Os Fundamentos: Métodos de Demonstração

Área de Conhecimento em Algoritmos e Teoria - DCC/UFMG

Introdução à Lógica Computacional

2024/2

Introdução

Métodos de demonstração: Introdução

- Uma **demonstração** é uma argumentação matemática da certeza a respeito de uma afirmação.
- O nível de detalhamento de uma demonstração pode depender do tipo de leitor ao qual ela se destina, levando em conta fatores como:
  - o conhecimento do leitor sobre o assunto;
  - a maturidade do leitor;
  - o nível de rigor almejado.
- Nesta seção vamos nos focar em demonstrações utilizando o rigor matemático esperado de um profissional em nível de graduação na área de ciências exatas.
- Demonstrações são importantes em várias áreas da Ciência da Computação:

1. correção de programas;
2. análise de complexidade de algoritmos;
3. propriedades de segurança de sistemas;
4. ...

Introdução às demonstrações

Terminologia

- Um **axioma (ou postulado)** é uma afirmação assumida como verdadeira sem a necessidade de uma demonstração, ou seja, uma "verdade a princípio".
- Um **resultado** é uma afirmação que se pode demonstrar ser verdadeira.

  Resultados recebem diferentes nomes, de maneira mais ou menos subjetiva:

  - Um **teorema** é um resultado considerado interessante em si mesmo.
  - Uma **proposição** é um resultado considerado "de menor interesse".
  - Um **lema** é um resultado auxiliar, geralmente usado para quebrar a demonstração de um resultado mais complexo em partes menores.
  - Um **corolário** é um resultado derivável facilmente a partir de outro resultado já demonstrado, consistindo em uma consequência mais ou menos imediata.
- Uma **demonstração (ou prova)** é um argumento que mostra que uma afirmação (teorema, proposição ou lema) segue de um conjunto de premissas.
- Uma **conjectura** é suposição bem fundada, porém (ainda) sem demonstração. Uma vez demonstrada, uma conjectura se torna um resultado.

Evidência versus demonstração

- Exemplo 1 Seja a fórmula $p(n) = n^2 + n + 41$.

  Conjectura: $\forall n \in \mathbb{N} : p(n)$ é primo.

  Temos evidências de que a conjectura poderia ser verdadeira?

  Testando valores de $n = 0, 1, \ldots, 39$ a proposição é sempre verdadeira, ou seja, $p(n)$ é primo para $0 \leq n \leq 39$:

n	0	1	2	3	...	20	...	39
$p(n)$	41	43	47	53	...	461	...	1601

  Daí, podemos ficar tentados a concluir:

  Isto não pode ser uma coincidência! A hipótese deve ser verdadeira!

  Mas não é: $p(40) = 1681 = 41 \cdot 41$, que não é primo!

  Logo, a conjectura é falsa. ◁

- Moral da história: evidência não é o mesmo que demonstração!

Evidência versus demonstração

- Exemplo 2 Em 1 769, Euler (1 707–1 783) conjecturou que

$$a^4 + b^4 + c^4 = d^4$$

não tem solução no conjunto dos números inteiros positivos.

Durante mais de dois séculos, ninguém conseguiu encontrar valores de a, b, c e d que satisfizessem a equação.

O insucesso de todos os matemáticos envolvidos era evidência de que a conjectura poderia ser verdadeira.

218 anos depois, em 1 987, Noam Elkies proveu um contra-exemplo:

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

Logo, esta conjectura também é falsa. ◁

- Ausência de demonstração não o mesmo que demonstração de ausência!

Métodos de demonstração

- Construir uma demonstração é uma arte.

  Cada caso é um caso: não existe uma "receita fechada" para construir demonstrações para todas as afirmações.

- Existem, entretanto, técnicas que são úteis para demonstrar uma grande quantidade de afirmações.

  Aqui vamos cobrir vários métodos de demonstração, incluindo:

  1. demonstração direta;
  2. demonstração por contraposição;
  3. demonstração por contradição (ou demonstração por redução ao absurdo).
  4. demonstração por contra-exemplo; e
  5. demonstração por exaustão e divisão em casos.

- Outros métodos de demonstração (e.g., demonstração por indução matemática) serão cobertos mais adiante neste curso.

Como escrever uma demonstração

- Escreva claramente qual a afirmação que se deseja demonstrar.

  (É comum preceder a afirmação com uma qualificação como **"Teorema"**, **"Lema"**, ou **"Proposição"**.)

- Delimite claramente o escopo da demonstração.

  Indique o início da demonstração com **"Demonstração."** ou **"Prova."**

  Indique o fim da demonstração com um marcador. Podem-se usar:

  - um quadradinho □, ou
  - a abreviação **Q.E.D.** (do latim *"quod erat demonstrandum"*), ou
  - sua tradução em português, **C.Q.D.** (*"conforme queríamos demonstrar"*).

- Escreva a demonstração de tal forma que ela seja autocontida.

  - Use linguagem natural (português) de forma clara, empregando sentenças completas e bem estruturadas.
  - Podem-se utilizar fórmulas matemáticas, equações, etc., quando necessário.

Como escrever uma demonstração

- Identifique cada variável usada na demonstração juntamente com seu tipo.

  Exemplos:

  1. Seja x um número real maior que 2.
  2. Suponha que m e n sejam inteiros sem divisores comuns.

- Importante:

  O objetivo principal de uma demonstração é convencer o leitor de que o resultado (teorema, proposição, lema) é verdadeiro.

  Não basta que você mesmo esteja convencido!

  Certifique-se de que está sendo conciso, mas claro.

Demonstração direta

- Forma geral:

  1. Expresse a afirmação a ser demonstrada na forma:

     $$\forall x \in D : (P(x) \rightarrow Q(x))$$

     Esta etapa às vezes é feita mentalmente.

  2. Comece a demonstração supondo que x é um elemento específico do domínio D, mas escolhido arbitrariamente, para o qual a hipótese $P(x)$ é verdadeira.

