0 &= 1 \\R_n &= R_{n-1} + n \quad \text{para todo } n \geq 1\end{aligned}$$

**Exercício 10.1:** 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  $n$ .

**Exercício 10.2:** A função de Ackermann (ou de Ackermann-Péter)  $A$  de  $\mathbb{N} \times \mathbb{N}$  para  $\mathbb{N}$  é definida recursivamente pelas fórmulas

$$A(m, n) = \begin{cases} n + 1 & \text{se } m = 0 \\ A(m - 1, 1) & \text{se } m > 0 \text{ e } n = 0 \\ A(m - 1, A(m, n - 1)) & \text{se } m > 0 \text{ e } n > 0 \end{cases} \quad (10.1)$$

Esta função é famosa por crescer muito rapidamente com o valor de  $m$ . Por exemplo,  $A(3, 1)$  é 13,  $A(4, 1)$  é 65.533, e  $A(5, 1)$  é grande demais para ser escrito aqui. Verifique que  $A(3, 3) = 61$ . (Nota: este cálculo é muito trabalhoso.)

## 10.4 Resolução de recorrências

Determinar uma fórmula explícita para uma sequência definida recursivamente é um problema difícil em geral, mas há técnicas que resolvem certos casos especiais.

### 10.4.1 Recorrência aditiva simples

Um desses casos especiais são as recorrências da forma  $x_n = x_{n-1} + f(n)$  para todo  $n \geq m$ , onde  $f$  é uma função qualquer. A progressão aritmética do exemplo 10.2 é um caso particular desta classe, cuja solução, como vimos, é  $x_n = a + rn$ . Uma fórmula semelhante resolve recorrências da forma  $x_n = x_{n-1} + r$  que valem somente a partir de um índice  $m$  diferente de zero.

**Exercício 10.3:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned} x_m &= a \\ x_n &= x_{n-1} + r \quad \text{para todo } n > m \end{aligned}$$

onde  $m$  é uma constante inteira, e  $a, b$  são constantes reais que não dependem de  $n$ .

No caso da recorrência geral  $x_n = x_{n-1} + f(n)$  para todo  $n > m$ , Pode-se verificar por indução em  $n$  que a solução desta recorrência é

$$x_n = x_m + \sum_{k=m+1}^n f(k)$$

**Exercício 10.4:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned} x_0 &= 2 \\ x_n &= x_{n-1} + \pi^2 \quad \text{para todo } n > 0 \end{aligned}$$

**Exercício 10.5:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned}x_0 &= 0 \\x_n &= x_{n-1} + n^2 \quad \text{para todo } n > 0\end{aligned}$$

**Exercício 10.6:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned}x_1 &= 1 \\x_n &= x_{n-1} + 2^n \quad \text{para } n > 1\end{aligned}$$

**Exercício 10.7:** Seja  $z_n$  o maior número de regiões em que o plano  $\mathbb{R}^2$  pode ser dividido por  $n$  círculos distintos de raio 1.

- (a) Determine uma recorrência para  $z_n$ .
- (b) Determine uma fórmula fechada para  $z_n$ .

**Exercício 10.8:** Seja  $x_n$  o número de sequências de  $n$  termos sobre o conjunto  $\{0, 1, 2\}$  que tem um número ímpar de termos iguais a zero.

- (a) Determine uma recorrência para  $x_n$ .
- (b) Determine uma fórmula fechada para  $x_n$ .

### 10.4.2 Recorrência multiplicativa simples

Outro caso importante são as recorrências da forma  $x_n = f(n)x_{n-1}$  para todo  $n > m$ , onde  $f$  é uma função qualquer. No caso particular da progressão geométrica (exemplo 10.3), em que  $f(n)$  é uma constante  $r$ ,  $m = 0$ , e  $x_0 = a$ , a solução, como vimos, é  $x_n = ar^n$  para todo  $n \geq 0$ . Recorrências com índice inicial  $m > 0$  tem solução semelhante.

**Exercício 10.9:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned} x_0 &= \pi \\ x_n &= \frac{x_{n-1} \sqrt{\pi}}{2} \quad \text{para todo } n > 0 \end{aligned}$$

**Exercício 10.10:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned} x_m &= a \\ x_n &= rx_{n-1} \quad \text{para todo } n > m \end{aligned}$$

onde  $m$  é uma constante inteira, e  $a, b$  são constantes reais que não dependem de  $n$ .

Quando  $f$  é uma função que depende de  $n$ , o resultado é uma produtória

$$x_n = x_m \prod_{k=m+1}^n f(k)$$

**Exercício 10.11:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned} x_0 &= 1 \\ x_n &= \frac{2}{n} x_{n-1} \quad \text{para todo } n > 0 \end{aligned}$$

**Exercício 10.12:** Determine a fórmula para o termo geral  $x_n$  da recorrência

$$\begin{aligned} x_0 &= 1 \\ x_n &= \frac{n+p}{n} x_{n-1} \quad \text{para todo } n > 0 \end{aligned}$$

onde  $p$  é um número natural que não depende de  $n$ .

### 10.4.3 Recorrências lineares homogêneas

Dizemos que uma relação de recorrência é *linear e homogênea de ordem  $k$*  se ela tem a forma

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} \quad (10.2)$$

onde  $k$  é um inteiro positivo e os coeficientes  $c_1, c_2, \dots, c_k$  são números reais, todos independentes de  $n$ . Pode-se provar por indução que esta recorrência é satisfeita por uma progressão geométrica  $x_n = r^n$ , onde  $r$  é qualquer raiz do polinômio

$$z^k - c_1 z^{k-1} - c_2 z^{k-2} - \cdots - c_k z^0 \quad (10.3)$$

Esta fórmula é chamada de *polinômio característico* da recorrência.

Por exemplo, a recorrência  $f_n = f_{n-2} + f_{n-1}$  dos números de Fibonacci é linear e homogênea de ordem 2, com coeficientes  $c_1 = c_2 = 1$ . Ela é satisfeita pelas sequências  $x$  e  $y$ , onde  $x_n = r^n$ ,  $y_n = s^n$ , e  $r, s$  são as duas raízes da equação  $z^2 = z + 1$ . Estas raízes são

$$r = \frac{1 + \sqrt{5}}{2} \quad s = \frac{1 - \sqrt{5}}{2} \quad (10.4)$$

A primeira raiz  $r \approx 1.6180339887 \dots$ , geralmente denotada pela letra  $\phi$ , é conhecida como *razão áurea*, porque na Grécia antiga os arquitetos e artistas acreditavam que o retângulo com lados 1 e  $\phi$  tinha as proporções mais belas dentre todos os retângulos. A segunda raiz  $s \approx -0.6180339887 \dots$ , que vários autores denotam por  $\hat{\phi}$ , é igual a  $1 - \phi$  e  $-\frac{1}{\phi}$ .

| $n$      | $r^n$       | $s^n$       |
|----------|-------------|-------------|
| 0        | 1.00000000  | 1.00000000  |
| 1        | 1.61803399  | -0.61803399 |
| 2        | 2.61803399  | 0.38196601  |
| 3        | 4.23606798  | -0.23606798 |
| 4        | 6.85410197  | 0.14589803  |
| 5        | 11.09016994 | -0.09016994 |
| 6        | 17.94427191 | 0.05572809  |
| 7        | 29.03444185 | -0.03444185 |
| $\vdots$ | $\vdots$    | $\vdots$    |

Nesta tabela pode-se verificar que  $r^2 = r^1 + r^0$ ,  $s^2 = s^1 + s^0$ ,  $r^3 = r^2 + r^1$ , e assim por diante.

As sequências  $x$  e  $y$  são apenas duas das possíveis soluções para a recorrência de fibon. Pode-se provar que qualquer combinação linear destas duas sequências

$$z_n = \alpha x_n + \beta y_n = \alpha \phi^n + \beta \hat{\phi}^n \quad (10.5)$$

também é uma solução da recorrência. Os valores de  $\alpha$  e  $\beta$  podem ser obtidos a partir dos valores iniciais dados  $f_0 = 0$  e  $f_1 = 1$ , e são

$$\alpha = 1/\sqrt{5} \quad \beta = -1/\sqrt{5} \quad (10.6)$$

Ou seja

$$f_n = \frac{1}{\sqrt{5}}(\phi^n - \hat{\phi}^n) \quad (10.7)$$

Uma vez que  $|\hat{\phi}| = 0.61803399$  é menor que 1, o valor absoluto do termo  $\hat{\phi}^n$  da fórmula (10.7) vai diminuindo rapidamente à medida que  $n$  aumenta. Portanto,

$$\lim_{n \rightarrow \infty} \frac{f_n}{f_{n-1}} = \phi \quad (10.8)$$

e podemos dizer que

$$f_n \approx \frac{1}{\sqrt{5}}\phi^n \quad (10.9)$$

Esta técnica resolve qualquer recorrência homogênea de ordem  $k$  cujo polinômio característico tem  $k$  raízes distintas. Quando o polinômio tem raízes iguais, ainda existem  $k$  soluções independentes, mas elas tem uma forma um pouco mais complicada. Especificamente para cada raiz  $r$  com multiplicidade  $p$ , toda sequência  $x_n = n^i r^n$ , para todo  $i$  entre 0 e  $p-1$ , é uma solução independente.

**Exercício 10.13:** Considere a situação descrita no exercício 10.1. Determine uma fórmula explícita para o número  $x_n$  de tatus que existem no ano  $n \geq 2000$ .

**Exercício 10.14:** Seja  $s_n$  o número de sequências de  $n$  vogais minúsculas (a, e, i, o ou u) que não possuem duas vogais 'e' consecutivas.

- (a) Determine uma recorrência para  $s_n$ .
- (b) Determine uma fórmula fechada para  $s_n$ .

**Exercício 10.15:** Numa mesa redonda com  $n$  lugares numerados ( $n \geq 2$ ), devem ser dispostos  $n$  pratos de  $k$  cores diferentes ( $k \geq 3$ ). Para um  $k$  genérico, determine uma fórmula explícita para o número  $x_n$  de possibilidades de fazer isso de tal maneira que cada prato tenha cor distinta das cores de seus dois vizinhos.

**Exercício 10.16:** Determine uma fórmula explícita para o número de maneiras de cobrir um tabuleiro de  $2 \times n$  casas com  $n$  dominós, cada um cobrindo duas casas adjacentes na vertical ou na horizontal.

## 10.5 Recorrências lineares não homogêneas

Uma *recorrência linear não homogênea* é uma fórmula que define o termo geral  $x_n$  como uma combinação linear de termos anteriores, com coeficientes constantes, mais uma função arbitrária do índice  $n$ . Por exemplo,

$$\begin{aligned} x_0 &= 0 \\ x_n &= 2x_{n-1} + 2^n \quad \text{para todo } n > 0 \end{aligned} \tag{10.10}$$

Pode-se verificar, por indução, que  $x_n = n2^n$  é a solução desta recorrência.

No caso geral, uma recorrência linear não homogênea de ordem  $k$  tem a forma

$$\left. \begin{aligned} x_0 &= a_0 \\ x_1 &= a_1 \\ \vdots \\ x_{k-1} &= a_{k-1} \end{aligned} \right\} \tag{10.11}$$

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} + f_n \quad \text{para todo } n \geq k \tag{10.12}$$

onde  $a_0, a_1, \dots, a_{k-1}, c_1, c_2, \dots, c_k$  são constantes (que não dependem de  $n$ ), e  $f$  (o *termo independente*) é uma sequência qualquer. Por exemplo, considere a recorrência

$$\left. \begin{aligned} x_0 &= 2 \\ x_1 &= 2 \end{aligned} \right\} \tag{10.13}$$

$$x_n = x_{n-1} + x_{n-2} + (-1)^n \quad \text{para todo } n \geq 2 \tag{10.14}$$

Note que esta recorrência é similar à de Fibonacci, exceto pelos termos iniciais e pela parcela  $(-1)^n$  na recorrência.

Não há uma técnica geral para resolver recorrências não homogêneas, como (10.11)–(10.12). Entretanto, suponha que conseguimos encontrar *uma* sequência particular  $x$  que satisfaz a fórmula do termo geral (10.12), mas não necessariamente os termos iniciais. No exemplo acima, pode-se verificar que  $x_n = (-1)^n$  é uma solução para a recorrência (10.14), embora tenha  $x_0 = +1$  e  $x_1 = -1$ . Considere agora a recorrência homogênea similar a (10.14),

$$z_n = z_{n-1} + z_{n-2} \quad (10.15)$$

Como vimos anteriormente, a solução geral para esta recorrência é  $z_n = \alpha\phi^n + \beta\hat{\phi}^n$ . Verifica-se então que a solução geral para a recorrência original (10.14) é a soma de  $z_n$  e da solução particular acima, isto é,

$$z_n = \alpha\phi^n + \beta\hat{\phi}^n + (-1)^n \quad (10.16)$$

Os valores de  $\alpha$  e  $\beta$  podem ser então determinados pelas condições iniciais  $x_0 = 2$  e  $x_1 = 2$ , resultando em

$$\begin{aligned} \alpha &= \frac{\phi+2}{2\phi-1} \\ \beta &= \frac{\phi-3}{2\phi-1} \end{aligned} \quad (10.17)$$

e portanto

$$x_n = \frac{\phi+2}{2\phi-1}\phi^n + \frac{\phi-3}{2\phi-1}\hat{\phi}^n + (-1)^n \quad (10.18)$$

De modo geral, podemos resolver a recorrência linear não homogênea (10.11)–(10.12) somando uma solução particular  $x$  da equação (10.12) com a solução geral da equação homogênea

$$y_n = c_1y_{n-1} + c_2y_{n-2} + \cdots + c_ky_{n-k} \text{ para todo } n \geq k \quad (10.19)$$

Esta solução geral vai depender de  $k$  parâmetros  $\alpha_1, \dots, \alpha_k$ , que podem ser determinados pelas condições iniciais (10.11).

**Exercício 10.17:** Resolva a recorrência

$$\begin{cases} x_0 &= 3 \\ x_n &= \frac{4}{3}x_{n-1} - 1 \end{cases} \quad (10.20)$$

## 10.6 Majoração e minoração de recorrências

Muitas vezes é difícil ou impossível obter uma fórmula explícita exata para uma sequência  $y$  definida recursivamente sobre um conjunto de índices  $D$ . Porém, nesses casos pode ser possível obter um *limitante inferior* para  $y$ : uma sequência  $x$ , com mesmo domínio  $D$ , tal que  $x_n \leq y_n$  para todo  $n$  em  $D$ . Analogamente, pode ser possível obter um *limitante superior*, uma sequência  $z$  tal que  $y_n \leq z_n$  para todo  $n$  em  $D$ . Tais limitantes podem ser suficientes para muitos fins — como, por exemplo, reserva de espaço de memória para certa tarefa ou estimativa do tempo de execução de um programa.

Por exemplo, considere a sequência  $y$  tal que

$$\begin{aligned} y_0 &= 3 \\ y_n &= y_{n-1} + \lfloor y_{n-1}/3 \rfloor \text{ para todo } n > 0 \end{aligned} \quad (10.21)$$

Os primeiros termos desta sequência são

|       |   |   |   |   |   |    |    |    |    |    |    |    |    |    |
|-------|---|---|---|---|---|----|----|----|----|----|----|----|----|----|
| $n$   | 0 | 1 | 2 | 3 | 4 | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 |
| $y_n$ | 3 | 4 | 5 | 6 | 8 | 10 | 13 | 17 | 22 | 29 | 38 | 50 | 66 | 88 |

Podemos obter um limitante superior para  $y$  trocando o lado direito da recorrência por uma fórmula mais simples que seja maior ou igual a esse termo. Por exemplo,

$$\begin{aligned} z_0 &= 3 \\ z_n &= z_{n-1} + z_{n-1}/3 \text{ para todo } n > 0 \end{aligned} \quad (10.22)$$

Podemos provar que  $z_n \geq y_n$  para todo  $n \in \mathbb{N}$ , por indução em  $n$ . Basta observar que  $z_{n-1} \geq y_{n-1}$ , pela hipótese de indução, e que  $u \geq \lfloor u \rfloor$  para qualquer número real  $u$ . A recorrência de  $z$  pode ser simplificada para  $z_n = (4/3)z_{n-1}$ . Esta é uma progressão geométrica com termo inicial 3 e razão  $4/3$ , e portanto a solução exata é  $z_n = 3(4/3)^n$ . Podemos então concluir que  $y_n \leq 3(4/3)^n$  para todo  $n$  em  $\mathbb{N}$ .

De maneira análoga, podemos obter um limitante inferior  $x$  observando que  $\lfloor u \rfloor \geq u - 1$  para todo número real  $u$ . Obtemos então a recorrência

$$\begin{aligned} x_0 &= 3 \\ x_n &= x_{n-1} + (x_{n-1}/3 - 1) \text{ para todo } n > 0 \end{aligned} \quad (10.23)$$

Esta recorrência pode ser reescrita  $x_n = (4/3)x_{n-1} - 1$  (veja o exercício 10.17).

**Exercício 10.18:** Prove que  $n! \leq n^n$  para todo inteiro  $n \geq 1$ .

**Exercício 10.19:** Prove que  $n! \leq 2^n$  para todo inteiro  $n \geq 0$ .

**Exercício 10.20:** Calcule  $9!$  e compare com  $5^9$ . Mais genericamente, compare  $n!$  (produto de  $n$  termos variando de 1 a  $n$ ) com  $[(n+1)/2]^n$  (produto de  $n$  termos todos iguais à média aritmética de 1 e  $n$ ).

**Exercício 10.21:** Calcule  $16!$  e compare com  $4^{16}$ . Mais genericamente, compare  $n!$  (produto de  $n$  termos variando de 1 a  $n$ ) com  $(\sqrt{n})^n$  (produto de  $n$  termos todos iguais à média geométrica de 1 e  $n$ ).



# Capítulo 11

## 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. Na seção 2.4.1, por exemplo, vimos que o número de subconjuntos de um conjunto com  $n$  elementos é  $2^n$ . Neste capítulo vamos examinar alguns dos problemas mais comuns deste tipo.

Neste tipo de problemas é importante notar se os objetos que aparecem no enunciado são considerados distintos ou não. Por exemplo, observe a questão “quantos resultados é possível 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 11.1:** 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.

**Exercício 11.2:** Em um balcão são colocados cem copos, enfileirados e virados com a boca para cima, numerados de 1 a 100. Cem pessoas percorrem essa fileira, invertendo alguns dos copos. A  $n$ -ésima pessoa inverte todos os copos cujo número é múltiplo de  $n$ . No final, quais copos estarão virados com a boca para baixo?

## 11.1 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. Concluimos que a resposta é  $2^{mn}$ . Pelo mesmo argumento, o número de relações sobre o conjunto  $X$  (isto é, de  $X$  para  $X$ ) é  $2^{m^2}$ .

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  $X \times X$ . Concluimos que o número de relações reflexivas sobre  $X$  é  $2^{m(m-1)}$ .

**Exercício 11.3:** Sejam  $X$  e  $Y$  conjuntos finitos, com  $|X| = m$  e  $|Y| = n$ , e  $\mathcal{R}$  uma relação de  $X$  para  $Y$ , com  $p$  pares. Quantas relações de  $X$  para  $Y$  existem que contêm a relação  $\mathcal{R}$ ? Quantas relações de  $X$  para  $Y$  existem que são disjuntas de  $\mathcal{R}$ ?

**Exercício 11.4:** Se  $X$  é um conjunto com  $m$  elementos, quantas relações *irreflexivas* distintas existem sobre  $X$ ? Quantas relações *simétricas*? E quantas *anti-simétricas*?

## 11.2 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. Além disso, em cada um desses pares, o segundo membro (o valor  $\mathcal{F}(a)$  da função) pode ser qualquer um dos  $n$  elementos de  $Y$ . Temos então  $n$  valores possíveis da função para cada um dos  $m$  elementos de  $X$ . Concluimos que o número de funções de  $X$  para  $Y$  é  $n^m$ .

**Exercício 11.5:** Quantas maneiras há de empilhar cinco frutas, que podem ser laranjas (indistinguíveis entre si) ou maçãs (também indistinguíveis) dentro um vaso estreito de vidro?

**Exercício 11.6:** Seja  $X$  um conjunto finito com  $m$  elementos. Quantos predicados distintos existem sobre  $X$ ?

**Exercício 11.7:** Um modelo de carro é vendido com 3 cores de exterior e 2 cores de estofamento. Se 10 pessoas comprem um carro cada uma, de quantas maneiras elas podem escolher as cores?

**Exercício 11.8:** Em uma reunião de  $n$  pessoas, cada uma escreve seu nome em um bilhete e o entrega a alguma outra pessoa do grupo. Quantos são os resultados possíveis dessa operação?

**Exercício 11.9:** Imagine que  $n$  dados, de cores diferentes, são lançados sobre uma mesa. Quantos são os resultados possíveis?

**Exercício 11.10:** Vinte pessoas precisam ser transportadas por um bondinho no qual cabem apenas 5 pessoas por viagem. Quantas maneiras há de distribuir essas pessoas nas 4 viagens necessárias?

## 11.3 Princípio multiplicativo da contagem

Considere agora o problema de contar 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 das quatro 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 número de maneiras de arranjar as crianças é

$$4 \times 3 \times 3 \times 2 \times 2 \times 1 \times 1 = 144 \quad (11.1)$$

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  $D_1, D_2, \dots, D_r$ , 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

$$n_1 \times n_2 \times \cdots \times n_r \quad (11.2)$$

**Exercício 11.11:** Em uma reunião de  $n$  pessoas, cada uma escreve seu nome em um bilhete e o entrega a alguma outra pessoa do grupo. Quantos são os resultados possíveis dessa operação?

