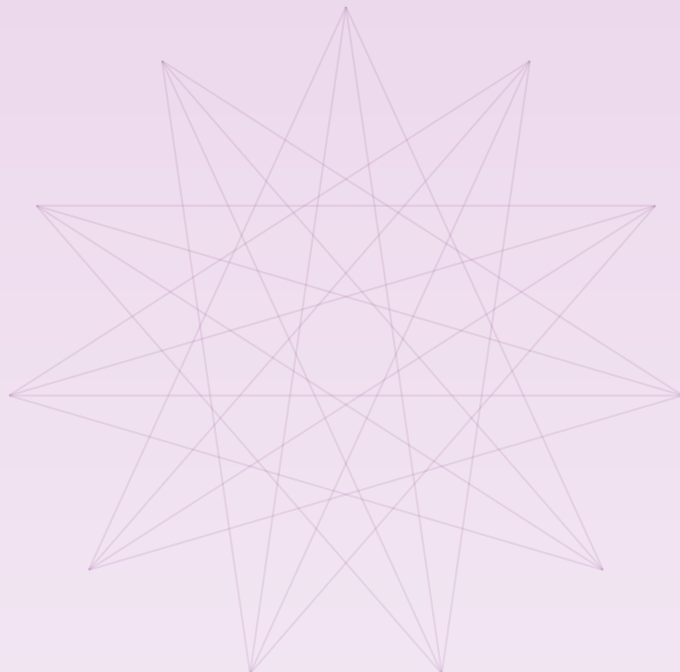


MARÇO DE 2026



Um passeio pela Matemática

Walner Mendonça (UFC)

Guilherme Mota (USP)

Sumário

Prefácio	3
1 Primeiras provas matemáticas	4
1.1 Somando inteiros positivos	5
1.1.1 Uma primeira prova	5
1.1.2 Uma prova algébrica	6
1.1.3 Uma prova diferente	8
1.2 Trabalhando a intuição	8
1.2.1 Um desafio linguístico	9
1.2.2 Um problema sobre chapéus	10
1.2.3 O problema de Monty Hall	11
1.2.4 Um problema sobre amigos e estranhos	12
1.3 Demonstrações e escrita matemática	14
1.3.1 O Teorema de Pitágoras	15
1.3.2 Infinitude dos números primos	17
1.3.3 Uma observação sobre polinômios	18
2 Lógica Proposicional	20
2.1 Proposições compostas	22
2.1.1 Conjunção e disjunção	22
2.1.2 Operadores condicionais	27
2.2 Equivalência lógica	31
2.3 Predicados e quantificadores	34
2.4 Estratégias de prova	41
2.4.1 Direta	41
2.4.2 Contrapositiva	42
2.4.3 Contradição	43
2.5 Escolhendo a melhor estratégia de demonstração	44

3	Teoria básica de conjuntos	48
3.1	Operações com conjuntos	49
3.1.1	Conjuntos comparáveis	52
3.1.2	Mais operações e identidades fundamentais	54
4	Princípio da Casa dos Pombos	57
4.1	Aplicações do Princípio da Casa dos Pombos	59
	Índice Remissivo	65

Prefácio

Neste documento você encontrará as notas de aula da disciplina MAC0105 - Fundamentos de Matemática para a Computação. O objetivo principal deste material é fornecer a base matemática e formal, além do raciocínio rigoroso, necessários para o estudo da Ciência da Computação. Mais do que isso, esperamos que você leitor(a) consiga apreciar a beleza e a importância da matemática.

Ao longo da leitura destas notas, você será apresentado(a) a conceitos essenciais. Iniciaremos com a compreensão do que constitui uma *prova matemática*, seguida pelos estudos de *conjuntos*, em que introduziremos alguns elementos básicos para trabalharmos. Feito isso, discutimos um pouco de *lógica proposicional* e nos aprofundaremos em diversos *métodos de provas*, estratégias que utilizaremos para conseguir demonstrar os resultados. Além disso, nos aprofundaremos no estudo mais detalhado de *predicados e quantificadores*.

Avançando no conteúdo, exploraremos as estruturas e relações entre elementos por meio do estudo de *relações e funções*. Veremos também técnicas de contagem fundamentais, como o *Princípio da Casa dos Pombos*, e uma poderosa ferramenta de demonstração, a *indução matemática*, o que encerra a primeira metade do curso.

Na segunda metade do curso, detalharemos propriedades estruturais essenciais através do estudo de *relações de equivalência*, *classes de equivalência* e *partições*, além de introduzir conceitos de *aritmética modular*. Em seguida, apresentamos *ordens e fechos*, e também *sequências e subsequências*. Por fim, consolidaremos as noções sobre tamanhos de conjuntos e o conceito de infinito discutindo a separação entre *conjuntos enumeráveis e não enumeráveis*.

Esperamos que este material sirva como um guia sólido para a sua jornada no aprendizado da matemática e suas aplicações.

Primeiras provas matemáticas

Um ponto fundamental na Matemática é a linguagem. É através da linguagem que nos comunicamos, que expressamos ideias e construímos conhecimento. Neste primeiro capítulo, nosso objetivo é nos familiarizarmos com a linguagem que vamos utilizar para expressar ideias matemáticas e, mais importante, aprendermos a pensar como matemáticos. O foco central desta jornada será adquirir um conhecimento sólido, desenvolver o raciocínio matemático e o aprendizado das demonstrações matemáticas, enquanto exploramos diversos exemplos envolvendo conceitos matemáticos fundamentais. Demonstrar um resultado matemático não é apenas aplicar regras, mas sim contar uma história lógica e irrefutável que convence o leitor da verdade de uma afirmação. Sempre que possível, queremos obter uma prova que seja a mais clara e elegante possível. Para ilustrar essa arte, começaremos com alguns exemplos simples e clássicos.

Para mergulhar de fato na matemática, algumas dicas iniciais são essenciais. Primeiramente, leia bastante sobre os assuntos estudados e faça muitos exercícios. A matemática exige reflexão profunda: pense e repense muito sobre cada conceito, tentando aproveitar o processo.

Questione constantemente e nunca aceite um argumento sem que você o entenda perfeitamente. O objetivo não é memorizar nada, mas sim aprender genuinamente. Ao longo desse processo, busque desenvolver a sua intuição, mas sempre com cuidado rigoroso para não se enganar. Por fim, a matemática é uma construção coletiva: pergunte, discorde e discuta as ideias com seus colegas.

1.1 Somando inteiros positivos

Um primeiro exemplo que discutimos aqui é um clássico conhecido da maioria de nós. Dado um número inteiro positivo n , como podemos determinar o valor da soma dos primeiros n números inteiros positivos? Em outras palavras, qual o valor de $1 + 2 + \dots + n$?

Alguém pode se sentir tentado a responder imediatamente que o resultado é fácil, pois é dado pela soma dos elementos de uma progressão aritmética de razão 1. Mas isso requer saber o significado de progressão aritmética e também alguma fórmula que dê o valor dessa progressão. Proponho aqui que demos um passo atrás e evitemos alguns conceitos que não discutimos ainda e, mais ainda, que evitemos fórmulas prontas.

1.1.1 Uma primeira prova

Um primeiro passo para começar a desenvolver as ideias para resolver a questão é talvez tentar visualizar de uma forma mais clara essa soma. Escrever exemplos para valores pequenos de n pode nos ajudar a entender melhor o problema, desenhar algumas figuras também pode ajudar a entender melhor o que está por trás da questão. Começemos desenhando os números que estamos somando como bolinhas, linha por linha, para um dado n qualquer. Trabalhar com valores pequenos de n pode ser útil para trabalhar nossa intuição sobre o problema, mas pensar de forma geral nos ajuda a pensar de forma abstrata e entender melhor o problema. Considere a visualização descrita na Figura 1.1.

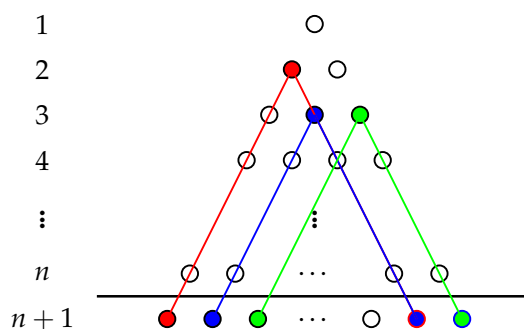


Figura 1.1: Uma visualização de $1 + 2 + \dots + n$ objetos, seguido de uma linha com $n + 1$ objetos.

Perceba que para cada uma das bolinhas nas primeiras n linhas, se traçamos as duas diagonais principais, uma à esquerda e outra à direita, até a linha $n + 1$, estamos associando cada uma das bolinhas nas n primeiras linhas a um único par de bolinhas na linha $n + 1$. Assim, conseguimos perceber que a quantidade de

bolinhas nas n primeiras linhas, que é exatamente $1 + 2 + \cdots + n$, é exatamente igual à quantidade de pares de bolinhas que temos na linha $n + 1$, que contém $n + 1$ bolinhas. Mas quanto é essa quantidade de pares? Dado um conjunto A com n elementos, denotamos por $\binom{n}{2}$ a quantidade de formas de escolhermos dois elementos distintos de A e dizemos n *escolhe 2* para nos referir ao valor de $\binom{n}{2}$.

Note agora que a quantidade de pares de bolinhas que queremos obter é exatamente $\binom{n+1}{2}$. Mas de quantos modos podemos formar pares de um conjunto de $n + 1$ elementos? Bem, podemos primeiramente escolher um elemento a de um total de $n + 1$ elementos, e o segundo elemento b pode ser escolhido de um total de n elementos, uma vez que a já foi escolhido. Essa análise nos dá um total de $n(n + 1)$ pares. Porém, poderíamos ter escolhido primeiro b e depois a na contagem que fizemos, de modo que contamos cada possível par, como o par $\{a, b\}$, duas vezes. Assim, o total de pares possíveis é na verdade $\frac{(n+1)n}{2}$, de modo que acabamos de finalizar nossa primeira demonstração, que $\binom{n+1}{2} = \frac{(n+1)n}{2}$, e temos nosso primeiro resultado abaixo. Uma afirmação verdadeira é chamada de *Teorema*.

Teorema 1.1

Para todo inteiro $n \geq 1$, temos que

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2} = \binom{n + 1}{2}.$$

A prova acima é uma prova elegante, que envolve uma observação esperta, mas não é a mais simples que podemos obter. Para cada resultado matemático podem existir diversas provas diferentes, e cada uma delas lança luz sobre uma técnica diferente, ou sobre alguma ideia ou estratégia que talvez possa ser aplicada em outros problemas.

1.1.2 Uma prova algébrica

A história (talvez apócrifa) conta que Carl Friedrich Gauss, ainda quando era uma criança, deduziu a soma dos primeiros n inteiros positivos ao ter sido solicitado a somar os números de 1 a 100.

A ideia de Gauss surge naturalmente quando visualizamos a soma em que estamos interessados de duas formas diferentes. Seja $S_n = 1 + 2 + \cdots + n$. Podemos

escrever S_n das seguintes formas:

$$\begin{aligned} S_n &= 1 + \textcolor{red}{2} + \textcolor{green}{3} + \dots + (n-1) + \textcolor{brown}{n}, \\ S_n &= n + (\textcolor{red}{n-1}) + (\textcolor{green}{n-2}) + \dots + \textcolor{blue}{2} + \textcolor{brown}{1}. \end{aligned}$$

Somando as duas igualdades acima, “coluna por coluna”, notamos que cada par soma exatamente $(n+1)$. Assim, como a soma S_n tem n termos, obtemos

$$2S_n = (n+1) + (n+1) + \dots + (n+1) = n(n+1),$$

o que conclui a nossa prova, uma vez que implica

$$S_n = \frac{n(n+1)}{2} = \binom{n+1}{2}.$$

Uma prova combinatória

Na Combinatória, é comum provar igualdades algébricas mostrando que ambos os lados da igualdade representam a quantidade de elementos em um mesmo conjunto, mas vistos de formas diferentes.

Seja $C = \{1, 2, \dots, n+1\}$ um conjunto com $n+1$ elementos. O conjunto cujos elementos vamos contar de duas maneiras diferentes é o conjunto S de todos os pares de elementos de C . Vamos contar os elementos de S de duas formas diferentes. Por definição, sabemos que

$$|S| = \binom{n+1}{2}. \quad (1.1)$$

Por outro lado, em todo elemento $\{i, j\}$ de S (cada elemento de S é um par de elementos de C , não se esqueça), existe um elemento que é maior que o outro. Assim, podemos contar os elementos de S da seguinte forma: primeiro escolhemos o maior elemento do par, digamos i , que pode ser qualquer um dos $n+1$ elementos de C , o que nos dá $n+1$ escolhas para o maior elemento do par. Uma vez escolhido i , precisamos ver de quantas formas podemos escolher o menor elemento do par, digamos j . Mas a quantidade de escolhas para j depende de qual foi o valor de i que escolhemos. Mas para qualquer i com $1 \leq i \leq n+1$ que foi escolhido, temos exatamente $i-1$ escolhas para j . Portanto, o total de pares é dado por

$$|S| = \sum_{i=1}^{n+1} (i-1) = 0 + 1 + 2 + \dots + n.$$

Mas note que juntamente com (1.1), a igualdade acima nos dá

$$1 + 2 + \cdots + n = \binom{n+1}{2},$$

o que conclui nossa prova.

1.1.3 Uma prova diferente

Vamos partir agora para uma última prova, que inclui conceitos mais avançados, mas que já podemos abordar agora de uma forma natural. Lembre que $S_n = 1 + 2 + \cdots + n$. Em todas as provas anteriores, assumimos que n era um inteiro positivo e nada mais. Feito isso, conseguimos concluir que para qualquer n que seja inteiro positivo, temos que $S_n = \frac{n(n+1)}{2}$.

Caso tivéssemos tempo infinito à nossa disposição, poderíamos verificar que o resultado vale para $n = 1$, isto é, que $1 = \frac{(1+1)1}{2}$, e assim por diante; verificamos que para $n = 2$, $1 + 2 = 3 = \frac{(2+1)2}{2}$, e assim sucessivamente. Mas como esse não é o caso, essa estratégia não tem chances de funcionar. Mas pensemos na seguinte estratégia: já verificamos que o resultado é válido para $n = 1$, de modo que podemos assumir que $n \geq 2$. Agora, *suponha* que o resultado seja válido para $n - 1$. Ou seja, assumimos que

$$S_{n-1} = 1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}. \quad (1.2)$$

Vamos agora prosseguir para mostrar que $S_n = 1 + 2 + \cdots + n = \frac{(n+1)n}{2}$. Mas ao observar S_n com atenção, notamos que

$$\begin{aligned} S_n &= (1 + 2 + \cdots + (n-1)) + n \\ &= S_{n-1} + n. \end{aligned}$$

Mas por (1.2), podemos substituir S_{n-1} na última igualdade por $\frac{n(n-1)}{2}$, obtendo

$$S_n = \frac{n(n-1)}{2} + n = \frac{n(n-1) + 2n}{2} = \frac{(n+1)n}{2}.$$

1.2 Trabalhando a intuição

Vamos analisar brevemente alguns problemas que têm a capacidade de nos fazer pensar com calma e trabalhar nossa intuição matemática, seja nos forçando a observar com calma as sutilezas do problema, seja nos mostrando que a intuição

pode nos enganar, ou mesmo nos obrigando a traçar alguma estratégia para conseguir avançar no problema.

1.2.1 Um desafio linguístico

Imagine que você está conversando com os amigos em uma noite tranquila em Recife, e de repente um amigo solta a seguinte frase: "Percebi que a palavra 'Pernambuco' não tem letras repetidas. Qual será o tamanho da maior palavra que conseguimos formar em português que não tem letras repetidas?". Como podemos ter uma ideia inicial para trabalhar nessa questão? Bem, uma estratégia inicial é tentar encontrar palavras que não têm letras repetidas. Mas nosso cérebro teria muito trabalho em buscar uma dessas palavras dentre todas que conhecemos. Precisamos de uma estratégia que restrinja o conjunto de palavras que queremos buscar.

Uma ideia é tentar utilizar todas as vogais, para nos permitir ter muitas sílabas. Nosso ponto de partida é conseguir uma palavra com mais de 10 letras, que é o total de letras de 'Pernambuco'. Note que 'Pernambuco' nem contém todas as vogais, de modo que devemos conseguir palavras maiores.

