Técnicas de Demonstração
Lógica Matemática

Marnes Augusto Hoff

11 de Março de 2008

Técnicas de Demonstração de Teoremas

Sobre o que é essa palestra?

Técnicas de Demonstração de Teoremas

Sobre o que é essa palestra?

- Técnicas
  - abordagens, estratégias para

Técnicas de Demonstração de Teoremas

Sobre o que é essa palestra?

- Técnicas
  - abordagens, estratégias para
- Demonstração
  - ato de demonstrar, provar, convencer-se (e aos outros) sobre a veracidade de

Técnicas de Demonstração de Teoremas

Sobre o que é essa palestra?

- Técnicas
  - abordagens, estratégias para
- Demonstração
  - ato de demonstrar, provar, convencer-se (e aos outros) sobre a veracidade de
- Teoremas
  - proposições lógicas que podem ser (já foram) provadas

Teoremas aparecem em Teorias

Componentes de uma Teoria

- Uma Teoria é um sistema

Teoremas aparecem em Teorias

Componentes de uma Teoria

- Uma Teoria é um sistema
  - elementos / entidades

Teoremas aparecem em Teorias

Componentes de uma Teoria

- Uma Teoria é um sistema
  - elementos / entidades
  - axiomas / postulados
    - aceitos como verdades imediatas
    - não se prova

Teoremas aparecem em Teorias

Componentes de uma Teoria

- Uma Teoria é um sistema
  - elementos / entidades
  - axiomas / postulados
    - aceitos como verdades imediatas
    - não se prova
  - definições
    - batizar / dar nomes
    - "macros"

Teoremas aparecem em Teorias

Componentes de uma Teoria

- Uma Teoria é um sistema
  - elementos / entidades
  - axiomas / postulados
    - aceitos como verdades imediatas
    - não se prova
  - definições
    - batizar / dar nomes
    - "macros"
  - e tudo que decorre deles através de teoremas

Teoria

Outros componentes

- lema
  - teorema auxiliar
  - usado para provar outro
- corolário
  - "teorema" que é conseqüência imediata de outro
  - não se costuma chamar de teorema
- conjectura
  - proposição que se suspeita ser verdadeira
  - mas ainda não foi provada (nem refutada)

Teoremas e Provas

- Teorema
  - qualquer proposição lógica que tenha sido provada

Teoremas e Provas

- Teorema
  - qualquer proposição lógica que tenha sido provada
- Prova
  - argumento lógico
  - bem construído
  - finito

Técnicas de Prova

- Principais
  - direta
  - por contraposição ou transposição
  - por contradição ou (redução ao) absurdo
  - indutiva (indução matemática)

Técnicas de Prova

- Principais
  - direta
  - por contraposição ou transposição
  - por contradição ou (redução ao) absurdo
  - indutiva (indução matemática)
- Outras
  - por exaustão
  - geométrica
  - coindutiva (coindução – coálgebras)
  - ...

Teorema

(maioria)

- Condicional ou de implicação
- $A \Longrightarrow B$
  - $A =$ hipótese ou premissa
  - $B =$ tese ou conclusão

Teorema

(maioria)

- Condicional ou de implicação
- $A \Longrightarrow B$
  - A = hipótese ou premissa
  - B = tese ou conclusão

- Formas como pode aparecer

se A, então B	B, se A
A somente se B	B, sempre que A
A implica em B	B segue de A
A não pode acontecer sem B	
sempre que A ocorre, B ocorre	
A é suficiente para B	B é necessário para A

Prova Direta

Teorema $A \Longrightarrow B$

- Como provar $A \Longrightarrow B$?
- podemos utilizar qualquer coisa válida (já conhecida e aceita/provada)
  - implicações e equivalências da lógica (passos lógicos)
    - modus ponens
    - introdução do $\vee$ (adição)
    - eliminação do $\wedge$ (simplificação)
    - leis de De Morgan
    - ...
  - da teoria em questão
    - axiomas
    - definições
    - teoremas

Prova Direta

Teorema $A \Longrightarrow B$

- O que queremos mostrar?
  - a tese: B

Prova Direta

Teorema $A \Longrightarrow B$

- O que queremos mostrar?
  - a tese: B
- O que temos para isso?
  - a hipótese: A

Prova Direta

Teorema $A \Longrightarrow B$

- O que queremos mostrar?
  - a tese: B
- O que temos para isso?
  - a hipótese: A
- De que/onde partimos?
  - geralmente, de um dos "lados" da tese (quando a tese tem estrutura interna de implicação, equivalência, igualdade, etc.)
  - eventualmente, da hipótese
  - raramente, de outra coisa

Prova Direta

Exemplo 1 de Teorema $A \Longrightarrow B$

- "A soma de dois inteiros ímpares é par."