     Normalmente abreviamos esta etapa dizendo *"Assuma que $x \in D$ e $P(x)$ é verdadeiro"* ou *"Seja $x \in D$ tal que $P(x)$"*.

  3. Mostre que a conclusão $Q(x)$ é verdadeira utilizando definições, resultados anteriores e as regras de inferência lógica.

- Importante: Como $x \in D$ é escolhido arbitrariamente,
  - ele não depende de nenhuma suposição especial sobre x, e,
  - portanto, ele pode ser generalizado para todos os elementos de D.

Demonstração direta

- **Definição:**

  (i) Um inteiro n é **par** se existe um inteiro k tal que $n = 2k$.

  (ii) Um inteiro n é **ímpar** se existe um inteiro k tal que $n = 2k + 1$.

- Exemplo 3 Mostre que se n é um inteiro ímpar, então n^2 é ímpar.

  Demonstração. Queremos mostrar que

  $$\forall n \in \mathbb{Z} : (\, P(n) \rightarrow Q(n)\,),$$

  onde

  - $P(n)$ é o predicado *"n é um inteiro ímpar"*, e
  - $Q(n)$ é o predicado *"n^2 é ímpar"*.

  Para produzir uma demonstração direta, assumimos que para um inteiro n a hipótese da implicação, $P(n)$, seja verdadeira, ou seja, que n é ímpar.

  Então, pela definição de número ímpar, existe um inteiro k tal que $n = 2k + 1$.

Demonstração direta

- Exemplo 3 (Continuação)

Queremos mostrar que a conclusão da implicação, $Q(n)$, é verdadeira, ou seja, que n^2 também é ímpar.

Para isto podemos calcular

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Mas note que isso significa que

$$n^2 = 2k' + 1,$$

onde $k' = 2k^2 + 2k$ é um inteiro.

Logo, pela definição de número ímpar, n^2 também é ímpar e está concluída nossa demonstração. □

Demonstração direta

- **Definição:** Um inteiro a é um **quadrado perfeito** se existe um inteiro b tal que $a = b^2$.

- Exemplo 4 Mostre que se m e n são quadrados perfeitos, então mn é um quadrado perfeito.

  Demonstração. Para demonstrar esta proposição, vamos assumir que m e n sejam quadrados perfeitos. Pela definição de quadrado perfeito, devem existir inteiros s e t tais que $m = s^2$ e $n = t^2$.

  O objetivo da demonstração é mostrar que mn será um quadrado perfeito quando m e n o forem. Para ver isto, podemos calcular

  $$mn \quad = \quad s^2 t^2 \quad = \quad (st)^2.$$

  Mas é claro que st também é um inteiro, logo mn satisfaz a definição de quadrado perfeito (já que $mn = (st)^2$), e a conclusão da implicação também é verdadeira.

  Logo concluímos a demonstração de que a afirmação é verdadeira. □

Demonstração direta

- **Definição:**

  (i) Um número real n é **racional** quando existem inteiros p e q, com $q \neq 0$, tais que $n = p/q$.

  (ii) Um número real n é **irracional** quando ele não é racional.

- Exemplo 5 Mostre que a soma de dois números racionais é um número racional.

  Demonstração. Formalmente, queremos mostrar que para todo número real r e todo número real s, se r e s são racionais, então $r + s$ também é racional.

  Para dar uma demonstração direta desta afirmação, vamos assumir que r e s sejam racionais. Pela definição de número racional, devem existir então inteiros p e q, com $q \neq 0$, tais que $r = p/q$, e devem existir também inteiros t e u, com $u \neq 0$, tais que $s = t/u$.

Demonstração direta

- Exemplo 5 (Continuação)

  Para mostrar que $r + s$ também será racional quando r e s o forem, podemos calcular

$$r + s \quad = \quad \frac{p}{q} + \frac{t}{u} \quad = \quad \frac{pu + qt}{qu}.$$

  Note que, por hipótese, q e u são diferentes de zero e, portanto, $qu \neq 0$.

  Consequentemente $r + s$ pode ser expresso como a razão de dois inteiros ($pu + qt$ e qu, com $qu \neq 0$) e, portanto, $r + s$ satisfaz a definição de número racional.

  Logo a afirmação é verdadeira. □

Demonstração por contraposição

- Forma geral:

  1. Expresse a afirmação a ser demonstrada na forma:

     $$\forall x \in D : (P(x) \rightarrow Q(x))$$

     Esta etapa às vezes é feita mentalmente.

  2. Encontre a afirmação contrapositiva da afirmação a ser demonstrada:

     $$\forall x \in D : (\neg Q(x) \rightarrow \neg P(x))$$

  3. Comece a demonstração supondo que x é um elemento específico do domínio D, mas escolhido arbitrariamente, para o qual a conclusão $Q(x)$ é falsa.

  4. Mostre que a hipótese $P(x)$ é falsa utilizando definições, resultados anteriores e as regras de inferência lógica.

- Importante: Como $x \in D$ é escolhido arbitrariamente,
  - ele não depende de nenhuma suposição especial sobre x, e,
  - portanto, ele pode ser generalizado para todos os elementos de D.

Demonstração por contraposição

- Exemplo 6 Mostre que se n é um inteiro e $3n+2$ é ímpar, então n é ímpar.

Demonstração. Queremos mostrar que $\forall n \in \mathbb{Z} : (P(n) \rightarrow Q(n))$, onde $P(n)$ é *"$3n+2$ é ímpar"*, e $Q(x)$ é *"n é ímpar"*.

Para produzir uma demonstração por contraposição, vamos demonstrar que $\forall n \in \mathbb{Z} : (\neg Q(n) \rightarrow \neg P(n))$. Ou seja, vamos mostrar que se um número inteiro n não é ímpar, então $3n+2$ também não é ímpar.