**Exercício 11.12:** Quantas bandeiras é possível formar com 5 listras horizontais com cores azul, branca e vermelha, sendo que duas listras adjacentes devem ter cores diferentes?

**Exercício 11.13:** Sejam  $X$  e  $Y$  conjuntos finitos, com  $|X| = m$  e  $|Y| = n$ . Seja  $R$  um subconjunto de  $X$  com  $r$  elementos, e  $S$  um subconjunto de  $Y$  com  $s$  elementos. Quantas funções  $\mathcal{F}$  distintas existem de  $X$  para  $Y$  tais que  $\mathcal{F}(x) \in S$  para todo  $x$  em  $R$ ?

**Exercício 11.14:** Um baralho padrão tem cartas de 4 naipes e 13 valores (52 cartas no total). De quantas maneiras é possível formar uma pilha de 3 cartas sem repetir nenhum naipe ou valor?

**Exercício 11.15:** Quantos números inteiros existem entre 1000 e 9999 (inclusive ambos) com todos os algarismos distintos?

**Exercício 11.16:** Os números  $0, 1, 2, \dots, 9$  são colocados em uma sequência  $x_0, x_1, \dots, x_9$ , de tal forma que  $x_k \geq k - 2$  para todo  $k$ . Ou seja,  $x_9 \geq 7$ ,  $x_8 \geq 6$ ,  $x_7 \geq 5$ , e assim por diante. De quantas maneiras podemos fazer isto?

**Exercício 11.17:** Uma placa de automóvel tem 3 letras maiúsculas seguidas de 4 algarismos. Quantas placas distintas existem?

## 11.4 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  $\{0, 1, \dots, n-1\}$  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,  $X = \{a, e, i, o, u\}$ . A função

$$\{(0, u), (1, e), (2, i), (3, a), (4, o)\}$$

é uma permutação de  $X$ . Esta função pode ser escrita também como

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ u & e & i & a & o \end{pmatrix}$$

ou como a sequência  $(u, e, i, a, o)$  ou, simplesmente,  $ueiao$ ; ficando subentendido que os índices da sequência começam com 0. Duas outras permutações, distintas dessa, são  $uieao = (u, i, e, a, o)$  e  $eaoui = (e, a, o, i, u)$ .

Quantas permutações de  $X$  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

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n! \quad (11.3)$$

Assim, por exemplo, o número de permutações das cinco vogais é  $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$ .

O conceito de permutação, como definido acima, é muito semelhante ao de *função permutação* de um conjunto  $X$ , que definimos na seção 8.7 como sendo uma bijeção de  $X$  para  $X$ . Na verdade, se  $X$  e  $Y$  são conjuntos finitos com  $n$  elementos, é possível associar cada permutação de  $X$  (ou de  $Y$ ) a uma bijeção de  $X$  para  $Y$ , e vice-versa. Veja o exercício 11.18. Portanto concluímos que  $n!$  também é o número de bijeções entre dois conjuntos de  $n$  elementos.

Observe que se o conjunto  $X$  é vazio (isto é, se  $n = 0$ ) há apenas uma permutação possível, que é a sequência vazia  $()$  (ou seja, o conjunto vazio de pares índice-elemento). Esta observação justifica a definição de  $0!$  como sendo 1.

O seguinte exemplo ilustra um uso menos trivial de permutações. 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?

Observe que Alice pode ficar à esquerda ou à direita de Beto; mas, em qualquer caso, o casal pode ser considerado uma única pessoa, e as duas cadeiras que eles ocupam podem ser consideradas uma única cadeira. Então, o número de soluções é  $2(n - 1)!$

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  $3.04 \times 10^{64}$ , 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.

**Exercício 11.18:** Sejam  $X$  e  $Y$  conjuntos finitos com  $n$  elementos, e  $h : \{0, 1, \dots, n-1\} \rightarrow X$  uma permutação dada de  $X$ . Prove as seguintes afirmações

- (a) Para qualquer permutação  $g : \{0, 1, \dots, n-1\} \rightarrow Y$ , a composição  $g \circ h^{-1}$  é uma bijeção de  $X$  para  $Y$ .
- (b) Para qualquer função bijetora  $f$  de  $X$  para  $Y$ , existe uma permutação  $g : \{0, 1, \dots, n-1\} \rightarrow Y$ , tal que  $f = g \circ h^{-1}$ .
- (c) Para quaisquer duas permutações  $g', g'' : \{0, 1, \dots, n-1\} \rightarrow Y$ , se  $g' \circ h^{-1} = g'' \circ h^{-1}$ , então  $g' = g''$ .

### 11.4.1 Fórmula de Stirling

A fórmula (11.3) 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  $e = 2.7182818\dots$ ). Aplicando  $\exp(x) = e^x$  em ambos os lados temos

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

**Exercício 11.19:** De quantas maneiras podemos dispor 8 torres de xadrez idênticas num tabuleiro com  $8 \times 8$  casas, de modo que não haja duas torres na mesma linha ou na mesma coluna? E se as torres tiverem 8 cores diferentes?

**Exercício 11.20:** Um trem de montanha russa tem 6 bancos de 2 lugares. De quantas maneiras podem sentar 6 meninas e 6 meninos, sendo que em cada banco deve haver um menino e uma menina?

## 11.5 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  $\{0 \dots r-1\}$  para o conjunto  $X$ .

Por exemplo, todos os arranjos de 3 elementos do conjunto  $X = \{a, e, i, o, u\}$  são

|     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|
| aei | aie | eai | eia | iae | iea |
| aeo | aoe | eaο | eoα | oae | oea |
| aio | aoi | iao | ioa | oai | oia |
| aeu | aue | eau | eua | uae | uea |
| aiu | auī | iau | iua | uai | uia |
| aou | auo | oau | oua | uao | uoa |
| eio | eoī | ieo | ioe | oei | oie |
| eiū | eui | ieu | iue | uei | uie |
| eou | euo | oeu | oue | ueo | ue  |
| iou | iuo | oiu | oui | uio | uoi |

onde aie significa a sequência (a, i, e), ou seja a função

$$\begin{pmatrix} 0 & 1 & 2 \\ a & i & e \end{pmatrix}$$

e assim por diante.

Pelo mesmo raciocínio usado na seção 11.4, 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

$$n \times (n - 1) \times (n - 2) \times \cdots \times (n - r + 1) \quad (11.4)$$

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

$$\frac{n!}{(n-r)!} \quad (11.5)$$

Note que os fatores do denominador cancelam uma parte dos fatores do numerador, deixando apenas os fatores da fórmula (11.4). 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 (11.5) 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.

**Exercício 11.21:** Sejam  $X$  e  $Y$  conjuntos finitos com  $m$  e  $n$  elementos, respectivamente. Quantas funções sobrejetoras  $\mathcal{F} : X \rightarrow Y$  existem?

## 11.6 Combinações

Outro problema muito comum é contar o número de subconjuntos de tamanho  $r$  de um conjunto  $X$  de  $n$  elementos. Note que este problema é diferente de contar os arranjos de  $r$  elementos de  $X$ : em ambos os casos desejamos tomar  $r$  elementos de  $X$ , sem repetições; mas 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  $\{a, i, u\}$ , 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  $r$ ”.

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  $\{a, i, o\}$ .

Como temos  $r$  elementos em cada arranjo, concluímos que cada combinação corresponde a  $r!$  arranjos diferentes. Portanto, o número de combinações é

$$\frac{A_n^r}{r!} = \frac{n \times (n-1) \times \cdots \times (n-r+1)}{r \times (r-1) \times \cdots \times 1} \quad (11.6)$$

Esta fórmula pode ser escrita em termos de fatoriais

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} \quad (11.7)$$

**Exercício 11.22:** Quantas “mãos” diferentes de cinco cartas podem ser obtidas de um baralho de 52 cartas?

**Exercício 11.23:** Quantas maneiras há de empilhar 3 laranjas (indistinguíveis) e 2 maçãs (indistinguíveis) dentro um vaso estreito de vidro?

**Exercício 11.24:** Há  $2^n$  sequências distintas de  $n$  bits (algarismos 0 e 1). Quantas dessas sequências tem exatamente  $k$  bits iguais a 1?

### 11.6.1 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  $n$ .

Uma vez que o número de elementos de um conjunto é um número natural, 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  $r < 0$ .

### 11.6.2 Propriedades

A função  $\binom{n}{r}$  tem várias propriedades interessantes. Por exemplo, para todo  $n, r \in \mathbb{N}$ , temos

$$\binom{n}{r} = \binom{n}{n-r}$$

Para demonstrar esta identidade, 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. Ou seja, a operação de complemento em relação a  $X$  é uma bijeção entre o conjunto dos subconjuntos de  $r$  elementos e o conjunto dos subconjuntos de  $n - r$  elementos.

Outra propriedade importante é a *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



### 11.6.3 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

$$\begin{aligned}(a + b)^4 &= \binom{4}{0}a^4b^0 + \binom{4}{1}a^3b^1 + \binom{4}{2}a^2b^2 + \binom{4}{3}a^1b^3 + \binom{4}{4}a^0b^4 \\ &= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4\end{aligned}$$

Por conta desta fórmula, os números  $\binom{n}{r}$  são também chamados de *coeficientes binomiais*. As seguintes propriedades são corolários imediatos da fórmula de Newton:

**Exercício 11.25:** Prove que  $\sum_{r=0}^n \binom{n}{r} = 2^n$ .

**Exercício 11.26:** Prove que  $\sum_{r=0}^n 2^r \binom{n}{r} = 3^n$ .

**Exercício 11.27:** Prove que  $\sum_{r=0}^n (-1)^r \binom{n}{r} = 0$ .

**Exercício 11.28:** Seja  $X$  um conjunto de  $n$  elementos. Usando a fórmula do exercício 11.27, prove que o número de subconjuntos de  $X$  de tamanho par é igual ao número de subconjuntos de tamanho ímpar.

**Exercício 11.29:** Prove que, para todos os naturais  $k$  e  $n$  com  $n \geq k$ , temos  $\sum_{k=r}^n \binom{k}{r} = \binom{n+1}{r+1}$ .

**Exercício 11.30:** Uma prova tem 10 questões do tipo verdadeiro/falso. Quantas maneiras há de responder essas questões, sem deixar nenhuma em branco, de modo a acertar exatamente 7 delas? E acertar pelo menos 7 delas?

### 11.6.4 Fórmula recursiva

A fórmula (11.7) 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 (11.6),  $C_n^r = A_n^r/r!$ . 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 11.6 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.  $C \leftarrow (C \times (n - r + k))/k$

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.

### 11.6.5 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  $(x_1, x_2, \dots, x_p)$  de inteiros positivos existem tais que  $x_1 + x_2 + \dots + x_p = n$ . Pelo mesmo raciocínio acima, concluímos que a resposta é

$$\binom{n-1}{p-1} = \frac{(n-1)!}{(n-p)!(p-1)!} = \binom{n-1}{n-p} \quad (11.8)$$

Suponha agora o problema 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

$$\binom{n+p-1}{p-1} = \frac{(n+p-1)!}{n!(p-1)!} = \binom{n+p-1}{n} \quad (11.9)$$

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 (11.9). 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 (11.8).

**Exercício 11.31:** 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.)

## 11.7 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, (A, E, I, O, U), ou com (U, A, E, I, O), ou com (O, U, A, E, 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

$$\frac{n!}{n} = (n - 1)! \quad (11.10)$$

**Exercício 11.32:** 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?

## 11.8 Contagem por divisão

Mais geralmente, suponha que temos que contar um conjunto  $Y$  da forma

$$Y = \{ f(x) : x \in X \} \quad (11.11)$$

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 acima,  $X$  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 11.33:** 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?

**Exercício 11.34:** Imagine um quadrado de 2 cm de lado desenhado numa folha de caderno. De quantas maneiras é possível colocar um dado com 2 cm de lado sobre esse quadrado? Quantas maneiras distintas há de numerar as faces de um cubo com os números de 1 a 6?

## 11.9 Permutações e arranjos com elementos indistinguíveis

Outro exemplo da técnica acima é contar os anagramas da palavra BANANA; 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,

$$\begin{aligned}
 f(1, 2, 3, 4, 5, 6, 7) &= \text{BNNAAS} \\
 f(4, 1, 5, 2, 3, 6, 7) &= \text{ABANNAS} \\
 f(1, 4, 2, 5, 3, 6, 7) &= \text{BANANAS} \\
 f(1, 6, 3, 5, 2, 4, 7) &= \text{BANANAS} \\
 f(7, 2, 1, 4, 5, 6, 3) &= \text{SABANAN}
 \end{aligned} \tag{11.12}$$

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  $(x_1, x_2, \dots, x_n)$  de  $n$  elementos, que podem ter  $p$  valores distintos  $v_1, v_2, \dots, v_p$ ; 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

$$\frac{n!}{m_1! m_2! \cdots m_p!} \tag{11.13}$$

## 11.10 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 seção 11.6, 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 seção 11.6 permite concluir que esse número é

$$\binom{n}{r_1, r_2, \dots, r_t} = \frac{n!}{r_1! r_2! \cdots r_t!} \quad (11.14)$$

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

$$\binom{10}{5, 3, 2} = \frac{10!}{5!3!2!} = 2520 \quad (11.15)$$

maneiras distintas.

**Exercício 11.35:** 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 11.36:** 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?

**Exercício 11.37:** Quanto vale  $\binom{n}{r_1, r_2, \dots, r_t}$  se  $t = 1$ ? E se  $r_t = 0$ ? E se  $r_1 = r_2 = \dots = r_t = 1$ ?

O número de distribuições de  $n$  elementos em  $t$  caixas de tamanhos fixos aparece na fórmula da soma de  $t$  variáveis,  $x_1 + x_2 + \dots + x_t$ , elevada a potência  $n$ . Mais precisamente,  $\binom{n}{r_1, r_2, \dots, r_t}$  é o coeficiente do termo  $x_1^{r_1} x_2^{r_2} \dots x_t^{r_t}$  na expansão da fórmula  $(x_1 + x_2 + \dots + x_t)^n$ :

$$(x_1 + x_2 + \dots + x_t)^n = \sum_{\substack{r_1, r_2, \dots, r_t \\ r_1 + r_2 + \dots + r_t = n}} \binom{n}{r_1, r_2, \dots, r_t} x_1^{r_1} x_2^{r_2} \dots x_t^{r_t}.$$

Esta igualdade é conhecida como *fórmula de Leibniz*.

**Exemplo 11.1:**

$$\begin{aligned}
(a + b + c)^4 &= \binom{4}{4,0,0}a^4b^0c^0 + \binom{4}{3,1,0}a^3b^1c^0 + \binom{4}{2,2,0}a^2b^2c^0 + \binom{4}{1,3,0}a^1b^3c^0 + \binom{4}{0,4,0}a^0b^4c^0 + \\
&\quad \binom{4}{3,0,1}a^3b^0c^1 + \binom{4}{2,1,1}a^2b^1c^1 + \binom{4}{1,2,1}a^1b^2c^1 + \binom{4}{0,3,1}a^0b^3c^1 + \\
&\quad \binom{4}{2,0,2}a^2b^0c^2 + \binom{4}{1,1,2}a^1b^1c^2 + \binom{4}{0,2,2}a^0b^2c^2 + \\
&\quad \binom{4}{1,0,3}a^1b^0c^3 + \binom{4}{0,1,3}a^0b^1c^3 + \\
&\quad \binom{4}{0,0,4}a^0b^0c^4 \\
&= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4 + \\
&\quad 4a^3c + 12a^2bc + 12ab^2c + 4b^3c + \\
&\quad 6a^2c^2 + 12abc^2 + 6b^2c^2 + \\
&\quad 4ac^3 + 4bc^3 + \\
&\quad 1c^4
\end{aligned}$$

Estes números são também chamados de *coeficientes multinomiais*. Note que o coeficiente binomial  $\binom{n}{r}$  equivale ao coeficiente multinomial  $\binom{n}{r, n-r}$ .

Os coeficientes multinomiais também contam as maneiras de listar  $t$  objetos distintos com número especificado de repetições de cada objeto. Mais precisamente, suponha que queremos formar uma lista de comprimento  $n$  com  $t$  itens distintos, sendo que o primeiro item aparece  $r_1$  vezes na lista, o segundo item aparece  $r_2$  vezes, e assim por diante. O número de listas desse tipo é justamente  $\binom{n}{r_1, r_2, \dots, r_t}$ . Para compreender esta afirmação, basta considerar que ao escrever tal lista, temos que escrever  $n$  elementos, e, para cada  $i$ , escolher  $r_i$  elementos que serão iguais ao item número  $i$ .

**Exercício 11.38:** Quantas maneiras há de dividir 16 alunos em 3 grupos de estudo, para Física, Química e Matemática; sendo que deve haver 6 alunos em cada um dos dois primeiros grupos, e 4 no último?

## 11.11 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 à 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  $A_1, A_2, \dots, A_n$ , *disjuntos dois a dois*, então o número total de objetos é  $|A_1| + |A_2| + \dots + |A_n|$ .

**Exercício 11.39:** De um baralho completo (com 52 cartas) são retiradas 3 cartas e colocadas em fileira na mesa. A carta mais à esquerda não é um ás, e a carta mais à direita não é de copas. Quantas configurações assim existem?

**Exercício 11.40:** Imagine uma lista de todos os números de 5 dígitos que podem ser formados com os algarismos ‘1’, ‘2’, ‘5’, ‘8’ e ‘9’, ordenada pelo valor crescente do número. A lista começa com 12589, 12598, 12859, 12895, ..., e termina com ..., 98512, 98521.

- (a) Qual é o 50º número desta lista?
- (b) Que posição ocupa o número 52819 nesta lista?

**Exercício 11.41:** Uma roleta tem 10 setores, numerados sequencialmente de 1 a 10. Cada setor deve ser pintado com uma cor diferente das cores dos dois setores vizinhos. Há 5 cores disponíveis. De quantas maneiras podemos pintar essa roleta?

## 11.12 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  $Y$ :

$$|X| = |Y| - |Y \setminus X| \quad \text{se } X \subseteq Y \quad (11.16)$$

Esta fórmula também pode ser escrita

$$|Y \setminus Z| = |Y| - |Z| \quad \text{se } Z \subseteq Y \quad (11.17)$$

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 11.42:** Quantos pares de inteiros  $(x, y)$  existem que satisfazem todas estas propriedades:

(a)  $x \in \{0 \dots 9\}$ , (b)  $y \in \{0 \dots 9\}$ , (c) se  $x \in \{2 \dots 7\}$ , então  $y \notin \{2 \dots 7\}$ .

**Exercício 11.43:** Quantas mãos de 4 cartas podem ser tiradas de um baralho comum (de 52 cartas) nas quais aparecem pelo menos dois ases?

**Exercício 11.44:** Quantos números há entre 1000 e 9999, inclusive ambos, nos quais aparecem pelo menos dois algarismos consecutivos iguais?

**Exercício 11.45:** Sejam  $n$  e  $m$  dois números naturais quaisquer. Quantas sequências de  $n$  números naturais, todos menores que  $m$ , possuem pelo menos dois elementos iguais?

## 11.13 Princípio da inclusão e exclusão

Outra técnica importante de contagem baseia-se na seguinte identidade, que vale para quaisquer conjuntos finitos  $A$  e  $B$ :

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (11.18)$$

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

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \quad (11.19)$$

As fórmulas (11.18) e (11.19) podem ser generalizadas para  $n$  conjuntos finitos  $A_1, A_2, \dots, A_n$ :

$$\begin{aligned}
 |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{i=1}^n |A_i| \\
 &- \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
 &+ \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\
 &\dots \\
 &+ (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|
 \end{aligned} \tag{11.20}$$

Para simplificar esta fórmula, vamos denotar por  $\mathcal{C}_n^r$  o conjunto de todas as combinações de  $r$  elementos do conjunto  $\{1, 2, \dots, n\}$ . Podemos escrever então

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{r=1}^n (-1)^{r-1} \left( \sum_{X \in \mathcal{C}_n^r} \left| \bigcap_{k \in X} A_k \right| \right) \tag{11.21}$$

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 11.46:** Quantos números entre 1 e 1.000.000 são divisíveis por 5, por 7, ou por 11?

**Exercício 11.47:** Quantos números entre 1 e 1.000.000 são quadrados perfeitos, cubos perfeitos, ou são divisíveis por 5?

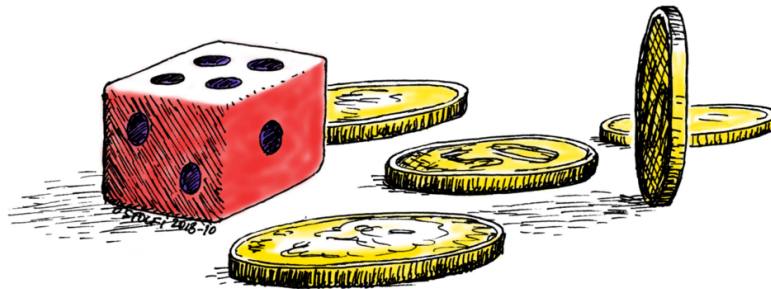
**Exercício 11.48:** Na notação decimal, quantos números entre 100000 e 999999 começam com algarismo par, terminam com algarismo maior que 5 ou possuem todos os algarismos iguais?