Prova Direta

Exemplo 1 de Teorema $A \Longrightarrow B$

- "A soma de dois inteiros ímpares é par."
- reescrevendo
  - Sejam x e y inteiros. Se x e y são ímpares, então $x + y$ é par
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow par(x + y)$

Prova Direta

Exemplo 1 de Teorema $A \Longrightarrow B$

- "A soma de dois inteiros ímpares é par."
- reescrevendo
  - Sejam x e y inteiros. Se x e y são ímpares, então $x + y$ é par
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow par(x + y)$
- mas o que significa "ser ímpar" e "ser par"?

Prova Direta

Exemplo 1 de Teorema $A \Longrightarrow B$

- "A soma de dois inteiros ímpares é par."
- reescrevendo
  - Sejam x e y inteiros. Se x e y são ímpares, então $x + y$ é par
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow par(x + y)$
- mas o que significa "ser ímpar" e "ser par"?
- Dica: **sempre** olhar as definições
  - geralmente, as definições ajudam a achar o caminho

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Definição de Par: Seja um inteiro a,
  - a é par, sse existe um inteiro k tal que $a = 2k$
  - $par(a) \Longleftrightarrow \exists k \in \mathbb{Z}.(a = 2k)$
- Definição de Ímpar: Seja um inteiro a,
  - a é ímpar, sse existe um inteiro k tal que $a = 2k + 1$
  - $impar(a) \Longleftrightarrow \exists k \in \mathbb{Z}.(a = 2k + 1)$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Definição de Par: Seja um inteiro a,
  - a é par, sse existe um inteiro k tal que $a = 2k$
  - $par(a) \Longleftrightarrow \exists k \in \mathbb{Z}.(a = 2k)$
- Definição de Ímpar: Seja um inteiro a,
  - a é ímpar, sse existe um inteiro k tal que $a = 2k + 1$
  - $impar(a) \Longleftrightarrow \exists k \in \mathbb{Z}.(a = 2k + 1)$

- Teorema
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow par(x + y)$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Definição de Par: Seja um inteiro a,
  - a é par, sse existe um inteiro k tal que $a = 2k$
  - $par(a) \Longleftrightarrow \exists k \in \mathbb{Z}.(a = 2k)$
- Definição de Ímpar: Seja um inteiro a,
  - a é ímpar, sse existe um inteiro k tal que $a = 2k + 1$
  - $impar(a) \Longleftrightarrow \exists k \in \mathbb{Z}.(a = 2k + 1)$

- Teorema
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow par(x + y)$
  - $$\forall x, y \in \mathbb{Z}, \left\{ \begin{array}{c} \exists k_1 \in \mathbb{Z}.(x = 2k_1 + 1) \\ \wedge \\ \exists k_2 \in \mathbb{Z}.(y = 2k_2 + 1) \end{array} \right\} \Rightarrow \exists k_3 \in \mathbb{Z}.(x + y = 2k_3)$$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$
- Temos a hipótese: $\begin{cases} x = 2k_1 + 1 \text{ para algum } k_1 \in \mathbb{Z} \\ y = 2k_2 + 1 \text{ para algum } k_2 \in \mathbb{Z} \end{cases}$
  - em algum lugar ela deve ser necessária

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$
- Temos a hipótese: $\begin{cases} x = 2k_1 + 1 \text{ para algum } k_1 \in \mathbb{Z} \\ y = 2k_2 + 1 \text{ para algum } k_2 \in \mathbb{Z} \end{cases}$
  - em algum lugar ela deve ser necessária

- Prova Direta
  $x + y$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$
- Temos a hipótese: $\begin{cases} x = 2k_1 + 1 & \text{para algum } k_1 \in \mathbb{Z} \\ y = 2k_2 + 1 & \text{para algum } k_2 \in \mathbb{Z} \end{cases}$
  - em algum lugar ela deve ser necessária