Se n não é ímpar, é porque n é par e, pela definição de número par, $n = 2k$ para algum $k \in \mathbb{Z}$. Portanto podemos derivar

$$\begin{aligned} 3n+2 &= 3(2k)+2 \\ &= 6k+2 \\ &= 2(3k+1), \end{aligned}$$

de onde concluímos que $3n+2$ satisfaz a definição de número par.

Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, concluímos com sucesso a demonstração por contraposição . □

Demonstração por contraposição

- **Exemplo 7** Mostre que se $n = ab$ onde a e b são inteiros positivos, então $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

  Demonstração. Em primeiro lugar, note que o resultado que queremos demonstrar pode ser formalizado como

  $$\forall n, a, b \in \mathbb{Z}^+ : \left(n = ab \ \rightarrow \ a \leq \sqrt{n} \vee b \leq \sqrt{n}\right) \ .$$

  Para produzir uma demonstração por contraposição, vamos demonstrar que sempre que a conclusão da implicação é falsa, sua hipótese também é falsa.

  A conclusão da implicação é $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$, logo por De Morgan, sua negação é

  $$\begin{aligned} \neg((a \leq \sqrt{n}) \vee (a \leq \sqrt{n})) &\equiv \neg(a \leq \sqrt{n}) \wedge \neg(b \leq \sqrt{n}) \\ &\equiv (a > \sqrt{n}) \wedge (b > \sqrt{n}). \end{aligned}$$

  Já a hipótese da implicação é $n = ab$, e sua negação é $n \neq ab$.

Demonstração por contraposição

- **Exemplo 7** (Continuação)

  Queremos mostrar a contrapositiva da proposição original, ou seja, que para todos inteiros positivos a, b, n se $(a > \sqrt{n}) \wedge (b > \sqrt{n})$ então $n \neq ab$.

  Para isto, note que se $(a > \sqrt{n}) \wedge (b > \sqrt{n})$ podemos derivar o seguinte

$$\begin{aligned} ab &> \sqrt{n} \cdot b && (\text{pois } a > \sqrt{n}) \\ &> \sqrt{n} \cdot \sqrt{n} && (\text{pois } b > \sqrt{n}) \\ &= n\ , \end{aligned}$$

  de onde se conclui que $ab > n$ e, portanto, $ab \neq n$.

  Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, a demonstração por contraposição é concluída com sucesso. □

Demonstração por vacuidade

- Forma geral:

  1. Expresse a afirmação a ser demonstrada na forma:

     $$p \rightarrow q$$

     Esta etapa às vezes é feita mentalmente.

  2. Mostre que p é falso.

     Conclua que $p \rightarrow q$ deve ser verdadeiro, pela definição de implicação.

- Esta técnica recebe o nome de **demonstração por vacuidade** porque demonstramos que a hipótese da implicação é "vácua", ou seja, falsa.

  Com isso nem precisamos analisar a conclusão da implicação para garantir que ela é verdadeira.

Demonstração por vacuidade

- **Definição:** Um inteiro a é um **cubo perfeito** se existe um inteiro b tal que $a = b^3$.

- Exemplo 8 Mostre que se n é um inteiro, com $10 \leq n \leq 15$, tal que n é um quadrado perfeito, então n é também um cubo perfeito.

  Demonstração.

  Note que queremos mostrar a seguinte implicação para todo inteiro n: se $10 \leq n \leq 15$ e n é um quadrado perfeito, então n é um cubo perfeito.

  Mas note que a hipótese da implicação é falsa: como $3^2 = 9$ e o próximo quadrado perfeito é $4^2 = 16$, não existe nenhum quadrado perfeito n tal que $10 \leq n \leq 15$.

  Consequentemente, a implicação a ser demonstrada é verdadeira, por vacuidade, para todos os inteiros n. □

Demonstração trivial

- Forma geral:

  1. Expresse a afirmação a ser demonstrada na forma:

     $$p \rightarrow q$$

     Esta etapa às vezes é feita mentalmente.

  2. Mostre que q é verdadeiro.

     Conclua que $p \rightarrow q$ deve ser verdadeiro, pela definição de implicação.

- Esta técnica recebe o nome de **demonstração trivial** porque demonstramos que a conclusão da implicação é sempre verdadeira, sem usar a hipótese.

Demonstração trivial

- Exemplo 9 Mostre que se $2\,310$ não tem fatores primos repetidos, então $(2\,310)^2$ é um número racional.

  Demonstração.

  Note que queremos mostrar a seguinte implicação: se $2\,310$ não tem fatores primos repetidos, então $2\,310^2$ é um número racional.

  Mas note que a conclusão da implicação é verdadeira:

  $$2\,310^2 = 5\,336\,100 = \frac{5\,336\,100}{1},$$

  que é a razão de dois inteiros $p = 5\,336\,100$ e $q = 1 \neq 0$.

  Consequentemente, a implicação a ser demonstrada é verdadeira, trivialmente. □

Demonstração por contradição ou por redução ao absurdo

- A **demonstração por contradição**, também chamada de **demonstração por redução ao absurdo**, se baseia no fato de que:

  1. se partimos de uma premissa p, e
  2. seguimos um processo em que realizamos uma inferência válida, e
  3. mesmo assim chegamos a uma conclusão falsa,

  então

  4. podemos concluir que a premissa p deve ser necessariamente falsa.

- Equivalentemente, se ao tomarmos como premissa a negação $\neg p$ de uma afirmação p chegamos a um absurdo (contradição), então a afirmação p deve ser necessariamente verdadeira.

Demonstração por contradição ou por redução ao absurdo

- Forma geral:

  1. Para demonstrar que a afirmação p é verdadeira, assuma que sua negação $\neg p$ seja verdadeira.
  2. Mostre que $\neg p$ leva a uma contradição, ou seja, que

  $$\neg p \rightarrow F.$$

  Conclua que p deve ser necessariamente verdadeiro.

Demonstração por contradição ou por redução ao absurdo

- Exemplo 10 Mostre que em qualquer grupo de 22 dias (consecutivos ou não), ao menos 4 dias caem no mesmo dia da semana.

