MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira

Instituto de computação

UNICAMP

28 de agosto de 2023

1. Segunda lista de exercícios
2. Contraexemplos. Ou provando que uma proposição é falsa
3. Princípio da indução matemática (PIM)
4. Algumas generalizações do princípio da indução matemática
5. Perguntas, observações, comentários?

Segunda lista de exercícios

Contraexemplos. Ou provando que uma proposição é falsa

Proposições com valor-verdade desconhecidas

Algumas possibilidades para uma proposição:

- Simplesmente assumimos ser verdadeiras: axioma

Proposições com valor-verdade desconhecidas

Algumas possibilidades para uma proposição:

- Simplesmente assumimos ser verdadeiras: axioma
- Sabemos que é verdadeira (consequência dos axiomas): teoremas, lemas, ou corolários

Proposições com valor-verdade desconhecidas

Algumas possibilidades para uma proposição:

- Simplesmente assumimos ser verdadeiras: axioma
- Sabemos que é verdadeira (consequência dos axiomas): teoremas, lemas, ou corolários
- Acreditamos que é verdadeira, mas não conhecemos uma prova: conjectura
  - Dada uma conjectura C
  - Podemos tentar provar que C é verdadeira
  - Podemos tentar mostrar que C é falsa (i.e., provar $\neg C$)

Provando a falsidade de uma proposição

Considere uma proposição C

- C é da forma $\exists x\, P(x)$
  - $\neg C = \forall z\, \neg P(z)$
  - Pode ser bem difícil de provar...
  - Frequentemente, prova-se usando redução ao absurdo

Provando a falsidade de uma proposição

Considere uma proposição C

- C é da forma $\exists x\, P(x)$
  - $\neg C = \forall z\, \neg P(z)$
  - Pode ser bem difícil de provar...
  - Frequentemente, prova-se usando redução ao absurdo
- C é da forma $\forall x\, P(x)$
  - $\neg C = \exists z\, \neg P(z)$
  - Um valor z tal que $P(z)$ é falso é chamado de contraexemplo
  - Achar um contraexemplo pode ser bem mais fácil que fazer uma prova matemática

Contraexemplos

Considere uma proposição C da forma $\forall x\, P(x)$

- Se $P(x)$ é uma proposição "simples", sem conectivos, só encontre z tal que $P(z) = F$

Contraexemplos

Considere uma proposição C da forma $\forall x\, P(x)$

- Se $P(x)$ é uma proposição "simples", sem conectivos, só encontre z tal que $P(z) = F$
- Se $P(x)$ é da forma $A(x) \Rightarrow B(x)$.

Contraexemplos

Considere uma proposição C da forma $\forall x\, P(x)$

- Se $P(x)$ é uma proposição "simples", sem conectivos, só encontre z tal que $P(z) = F$
- Se $P(x)$ é da forma $A(x) \Rightarrow B(x)$.
  - $P(z) = F$ implica $A(z) = V$ e $B(z) = F$.

Considere uma proposição C da forma $\forall x \, P(x)$

- Se $P(x)$ é uma proposição "simples", sem conectivos, só encontre z tal que $P(z) = F$
- Se $P(x)$ é da forma $A(x) \Rightarrow B(x)$.
  - $P(z) = F$ implica $A(z) = V$ e $B(z) = F$.
- Se $P(x)$ é da forma $A(x) \Leftrightarrow B(x)$.

Contraexemplos

Considere uma proposição C da forma $\forall x\, P(x)$

- Se $P(x)$ é uma proposição "simples", sem conectivos, só encontre z tal que $P(z) = F$
- Se $P(x)$ é da forma $A(x) \Rightarrow B(x)$.
  - $P(z) = F$ implica $A(z) = V$ e $B(z) = F$.
- Se $P(x)$ é da forma $A(x) \Leftrightarrow B(x)$.
  - ache z tal que $A(x) \Rightarrow B(x)$ é falso

Contraexemplos

Considere uma proposição C da forma $\forall x\, P(x)$

- Se $P(x)$ é uma proposição "simples", sem conectivos, só encontre z tal que $P(z) = F$
- Se $P(x)$ é da forma $A(x) \Rightarrow B(x)$.
  - $P(z) = F$ implica $A(z) = V$ e $B(z) = F$.
- Se $P(x)$ é da forma $A(x) \Leftrightarrow B(x)$.
  - ache z tal que $A(x) \Rightarrow B(x)$ é falso
  - ou ache z tal que $B(x) \Rightarrow A(x)$ é falso

Encontre contraexemplos simples e específicos

Tente encontrar valores concretos para seus contraexemplos, pois isso diminui a possibilidade de erros (e facilita a verificação).