Após pensar um pouco, possivelmente chegamos a palavras como 'computáveis' ou 'republicano', que possuem 11 letras. Mas notando que 'computáveis' está no plural, obviamente podemos fazer o mesmo com 'republicano', obtendo 'republicanos', que possui 12 letras. Temos então uma palavra com 12 letras sem repetições. Mas ok, será que conseguimos encontrar uma palavra maior? Podemos adicionar ao rol de regras que estamos aplicando às palavras que estamos buscando o seguinte: queremos palavras que, além de ter todas as vogais, estejam no plural (terminando com 's') e, para garantir a possibilidade de plural, não podem ter 's' no meio da palavra.

Esse é um problema em que não iremos provar que não existe uma palavra com mais letras do que a maior que encontrarmos, pois certamente podemos formar palavras respeitando as regras do português, mas que ainda nem mesmo existem. Por exemplo, 'blandrifusteco' é uma palavra que respeita as regras do português, mas que não existe (e tem 14 letras). Mas voltando ao mundo real, das palavras que existem, será que conseguimos uma palavra com 13 letras utilizando o refinamento de regras que propomos? A resposta é sim! A palavra 'penduricalhos' tem 13 letras, todas distintas (contém também todas as vogais e é um plural, mas não precisamos disso). Com algum esforço maior, notamos que o diminutivo do particípio plural de expurgar é 'expurgadinhos', que tem 13 letras, todas distintas. Você consegue obter alguma outra palavra com 13 letras sem repetições?

1.2.2 Um problema sobre chapéus

Considere a situação em que quatro prisioneiros, A , B , C e D , estão em um corredor. Três deles (A , B e C) estão em fila, A atrás de B , que está atrás de C , que está de frente para uma parede. O quarto prisioneiro, D , está do outro lado dessa parede e não pode ver nem ser visto pelos outros. Dessa forma, A consegue ver os chapéus de B e C ; B consegue ver apenas o chapéu de C , que não vê o chapéu de ninguém; D , que está do outro lado da parede, não vê o chapéu de ninguém. Sabe-se que há dois chapéus azuis e dois vermelhos, e os prisioneiros conhecem essa distribuição. Eles não podem falar nada a não ser a cor do seu próprio chapéu, caso saibam. Não podem se comunicar de maneira nenhuma e precisam sempre olhar para frente. Eles têm alguns minutos para que um deles fale a cor do próprio chapéu, situação em que todos são libertados! Porém, caso o tempo se esgote ou algum prisioneiro fale a cor errada do seu próprio chapéu, todos os prisioneiros serão executados. Antes de destrinchar a solução correta, vamos avaliar alguns instintos e pensamentos iniciais comuns, mas equivocados, sobre esse problema.

1. “É impossível, pois ninguém tem informações suficientes de início.” Muitas pessoas desistem do problema rapidamente, argumentando que nem C nem D veem nada, B vê apenas um chapéu (o que o deixa com duas possibilidades para o seu próprio chapéu), e A vê dois chapéus (mas se forem um de cada cor, não terá certeza do seu próprio chapéu). O erro aqui é assumir que o jogo acaba no primeiro instante, quando cada prisioneiro analisa a informação que recebe de sua visão, ignorando a atitude dos outros prisioneiros. Como a regra do jogo permite que alguns minutos se passem, o silêncio de algum prisioneiro após um pequeno tempo pode dar alguma informação importante.
2. “O prisioneiro A é a única esperança de salvação.” Como A é o único que enxerga o maior número de chapéus (dois), é natural pensar que toda a responsabilidade cai sobre ele. O problema desse argumento é não perceber que B possui uma vantagem tática: ele pode não ganhar muita informação com o que está vendo, mas pode escutar o que o prisioneiro A faz... ou, na verdade, o que A não faz.

Para resolver esse enigma, precisamos analisar a situação passo a passo, do ponto de vista de alguns prisioneiros. Começemos com A , que pode ver os chapéus de B e C . Como há exatamente dois chapéus de cada cor (vermelhos e azuis), se A visse que B e C têm chapéus da *mesma cor*, ele saberia imediatamente que o seu é vermelho (já que os dois azuis se esgotaram). Nessa situação, A prontamente falaria a cor do seu chapéu e salvaria a todos.

No entanto, suponha que um minuto se passe e *A* permaneça em silêncio. O que esse silêncio significa? Transmite a todos (em especial a *B*) uma informação vital: *A* não viu dois chapéus da mesma cor e não consegue ter certeza da cor de seu próprio chapéu. Logo, *A* está necessariamente vendo um chapéu azul e um vermelho nas cabeças de *B* e *C*. Isso significa que *B* e *C* obrigatoriamente têm chapéus de cores diferentes. O prisioneiro *B*, que é uma pessoa esperta e conhece as regras, rapidamente deduz isso. Com essa nova informação em mente, a tarefa de *B* se torna trivial: ele só precisa olhar para a cabeça de *C*. Se *C* estiver usando um chapéu vermelho, *B* sabe que o seu só pode ser azul. Se *C* estiver usando um chapéu azul, *B* sabe que o seu só pode ser vermelho. Assim, *B* consegue salvar a todos.

Portanto, a partir da dedução de que *A* não pôde responder, o prisioneiro *B* consegue descobrir com 100% de certeza a exata cor do seu próprio chapéu, o que garante a liberdade de todos.

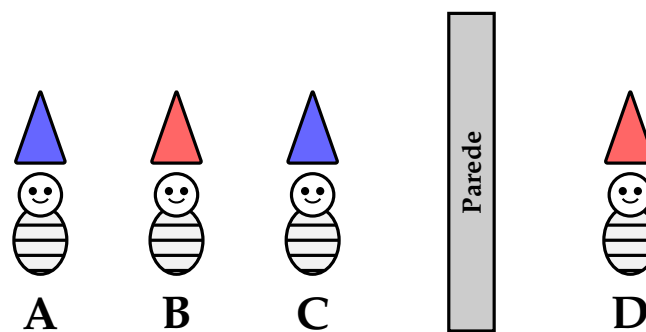


Figura 1.2: Ilustração do problema dos chapéus. *A* vê *B* e *C*, mas não *D*. *B* vê *C*. O prisioneiro *C* vê apenas a parede e *D* está isolado.

1.2.3 O problema de Monty Hall

Discutiremos agora um problema clássico da década de 1970: um participante de um *programa de auditório* escolhe uma entre três portas, digamos, *A*, *B* e *C*. Atrás de uma delas há um prêmio, e atrás das outras, há bodes. A probabilidade de o prêmio estar na porta *A*, *B* ou *C* é de $1/3$. Após o participante fazer sua escolha inicial (digamos, a porta *A*), o apresentador, que sabe o que há atrás das portas, abre uma das outras duas portas, aquela que contém um bode (digamos, a porta *B*). Ele então pergunta: “Você quer trocar para a porta *C* ou mantém sua escolha na porta *A*?”.

Antes de apresentarmos a solução correta, mais uma vez é instrutivo discutirmos alguns pensamentos comuns, porém incorretos, que a maioria das pessoas tem ao se deparar com esse problema pela primeira vez:

1. “Quando restam apenas duas portas, a chance é de 50% para cada uma.” Esse é certamente um dos erros mais comuns. A intuição nos diz que, como há apenas duas opções restantes (a porta escolhida e a porta que continua fechada) e um prêmio, as chances devem ser iguais. O erro aqui está em assumir que a ação do apresentador alterou a probabilidade da porta escolhida inicialmente, ou que ambas as portas restantes são simétricas na forma como a informação foi revelada.
2. “O apresentador não adiciona nenhuma informação nova sobre a minha escolha ao abrir a porta com o bode.” Outro pensamento comum é achar que o fato de o apresentador revelar um bode simplesmente não muda nada sobre a nossa aposta inicial. A falha nesse raciocínio é ignorar que o apresentador *não faz uma escolha aleatória*. Ele é obrigado a abrir uma porta que contenha um bode e que não seja a porta que o participante escolheu. Essa ação deliberada fornece uma informação crucial para o jogo.

Talvez contraintuitivamente para algumas pessoas, a resposta correta é *sim, é melhor trocar!* Também contraintuitivamente, como discutido acima, a chance de vitória não é de 50% para cada porta. Na verdade, com a estratégia de sempre trocar de porta, a probabilidade de vitória é de incríveis $2/3$. Vamos entender isso em detalhes. Ao escolher uma porta no início (digamos, a porta A), a probabilidade de nela estar o prêmio é de $1/3$. Consequentemente, a probabilidade de o prêmio estar em *alguma das outras duas portas* (portas B ou C) é de $2/3$. Até aí, tudo bem. Se o jogo se encerrasse aí, a chance de vitória seria de $1/3$ e a de derrota seria $2/3$.

Mas o jogo não se encerra aqui. O apresentador abre a porta B para revelar um bode e agora tomamos a decisão de trocar de porta. Se o prêmio estivesse na porta A, que escolhemos inicialmente, ao mudar de porta certamente perderíamos o jogo. Por outro lado, se o prêmio não está na porta A, e o apresentador abriu a porta B, que contém um bode, ao mudar de porta certamente escolheremos a porta C, que contém o prêmio. Portanto, se inicialmente escolhemos a porta com prêmio, nós perdemos. Por outro lado, se inicialmente escolhemos a porta errada nós ganhamos. Portanto, as probabilidades de vitória e derrota se invertem e temos $2/3$ de chance de vitória caso optemos por mudar de porta.

1.2.4 Um problema sobre amigos e estranhos

Deixamos para o final desta seção um problema que traduz bem a ideia de uma belíssima área conhecida como Teoria de Ramsey, cujo ponto fundamental é a ideia de que ‘não existe caos completo’, no sentido de que, se uma determinada estrutura for grande o suficiente, certamente existem subestruturas que respeitam

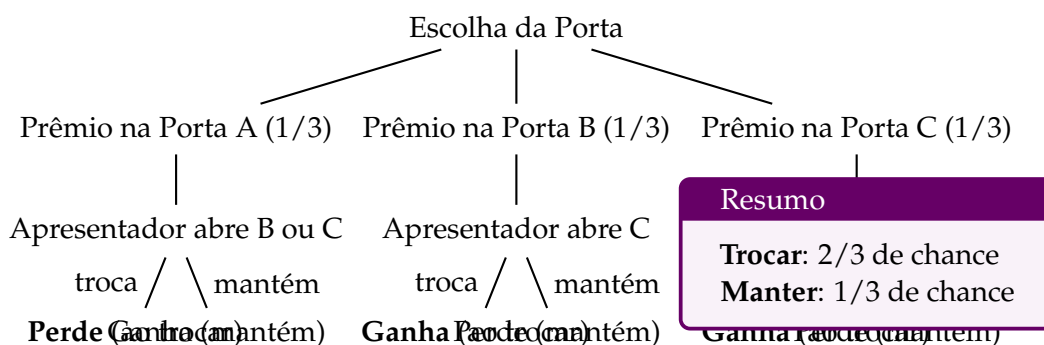


Figura 1.3: Árvore de decisão para o Problema de Monty Hall (assumindo escolha inicial na Porta A).

uma determinada propriedade. Considere a questão a seguir: Qual a menor quantidade de pessoas necessárias em uma sala para garantirmos que existam 3 pessoas que se conheçam todas entre si ou 3 pessoas em que nenhuma delas se conheça?

Antes de resolver o problema, vamos convertê-lo em algum problema que nos permita estruturar as ideias mais facilmente. Podemos simplesmente representar as pessoas como ‘bolinhas’ e as relações de conhecimento (se conhecem ou não) como segmentos ligando duas bolinhas. Caso duas pessoas se conheçam, vamos conectar as duas bolinhas correspondentes com um segmento azul; caso contrário, conectaremos com um segmento vermelho. Portanto, o problema original se transforma no seguinte problema: determinar o menor número n tal que para quaisquer maneiras que pintarmos os segmentos entre todos os pares de um conjunto com n bolinhas com vermelho e azul, sempre existe um triângulo todo azul ou todo vermelho.

Ao tentar resolver esse problema, rapidamente notamos que 3 ou 4 não é a resposta certa. De fato, observando com cuidado, percebemos que nem mesmo 5 é a resposta certa, pois existe uma forma de colorir os segmentos entre as 5 bolinhas de forma que não exista um triângulo todo azul ou todo vermelho. Veja o exemplo da Figura 1.4.

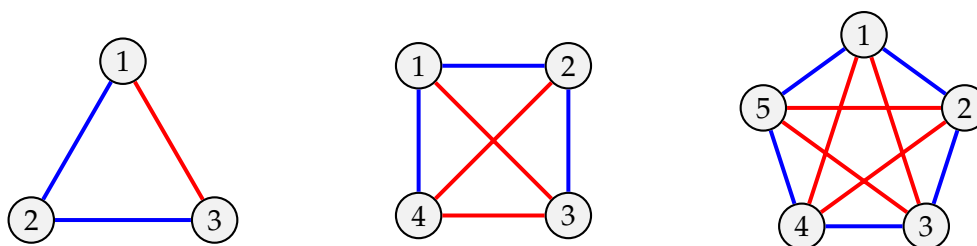


Figura 1.4: Colorações sem triângulos monocromáticos.

A resposta para nossa pergunta é 6 pessoas. Para demonstrar esse fato, note

que já excluímos o caso em que temos menos de 6 pessoas, de modo que basta mostrar que 6 pessoas é suficiente. Assim, selecione um grupo qualquer de 6 pessoas e escolha uma das pessoas, digamos, Joana. Ainda existem outras 5 pessoas, as quais vamos separar em dois grupos, aquelas que conhecem Joana e as que não conhecem. Mas perceba que, como existem 5 pessoas e dois grupos, certamente (reflita) um desses dois grupos tem pelo menos 3 pessoas. Ou seja, Joana conhece pelo menos 3 pessoas, ou desconhece pelo menos 3 pessoas.

Suponha, sem perda de generalidade, que Joana conheça 3 pessoas: Helena, Carlos e Pedro. Agora, vamos concentrar nossas atenções somente nessas 3 pessoas. Se duas delas se conhecerem (por exemplo, Helena e Carlos), então Joana, Helena e Carlos formam um trio onde todos se conhecem. Caso contrário, se nenhuma delas se conhecer, então elas mesmas formam um trio de completos desconhecidos. Em ambos os casos, o problema é satisfeito.

Uma curiosidade é que se em vez de 3 pessoas que se conhecem ou não, queremos saber a quantidade de pessoas necessárias para garantir que existam 4 pessoas que se conhecem todas entre si ou 4 pessoas que não conhecem nenhuma entre si, a resposta é 18. Se formos um passo além e quisermos garantir 5 pessoas que se conhecem ou não, precisamos trabalhar bastante, pois no momento em que este texto foi escrito, o melhor que se sabia é que precisamos de uma quantidade entre 43 e 46 pessoas.

1.3 Demonstrações e escrita matemática

Costuma-se pensar que a matemática se resume a cálculos, muitas vezes longos e tediosos, mas ela é muito mais do que fazer continhas. Trata-se de um trabalho profundamente criativo que também envolve a arte de escrever de forma precisa, clara e elegante.

Mas afinal, o que é uma demonstração (ou prova)? Quando nos perguntamos, por exemplo, se em um triângulo retângulo a soma dos quadrados dos catetos é de fato igual ao quadrado da hipotenusa, precisamos justificar por que isso é verdadeiro. Em matemática, algo é considerado "verdadeiro" somente se for verdadeiro sempre. O grande objetivo da matemática é justamente descobrir e divulgar essas verdades absolutas.

Podemos pensar em uma demonstração como um meio de comunicar uma verdade matemática para aqueles que conseguem compreender essa linguagem. Essa linguagem deve ser precisa e sem ambiguidades. Uma boa demonstração não deve deixar dúvidas sobre a veracidade do resultado que está sendo apresentado. Mas certamente, assim como foi necessário aprender uma linguagem para nos

comunicarmos no dia a dia, é fato que muitas provas requerem conhecimento prévio dessa linguagem formal para serem devidamente apreciadas. Para que isso aconteça é necessário muita prática e reflexão para nos permitir “desbloquear” uma nova forma de pensar.

1.3.1 O Teorema de Pitágoras

Voltamos agora a um resultado clássico, conhecido por todos, o Teorema de Pitágoras.