- Prova Direta

$x + y$	$=$	pelas hipóteses
$(2k_1 + 1) + (2k_2 + 1)$		

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$
- Temos a hipótese: $\begin{cases} x = 2k_1 + 1 & \text{para algum } k_1 \in \mathbb{Z} \\ y = 2k_2 + 1 & \text{para algum } k_2 \in \mathbb{Z} \end{cases}$
  - em algum lugar ela deve ser necessária

- Prova Direta

$$\begin{array}{lcl} x + y & = & \text{pelas hipóteses} \\ (2k_1 + 1) + (2k_2 + 1) & = & \\ 2k_1 + 2k_2 + 2 & & \end{array}$$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$
- Temos a hipótese: $\begin{cases} x = 2k_1 + 1 & \text{para algum } k_1 \in \mathbb{Z} \\ y = 2k_2 + 1 & \text{para algum } k_2 \in \mathbb{Z} \end{cases}$
  - em algum lugar ela deve ser necessária

- Prova Direta

$$
\begin{array}{lcl}
x + y & = & \text{pelas hipóteses} \\
(2k_1 + 1) + (2k_2 + 1) & = & \\
2k_1 + 2k_2 + 2 & = & \\
2(k_1 + k_2 + 1) & &
\end{array}
$$

Prova Direta

Exemplo de Teorema $A \Longrightarrow B$

- Queremos mostrar a tese: $x + y = 2k_3$ para algum $k_3 \in \mathbb{Z}$
  - tem uma estrutura interna de igualdade
- Como mostrar? Sugestão: $x + y = ... = ... = ... = 2k_3$
- Temos a hipótese: $\begin{cases} x = 2k_1 + 1 & \text{para algum } k_1 \in \mathbb{Z} \\ y = 2k_2 + 1 & \text{para algum } k_2 \in \mathbb{Z} \end{cases}$
  - em algum lugar ela deve ser necessária

- Prova Direta

$x + y$	$=$	pelas hipóteses
$(2k_1 + 1) + (2k_2 + 1)$	$=$	
$2k_1 + 2k_2 + 2$	$=$	
$2(k_1 + k_2 + 1)$	$=$	assumindo $k_3 = k_1 + k_2 + 1$
$2k_3$		$\square$

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- "A composição de funções injetoras é uma função injetora."

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- "A composição de funções injetoras é uma função injetora."
- reescrevendo
  - Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow C$ funções.
    Se f e g são injetoras, então $g \circ f : A \longrightarrow C$ é injetora

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- "A composição de funções injetoras é uma função injetora."
- reescrevendo
  - Sejam $f : A \to B$ e $g : B \to C$ funções.
    Se f e g são injetoras, então $g \circ f : A \to C$ é injetora

- Definição de Injetora: Seja $m : A \to B$ uma função
  - m é injetora $\Longleftrightarrow \forall x, y \in A.(m(x) = m(y) \Longrightarrow x = y)$

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- "A composição de funções injetoras é uma função injetora."
- reescrevendo
  - Sejam $f : A \to B$ e $g : B \to C$ funções.
    Se f e g são injetoras, então $g \circ f : A \to C$ é injetora

- Definição de Injetora: Seja $m : A \to B$ uma função
  - m é injetora $\Longleftrightarrow \forall x, y \in A.(m(x) = m(y) \Longrightarrow x = y)$

- A tese que queremos mostrar
  - $\forall x, y \in A.(g \circ f(x) = g \circ f(y) \Longrightarrow x = y)$
  - tem uma estrutura interna de implicação

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- Mostrar: $\forall x, y \in A.(g \circ f(x) = g \circ f(y) \Longrightarrow x = y)$
  - usar $x, y \in A$ quaisquer (genéricos)
  - tentar: $g \circ f(x) = g \circ f(y) \Longrightarrow ... \Longrightarrow ... \Longrightarrow x = y$
  - em algum lugar, as hipóteses devem ser necessárias

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- Mostrar: $\forall x, y \in A.(g \circ f(x) = g \circ f(y) \Longrightarrow x = y)$
  - usar $x, y \in A$ quaisquer (genéricos)
  - tentar: $g \circ f(x) = g \circ f(y) \Longrightarrow ... \Longrightarrow ... \Longrightarrow x = y$
  - em algum lugar, as hipóteses devem ser necessárias