**Exercício 11.49:** Demonstre a fórmula (11.21), por indução em  $n$ .



# Capítulo 12

## 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. Todas as fontes de informação que temos — notícias, contagens, medidas, evidências, e nossos próprios sentidos e mente — podem ser errôneas ou enganosas; de modo que toda proposição que acreditamos verdadeira pode ser falsa, e vice-versa. Como podemos então usar a lógica, ou tomar qualquer decisão, nessas condições?

Por outro lado, 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 amanhã”, é prudente pensar na possibilidade de que chova.

Para certas afirmações, nossa confiança pode vir do histórico de situações semelhantes que já presenciávamos. Podemos tratar como certa a proposição “uma pedra solta no ar cai para baixo” com base em incontáveis experiências que tivemos ao longo da vida. As leis da física, em particular, são “certezas” adquiridas por meio de experimentos cuidadosos e exaustivamente analisados. Mesmo assim sempre é possível que, em situações especiais que nunca encontramos antes, essas afirmações “certamente verdadeiras” venham a ser falsas.

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.

## 12.1 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  $\text{Pr}(P)$ . 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  $25/100 = 0,25$ .

### 12.1.1 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.

### 12.1.2 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,  $P \rightarrow \neg Q$  e  $Q \rightarrow \neg P$ ), 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.

Essa regra pode ser generalizada para três ou mais proposições  $P_1, P_2, \dots, P_n$ . Essas proposições são *mutuamente exclusivas* se sabemos que  $P_i \rightarrow \neg P_j$ , para quaisquer  $i$  e  $j$  entre 1 e  $n$  com  $i \neq j$ . Nesse caso, o princípio da exclusão mútua exige que  $\Pr(P_1) + \Pr(P_2) + \dots + \Pr(P_n) \leq 1$ .

### 12.1.3 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  $P_1 \vee P_2 \vee \dots \vee P_n$  é verdadeiro, então devemos ter  $\Pr(P_1) + \Pr(P_2) + \dots + \Pr(P_n) \geq 1$ .

### 12.1.4 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

$$\Pr(P) + \Pr(\neg P) = 1 \quad (12.1)$$

ou seja

$$\Pr(\neg P) = 1 - \Pr(P) \quad (12.2)$$

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  $P_1, P_2, \dots, P_n$  é verdadeira. Isto é, sabemos que elas são mutuamente exclusivas, mas também que uma delas tem que ser verdadeira. Então devemos ter

$$\Pr(P_1) + \Pr(P_2) + \dots + \Pr(P_n) = 1 \quad (12.3)$$

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.

### 12.1.5 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

$$\Pr(P \vee Q) = \Pr(P) + \Pr(Q) - \Pr(P \wedge Q) \quad (12.4)$$

Compare este princípio com a fórmula para cardinalidade de conjuntos

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (12.5)$$

**Exercício 12.1:** 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?

### 12.1.6 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

$$\begin{array}{ll}
 D(1) \wedge M(\text{cara}) & D(1) \wedge M(\text{coroa}) \\
 D(2) \wedge M(\text{cara}) & D(2) \wedge M(\text{coroa}) \\
 D(3) \wedge M(\text{cara}) & D(3) \wedge M(\text{coroa}) \\
 D(4) \wedge M(\text{cara}) & D(4) \wedge M(\text{coroa}) \\
 D(5) \wedge M(\text{cara}) & D(5) \wedge M(\text{coroa}) \\
 D(6) \wedge M(\text{cara}) & D(6) \wedge M(\text{coroa})
 \end{array} \tag{12.6}$$

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

$$\Pr(P \wedge Q) = \Pr(P) \Pr(Q) \quad (12.7)$$

O princípio da independência diz que, se não sabemos de nenhuma ligação ou influência entre o valor lógico de uma afirmação  $P$  e o de outra afirmação  $Q$ , então é razoável supor que elas são independentes; ou seja, é razoável atribuir à conjunção  $P \wedge Q$  o produto das respectivas probabilidades.

**Exercício 12.2:** 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?

**Exercício 12.3:** Se as afirmações  $P$  e  $Q$  são independentes, quanto vale  $\Pr(P \vee Q)$  em função de  $\Pr(P)$  e  $\Pr(Q)$ ?

**Exercício 12.4:** Contagens em uma fábrica mostraram que 20% dos parafusos tem um defeito na rosca, 30% tem um defeito na cabeça. Supondo que os defeitos afetam as duas partes do parafuso de maneira independente, qual é a probabilidade de que um desses parafusos, escolhido ao acaso, tenha algum defeito?

**Exercício 12.5:** Uma empreiteira construiu um condomínio de casas, e percebeu que a lâmpada da sala não estava acendendo em algumas delas. Então ela mandou dois empregados,  $A$  e  $B$ , visitarem todas as casas, em dias diferentes, para verificar quais casas tinham esse defeito. O empregado  $A$  relatou que a lâmpada não acendia em 30 das casas, enquanto que  $B$  notou esse mesmo defeito em 20 das casas. Apenas 15 casas estavam nas duas listas. Evidentemente, os dois empregados não foram muito cuidadosos. Sejam  $p_A$  e  $p_B$  as probabilidades de  $A$  e  $B$ , respectivamente, terem percebido o defeito numa casa em que ele existia. Estime  $p_A$ ,  $p_B$ , e o número  $N$  de casas onde o defeito realmente ocorria. Suponha que os empregados não cometeram erros no sentido oposto, isto é, não anotaram como defeituosa nenhuma casa onde a lâmpada acendia.

### 12.1.7 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  $P \rightarrow Q$  equivale a afirmar que  $\Pr(Q \mid P) = 1$ .

## 12.2 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 12.1:** 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  $D = \{1, 2, \dots, 6\}$ . 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  $\Pr(X = 0) = \Pr(X = 7) = \Pr(X = 1/2) = 0$ .

Variáveis aleatórias com valores numéricos podem ser combinadas com operações aritméticas e funções matemáticas, resultando em outras variáveis aleatórias. Por exemplo, se  $\alpha$  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 12.6:** 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  $Y$ :

- (a)  $X^2$
- (b)  $X \bmod 3$
- (c)  $X + Y$
- (d)  $\min \{X, Y\}$

Neste livro 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.

### 12.2.1 Variáveis aleatórias independentes

A *distribuição conjunta* de duas variáveis aleatórias  $X$  e  $Y$  com domínios  $A$  e  $B$  é a função de dois argumentos  $u, v$  que a cada elemento de  $A \times B$  associa a probabilidade  $\Pr(X = u \wedge Y = v)$ . Mais geralmente, a *distribuição conjunta* de  $n$  variáveis  $X_1, X_2, \dots, X_n$  com domínios  $D_1, D_2, \dots, D_n$  é a função que a cada tupla  $(v_1, v_2, \dots, v_n)$  associa a probabilidade  $\Pr(X_1 = v_1 \wedge X_2 = v_2 \wedge \dots \wedge X_n = v_n)$ .

Por exemplo, suponha que as variáveis aleatórias  $M_1$ ,  $M_2$ , e  $M_3$  são o resultado de jogar uma moeda três vezes, contando cara como 0 e coroa como 1. Seja  $X = M_1 + M_2$  a soma dos dois primeiros resultados, e  $Y = M_2 + M_3$  a soma dos dois últimos. Temos 8 possíveis tuplas de valores  $(v_1, v_2, v_3)$  para as variáveis  $(M_1, M_2, M_3)$ , todas igualmente prováveis. As variáveis  $X$  e  $Y$  tem o mesmo domínio  $\{0, 1, 2\}$ , e a mesma distribuição de probabilidade,  $\{(0, 1/4), (1, 1/2), (2, 1/4)\}$ . Sua distribuição conjunta é dada pela tabela

|   |   | Y   |     |     |
|---|---|-----|-----|-----|
|   |   | 0   | 1   | 2   |
| X | 0 | 1/8 | 1/8 | 0   |
|   | 1 | 1/8 | 2/8 | 1/8 |
|   | 2 | 0/8 | 1/8 | 1/8 |

Dizemos que duas variáveis aleatórias  $X$  e  $Y$  são *independentes* se e somente se, para quaisquer valores  $u$  e  $v$  em seus respectivos domínios,

$$\Pr(X = u \wedge Y = v) = \Pr(X = u) \Pr(Y = v) \quad (12.8)$$

Ou seja, se sua distribuição conjunta é simplesmente o produto de suas distribuições individuais. 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 quando sabemos que há 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 12.7:** 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.
- (b) Sejam  $S'$  e  $D'$  os restos da divisão de  $S$  e  $D$  por 6, ambos inteiros entre 0 e 5 inclusive. As variáveis  $S'$  e  $D'$  são independentes? Justifique.

## 12.3 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 R\$ 30 contra R\$ 10 que o resultado será cara. Temos igual chance de ganhar R\$ 10 (se sair cara) e perder R\$ 30 (se sair coroa). Ou

seja,

$$\Pr(\text{“nosso ganho será R\$ +10”}) = \Pr(\text{“nosso ganho será R\$ -30”}) = \frac{1}{2}$$

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

$$\frac{\frac{n}{2}(\text{R\$ +10}) + \frac{n}{2}(\text{R\$ -30})}{n} = \text{R\$ -10} \quad (12.9)$$

Para entender melhor este exemplo, suponha que repetimos duas vezes essa aposta. Temos quatro possibilidades: perder nas duas vezes, só na primeira, só na segunda, ou ganhar nas duas. Nosso ganho médio por aposta será respectivamente,  $((-30) + (-30))/2 = -30$ ,  $((-30) + (+10))/2 = -10$ ,  $((+10) + (-30))/2 = -10$ , e  $((+10) + (+10))/2 = +10$ . Supondo que o resultado de cada lance seja independente dos anteriores, e denotando por  $G(x)$  o predicado “nosso ganho médio por aposta será  $x$ ”, teremos então

$$\begin{aligned} \Pr(G(-30)) &= 1/4 \\ \Pr(G(-10)) &= 1/4 + 1/4 = 1/2 \\ \Pr(G(+10)) &= 1/4 \end{aligned} \quad (12.10)$$

Ou seja, o ganho médio R\\$ - 10 é duas vezes mais provável que R\\$ -30 ou R\\$ +10. Para quatro apostas seguidas, podemos ter 0, 1, 2, 3, ou 4 acertos, com ganhos médios por aposta de -30, -20,

−10, 0 e +10, respectivamente. As probabilidades são

$$\begin{aligned}
 \Pr(G(-30)) &= \binom{4}{0}/2^4 = 1/16 \\
 \Pr(G(-20)) &= \binom{4}{1}/2^4 = 4/16 \\
 \Pr(G(-10)) &= \binom{4}{2}/2^4 = 6/16 \\
 \Pr(G(0)) &= \binom{4}{3}/2^4 = 4/16 \\
 \Pr(G(+10)) &= \binom{4}{4}/2^4 = 1/16
 \end{aligned} \tag{12.11}$$

Como se pode ver, é muito mais provável que o ganho médio por aposta seja R\$ −10 do que qualquer outro valor. A medida que o número de apostas aumenta, essa tendência permanece: o valor mais provável para o ganho médio por aposta será R\$ −10.

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

$$\mathcal{E}(X) = \sum_{v \in D} v \Pr(X = v) \tag{12.12}$$

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 (12.12) reduz-se à média aritmética dos elementos de  $D$ .

**Exercício 12.8:** 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?

Quando o domínio da variável é um conjunto infinito, o valor esperado pode ser infinito, mesmo que todos os seus valores possíveis sejam finitos. Por exemplo, considere a variável  $X$  cujo valor é um inteiro positivo, tal que  $\Pr(X = k) = (6/\pi^2)/k^2$  para todo  $k \in \mathbb{N} \setminus \{0\}$ . Esta distribuição de probabilidades é válida, pois verifica-se que a soma de todas as probabilidades é 1. Entretanto, o valor esperado de  $X$  deveria ser a somatória

$$\mathcal{E}(X) = \sum_{k=1}^{\infty} k \cdot \frac{A}{k^2} = A \sum_{k=1}^{\infty} \frac{1}{k}$$

que, como sabemos, não tem valor finito (veja seção 9.6).

O valor esperado pode ser definido para qualquer variável cujos valores podem ser somados e multiplicados por um número real. Por exemplo, suponha que o valor de uma variável aleatória  $X$  é um par  $(u, v)$ , onde  $u$  é o resultado de lançar uma moeda (0 = cara, 1 = coroa), e  $v$  é o resultado de lançar um dado (um inteiro entre 1 e 6); sendo que cada par possível tem a mesma probabilidade  $1/12$ . Note que esses pares podem ser considerados vetores do espaço  $\mathbb{R}^2$ . Portanto

podemos calcular o valor esperado de  $X$

$$\mathcal{E}(X) = \frac{1}{12} ((0, 1) + (0, 2) + \cdots + (1, 5) + (1, 6)) = \left(\frac{1}{6}, \frac{7}{2}\right)$$

### 12.3.1 Propriedades do valor esperado

Seja  $X$  uma variável aleatória com domínio numérico, sejam  $\alpha$  e  $\beta$  dois números reais quaisquer, e seja  $Z$  a variável aleatória  $\alpha X + \beta$ . Nesse caso, pode-se provar que

$$\mathcal{E}(Z) = \mathcal{E}(\alpha X + \beta) = \alpha \mathcal{E}(X) + \beta \quad (12.13)$$

Porém, se uma variável aleatória  $Z$  depende de  $X$  de maneira não linear (por exemplo, se  $Z$  é o quadrado de  $X$ ), não existe uma fórmula geral que relacione  $\mathcal{E}(Z)$  a  $\mathcal{E}(X)$  (Veja o exercício 12.10.)

Sejam  $X$  e  $Y$  duas variáveis aleatórias com valores numéricos, e seja  $Z$  a variável aleatória, denotada por  $X + Y$ , cujo valor é a soma dos valores de  $X$  e de  $Y$ . Verifica-se que

$$\mathcal{E}(Z) = \mathcal{E}(X) + \mathcal{E}(Y) \quad (12.14)$$

Estas fórmulas valem mesmo que as variáveis  $X$  e  $Y$  tenham alguma dependência entre si. Note que não há fórmulas análogas para outras operações (como produto, divisão, etc.).

**Exercício 12.9:** Um dado vai ser lançado, e a seguinte aposta é oferecida: o cliente paga R\$7,00 ao banqueiro, e recebe em reais o dobro do valor que sair no dado. Por exemplo, se sair um 4, o cliente recebe R\$8,00, obtendo um ganho líquido de R\$1,00. Qual é o ganho esperado do cliente?

**Exercício 12.10:** Na mesma situação do exercício 12.9, uma outra aposta é oferecida: cliente paga R\$49,00 ao banqueiro, e recebe em reais o dobro do quadrado do valor que sair no dado. Por exemplo, se sair um 6, o cliente recebe  $2 \times 6^2 = \text{R\$}72,00$ , obtendo um ganho líquido de R\$23,00. Qual é o ganho esperado do cliente?

## 12.4 Mediana

O valor esperado de uma variável aleatória  $X$  pode em muitos casos ser considerado o “valor típico” de  $X$ . Por exemplo, se  $X$  é a altura (em metros) de uma pessoa que não vimos ainda, o valor esperado de  $X$  para a população brasileira é próximo a 1,70 m. Podemos então imaginar o “brasileiro típico” como tendo essa altura.

Porém este raciocínio nem sempre é apropriado. Por exemplo, suponha uma vila com 99 casas térreas e um prédio de 101 andares, e considere a variável aleatória  $X$  que é o número de andares de um edifício arbitrário dessa vila, escolhido com probabilidade uniforme. O valor esperado da variável  $X$  será 2, mas obviamente não é correto dizer que o “edifício típico” dessa vila tem dois andares.

Devido a exemplos como esse, foram propostas outras maneiras de obter o “valor típico” de uma variável aleatória. O mais comum é a *mediana*. Idealmente, este é um valor  $v$  tal que  $\Pr(X \leq v) \geq 1/2$  e  $\Pr(X \geq v) \geq 1/2$ .

Por exemplo, suponha que a variável aleatória  $X$  pode ter qualquer valor inteiro entre 1 e 6, com

as seguintes probabilidades

|              |                |                |                |                |                |                |
|--------------|----------------|----------------|----------------|----------------|----------------|----------------|
| $k$          | 1              | 2              | 3              | 4              | 5              | 6              |
| $\Pr(X = k)$ | $\frac{6}{20}$ | $\frac{2}{20}$ | $\frac{1}{20}$ | $\frac{3}{20}$ | $\frac{7}{20}$ | $\frac{1}{20}$ |

Neste caso podemos tomar a mediana de  $X$  como sendo 4, pois

$$\begin{aligned}\Pr(X \leq 4) &= \frac{6}{20} + \frac{2}{20} + \frac{1}{20} + \frac{3}{20} = \frac{12}{20} \geq \frac{1}{2} \\ \Pr(X \geq 4) &= \frac{3}{20} + \frac{7}{20} + \frac{1}{20} = \frac{11}{20} \geq \frac{1}{2}\end{aligned}$$

Note que o valor esperado de  $X$  é

$$1 \cdot \frac{6}{20} + 2 \cdot \frac{2}{20} + 3 \cdot \frac{1}{20} + 4 \cdot \frac{3}{20} + 5 \cdot \frac{7}{20} + 6 \cdot \frac{1}{20} = \frac{66}{20} = 3,3$$

Note porém que pode haver diversos valores  $v$  que satisfazem a condição  $\Pr(X \leq v) = \Pr(X \geq v)$ . Por exemplo, se a distribuição de probabilidades de  $X$  for

|              |                |                |                |                |                |                |
|--------------|----------------|----------------|----------------|----------------|----------------|----------------|
| $k$          | 1              | 2              | 3              | 4              | 5              | 6              |
| $\Pr(X = k)$ | $\frac{6}{20}$ | $\frac{2}{20}$ | $\frac{2}{20}$ | $\frac{1}{20}$ | $\frac{8}{20}$ | $\frac{1}{20}$ |

então, para qualquer valor  $v$  tal que  $3 < v < 4$ , teremos  $\Pr(X \leq v) = (6 + 2 + 2)/20 = 1/2$  e  $\Pr(X \geq v) = (1 + 8 + 1)/20 = 1/2$ .

Quando isso acontece, pode-se provar que os valores de  $v$  que satisfazem a definição formam um intervalo finito dos números reais. Nesses casos, alguns autores definem a mediana como sendo o ponto médio desse intervalo; no exemplo acima, seria  $v = (3 + 4)/2 = 3,5$ .

**Exercício 12.11:** Seja  $X$  o quadrado de um número entre 1 e 6 que será obtido pelo lançamento de um dado. Note que o valor de  $X$  pode ser 1, 4, 9, 16, 25, ou 36. Qual é o valor esperado da variável  $X$ ? E sua mediana?

**Exercício 12.12:** Seja  $X$  o *produto* dos dois números entre 1 e 6 que serão obtidos pelo lançamento de dois dados. Qual é a distribuição de probabilidades da variável  $X$ ? Qual é seu valor esperado? E sua mediana?

**Exercício 12.13:** Prove que qualquer variável aleatória com valores inteiros tem uma mediana.

## 12.5 Moda

Outra maneira de definir o “valor típico” de uma variável aleatória é tomar o *valor mais provável*, também chamado de *moda* da variável. Por exemplo, se a distribuição for

| $k$          | 1              | 2              | 3              | 4              | 5              | 6              |
|--------------|----------------|----------------|----------------|----------------|----------------|----------------|
| $\Pr(X = k)$ | $\frac{6}{20}$ | $\frac{2}{20}$ | $\frac{1}{20}$ | $\frac{3}{20}$ | $\frac{7}{20}$ | $\frac{1}{20}$ |

diremos que a moda de  $X$  é 5. Por outro lado, se as probabilidades forem um pouco diferentes

| $k$          | 1              | 2              | 3              | 4              | 5              | 6              |
|--------------|----------------|----------------|----------------|----------------|----------------|----------------|
| $\Pr(X = k)$ | $\frac{7}{20}$ | $\frac{2}{20}$ | $\frac{1}{20}$ | $\frac{3}{20}$ | $\frac{6}{20}$ | $\frac{1}{20}$ |

A moda será 1.

## 12.6 Variância e desvio padrão

Em muitas situações, não basta saber o valor esperado  $\mathcal{E}(X)$  de uma variável aleatória; é preciso também saber até que ponto o valor da variável pode diferir desse valor esperado.

Considere por exemplo as variáveis aleatórias  $X$  e  $Y$ , que podem assumir valores entre 1 e 5 com as seguintes probabilidades:

| $k$          | 1              | 2              | 3              | 4              | 5              |
|--------------|----------------|----------------|----------------|----------------|----------------|
| $\Pr(X = k)$ | $\frac{1}{20}$ | $\frac{7}{20}$ | $\frac{4}{20}$ | $\frac{7}{20}$ | $\frac{1}{20}$ |
| $\Pr(Y = k)$ | $\frac{7}{20}$ | $\frac{2}{20}$ | $\frac{2}{20}$ | $\frac{2}{20}$ | $\frac{7}{20}$ |

As duas variáveis tem o mesmo valor esperado  $v = 3$ , mas intuitivamente podemos ver que  $Y$  varia mais do que  $X$ . Como podemos transformar essa intuição em números?

A maneira mais comum é calcular a *variância*  $\mathcal{V}(X)$  da variável, definida pela fórmula

$$\mathcal{V}(X) = \sum_{v \in D} (v - \mathcal{E}(X))^2 \Pr(X = v) \quad (12.15)$$

Pode-se verificar que este é o valor esperado da variável  $Y = (X - \mathcal{E}(X))^2$ .