Teorema 1.2

Dado um triângulo retângulo com catetos de comprimentos a e b , e hipotenusa de comprimento c , vale que $a^2 + b^2 = c^2$.

Na prática matemática, não basta ter uma ideia correta, precisamos de uma forma correta de nos convencer do resultado e, mais ainda, convencer qualquer um que entenda a linguagem matemática que for utilizada; a forma de escrever uma prova é fundamental. Considere a seguinte tentativa de prova, baseada em áreas:

“Imagine um quadrado com lado de tamanho $a + b$. Dentro desse quadrado, imagine um segundo quadrado, de lado c , posicionado de modo a formar 4 triângulos retângulos com catetos de tamanho a e b entre os quadrados. Note que a área do quadrado maior é $(a + b)^2$, mas também pode ser vista como $2ab + c^2$, de modo que $(a + b)^2 = 2ab + c^2$. Portanto, $a^2 + b^2 = c^2$.”

Apesar de a matemática por trás desse argumento estar essencialmente correta, existem muitos problemas no modo em que essas ideias foram comunicadas. Uma apresentação que fornece o argumento às pressas com descrições incompletas é considerada uma prova ruim. Ela possui ideias corretas, mas pode deixar o leitor confuso sobre a disposição geométrica das figuras mencionadas. Leia uma versão melhorada abaixo e reflita sobre as diferenças entre os argumentos. Perceba como o argumento abaixo é muito mais preciso e não dá margem para interpretações ambíguas. Incluímos uma figura na prova, para facilitar a visualização, mas é importante que a demonstração não dependa da figura, que serve somente para auxiliar o entendimento.

Prova do Teorema 1.2. Considere inicialmente um quadrado X com lado de comprimento $a + b$. Agora subdivida X em quatro triângulos retângulos congruentes, cada um com catetos de comprimentos a e b e hipotenusa c , dispostos nos cantos do quadrado X . Para facilitar a visualização, perceba que esta construção delimita, em seu interior, um quadrado de lado c (veja a Figura 1.5).

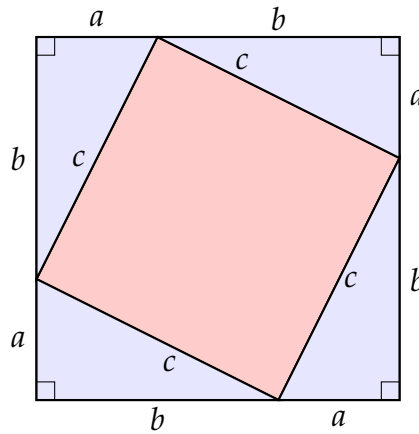


Figura 1.5: O quadrado X particionado em quatro triângulos de catetos a , b e hipotenusa c , e um quadrado de lado c .

Note que a área total do quadrado X pode ser expressa das seguintes maneiras:

1. Pelo quadrado do comprimento de seus lados: $(a + b)^2 = a^2 + 2ab + b^2$;
2. Pela soma das áreas das figuras que o compõem (os quatro triângulos e o quadrado interno): $4 \cdot \left(\frac{ab}{2}\right) + c^2 = 2ab + c^2$.

Igualando as duas expressões para a mesma área, temos que

$$a^2 + 2ab + b^2 = 2ab + c^2.$$

Subtraindo $2ab$ de ambos os membros da igualdade, obtemos

$$a^2 + b^2 = c^2,$$

o que conclui nossa demonstração. □

Mais uma vez, contar algo de duas formas diferentes nos ajudou a resolver o problema. Agora que escrevemos nossa primeira prova completa, podemos observar alguns detalhes sobre a escrita: Após cada fórmula, mesmo que ela esteja em destaque, sempre utilizamos pontuação. Os caracteres matemáticos fazem parte do texto e seguem as regras de escrita. Toda figura que for usada deve ter uma legenda descritiva, para que faça sentido e o leitor saiba exatamente o que está olhando. Por fim, sempre utilizamos o símbolo “□” ao final da demonstração para indicar que finalizamos.

1.3.2 Infinitude dos números primos

Para finalizar nossa introdução à arte de demonstrar e tentar ser convincente ao mostrar a importância de termos cuidado com a escrita para comunicar um resultado matemático, vejamos o *Teorema de Euclides*. Para entender esse resultado, basta que saibamos o conceito de divisibilidade e números primos: dados números inteiros a e b , dizemos que a é *divisível* por b quando a divisão a/b tem resto 0; um *número primo* é um número inteiro maior que 1 e que é divisível somente por 1 e por ele mesmo.

Teorema 1.3

Existem infinitos números primos.

Demonstração. Seja n um inteiro positivo qualquer e considere o conjunto $P = \{p_1, p_2, \dots, p_n\}$ que contém os n primeiros números primos. Note primeiramente que basta mostrar que existe um número primo q que não pertence ao conjunto P , uma vez que para qualquer inteiro n que quisermos, conseguiremos um conjunto com mais que n primos. No que segue, mostraremos que tal número primo q existe.

Seja $N = p_1 \cdot p_2 \cdot \dots \cdot p_n$ o produto de todos os números em P . Defina agora $q = N + 1$, que obviamente é um número inteiro maior que N . Existem apenas duas situações possíveis para q .

Primeiramente, suponha que $i) q$ é primo. Como $q > N$ e todos os números do nosso conjunto são menores ou iguais a N , o número q é um inteiro que não pertence a P , como queríamos.

Suponha agora que q não é primo. Nesse caso, precisamos conseguir um outro número primo p que não está em P . Mas note que, pelo Teorema Fundamental da Aritmética, existe um número primo p que divide q . No que segue, mostraremos que tal número p não está em P .

Como p divide $q = N + 1$, sabemos que p não divide N , pois caso dividisse, teríamos que p também dividiria a diferença $(N + 1) - N = 1$, o que é impossível, pois nenhum número inteiro maior ou igual a 2 pode dividir 1. Portanto, como p não divide $N = p_1 \cdot p_2 \cdot \dots \cdot p_n$, sabemos que p não é nenhum elemento de $P = \{p_1, p_2, \dots, p_n\}$, como queríamos demonstrar. $\square$

Note como a prova acima é construída com extremo cuidado e precisão. A estratégia central consiste em mostrar que qualquer lista finita de números primos está, necessariamente, incompleta. O ponto crucial é a construção do número $q = N + 1$, em que N é o produto de todos os primos no conjunto finito P . Ao analisar os dois únicos casos possíveis para q , a demonstração não deixa lacunas:

1. Se q for primo, ele é o próprio primo que queríamos encontrar que não está em P (pois sendo maior que N , q é estritamente maior que qualquer um dos elementos em P).
2. Se q não for primo, ele deve ter um divisor primo p . A prova então utiliza propriedades fundamentais de divisibilidade para mostrar que esse p não pode pertencer à lista original P , pois nenhum primo em P divide $N + 1$ sem deixar resto 1.

Essa exaustão coerente de possibilidades garante que, independentemente de como escolhemos nossa coleção inicial finita, sempre haverá um novo número primo.

1.3.3 Uma observação sobre polinômios

Na matemática, a intuição e a observação de padrões iniciais podem nos levar a conjecturas fascinantes. Considere o polinômio $P(x) = x^2 + x + 41$ e note que, ao testar alguns valores para x , os resultados obtidos nos levam a conjecturar que sempre obtemos números primos. Será que isso é sempre verdade? Vamos observar os primeiros valores para ver se há chances de que isso seja verdade.

- $P(0) = 0^2 + 0 + 41 = 41$;
- $P(1) = 1^2 + 1 + 41 = 43$;
- $P(2) = 2^2 + 2 + 41 = 47$;
- $P(3) = 3^2 + 3 + 41 = 53$;
- $P(4) = 4^2 + 4 + 41 = 61$.

De fato, para os 5 primeiros inteiros positivos, o polinômio é sempre um número primo. Mas nunca devemos aceitar um resultado geral como verdadeiro verificando somente uma quantidade pequena de possibilidades. Assim, note que a intuição é importante, mas sozinha ela pode nos levar a conclusões erradas. Essa sequência continua gerando primos até $P(39) = 39^2 + 39 + 41 = 1601$. Contudo, a conjectura de que o polinômio gera apenas números primos falha quando testamos $x = 40$, pois temos que

$$P(40) = 40^2 + 40 + 41 = 1681 = 41^2,$$

de modo que não é primo, uma vez que tem divisores além de 1 e dele mesmo (o número 41). O mesmo ocorre para $x = 41$, onde $P(41) = 41^2 + 41 + 41$, que

pode ser fatorado como $41(41 + 1 + 1)$, comprovando novamente que não é primo. Este exemplo ilustra a importância da prova formal completa em oposição à mera verificação de casos iniciais.

Lógica Proposicional

Uma *proposição* é simplesmente uma afirmação que é *verdadeira* ou *falsa*, mas nunca as duas coisas ao mesmo tempo. Por exemplo, a seguir temos diversos exemplos de proposições.

Exemplo 2.1

Exemplos de proposições.

p : Uma hora tem 60 minutos.

q : Tomate é uma fruta.

r : Futebol é uma religião.

s : Três é um número par.

t : Se $x > 2$ é par, então x pode ser expresso como a soma de dois números primos.

u : 5 é um gato com rodas.

Dizemos que uma proposição tem o *valor-verdade* V se ela for verdadeira; do contrário, a proposição é falsa e dizemos que ela tem o valor-verdade F. Em geral, usamos letras minúsculas tais como p , q e r para indicar proposições.

Note que, no Exemplo 2.1, as proposições p e q claramente têm valor-verdade V. Já as proposições r e s são claramente falsas, de modo que têm valor-verdade F. Perceba que, mesmo que não saibamos o valor-verdade de t , ela é uma proposição, pois é verdadeira ou falsa, mas não sabemos a resposta¹. Para não esquecermos de comentar, u é uma proposição com valor-verdade falso.

¹esta é a famosa Conjectura de Goldbach e, no momento em que este livro foi escrito, continua sem que saibamos se é verdadeira ou falsa.

Vale notar que na escrita de textos matemáticos, é comum enunciar certos fatos matemáticos que são verdadeiros como *proposições*, embora nem toda proposição precise ser verdadeira.

Vejam agora exemplos de sentenças que não são proposições, pois não é possível associar um valor-verdade a elas.

Exemplo 2.3

Exemplos de sentenças que não são proposições.

p : *Lembre-se de beber água.*

q : *Qual é o seu nome?*

r : *Você só estuda?*

s : *Bom dia!*

t : *Que gato lindo!*

A sentença p do Exemplo 2.3 não faz nenhuma afirmação, trata-se apenas de um lembrete. Aliás, aproveite para beber um pouco de água agora! A sentença q é apenas uma pergunta, não uma afirmação. Quanto à sentença r , ainda que seja verdade que “você só estuda”, ela também é uma pergunta. Mesmo que o seu dia esteja sendo bom, a sentença s não tem o propósito de fazer uma afirmação, mas sim um desejo. Certamente você agora consegue perceber que as sentenças s e t também não são proposições.

Dada uma proposição p , definiremos agora uma forma de nos referir a uma proposição que tem o valor-verdade diferente de p .

Definição 2.4

A *negação* de uma proposição p , denotada por $\neg p$, é a proposição com valor-verdade V quando p tem o valor-verdade F e vice-versa.

Podemos ler $\neg p$ como “não p ” ou “não é verdade que p ”.

Em geral, podemos reafirmar a proposição $\neg p$ simplesmente negando o verbo da oração que define p . A proposição obtida desta forma afirma a mesma coisa que a proposição definida acima. Vejam alguns exemplos a seguir.

Exemplo 2.5

Considere as seguintes proposições do Exemplo 2.1:

p : *Uma hora tem 60 minutos.*

q : *Tomate é uma fruta.*

As negação de p é dada por:

$\neg p$: *Não é verdade que uma hora tem 60 minutos.*

Que também pode ser reescrita da seguinte forma.

$\neg p$: *Uma hora **não** tem 60 minutos.*

Da mesma forma, a negação da proposição q é a seguinte:

$\neg q$: *Não é verdade que tomate é uma fruta.*

Ou, de forma equivalente,

$\neg q$: *Tomate **não** é uma fruta.*

2.1 Proposições compostas

Dadas duas proposições p e q , podemos construir uma terceira proposição com base nas proposições p e q de diversas formas possíveis e dizemos que a proposição resultante é uma *composição* de p e q . Os *conectivos binários* (que combinam duas proposições) que discutiremos aqui são aqueles mais comuns e, a partir deles, conseguimos gerar proposições tão complexas quanto precisemos. Esses conectivos são: $\wedge$ (conjunção, o famoso "e"), $\vee$ (disjunção, o famoso "ou"), $\rightarrow$ (condicional, o não tão famoso "se ..., então ...") e $\leftrightarrow$ (condicional dupla, que é o "condicional para dois lados").

2.1.1 Conjunção e disjunção

Iniciaremos nosso estudo dos conectivos binários pelas operações de conjunção e disjunção. Esses conectivos permitem combinar duas proposições simples de forma direta, refletindo construções que utilizamos diariamente em nossa linguagem natural por meio das palavras “e” e “ou”. A seguir, definiremos formalmente como esses conectivos operam sobre os valores-verdade das proposições envolvidas.

Definição 2.6

Dadas duas proposições p e q , a *conjunção* de p e q , denotada por $p \wedge q$, é a proposição que corresponde à afirmação

é verdade que p e é verdade que q ,

que tem valor-verdade V quando ambos p e q são verdadeiros e, caso contrário, tem valor-verdade.

Podemos resumir as possibilidades de valor-verdade para um conjunto de proposições em uma tabela, como na Tabela 2.1. Tabelas desse tipo são chamadas de *tabela verdade* e seu propósito é listar todas as possibilidades de valores-verdade para um proposições p , q etc, e um conjunto de proposições compostas dessas.

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

Tabela 2.1: Tabela verdade de $p \wedge q$.

Em linguagem portuguesa, em geral escrevemos a proposição $p \wedge q$ simplesmente juntando as orações que definem p e q e as conectando com a conjunção *e*.

Exemplo 2.7

Considere as seguintes proposições.

p : Estudei bem ao longo do semestre.

q : Fui aprovado na disciplina.

A conjunção de p e q corresponde à seguinte afirmação:

$p \wedge q$: *É verdade que estudei bem ao longo do semestre
e é verdade que fui aprovado na disciplina.*

Podemos também expressar essa proposição da forma mais natural a seguir.

$p \wedge q$: Estudei para a prova e fui aprovado na disciplina.

Definição 2.8

Dadas duas proposições p e q , a *disjunção* de p e q , denotada por $p \vee q$, é a proposição que corresponde à seguinte afirmação:

$p \vee q$: É verdade que p **ou** que q .

O valor-verdade de $p \vee q$ é F quando ambos p e q são falsos; caso pelo menos uma dentre p e q seja verdadeira, $p \vee q$ tem valor-verdade V (veja Tabela 2.2).

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

Tabela 2.2: Tabela verdade de $p \vee q$.

É comum alunos se confundirem com os símbolos $\vee$ e $\wedge$. De fato, à primeira vista a escolha destes símbolos parece um pouco arbitrária, mas eles são baseados nos dois símbolos $\cup$ e $\cap$ que representam a união e a interseção de dois conjuntos, respectivamente. Veremos mais à frente, quando tratarmos de conjuntos, como se dá essa conexão entre os conectivos lógicos e as operações entre conjuntos.

Em geral, em língua portuguesa, escrevemos a proposição $p \vee q$ simplesmente juntando as duas orações que definem p e q e as conectando com a conjunção *ou*.

Exemplo 2.9

Considere as seguintes proposições.

p : Matemática é uma ciência exata.

q : Pessoas têm asas.

A disjunção de p e q corresponde à afirmação

$p \vee q$: É verdade que Matemática é uma ciência exata
ou que pessoas têm asas.

Ou, simplificando, podemos também escrever da seguinte forma:

$p \vee q$: Matemática é uma ciência exata **ou** pessoas têm asas.

Note que no Exemplo 2.9, mesmo que q seja uma proposição falsa, $p \vee q$ é uma proposição verdadeira, uma vez que p tem valor-verdade V. Por outro lado, se temos uma proposição $r : 2$ é ímpar, então $q \vee r$ é uma proposição falsa, uma vez que tanto q quanto r são proposições falsas.