  Demonstração. Seja p a proposição *"Em qualquer grupo de* 22 *dias (consecutivos ou não), ao menos* 4 *dias caem no mesmo dia da semana"*.

  Suponha que $\neg p$ seja verdadeiro, ou seja, que *"Existe um grupo de* 22 *dias (consecutivos ou não) em que no máximo* 3 *dias caem no mesmo dia da semana"*.

  Mas note que existem apenas 7 dias na semana e, portanto, se cada dia só pode aparecer 3 vezes em um grupo, o grupo pode ter no máximo 21 dias. Mas isso contradiz a premissa de que o grupo tem 22 dias.

  Em outras palavra, se r é a proposição *"22 dias são escolhidos para fazer parte do grupo"*, teríamos $\neg p \rightarrow (r \wedge \neg r)$, ou seja, $\neg p \rightarrow F$.

  Logo, $\neg p$ não pode ser verdadeiro, ou seja, p é verdadeiro. □

Demonstração por contradição ou por redução ao absurdo

- Exemplo 11 Mostre que se $3n + 2$ é ímpar, então n é ímpar.

Demonstração. Queremos mostrar a proposição *"se $3n + 2$ é ímpar, então n é ímpar"*. Podemos escrever esta proposição como $p \to q$.

Para demonstrar por contradição, vamos assumir que $p \to q$ seja falso. Isso quer dizer que estamos assumindo $p \wedge \neg q$, ou seja, que *"$3n + 2$ é ímpar e n não é ímpar"*.

Mas se n não é ímpar, é porque n é par e existe um inteiro k tal que $n = 2k$. Podemos, então, derivar

$$3n + 2 \quad = \quad 3(2k) + 2 \quad = \quad 6k + 2 \quad = \quad 2(3k + 1),$$

o que implica que $3n + 2$ é par. Mas isto significa que concluímos exatamente que p é falso, o que contradiz a hipótese de que p é verdadeiro.

Logo, não é possível ter $p \wedge \neg q$ sem cair em contradição, e, portanto, se $3n + 2$ é ímpar então n é ímpar. □

Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos revisitar o exemplo da primeira aula deste curso (recordar é viver!) e mostrar que $\sqrt{2}$ é irracional.

  Demonstração. Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que $\sqrt{2}$ seja racional.

  Neste caso, existem $p, q \in \mathbb{Z}$, com $mdc(p, q) = 1$, tais que $\sqrt{2} = p/q$. Elevando os dois lados ao quadrado, obtemos $2 = p^2/q^2$, ou seja, $p^2 = 2q^2$. Note que $2q^2$ é par, portanto pela igualdade acima p^2 também tem que ser par. Isto implica que p deve ser par.

  Agora, já que p é par, existe algum $s \in \mathbb{Z}$ tal que $p = 2s$. Isso implica que $2q^2 = p^2 = (2s)^2 = 4s^2$, o que resulta em $q^2 = 2s^2$. Note que então q^2 é par, portanto q deve ser par.

  Mas se ambos p e q são pares, isto contradiz a suposição de que o $mdc(p, q) = 1$: encontramos uma contradição.

  Logo podemos concluir que não existem $p, q \in \mathbb{Z}$, com $q \neq 0$ e $mdc(p, q) = 1$, tais que $\sqrt{2} = p/q$. Portanto $\sqrt{2}$ é irracional. □

Demonstração de equivalências

- É muito comum termos que mostrar que um conjunto de afirmações são todas equivalentes.
- Forma geral:
  1. Para mostrar que $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$, mostre, separadamente, cada uma das implicações

$$p_1 \rightarrow p_2$$
$$p_2 \rightarrow p_3$$
$$\ldots \rightarrow \ldots$$
$$p_n \rightarrow p_1$$

- Importante: A demonstração não está completa se não se fechar o ciclo de implicações, demonstrando que a última proposição implica de volta na primeira: $p_n \rightarrow p_1$.
- Caso especial: Para demonstrar que $p_1 \leftrightarrow p_2$ podemos mostrar, separadamente, que $p_1 \rightarrow p_2$ e que $p_2 \rightarrow p_1$.

Demonstração de equivalências

- Exemplo 13 Mostre que as seguintes afirmações sobre um inteiro n são equivalentes:

$$\begin{aligned} p_1 &: \quad \text{“}n \text{ é par”} \\ p_2 &: \quad \text{“}n-1 \text{ é ímpar”} \\ p_3 &: \quad \text{“}n^2 \text{ é par”} \end{aligned}$$

Demonstração.

Vamos demonstrar que as três afirmações são equivalentes mostrando que as três implicações são verdadeiras: $p_1 \to p_2$, $p_2 \to p_3$, e $p_3 \to p_1$.

- $p_1 \to p_2$: Vamos usar uma demonstração direta.

  Se n é par, então $n = 2k$ para algum inteiro k. Logo:

$$n-1 \quad = \quad 2k-1 \quad = \quad 2(k-1)+1 \ ,$$

  e, portanto $n-1$ é ímpar, por ser da forma $2m+1$ para o inteiro $m = k-1$.

Demonstração de equivalências

- Exemplo 13 (Continuação)

  - $p_2 \to p_3$: Vamos usar uma demonstração direta.

    Se $n-1$ é ímpar, então $n-1 = 2k+1$ para algum inteiro k. Logo:

    $$n \quad = \quad (2k+1)+1 \quad = \quad 2k+2 \ .$$

    Portanto podemos derivar

    $$n^2 \quad = \quad (2k+2)^2 \quad = \quad 4k^2+8k+4 \quad = \quad 2(k^2+4k+2) \ ,$$

    de onde concluímos que n^2 é par por ser da forma $n = 2m$ para o inteiro $m = k^2+4k+2$.

  - $p_3 \to p_1$: Vamos usar uma demonstração por contraposição.

    Mas note que a contraposição desejada, $\neg p_1 \to \neg p_3$, é a afirmação *"Se n é ímpar, então n^2 é ímpar"*, que já demonstramos em um exemplo anterior.