No exemplo acima, temos

$$\begin{aligned} \mathcal{V}(X) &= (1 - 3)^2 \cdot \frac{1}{20} + (2 - 3)^2 \cdot \frac{7}{20} + (3 - 3)^2 \cdot \frac{4}{20} + (4 - 3)^2 \cdot \frac{7}{20} + (5 - 3)^2 \cdot \frac{1}{20} = \frac{26}{20} = 1,3 \\ \mathcal{V}(Y) &= (1 - 3)^2 \cdot \frac{7}{20} + (2 - 3)^2 \cdot \frac{2}{20} + (3 - 3)^2 \cdot \frac{2}{20} + (4 - 3)^2 \cdot \frac{2}{20} + (5 - 3)^2 \cdot \frac{7}{20} = \frac{60}{20} = 3,0 \end{aligned}$$

evidenciando assim que os valores de  $Y$  tendem a estar mais longe de sua média do que os valores de  $X$ .

Observe que as parcelas  $(v - \mathcal{E}(X))^2$  da somatória (12.15) nunca são negativas, portanto a variância também não pode ser negativa. Além disso, a variância só pode ser zero se todas as parcelas forem zero, ou seja se a variável  $X$  só pode ter um valor — que é portanto seu valor esperado  $\mathcal{E}(X)$ . Se ela pode assumir dois ou mais valores distintos, com probabilidades diferentes de zero, então a variância será estritamente positiva.

Observe que, se o domínio  $D$  da variável  $X$  é um conjunto infinito, a variância pode ser infinita (mesmo que o valor esperado exista e seja finito). Por exemplo, seja  $D = \mathbb{Z} \setminus \{0\}$ , e  $\Pr(X = v) = B/|v|^3$ , onde  $B$  é uma constante tal que a soma das probabilidades seja 1. O valor esperado existe ( $\mathcal{E}(X) = 0$ ). Porém, temos

$$\mathcal{V}(X) = \sum_{v \in D} (v - \mathcal{E}(X))^2 \Pr(X = v) = 2 \sum_{k=1}^{+\infty} \frac{B}{v^3} v^1 = 2B \sum_{k=1}^{+\infty} \frac{1}{v}$$

que, como sabemos, é infinita.

### 12.6.1 Propriedades da variância

Seja  $X$  uma variável aleatória com valores numéricos. Sejam  $\alpha$  e  $\beta$  dois valores reais arbitrários. Verifica-se então que

$$\mathcal{V}(\alpha X + \beta) = \alpha^2 \mathcal{V}(X) \quad (12.16)$$

Note que somar uma constante  $\beta$  a uma variável não altera sua variância.

Se  $X$  e  $Y$  são duas variáveis aleatórias *independentes*, verifica-se que

$$\mathcal{V}(X + Y) = \mathcal{V}(X) + \mathcal{V}(Y) \quad (12.17)$$

Esta fórmula não vale se soubermos de alguma dependência entre as variáveis  $X$  e  $Y$  (isto é, se atribuirmos a alguma afirmação do tipo “ $(x = u) \wedge (Y = v)$ ” uma probabilidade diferente de  $\Pr(X = u) \Pr(Y = v)$ ). Nesse caso, a variância de  $X + Y$  pode ser maior ou menor que  $\mathcal{V}(X) + \mathcal{V}(Y)$ .

### 12.6.2 Desvio padrão

Pode-se dizer que, quanto maior a variância, mais “espalhada” é a distribuição de probabilidade da variável. Entretanto, não é fácil interpretar o valor numérico da variância. Por exemplo, se o valor de  $X$  é uma medida em metros, a variância é medida em metros quadrados. Uma medida de “espalhamento” que é mais fácil de interpretar é o *desvio padrão*, definido como a raiz quadrada da variância:

$$\mathcal{D}(X) = \sqrt{\mathcal{V}(X)} = \sqrt{\sum_{v \in D} (v - \mathcal{E}(X))^2 \Pr(X = v)}$$

O desvio padrão é medido com as mesmas unidades da variável. Informalmente, pode ser interpretado como o valor “típico” da diferença entre o valor da variável e seu valor esperado.

**Exemplo 12.2:** Suponha um lote de parafusos que deveriam ser todos iguais, e Seja  $X$  o comprimento real de um desses parafusos, escolhido ao acaso. Se dissermos que o valor esperado de  $X$  é 150 mm e o desvio padrão é 1 mm, estamos dizendo que o comprimento do parafuso dificilmente será muito maior que 151 mm ou muito menor que 149 mm.

Esta interpretação informal do desvio padrão tem por base o seguinte resultado, devido ao matemático russo Pafnuti Chebyshev ou Tchebychev (1821–1894):

**Teorema 12.1:** Para qualquer variável aleatória  $X$  e qualquer número real  $\alpha \geq 1$ ,

$$\Pr(|X - \mathcal{E}(X)| \geq \alpha \mathcal{D}(X)) \leq \frac{1}{\alpha^2} \quad (12.18)$$

A demonstração deste resultado foge do escopo deste livro. Em outras palavras, se  $\mathcal{E}(X) = \mu$  e  $\mathcal{D}(X) = \sigma$ , então o valor de  $X$  estará dentro do intervalo  $[\mu - \alpha\sigma, \mu + \alpha\sigma]$  com probabilidade  $1 - 1/\alpha^2$ . Para a variável  $X$  do exemplo 12.2, o teorema de Tchebychev diz que o comprimento do parafuso (em milímetros) está:

- no intervalo  $[150 - 2 \cdot 1, 150 + 2 \cdot 1] = [148, 152]$  com probabilidade maior ou igual a  $1 - 1/2^2 = 75\%$ ;
- no intervalo  $[150 - 3 \cdot 1, 150 + 3 \cdot 1] = [147, 153]$  com probabilidade maior ou igual a  $1 - 1/3^2 \approx 88\%$ ;
- no intervalo  $[150 - 4 \cdot 1, 150 + 4 \cdot 1] = [146, 154]$  com probabilidade maior ou igual a  $1 - 1/4^2 \approx 93\%$ ;

e assim por diante.

Observe que o resultado de Tchebychev vale qualquer que seja a distribuição de probabilidade da variável  $X$ .

**Exercício 12.14:** Seja  $X$  uma variável aleatória que pode assumir qualquer valor entre 0 e 100, com igual probabilidade. Calcule o valor esperado, a variância e o desvio padrão de  $X$ . Calcule a probabilidade de  $X$  estar entre 40 e 60 (inclusive ambos). Compare esse resultado com a probabilidade obtida pelo teorema de Tchebychev.

### 12.6.3 Covariância

Se  $X$  e  $Y$  são variáveis aleatórias numéricas, a *covariância* entre as duas é definida pela fórmula

$$\mathcal{C}(X, Y) = \sum_{u,v} \Pr((X = u) \wedge (Y = v))(u - \mathcal{E}(X))(v - \mathcal{E}(Y))$$

A covariância é uma medida da dependência entre  $X$  e  $Y$ . A grosso modo, ela tende a ser positiva quando é muito provável que os valores de  $X$  e  $Y$  sejam ambos maiores ou ambos menores que suas médias (caso em que o produto  $(u - \mathcal{E}(X))(v - \mathcal{E}(Y))$  é positivo). Ela tende a ser negativa quando  $X$  e  $Y$  tendem a variar em direções opostas em relação a suas médias — quando um está acima da média, o outro provavelmente está abaixo. Observe que  $\mathcal{V}(X)$  é a mesma coisa que  $\mathcal{C}(X, X)$ .

É fácil provar que, se  $X$  e  $Y$  são independentes, então sua covariância é zero. Prova-se também que, para quaisquer variáveis aleatórias numéricas  $X$  e  $Y$ ,

$$\mathcal{V}(X + Y) = \mathcal{V}(X) + \mathcal{V}(Y) + 2 \mathcal{C}(X, Y)$$

Note que esta fórmula implica na fórmula (12.17) quando  $X$  e  $Y$  são independentes.

**Exercício 12.15:** Encontre duas variáveis aleatórias  $X$  e  $Y$  que possuem covariância nula mas *não* são independentes.

### 12.6.4 Coeficiente de correlação

O sinal de  $\mathcal{C}(X, Y)$  revela o sentido geral da dependência entre  $X$  e  $Y$ , mas seu valor numérico é difícil de interpretar. Por essa razão é interessante definir o *coeficiente de correlação*

$$\kappa(X, Y) = \frac{\mathcal{C}(X, Y)}{\sqrt{\mathcal{V}(X)\mathcal{V}(Y)}} = \frac{\mathcal{C}(X, Y)}{\mathcal{D}(X)\mathcal{D}(Y)}$$

Prova-se que este número está sempre entre  $-1$  e  $+1$ . Ele é zero se  $X$  e  $Y$  são independentes,  $+1$  se cada variável é função linear crescente da outra (isto é, se  $Y = \alpha X + \beta$  com  $\alpha > 0$ ) e  $-1$  se cada variável é função linear decrescente da outra ( $Y = \alpha X + \beta$  com  $\alpha < 0$ ). Um valor intermediário, por exemplo  $0,50$ , significa que o valor de cada variável é parcialmente função da outra, mas inclui um termo que não depende dela. Neste caso diz-se que *há correlação entre  $X$  e  $Y$  (positiva ou negativa, conforme o sinal do coeficiente)*.

## 12.7 Probabilidade condicional

Seja  $X$  a variável aleatória cujo valor é o resultado do lançamento de um dado, e considere as duas afirmações “ $X$  é par” e “ $X$  é ímpar”. Se não temos nenhuma outra informação sobre  $X$ , como vimos, é razoável atribuir a probabilidade  $1/6$  a cada um dos possíveis valores  $1, 2, \dots, 6$ , e portanto

$$\begin{aligned}\Pr(X \text{ é par}) &= \Pr(X = 2) + \Pr(X = 4) + \Pr(X = 6) = 1/2 \\ \Pr(X \text{ é ímpar}) &= \Pr(X = 1) + \Pr(X = 3) + \Pr(X = 5) = 1/2\end{aligned}$$

Suponha agora que sabemos que o valor de  $X$  não é 3. Que probabilidade devemos atribuir a essas duas afirmações? Não podemos simplesmente eliminar o termo  $\Pr(X = 3)$  na segunda fórmula, pois a soma não seria 1. Como a probabilidade do valor ser 3 é zero, temos que corrigir a probabilidade dos demais valores para que elas tenham soma 1. Ou seja, temos que supor  $\Pr(X = 3) = 0$  e  $\Pr(X = v) = 1/5$  para os demais valores. Então teremos

$$\begin{aligned}\Pr(X \text{ é par}) &= \Pr(X = 2) + \Pr(X = 4) + \Pr(X = 6) = 3/5 \\ \Pr(X \text{ é ímpar}) &= \Pr(X = 1) + \Pr(X = 5) = 2/5\end{aligned}$$

Observe que a informação adicional “ $X \neq 3$ ” afetou não apenas a probabilidade de  $X$  ser ímpar, mas também a probabilidade de ele ser par.

Em casos como este, costuma-se usar a notação  $\Pr(P \mid Q)$  para denotar a *probabilidade condicional* da afirmação  $P$ , *sabendo-se que* (ou *dado que*) a afirmação  $Q$  é verdadeira. Verifica-se que essa probabilidade pode ser calculada pela fórmula

$$\Pr(P \mid Q) = \frac{\Pr(P \wedge Q)}{\Pr(Q)} \quad (12.19)$$

Aplicando esta fórmula ao exemplo acima, a afirmação  $P$  seria “ $X$  é ímpar” e  $Q$  a afirmação “ $X \neq 3$ ”. Temos então que

$$\begin{aligned}\Pr(P \wedge Q) &= \Pr(X = 1) + \Pr(X = 5) &= 2/6 \\ \Pr(Q) &= \Pr(X = 1) + \Pr(X = 2) + \Pr(X = 4) + \Pr(X = 5) + \Pr(X = 6) &= 5/6 \\ \Pr(P \mid Q) &= \frac{2/6}{5/6} &= 2/5\end{aligned}$$

**Exercício 12.16:** Seja  $X$  o valor obtido lançando um dado. Calcule, pela fórmula (12.19)

- (a)  $\Pr(X \text{ é par} \mid X \neq 3)$
- (b)  $\Pr(X \text{ é par} \mid X \text{ é quadrado perfeito})$
- (c)  $\Pr(X \text{ é primo} \mid X \text{ é maior que } 2)$

**Exercício 12.17:** Seja  $X$  a soma dos valores obtidos no lançamento de dois dados. Calcule, pela fórmula (12.19)

- (a)  $\Pr(X \text{ é par} \mid \text{os dois dados deram o mesmo resultado})$
- (b)  $\Pr(X \text{ é par} \mid \text{os dois dados deram resultados diferentes})$
- (c)  $\Pr(X = 6 \mid \text{os dois valores não são primos entre si})$

A fórmula da probabilidade condicional é também muito usada na forma inversa:

$$\Pr(P \wedge Q) = \Pr(P \mid Q) \Pr(Q) \quad (12.20)$$

Ou seja, uma vez definida a probabilidade de  $P$  dado  $Q$ , e também a probabilidade de  $Q$ , a probabilidade da afirmação “ $P$  e  $Q$ ” é simplesmente o produto das duas.

**Exercício 12.18:** Suponha que a probabilidade de algum hacker tentar violar seu computador no próximo minuto é 10%, e que a probabilidade de tal tentativa ter sucesso é 80%. Qual é a probabilidade de seu computador ser violado por algum hacker no próximo minuto? (Ignore a possibilidade de haver mais de um ataque por minuto.)

**Exercício 12.19:** Suponha que atiramos dois dados, um verde e um vermelho. Qual a probabilidade de que o dado verde mostre o valor 2, e o dado vermelho mostre o valor 3? E qual é a probabilidade de que um deles mostre o valor 2, e o outro 3? Agora suponha que os dois dados são idênticos, a tal ponto que não podemos dizer qual é um e qual é o outro. Qual é a probabilidade de que um deles mostre 2, e o outro 3?

## 12.8 Inferência bayesiana

Combinando as fórmulas (12.19) e (12.20), obtemos a equação

$$\Pr(P \mid Q) = \frac{\Pr(Q \mid P) \Pr(P)}{\Pr(Q)} \quad (12.21)$$

Esta fórmula é conhecida como *regra de Bayes* ou *teorema de Bayes*, desenvolvida pelo matemático inglês Thomas Bayes ( $\approx 1702$ – $1761$ ) e, independentemente, pelo matemático francês Pierre-Simon Laplace ( $1749$ – $1827$ ). Ela é geralmente usada quando se quer obter a probabilidade  $\Pr(P \mid Q)$  de uma possível causa  $P$ , sabendo-se que uma consequência  $Q$  ocorreu, a partir da probabilidade condicional inversa  $\Pr(Q \mid P)$  (de que essa consequência produza essa causa). Este raciocínio probabilístico é conhecido como *inferência bayesiana* ou *dedução bayesiana*.

Por exemplo, considere uma coleção de caixas quadradas e redondas, cada uma contendo uma bola que pode ser azul ou branca. Suponha que há igual número de caixas de cada formato, sendo que há bolas azuis em metade das caixas quadradas, mas em apenas 10% das caixas redondas. Imagine

que alguém escolheu uma caixa ao acaso, e encontrou nela uma bola azul. Qual a probabilidade de que ele tenha escolhido uma caixa quadrada? E se a bola for branca?

Se não tivéssemos a informação sobre a bola, seria razoável supor que a caixa era quadrada com probabilidade  $1/2$ . Porém, como bolas brancas são mais comuns nas caixas redondas, intuitivamente, a informação de que a bola era branca aumenta a probabilidade de que a caixa seja redonda.

Para calcular essas probabilidades, vamos denotar por  $Q$ ,  $R$ ,  $A$  e  $B$  as afirmações “a caixa era quadrada”, “a caixa era redonda”, “a bola era azul” e “a bola era branca”, respectivamente. Pelo enunciado do problema, temos

$$\begin{array}{ll} \Pr(Q) &= \frac{1}{2} & \Pr(R) &= \frac{1}{2} \\ \Pr(A | Q) &= \frac{1}{2} & \Pr(B | Q) &= \frac{1}{2} \\ \Pr(A | R) &= \frac{1}{10} & \Pr(B | R) &= \frac{9}{10} \end{array}$$

O que se pede são as probabilidade condicionais  $\Pr(Q | A)$  e  $\Pr(Q | B)$ . Para aplicar a fórmula (12.19), precisamos determinar  $\Pr(B)$  e  $\Pr(Q \wedge B)$ . Para chegar lá, temos que calcular as probabilidades de todas as combinações válidas dessas afirmações. Aplicando a fórmula (12.20) temos

$$\begin{array}{llll} \Pr(Q \wedge A) &= \Pr(A \wedge Q) &= \Pr(A | Q) \Pr(Q) &= \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \\ \Pr(Q \wedge B) &= \Pr(B \wedge Q) &= \Pr(B | Q) \Pr(Q) &= \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \\ \Pr(R \wedge A) &= \Pr(A \wedge R) &= \Pr(A | R) \Pr(R) &= \frac{1}{10} \cdot \frac{1}{2} = \frac{1}{20} \\ \Pr(R \wedge B) &= \Pr(B \wedge R) &= \Pr(B | R) \Pr(R) &= \frac{9}{10} \cdot \frac{1}{2} = \frac{9}{20} \end{array}$$

Daí tiramos

$$\begin{aligned}\Pr(A) &= \Pr(B \wedge Q) + \Pr(B \wedge R) = \frac{1}{4} + \frac{1}{20} = \frac{3}{10} \\ \Pr(B) &= \Pr(A \wedge Q) + \Pr(A \wedge R) = \frac{1}{4} + \frac{9}{20} = \frac{7}{10}\end{aligned}$$

portanto

$$\begin{aligned}\Pr(Q | A) &= \frac{\Pr(Q \wedge A)}{\Pr(A)} = \frac{\Pr(A|Q) \Pr(Q)}{\Pr(A)} = \frac{1/4}{3/10} = \frac{5}{6} \approx 0,833 \\ \Pr(Q | B) &= \frac{\Pr(Q \wedge B)}{\Pr(B)} = \frac{\Pr(B|Q) \Pr(Q)}{\Pr(B)} = \frac{1/4}{7/10} = \frac{5}{14} \approx 0,357\end{aligned}$$

Observe que a informação adicional “a bola sorteada é azul” aumenta a probabilidade de que a caixa escolhida seja quadrada, de 0,5 a 0,833

Generalizando este exemplo, suponha que temos  $m$  afirmações, exaustivas e mutuamente exclusivas,  $A_1, A_2, \dots, A_m$ , chamadas *antecedentes*, cujos valores lógicos podem influir na probabilidade de outras  $n$  afirmações  $B_1, B_2, \dots, B_n$ , chamadas *consequentes*, também exaustivas e mutuamente exclusivas. As afirmações  $A_i$  podem ser as alternativas possíveis para um evento-causa (no exemplo acima, a escolha da caixa, quadrada ou redonda), e as afirmações  $B_j$  as possíveis consequências do mesmo (a cor da bola). Suponha que atribuímos probabilidades  $\Pr(A_i)$  para cada antecedente  $A_i$ , sem levar em conta as afirmações  $B_j$ ; e temos também a probabilidade condicional  $\Pr(B_j | A_i)$  de cada consequente, dado o antecedente. Uma vez sabido que um determinado  $B_j$  é verdadeiro, a probabilidade de cada  $A_i$  passa a ser

$$\Pr(A_i | B_j) = \frac{\Pr(A_i \wedge B_j)}{\Pr(B_j)} = \frac{\Pr(A_i \wedge B_j)}{\sum_{k=1}^m \Pr(B_j \wedge A_k)} = \frac{\Pr(B_j | A_i) \Pr(A_i)}{\sum_{k=1}^m \Pr(B_j | A_k) \Pr(A_k)} \quad (12.22)$$

Note que para aplicar a fórmula (12.22) precisamos atribuir uma probabilidade  $\Pr(A_i)$  a cada antecedente, independente de qual consequente é verdadeiro. O fator  $\Pr(A_i)$  nesta fórmula é chamado

de *probabilidade a priori* do antecedente  $A_i$ , enquanto que o resultado  $\Pr(A_i | B_j)$  é sua *probabilidade a posteriori*.

A influência das probabilidades *a priori*  $\Pr(A_i)$  é uma característica essencial da inferência bayesiana. Elas podem ser vistas como “preconceitos” que temos a respeito das afirmações  $A_i$ , antes de olharmos para as evidências  $B_j$ . A fórmula, portanto, explicita quantitativamente a constatação comum, de que nossos preconceitos sempre afetam nossa interpretação dos fatos.

**Exercício 12.20:** Suponha que há duas gavetas em uma mesa de jogo. Uma delas contém um dado “honesto”, que dá cada valor de 1 a 6 com igual probabilidade  $1/6$ ; a outra contém um dado “viciado”, que dá o valor 6 com probabilidade  $1/2$ , e os valores de 1 a 5 com probabilidade  $1/10$  cada.

- (a) Uma pessoa escolhe (sem você ver) um desses dois dados. Na falta de informações, você atribui a probabilidade *a priori*  $1/2$  de que esse dado seja viciado. O dado é então lançado e o resultado é 6. Como fica a probabilidade de que o dado seja viciado?
- (b) Suponha agora que a pessoa seja um notório vigarista, de modo que, mesmo antes de lançar, você dá 90% de chance de que ele tenha escolhido o dado viciado. Como fica essa probabilidade depois que o dado foi lançado, com resultado 6?
- (c) Finalmente suponha que você confia na pessoa e portanto acredita que ela escolheu o dado honesto, com 90% de probabilidade. Como fica sua confiança nessa hipótese depois que o dado deu 6?