Vale ressaltar que o *ou* em lógica expressa a possibilidade de que pelo menos uma das proposições seja verdadeira, o que também inclui o caso em que ambas as proposições são verdadeiras. Por isso, também dizemos que $\vee$ é uma *disjunção inclusiva*. Na língua portuguesa, entretanto, muitas das vezes queremos que um *ou* expresse a possibilidade em que apenas uma das proposições seja verdadeira. Por exemplo, imagine que você está em um restaurante e o garçom quer saber sua preferência de acompanhamento:

— *O prato de hoje é filé de frango grelhado. Como acompanhamento, você prefere purê de batatas ou salada?*

Nesse contexto, o *ou* indica que as opções de acompanhamento apresentadas são mutuamente exclusivas, isto é, apenas uma delas deve ser escolhida. Do ponto de vista lógico, não estaria errado responder que você prefere os dois tipos de acompanhamento ao mesmo tempo. Contudo, como já convivemos em sociedade há algum tempo, sabemos que a intenção do garçom era apresentar as duas únicas opções de acompanhamento e ele espera que apenas uma dentre as duas opções seja escolhida. Mas, de fato, estaria logicamente coerente você responder ao garçom da seguinte forma:

— *Isso, prefiro purê de batatas ou salada.*

Ao responder desta forma, você estaria indicando que a afirmação “você prefere purê de batata ou salada” está correta, pois você de fato prefere ter uma destas duas opções como acompanhamento. Assim, você está indicando que ficaria feliz recebendo somente purê de batatas, somente salada ou os dois tipos de acompanhamento.

Outro exemplo que podemos explorar é o seguinte. Imagine que você pediu instruções a um matemático de como chegar na Biblioteca Central da universidade que você estuda. Você então pergunta:

— *Quando eu chegar na rotatória, eu devo seguir na primeira ou na segunda saída?*

O matemático então responde:

— *Sim, você deve seguir em uma das duas primeiras saídas.*

Obviamente, ao fazer a pergunta você utilizou o *ou* de forma exclusiva, e portanto, você esperaria que o matemático indicasse qual dentre as duas possibilidades apresentadas está correta. Mas matemáticos, em geral, assumem que o *ou* é inclusivo. Para indicar um *ou* exclusivo, eles em geral diriam a frase de uma forma um pouco diferente.

Em geral, em língua portuguesa, o artifício que utilizamos para tentar reforçar que estamos utilizando um *ou* exclusivo é escrevermos a proposição $p \oplus q$ de uma das seguintes formas possíveis:

“Ou p ou q .”

“Ou p ou q , mas não ambos.”

Definição 2.10

Dadas duas proposições p e q , a *disjunção exclusiva* de p e q , a qual denotamos por $p \oplus q$, é a proposição que corresponde à seguinte afirmação:

$p \oplus q$: É verdade que **ou** p **ou** q , mas não ambos.

O valor-verdade de $p \oplus q$ é V quando p e q possuem valores-verdade distintos; caso contrário, é F (veja Tabela 2.3).

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

Tabela 2.3: Tabela verdade de $p \oplus q$ (ou exclusivo).

Em geral, em língua portuguesa, o artifício que utilizamos para tentar reforçar que estamos utilizando um *ou* exclusivo é escrevermos a proposição $p \oplus q$ de uma das seguintes formas possíveis:

“Ou p ou q .”

“Ou p ou q , mas não ambos.”

Exemplo 2.11

Considere as proposições s e t a seguir:

s : A lista de exercícios 1 deve ser entregue hoje

t : A lista de exercícios 2 deve ser entregue hoje.

A disjunção exclusiva de s e t corresponde à afirmação

$s \oplus t$: **ou** a lista de exercícios 1 deve ser entregue hoje

ou a lista de exercícios 2 deve ser entregue hoje, mas não ambos.

Note que se for constatado que a lista de exercícios 1 deve ser entregue hoje, ao afirmarmos que $s \oplus t$ é uma proposição verdadeira, impedimos que a lista de exercícios 2 deva ser entregue hoje.

2.1.2 Operadores condicionais

Nesta seção trataremos de operadores fundamentais. O primeiro deles é o operador condicional, que nos permite formar proposições da forma “se p , então q ”.

Definição 2.12

Dadas duas proposições p e q , a *condicional* de p e q , denotada por $p \rightarrow q$, é a proposição que corresponde à seguinte afirmação:

$p \rightarrow q$: Se p é verdade, **então** q é verdade.

A proposição p é chamada de *hipótese* (ou *premissa*) e q é a *tese* (ou *consequência*). O valor-verdade de $p \rightarrow q$ é F quando p é verdadeiro e q é falso; caso contrário, é V (veja Tabela 2.4).

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Tabela 2.4: Tabela verdade de $p \rightarrow q$.

Vamos analisar o seguinte exemplo com bastante atenção, pois à primeira vista, o condicional de p e q pode soar um pouco estranho quando p é falso.

Exemplo 2.13

Considere as seguintes proposições.

p : Gatos são peixes.

q : 10 é divisível por 2.

r : 10 é par.

A proposição condicional de p e q corresponde à afirmação

$p \rightarrow q$: *Se gatos são peixes,
então 10 é divisível por 2.*

A proposição condicional de q e r corresponde à afirmação

$q \rightarrow r$: *Se 10 é divisível por 2,
então 10 é par.*

A proposição condicional de r e p corresponde à afirmação

$r \rightarrow p$: *Se 10 é par,
então gatos são peixes.*

Das três condicionais descritas no Exemplo 2.13, diferentemente do que talvez você possa pensar, somente a condicional $r \rightarrow p$ é falsa. Que $r \rightarrow p$ é falsa, é bem claro. Afinal de contas, sabemos que 10 é par, e como $r \rightarrow p$ corresponde à "Se 10 é par, então gatos são peixes", $r \rightarrow p$ seria verdadeira somente se gatos fossem peixes. Por outro lado, entendemos que a condicional "Se 10 é divisível por 2, então 10 é par" é verdadeira, pois 10 ser divisível por 2 de fato implica que 10 é par. Mas algo que pode incomodar em um primeiro momento é a proposição $p \rightarrow q$ "se gatos são peixes, então 10 é divisível por 2". Essa é uma proposição verdadeira, pois a hipótese é falsa e a tese é verdadeira e se pensarmos com calma, de fato faz sentido que assim seja, uma vez que a falsidade da hipótese não nos diz nada sobre a veracidade da tese.

O seguinte exemplo pode ajudar a aceitar melhor a definição de condicional. Imagine que você diz a seguinte proposição: "Se eu ganhar na loteria, então eu darei R\$ 1.000,00 para cada aluno da turma". Pela definição de condicional, essa expressão é verdadeira nas seguintes situações:

- Você ganha na loteria e dá R\$ 1.000,00 para cada aluno da turma.
- Você não ganha na loteria e dá R\$ 1.000,00 para cada aluno da turma.
- Você não ganha na loteria e não dá R\$ 1.000,00 para cada aluno da turma.

O ponto é que você prometeu que caso ganhasse na loteria, você daria os mil reais, e esse seria o comportamento que a turma esperaria de você. Porém, caso você não ganhe na loteria, bem, você não está descumprindo sua promessa.

É comum expressar uma proposição condicional $p \rightarrow q$ de diversas formas distintas. A seguinte lista contém apenas algumas das possíveis expressões que você poderá encontrar em muitos dos textos matemáticos.

“Se p , então q .”

“ q , se p .”

“ p implica q .”

“ q segue de p .”

“Sempre que p , q .”

“ q sempre que p .”

“ p é suficiente para q .”

“ q é necessário para p .”

“Uma condição necessária para p é q .”

“uma condição suficiente para q é p .”

A *recíproca* de uma proposição condicional $p \rightarrow q$ é a proposição $q \rightarrow p$ obtida trocando-se a hipótese pela tese. Em geral, a veracidade de $p \rightarrow q$ não garante a veracidade de $q \rightarrow p$, como podemos ver no exemplo seguinte.

Exemplo 2.14

Considere a seguinte proposição condicional (verdadeira):

$p \rightarrow q$: *Se um polígono é um quadrado, então ele é um retângulo.*

A recíproca da proposição condicional acima é a seguinte:

$q \rightarrow p$: *Se um polígono é um retângulo, então ele é um quadrado.*

Esta proposição é falsa, uma vez que nem todo retângulo é um quadrado. Isso exemplifica que podemos ter proposições condicionais verdadeiras cuja recíproca seja falsa.

Podemos entender a proposição $p \rightarrow q$ como uma afirmação de que p é uma condição *mais forte* que q . O sentido de *força* aqui é que, se a condicional for verdadeira, a veracidade de p garante a veracidade de q . É importante notar que essa relação de força não é, necessariamente, mútua. A veracidade de $p \rightarrow q$ não implica na veracidade de $q \rightarrow p$.

Apesar de nem sempre ser verdade que $p \rightarrow q$ implica a veracidade de $q \rightarrow p$, existem situações em que ambas as condicionais são verdadeiras. Para representar isso, definimos o próximo conectivo lógico.

Definição 2.15

Dadas duas proposições p e q , a *condicional dupla* de p e q , a qual denotamos por $p \leftrightarrow q$, é a proposição que corresponde à seguinte afirmação:

$p \leftrightarrow q$: É verdade que p *se, e somente se*, é verdade que q .

O valor-verdade de $p \leftrightarrow q$ é V quando p e q possuem o mesmo valor-verdade; caso contrário, é F (veja Tabela 2.5).

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

Tabela 2.5: Tabela verdade de $p \leftrightarrow q$.

Assim como a condicional, a proposição condicional dupla $p \leftrightarrow q$ também pode ser expressa de diversas formas. A seguinte lista contém algumas das expressões mais comuns.

“ p se, e somente se, q .”

“ p se, e só se, q .”

“ p é equivalente a q .”

“Se p então q , e reciprocamente.”

“ p é condição necessária e suficiente para q .”

Exemplo 2.16

Considere as seguintes proposições.

p : x é par. q : x é divisível por 2.

A proposição condicional dupla de p e q corresponde à afirmação:

$p \leftrightarrow q : x \text{ é par se, e somente se,}$
 $x \text{ é divisível por 2.}$

Podemos também escrever a proposição resultante da seguinte forma:

$p \leftrightarrow q : x \text{ é par é equivalente a}$
 $x \text{ é divisível por 2.}$

Note que ao afirmarmos que $p \leftrightarrow q$ é uma proposição verdadeira, criamos uma ligação muito mais forte do que na condicional. Agora, as duas proposições são inseparáveis: elas devem ter sempre o mesmo valor-verdade. Portanto, se x não é par (p é Falso), obrigatoriamente x não pode ser divisível por 2 (q também deve ser Falso). Da mesma forma, caso seja verdade que x é par, devemos ter que ele é divisível por 2. Qualquer combinação em que uma proposição seja verdadeira e a outra falsa tornaria a proposição $p \leftrightarrow q$ falsa.

É possível definir alguns outros conectivos lógicos (tais como *NAND* ou *NOR*), bem como outras operações mais complexas, mas com o que apresentamos você deve conseguir obter outras proposições úteis, de modo que o que foi discutido até agora é suficiente para os nossos propósitos. Dadas proposições p e q , reunimos na Tabela 2.6 os valores-verdade dos conectivos que apresentamos até aqui, além dos possíveis valores de $\neg p$ e $\neg q$.

p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
V	V	F	F	V	V	F	V	V
V	F	F	V	F	V	V	F	F
F	V	V	F	F	V	V	V	F
F	F	V	V	F	F	F	V	V

Tabela 2.6: Tabela-verdade resumo dos conectivos lógicos.

2.2 Equivalência lógica

Agora que já sabemos como compor proposições, podemos formar proposições complexas envolvendo vários conectivos lógicos e proposições. Por exemplo, suponha que p_1 , p_2 e p_3 são proposições e considere a proposição

$$q : (\neg(p_1 \rightarrow p_2)) \wedge (\neg p_2 \vee p_3).$$

Note que usamos os parênteses para indicar a ordem em que os conectivos devem ser considerados, evitando assim ambiguidades. No caso, os parênteses indicam que a fim de determinarmos o valor-verdade da proposição q , precisamos antes determinar o valor-verdade da conjunção entre as seguintes duas proposições:

$$r : \neg(p_1 \rightarrow p_2),$$

$$s : \neg p_2 \vee p_3,$$

de modo que $q : r \wedge s$. Quanto à proposição s , note que a princípio, poderíamos interpretar que o conectivo $\neg$ está negando a proposição $p_2 \vee p_3$. Mas se este fosse o caso, escreveríamos $\neg(p_2 \vee p_3)$ no lugar de $\neg p_2 \vee p_3$.

Dados os valores-verdade para p_1 , p_2 e p_3 , para determinar o valor-verdade de q , podemos primeiramente determinar o valor-verdade de $p_1 \rightarrow p_2$, e então conseguimos determinar o valor-verdade de r . Seguimos determinando $\neg p_2$, que nos permite determinar s . Por fim, determinamos o valor-verdade de $q : r \wedge s$. Abaixo temos a tabela-verdade contendo todas essas proposições, que considera todas as possibilidades de valor-verdade para p_1 , p_2 e p_3 .

p_1	p_2	p_3	$\neg p_2$	$p_1 \rightarrow p_2$	$\neg(p_1 \rightarrow p_2)$	$\neg p_2 \vee p_3$	q
V	V	V	F	V	F	V	F
V	V	F	F	V	F	F	F
V	F	V	V	F	V	V	V
V	F	F	V	F	V	V	V
F	V	V	F	V	F	V	F
F	V	F	F	V	F	F	F
F	F	V	V	V	F	V	F
F	F	F	V	V	F	V	F

Tabela 2.7: Tabela-verdade em que $q : (\neg(p_1 \rightarrow p_2)) \wedge (\neg p_2 \vee p_3)$.

Mais geralmente, se uma proposição q é dada como composições de proposições $p_1, \dots, p_n$ por meio de conectivos lógicos, então dizemos que q é uma *expressão lógica* e que $p_1, \dots, p_n$ são as suas *variáveis proposicionais*.

Definição 2.17

Uma *tautologia* é uma expressão lógica cujo valor-verdade é sempre V, seja qual for o valor-verdade das variáveis proposicionais. Uma *contradição* é uma expressão lógica cuja negação é uma tautologia, ou seja, cujo valor-verdade é sempre F.

Qualquer expressão da forma $p \vee \neg p$ é uma tautologia e qualquer expressão da forma $p \wedge \neg p$ é uma contradição. Por exemplo, o famoso dilema de Hamlet sobre a vida e a morte é, em sua essência, uma tautologia.

— *Ser ou não ser, eis a questão.*

Já a expressão $\text{ser} \wedge \neg \text{não ser}$ é uma contradição, fundamentada no princípio de que é impossível que algo, ao mesmo tempo, *seja e não seja*.

Definição 2.18

Duas expressões lógicas p e q são ditas *logicamente equivalentes* se $p \leftrightarrow q$ for uma tautologia. Denotamos $p \equiv q$ para indicar que p e q são logicamente equivalentes.

Podemos verificar que duas proposições p e q são logicamente equivalentes analisando a tabela-verdade das proposições e das variáveis proposicionais que as definem. Se as colunas correspondentes a p e a q são iguais, então é porque elas são equivalentes. Note que as expressões $p \rightarrow q$ e $\neg p \vee q$ são logicamente equivalentes. Podemos verificar esta equivalência construindo uma tabela-verdade e comparando os resultados de cada expressão para todas as combinações de valores-verdade das variáveis proposicionais p e q . Como as colunas finais para $p \rightarrow q$ e $\neg p \vee q$ na Tabela 2.8 são idênticas, as duas proposições são logicamente equivalentes.

p	q	$\neg p$	$p \rightarrow q$	$\neg p \vee q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

Tabela 2.8: Tabela-verdade comparando $p \rightarrow q$ e $\neg p \vee q$.

Outro exemplo de expressões logicamente equivalentes são $p \rightarrow q$ e $\neg q \rightarrow \neg p$. Dada sua importância e relevância, vamos destacar a definição dessa última proposição.

Definição 2.19

Dadas proposições p e q , dizemos que a expressão $\neg q \rightarrow \neg p$ é a *contrapositiva* da proposição $p \rightarrow q$.