- Prova Direta
  - Sejam $x, y \in A$ quaisquer,
    $g \circ f(x) = g \circ f(y)$

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- Mostrar: $\forall x, y \in A.(g \circ f(x) = g \circ f(y) \Longrightarrow x = y)$
  - usar $x, y \in A$ quaisquer (genéricos)
  - tentar: $g \circ f(x) = g \circ f(y) \Longrightarrow ... \Longrightarrow ... \Longrightarrow x = y$
  - em algum lugar, as hipóteses devem ser necessárias

- Prova Direta
  - Sejam $x, y \in A$ quaisquer,
    $g \circ f(x) = g \circ f(y) \quad \Longrightarrow \quad$ composição de funções
    $g(f(x)) = g(f(y))$

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- Mostrar: $\forall x, y \in A.(g \circ f(x) = g \circ f(y) \Longrightarrow x = y)$
  - usar $x, y \in A$ quaisquer (genéricos)
  - tentar: $g \circ f(x) = g \circ f(y) \Longrightarrow ... \Longrightarrow ... \Longrightarrow x = y$
  - em algum lugar, as hipóteses devem ser necessárias

- Prova Direta
  - Sejam $x, y \in A$ quaisquer,

$$
\begin{array}{lcl}
g \circ f(x) = g \circ f(y) & \Longrightarrow & \text{composição de funções} \\
g(f(x)) = g(f(y)) & \Longrightarrow & \text{hipótese: } g \text{ é injetora} \\
f(x) = f(y) & &
\end{array}
$$

Prova Direta

Exemplo 2 de Teorema $A \Longrightarrow B$

- Mostrar: $\forall x, y \in A.(g \circ f(x) = g \circ f(y) \Longrightarrow x = y)$
  - usar $x, y \in A$ quaisquer (genéricos)
  - tentar: $g \circ f(x) = g \circ f(y) \Longrightarrow ... \Longrightarrow ... \Longrightarrow x = y$
  - em algum lugar, as hipóteses devem ser necessárias

- Prova Direta
  - Sejam $x, y \in A$ quaisquer,

$$
\begin{array}{lcl}
g \circ f(x) = g \circ f(y) & \Longrightarrow & \text{composição de funções} \\
g(f(x)) = g(f(y)) & \Longrightarrow & \text{hipótese: } g \text{ é injetora} \\
f(x) = f(y) & \Longrightarrow & \text{hipótese: } f \text{ é injetora} \\
x = y & & \square
\end{array}
$$

Símbolos × Palavras

- Uma demonstração precisa ser escrita com símbolos?
  - Não!!!
  - Mas precisa ser correta!

Símbolos × Palavras

- Uma demonstração precisa ser escrita com símbolos?
  - Não!!!
  - Mas precisa ser correta!

- Demonstração correta para o teorema anterior (é exatamente a mesma demonstração)
  - Sejam x e y dois elementos quaisquer do conjunto A. Supõe-se que $g \circ f(x)$ é igual a $g \circ f(y)$. Com isso, pode-se usar a definição de composição de funções para se chegar no fato que $g(f(x))$ é igual a $g(f(y))$. Daí, como, pela hipótese, a função g é injetora, pode-se concluir que $f(x)$ é igual a $f(y)$. Da mesma forma, como a função f é injetora, conclui-se que x é igual a y.

Demonstração × "Enrolação"

- Tentativa de "enrolar"
  - Como a primeira função, f, não envia dois elementos distintos x e y, pertencentes ao conjunto origem A, para um mesmo elemento $z \in B$, até chegar no segundo conjunto, não feriu a injetividade da função. A segunda função, g, se comporta da mesma forma, ou seja, não envia dois elementos distintos z e w de B para um mesmo elemento v de C. Portanto, a composição das duas funções claramente também será injetora, pois também não enviará dois elementos distintos da origem para um mesmo elemento no conjunto destino.
    - enunciou o teorema novamente, de forma mais "enrolada"
- intuição $\neq$ demonstração
- demonstração
  - entra nos detalhes
  - não deixa algo obscuro ("... **claramente** também será ...")
  - convence!