Concluídas as demonstrações das três implicações, as equivalências desejadas estão estabelecidas. □

Demonstração por contra-exemplo

- Demonstrações por contra-exemplos funcionam para mostrar que afirmações são falsas.
- Forma geral:
  1. Expresse a afirmação a ser demonstrada na forma:

     $$\forall x \in D : P(x)$$

     Esta etapa às vezes é feita mentalmente.
  2. Encontre um $x \in D$ tal que $P(x)$ seja falso.

     Conclua que a afirmação em questão é falsa.

Demonstração por contra-exemplo

- **Exemplo 14** Seja $p(n) = n^2 + n + 41$. Demonstre que a afirmação "$\forall n \in \mathbb{N} : p(n)$ *é primo*" é falsa.

  Demonstração. Tome o contra-exemplo $n = 40$. Neste caso temos $p(n) = 1681 = 41 \cdot 41$, que não é primo.

  Logo a afirmação é falsa. □

Demonstração por contra-exemplo

- Exemplo 15 Mostre que a afirmação *"Todo inteiro positivo pode ser escrito como a soma do quadrado de dois inteiros"* é falsa.

  Demonstração. Daremos como contra-exemplo o número 3, que é um inteiro que não pode ser escrito como a soma dos quadrados de dois inteiros.

  Para ver isto, basta ver que os únicos quadrados menores que 3 são 0 e 1, e as somas possíveis de dois destes quadrados são $0 + 0 = 0$, $0 + 1 = 1$, e $1 + 1 = 2$, nenhuma das quais se iguala a 3.

  Logo 3 é um contra-exemplo e a afirmação é falsa. □

Demonstração por exaustão ou divisão em casos

- Utilizada geralmente para demonstrar que $p \rightarrow q$.
- A demonstração divide p em casos exaustivos, e mostra que q segue de qualquer caso possível.
- Forma geral:
  1. Primeiro mostre que
  $$p \equiv p_1 \vee p_2 \vee \ldots \vee p_n$$
  2. Mostre, separadamente, cada uma das implicações
  $$p_1 \rightarrow q$$
  $$p_2 \rightarrow q$$
  $$\ldots \rightarrow \ldots$$
  $$p_n \rightarrow q$$
  3. Conclua que $p \rightarrow q$.

Demonstração por exaustão ou divisão em casos

- **Definição:** Dado dois números reais x e y, definimos as funções máximo e mínimo, respectivamente, como a seguir

$$\max(x, y) = \begin{cases} x, & \text{se } x \geq y, \\ y, & \text{se } x < y. \end{cases} \qquad \min(x, y) = \begin{cases} x, & \text{se } x \leq y, \\ y, & \text{se } x > y. \end{cases}$$

- Exemplo 16 Mostre que, dados $x, y \in \mathbb{R}$, $\min(x, y) + \max(x, y) = x + y$.

  Demonstração. Há somente três possibilidades para x e y:

  $$x < y \quad \text{ou} \quad x = y \quad \text{ou} \quad x > y.$$

  Vamos analisar cada caso separadamente:

  - Se $x < y$, então $\min(x, y) + \max(x, y) = x + y$.
  - Se $x = y$, então $\min(x, y) + \max(x, y) = x + x = y + y = x + y$.
  - Se $x > y$, então $\min(x, y) + \max(x, y) = y + x = x + y$.

  Logo, sempre teremos $\min(x, y) + \max(x, y) = x + y$. □

Demonstração por exaustão ou divisão em casos

- **Definição:** Dado um número real a, seu **módulo** $|a|$ é definido como

$$|a| = \begin{cases} a, & \text{se } a \geq 0, \\ -a, & \text{se } a < 0. \end{cases}$$

- Exemplo 17 Mostre que $|xy| = |x||y|$, onde x e y são números reais.

Demonstração. Note que podemos identificar cinco casos exaustivos para a combinação de x e y:

1. pelo menos um entre x e y é zero,
2. x e y são ambos positivos,
3. x é positivo e y é negativo,
4. x é negativo e y é positivo, ou
5. x e y são ambos negativos.

Demonstração por exaustão ou divisão em casos

- **Exemplo 17** (Continuação)

Vamos analisar cada caso separadamente:

1. Se pelo menos um entre x e y é zero, então $xy = 0$ e pelo menos um entre $|x|$ e $|y|$ é zero e, portanto, temos
$$|xy| = 0 = |x||y|.$$
2. Se x e y são ambos positivos, então $xy > 0$ e temos
$$|xy| = xy = |x||y|.$$
3. Se x é positivo e y é negativo, então $xy < 0$ e temos
$$|xy| = -xy = x(-y) = |x||y|.$$
4. Se x é negativo e y é positivo, então $xy < 0$ e temos
$$|xy| = -xy = (-x)y = |x||y|.$$
5. Se x e y são ambos negativos, então $xy > 0$ e temos
$$|xy| = xy = (-x)(-y) = |x||y|.$$

Logo, podemos concluir que a afirmação é sempre verdadeira. □

Demonstração de existência

- Uma demonstração de um resultado do tipo $\exists x : P(x)$ é chamada de **demonstração de existência**.
- Há duas maneiras de se produzir uma demonstração de existência:
  1. Uma demonstração **construtiva**
     produz um elemento a tal que $P(a)$ seja verdadeiro.

     O elemento a é chamado de **testemunha** da demonstração.
  2. Uma demonstração **não-construtiva** não produz uma testemunha, demonstrando $\exists x : P(x)$ de alguma outra forma.

     Uma maneira é produzir, por exemplo, uma demonstração por contradição.

Demonstração de existência: construtiva

- Exemplo 18 Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas maneiras distintas.

  Demonstração. Após uma busca trabalhosa (por exemplo, usando um programa de computador), encontramos que

  $$1\,729 = 10^3 + 9^3 = 12^3 + 1^3.$$

  □

- A demonstração acima é construtiva porque ela produz uma testemunha (o número 1 729 junto com suas decomposições) que atesta a existência desejada.