Por exemplo, considere a proposição a seguir, em que p é a proposição "está chovendo" e q é a proposição "a rua está molhada":

$p \rightarrow q$: Se está chovendo, então a rua está molhada.

Sua contrapositiva corresponde à seguinte proposição:

$\neg q \rightarrow \neg p$: Se a rua **não** está molhada, então **não** está chovendo.

Tire um tempo para refletir que de fato as duas proposições são equivalentes, pensando em seu sentido, sem precisar olhar linha a linha da tabela-verdade abaixo.

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

Tabela 2.9: Tabela-verdade comparando $p \rightarrow q$ e $\neg q \rightarrow \neg p$.

Finalizamos esta seção apresentando a Tabela 2.10, que contém uma lista de equivalências lógicas que são comumente utilizadas para simplificar a análise de expressões lógicas complexas. Encorajamos o leitor a refletir com calma sobre cada uma delas e escrever a tabela-verdade para verificar de fato que se tratam de equivalências lógicas.

2.3 Predicados e quantificadores

Até agora, lidamos com proposições, que são afirmações com um valor-verdade fixo, seja ele V ou F. Contudo, podemos estender o conceito de proposições para que a veracidade de uma afirmação dependa de variáveis. Por exemplo, considere a seguinte afirmação:

Tabela 2.10: *Equivalências lógicas.*

Propriedade	Equivalências
Elemento neutro	$p \wedge V \equiv p$ $p \vee F \equiv p$
Dominação	$p \vee V \equiv V$ $p \wedge F \equiv F$
Idempotência	$p \vee p \equiv p$ $p \wedge p \equiv p$
Dupla negação	$\neg(\neg p) \equiv p$
Comutatividade	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Associatividade	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributividade	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Leis de De Morgan	$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$
Absorção	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$
Negação	$p \vee \neg p \equiv V$ $p \wedge \neg p \equiv F$

$P(x)$: O número inteiro positivo x é um número par.

Indicamos a afirmação acima por $P(x)$ porque x é um número que a princípio não conhecemos ou que não foi explicitado e a veracidade da afirmação depende totalmente do valor que x pode assumir. Assim, para cada valor de x , a afirmação $P(x)$ assume um valor-verdade e, portanto, se torna uma proposição. Por exemplo, $P(2)$ é uma proposição verdadeira, enquanto que $P(3)$ é uma proposição falsa. A

seguinte definição estende esse conceito para proposições mais gerais.

Definição 2.20

Um *predicado* é uma afirmação que contém uma ou mais *variáveis* e que se torna uma proposição (ou seja, adquire um valor-verdade V ou F) quando valores ou objetos específicos são atribuídos às suas variáveis. O *domínio* de uma variável é o conjunto de valores ou objetos que a variável pode assumir.

Frequentemente, representamos um predicado por uma letra maiúscula seguida das variáveis entre parênteses, como $P(x)$ ou $Q(x, y)$. A fim de que um predicado esteja bem definido, é preciso explicitar o *domínio* de suas variáveis, que é o conjunto em que elas podem assumir valores. Por exemplo, o predicado $P(x)$ dado como exemplo no início desta seção tem como domínio o conjunto dos inteiros positivos.

Exemplo 2.21

Considere os seguintes predicados:

$P(x, y)$: Os números reais x e y são tais que $x = y/2$.

$Q(A)$: O conjunto A contém dois elementos.

$R(x)$: $x^2 \neq 2$.

O predicado P explicita o seu domínio como o conjunto dos pares de números reais (x, y) . Já o predicado Q não deixa claro o seu domínio, mas podemos assumir que é a classe de todos os conjuntos possíveis. Da mesma forma, R não define o seu domínio, mas nesse caso, há diversas possibilidades razoáveis para a escolha do domínio de R . Por exemplo, o domínio poderia ser o conjunto dos números reais ou o conjunto dos números racionais. Para os racionais, $R(x)$ é sempre falso, qualquer que seja o valor de x , mas se o domínio é o conjunto dos números reais, então $x = \sqrt{2}$ é um valor para o qual $R(x)$ é verdadeiro. Mas já discutimos que não pode haver ambiguidade em matemática. Portanto, é essencial que deixemos claro na definição de um predicado o seu domínio:

$R(x)$: O número real x é tal que $x^2 \neq 2$.

Em lógica, predicados expressam propriedades ou relações. Contudo, para determinar a extensão em que uma propriedade é válida – se para todos os elementos de um conjunto ou para ao menos um – é necessário o uso de *quantificadores*. Por exemplo, gostaríamos de um jeito curto e preciso de expressar a proposição

"*todo* número natural é par". Fazemos isso na definição a seguir.

Definição 2.22

Seja $P(x)$ um predicado e D o domínio de x . Escrevemos $\forall x \in D, P(x)$ para indicar a proposição p que afirma que $P(x)$ é verdadeiro para todo $x \in D$, i.e.,

$\forall x \in D, P(x) : \textit{Para todo } x \in D, \textit{ é verdade que } P(x).$

Quando o domínio de x estiver claro pelo contexto, podemos escrever somente $\forall x P(x)$ em vez de $\forall x \in D, P(x)$.

Note que $\forall x P(x)$ é uma proposição falsa se, e somente se, houver algum $x \in D$ para o qual o predicado $P(x)$ é falso.

A observação acima nos dá o gancho para definir um conceito importantíssimo.

Definição 2.24

Dada uma proposição $p : \forall x \in D, P(x)$, um elemento $x \in D$ para o qual $P(x)$ é falso é chamado de *contraexemplo* para a proposição p .

Exemplo 2.25

Considere o seguinte predicado $P(x)$, cujo domínio de x é o conjunto $D = \{2, 3, 5, 7, 11, 13, 17\}$:

$P(x) : x \text{ é um número primo}.$

A proposição $\forall x P(x)$ é verdadeira, pois todo número $x \in D$ é de fato um número primo. Agora suponha que o domínio de x é o conjunto de todos os números inteiros positivos. Então, nesse caso, a proposição $\forall x P(x)$ é falsa, pois $x = 4$ é um contraexemplo para essa proposição, uma vez que $P(4)$ é falso.

Muitas vezes queremos indicar a existência de pelo menos um elemento em um conjunto que satisfaz uma determinada propriedade. Para isso, usamos o quantificador existencial.

Definição 2.26

Seja $P(x)$ um predicado e D o domínio de x . Denotamos por $\exists x \in D, P(x)$ a proposição que afirma que $P(x)$ é verdadeiro para pelo menos um $x \in D$, i.e.,

$$\exists x \in D, P(x) : \text{Existe } x \in D \text{ para o qual é verdade que } P(x).$$

Quando o domínio de x estiver claro pelo contexto, podemos escrever somente $\exists x P(x)$ em vez de $\exists x \in D, P(x)$.

Note que $\exists x P(x)$ é uma proposição falsa se, e somente se, $\forall x (\neg P(x))$ for verdadeiro.

Exemplo 2.28

Considere o seguinte predicado $P(x)$, cujo domínio de x é o conjunto $D = \{1, 2, 3, 5, 8, 13, 21\}$:

$$P(x) : x \text{ é um número composto}^a.$$

A proposição $\exists x P(x)$ é verdadeira, pois se tomarmos $x = 8$, então temos que $P(x)$ é verdadeiro, uma vez que basta que exista um número $x \in D$ para o qual $P(x)$ é verdadeiro. Agora suponha que o domínio de x é o conjunto D' de todos os números primos. Nesse caso, a proposição $\exists x \in D', P(x)$ é falsa, pois todo número $x \in D'$ é primo (não é composto), e portanto $\forall x \in D', \neg P(x)$ é verdadeiro.

^aUm número *composto* é um número natural maior que 1 que não é primo.

Caso você estivesse muito atento ao ler o exemplo anterior, pode ter percebido que talvez haja uma relação entre os quantificadores universal e existencial, de um modo bem amplo. De fato, a negação da proposição $\exists x P(x)$ é a proposição $\forall x (\neg P(x))$. Pois a fim de que $\exists x P(x)$ seja falso, devemos ter $P(x)$ falso para todo x em seu domínio. Por outro lado, a negação da proposição $\forall x P(x)$ é a proposição $\exists x (\neg P(x))$. Pois agora, a fim de que $\forall x P(x)$ seja falso, devemos ter $P(x)$ falso para algum x em seu domínio. O símbolo $\nexists$ é uma notação bastante comum para a negação do quantificador existencial. O equivalente para o quantificador universal já não é tão comum.

Agora que já entendemos os quantificadores, estamos prontos para formular expressões lógicas mais complexas. Por exemplo, se $P(x, y)$ é um predicado com duas variáveis x e y cujos domínios são X e Y , respectivamente, então podemos

considerar a seguinte proposição:

$\forall x \exists y P(x, y)$: Para todo $x \in X$, existe $y \in Y$ para o qual é verdade que $P(x, y)$.

De forma similar, podemos considerar a proposição $\exists x \forall y P(x, y)$, ou a proposição $\forall x \forall y P(x, y)$, ou ainda a proposição $\exists x \exists y P(x, y)$. Essas duas últimas, no caso em que as variáveis x e y possuem o mesmo domínio, é comum escrevermos apenas $\forall x, y P(x, y)$ ou $\exists x, y P(x, y)$.

Atenção especial deve ser dada à ordem dos quantificadores. Por exemplo, as proposições $\forall x \exists y P(x, y)$ e $\exists x \forall y P(x, y)$ não são equivalentes. Por exemplo, se $P(x, y)$ é o predicado " $x + y = 1$ ", então $\forall x \exists y P(x, y)$ é verdadeiro, pois para cada x existe um y tal que $x + y = 1$. No entanto, $\exists x \forall y P(x, y)$ é falso, pois não existe um x tal que $x + y = 1$ para todo y .

Leia o seguinte exemplo com atenção, pois agora conseguimos conectar os quantificadores com o conceito de limite que você viu ou verá em suas aulas de cálculo.

Exemplo 2.30

A definição de limite de uma função real é comumente formulada com a ajuda de quantificadores lógicos. Por exemplo, suponha que f é uma função real definida em um intervalo aberto^a contendo um número real a .

Dizemos que $\lim_{x \rightarrow a} f(x) = L$ se é verdade que para todo número real $\varepsilon > 0$, existe um número real $\delta > 0$ tal que $|f(x) - L| \leq \varepsilon$, sempre que x é um número real satisfazendo $|x - a| \leq \delta$ (veja a Figura 2.1 para uma visualização). Podemos escrever essa definição da seguinte forma:

$$\lim_{x \rightarrow a} f(x) = L : \forall \varepsilon > 0, \exists \delta > 0, \forall x \in \mathbb{R} (|x - a| \leq \delta \rightarrow |f(x) - L| \leq \varepsilon).$$

A negação da proposição acima então tem a seguinte forma:

$$\lim_{x \rightarrow a} f(x) \neq L : \exists \varepsilon > 0, \forall \delta > 0, \exists x \in \mathbb{R} (|x - a| \leq \delta \wedge |f(x) - L| > \varepsilon).$$

Em particular, dizemos que o limite de f em a existe se $\exists L \in \mathbb{R} (\lim_{x \rightarrow a} f(x) = L)$. Portanto, o simples fato de que existe o limite de uma função em um ponto específico envolve o uso de quatro quantificadores lógicos.

^aUm intervalo aberto (c, d) é o conjunto $\{x \in \mathbb{R} : c < x < d\}$, com $c, d \in \mathbb{R}$.

Por fim, definimos um último quantificador que é uma variante do quantificador existencial e que é bastante utilizado em matemática.

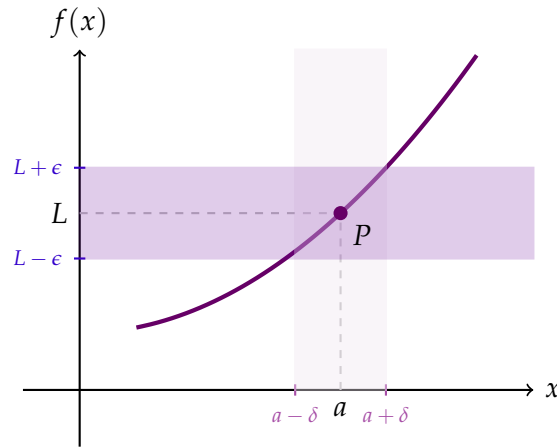


Figura 2.1: Representação visual da definição de limite.

Definição 2.31

Seja $P(x)$ um predicado e D o domínio de x . Denotamos por $\exists!x \in D, P(x)$ a proposição que afirma que $P(x)$ é verdadeiro para exatamente um $x \in D$. Escrevemos $\exists!x \in D, P(x)$, corresponde à proposição dada pela seguinte afirmação:

$\exists!x \in D, P(x) : \text{Existe um único } x \in D \text{ para o qual é verdade que } P(x).$

Quando o domínio de x estiver claro pelo contexto, podemos escrever somente $\exists!xP(x)$ em vez de $\exists!x \in D, P(x)$.

Em outras palavras, $\exists!xP(x)$ significa que $\exists xP(x)$ é uma proposição verdadeira e, adicionalmente, se x e y são variáveis para os quais $P(x)$ e $P(y)$ são ambos verdadeiros, então devemos ter $x = y$. Podemos expressar isto da seguinte forma:

$$\exists!xP(x) : (\exists xP(x)) \wedge (\forall x, y((P(x) \wedge P(y)) \rightarrow (x = y))).$$

Exemplo 2.32

Considere o seguinte predicado $P(x)$, cujo domínio de x é o conjunto $D = \{2, 4, 8, 16, 32, 64\}$:

$P(x) : x \text{ é um número primo.}$

Então a proposição $\exists!xP(x)$ é verdadeira, pois existe apenas um número primo pertencente ao conjunto D , a saber, $x = 2$. Mas digamos que o domínio de x é, na verdade, o conjunto dos números inteiros positivos. Então, neste caso, a proposição $\exists!xP(x)$ é falsa, pois 2 e 3 são dois elementos no domínio de x para

o qual $P(x)$ é verdadeiro. Agora suponha que o domínio de x é o conjunto $D = \{1, 4, 6, 8, 9, 10, 12\}$. Nesse caso, a proposição $\exists!xP(x)$ também é falsa, pois não existe nenhum $x \in D$ para o qual $P(x)$ é verdadeira.

Note que a negação de $\exists!xP(x)$ é equivalente a dizer que $P(x)$ é falso, para todo x , ou que existem dois elementos distintos x e y no domínio para os quais temos $P(x)$ e $P(y)$ ambos verdadeiros. Isto é,

$$\neg \exists!xP(x) : (\forall x \neg P(x)) \vee (\exists x, y (P(x) \wedge P(y) \wedge (x \neq y))).$$

2.4 Estratégias de prova

Muitas vezes, a demonstração de uma propriedade matemática envolve a manipulação de sentenças que contêm quantificadores. Nesta seção, exploraremos como a estrutura dos quantificadores $\forall$ e $\exists$ orienta o fluxo de uma prova e como podemos utilizar os conceitos de lógica proposicional para validar afirmações que dependem de variáveis em um domínio. Considere a seguinte proposição:

Proposição 2.33

Seja $x \in \mathbb{Z}$. Se $3x + 3$ é par, então x é ímpar.

Vamos demonstrar a Proposição 2.33 de três formas diferentes: *prova direta*, *prova por contrapositiva* e *prova por contradição*. Note que não é necessário escrever a Proposição 2.33 como: $P(x) : \forall x \in \mathbb{Z}, 3x + 3 \text{ é par} \rightarrow (x \text{ é ímpar})$. Utilizamos a linguagem por extenso para facilitar a compreensão e fluidez da leitura.

2.4.1 Direta

Iniciamos com uma prova direta, que dadas proposições $p_1, p_2, \dots, p_k$ que sabemos que são verdadeiras como premissas, utilizamos as regras de lógica proposicional para concluir que uma proposição q é verdadeira. Por exemplo, na Proposição 2.33, temos duas premissas (ou hipóteses): “ $x \in \mathbb{Z}$ ” e “ $3x + 3$ é par”. Nosso objetivo é concluir que a proposição “ x é ímpar” é verdadeira.