Equivalências Úteis

- Qualquer equivalência serve para reestruturar uma prova

Mostrar	$\iff$	Mostrar
$A \implies (B \implies C)$	$\iff$	$(A \wedge B) \implies C$
$A \implies (B \implies (C \implies D)$	$\iff$	$(A \wedge B \wedge C) \implies D$
$A \implies (B \vee C)$	$\iff$	$(A \wedge \neg B) \implies C$
...	$\iff$	...

Equivalências Úteis

- Qualquer equivalência serve para reestruturar uma prova

Mostrar	$\iff$	Mostrar
$A \implies (B \implies C)$	$\iff$	$(A \wedge B) \implies C$
$A \implies (B \implies (C \implies D)$	$\iff$	$(A \wedge B \wedge C) \implies D$
$A \implies (B \vee C)$	$\iff$	$(A \wedge \neg B) \implies C$
...	$\iff$	...

- Em especial

Mostrar	$\iff$	Mostrar	Prova por
$A \implies B$	$\iff$	$\neg B \implies \neg A$	Contraposição
$A \implies B$	$\iff$	$A \wedge \neg B \implies F$	Contradição ou Absurdo

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$
- a contraposição
  - $\forall x, y \in \mathbb{Z},\ \neg par(x) \wedge \neg par(y) \Longrightarrow \neg par(xy)$
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow impar(xy)$

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$
- a contraposição
  - $\forall x, y \in \mathbb{Z},\ \neg par(x) \wedge \neg par(y) \Longrightarrow \neg par(xy)$
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow impar(xy)$

- Prova por Contraposição
  xy

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$
- a contraposição
  - $\forall x, y \in \mathbb{Z},\ \neg par(x) \wedge \neg par(y) \Longrightarrow \neg par(xy)$
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow impar(xy)$

- Prova por Contraposição

  xy $=$ pelas hipóteses

  $(2k_1 + 1)(2k_2 + 1)$

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$
- a contraposição
  - $\forall x, y \in \mathbb{Z},\ \neg par(x) \wedge \neg par(y) \Longrightarrow \neg par(xy)$
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow impar(xy)$

- Prova por Contraposição

$$
\begin{array}{lcl}
xy & = & \text{pelas hipóteses} \\
(2k_1 + 1)(2k_2 + 1) & = & \\
4k_1k_2 + 2k_1 + 2k_2 + 1 & &
\end{array}
$$

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$
- a contraposição
  - $\forall x, y \in \mathbb{Z},\ \neg par(x) \wedge \neg par(y) \Longrightarrow \neg par(xy)$
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow impar(xy)$

- Prova por Contraposição

$$
\begin{array}{lcl}
xy & = & \text{pelas hipóteses} \\
(2k_1+1)(2k_2+1) & = & \\
4k_1k_2 + 2k_1 + 2k_2 + 1 & = & \\
2(2k_1k_2 + k_1 + k_2) + 1 & &
\end{array}
$$

Prova por Contraposição

Exemplo de Teorema $A \Longrightarrow B$

- $\forall x, y \in \mathbb{Z},\ par(xy) \Longrightarrow par(x) \vee par(y)$
- a contraposição
  - $\forall x, y \in \mathbb{Z},\ \neg par(x) \wedge \neg par(y) \Longrightarrow \neg par(xy)$
  - $\forall x, y \in \mathbb{Z},\ impar(x) \wedge impar(y) \Longrightarrow impar(xy)$

- Prova por Contraposição

$$
\begin{array}{lcl}
xy & = & \text{pelas hipóteses} \\
(2k_1+1)(2k_2+1) & = & \\
4k_1k_2 + 2k_1 + 2k_2 + 1 & = & \\
2(2k_1k_2 + k_1 + k_2) + 1 & = & \text{com } k_3 = 2k_1k_2 + k_1 + k_2 \\
2k_3 + 1 & & \square
\end{array}
$$

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \longrightarrow B$ e $S : A \longrightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \longrightarrow B$ e $S : A \longrightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \longrightarrow B$ e $S : A \longrightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \longrightarrow B$ e $S : A \longrightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo
  - Como $R \cap S$ não é simétrica,
    $\exists \langle x, y \rangle \in R \cap S$ tal que $\langle y, x \rangle \notin R \cap S$.