**Exercício 12.21:** Uma moeda é lançada 10 vezes seguidas, e o resultado é sempre cara. Talvez a moeda seja normal, e esse resultado seja coincidência; ou talvez ela seja uma moeda anormal, com cara dos dois lados. Suponha que a probabilidade *a priori* da moeda ser anormal é  $p$ . Qual é a probabilidade *a posteriori*, depois desses 10 lances? Faça um gráfico dessa probabilidade em função de  $p$ .

## 12.9 Teoria da informação

Hoje em dia todos conhecem o conceito de *bit* e outras unidades derivadas, como *byte* (8 bits), *megabyte* ( $10^6$  ou  $2^{20}$  bytes, conforme o contexto), *gigabyte* ( $10^9$  ou  $2^{30}$  bytes) etc. Em geral esses conceitos são usados para descrever tamanhos de arquivos, capacidade de memória, taxas de transmissão, etc. Porém é necessário distinguir entre a *capacidade de armazenamento de informação* de tais sistemas, e a *quantidade de informação* contida neles em determinado momento. Este segundo conceito é o centro da *teoria da informação*, desenvolvida principalmente pelo matemático e engenheiro americano Claude Shannon (1916–2001), em meados do século 20.

### 12.9.1 Capacidade de informação

Considere um sistema físico (real ou imaginário) que em qualquer momento pode assumir um único estado dentre uma coleção finita de estados possíveis; sendo que esse estado pode ser identificado com precisão por algum tipo de teste ou medida. Por exemplo, uma moeda sobre uma mesa,

que pode estar na posição ‘cara’ ou ‘coroa’; um dado de jogar, que pode estar virado com qualquer face, entre 1 e 6, para cima; uma chave elétrica, que pode estar ‘desligada’ ou ‘ligada’; um fio elétrico, que pode estar a zero volts ou a +5 volts; uma barra de ferro, que pode estar magnetizada em dois sentidos diferentes; e assim por diante. Tal objeto é dito um *sistema discreto*.

Suponha que o sistema tem apenas dois estados possíveis (ou seja, é um *sistema binário*). Por definição, a capacidade de informação de tal sistema é 1 bit. Se o sistema tem  $2^b$  estados possíveis, sua capacidade é  $b$  bits. Observe que podemos numerar os estados de tal sistema em base 2 usando  $b$  algarismos, cada qual 0 ou 1: —  $0 \cdots 00 = 0$ ,  $0 \cdots 01 = 1$ ,  $0 \cdots 10 = 2$ ,  $0 \cdots 11 = 3$ , ...,  $1 \cdots 11 = 2^b - 1$ . Daí o nome “bit”, que é abreviação do inglês *binary digit*.

Mais geralmente, se o número de estados possíveis  $n$ , a capacidade de informação é definida como  $\log_2 n = (\ln n)/(\ln 2)$ , o logaritmo de  $n$  na base 2. Assim, por exemplo, a capacidade de informação de um dado de jogar, em repouso sobre a mesa, é  $\log_2 6 = 2,5849625007 \dots$  bits. Note que, se  $n$  não é uma potência de 2, a capacidade em bits não é um número inteiro (e, na verdade, é um número irracional). Note também que se o sistema tem apenas um estado possível, sua capacidade de armazenar informação é (como se pode esperar) zero bits.

Esta definição implica na seguinte propriedade:

**Teorema 12.2:** Se um sistema  $S$  consiste de dois sub-sistemas discretos  $A$  e  $B$  independentes (no sentido de que cada estado possível de  $A$  pode co-existir com qualquer estado possível de  $B$ , e vice-versa), então a capacidade de  $S$  é a soma das capacidades de  $A$  e de  $B$ .

**Exercício 12.22:** Determine a capacidade de informação dos seguintes sistemas:

- (a) Um odômetro (mostrador de quilometragem) de automóvel com 6 algarismos decimais.
- (b) Um dado em forma de octaedro, com faces numeradas de 1 a 8, em repouso sobre a mesa.
- (c) Uma cadeia de DNA com 100 elementos (*nucleotídeos*), cada qual podendo ter quatro estruturas químicas possíveis — adenosina (A), timina (T), guanina (G), ou citosina (C).

**Exercício 12.23:** Determine a capacidade de informação dos seguintes sistemas, constituídos de 4 moedas, cada qual podendo ser de 5, 10, 25, ou 50 centavos, que somente podem ser distinguidas pelo seu valor:

- (a) Uma pilha, em qualquer ordem.
- (b) Uma pilha, em ordem crescente de valor.
- (c) Uma coleção em um saco.
- (d) Uma pilha onde todas as moedas tem o mesmo valor.

**Exercício 12.24:** Refaça o exercício 12.23, supondo que todas as moedas de mesmo valor estão marcadas com letras distintas entre 'A' e 'D'. Assim, por exemplo, na primeira alternativa, as moedas poderiam ser, na ordem, (10, D), (25, C), (10, B), (10, C) mas não poderiam ser (10, D), (25, C), (10, B), (10, D).

**Exercício 12.25:** Qual é a capacidade de informação de uma carta retirada de um baralho com 13 cartas? E de um baralho com 52 cartas? Se acrescentarmos um coringa ao baralho, de quanto aumenta a capacidade, em cada caso?

## 12.9.2 Quantidade de informação

A capacidade de informação de um sistema discreto diz apenas o limite máximo de informação que pode ser armazenada nele. Porém, dependendo de como o sistema é usado, nem toda a capacidade pode ser utilizada.

Por exemplo, considere uma lâmpada que, ao meio-dia, pode estar acesa ou apagada conforme o sol tenha nascido ou não naquele dia. Embora a capacidade de informação desse sistema seja 1 bit, intuitivamente a notícia de que essa lâmpada está acesa não traz muita informação. Por outro lado, uma lâmpada que indica se está chovendo ou não fora do prédio parece fornecer mais informação — muito embora sua *capacidade* de informação seja exatamente a mesma.

A diferença entre estes dois exemplos está na probabilidade que atribuímos aos dois estados do sistema. No primeiro caso, é natural atribuir probabilidade bem próxima a 1 à afirmação “a lâmpada está acesa” (a menos que sejamos extremamente pessimistas!). Por isso, a notícia de que essa informação é verdadeira não muda muito nosso estado de conhecimento. Já, no segundo exemplo, faz sentido atribuir probabilidade bem menor que 1 a essa afirmação (a menos que estejamos na Bolívia, onde nunca chove!).

Para tornar esta intuição mais precisa, suponha que  $X$  é uma variável aleatória que pode assumir um

certo valor  $v$ . A *quantidade de informação* trazida pela notícia “o valor de  $X$  é  $v$ ” é, por definição,

$$\mathbb{Q}(X = v) = \log_2 \frac{1}{\Pr(X = v)} = -\log_2 \Pr(X = v)$$

Este valor, como a capacidade de informação, é medido em bits, e nunca é negativo. Em particular, se  $X$  pode assumir  $n$  valores distintos com igual probabilidade  $\Pr(X = v) = 1/n$ , a quantidade de informação que recebemos quando ficamos sabendo o valor de  $X$  (qualquer valor de  $X$ ) é exatamente  $\mathbb{Q}(X = v) = \log_2 n$  bits — ou seja, a capacidade da variável  $X$ .

Porém, se as probabilidades dos valores de  $X$  não são iguais, a quantidade de informação pode ser menor ou maior, dependendo do valor. Por exemplo:

**Exemplo 12.3:** Suponha que um dado está para ser lançado, e  $X$  é uma variável que vale 100 se o resultado do dado é 1, e 200 caso contrário. Então as notícias “ $X = 100$ ” e “ $X = 200$ ” carregam as seguintes quantidades de informação:

$$\begin{aligned}\mathbb{Q}(X = 100) &= -\log_2 \Pr(X = 100) = -\log_2 \frac{1}{6} \approx 2,5849625 \dots \\ \mathbb{Q}(X = 200) &= -\log_2 \Pr(X = 200) = -\log_2 \frac{5}{6} \approx 0,2630344 \dots\end{aligned}$$

Neste exemplo, observe que a notícia “ $X = 200$ ” traz muito menos informação do que a notícia “ $X = 100$ ”, porque tem probabilidade maior —  $5/6$  em vez de  $1/6$ .

### 12.9.3 Quantidade esperada de informação

No exemplo 12.3, observe também que a notícia “ $X = 100$ ” traz mais que 1 bit de informação — muito embora a variável  $X$  tenha apenas dois valores possíveis, e portanto tenha apenas 1 bit de capacidade.

Este paradoxo é resolvido se considerarmos a *quantidade esperada de informação*, ou *entropia*, da variável  $X$ . Ou seja, a quantia

$$\mathcal{H}(X) = \sum_v \Pr(X = v) \mathcal{Q}(X = v) = \sum_v -\Pr(X = v) \log_2 \Pr(X = v) \quad (12.23)$$

Nesta fórmula, o índice  $v$  do somatório assume todos os valores possíveis da variável  $X$ . Observe que, como na fórmula (12.12), cada termo desta soma é a quantidade de informação trazida pela notícia “ $X = v$ ”, vezes a probabilidade de recebermos essa notícia. Pode-se verificar que  $\mathcal{H}(X)$ , assim como cada termo  $\mathcal{Q}(X = v)$ , é um valor real não negativo.

No exemplo 12.3, a quantidade esperada de informação que recebemos ao conhecer o valor de  $X$  é

$$\begin{aligned} \mathcal{H}(X) &= \Pr(X = 100) \mathcal{Q}(X = 100) + \Pr(X = 200) \mathcal{Q}(X = 200) \\ &= \frac{1}{6} \log_2 \frac{6}{1} + \frac{5}{6} \log_2 \frac{6}{5} \\ &\approx \frac{1}{6} 2,5849625 \dots + \frac{5}{6} 0,2630344 \dots \\ &\approx 0,65002241 \dots \end{aligned}$$

Observe que, embora a notícia “ $X = 100$ ” forneça mais de 2,5 bits de informação, ela é muito menos provável que a notícia “ $X = 200$ ”, que fornece menos que 0,27 bits de informação. Assim, a quantidade esperada de informação que ganhamos ao saber o valor de  $X$  é cerca de 0,65 bits, ou seja abaixo da capacidade de  $X$  (1 bit). Esta última observação é um resultado importante:

**Teorema 12.3:** Se uma variável aleatória  $X$  pode assumir  $n$  valores distintos, então a quantidade esperada de informação que ganhamos conhecendo o valor de  $X$  é no máximo a capacidade de  $X$ ,  $\log_2 n$ ; e é exatamente  $\log_2 n$  apenas quando todos esses valores podem ocorrer com igual probabilidade  $1/n$ .

Devido a este teorema, a fórmula (12.23) é muito usada para medir a “uniformidade” da distribuição de probabilidades de uma variável aleatória  $X$ . O valor de  $\mathcal{H}(X)$  varia entre 0 e  $\log_2 n$ , onde  $n$  é o número de valores possíveis de  $X$ . Quanto maior  $\mathcal{H}(X)$ , mais uniforme a distribuição. Na verdade, a fórmula (12.23) pode ser usada com qualquer lista de  $n$  valores reais  $p_0, p_1, \dots, p_{n-1}$  não negativos cuja soma é 1.

Observe que se  $X$  tem uma distribuição degenerada — com  $\Pr(X = v) = 1$  para um único valor  $v$ , e zero para os demais valores — então  $\mathcal{H}(X)$  é zero. Ou seja, se temos certeza de qual vai ser o valor de  $X$ , nossa expectativa é que a revelação desse valor não vai nos trazer nenhuma informação.

## 12.10 Exercícios adicionais

**Exercício 12.26:** Você atribuiu probabilidades 0.25, 0.80, e 0.50, respectivamente, às afirmações  $A$ ,  $B$  e  $C$ .

- (a) Supondo que as afirmações  $A$  e  $B$  são independentes, calcule  $\Pr(A \vee B)$ .
- (b) Quais são os valores máximo e mínimo que você pode atribuir a  $\Pr(B \wedge C)$ , respeitando as leis da probabilidade?

**Exercício 12.27:** Sejam  $M_1, M_2, M_3$  variáveis aleatórias que representam os resultados de três lançamentos independentes de moedas, representando *Cara* como valor 0 e *Coroa* como valor 1. Seja  $X = M_1 + M_2 + M_3$ , seja  $Y = M_1 + M_2$ , e seja  $Z = M_2 + M_3$ .

- (a) Qual é a distribuição de probabilidade de  $X$ ?
- (b) Calcule o valor esperado  $\mathcal{E}(X)$ .
- (c) Calcule a variância  $\mathcal{V}(X)$  e o desvio padrão  $\mathcal{D}(X)$ .
- (d) Calcule a covariância  $\mathcal{C}(Y, Z)$ .
- (e) Calcule o coeficiente de correlação  $\kappa(X, Y)$ .

**Exercício 12.28:** Uma pessoa repetidamente joga dois dados, um azul e um branco, até que o resultado  $A$  do azul seja estritamente maior que o resultado  $B$  do branco.

- (a) Quanto é  $\Pr(A = 5)$ ?
- (b) Quanto é  $\Pr(A = 5 \mid B = 3)$ ?
- (c) Quanto é  $\Pr(B = 3 \mid A = 5)$ ?

**Exercício 12.29:** Uma empresa tem duas fábricas que colocam seus produtos — bolinhas de gude azuis ( $A$ ) ou brancas ( $B$ ) — em caixas de 20 bolinhas cada. A fábrica  $F$  coloca 18 bolinhas azuis e 2 brancas em cada caixa. A fábrica  $G$  coloca 10 bolinhas de cada cor. Por fora, as caixas são todas iguais, sem identificação de origem. Você recebe uma caixa que pode ter vindo de qualquer das duas fábricas. Você tira uma bolinha de dentro da caixa, e constata que é branca. Usando a fórmula de Bayes, calcule a probabilidade da caixa ter vindo da fábrica  $F$ .

**Exercício 12.30:** Quatro cartões com os números 1, 2, 3 e 4 são embaralhados, e alguém escolhe dois deles ao acaso. Sejam  $X$  e  $Y$  os dois resultados, na ordem que foram sorteados, e  $Z = X + Y$ .

- (a) Qual é a quantidade de informação que obteríamos se fôssemos informados de que  $Z = 5$ ?
- (b) Qual é a entropia de  $Z$ ?
- (c) Qual é a quantidade esperada de informação que o valor de  $Z$  daria sobre o valor de  $X$ ?

**Exercício 12.31:** Você está apostando cara ou coroa com seu colega, usando uma moeda sabidamente honesta. As últimas quatro jogadas deram cara. Qual é a probabilidade de dar cara na próxima jogada?

**Exercício 12.32:** Você está apostando dados com seu colega — com um só dado, a dinheiro. Você começa apostando 1 real, e a cada vez você aposta que vai sair 1, 2, ou 3. A cada jogada, se você perde, você paga o valor apostado, e aposta de novo, o dobro do valor. Se você ganha, você recebe o valor da última aposta, e o jogo termina. De qualquer maneira o jogo termina depois de quatro jogadas, mesmo que você tenha perdido todas; e nesse caso também você paga o valor de cada aposta perdida, inclusive a última.

- (a) Calcule as probabilidades de todos os resultados possíveis nesse jogo.
- (b) Para cada resultado possível, calcule o total líquido  $T$  que você ganha (ou perde,  $T < 0$ ).
- (c) Calcule o valor esperado de  $T$ .
- (d) Repita estes cálculos supondo que a cada rodada você aposta que vai sair 1 ou 6.

**Exercício 12.33:** Você aposta cara ou coroa com seu colega cinco vezes, e nas cinco vezes aposta cara e perde. Mais tarde você desconfia que seu colega trapaceou usando uma moeda viciada ( $V$ ) com coroa nos dois lados, em vez de uma honesta ( $H$ ). Usando a fórmula de Bayes, calcule a probabilidade da hipótese  $V$  levando em conta o resultado desses cinco lances:

- (a) Supondo que a probabilidade de  $V$  *a priori* é 1%.
- (b) Supondo que essa probabilidade é 50%.

**Exercício 12.34:** Você joga cara ou coroa com seu colega dez vezes, e você nota que em oito das dez vezes o resultado é coroa. Mais tarde você desconfia que seu colega trapaceou usando uma coroa viciada, feita de tal forma que dá coroa com frequência bem maior que 50% em média. Calcule a probabilidade de obter um número de coroas maior ou igual a oito com uma moeda honesta.

**Exercício 12.35:** Um laboratório desenvolveu uma pílula que supostamente cura unha encravada em menos de uma semana. A pílula é testada em 20 voluntários com essa condição, sendo que 10 (o *grupo de teste*,  $T$ ) recebem a pílula e os outros 10 (o *grupo de controle*,  $C$ ) recebe um produto que sabidamente não tem efeito na condição (um *placebo*). Após uma semana, constata-se que a condição desapareceu em 7 pessoas (70%) do grupo de teste e em 5 pessoas (50%) do grupo de controle. Suponha que a probabilidade da unha encravada sumir por conta própria, sem medicação, é mesmo 50%. Calcule (usando um computador) qual seria a probabilidade de obter 70% ou mais de sucessos se a pílula não tivesse nenhum efeito.

**Exercício 12.36:** Um astrônomo descobre um novo planeta no Sistema Solar e calcula sua distância por dois métodos diferentes. O método 1 dá distância  $D_1 = 10$  Tm (10 terâmetros, ou 10 bilhões de km), mas é sabidamente afetado por um erro aleatório  $R_1$  com valor esperado zero e desvio padrão  $\sigma_1 = 2$  Tm. O método 2 dá  $D_2 = 12$  Tm mas tem erro  $R_2$ , independente de  $R_1$ , com valor esperado zero e desvio padrão  $\sigma_2 = 4$  Tm. O astrônomo quer anunciar que a distância é uma média ponderada das duas medidas,  $D = aD_1 + (1 - a)D_2$ , para algum peso  $a$  entre 0 e 1.

- (a) Supondo escolhido o peso  $a$ , qual será o desvio padrão  $\sigma$  do erro  $R$  na média  $D$ ?
- (b) Qual valor de  $a$  tornaria  $\sigma$  o menor possível?
- (c) Quando será a media final  $D$  com esses pesos?
- (d) Quanto será o desvio padrão  $\sigma$  do erro  $R$  com esses pesos? Compare com  $\sigma_1$  e  $\sigma_2$ .
- (e) Quanto seria o desvio  $\sigma$  do erro  $R$  em  $D$  se o astrônomo usasse média simples ( $a = 1/2$ )?

**Exercício 12.37:** Dias antes de uma eleição com dois candidatos, Jânio e Adhemar, uma agência de pesquisas de mercado faz uma prévia com  $m$  eleitores escolhidos ao acaso, e registra o número  $m_J$  deles que dizem que vão votar no Jânio, e o número  $m_A = m - m_J$  que vão votar no Adhemar.

- (a) Escreva a fórmula da probabilidade *a priori*  $\Pr(m_J = y \mid g_J = z)$  de obter  $m_J = y$  nessa pesquisa, fixado o tamanho  $m = x$  de amostra e supondo que a fração real  $g_J$  de apoiadores do Jânio, entre os 100 milhões de eleitores, seja  $z$  (um número entre 0 e 1).
- (b) Para simplificar, vamos supor que  $g_J$  é uma percentagem inteira, então existem só 101 casos possíveis ( $g_J = 0\%$ ,  $g_J = 1\%$ , ...,  $g_J = 100\%$  do eleitorado). Usando a fórmula de Bayes, escreva um procedimento em alguma linguagem (Python, C, etc) que calcula distribuição de probabilidade de  $g_J$ ,  $\Pr(g_J = z \mid m_J = y)$ , dado  $m$  e o valor observado  $y$  de  $m_J$ .
- (c) Usando esse procedimento, escreva outro que calcula o valor esperado e o desvio padrão de  $g_J$ , dado  $m$  e o valor  $y$  de  $m_J$ .
- (d) Usando o procedimento acima, escreva um programa para calcular  $\Pr(g_J < 50\% \mid m_J = 110)$  — a probabilidade de Adhemar ainda ganhar a eleição, dado que  $m_J = 110$  de  $m = 200$  entrevistados (55%) escolheram Jânio. Supõe-se que essas pessoas não estão mentindo e nenhum eleitor vai mudar de idéia até lá.
- (e) Com esses procedimentos, determine o número  $m$  de pessoas que deveriam ser entrevistadas para que essa probabilidade fosse menor que 1%, supondo que o valor  $y$  de  $m_J$  ainda seria aproximadamente 55% de  $m$ .

**Exercício 12.38:** O *Problema de Monty Hall* é baseado num programa da TV americana com um apresentador desse nome. A cada rodada, ele pedia para um candidato escolher uma dentre três portas fechadas, sendo que atrás de uma delas havia um carro zero e cada uma das outras duas escondia um bode. Depois que o candidato escolhia, o apresentador abria uma das outras duas portas que tinha um bode, e pedia para o candidato escolher de novo dentre as duas que ficaram fechadas – a que ele escolheu antes, e a terceira. O que estivesse atrás da nova escolha seria seu prêmio. A questão é o que o candidato deveria fazer: manter a escolha anterior, escolher a outra porta, ou daria na mesma?