Prova da Proposição 2.33 - Direta. Suponha que x é um inteiro e que $3x + 3$ é par. Como $3x + 3$ é par, existe $k \in \mathbb{Z}$ tal que $3x + 3 = 2k$. Assim, isolando o termo que contém x , temos que

$$3x = 2k - 3 = 2(k - 2) + 1,$$

que mostra que $3x$ é ímpar. Como o produto de dois números (nos referimos aos números 3 e x é ímpar se e somente se ambos são ímpares, e 3 é ímpar, então x certamente é ímpar. $\square$

Perceba que o que fizemos na demonstração acima foi provar uma série de implicações lógicas. De fato, considere as seguintes proposições:

- q : O produto de dois números é ímpar se e somente se ambos são ímpares.
- r : 3 é ímpar.
- $P_1(x)$: $x \in \mathbb{Z}$;
- $P_2(x)$: $3x + 3$ é par;
- $P_3(x)$: $\exists k \in \mathbb{Z}$ tal que $3x + 3 = 2k$;
- $P_4(x)$: $3x$ é ímpar;
- $Q(x)$: x é ímpar.

Note que a demonstração que fizemos da Proposição 2.33, em que inicialmente supomos que $P_1(x)$ e $P_2(x)$ são verdadeiras e nosso objetivo é confirmar $Q(x)$.

$$P_1(x) \wedge P_2(x) \rightarrow P_3(x) \rightarrow P_4(x).$$

Como $P_4(x)$ é verdadeira, temos

$$P_4(x) \wedge q \wedge r \rightarrow Q(x).$$

Mas concordemos que seria muito entediante ler uma prova como essa, especialmente dado que sabemos escrever uma prova bem mais fluida como a que escrevemos na prova direta. Mas talvez você ainda assim não tenha ficado satisfeito com a demonstração que apresentamos. Apresentamos a seguir uma outra estratégia para demonstrar resultados matemáticos.

2.4.2 Contrapositiva

Lembre da Definição 2.19 que, dadas proposições p e q , a expressão $\neg q \rightarrow \neg p$ é o que chamamos de contrapositiva da proposição $p \rightarrow q$. Na prova a seguir, vamos utilizar essa estratégia para provar a Proposição 2.33.

Prova da Proposição 2.33 - Contrapositiva. Mostraremos, por contrapositiva, que se x não é ímpar (ou seja, x é par), então $3x + 3$ não é par (ou seja, $3x + 3$ é ímpar).

Assim, suponha que x seja um número inteiro par. Assim, por definição, existe um inteiro k tal que $x = 2k$. Portanto,

$$3x + 3 = 3(2k) + 3 = 6k + 3 = 6k + 2 + 1 = 2(3k + 1) + 1.$$

Note que como k é um inteiro, $3k + 1$ também é um inteiro. Assim, Pela igualdade acima, concluimos que $3x + 3$ é ímpar. $\square$

2.4.3 Contradição

Apresentamos ainda uma outra forma de demonstrar resultados matemáticos, em que assumimos que o que queremos provar é falso e mostramos que isso leva a uma contradição, algum absurdo. Antes de apresentarmos a prova, vamos inicialmente entender exatamente que proposição estamos querendo provar, que é a seguinte proposição q em que $P(x)$ e $Q(x)$ são, respectivamente “ $3x + 3$ é par” e “ x é ímpar”.

$$q : \forall x \in \mathbb{Z}, P(x) \rightarrow Q(x).$$

Lembre que, dadas proposições p e q , a expressão $\neg(p \rightarrow q)$ é equivalente a $p \wedge \neg q$. Assim, nosso objetivo é equivalente a mostrar que a proposição

$$q : \forall x \in \mathbb{Z}, P(x) \wedge \neg Q(x).$$

é verdadeira e é exatamente o que fazemos na demonstração a seguir.

Prova da Proposição 2.33 - Contradição. Suponha, por contradição, que $3x + 3$ é par e que x é par. Como x é par, existe um inteiro k tal que $x = 2k$. Assim, temos que

$$3x + 3 = 3(2k) + 3 = 6k + 3 = 2(3k + 1) + 1.$$

Logo, $3x + 3$ é ímpar. Porém sabemos, por hipótese, que $3x + 3$ é par, uma contradição, uma vez que nenhum número é par e ímpar ao mesmo tempo. Logo, nossa suposição de que x é par estava errada, e portanto x é ímpar. $\square$

Vale à pena refletirmos sobre o porquê da prova por contradição ser de fato uma demonstração válida. Utilizamos a prova por contradição para provar uma afirmação do tipo $p \rightarrow q$. Inicialmente **supomos** que a afirmação é falsa, i.e., que $p \wedge \neg q$ (que é equivalente a $\neg(p \rightarrow q)$) é verdadeira. Com isso, temos como hipótese para utilizar em nossa prova que p e $\neg q$ são verdadeiras. Utilizando esses fatos e implicações lógicas, obtemos novas proposições $p_1, p_2, \dots, p_k$, até que chegamos a uma contradição (uma proposição cujo valor-verdade é sempre F. No

caso, obtivemos a proposição “ $3x + 3$ é par e $3x + 3$ é ímpar”, que é falsa). Para uma melhor visualização, note que seguimos a sequência abaixo de implicações lógicas, obtendo sempre proposições verdadeiras, até que chegamos a uma contradição.

$$\neg(p \rightarrow q) \rightarrow p_1 \rightarrow p_2 \rightarrow \cdots \rightarrow p_k \rightarrow F.$$

Mas como $p_1, p_2, \dots, p_k$ são verdadeiras e a implicação $p_k \rightarrow F$ é verdadeira, a única possibilidade de se obter uma contradição como obtemos é termos iniciado a prova com uma proposição falsa. Mas a proposição que começamos foi $\neg(p \rightarrow q)$. Portanto, como concluímos que $\neg(p \rightarrow q)$ não é válida, sua negação, que é $p \rightarrow q$, é verdadeira.

2.5 Escolhendo a melhor estratégia de demonstração

No caso da Proposição 2.33, em que mostramos que se um número inteiro x é tal que $3x + 3$ é par, então x é ímpar, percebemos que todas as estratégias que utilizamos nos forneceram provas simples. No entanto, a escolha da estratégia de prova pode fazer a diferença para conseguirmos demonstrar um resultado ou não. Vamos analisar o seguinte resultado simples.

Teorema 2.34

Sejam x e y números reais positivos. Se $xy > 100$, então $x > 10$ ou $y > 10$.

Sem pensar muito, podemos imediatamente partir para uma prova direta. Vamos analisar com cuidado a prova abaixo.

Prova direta do Teorema 2.34. Suponha que $xy > 100$. Queremos mostrar que $x > 10$ ou $y > 10$. Para isso, consideremos dois casos possíveis de valores para x : certamente temos que ou $x \leq 10$ ou $x > 10$. Ora, mas se $x > 10$, então já obtivemos o que queríamos demonstrar, de modo que podemos assumir daqui por diante que $x \leq 10$.

Como sabemos que x é positivo, podemos dividir ambos os lados da nossa hipótese por x sem alterar o sinal da desigualdade, obtendo

$$y > \frac{100}{x}.$$

Sabendo que $0 < x \leq 10$, temos $1/x \geq 1/10$. Assim, multiplicando ambos os

lados por 100 (que é positivo), obtemos

$$\frac{100}{x} \geq \frac{100}{10} = 10.$$

Finalmente, concluímos que

$$y > \frac{100}{x} \geq 10.$$

Logo, $y > 10$. Portanto, mostramos que ou $x > 10$ ou $y > 10$, que ocorre sempre que $x < 10$. Em ambos os casos temos $x > 10$ ou $y > 10$, como queríamos. $\square$

Podemos nos dar por satisfeitos, mas vamos analisar como ficaria uma prova por contradição. O ponto chave que devemos entender é o seguinte: na prova direta, supomos inicialmente que $xy > 100$, mas isso não nos fornece uma informação imediatamente útil. Foi preciso utilizar esse fato para obter $y > 100/x$, mas essa informação foi útil somente após percebermos que por podermos assumir (nesse ponto da prova) que $x \leq 10$, que conseguimos combinar esses dois fatos para mostrar que $y \geq 10$.

Mas se tentarmos provar o resultado por contradição, inicialmente consideramos dois números reais x e y quaisquer e assumimos que o resultado é falso, isto é, que $\neg(xy > 100) \rightarrow (x > 10 \vee y > 10)$, que é equivalente a $xy > 100 \wedge \neg(x > 10 \vee y > 10)$, que é equivalente a $xy > 100 \wedge x \leq 10 \wedge y \leq 10$, que é a forma que iremos utilizar (ufa!). Mas assim, já começamos com três proposições para trabalharmos, $xy > 100$, $x \leq 10$ e $y \leq 10$, e nosso objetivo é chegar em alguma contradição. Vejamos como a prova por contradição fica simples, curta e elegante nesse caso.

Demonstração por contradição do Teorema 2.34. Dados inteiros positivos x e y , suponha por contradição que $xy > 100$ e

$$x \leq 10 \text{ e } y \leq 10. \tag{2.1}$$

Pelas desigualdades em (2.1), temos $xy \leq 100$, uma contradição com $xy > 100$. $\square$

Mas caso você ainda não esteja satisfeito com nossa prova, você pode pensar que talvez seja uma pessoa que não se dá muito bem com contradições. Mas neste caso você está completamente certo. Ao buscar uma prova por contrapositiva, nos deparamos com um argumento ainda mais simples.

Demonstração por contrapositiva do Teorema 2.34. Suponha que x e y sejam inteiros positivos e que $x \leq 10$ e $y \leq 10$. Assim, $xy \leq 100$. $\square$

Para que não passemos a impressão de que sempre a prova direta é mais complicada que a Demonstração por contradição, e que essa é mais complicada que a prova por contrapositiva, vamos analisar um outro resultado. Mais uma vez, demonstraremos o mesmo resultado de três maneiras diferentes. Motivados pelo exemplo anterior, podemos nos jogar diretamente em uma prova por contrapositiva.

Teorema 2.35

Seja x um número real. Se $0 < x < 1$, então $x^2 < x$.

Demonstração do Teorema 2.34 por contrapositiva. Suponha que $x^2 \geq x$. Queremos mostrar que não vale que $0 < x < 1$, mas isso é uma conjunção disfarçada, que equivale a $x > 0$ e $x < 1$. Assim, nosso objetivo é provar que $x \leq 0$ ou $x \geq 1$. Como $x^2 \geq x$, temos que $x^2 - x \geq 0$, que fatoramos da seguinte forma:

$$x(x - 1) \geq 0.$$

Para que o produto de dois números reais seja não negativo, existem duas possibilidades, que analisamos a seguir, mostrando que temos $x \geq 1$ em um caso e $x \leq 0$ no outro.

Caso 1 ($x \geq 0$ e $x - 1 \geq 0$): Por hipótese, vale que $x \geq 1$.

Caso 2 ($x \leq 0$ e $x - 1 \leq 0$): Por hipótese, temos $x \leq 0$.

Como no primeiro caso obtivemos $x \geq 1$ e no segundo caso $x \leq 0$, em ambos os casos conseguimos mostrar que $x \geq 1$ ou $x \leq 0$, como queríamos. $\square$

Agora que temos um pouco de experiência, talvez essa prova cause um certo incômodo, talvez algo nos diga que há uma prova mais simples. Por que esse sentimento surge? Essencialmente, a lógica nos forçou a transformar um problema simples de desigualdade em um estudo de sinais de uma parábola. A introdução do conectivo “ou” exigiu uma ramificação em casos, aumentando a chance de cometermos erros.

O problema de analisar uma disjunção some quando fazemos uma prova por contradição, pois iremos supor que a hipótese $x > 0$ e $x < 1$ é verdadeira, e que $x^2 \geq x$.

Demonstração por contradição do Teorema 2.34 por contradição. Suponha, por contradição, que $x > 0$ e $x < 1$ e que $x^2 \geq x$. Como $x > 0$ podemos dividir ambos os lados da nossa suposição $x^2 \geq x$ por x sem alterar o sinal da desigualdade, obtendo $x \geq 1$, o que contradiz a hipótese de que $x < 1$. $\square$

Perceba que essa prova é consideravelmente mais clara e curta que a prova que demos por contradição. Mas no caso desse resultado, a prova direta consegue ser ainda mais curta e simples.

Prova direta do Teorema 2.34. Suponha que $x > 0$ e $x < 1$. Como x é positivo, de $x < 1$, temos que $x^2 < x$, como queríamos. $\square$

Teoria básica de conjuntos

Para avançarmos na matemática formal, precisamos de uma base sólida. A Teoria dos Conjuntos nos fornece essa base.

Definição 3.1

Um *conjunto* é, de forma intuitiva, uma coleção bem definida de objetos. Esses objetos são chamados de *elementos* ou *membros* do conjunto e a relação de pertinência é denotada por $a \in A$ (lê-se " a pertence a A "). A quantidade de elementos de um conjunto A é chamada de *cardinalidade* de A e é denotada por $|A|$.

Por exemplo, a cardinalidade do conjunto $A = \{1, 2, \dots, 10\}$ é $|A| = 10$.

Definição 3.2

Dizemos que um conjunto A é *subconjunto* de B , denotado por $A \subseteq B$, se todo elemento de A também é elemento de B .

Vamos escrever $A \not\subseteq B$ para denotar que A não é subconjunto de B . É importante notar que, para todo conjunto X , temos que $X \subseteq X$, uma vez que, obviamente, todos os elementos de X pertencem a X . No início, precisamos ter um cuidado para não confundir elementos e subconjuntos de um conjunto. Por exemplo, para o conjunto $A = \{1, 2, 3, \{1\}, \{1, 4\}\}$ temos $|A| = 5$ e $\{1, 4\}$ é um elemento de A (i.e., $\{1, 4\} \in A$) mas $\{1, 4\}$ não é subconjunto de A (i.e., $\{1, 4\} \not\subseteq A$), uma vez que apesar de $1 \in A$, temos que $4 \notin A$. Por outro lado, devemos agora conseguir perceber que $\{1\} \in A$ e $\{1\} \subseteq A$.

Mas nem todos os conjuntos têm uma quantidade finita de elementos. Já estamos acostumados com conjuntos assim, como por exemplo os conjuntos a seguir que já são de conhecimento de todos nós:

- *Naturais*: $\mathbb{N} = \{1, 2, 3, \dots\}$;
- *Inteiros*: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- *Racionais*: $\mathbb{Q} = \{x : \text{existem inteiros } p \text{ e } q \text{ com } q \neq 0 \text{ e } x = p/q\}$;
- *Irracionais*: números que não podem ser expressos como razão de dois inteiros, como $\sqrt{2}$ e π ;
- *Reais*: $\mathbb{R}$ (o conjunto dos números que são racionais ou irracionais).

Por enquanto, vamos ficar apenas com essa noção simplista sobre infinito. Ao final deste livro trabalharemos esse fascinante tópico com a atenção que ele merece. Tendo discutido conjuntos de cardinalidade infinita, precisamos falar do outro extremo, de um conjunto de cardinalidade zero.

Definição 3.3

O *conjunto vazio*, denotado por $\emptyset$, é o único conjunto que não possui elementos, tendo assim cardinalidade zero, i.e., $|\emptyset| = 0$.

Não confunda $\emptyset$ com $\{\emptyset\}$, que é um conjunto cuja cardinalidade é 1, pois contém o conjunto vazio como elemento.

Em matemática, existem muitas formas úteis e práticas de se definir um conjunto. Por exemplo, considere o conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$. Já temos utilizado a notação natural $\{1, 2, \dots, 15\}$ para denotar o mesmo conjunto. Mas outras formas de definir o mesmo conjunto são

$$A = \{x : x \in \mathbb{Z} \text{ e } 1 \leq x \leq 15\},$$

$$A = \{x : x \in \mathbb{N} \text{ e } x \leq 15\}, \text{ e}$$

$$A = \{x : x \in \mathbb{N} \text{ e } x < 16\}.$$

3.1 Operações com conjuntos

Algumas operações são essenciais entre conjuntos e podemos combiná-las de várias formas. Apresentamos a seguir algumas operações básicas sobre conjuntos. Veja a Figura 3.1 para uma representação visual das operações definidas a seguir.

Definição 3.4

Dados conjuntos A e B , definimos as operações de união, interseção e diferença como segue.

- *União:* $A \cup B = \{x : x \in A \text{ ou } x \in B\}$;
- *Interseção:* $A \cap B = \{x : x \in A \text{ e } x \in B\}$;
- *Diferença:* $A \setminus B = \{x : x \in A \text{ e } x \notin B\}$.