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \longrightarrow B$ e $S : A \longrightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo
  - Como $R \cap S$ não é simétrica,
    $\exists \langle x, y \rangle \in R \cap S$ tal que $\langle y, x \rangle \notin R \cap S$.
  - Entretanto, considerando-se esse mesmo par
    $\langle x, y \rangle \in R \cap S$

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \rightarrow B$ e $S : A \rightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo
  - Como $R \cap S$ não é simétrica,
    $\exists \langle x, y \rangle \in R \cap S$ tal que $\langle y, x \rangle \notin R \cap S$.
  - Entretanto, considerando-se esse mesmo par
    $\langle x, y \rangle \in R \cap S \quad \Longrightarrow \quad$ definição de $\cap$
    $\langle x, y \rangle \in R \ \wedge \ \langle x, y \rangle \in S$

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \rightarrow B$ e $S : A \rightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo
  - Como $R \cap S$ não é simétrica,
    $\exists \langle x, y \rangle \in R \cap S$ tal que $\langle y, x \rangle \notin R \cap S$.
  - Entretanto, considerando-se esse mesmo par

$$\begin{array}{lcl} \langle x, y \rangle \in R \cap S & \Longrightarrow & \text{definição de } \cap \\ \langle x, y \rangle \in R \ \wedge \ \langle x, y \rangle \in S & \Longrightarrow & R \text{ e } S \text{ são simétricas} \\ \langle y, x \rangle \in R \ \wedge \ \langle y, x \rangle \in S & & \end{array}$$

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \rightarrow B$ e $S : A \rightarrow B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo
  - Como $R \cap S$ não é simétrica,
    $\exists \langle x, y \rangle \in R \cap S$ tal que $\langle y, x \rangle \notin R \cap S$.
  - Entretanto, considerando-se esse mesmo par

$$
\begin{array}{lcl}
\langle x, y \rangle \in R \cap S & \Longrightarrow & \text{definição de } \cap \\
\langle x, y \rangle \in R \ \wedge \ \langle x, y \rangle \in S & \Longrightarrow & R \text{ e } S \text{ são simétricas} \\
\langle y, x \rangle \in R \ \wedge \ \langle y, x \rangle \in S & \Longrightarrow & \text{definição de } \cap \\
\langle y, x \rangle \in R \cap S & &
\end{array}
$$

Prova por (Redução ao) Absurdo

Exemplo de Teorema $A \Longrightarrow B$

- Sejam $R : A \to B$ e $S : A \to B$ relações binárias.
  R e S são simétricas $\Longrightarrow$ $R \cap S$ é simétrica
- a forma do absurdo
  - (R e S são simétricas) e $R \cap S$ não é simétrica $\Longrightarrow$ *Falso*
- Prova por Absurdo
  - Como $R \cap S$ não é simétrica,
    $\exists \langle x, y \rangle \in R \cap S$ tal que $\langle y, x \rangle \notin R \cap S$.
  - Entretanto, considerando-se esse mesmo par

    $\langle x, y \rangle \in R \cap S \quad \Longrightarrow \quad$ definição de $\cap$

    $\langle x, y \rangle \in R \ \wedge \ \langle x, y \rangle \in S \quad \Longrightarrow \quad R$ e S são simétricas

    $\langle y, x \rangle \in R \ \wedge \ \langle y, x \rangle \in S \quad \Longrightarrow \quad$ definição de $\cap$

    $\langle y, x \rangle \in R \cap S$
  - O que é um absurdo. Portanto, $R \cap S$ é simétrica. $\square$

Teorema

- Bicondicional ou de Equivalência
  - $A \iff B$
  - Formas como pode aparecer

    A se, e somente se, B
    A é equivalente a B
    A é necessário e suficiente para B

  - Como Provar?
    - geralmente, provando $A \implies B$ e $B \implies A$
    - eventualmente, provando a própria equivalência $A \iff B$

Princípio da Indução Matemática

- É um dos axiomas de Peano (definição de $\mathbb{N}$)
  - é aceito (não se prova)
- Idéia aplicada a
  - definições indutivas
  - funções recursivas
  - provas indutivas
    - proposições sobre $\mathbb{N}$
    - generalização: proposições sobre conjuntos enumeráveis
- Dois Tipos
  - Primeiro Princípio de Indução — Indução Tipo 1 — Indução Fraca
  - Segundo Princípio de Indução — Indução Tipo 2 — Indução Forte