**Exercício 12.39:** Numa guerra, um capitão de navio precisa escolher entre dois caminhos, pelo norte (N) ou pelo sul (S) de uma ilha. Ele sabe que há um navio inimigo esperando num dos lados, mas não sabe qual. Se ele for pelo lado oposto, vai passar sem dano. Se ele for pelo norte e o inimigo estiver lá, as condições são tais que o inimigo tem 40% de chance de afundar seu barco. Se ele for pelo sul, e o inimigo estiver lá, as chances disso acontecer são só 10%. O sul pode parecer mais seguro, mas o inimigo sabe que o capitão sabe dessas probabilidades, e se o capitão for bobo o inimigo vai esperar no sul. Então é melhor ir pelo norte. Mas o inimigo, prevendo que o capitão vai pensar assim, vai esperar no norte. E aí? Será que é melhor tirar cara ou coroa?

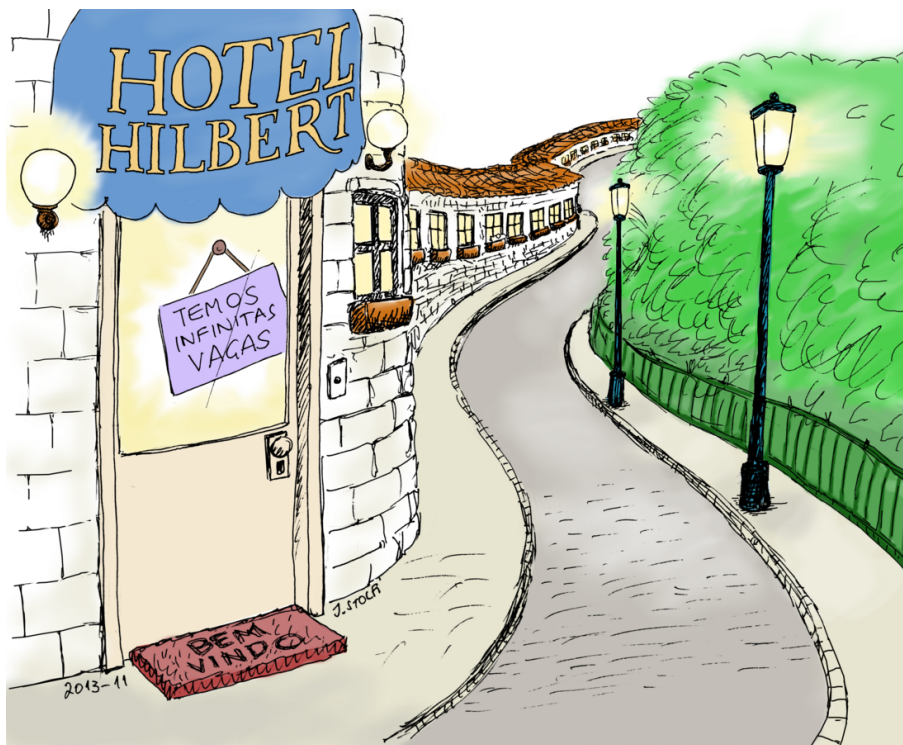
Felizmente o Manual da Marinha especifica como o comandante deve escolher a rota a fim de minimizar suas chances de perda. O inimigo também sabe o que o Manual diz, e sabe que o capitão vai seguir à risca, mas isso não importa — é ainda a melhor estratégia para o capitão.

- (a) O que diz o Manual?
- (b) Sabendo disso, como o inimigo deve escolher de que lado da ilha vai ficar?
- (c) Qual é a probabilidade do navio ser afundado, nessas condições?



# **Capítulo 13**

## **Cardinalidade de conjuntos**



No capítulo 2 definimos informalmente a cardinalidade de conjuntos finitos, mas só agora temos condições de dar uma definição mais precisa de cardinalidade, inclusive para conjuntos infinitos.

**Definição 13.1:** Sejam  $A$  e  $B$  dois conjuntos. Se existir uma função bijetora  $f : A \rightarrow B$ ,

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  $|A| = |B|$ .

**Exercício 13.1:** Prove que  $\sim$  é uma relação de equivalência.

## 13.1 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  $\{\}$  é finito e  $|\{\}| = 0$ .

**Exercício 13.2:** Prove que

- (a) para todo número natural  $m$  e  $n$ , se  $I_n \sim I_m$  então  $m = n$ .  
(Sugestão: use indução em  $n$ .)
- (b) se  $A$  é finito, então existe exatamente um número natural tal que  $I_n \sim A$ .

## 13.2 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 13.1:** Seja  $\mathbb{E} \subset \mathbb{N}$  o conjunto dos números naturais pares,  $\{2k : k \in \mathbb{N}\}$ . Considere a função  $f : \mathbb{N} \rightarrow \mathbb{E}$  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 acima 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 são os seguintes:

**Exemplo 13.2:** Considere a função  $f : \mathbb{N} \rightarrow \mathbb{Z}$  definida por

$$f(n) = (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor = \begin{cases} k & \text{se } n \text{ é par } (n = 2k) \\ -(k+1) & \text{se } n \text{ é ímpar } (n = 2k+1) \end{cases} \quad (13.1)$$

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 13.3:** Considere a função  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  definida pela fórmula

$$f(u, v) = \frac{(u+v)(u+v+1)}{2} + u \quad (13.2)$$

A tabela abaixo ilustra a função  $f$ . Ela associa a cada par  $(u, v)$  um número natural na sequência,

segundo diagonais sucessivas:

|     |          | $v$      |     |     |     |     |     |
|-----|----------|----------|-----|-----|-----|-----|-----|
|     |          | 0        | 1   | 2   | 3   | 4   | ... |
| $u$ | 0        | 0        | 1   | 3   | 6   | 10  | ... |
|     | 1        | 2        | 4   | 7   | 11  | ... |     |
|     | 2        | 5        | 8   | 12  | ... |     |     |
|     | 3        | 9        | 13  | ... |     |     |     |
|     | 4        | 14       | ... |     |     |     |     |
|     | $\vdots$ | $\vdots$ |     |     |     |     |     |

Verifica-se que esta função é uma bijeção de  $\mathbb{N} \times \mathbb{N}$  para  $\mathbb{N}$ , e portanto  $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ .

**Exemplo 13.4:** Considere a função  $f : [0, 1] \rightarrow [1, 3]$  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.

Podemos demonstrar também que

**Teorema 13.1:** Para todo inteiro positivo  $n$ ,  $\mathbb{N}^n \sim \mathbb{N}$ .

A demonstração pode ser feita por indução em  $n$ , usando a função  $f$  do exemplo 13.3, e a bijeção  $g$  entre os conjuntos  $\mathbb{N}^n$  e  $(\mathbb{N}^{n-1}) \times \mathbb{N}$ , definida por

$$g((a_1, a_2, \dots, a_n)) = ((a_1, a_2, \dots, a_{n-1}), a_n)$$

para toda ênupla  $(a_1, a_2, \dots, a_n)$  em  $\mathbb{N}^n$ .

**Exercício 13.3:** Demonstre o teorema 13.1.

Outro resultado importante é o seguinte:

**Teorema 13.2:** 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  $\{0, 1, \dots, m^n - 1\}$ . Considere a função  $g : X^* \rightarrow \mathbb{N}$ , 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,

$$\begin{array}{lll} \text{se } x \in X^0 & \text{então } g(x) = f_0(x) & = 0; \\ \text{se } x \in X^1 & \text{então } g(x) = 1 + f_1(x) & \in \{1, \dots, 1 + (m - 1)\}; \\ \text{se } x \in X^2 & \text{então } g(x) = 1 + m + f_2(x) & \in \{1 + m, \dots, 1 + m + (m^2 - 1)\}; \\ \text{se } x \in X^3 & \text{então } g(x) = 1 + m + m^2 + f_3(x) & \in \{1 + m + m^2, \dots, 1 + m + m^2 + (m^3 - 1)\}; \end{array}$$

e assim por diante. Pode-se ver que a função  $g$  é uma bijeção de  $X^*$  para  $\mathbb{N}$ , e portanto  $X^* \sim \mathbb{N}$ .

**Fim.**

Observe que este teorema não se aplica ao conjunto das sequências *infinitas* sobre um conjunto finito  $X$ . Um contra-exemplo será visto na seção 13.4.

### 13.3 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  $a_0, a_1, a_2, \dots$ ; isto é, podemos indexá-los pelos números naturais.

**Exemplo 13.5:** O conjunto  $\mathbb{N} \times \{i\}$ , para qualquer  $i \in \mathbb{N}$ , é enumerável. Para provar esta afirmação, considere a função  $f : \mathbb{N} \rightarrow \mathbb{N} \times \{i\}$  tal que  $f(j) = (j, i)$  para todo  $j \in \mathbb{N}$ , que é trivialmente bijetora.

**Exemplo 13.6:** Todo subconjunto  $A$  de  $\mathbb{N}$  é contável. Se  $A$  é finito, ele é contável. Se  $A$  não é finito, considere a função bijetora  $f : A \rightarrow \mathbb{N}$  onde  $f(a)$  é número de elementos de  $A$  que são menores que  $a$ , para todo  $a \in A$ .

**Exemplo 13.7:** 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 13.6,  $A$  é contável. A restrição de  $f$  a  $A$  é uma bijeção de  $A$  para  $C$ , e portanto  $C$  também é contável.

**Exercício 13.4:** Prove que  $\mathbb{Z} \times \mathbb{N}$  e  $\mathbb{Z} \times \mathbb{Z}$  são enumeráveis.

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 13.3:** Seja  $X$  um conjunto enumerável cujos elementos são conjuntos enumeráveis, disjuntos dois a dois. A união de todos os elementos de  $X$  é enumerável.

**Prova:**

Como  $X$  é enumerável, podemos indexar seus elementos com números naturais,  $X_0, X_1, \dots$ . Como cada conjunto  $X_i$  é enumerável, podemos também indexar seus elementos com números naturais,  $x_{i,0}, x_{i,1}, \dots$ .

Seja então  $Y$  a união de todos esses conjuntos,  $Y = \cup_{i \in \mathbb{N}} X_i$ , e considere a função  $g : \mathbb{N} \times \mathbb{N} \rightarrow Y$  tal que  $g(i, j) = x_{i,j}$  para quaisquer  $i$  e  $j$  em  $\mathbb{N}$ . Esta função é uma bijeção, pois para todo elemento  $y$  de  $Y$  existe um único  $i$  tal que  $y \in X_i$ , e um único  $j$  tal que  $y = x_{i,j}$ . Portanto  $Y \sim \mathbb{N} \times \mathbb{N}$ , ou seja  $Y \sim \mathbb{N}$  pelo exemplo 13.3.

**Fim.**

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.

**Exercício 13.5:** Prove que o conjunto  $\mathbb{Q}$  dos números racionais é contável. (Dica: todo número racional pode ser escrito de maneira única como uma fração  $m/n$  onde  $m$  é inteiro e  $n$  é um inteiro positivo, relativamente primo com  $m$ .)

**Exercício 13.6:** Prove todo conjunto infinito tem um subconjunto enumerável.

**Exercício 13.7:** Prove que, se  $A$  é infinito, então para qualquer  $n \in \mathbb{N}$  existe um subconjunto de  $A$  com cardinalidade  $n$ .

**Exercício 13.8:** Prove que um conjunto  $A$  é contável se e somente se existe uma função de  $\mathbb{N}$  para  $A$  sobrejetora em  $A$  (não necessariamente injetora).

**Exercício 13.9:** Seja  $X$  um conjunto contável. Prove que, para todo número natural  $n$ ,  $X^n$  é um conjunto contável.

## 13.4 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 conjectura 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 13.4:** 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  $a_i = 0, a_{i0}a_{i1}a_{i2} \dots$  do mesmo. Temos então uma lista infinita de sequências infinitas de algarismos

$$\begin{aligned} f(0) &= a_0 = 0, a_{00}a_{01}a_{02} \dots \\ f(1) &= a_1 = 0, a_{10}a_{11}a_{12} \dots \\ f(2) &= a_2 = 0, a_{20}a_{21}a_{22} \dots \\ &\vdots \end{aligned}$$

Observe que alguns números reais tem duas representações distintas deste tipo, uma delas terminando com uma sequência infinita de zeros, e a outra com uma sequência infinita de noves. Por exemplo, o número  $1/4$  pode ser escrito como  $0,250000 \dots$  ou  $0,249999 \dots$ . Isto ocorre se, e somente se, o número é uma fração da forma  $m/10^n$ , com  $m$  e  $n$  inteiros,  $m \neq 0$  e  $n \geq 0$ . 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  $0,000000 \dots$  e  $0,999999 \dots$  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  $0, \dots$  representa algum número real no intervalo  $(0, 1)$ .

Considere agora a representação decimal infinita  $b = 0, b_0 b_1 b_2 \dots$  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  $\mathbb{N}$ .

Concluimos que nenhuma função  $f$  de  $\mathbb{N}$  para  $(0, 1)$  pode ser sobrejetora. Logo  $(0, 1)$  não é enumerável.

**Fim.**

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  $\mathbb{R}$  (Veja exercício 13.10). Portanto, em vista do teorema 13.4 a cardinalidade de  $\mathbb{R}$  é estritamente maior que a cardinalidade de  $\mathbb{N}$ . Na verdade, pode-se demonstrar [?] que

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| \tag{13.3}$$

**Exercício 13.10:** Prove que  $(0, 1) \sim \mathbb{R}$ .

**Exercício 13.11:** Seja  $\mathcal{F}$  o conjunto de todas as funções de  $\mathbb{N}$  para o conjunto  $\{1, 2\}$ . Usando a técnica de diagonalização de Cantor, prove que o conjunto  $\mathcal{F}$  não é enumerável.

## 13.5 Comparação de cardinalidades

Sejam  $A$  e  $C$  conjuntos. Definimos a relação  $C$  *domina*  $A$  e escrevemos  $A \leq C$  se existe um conjunto  $B$  tal que  $A \sim B$  e  $B \subseteq C$ . Em outras palavras,  $A \leq C$  se e somente se existe uma função injetora de  $A$  para  $C$ .

**Exemplo 13.8:** Seja  $\mathbb{C}$  o conjunto dos números primos, e  $\mathbb{M}$  o conjunto dos quadrados perfeitos,  $\{n^2 : n \in \mathbb{N}\}$ . Observe que a função  $f$  de  $\mathbb{C}$  para  $\mathbb{M}$  definida por  $f(p) = p^2$  é uma função injetora. Portanto, concluímos que  $\mathbb{C} \leq \mathbb{M}$ .

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  $A \leq B$ . Em particular,  $A \leq A$  para qualquer conjunto  $A$ ; ou seja,  $\leq$  é uma relação reflexiva. Prova-se também que, se  $A \leq B$  e  $B \leq C$ , então  $A \leq C$ ; isto é,  $\leq$  é transitiva. (Veja exercício 13.12)

Finalmente, prova-se que, se  $A \leq B$  e  $B \leq A$ , então  $A \sim B$  (isto é,  $A$  e  $B$  tem a mesma cardinalidade). Porém, a demonstração deste fato (devida a Cantor, Schröder e Bernstein) [?] foge do escopo deste

livro. Outro resultado cuja prova não cabe aqui é que, dados quaisquer dois conjuntos  $A$  e  $B$ , pelo menos uma das condições  $A \leq B$  e  $B \leq A$  deve ser verdadeira.

Pode-se verificar também (veja exercício 13.13) que se  $A \sim A'$ ,  $B \sim B'$ , e  $A \leq B$ , então  $A' \leq B'$ . Portanto a relação  $\leq$  entre conjuntos depende apenas de suas cardinalidades, e não dos conjuntos em si. Podemos então substituir  $\leq$  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  $C$* , e escrevemos  $|A| \leq |B|$ , se e somente se  $A \leq B$ .

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  $B \subset A \rightarrow |B| < |A|$ .

**Exercício 13.12:** Prove que, se  $A \leq B$  e  $B \leq C$ , então  $A \leq C$ .

**Exercício 13.13:** Prove que se  $A \sim A'$ ,  $B \sim B'$  e  $A \leq B$ , então  $A' \leq B'$ .

### 13.5.1 Teorema de Cantor

Cantor mostrou também o seguinte resultado importante:

**Teorema 13.5:** Para todo conjunto  $A$ ,  $|A| < |\mathcal{P}(A)|$ .

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  $|\mathcal{P}(A)| = 2^n$  (vide seção 2.4.1) e  $2^n > n$  para todo natural  $n$ . A contribuição de Cantor foi mostrar que o resultado vale também para conjuntos infinitos.

**Prova:**

Sejam  $A$  um conjunto e  $f$  uma função qualquer de  $A$  para  $\mathcal{P}(A)$ , 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  $\mathcal{P}(A)$ .

Observe que o elemento  $a$  pode pertencer ou não ao subconjunto  $f(a)$ . Considere agora o seguinte conjunto:

$$X = \{ a \in A : a \notin f(a) \}$$

Observe que  $X$  é um subconjunto de  $A$ , logo  $X \in \mathcal{P}(A)$ . 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  $\mathcal{P}(A)$ .

Concluimos que, para qualquer conjunto  $A$ , não existe nenhuma bijeção de  $A$  para  $\mathcal{P}(A)$ ; 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  $\mathcal{P}(A)$ . Isto mostra que  $|A| \leq |\mathcal{P}(A)|$ . Juntando estes dois resultados, concluimos que  $|A| < |\mathcal{P}(A)|$ .

**Fim.**

Em particular, a cardinalidade de  $\mathcal{P}(\mathbb{N})$  é estritamente maior que a de  $\mathbb{N}$ .

### 13.5.2 A hipótese do contínuo

Depois de mostrar que  $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$ , 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 conjectura 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.

## 13.6 Cardinalidade e Computabilidade

Os conceitos de cardinalidade de conjuntos infinitos permitem responder a questão: “toda função pode ser computada?”. Para isto observamos que qualquer programa de computador, em qualquer linguagem, pode ser visto como uma sequência finita de caracteres, tirados de um conjunto finito de caracteres válidos. Então, pelo teorema 13.2,

**Teorema 13.6:** O conjunto de todos os programas em uma dada linguagem de programação é contável.

Por outro lado, temos também o seguinte fato:

**Teorema 13.7:** 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 na demonstração do teorema 13.4, todo número  $a$  nesse conjunto pode ser representado na notação decimal por uma sequência infinita  $0.a_1a_2 \dots a_n \dots$  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  $\mathcal{G} = \text{Im}(f) \subset \mathcal{F}$ .

Pelo teorema 13.4,  $S$  não é enumerável. Concluimos que  $\mathcal{F}$  tem um subconjunto que não é enumerável. Portanto pelo exercício 13.7,  $\mathcal{F}$  não é enumerável.

**Fim.**

Diz-se que uma função  $f : \mathbb{N} \rightarrow \mathbb{N}$  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. O teorema 13.6 mostra que  $|\mathcal{C}| \leq |\mathbb{N}|$ . Por outro lado o teorema 13.7 mostra que  $|\mathcal{F}| > |\mathbb{N}|$ . Logo, concluímos que existem funções de  $\mathbb{N}$  para  $\mathbb{N}$  que não são computáveis.