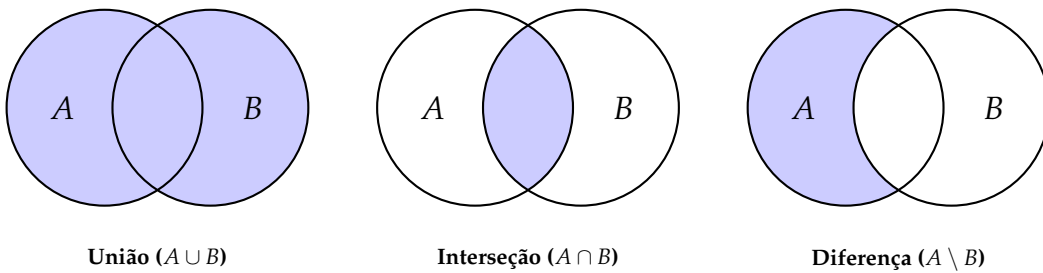


Figura 3.1: Diagramas de Venn representando as operações básicas com conjuntos.

Podemos generalizar essas operações naturalmente para múltiplos conjuntos $A_1, \dots, A_n$, como a união desses n conjuntos, que é denotada por $\bigcup_{i=1}^n A_i$, além da interseção deles, que é denotada por $\bigcap_{i=1}^n A_i$.

Apresentamos um resultado clássico que relaciona a cardinalidade da união de conjuntos com a cardinalidade de suas interseções. Trata-se de um aperitivo para algumas técnicas que exploraremos adiante no curso.

Teorema 3.5

Sejam A e B dois conjuntos finitos. A cardinalidade de $A \cup B$ é dada por

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Demonstração. Ao somarmos as cardinalidades $|A|$ e $|B|$ com o intuito de obter o total de elementos da união, estamos contabilizando os elementos que estão em A e os elementos que estão em B . No entanto, acabamos contando os elementos da interseção $A \cap B$ exatamente duas vezes (uma vez quando somamos $|A|$ e outra quando somamos $|B|$). Para corrigir essa contagem duplicada e obter exatamente a quantidade de elementos de $A \cup B$, basta subtrairmos a cardinalidade da interseção $|A \cap B|$ uma vez, chegando ao resultado desejado. $\square$

Além de resultados envolvendo a cardinalidade de conjuntos, é importante

estabelecer propriedades que regem as operações fundamentais. A proposição a seguir descreve como a interseção se distribui em relação à união.

Proposição 3.6

Dados conjuntos A , B e C , vale que

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

Antes de iniciarmos a prova, observe que para mostrar que dados conjuntos X e Y , temos $X = Y$, devemos mostrar que $X \subseteq Y$ e $Y \subseteq X$, que indicam que todo elemento de X é também elemento de Y e vice-versa. Assim, seguiremos essa estratégia, dividindo nossa demonstração em duas partes.

Demonstração da Proposição 3.6. Provaremos inicialmente que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Para isso, considere um elemento $a \in A \cap (B \cup C)$. Pela definição de interseção, sabemos que $a \in A$ e que também vale que $a \in B \cup C$. Como $a \in A$, se $a \in B$, temos que $a \in (A \cap B)$. Por outro lado, se $a \in C$, temos que $a \in (A \cap C)$. Portanto, concluímos que $a \in (A \cap B) \cup (A \cap C)$.

Resta demonstrar que se $a \in (A \cap B) \cup (A \cap C)$, então $a \in A \cap (B \cup C)$. De fato, se $a \in (A \cap B) \cup (A \cap C)$, então $a \in A \cap B$ ou $a \in A \cap C$. Em ambos os casos, $a \in A$. Além disso, se $a \in A \cap B$, então $a \in B$, o que implica $a \in B \cup C$. Analogamente, se $a \in A \cap C$, então $a \in C$, o que também implica $a \in B \cup C$. Portanto, $a \in A$ e $a \in B \cup C$, o que conclui a prova de que $a \in A \cap (B \cup C)$. $\square$

Tiremos um momento para refletir sobre a relação $A \subseteq B$ entre conjuntos A e B . Se comparamos com a relação de um número inteiro ser menor ou igual a outro, temos uma diferença fundamental: para quaisquer dois números inteiros a e b , sabemos que $a \leq b$ ou $b \leq a$. Por outro lado, para quaisquer dois conjuntos A e B , não é necessário que $A \subseteq B$ ou $B \subseteq A$. Por exemplo, se $A = \{1, 2, 3\}$ e $B = \{2, 3, 4\}$, temos que $A \not\subseteq B$ e $B \not\subseteq A$. Essa é uma observação óbvia, mas muito importante. Trataremos bem dessas relações mais adiante quando discutirmos *ordens parciais e totais*. Mas agora, consideremos a seguinte definição que trata daqueles conjuntos A e B em que é verdade que $A \subseteq B$ ou $B \subseteq A$.

Definição 3.7

Dizemos que dois conjuntos A e B são *comparáveis* se $A \subseteq B$ ou $B \subseteq A$, isto é, se um deles está contido no outro.

3.1.1 Conjuntos comparáveis

Considere novamente um conjunto qualquer A com n elementos e considere o problema de determinar o tamanho da maior quantidade de subconjuntos de A que podemos formar de modo que sejam dois a dois comparáveis. Para facilitar fazer referência a essa quantidade, dado um conjunto A , definimos a seguinte quantidade.

Definição 3.8

Seja A um conjunto qualquer. Defina

$C(A)$: maior quantidade de subconjuntos de A que são dois a dois comparáveis.

Assim, para resolver o problema em questão, nossa tarefa é determinar o valor de $C(A)$ para qualquer conjunto A .

Quando nos deparamos com um problema como esse, uma ideia inicial é observar alguns exemplos para tentar descobrir que valor estamos buscando. Bem, sem pensar muito, podemos tentar verificar se a família de todos os subconjuntos possíveis de A é dois a dois comparável. Dado um conjunto A com n elementos, quantos subconjuntos ele possui? Claramente, para cada elemento de A , temos duas opções: ou ele está ou não está no subconjunto. Portanto, dado um conjunto A com n elementos, podemos formar 2^n subconjuntos distintos. Assim, 2^n é nosso primeiro palpite ingênuo para o valor de $C(A)$. Porém, esse é um palpite ruim, pois em qualquer conjunto com pelo menos 3 elementos existem pares de subconjuntos que não são comparáveis. Por exemplo, para $A = \{1, 2, 3\}$, temos que os subconjuntos $\{1\}$ e $\{2\}$ de A não são comparáveis. Conseguimos assim nossa primeira relação a respeito do valor de $C(A)$. Mostramos que $C(A) \leq 2^n - 1$, mas certamente conseguimos fazer bem melhor que isso.

Vamos então observar um conjunto A pequeno, considerando que $n = 3$, somente para tentar ter uma ideia de como podemos construir uma grande coleção de subconjuntos comparáveis. Por exemplo, seja $A = \{a_1, a_2, a_3\}$ um conjunto qualquer com 3 elementos, percebemos facilmente ser possível formar uma coleção com 3 subconjuntos de A que são dois a dois comparáveis. De fato, considere a coleção de subconjuntos de A a seguir.

$$\mathcal{A} = \{\{a_1\}, \{a_1, a_2\}, \{a_1, a_2, a_3\}\}.$$

Note que quaisquer dois conjuntos de $\mathcal{A}$ são comparáveis. Assim, conseguimos uma coleção de 3 subconjuntos de A que são dois a dois comparáveis.

Tentemos agora estender a ideia discutida anteriormente para conjuntos A com

n elementos, para qualquer número natural n , e não somente $n = 3$. Para tanto, dado um conjunto $A = \{a_1, a_2, \dots, a_n\}$, considere a coleção

$$\mathcal{A} = \{\{a_1\}, \{a_1, a_2\}, \dots, \{a_1, a_2, \dots, a_{n-1}\}, \{a_1, a_2, \dots, a_{n-1}, a_n\}\}$$

e perceba que quaisquer dois conjuntos de $\mathcal{A}$ são comparáveis. Veja a Figura 3.2 para um esquema visual de $\mathcal{A}$. Conseguimos obter uma coleção de n subconjun-

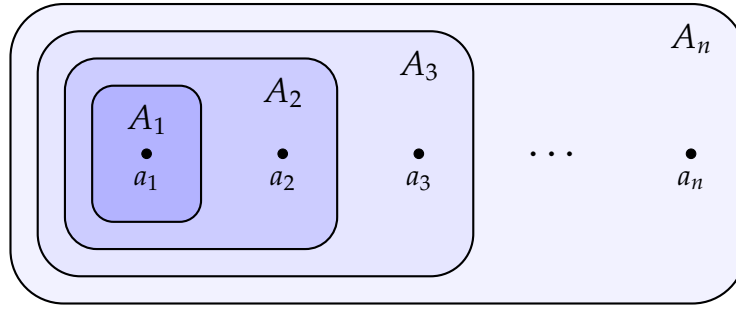


Figura 3.2: Representação de uma família de subconjuntos de A em que quaisquer dois elementos são comparáveis, com $A_1 \subseteq A_2 \subseteq \dots \subseteq A_n$.

tos de A que são comparáveis. Mas será então que $C(A) = n$? Lembrando da definição de $C(A)$: "maior quantidade de subconjuntos de A que são dois a dois comparáveis", percebemos que o que acabamos de demonstrar foi que $C(A) \geq n$, pois mostramos que sempre existem n subconjuntos de A que são dois a dois comparáveis. Mas então lembramos que dois conjuntos são comparáveis se um está contido no outro e que o conjunto vazio é subconjunto de qualquer conjunto. Ora, então podemos adicionar o conjunto vazio em nossa coleção! Assim, já sabemos que $C(A) \geq n + 1$, pois na família a seguir, qualquer par de seus elementos (que são subconjuntos de A) são comparáveis.

$$\mathcal{A} = \{\emptyset, \{a_1\}, \{a_1, a_2\}, \dots, \{a_1, a_2, \dots, a_{n-1}\}, \{a_1, a_2, \dots, a_{n-1}, a_n\}\}.$$

Mas será que agora acertamos? Talvez exista alguma coleção maior de subconjuntos de A em que seus elementos sejam dois a dois comparáveis.

No teorema a seguir demonstramos que também vale que $C(A) \geq n + 1$, de onde concluímos então que $C(A) = n + 1$. Para demonstrar esse resultado, faremos o seguinte: vamos provar que toda coleção com $n + 2$ subconjuntos de A sempre vai ter dois desses subconjuntos que não são comparáveis. Dessa forma, a maior quantidade possível desses subconjuntos é $n + 1$.

Teorema 3.9

Seja A um conjunto com n elementos. Então $C(A) \leq n + 1$.

Demonstração. Mostraremos que para toda família $\mathcal{A} = \{A_1, A_2, \dots, A_{n+2}\}$ de $n + 2$ subconjuntos de A , existem dois subconjuntos A_i e A_j de A que são não comparáveis. Seja $A_i \subseteq A$ um elemento qualquer de $\mathcal{A}$. Como A tem n elementos, a cardinalidade de A_i pode assumir valores no conjunto $\{0, 1, 2, \dots, n\}$, que tem cardinalidade $n + 1$. Logo, existem $n + 1$ cardinalidades possíveis para os elementos de $\mathcal{A}$. Mas como $\mathcal{A}$ tem $n + 2$ elementos, então obrigatoriamente dois elementos de $\mathcal{A}$, digamos A_i e A_j , certamente têm a mesma cardinalidade. Mas note que como A_i e A_j são conjuntos distintos, é impossível que tendo a mesma cardinalidade eles estejam um contido no outro. Portanto, concluímos que A_i e A_j não são comparáveis. Com isso, concluímos a prova do teorema. $\square$

3.1.2 Mais operações e identidades fundamentais

Além das três operações fundamentais já apresentadas, existem outras construções essenciais na Teoria dos Conjuntos. A fim de expandirmos nossa caixa de ferramentas, vamos definir um conjunto de referência, em que os elementos de todos os conjuntos que estamos trabalhando vão fazer parte. Em muitos contextos, todos os conjuntos discutidos são subconjuntos de um conjunto fixo maior.

Definição 3.10

Um *conjunto universo* (ou simplesmente *universo*), denotado por U , é o conjunto que contém todos os elementos da discussão aplicável.

Por exemplo, em uma disciplina em uma universidade, precisamos ter controle de diversos conjuntos de alunos, como aqueles que foram aprovados, os que ficaram de recuperação ou os que precisam de ajuda em um determinado tópico. Mas todos esses conjuntos têm em comum a propriedade que seus elementos são todos alunos da disciplina, que é o conjunto universo em questão. Com isso em mente, podemos definir a operação de complementar.

Definição 3.11

Dados conjuntos U e $A \subseteq U$, o *complementar* de A , denotado por A^c (ou $\overline{A}$), é o conjunto de todos os elementos de U que não pertencem a A , i.e.,

$$A^c = U \setminus A = \{x \in U : x \notin A\}.$$

As operações de união, interseção e complementar interagem entre si de maneiras muito bem comportadas. Duas relações importantes da teoria de conjuntos mostram como o complementar se distribui invertendo as operações de união e

interseção.

Teorema 3.12

Sejam A e B subconjuntos de um conjunto U . Então:

1. $(A \cup B)^c = A^c \cap B^c$;
2. $(A \cap B)^c = A^c \cup B^c$.

Demonstração. Provaremos aqui somente a primeira igualdade e deixamos a demonstração da segunda igualdade, que segue um raciocínio análogo, como exercício. Para mostrar que $(A \cup B)^c = A^c \cap B^c$, mostraremos a inclusão nos dois sentidos.

Primeiro, mostraremos que $(A \cup B)^c \subseteq A^c \cap B^c$. Seja $x \in (A \cup B)^c$. Por definição de conjunto complementar, temos que $x \notin A \cup B$. Consequentemente, x não pode pertencer a A e também não pode pertencer a B (pois se pertencesse a qualquer um dos dois, ele estaria na união $A \cup B$). Logo, $x \notin A$ e $x \notin B$. Isso implica diretamente que $x \in A^c$ e $x \in B^c$. Pela definição de interseção, concluímos que $x \in A^c \cap B^c$.

Agora, mostraremos que $A^c \cap B^c \subseteq (A \cup B)^c$. Seja $x \in A^c \cap B^c$. Isso significa que $x \in A^c$ e $x \in B^c$, ou seja, $x \notin A$ e $x \notin B$. Como x não pertence a nenhum dos dois conjuntos, ele certamente não pertence à união deles. Logo, $x \notin A \cup B$, o que por sua vez significa que $x \in (A \cup B)^c$.

Como provamos a inclusão em ambos os sentidos, concluímos que os conjuntos $(A \cup B)^c$ e $A^c \cap B^c$ são iguais. $\square$

Outra operação extremamente útil, com aplicações diretas na Ciência da Computação (por sua forte relação com o operador lógico XOR), é a diferença simétrica.

Definição 3.13

A *diferença simétrica* entre dois conjuntos A e B , denotada por $A \Delta B$, é o conjunto de elementos que pertencem a A ou a B , mas não a ambos, i.e.,

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

É um excelente exercício de fixação verificar que a diferença simétrica também pode ser expressa de uma segunda forma: $A \Delta B = (A \cup B) \setminus (A \cap B)$.

Uma última operação que descrevemos neste capítulo é a operação de produto cartesiano, que é uma operação entre conjuntos que, dados conjuntos A e B , gera

um novo conjunto $A \times B$ que é formado por todos os pares ordenados (a, b) em que $a \in A$ e $b \in B$.

Definição 3.15

Dados dois conjuntos A e B , o *produto cartesiano* de A e B , denotado por $A \times B$, é o conjunto formado por todos os pares ordenados (a, b) em que o primeiro elemento a pertence a A e o segundo elemento b pertence a B . Formalmente, $A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$.

Diferente de um conjunto $\{a, b\}$, a ordem dos elementos importa fundamentalmente em um par ordenado. Ou seja, se $a \neq b$, então o par (a, b) é estritamente diferente do par (b, a) .

Princípio da Casa dos Pombos

Apresentamos aqui um princípio simples, mas fundamental na matemática. Mesmo com pouquíssima informação sobre um problema, muitas vezes somos capazes de obter informações importantes para a resolução do problema. Uma das ferramentas que nos permitem obter informações valiosas é o *Princípio da Casa dos Pombos* (ou *Princípio das Gavetas de Dirichlet*).