Primeiro Princípio da Indução Matemática

- Objetivo
  - demonstrar uma proposição $P(n)$ para qualquer $n \in \mathbb{N}$

Primeiro Princípio da Indução Matemática

- Objetivo
  - demonstrar uma proposição $P(n)$ para qualquer $n \in \mathbb{N}$
- $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$
  - Nomenclatura
    - Base de Indução: $P(0)$
    - Hipótese de Indução: $\forall k \in \mathbb{N} \; . \; P(k)$
    - Passo de Indução: $\forall k \in \mathbb{N} \; . \; P(k) \Longrightarrow P(k+1)$

Primeiro Princípio da Indução Matemática

- Objetivo
  - demonstrar uma proposição $P(n)$ para qualquer $n \in \mathbb{N}$
- $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$
  - Nomenclatura
    - Base de Indução: $P(0)$
    - Hipótese de Indução: $\forall k \in \mathbb{N} \; . \; P(k)$
    - Passo de Indução: $\forall k \in \mathbb{N} \; . \; P(k) \Longrightarrow P(k+1)$
  - Para se considerar a conclusão provada basta se provar as duas premissas da regra
    - base
    - passo
    - (como sempre, não se prova a hipótese)

Estratégia

Primeiro Princípio da Indução Matemática

- provar a Base: $P(0)$
  - geralmente é simples

Estratégia

Primeiro Princípio da Indução Matemática

- provar a Base: $P(0)$
  - geralmente é simples
- "provar o Passo"
  - acreditar na Hipótese: $P(k)$
    (supor que é verdadeira)
  - provar a tese do Passo: $P(k+1)$
    - prova direta, por contraposição, por absurdo, por indução, ...
    - provavelmente a hipótese será necessária

Primeiro Princípio da Indução Matemática

Variação

- Original
  - $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$

Primeiro Princípio da Indução Matemática

Variação

- Original
  - $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$
- Generalização: para qualquer valor inicial $b \in \mathbb{N}$
  - $$\frac{P(b) \qquad \forall k \geq b \in \mathbb{N}.P(k) \Longrightarrow P(k+1)}{\forall n \geq b \in \mathbb{N}.P(n)}$$
- Também se pode generalizar para o conjunto $\mathbb{Z}$ e $b < 0$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- "A soma dos primeiros n ímpares positivos é n^2."

n	ímpares	soma
1	1	1
2	1,3	4
3	1,3,5	9
4	1,3,5,7	16

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- "A soma dos primeiros n ímpares positivos é n^2."

n	ímpares	soma
1	1	1
2	1,3	4
3	1,3,5	9
4	1,3,5,7	16

- reescrevendo
  - Para $n \geq 1 \in \mathbb{N}$, $\quad 1 + 3 + ... + (2n - 1) = n^2$
  - Para $n \geq 1 \in \mathbb{N}$,

$$\sum_{i=1}^{n} (2i - 1) = n^2$$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}$, $\quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$
  - Passo: deve-se mostrar $P(k + 1)$, provavelmente usando $P(k)$
    $1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \quad ... \quad = \quad (k + 1)^2$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$
  - Passo: deve-se mostrar $P(k + 1)$, provavelmente usando $P(k)$
    $1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \quad ... \quad = \quad (k + 1)^2$
    $\overline{\left| \; 1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \qquad = \right.}$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$
  - Passo: deve-se mostrar $P(k + 1)$, provavelmente usando $P(k)$
    $1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \quad ... \quad = \quad (k + 1)^2$

$$\begin{array}{|l} 1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \\ (1 + 3 + ... + (2k - 1)) \; + \; (2(k + 1) - 1) \quad = \end{array}$$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$
  - Passo: deve-se mostrar $P(k + 1)$, provavelmente usando $P(k)$
    $1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \quad ... \quad = \quad (k + 1)^2$

$$
\begin{array}{|lll|}
\hline
1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) & = & \\
(1 + 3 + ... + (2k - 1)) \; + \; (2(k + 1) - 1) & = & \text{pela hipótese} \\
k^2 \quad + \quad 2k + 2 - 1 & = & \\
\hline
\end{array}
$$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}$, $\quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$
  - Passo: deve-se mostrar $P(k + 1)$, provavelmente usando $P(k)$
    $1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \quad ... \quad = \quad (k + 1)^2$

$$
\begin{array}{lll}
1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) & = & \\
(1 + 3 + ... + (2k - 1)) \; + \; (2(k + 1) - 1) & = & \text{pela hipótese} \\
k^2 \quad + \quad 2k + 2 - 1 & = & \\
(k + 1)^2 & & \square
\end{array}
$$