# Índice Remissivo

pi

algarismos, 29

$n$ -upla, *veja* ênupla

água, 231

álgebra, 17

de Boole, 36

árvore, *veja* grafo árvore

ócupla, *veja* ênupla

órbita, *veja* função permutação, ciclo

índice

de somatória, *veja* somatória, índice

ângulo

interno, 80

ênupla, 26, *veja* sequência finita

definição, 26

elementos, 26

absurdo, *veja* demonstração, implicação por absurdo

Ackermann

Wilhelm, 161

Al-Khowarizmi, 17

algarismo, 123, 186

algoritmo

de Euclides, 17

demonstração, 15

geométrico, 15

alunos, 183

ambiguidade, 31, 35, 60

amigo, 52

análise de algoritmos, 17

antecedente, 33

Appel, Kenneth, 61

- Appel, Kenneth Ira, 236
- Argentina, 30
- Aristóteles, 15
- arquivo, 116
- Arranjo
  - circular, 180
  - com elementos indistinguíveis, 181
- arranjo, 174–175
  - contagem, *veja* contagem de arranjos de letras, 174
  - definição, 174
  - e permutação, 175
- arroz, 31
- Artur, Rei da Inglaterra, 228
- associatividade, 41
  - da diferença simétrica, 24
  - da intersecção, 23
  - da união, 23
- auto-referência, *veja* proposição auto-referente
- axioma, 15, 19, 59, 60
  - da aritmética, 76
  - de Euclides, 16
  - do contínuo, 246
  - balança, 84, 88
  - banana, 51, 52, 54, 120
  - banco de dados, 208
  - bancos de dados, 112
  - bandeira, 172
  - baralho, 169, 176, 182, 184, 185, 204
  - base neperiana (*e*), 158
  - bateria, 35
  - Bayes, Thomas, 201
  - Bernoulli, Jacob, 83
  - Bernstein, Felix, 245
  - bijeção, *veja* função bijetora, 239–247
  - binômio de Newton, 177
  - bipartição, 226
  - bit, 121, 123, 203
    - contagem de cadeias, 176
    - definição, 204
  - bloco
    - de partição, 25
  - boi, 53
  - bola, 78, 201
  - branco, 32
  - Brasília, 30, 33
  - Brasil, 29, 30

- byte, 203
- C (linguagem), 141
- cálculo
  - de predicados, 17, 50
  - proposicional, 29–47
- código genético, 204
- círculo, 16, 94, 95
- cadeia, *veja* sequência finita
- caixa, 116, 117, 201
  - jeitos de tampar, 136
  - rotulada, 135
- Cantor, Georg, 19
- Cantor, Georg Ferdinand Ludwig Philipp, 243, 245, 246
- capacidade de armazenamento, *veja* informação, capacidade
- capacidade de informação, *veja* informação, capacidade
- cardinalidade, *veja* conjunto, 239–247
  - comparação, 244
  - contável, 242–243
  - da união, 185, 242
  - das sequências finitas, 241
  - de conjunto finito, 240
  - de conjunto infinito, 240, 243
  - de conjuntos finitos, 245
  - de subconjunto, 242, 243
  - de subconjuntos, 245
- definição, 239
- do produto cartesiano, 241, 242
- dos inteiros, 240
- dos números naturais, 242–243, 246
- dos números reais, 241, 243–244, 246
- dos pares de inteiros, 242, 243
- dos pares de naturais, 241
- dos racionais, 243
- e computabilidade, 246–247
- igualdade, 239
- menor, 245
- menor ou igual ( $\leq$ ), 244
- carro, 171
- casa, 32, 33
- casas, 31
- cavalo, 81, 231
- celular, 32
- { } (chaves), 20
- Chebyshev, *veja* Tchebychev

- cheque, 35
- ciclo, *veja* função permutação, ciclo
- circuito
  - digital, 208
  - elétrico, 208
- classe
  - de equivalência, 124–127, 221
  - representante, 125
  - de isomorfismo, 221
- coeficiente binomial, *veja* combinação
  - casos especiais, 176
  - definição, 175
- coeficiente multinomial, *veja* combinação múltipla
- cofre, 230
- Cohen, Paul, 246
- Cole, Frank Nelson, 61
- coloração, *veja* grafo, coloração
- combinação, 175–181
  - algoritmo, 178
  - casos especiais, 176
  - com repetições, *veja* partição rotulada, con-  
tagem, *veja* combinação múltipla
  - contagem, 175
  - de letras, 175
  - de respostas em prova, 178
  - definição, 175
  - e arranjo, 175
  - fórmula de Leibniz, 182
  - fórmula de Newton, 177
  - fórmula recursiva, 178
  - identidade de Pascal, 177
  - múltipla, 182–183
  - notação, 175
  - propriedades, 176
  - simetria, 176
  - somatória, 178
  - triângulo de Pascal, 177
- complemento, *veja* conjunto, complemento
- composição
  - de relações, *veja* relação, composição
- comutatividade, 40
  - da diferença simétrica, 24
  - da intersecção, 23
  - da união, 23
- conclusão, 33
- condição
  - necessária, 33
  - suficiente, 33

conectivo lógico, *veja* operador lógico

em linguagem natural, 31

conectivo lógico, *veja* operador lógico

conjectura, *veja* conjetura

conjetura, 61

aberta, 61

das quatro cores, 61

de Fermat, 61

de Goldbach, 61

de Mersenne, 61

refutação, 73

refutada, 61

conjunção, *veja* operador conjunção

conjunto

cardinalidade, 21, 22, 28, 84, *veja* cardinalidade

complemento, 22, 24, 182

contável, 242–243

continência, 63, 68

de conjuntos, 25

de sequências, 117

definição, 19

diferença, 25, 68

diferença ( $\setminus$ ), 22

diferença simétrica ( $\Delta$ ), 22, 24

disjunto, 22, 25

dos subconjuntos, *veja* conjunto potência

enumerável, 242–243

finito, 21, 240

igualdade, 21

infinito, 21, 240

interseção ( $\cap$ ), 22

intersecção, 23–24, 68

leis de De Morgan, 24

notação, 20

operação, 22–24, 27

ordenado, 115, 121

parcialmente, 118

totalmente, 117

parcialmente ordenado, 118

partição, 25, 226

por propriedade, 20

potência, 22, 84, 115, 124, 245

cardinalidade, 25

igualdade, 25

potência ( $\mathcal{P}(A)$ )

definição, 25

totalmente ordenado, 117

- união, 23–24, 68
- união ( $\cup$ ), 22
- universal, 24, 57, 158
- universal ( $\mathcal{U}$ ), 22
- vazio, 21, 24, 69, 101, 158
  - cardinalidade, 21
  - como elemento, 25
  - inclusão, 21
  - partição, 25
  - potência, 25
- vs. sequência, 141
- consequência, 33
- consequência lógica, 43
- $\nsubseteq$  (não estr. contém), *veja* inclusão
- $\not\subseteq$  (não contém), *veja* inclusão
- $\subseteq$  (contido), 19
- $\supset$  (estr. contém), *veja* inclusão
- $\supseteq$  (contém), *veja* inclusão
- Contagem
  - por divisão, 181
- contagem, 169–186
  - arranjos, 175
  - bijeções, 173
  - cadeias de bits, 176
  - combinações, 175
  - de funções, 171–172
  - de relações, 170
    - anti-simétricas, 170
    - irreflexivas, 170
    - reflexivas, 170
    - simétricas, 170
  - funções
    - bijetoras, 173
  - funções sobrejetoras, 175
  - ordens, 169
  - permutações, 173–174
  - união, 185
- $\nsubseteq$  (não estr. contido), *veja* inclusão
- $\not\subseteq$  (não contido), *veja* inclusão
- $\subset$  (estr. contido), *veja* inclusão
- $\subseteq$  (contido), *veja* inclusão
- contra-exemplo, 73, 74
- contradição, 39, 40, 50
- contrapositiva
  - de implicação, *veja* proposição contrapositiva
- copos, 170
- cor, 81

cores, 182, *veja* grafo, coloração de faces  
 corolário, 60  
 correio, 35, 80  
 criança, 179  
 criptografia digital, 17  
 cubo, 81, 231  
 cubo perfeito, 71

dado de jogar, 190–192, 195, 201, 203–205  
 de equivalência, 68  
 De Morgan, *veja* conjunto, leis de  
 De Morgan, Augustus, 24, 41, 236  
 definição, 60  
     circular, 20  
     contraditória, 20  
     definição, 60  
     recursiva, 117  
 demonstração, 17, 59–74  
     construtiva, 70–71, 73  
     de conjunção, 65  
     de disjunção, 64  
     de equivalência, 67–68  
     de existência e unicidade, 73  
     de falsidade, 73

de implicação, 62–66  
     contrapositiva, 64  
     direta, 62, 65  
     hipótese disjuntiva, *veja* demonstração por casos  
     tese conjuntiva, 65  
 de quantificador existencial, 68, 70–74  
 de quantificador universal, 64, 66, 68  
 de unicidade, 73  
 direta, 63  
 estratégia, *veja* demonstração, método  
 existência e unicidade, 72–73  
 indireta, *veja* prova, implicação por absurdo  
 método, 61–74  
 não construtiva, 72  
 por absurdo, 64, *veja* demonstração, implicação  
     por absurdo, 72  
 por casos, 65, 66  
 por computador, 236  
 por contra-exemplo, 73–74  
 por contradição, *veja* demonstração, implicação  
     por absurdo  
 por exemplo, 70  
 por partes, 65

- por vacuidade, 69
  - quantificador universal, 69–70
  - técnica, *veja* prova, método
- desarranjo, 135
- desigualdade
  - de Bernoulli, 83
- dia da semana, 137
- diagonal, 80
- diagonalização, 241, 243–244
- diagrama
  - de Hasse, 119, 120, 122, 123
  - de Venn, 23, 24, 27, 68
- dicionário, 117, 121
- diferença, *veja* conjunto, diferença
  - de grafos, *veja* grafo, subgrafo, diferença
- $\setminus$ , *veja* conjunto, diferença
- diferença simétrica, *veja* conjunto, diferença simétrica
- $\Delta$ , *veja* conjunto, diferença simétrica
- digitos, 184, 186
- dinheiro, 81
- Dirichlet, Johann Peter Gustav Lejeune, 84
- disco, 110
- disjunção, *veja* operador disjunção
  - exclusiva, 49
  - disjunção exclusiva
    - operador, *veja* operador disjunção exclusiva
- distributividade, 41
  - da intersecção, 24
  - da união, 24
- divisão
  - do plano
    - por círculos, 162
- divisibilidade, 65, 66, 209
- divisor, 60, 70
  - comum, 17
  - definição, 60
- DNA, 204
- doce, 179
- dodecaedro, 229, 231
- domínio, *veja* relação, domínio
  - de quantificador, 48
  - mudança, 53–54
  - omissão, 56
  - universal, 56
- dominó, 165
- domingo, 52
- dualidade lógica, 46–47

- e*, *veja* base neperiana
- eleição, 37
- elemento
  - definição, 19
  - máximo, *veja* máximo
  - mínimo, *veja* mínimo
  - neutro, 40, 158
- elemento maximal, *veja* maximal
- elemento minimal, *veja* minimal
- encomenda, 35
- entropia, 205, 206
  - como medida de uniformidade, 206
  - máxima, 206
  - nula, 206
- equivalência, 68, *veja* relação de equivalência
  - de operadores, 46
  - lógica, 39–44
  - operador, *veja* operador equivalência
- equivalência lógica, 42, 43, 47, 50, 127
- escopo
  - de quantificador, 56
- esfera, 110
- esgoto, 231
- estado
  - de um sistema, *veja* informação, capacidade estatística, 17
- estrutura de programa, 208
- estudante, 50–52
- Euclides, 16, 17, 72
- Euler, Leonhard, 208
- exponencial, 158
- fórmula
  - de Bayes, *veja* inferência bayesiana
  - de Euler, 232
  - de Pólya, 222
  - de Tchebychev, *veja* variável aleatória, teorema de Tchebychev
- fórmula de Stirling, 174
- fatorial, 78, 138–139, 157, 158, 167, 173
  - aproximação, 174
  - crescimento, 173
- ! (fatorial), 138
- fechadura, 230
- fecho, 109
  - geral, 108
  - reflexivo, 105, 109
  - simétrico, 106, 109

- transitivo, 106, 109
- feijão, 31
- Fermat, Pierre de, 61
- forma normal
  - conjuntiva, 45–46
  - disjuntiva, 45–46
- FORTTRAN, 141
- Fourier, Joseph, 143
- função, 129–142
  - bijetora, 134–135, *veja* permutação, 146, 220
  - característica, 139
  - chão, *veja* função piso
  - classes de equivalência, 130
  - composição, 132–173
  - contagem, *veja* contagem de funções
  - contra-domínio, *veja* função, imagem
  - de Ackermann, 161
  - definição, 129
  - definição alternativa, 130
  - domínio, 130–133
  - elemento fixo, 135
  - expressões lógicas, 134
  - gama, 138
  - idempotente, 133
  - igualdade, 130
  - imagem, 130, 132, 133
    - de conjunto, 131
  - imagem inversa
    - de conjunto, 131
  - injetora, 133–134, 244
  - injetora, 134
  - intersecção, 131, 134
  - inversa, 131, 134, 135
  - involução, 136
  - logaritmo, 133
  - notação ( $\rightarrow$ ), 129
  - permutação, *veja* permutação, 173
    - ciclo, 136
    - fecho reflexivo, 136
    - fecho transitivo, 136
    - involução, *veja* função, involução
    - potência, 136
    - relação de equivalência, 136
  - piso ( $\lfloor \cdot \rfloor$ ), 137
  - potência, 133
  - potência de, 133
  - projeção, 133
  - quadrado, 130

- quantificadores, 134
- raiz quadrada, 133
- relação, 134
- relação de equivalência, 130
- restrição, 131, 134
- seno, 130
- sobre, *veja* função sobrejetora
- sobrejetora, 134–135, 243
  - contagem, 175
- solo, *veja* função piso
- teto ( $\lceil \cdot \rceil$ ), 137
- Gödel, Kurt, 246
- $\Gamma$  (função gama), 138
- generalização
  - existencial, 70
  - universal, 69
- geometria, 15–17
- Goldbach, Christian, 61
- gorila, 52
- grafo, 207–237
  - $k$ -coloração, 237
  - $n$ -cubo, 231
  - árvore, 224, 225, 232
  - definição, 224
  - número de arestas, 225
- acíclico, 215, 224
- adjacência
  - matriz, *veja* grafo, matriz de adjacência
- arco, *veja* grafo, aresta
- aresta, 207, 209
  - antiparalela, 210
  - de corte, 223
  - destino, 209
  - direção, 209
  - extremos, 209
  - laço, 210
  - múltipla, 210, 219
  - orientação, 209
  - origem, 209
  - paralela, 210, 219
  - ponte, 224
- automorfismo, 220
- bipartido, 226, 230, 231
  - caracterização, 226
  - coloração, 237
  - completo, 226, 231, 235, 237
  - conexo, 234

- definição, 226
- caminho, 214, 215, 224
  - comprimento, 226
  - hamiltoniano, 230
  - orientado, 223
- ciclo, *veja* grafo, circuito
- circuito, 215, 223, 229, 232, 234, 237
  - hamiltoniano, 229
- coloração, 236–237
  - de faces, 236
  - de vértices, 237
- complementar, 218
- complemento, *veja* grafo complementar
- completo, 213, 228, 230, 234, 235
  - coloração, 237
- componente, 222–224
  - fechamento, 222
  - fortemente conexa, 223
- componentes conexas, 225
- conexidade, *veja* grafo conexo
- conexo, 222–224, 234
  - definição, 222
  - fortemente, 223
  - fracamente, 224
- contagem, 222
- convenções do livro, 209
- de Hamilton, *veja* grafo hamiltoniano
- de Petersen, 234
- definição, 209–211
  - informal, 207
- desconexo, 223
  - totalmente, 223
- desenho, 207–209, 227, 231
- diferença, 223
- dual, 235, 237
- em computação, 208
- euleriano, 226–228, 230, 231
  - definição, 226
- face, 232, 235
  - externa, 232
- finito, 210
- fortemente conexo, *veja* grafo conexo, fortemente
- fracamente conexo, *veja* grafo conexo, fracamente
- função
  - de incidência, 209
- grafo-circuito, 225

- grau do vértice, 225
- hamiltoniano, 228–231
  - definição, 229
  - teste, 230
- incidência, 211
  - matriz, *veja* grafo, matriz de incidência
- induzido
  - por vértices, 223
- infinito, 210
- isomorfismo, 219–222, 226, 234
  - algoritmo, 220
  - definição, 220
  - motivação, 219
- laço, 210, 211
- matriz
  - de adjacência, 218
  - de entrada, 219
  - de incidência, 219
  - de saída, 219
- número cromático, 237
  - limitantes, 237
- não orientado, 213
- não rotulado, 221
  - contagem, 222
  - enumeração, 221
- nulo, 210
- orientado, 209, 213
- passeio, 214
  - atravessa, 214
  - comprimento, 214
  - concatenação, 214, 215
  - fechado, 215
  - início, 214
  - inverso, 214
  - orientado, 215
  - passa por, 214
  - término, 214
  - trivial, 214, 215
  - vértice interno, 214
  - visita, 214
- percurso, 214–215
- planar, 231–236
  - coloração, 237
  - definição, 231
  - dual, *veja* grafo dual
  - número de arestas, 233
- regular, 213, 215, 226
- relação

- de adjacência, 211
- de chegada, 211
- de dominância, 211
- de incidência, *veja* grafo, incidência
- de saída, 211
- representação
  - planar, *veja* grafo, desenho
- representação matricial, 218–219
- rotulado, 221
  - contagem, 222
  - enumeração, 221
- sem arestas, 210
- sequência
  - de graus, 213
- simples, 210, 213, 224
- subdivisão, 234
- subgrafo, 216, 222, 225, 234, 235
  - diferença, 218
  - espalhado, 216
  - gerador, 216
  - intersecção, 217
  - união, 217, 223
- tour
  - de Euler, *veja* grafo, tour euleriano
  - euleriano, 226, 228
- trilha, 214, 215
  - de Euler, *veja* grafo, trilha euleriana
  - euleriana, 226
- vértice, 207, 209
  - adjacente, 211
  - atinge, 211
  - conectado, *veja* grafo, vértice ligado, 223
  - domina, 211
  - grau, 211, 215, 230
  - ligado, 222, 223
  - vizinho, 211
- vazio, 223
- Guthrie, Francis, 61, 236
- hacker, 201
- Haken, Wolfgang, 61, 236
- Hamilton, William Rowland, 229
- Hasse, Helmut, 119
- Hilbert, David, 240
- hipótese, 33
  - do contínuo, 246
- hotel, 240
- icosaedro, 231

- idempotência
  - da intersecção, 24
  - da união, 24
- igualdade
  - de funções, 130
  - de sequências, 140
- imagem, *veja* relação, contradomínio
  - de conjunto
    - por função, *veja* função, imagem de conjunto
    - inversa, *veja* relação, imagem inversa
- implica, *veja* operador implica
- implicação, *veja* operador implicação
  - lógica, 43–44
- implicação lógica, 43, 50
- inclusão
  - de conjuntos, 19
  - definição, 21
  - estrita
    - definição, 21
    - notação ( $\subset$ ,  $\supset$ ), 21
    - notação ( $\subseteq$ ,  $\supseteq$ ), 21
- inclusão e exclusão, 185
- indução, 20, 75–92, 178, 186
  - ao contrário, 82
  - base genérica, 79
  - boa ordenação, 89–90
  - completa, 85–91
  - conjunto, 81
  - definição, 76
  - desigualdade, 79, 81
  - equivalência das formas, 89–91
  - forte, *veja* indução completa
  - incorreta, 81–83, 88
  - motivação, 75
  - passo genérico, 80
  - por conjuntos, 78
  - troca de variável no passo, 80
  - variações, 78–81
- indução completa
  - base genérica, 86
- inferência bayesiana, 201–203
  - antecedente, 202
  - consequente, 202
  - fórmula, 201
  - interpretação, 203
  - preconceito, 203
  - probabilidade

- a posteriori, 202, 203
- a priori, 202, 203
- infinito
  - como limitante, 27
- inflação, 30
- informação, 203–206
  - capacidade, 203–204
    - versus* quantidade, 205
  - aditividade, 204
  - de sistema físico, 203
  - de sistemas independentes, 204
- quantidade, 203, 205
  - versus* capacidade, 205
- definição, 205
- esperada, *veja* entropia
- injeção, *veja* função injetora
- instanciação
  - existencial, 70
  - universal, 69
- integral, 153, 155
- inteiro
  - ímpar, 20, 63, 64, 67, 69, 116
  - definição, 60
  - congruência, 124
  - múltiplo, 123, 124
- par, 61–64, 69, 73, 94, 95, 116, 121
  - definição, 60
  - pitagórico, *veja* tripla pitagórica
  - primo, *veja* primo
- internet, 208, 231
- interseção, *veja* conjunto
- $\cap$ , *veja* conjunto, interseção
- intersecção
  - de grafos, *veja* grafo, subgrafo, intersecção
- intervalo
  - de números reais, 27
- inversa
  - de implicação, *veja* proposição inversa
  - de relação, *veja* relação inversa
- involução, *veja* função, involução
- iteração
  - de conjunção, 158
  - de disjunção, 158
  - de disjunção exclusiva, 158
  - de intersecção, 158
  - de operação associativa, 158
  - de união, 158
  - vazia, 158

- Java (linguagem), 141
- jogo, 229
- jogos de azar, 188
- Königsberg, 208, 210, 226
- Kempe, Alfred Bray, 236
- Knuth
  - Donald Erwin, 175
- Kuratowski, Kasimierz, 234
- lógica, 15, 17–18, 29–57, 59–74
  - clássica, 17
  - de predicados, 47–57
  - proposicional, *veja* cálculo proposicional
  - relação com probabilidade, 192
- lâmpada, 191, 205
- ladrão, 230
- Laplace, Pierre-Simon, 201
- laptop, 32
- laranja, 171, 176
- lei
  - da adição, 43
  - da associatividade, 41
  - da comutatividade, 40
  - da contrapositiva, 41
  - da distributividade, 41
  - da dominação, 40
  - da idempotência, 40
  - da identidade, 40
  - da implicação, 41
  - da redução ao absurdo, 41, 44
  - da simplificação, 43
  - de De Morgan, 41, 51
  - do modus ponens, 43
  - do modus tollens, 43
  - silogismo disjuntivo, 43
  - silogismo hipotético, 43
- Leibniz, Gottfried Wilhelm, 182
- leis de absorção, 42
- lema, 60
- letra, 209
- limitante
  - de somatória, *veja* somatória, majoração
  - inferior
    - de sequência, 167
  - superior
    - de sequência, 166
- linguagem natural
  - interpretação, 51–53

lista, *veja* sequência finita

logaritmo, 150, 154–158

    como função, *veja* função logaritmo

Londres, 29

Lucas, Edouard, 61

máximo, 120–121, 123

    de dois números, 66

    divisor comum, 17

média

    aritmética, 64, 68, 167

    geométrica, 167

métodos de demonstração, *veja* demonstração,  
    método

módulo

    um inteiro, *veja* inteiro, congruência

    uma relação, 124

múltiplo, 60, 65, 70

    definição, 60

mínimo, 120–121, 123

    de dois números, 66

mãe, 52

maçã, 171, 176

macaco, 29, 51, 54

majoração

    de somatória, *veja* somatória, majoração

malha viária, 208

malote, 35

mamífero, 15, 29

mapa, 236

matriz

    booleana, 103

    composição, 103

    conjunção, 104

    disjunção, 104

    intersecção, 104

    produto, 103

    união, 104

    de relação, 103

    quadrada, 73

maximal, 122–123

meninos e meninas, 174

Mersenne, Marin, 61

mesa

    redonda, 165

minimal, 122–123

minoração

    de somatória, *veja* somatória, majoração

modus ponens, 43, *veja* lei do modus ponens  
 modus tollens, *veja* lei do modus tollens  
 moeda, 190, 193, 203, 204  
     falsa, 84, 88  
 Moivre, Abraham de, 174  
 molécula, 208  
 montanha russa, 174  
 Montevidéu, 30  
 morcego, 15, 29  
 Morgan, *veja* De Morgan  
 mostrador de quilometragem, 204  
 multiconjunto, 139–140, 180  
 multiplicidade, *veja* multiconjunto