A intuição por trás desse princípio é muito simples: se existem mais pombos que casas de pombos e todos os pombos entrarem em alguma casa, então uma casa obrigatoriamente terá mais de um pombo. Podemos escrever esse princípio de forma mais precisa como no resultado a seguir, que futuramente enunciaremos de forma mais precisa com funções.

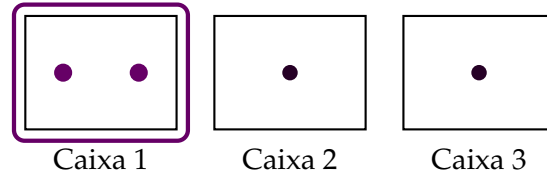
Teorema 4.1 (Princípio da Casa dos Pombos)

Sejam n e k inteiros positivos. Se n pombos são distribuídos em k caixas então vale o seguinte:

- (i) Se $n > k$, então pelo menos uma caixa tem mais de um pombo;
- (ii) Se $n < k$, então pelo menos uma caixa está vazia.

Prova do Teorema 4.1. Você perceberá que uma demonstração por contradição é ideal para esse resultado. Sejam $k_1, \dots, k_k$ as quantidades de pombos nas k casas.

Começemos provando (i). Seja $n > k$ e suponha por contradição que não existe



Pombos (n): 4
Casas (k): 3
Conclusão: pelo menos 1 caixa com 2 pombos.

Figura 4.1: Visualização do Princípio da Casa dos Pombos para $n = 4$ e $k = 3$.

nenhuma caixa com mais de um objeto. Então temos que

$$\sum_{i=1}^k k_i \leq \sum_{i=1}^k 1 = k < n. \quad (4.1)$$

Por outro lado, como todos os pombos entram em alguma casa, temos que

$$\sum_{i=1}^k k_i = n, \quad (4.2)$$

Combinando (4.1) e (4.2), obtemos

$$n = \sum_{i=1}^k k_i < n,$$

uma contradição.

Para provar (ii), seja $n < k$ e suponha por contradição que não existe nenhuma caixa vazia. Assim, utilizando (4.2), temos que $n = \sum_{i=1}^k k_i \geq k > n$, uma contradição. $\square$

Se estivermos atentos, perceberemos que a conclusão (i) do Teorema 4.1 na verdade é mais forte. Conseguimos muitas vezes garantir que em uma caixa temos não somente 2 objetos, mas vários. Para podermos descrever perfeitamente essa versão, precisamos definir dois conceitos simples, mas fundamentais: o *piso* e *teto* de um número real.

Definição 4.2

Dado $x \in \mathbb{R}$, definimos o *teto* e o *piso* de x , denotados respectivamente por $\lceil x \rceil$ e $\lfloor x \rfloor$, como

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\};$$

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}.$$

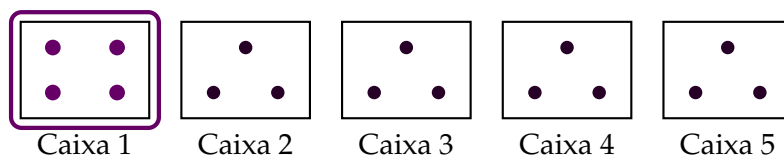
Com essas definições em mãos, podemos perceber que na verdade, o Princípio da Casa dos Pombos pode ser enunciado da seguinte forma, que conclui algo mais forte que o Teorema 4.1 (veja a Figura 4.2).

Teorema 4.3 (Versão mais forte do Princípio da Casa dos Pombos)

Sejam n e k inteiros positivos. Se n objetos são distribuídos em k caixas então

- (i) pelo menos uma caixa tem pelo menos $\lceil n/k \rceil$ objetos;
- (ii) pelo menos uma caixa tem no máximo $\lfloor n/k \rfloor$ objetos.

Experimente provar esse resultado.



Pombos (n): 16

Casas (k): 5

Conclusão: pelo menos 1 caixa com $\geq \lceil 16/5 \rceil = 4$.

Figura 4.2: Visualização da versão forte do Princípio da Casa dos Pombos para $n = 16$ e $k = 5$.

4.1 Aplicações do Princípio da Casa dos Pombos

Vamos explorar alguns exemplos simples, do cotidiano, bem como alguns exemplos matemáticos abstratos, para entendermos bem como aplicar o Princípio da Casa dos Pombos. No início, pode não ser imediato como associar caixas e pombos a estruturas de nosso problema. Mas rapidamente nossa mente estará acostumada com problemas desse tipo e essa associação será feita tranquilamente. Começemos com um exemplo bem simples.

A partir de agora, iremos nos referir a um resultado simples por "Afirmção".

Afirmção 4.4

Em uma grande metrópole como São Paulo, existem pelo menos duas pessoas com *exatamente* o mesmo número de fios de cabelo na cabeça.

Demonstração. Para aplicar o princípio, precisamos identificar quem são os pombos e quem são as casas em nossa modelagem do problema.

- **As Casas:** A biologia nos diz que o número máximo de fios de cabelo na cabeça de um ser humano certamente não passa de 199.999. Podemos considerar que os números possíveis de fios de cabelo (de 0 até 199.999) representam as nossas “casas”, totalizando $k = 200.000$ casas.
- **Os Pombos:** A população da cidade de São Paulo tem mais de 11 milhões e 300 mil habitantes. Nossos “pombos” são os habitantes, logo, $n > 11.300.000$.

Como o número de habitantes (n) é imensamente maior que o número de quantidades possíveis de fios de cabelo (k), o Princípio da Casa dos Pombos não deixa margem para dúvidas: existem duas pessoas com o mesmo número de fios de cabelo. $\square$

Uma vez que aprendemos a versão mais forte do Princípio da Casa dos Pombos (Teorema 4.3), já conseguimos imaginar que na verdade mais que 2 pessoas devem ter a mesma quantidade de fios de cabelo. De fato, pelo Teorema 4.3 (item (i)), pelo menos uma caixa tem pelo menos $\lceil n/k \rceil$ objetos, que em nosso caso implica

$$\lceil 11.300.000/200.000 \rceil = \lceil 56,5 \rceil = 57$$

pessoas com a mesma quantidade de fios de cabelo.

Após provar um resultado, devemos sempre nos questionar se a conclusão obtida é a mais forte possível. No exemplo anterior, concluimos corretamente que existem pelo menos 2 pessoas com a mesma quantidade de fios de cabelo. Mas essa conclusão não é a mais forte possível, pois como verificamos, na verdade existem pelo menos 57 pessoas com a mesma quantidade de fios de cabelo.

O exemplo a seguir ilustra como o Princípio da Casa dos Pombos nos ajuda a encontrar garantias em problemas de contagem, eliminando qualquer dependência do acaso.

Afirmção 4.6

Sejam k , ℓ , e m inteiros positivos. Na gaveta de um quarto totalmente escuro há k meias pretas, ℓ meias brancas e m meias azuis (todas soltas e misturadas). O número mínimo de meias que devemos retirar para formar um par da mesma cor é 4.

Demonstração. A intuição inicial poderia sugerir o cálculo de proporções ou analisar a sorte, mas basta utilizar o Princípio da Casa dos Pombos.

- **As Casas:** As cores disponíveis definem nossas restrições: preto, branco e azul. Temos $m = 3$ casas.
- **Os Pombos:** As meias que você tira da gaveta. Queremos saber quantos pombos (n meias) precisamos retirar para garantir que 2 pombos (meias) estejam na mesma casa (tenham a mesma cor).

Se você retirar 3 meias (pombos), o pior cenário possível é ter o maior azar do mundo e retirar exatamente uma meia de cada cor, preenchendo as 3 casas. Mas, ao retirar a quarta meia ($n = 4$), passamos a ter 4 pombos para 3 casas. Obrigatoriamente, pelo Teorema 4.1, essa quarta meia terá que combinar com a cor de uma das três meias retiradas anteriormente. Logo, a resposta para garantir um par é 4. $\square$

Podemos também aplicar o Princípio da Casa dos Pombos em problemas de geometria, como veremos a seguir.

Afirmção 4.7

Seja Q um quadrado de lado 2. Se 5 pontos são colocados em qualquer lugar dentro ou na borda de Q , então sempre haverá pelo menos dois pontos cuja distância geométrica entre eles seja no máximo $\sqrt{2}$.

Demonstração. Divida o quadrado Q de lado 2 em quatro quadrados menores e congruentes, de lado 1, como na Figura 4.3. Estas serão as nossas $m = 4$ casas. Temos $n = 5$ pontos (nossos pombos) que foram distribuídos dentro de Q .

Como $n > m$, o princípio garante que pelo menos um desses 4 quadrados menores deverá conter dois ou mais pontos em seu interior (ou fronteira). Agora, avaliemos a geometria dessa região restrita: qual é a distância máxima possível entre dois pontos confinados em um mesmo quadrado de lado 1?

Pelo Teorema de Pitágoras (Teorema 1.2), a maior distância ocorre quando os pontos habitam vértices opostos, correspondendo à medida da diagonal do

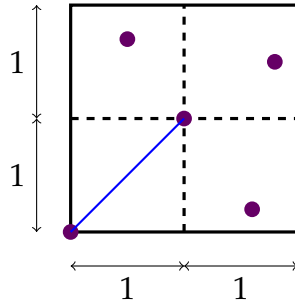


Figura 4.3: Quadrado de lado 2 subdividido em quatro quadrados de lado 1.

quadrado menor, que é $\sqrt{1^2 + 1^2} = \sqrt{2}$. Portanto, a distância entre os dois pontos confinados nesse quadrado menor é no máximo $\sqrt{2}$. $\square$

O exemplo a seguir ilustra uma estratégia que faz uso da interseção de conjuntos, juntamente com o Princípio da Casa dos Pombos, para provar um resultado numérico sobre pares de inteiros. Essa é uma ideia simples e interessante, que é útil em outros contextos.

Afirmção 4.8

Em qualquer conjunto de $n + 1$ inteiros distintos em $[2n] = \{1, 2, \dots, 2n\}$, existem dois números cuja soma é $2n + 1$.

Demonstração. Seja $A \subseteq [2n]$ um conjunto com $n + 1$ elementos. Queremos provar que existem dois elementos distintos $x, y \in A$ tais que $x + y = 2n + 1$.

Vamos construir um novo conjunto B formado pela diferença entre $2n + 1$ e os elementos de A :

$$B = \{2n + 1 - a : a \in A\}.$$

Note que, como todo elemento de A pertence a $[2n]$, temos $1 \leq a \leq 2n$ e, portanto, $1 \leq 2n + 1 - a \leq 2n$. Logo, os elementos de B também pertencem ao mesmo universo, ou seja, $B \subseteq [2n]$. Além disso, cada elemento de A gera exatamente um elemento em B . Logo, temos que $|B| = |A| = n + 1$. Portanto,

$$|A| + |B| = (n + 1) + (n + 1) = 2n + 2 > 2n = |[2n]|.$$

Assim, sabemos (pelo Princípio da Casa dos Pombos) que $A \cap B \neq \emptyset$, de modo que existe pelo menos um elemento $k \in A \cap B$.

Como $k \in B$, sabemos que $k = 2n + 1 - a$ para algum $a \in A$ (pela definição do conjunto B), de onde concluímos que

$$a + k = 2n + 1. \tag{4.3}$$

Por outro lado, como a e k são elementos de A , encontramos dois elementos do nosso conjunto original cuja soma resulta em $2n + 1$.

Resta garantir que $a \neq k$. Mas se tivéssemos $a = k$, então $a + k$ é par, contradizendo (4.3). Portanto, $a \neq k$ e assim concluímos que sempre haverá pelo menos dois números distintos escolhidos cuja soma totaliza $2n + 1$. $\square$

Finalizamos este capítulo discutindo *conjuntos livres de soma*, em que utilizamos $[n]$ para denotar o conjunto $\{1, 2, \dots, n\}$.

Definição 4.9

Um conjunto $A \subseteq [n]$ é *livre de soma* se $x + y \notin A$ para quaisquer $x, y \in A$.

Por exemplo, o conjunto $C = \{1, 3, 7\}$ é livre de soma, pois a soma de quaisquer dois elementos de C resulta em um elemento que não está em C . De fato, o conjunto $S = \{1 + 1, 1 + 3, 1 + 7, 3 + 3, 3 + 7, 7 + 7\} = \{2, 4, 6, 8, 10, 14\}$ não contém nenhum elemento de C . Mas será que é possível encontrar um conjunto livre de soma $A \subseteq [n]$ com mais elementos?

Sabemos que a soma de quaisquer dois ímpares é um número par. Assim, o conjunto de todos números ímpares em $[n]$ é livre de soma e tem $\lceil n/2 \rceil$ elementos (tenha certeza que você está convencido desse fato). Mas a mesma pergunta que fizemos anteriormente persiste: é possível encontrar um conjunto livre de soma $A \subseteq [n]$, mas agora com mais do que $\lceil n/2 \rceil$ elementos? Já está claro qual é a pergunta interessante: qual o **maior** tamanho possível para um conjunto livre de soma em $[n]$?

Mas o conjunto que encontramos, dos ímpares, parece ser o maior possível. De fato, aqui nossa intuição está certa e demonstramos isso a seguir. Iremos nos inspirar na ideia que utilizamos na demonstração da Afirmação 4.8.

Teorema 4.10

Seja n um inteiro positivo. Se $A \subseteq [n]$ é livre de soma, então $|A| \leq \lceil n/2 \rceil$.

Demonstração. Seja $A \subseteq [n]$ um conjunto livre de soma e suponha por contradição que $|A| > \lceil n/2 \rceil$. Seja $m = \max\{a : a \in A\}$ e defina o conjunto das diferenças em relação a m , excluindo a diferença $m - m = 0$, pois queremos que esse conjunto tenha cardinalidade $|A| - 1$:

$$B = \{m - a : a \in A \setminus \{m\}\}.$$

Note que, pela escolha de m , todos os elementos gerados em B são estritamente

maiores que 0. Além disso, como o menor elemento possível de A é no mínimo 1, o maior elemento de B é estritamente menor que m . Como $A \subseteq [n]$, temos que $m \leq n$. Portanto, $B \subseteq [n]$. Note também que, como mencionamos, $|B| = |A| - 1$. Portanto,

$$|A| + |B| > 2 \left\lceil \frac{n}{2} \right\rceil \geq n + 1 > n.$$

Pelo Princípio da Casa dos Pombos, sabemos então que existe $k \in [n]$ que pertence a A e B . Como $k \in B$, temos pela construção de B que $k = m - a$ para algum $a \in A$. Assim, como $a \in A$ e $k = m - a \in A$, temos que $a + k = m \in A$, contradizendo o fato de A ser livre de soma. Portanto, concluímos que $|A| \leq \lceil n/2 \rceil$. $\square$

Em todos os exemplos que discutimos, o Princípio da Casa dos Pombos atua como uma ferramenta de *garantia de existência*. Ele nos prova, sem qualquer sombra de dúvida, que algo *deve* ocorrer. No entanto, isso *não* significa que sabemos *quais* são as estruturas que garantimos a existência. Por exemplo, no exemplo sobre pessoas e fios de cabelo, sabemos que existem pelo menos 56 pessoas com o mesmo número de fios de cabelo, mas não sabemos quais são essas pessoas.

Índice Remissivo

cardinalidade, 48
complementar, 54
condicional, 27
condicional dupla, 30
condicional para dois lados, 30
conjunto, 48
conjunto livre de soma, 63
conjunto universo, 54
conjunto vazio, 49
conjuntos comparáveis, 51
conjunção, 23
consequência, 27
contradição, 33
contrapositiva, 34

diferença, 50
diferença simétrica, 55
disjunção, 24
disjunção exclusiva, 26
divisibilidade, 17
domínio de predicado, 36

e, 23
equivalência lógica, 33
existe, 38
existe um único, 40

hipótese, 27

interseção, 50

número primo, 17

ou, 24
ou exclusivo, 26

para todo, 37
 piso, 59
predicado, 36
premissa, 27
primo, 17
produto cartesiano, 56

quantificador de unicidade, 40
quantificador existencial, 38
quantificador universal, 37

subconjunto, 48

tautologia, 33
tese, 27
teto, 59

universo, 54
união, 50