Demonstração de existência: não-construtiva

- Exemplo 19 Existem números irracionais x e y tais que x^y é racional.

  Demonstração. Sabemos que $\sqrt{2}$ é irracional (já demonstarmos isto). Considere o número $\sqrt{2}^{\sqrt{2}}$. Há duas possibilidades para este número:

  1. Ele é racional. Neste caso temos dois irracionais $x = \sqrt{2}$ e $y = \sqrt{2}$ tais que x^y é racional.
  2. Ele é irracional. Neste caso podemos calcular

  $$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

  que é um número racional. Assim temos dois irracionais $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$ tais que x^y é racional. □

- A demonstração acima é não-construtiva porque ela não produz uma testemunha que atesta a existência desejada.

  Sabemos que ou o par $x = \sqrt{2}$, $y = \sqrt{2}$ ou o par $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ satisfaz a propriedade, mas não sabemos qual destes dois pares é o certo!

Demonstração de unicidade

- Alguns resultados afirmam a existência de um único objeto com uma certa propriedade.

  Para construir uma **demonstração de unicidade**, precisamos mostrar que um objeto com a propriedade desejada existe, e que nenhum outro objeto apresenta a mesma propriedade.

- Forma geral:

  1. **Demonstração de existência**: Mostre que um objeto x com a propriedade deseja existe.

     $$\exists x : P(x)$$

  2. **Demonstração de unicidade:** Mostre que se dois objetos x e y apresentam ambos a mesma propriedade desejada, então $x = y$.

     $$\forall x : \forall y : (P(x) \wedge P(y) \rightarrow x = y)$$

Demonstração de unicidade

- Exemplo 20 Mostre que se a e b são números reais tais que $a \neq 0$, então existe um único número real r tal que $ar + b = 0$.

Demonstração.

Primeiro mostramos a existência de um real r com a propriedade desejada.

Para isto, fazemos $r = {}^{-b}/_{a}$ e verificamos que neste caso

$$ar + b \quad = \quad a\left(\frac{-b}{a}\right) + b \quad = \quad -b + b \quad = \quad 0\ .$$

Em seguida, mostramos que $r = {}^{-b}/_{a}$ é o único real satisfazendo a propriedade.

Para isto, assuma que exista um outro número real s tal que $as + b = 0$.

Então $ar + b = as + b$. Daí concluímos:

$$\begin{aligned} ar + b = as + b \quad &\rightarrow \quad ar = as \qquad \text{(subtraindo } b \text{ dos dois lados)} \\ &\rightarrow \quad r = s \qquad \text{(dividindo os dois lados por } a\text{)} \end{aligned}$$

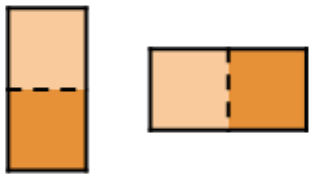
□

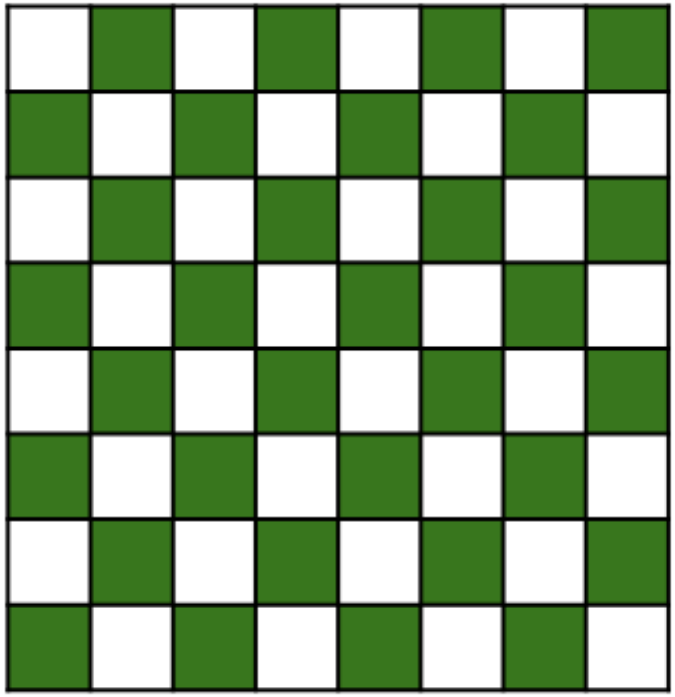
Estratégias de demonstração

Estratégias de demonstração: Tabuleiro de xadrez e dominós

- Vamos agora cobrir algumas estratégias de demonstração criativas, usando exemplos baseados no seguinte cenário.

  Considere um tabuleiro de xadrez de dimensões 8×8 e peças de dominó de dimensões 2×1 (peça vertical) ou 1×2 (peça horizontal).



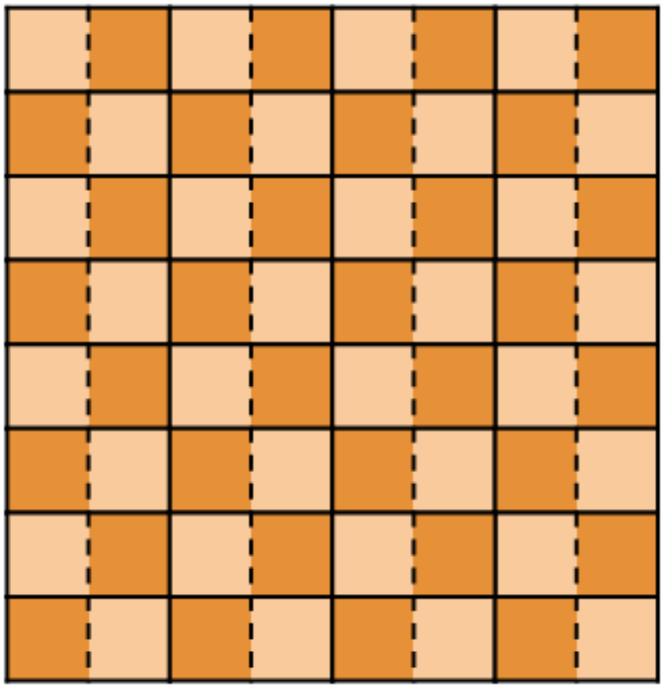


Estratégias de demonstração: Tabuleiro de xadrez e dominós

- Exemplo 21 É possível cobrir todo o tabuleiro usando peças de dominós?