$\mathbb{N}$  (números naturais), *veja* número natural  
 número

    ímpar, *veja* inteiro ímpar, 82, 88  
     de Fibonacci, 160  
     definição, 88  
     fórmula, 88  
     limite superior, 88  
     operações, 88  
     potência, 88  
     produto, 88

    somatória, 88  
     de fibonacci, 163  
     de Mersenne, 61  
     divisor, 78  
     em binário, 88  
     harmônico, 150, 151, 154, 156  
     ímpar  
         de zeros, 162  
     inteiro, 64, 88, 240  
         conjunto ( $\mathbb{Z}$ ), 20  
         partição, 25  
     irracional, 64, 72, 73  
     natural, 76, 240  
         conjunto ( $\mathbb{N}$ ), 20  
     par, *veja* inteiro par, 88, 240  
     pitagórico, *veja* tripla pitagórica  
     primo, *veja* primo, 86, 88, 159  
     racional, 63, 64, 126  
         conjunto ( $\mathbb{Q}$ ), 20  
     real, 73  
         conjunto ( $\mathbb{R}$ ), 20  
         partição, 28  
 número par, 33  
 número primo, 17

## números

cubos, 186

divisibilidade, 185, 186

quadrados, 186

negação, *veja* operador negação, 53, 56

de quantificador, 50

negação dupla, 40

Newton, Isaac, 177

nome, 172

nota, 81

notação decimal, 123

nucleotídeo, 204

octaedro, 204, 231

odômetro, 204

## operação

aritmética, 17

## operador

associativo, 36, 41

bicondicional, *veja* operador equivalência

comutativo, 40

condicional, *veja* operador implicação

conjunção, 65

em probabilidade, 190

conjunção (“e”,  $\wedge$ ), 31–32, 35–44, 46, 47

de implicação, 101

diferença, 63

de grafos, *veja* grafo, subgrafo, diferença

disjunção, 65

em probabilidade, 189, 190

disjunção (“ou”,  $\vee$ ), 32, 34–44, 46, 47

disjunção exclusiva, 49

em probabilidade, 189

disjunção exclusiva ( $\leftrightarrow$ ), 35disjunção exclusiva ( $\oplus$ ), 35–42, 44, 47disjunção exclusiva (“ou exclusivo”,  $\oplus$ ), 41

distributivo, 41

dual ( $\otimes$ ), 47elemento neutro, *veja* elemento neutro

equivalência, 60, 68

equivalência ( $\leftrightarrow$ ), 34–35equivalência (“se e somente se”,  $\leftrightarrow$ ), 41equivalência (“sse”,  $\leftrightarrow$ ), 35, 36, 38–42, 44, 47genérico ( $\odot$ ), 47

idempotência, 40

implica (“se”,  $\rightarrow$ ), 33–44, 47

implicação

- prova, *veja* prova de implicação
- intersecção, 63
  - de grafos, *veja* grafo, subgrafo, intersecção
- lógico, 30–36
- não-e (“nand”,  $\overline{\wedge}$ ), 38, 47
- não-e (“nor”,  $\overline{\vee}$ ), 42
- não-ou (“nor”,  $\overline{\vee}$ ), 38, 42, 47
- negação
  - em probabilidade, 189
- negação (“não”,  $\neg$ ), 32, 34, 35, 37–39, 41–44, 47
- precedência, 35–36
- união, 63
  - de grafos, *veja* grafo, subgrafo, união
- ordenação, 135
- Péter
  - Rózsa, 161
- Pólya, George, 82, 222
- palavra, *veja* sequência finita, 209
- papagaio, 54
- par ordenado, 116, 141
  - definição, 26
- Paradoxo
  - de Russel, 20
  - do Barbeiro, 20
- paradoxo
  - do barbeiro, 37
  - do hotel infinito, 240
  - dos cavalos, 81
- parafuso, 190, 191, 198
- parte
  - de partição, 25
- partição, 146
  - de conjunto, *veja* conjunto, partição
  - de um conjunto, 125–127
  - rotulada, 179–180
- Pascal, Blaise, 177
- PBO, *veja* indução, boa ordenação
- Peano, Giuseppe, 76
- pentágono
  - construção, 15
- perfeito, 52
- Permutação
  - circular, 180
  - com elementos indistinguíveis, 181
- permutação, 111, 135–136, 172–174
  - com casal, 173

- composição, 135, 136
- das faces de um dado, 136
- de letras, 172
- de termos em somatória, 146
- definição, 135, 172
- desarranjo, *veja* desarranjo
- do conjunto vazio, 173
- dos lados de uma tampa, 136
- inversa, 135
- sem elemento fixo, *veja* desarranjo
- $\in$  (pertence), 19
- $\notin$  (não pertence), 19
- pertinência
  - em conjunto, 19
- pessoa conhecida, 218
- Petersen, Julius, 234
- PIC, *veja* indução completa
- PIF, *veja* indução completa
- PIM, *veja* indução, definição
- Pitágoras
  - teorema de, 16
- placa de carro, 172
- poço de petróleo, 194
- polígono
  - convexo, 80
  - diagonais, 80
  - soma de ângulos, 80
- poliedro
  - definição, 231
  - platônico, 231
- polinômio
  - característico, 163
- ponte
  - de Königsberg, 208, 210, 226
- ponto, 16
- poset*, *veja* conjunto parcialmente ordenado
- $\ni$  (possui), 19
- $\nexists$  (não possui), 19
- postulado, *veja* axioma
- potência
  - de 2, 78
  - de binômio, 177
  - de conjunto, *veja* conjunto potência
  - de função, *veja* função, potência de
- Potência cadente, 175
- $2^A$ , *veja* conjunto potência
- $\mathcal{P}(A)$ , *veja* conjunto potência
- pratos, 165

- preconceito, 203
- predicado, 47, 60
- premissa, 33
- presidente, 94
- primo, 61, 69–73
  - definição, 60
- princípio
  - aditivo
    - da contagem, 183
  - da boa ordenação, *veja* indução, boa ordenação
  - da complementaridade, 189
  - da contagem
    - aditivo, *veja* princípio aditivo da contagem
    - subtrativo, *veja* princípio subtrativo da contagem
  - da exaustão, 189
  - da exclusão mútua, 189
  - da inclusão e exclusão, 185–186, 190
  - da independência, 190, 191
  - da indução completa, *veja* indução completa
  - da indução forte, *veja* indução completa
  - da indução matemática, *veja* indução, definição
  - das casas de pombos, *veja* princípio dos escaninhos
  - caninhos
    - das gavetas, *veja* princípio dos escaninhos
    - do pombal, *veja* princípio dos escaninhos
    - dos escaninhos, 84
  - multiplicativo
    - da contagem, 171–172
  - subtrativo
    - da contagem, 184
  - princípio da independência, 193
- princípio
  - subtrativo
    - da contagem, 185
- probabilidade, 187–206
  - a posteriori, *veja* inferência bayesiana, probabilidade a posteriori
  - a priori, *veja* inferência bayesiana, probabilidade a priori
  - como percentagem, 188
  - condicional, 200–201
    - definição, 200
    - inversão, 201
    - justificativa, 200
  - da conjunção, 190, 191
  - da disjunção, 190, 191

- definição, 188
- distribuição, 192
  - definição, 192
  - degenerada, 206
  - entropia, *veja* entropia
  - uniforme, 188, 190, 206
- em jogos de azar, 188
- fórmula de Bayes, *veja* inferência bayesiana
- inferência bayesiana, *veja* inferência bayesiana
- justificativa, 187
- princípio da complementaridade, 189
- princípio da exaustão, 189
- princípio da exclusão mútua, 189
- princípio da inclusão e exclusão, 190
- princípio da independência, 190, 191
- princípio de exclusão e inclusão, 192
- relação com lógica, 192
- subjetividade, 189
- teorema de Bayes, *veja* inferência bayesiana
- variável aleatória, *veja* variável aleatória
- problema
  - das quatro cores, *veja* grafo, coloração de faces
- produtória, 157–158, 162–163
  - analogia com somatória, 158
  - básica, 157
  - de constante, 157
  - de exponenciais, 158
  - de potências, 157
  - de progressão aritmética, 157, 158
  - definição, 157
  - fórmula, 157
  - majoração, 158
  - manipulação, 158
  - vazia, 157
  - via logaritmos, 158
- produtório, *veja* produtória
- produto
  - cartesiano, 124, 129
- produto cartesiano, 26–27, 93, 241
  - ênupla, 26
  - de  $n$  conjuntos, 26
  - de dois conjuntos, 26
  - definição, 26
  - iterado, 26
  - par ordenado, 26
  - tamanho, 26

## progressão

- aritmética, 161
  - definição, 160
  - incremento, 160
  - passo, 160
  - termo inicial, 160
- geométrica, 163
- definição, 160
  - razão, 160
  - termo inicial, 160

## proposição

- aberta, 47–55
- atômica, 30
- auto-referente, 37
- contraditória, *veja* contradição
- contrapositiva, 34, 37
- definição, 29–30
- fechada, 47, 55
- inversa, 34, 37
- mais forte, 34
- mais fraca, 34
- possível, 32
- recíproca, 34, 37
- simples, 30

tautológica, *veja* tautologia

transformação, 38

viável, 32

prova, 17, *veja* demonstração

de equivalência, 67

de implicação

contrapositiva, 63

por absurdo, 64

por vacuidade, 101

qualidades, 61

Python, 141

$\mathbb{Q}$  (números racionais), *veja* número racional

quádrupla, *veja* ênupla, 110

quíntupla, *veja* ênupla

quadrado perfeito, 66, 69, 71, 94

quando, *veja* operador implica

quantificador

de existência única, 49

em conjunto vazio, 50

escopo, 56

existencial, 48–50, 53, 70

múltiplo, 69

universal, 48, 50, 53

- suspensão, 69
- quebra-cabeças, 227, 228, 231
- queijo, 56
- $\mathbb{R}$  (números reais), *veja* número real
- régua e compasso, 15
- rótulo, 135
- raiz quadrada, 93
  - como função, *veja* função raiz quadrada
  - como relação, 130
- rato, 56
- razão áurea, 163
- recíproca, *veja* proposição recíproca
- recíproco
  - de um número, 88
- recho, 105
- recorrência, 160–167
  - aditiva, 161–162
  - resolução, 161
- linear
  - homogênea, 163
  - não homogênea, 165
  - termo independente, 165
- majoração, 166–167
- minoração, 166–167
- multiplicativa, 162–163
- resolução, 161–166
- rede, 224
- redução ao absurdo, 41, 44, *veja* prova, implicação
  - por absurdo
- refutação, *veja* conjectura refutada
- regra de inferência, 15
- relação, 93–113, 115–127
  - anti-simétrica, 100, 101, 105, 115, 116, 118, 170
  - aproximadamente igual, 127
  - binária, 93
  - completa, 124
  - composição, 102, 112, 113, 132, 135
    - associatividade, 100
    - com identidade, 98
    - com inversa, 98
    - de potências, 100
    - definição, 96, 97
    - distributiva sobre união, 100
    - domínio, 97
    - e inclusão, 99
    - e intersecção, 100

- em forma matricial, 103
- imagem, 97
- inversa da, 99
- não-comutatividade, 97
- notação alternativa, 98
- potência, 99
- repetida, *veja* potência
- composição ( $\circ$ ), 96–100
- conjunção de, 104
- contém ( $\supseteq$ ), 96
- contém estritamente ( $\supset$ ), 96
- contagem, *veja* contagem de relações
- contido, 115, 117, 123, 124
- contido ( $\subseteq$ ), 94
- contradomínio, *veja* relação, imagem
- de adjacência, 221
- de equivalência, 124–127, 132, 221, 223
  - classe, *veja* classe de equivalência
  - definição, 124
  - entre pares, 126, 127
- de ordem, 115–123, 245
  - alfabética, 117, 121
  - definição, 115
  - entre pares, 116, 117
  - estrita, 116, 117
  - lexicográfica, 117
  - parcial, 118
  - restrição, 116
  - subcadeia, 116
  - total, 117, 118, 120, 135
  - união, 116
- definição, 93
- dentro de, 116, 117
- diagrama, 93
  - de Hasse, 119
- disjunção de, 104
- divide, 120
- divisível, 123
- divisibilidade, 115
- domínio, 94, 95
- entre números, 17
- fecho, *veja* fecho
- fecho simétrico, 211
- função, *veja* função
- identidade, 95, 101, 124
- igual ( $=$ ), 96
- igualdade, 95
- imagem, 94, 95

- de conjunto, 131
- imagem inversa, 96
  - de conjunto, 131
- intersecção de, 104
- inversa, 95–96, 101, 111, 121, 131, 134, 135
  - potência, *veja* relação, potência negativa
- irreflexiva, 100, 101, 105, 116, 170
- maior, 116
- maior ou igual, 121
- menor, 94, 116
- menor ( $<$ ), 94, 96
- menor ou igual, 115, 117, 121
- menor ou igual ( $\leq$ ), 94
- menor que, 117
- $n$ -ária, 110–113
  - $i$ -ésimo domínio, 110
  - definição, 110
  - grau, 110
  - junção, 111–113
  - ordem, 110
  - permutação de componentes, 111
  - projeção, 110, 111
  - restrição, 111
  - paralela, 124
  - pertence ( $\in$ ), 94, 96
  - possui ( $\ni$ ), 96
  - potência, 100, 102, 107, 109
    - negativa, 100
  - raiz quadrada, 130
  - reflexiva, 100, 101, 105, 108, 115, 118, 124, 170
  - representação matricial, 103–105
  - restrição, 95, 115, 131
  - simétrica, 100, 101, 105, 124, 170
  - sobre, 94
  - tipos, 100–105
  - transitiva, 100–102, 115, 116, 118, 119, 124
  - união de, 104
  - vazia, 95
- repetição, *veja* iteração
- representante
  - de classe de equivalência, 125
- restrição
  - de relação, *veja* relação, restrição
- retórica, 15
- reta, 16
  - dividindo plano, 77, 161

paralela, 16, 124  
 perpendicular, 16  
 reunião, 33  
 Rio de Janeiro, 29  
 Robertson, Neil, 61, 236  
 roleta, 184  
 ruminante, 53  
 Russel, Bertrand, 20  
  
 séptupla, *veja* ênupla  
 série, *veja* somatória infinita  
 Sócrates, 15  
 sêxtupla, *veja* ênupla  
 síntese de operadores, 45–46  
 Sanders, Daniel, 61  
 Sanders, Daniel P., 236  
 Schröder, Ernst, 245  
 se e somente se, *veja* operador equivalência  
 selos, 80  
 seno, 130  
 sentença declarativa, 29  
 sequência, 242  
     índice, 140, 159  
         inicial, 140–142, 159

bi-infinita, 159  
 comprimento, 141  
 de bits, 121, 123  
 elemento, 159  
     índice, 140, 159  
     valor, 140, 159  
 finita, 140–142  
     comprimento, 141  
     concatenação, 141, 142  
     definição, 140  
     notação  $(\cdot, \cdot, \dots)$ , 140  
     notação  $[\cdot, \cdot, \dots]$ , 141  
     notação  $\langle \cdot, \cdot, \dots \rangle$ , 141  
     vazia, *veja* sequência vazia  
 igualdade, 140  
 infinita, 159–167  
     índice inicial, 159  
     completando, 160  
     definição, 159  
     dos primos, 159  
     por fórmula, 159  
 $n$ -ésimo termo, 141  
 notação  $x_n$ , 140  
 ordem dos termos, 140

- repetição de termos, 140
- sem ‘e’ repetidos, 164
- termo, 140, 159
  - índice, 140, 159
  - geral, 159
  - valor, 140, 159
- trivial, 26, 141
- vazia, 26, 117, 141
  - comprimento, 141
  - concatenação, 142
- vs. conjunto, 141
- Seymour, Paul, 61
- Seymour, Paul D., 236
- Shannon, Claude, 203
- sigma ( $\Sigma$ ), *veja* somatória
- silogismo
  - disjuntivo, 43
  - hipotético, 43
- sistema binário, 204
- sistema completo, 46
- soma, *veja* somatória
- somatória, 143–157, 161–162
  - índice, 143, 144, 149
  - índice final
    - infinito, 156
- associatividade, 146
- básica, 145
- comutatividade, 146
- de ímpares, 144
- de constante, 145
- de cubos, 81
- de exponencial, 145, 147, 148
- de frações, 148
- de números de Fibonacci, 148
- de PG, 78
- de potências, 145–147, 154
- de potências crescentes, 147, 148
- de potências de 2, 145, 147
- de primos, 144, 145
- de progressão geométrica, 151
- de progressão aritmética, 145, 148, 157, 158
- de progressão geométrica, 145, 147, 148, 156, 157
- de quadrados, 147
- de senos, 148
- decomposição de domínio, 146
- definição, 143
- distributividade, 146, 150

divergente, 194  
 domínio, 144  
 fórmula, 145  
 fator comum, 146  
 fatoração, 150  
 índice final, 144  
 índice inicial, 144  
 infinita, 156–157  
     dos inversos, 194  
 limitante, *veja* somatória, majoração  
 múltipla, 149–150  
     definição, 149  
     troca de ordem, 149, 150  
 majoração, 151–156  
     pelo maior termo, 151  
     por indução, 151  
     por integral, 153–154  
     por somatória infinita, 156  
     termo a termo, 151, 154  
 manipulação, 145–148  
 minoração, *veja* somatória, majoração  
     por integral, 155–156  
 notação, 143  
 ordem dos termos, 146

produto, 150  
 propriedades, 145  
 telescópica, 146–148  
 termo, 143  
 troca de índice, 145, 146, 149  
 troca de domínio, 146, 149  
 vazia, 144  
 somatório, *veja* somatória  
 Stirling, James, 174  
 sub-conjunto, *veja* inclusão  
     definição, 21  
     próprio  
         definição, 21  
 sub-palavra, 120  
 subcadeia, 142  
 subconjunto, 63  
 subsequência, 142, 159  
  
 Távola Redonda, 228  
 tabela-verdade, 31–35, 38–42, 44–46  
 tabuleiro, 165  
 tampa de caixa, 136  
 tanque, 35  
 tatu, 161, 164

- tautologia, 38–40, 43, 50
- taxa de juros, 29, 30
- Tchebychev, Pafnuti, 198
- teorema, 16, 60
  - da infinidade de primos, 72
  - de Bayes, *veja* inferência bayesiana
  - de Cantor, 243–244
  - de Euler
    - para grafos planares, 232
    - para tours em grafos, 227
  - de Fermat, *veja* conjectura de Fermat
  - de Kuratowski, 234
  - de Pólya, 222
  - do deserto de primos, 71
- teoria
  - da computabilidade, 17
  - da informação, 17, *veja* informação
  - da probabilidade, 17
  - de conjuntos, 17
  - dos conjuntos, 19–28
  - dos grafos, *veja* grafo
- tese, 33
- tetraedro, 231
- Thomas, Robin, 61, 236
- tijolos, 31
- torre
  - de xadrez, 174
- triângulo equiângulo, 52
- treliça, 208
- triângulo, 16
  - congruência, 16
  - retângulo, 16
- tripla, *veja* ênupla, 110
- troca, *veja* permutação
- troco, 81
- união, *veja* conjunto
  - de grafos, *veja* grafo, subgrafo, união
- $\cup$ , *veja* conjunto, união
- $\mathcal{U}$ , *veja* conjunto universal
- urna, 78
- vacuidade, 50
- valor absoluto, 73
- valor lógico, 30
  - falso, 158
  - verdadeiro, 158
- valor-verdade, 30

- variáveis independentes, *veja* variável aleatória, independência
- variável, 17
  - aleatória, 192–200
    - contínua, 192
    - discreta, 192
  - amarrada, 55, 60
  - lógica, 31
  - livre, 55, 60
- variável aleatória
  - coeficiente de correlação, *veja* correlação
  - correlação, 200
  - covariância, 199
  - definida por fórmula, 192, 195
  - desvio padrão, 198–199
    - definição, 198
    - teorema de Tchebychev, 198
  - esperança, *veja* variável aleatória, valor esperado
  - independência, 193
  - média, *veja* variável aleatória, valor esperado
  - mediana, 196
  - moda, 197
  - teorema de Tchebychev, 198
  - valor esperado, 193–195
    - com distribuição uniforme, 194
    - função afim, 195
    - função linear, *veja* função afim
    - função não linear, 195
    - infinito, 194
    - soma, 195
  - valor médio, *veja* variável aleatória, valor esperado
  - valor mais provável, *veja* moda
  - variância, 197–200
    - definição, 197
    - função afim, 198
    - infinita, 197
    - justificativa, 197
    - sinal, 197
    - soma, 198
  - vetorial
    - valor esperado, 195
- variável aleatória
  - vetorial, 195
- Venn, John, 23
- voto, 37

xadrez, 174, 231

$\mathbb{Z}$  (números inteiros), *veja* número inteiro

zebra, 53

Zermelo, Ernest, 19

zoológico, 29