Encontre contraexemplos simples e específicos

Tente encontrar valores concretos para seus contraexemplos, pois isso diminui a possibilidade de erros (e facilita a verificação).

Por exemplo: considere a proposição

$$\forall x, y, z \in \mathbb{N},\ x^2 + y^2 = z^2$$

Encontre contraexemplos simples e específicos

Tente encontrar valores concretos para seus contraexemplos, pois isso diminui a possibilidade de erros (e facilita a verificação).

Por exemplo: considere a proposição

$$\forall x, y, z \in \mathbb{N},\ x^2 + y^2 = z^2$$

- $x = y$ e $z = 2$ é um contraexemplo

Encontre contraexemplos simples e específicos

Tente encontrar valores concretos para seus contraexemplos, pois isso diminui a possibilidade de erros (e facilita a verificação).

Por exemplo: considere a proposição

$$\forall x, y, z \in \mathbb{N},\, x^2 + y^2 = z^2$$

- $x = y$ e $z = 2$ é um contraexemplo
- $x = y = 0$ e $z = 1$ é um contraexemplo.

Encontre contraexemplos simples e específicos

Tente encontrar valores concretos para seus contraexemplos, pois isso diminui a possibilidade de erros (e facilita a verificação).

Por exemplo: considere a proposição

$$\forall x, y, z \in \mathbb{N},\ x^2 + y^2 = z^2$$

- $x = y$ e $z = 2$ é um contraexemplo
- $x = y = 0$ e $z = 1$ é um contraexemplo.
- Atenção! Cuidado com falsos contraexemplos: $x = y = 0$ e $z = \sqrt{2}$ não é um contraexemplo!

Considere a afirmação a seguir:

Seja $2\mathbb{Z}$ o conjunto dos números pares.

$$\forall w, x, y, z \in \mathbb{N}^* \, (w^2 + x^2 + y^2 = z^2 \Rightarrow (z \in 2\mathbb{Z} \Leftrightarrow w, x, y \in 2\mathbb{Z})).$$

Mais um caso de contraexemplo errado

Considere a afirmação a seguir:

Seja $2\mathbb{Z}$ o conjunto dos números pares.

$$\forall w, x, y, z \in \mathbb{N}^* \, (w^2 + x^2 + y^2 = z^2 \Rightarrow (z \in 2\mathbb{Z} \Leftrightarrow w, x, y \in 2\mathbb{Z})).$$

Na verdade, ela é o exercício 12 da primeira lista. Então, sabemos que é verdadeira.

Mas então, qual o problema com o seguinte contraexemplo?

- Sejam $w = x = 1$, logo, ímpares.
- Seja $y = 2$.
- Então $w^2 + x^2 + y^2 = z^2 \Rightarrow z^2 = 1 + 1 + 4 = 6 \Rightarrow z^2$ é par $\Rightarrow z$ é par

Exemplo de contraexemplos

Refute as seguintes afirmações (i.e., prove que elas são falsas):

1. O produto de dois números irracionais é irracional
2. Para quaisquer conjuntos A, B, C, temos $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$
3. Se p é primo, então $2^p - 1$ também o é

Princípio da indução matemática (PIM)

Princípio da indução matemática (PIM)

Essa é uma técnica útil para provar afirmações do tipo

$$\forall n \in \mathbb{N}\, P(n)$$

Princípio da indução matemática (PIM)

Essa é uma técnica útil para provar afirmações do tipo

$$\forall n \in \mathbb{N}\, P(n)$$

Ela funciona da seguinte forma:

- Primeiro, mostramos que $P(0)$ vale.
- Depois, mostramos que para qualquer $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$:
  - Assumimos $P(k)$
  - Inferimos $P(k+1)$

Se conseguirmos fazer isso, concluímos que $P(n)$ vale para todo $n \in \mathbb{N}$.

Intuição

Provamos que $P(0)$ vale e que $P(k)$ implica em $P(k+1)$. Logo,

- $P(0)$ implica em $P(1)$
- Mas então, $P(1)$ implica em $P(2)$
- Mas então, $P(2)$ implica em $P(3)$
- ...

Estrutura

1. *Caso base:* provamos $P(0)$
2. *Hipótese indutiva:* explicitamente assumimos $P(k)$
3. *Passo indutivo:* provamos $P(k+1)$ (usando $P(k)$)

Primeiro exemplo: somando como Gauss

Diz a lenda* que Gauss, quando tinha 7 anos, calculou a soma $1 + 2 + ... + 100$ em alguns segundos...