Solução.

Sim, podemos usar 32 dominós, todos de forma horizontal, como mostra a figura ao lado.

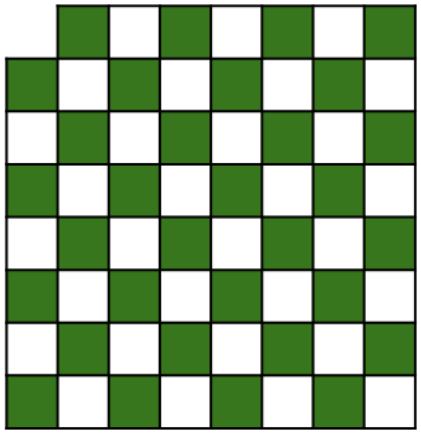


◁

Estratégias de demonstração: Tabuleiro de xadrez e dominós

- Exemplo 22 Suponha que um novo tabuleiro seja obtido a partir de um tabuleiro padrão removendo uma de suas quinas.

  É possível cobrir todo este novo tabuleiro usando peças de dominós?



Solução.

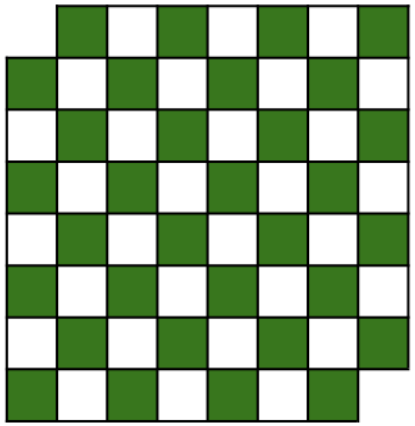
Note que ao remover uma quina, novo tabuleiro tem exatamente 63 casas.

Como cada dominó cobre um número par de casas (2), é impossível cobrir todas as casas do tabuleiro com dominós. ◁

Estratégias de demonstração: Tabuleiro de xadrez e dominós

- Exemplo 23 Suponha que um novo tabuleiro seja obtido a partir de um tabuleiro padrão removendo duas quinas opostas.

  É possível cobrir todo este novo tabuleiro usando peças de dominós?



Solução. Por contradição, assuma que haja uma cobertura de dominós para este tabuleiro. Como o tabuleiro tem $64 - 2 = 62$ casas, 31 dominós são usados na cobertura. Como cada dominó cobre exatamente uma casa escura e uma clara, a cobertura cobre exatamente 31 casas claras e 31 casas escuras.

Entretanto, note que ao remover duas quinas opostas, estamos removendo duas casas de mesma cor (ou ambas escuras, ou ambas claras). Logo a cobertura necessariamente cobre 32 casas de um tipo (no nosso exemplo, escuras) e apenas 30 de outro tipo (no nosso exemplo, claras).

Claramente isto é uma contradição, e tal cobertura não pode existir. ◁

Outras considerações sobre demonstrações

Erros comuns em demonstrações

- Existem muitos erros comuns na construção de demonstrações matemáticas.

  Aqui vamos brevemente ver alguns deles.

- Entre os erros mais comuns estão os erros aritméticos e básicos álgebra.

  Até mesmo matemáticos profissionais cometem esses erros, especialmente quando trabalham com fórmulas complicadas: atenção nunca é demais!

- Além disso, cada etapa de uma demonstração matemática precisa estar correta, e a conclusão precisa seguir logicamente das etapas que a precedem.

Erros comuns em demonstrações

- Muitos erros resultam da introdução de um passo que não segue logicamente daqueles que o precedem.

- Exemplo 24 Qual o erro na seguinte "demonstração" de que $1 = 2$?

Passo	**Justificativa**
1. $\exists x, y \in \mathbb{R} : x = y$	Premissa
2. $a = b$	Instanciação existencial de (1)
3. $a^2 = ab$	Multiplicando ambos os lados de (2) por a
4. $a^2 - b^2 = ab - b^2$	Subtraindo b^2 de ambos os lados de (3)
5. $(a + b)(a - b) = b(a - b)$	Fatorando ambos os lados de (4)
6. $a + b = b$	Dividindo ambos os lados de (5) por $(a - b)$
7. $2b = b$	Substituindo (2) em (6) e simplificando
8. $2 = 1$	Dividindo ambos os lados de (7) por b

Erros comuns em demonstrações

- Exemplo 24 (Continuação)

Solução.

Todos os passos na "demonstração" estão corretos, exceto pelo passo (6) e pelo passo (8).

Como $a = b$ (pelo passo (2)), temos que $a - b = 0$ e, portanto, a divisão de um real por $(a - b)$ não pode ser realizada.

Além disso, no passo (8) não sabemos se $b \neq 0$, logo não podemos dividir por b. $\triangleleft$

Erros comuns em demonstrações

- Outro erro comum em demonstrações é argumentar a partir de exemplos.

- Exemplo 25 **Teorema:** *"Se $m + n$ é par então $m - n$ é par."*

  Demonstração incorreta: Se $m = 14$ e $n = 6$ então $m + n = 20$, que é par, e $m - n = 8$, que também é par.

  Logo se $m + n$ é par então $m - n$ é par. □

Erros comuns em demonstrações

- Mais um tipo comum de erro é pular para uma conclusão, ou alegar a verdade de alguma coisa sem dar uma razão adequada.

- Exemplo 26 **Teorema:** *"Se $m + n$ é par então $m - n$ é par."*

  Demonstração incorreta: Suponha que m e n sejam inteiros e que $m + n$ é par. Pela definição de par, $m + n = 2k$ para algum inteiro k. Então $m = 2k - n$ e assim $m - n$ é par. □

- Exemplo 27 Corrija as demonstrações acima, demonstrando corretamente a afirmação *"Se $m + n$ é par então $m - n$ é par"*.

  Solução. Exercício para o(a) estudante! ◁

- Muitas das falácias que vimos na aula sobre inferência lógica são erros comuns em demonstrações.

O papel de problemas em aberto

- Algumas conjecturas ficam em aberto por muito tempo antes que se consiga demonstrar sua veracidade ou falsidade.
- Mesmo que falhem em demonstrar a veracidade ou falsidade da conjectura, frequentemente matemáticos fazem muitos avanços importantes ao tentar.
- Exemplos:
  1. **O Último Teorema de Fermat:** Não existem inteiros positivos x, y, z que satisfaçam a equação
  $$x^n + y^n = z^n$$
  para algum $n > 2$.

  Esta conjectura ficou em aberto de 1 621 até 1 994, quando foi resolvida.

  Tentando demonstrá-la, alguns matemáticos criaram o importante campo de teoria dos números algébrica (mas que não resolveu a conjectura).
  2. O maior problema em aberto em ciência da computação é o **Problema de P vs. NP**:

  "Todo problema cuja solução pode ser rapidamente verificada por um computador pode também ser rapidamente resolvido por um computador?"

Apêndice - Uma Última Demonstração: O Jogo de Chomp

Demonstração de existência não-construtiva: Jogo Chomp

- Vamos ver agora um último exemplo interessante de demonstração de existência não construtiva, baseada no conceito de **"roubo de estratégia"**.

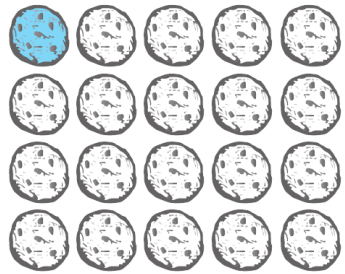
- Exemplo 28

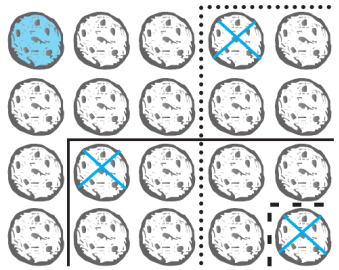
  Chomp é um jogo de dois jogadores, em que cookies são dispostos em uma grade retangular, e o cookie colocado na canto superior esquerdo é envenenado.

  A cada rodada, um jogador é obrigado a comer um biscoito restante, juntamente com todos os cookies à direita e/ou abaixo dele.

  O perdedor é o jogador quem não tem mais escolha a não ser comer o biscoito envenenado.

  Demonstre que um dos dois jogadores tem um **estratégia vencedora** (ou seja, que um dos jogadores pode sempre fazer movimentos que garantam sua eventual vitória sobre o oponente, não importa o que o oponente faça).





Demonstração de existência não-construtiva: Jogo Chomp

- Exemplo 28 (Continuação)

Solução.

Daremos uma demonstração não-construtiva de uma estratégia vencedora para o primeiro jogador.

(Ou seja, mostraremos que o primeiro jogador sempre tem uma estratégia vencedora sem explicitamente descrever os movimentos que este jogador deve seguir.)

Primeiro, note que o jogo sempre tem um fim, e que não é possível terminar em empate pois em cada movimento pelo menos um cookie é comido e, portanto, em no máximo $m \times n$ rodadas o jogo termina (onde m e n são o número de linhas e colunas da grade inicial). Logo, o jogo sempre tem um vencedor.

Agora, suponha que o primeiro jogador comece o jogo comendo apenas o biscoito na quina inferior direita.

Demonstração de existência não-construtiva: Jogo Chomp

- Exemplo 28 (Continuação)

Note que existem apenas duas possibilidades, mutuamente exclusivas:

Caso 1. Comer apenas o biscoito na quina inferior direita é o primeiro movimento de uma estratégia vencedora para o primeiro jogador.

(Ou seja, independentemente do que o segundo jogador fizer a partir deste momento no jogo, sempre existe uma maneira de o primeiro jogador reagir de forma a vencer o jogo no final.)

Caso 2. Logo em seguida ao primeiro jogador comer apenas o biscoito na quina inferior direita, o segundo jogador pode fazer um movimento que é o primeiro movimento de uma estratégia vencedora para o segundo jogador.

(Ou seja, este movimento permite que o segundo jogador sempre tenha uma resposta a qualquer movimento do primeiro jogador a partir deste momento, garantindo a eventual vitória do segundo jogador.)

Demonstração de existência não-construtiva: Jogo Chomp

- **Exemplo 28** (Continuação)

  Mas note que se o Caso (1) for verdade, a demonstração está terminada trivialmente.

  Vamos considerar, então, o Caso (2). Nesse caso, em vez de comer apenas o cookie no canto inferior direito, o primeiro jogador poderia ter feito o mesmo movimento que o segundo jogador fez como o primeiro movimento de uma estratégia vencedora (e depois continuar a seguir essa estratégia vencedora).

  Isso é suficiente para garantir que o primeiro jogador pode atingir a vitória com certeza! □

Demonstração de existência não-construtiva: Jogo Chomp

- Observe que no exemplo anterior mostramos que existe uma estratégia vencedora para o primeiro jogador, mas não especificamos uma vitória real estratégia.

  Consequentemente, a demonstração é uma demonstração de existência não-construtiva.

- Na verdade, ninguém foi capaz de descrever uma estratégia vencedora para Chomp que se aplique a todas as redes retangulares, descrevendo os movimentos que o primeiro jogador deve seguir!