Dizem que ele inventou e usou a fórmula

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

Como podemos prová-la usando indução matemática?

*Veracidade questionável, mas amplamente difundida

Formalização

Provar $P(0)$ e uma sequência finita de implicações, como

$$P(0) \Rightarrow P(1) \Rightarrow ... \Rightarrow P(200)$$

realmente implica que $P(k)$ é verdade para $0 \leq k \leq 200$.

No entanto, com uma sequência infinita, a situação é diferente: Não há uma justificativa simples, apenas usando inferência lógica, de que

$$P(0) \wedge (P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow ...)$$

implica que $P(k)$ é verdade para todo $k \in \mathbb{N}$.

Formalização

Provar $P(0)$ e uma sequência finita de implicações, como

$$P(0) \Rightarrow P(1) \Rightarrow ... \Rightarrow P(200)$$

realmente implica que $P(k)$ é verdade para $0 \leq k \leq 200$.

No entanto, com uma sequência infinita, a situação é diferente: Não há uma justificativa simples, apenas usando inferência lógica, de que

$$P(0) \wedge (P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow ...)$$

implica que $P(k)$ é verdade para todo $k \in \mathbb{N}$.

Então, o princípio da indução matemática é tomado como um axioma!

Formalização

Provar $P(0)$ e uma sequência finita de implicações, como

$$P(0) \Rightarrow P(1) \Rightarrow ... \Rightarrow P(200)$$

realmente implica que $P(k)$ é verdade para $0 \leq k \leq 200$.

No entanto, com uma sequência infinita, a situação é diferente: Não há uma justificativa simples, apenas usando inferência lógica, de que

$$P(0) \wedge (P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow ...)$$

implica que $P(k)$ é verdade para todo $k \in \mathbb{N}$.

Então, o princípio da indução matemática é tomado como um axioma!

No entanto, mais tarde veremos que PIM pode ser derivado de um axioma simples (princípio da boa ordem).

Segundo exemplo: Somando ímpares

Ao somarmos números ímpares consecutivos, observamos o seguinte:

- Somando 1 número: $1 = 1^2$
- Somando 2 números: $1 + 3 = 4 = 2^2$
- Somando 3 números: $1 + 3 + 5 = 9 = 3^2$

Segundo exemplo: Somando ímpares

Ao somarmos números ímpares consecutivos, observamos o seguinte:

- Somando 1 número: $1 = 1^2$
- Somando 2 números: $1 + 3 = 4 = 2^2$
- Somando 3 números: $1 + 3 + 5 = 9 = 3^2$

Será que, em geral, temos que a soma dos n primeiros ímpares positivos é igual a n^2?
Como podemos provar isso usando indução matemática?

Algumas generalizações do princípio da indução matemática

Princípio da indução matemática com caso base arbitrário

Em vez de usar o caso base como zero, podemos na verdade começar provando $P(n_0)$ para qualquer $n_0 \in \mathbb{N}$.

A hipótese de indução agora é $P(k) = V$ para algum inteiro $k \geq n_0$.

O passo indutivo ainda é da forma $P(k) \Rightarrow P(k+1)$.

Finalmente, concluímos

$$\forall n \in D\, P(n)$$

onde $D = \{n_0, n_0 + 1, n_0 + 2...\}$ em vez de $D = \mathbb{N}$.

Princípio da indução matemática com caso base arbitrário

Em vez de usar o caso base como zero, podemos na verdade começar provando $P(n_0)$ para qualquer $n_0 \in \mathbb{N}$.

A hipótese de indução agora é $P(k) = V$ para algum inteiro $k \geq n_0$.

O passo indutivo ainda é da forma $P(k) \Rightarrow P(k+1)$.

Finalmente, concluímos

$$\forall n \in D \, P(n)$$

onde $D = \{n_0, n_0 + 1, n_0 + 2 ...\}$ em vez de $D = \mathbb{N}$.

Isso é formalizado definindo $Q(n) = P(n + n_0)$...

Exemplo PIM com caso base maior que 0

Algumas propriedades valem para quase todos os naturais, i.e., existem apenas algumas exceções.
Por exemplo:

$$\forall n \in \mathbb{N}, 2^n \geq n^2 + 1$$

é falso.
Mas definindo $D = \mathbb{N} \setminus \{0, 1, 2, 3, 4\} = \{5, 6, 7, ...\}$,

$$\forall n \in D,\ 2^n \geq n^2 + 1$$

é verdadeiro.
Como provar tal afirmação usando indução?

Perguntas, observações, comentários?