Prova por Indução

Exemplo 1 — Indução do Tipo 1

- Para $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$
- Prova por Indução
  - Base: $P(1)$
    para $n = 1$, tem-se $(2 \cdot 1 - 1) = 1 = 1^2$
  - Hipótese: supõe-se que $P(k)$ vale, para qualquer $k \geq 1$
    $\forall k \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2k - 1) = k^2$
  - Passo: deve-se mostrar $P(k + 1)$, provavelmente usando $P(k)$
    $1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) \quad = \quad ... \quad = \quad (k + 1)^2$

$$
\begin{array}{lll}
1 + 3 + ... + (2k - 1) + (2(k + 1) - 1) & = & \\
(1 + 3 + ... + (2k - 1)) \; + \; (2(k + 1) - 1) & = & \text{pela hipótese} \\
k^2 \quad + \quad 2k + 2 - 1 & = & \\
(k + 1)^2 & & \square
\end{array}
$$

- A prova acima mostra que
  $n \geq 1 \in \mathbb{N}, \quad 1 + 3 + ... + (2n - 1) = n^2$

Idéia da Indução Matemática

Por que funciona?

- Situação
  1. $P(a)$ (premissa)
  2. $P(a) \Longrightarrow P(b)$ (premissa)
  3. $P(b) \Longrightarrow P(c)$ (premissa)
  4. $P(c) \Longrightarrow P(d)$ (premissa)

Idéia da Indução Matemática

Por que funciona?

- Situação
  1. $P(a)$ (premissa)
  2. $P(a) \Longrightarrow P(b)$ (premissa)
  3. $P(b) \Longrightarrow P(c)$ (premissa)
  4. $P(c) \Longrightarrow P(d)$ (premissa)
  5. $P(b)$ Modus Ponens 2, 1

Idéia da Indução Matemática

Por que funciona?

- Situação

1.	$P(a)$	(premissa)
2.	$P(a) \Longrightarrow P(b)$	(premissa)
3.	$P(b) \Longrightarrow P(c)$	(premissa)
4.	$P(c) \Longrightarrow P(d)$	(premissa)
5.	$P(b)$	Modus Ponens 2, 1
6.	$P(c)$	Modus Ponens 3, 5

Idéia da Indução Matemática

Por que funciona?

- Situação

1.	$P(a)$	(premissa)
2.	$P(a) \Longrightarrow P(b)$	(premissa)
3.	$P(b) \Longrightarrow P(c)$	(premissa)
4.	$P(c) \Longrightarrow P(d)$	(premissa)
5.	$P(b)$	Modus Ponens 2, 1
6.	$P(c)$	Modus Ponens 3, 5
7.	$P(d)$	Modus Ponens 4, 6

Idéia da Indução Matemática

Por que funciona?

- Situação
  1. $P(a)$ (premissa)
  2. $P(a) \Longrightarrow P(b)$ (premissa)
  3. $P(b) \Longrightarrow P(c)$ (premissa)
  4. $P(c) \Longrightarrow P(d)$ (premissa)
  5. $P(b)$ Modus Ponens 2, 1
  6. $P(c)$ Modus Ponens 3, 5
  7. $P(d)$ Modus Ponens 4, 6
- Se houver infinitas implicações

  $P(0) \qquad P(0) \Longrightarrow P(1) \qquad P(1) \Longrightarrow P(2) \qquad P(2) \Longrightarrow P(3) \qquad \ldots$

  aplica-se Modus Ponens tantas vezes quantas necessárias
- De fato, o passo de indução significa "infinitas implicações"

  $\forall k \in \mathbb{N} \,.\, P(k) \Longrightarrow P(k+1)$

Idéia da Indução Matemática

- "Algoritmo" usado para $P(k+1)$ em função de $P(k)$
  - é genérico
  - pode ser instanciado para qualquer k
  - exemplo para $P(8)$ (ou seja, $P(7+1)$, com $k=7$)

$$
\begin{array}{lcl}
1+3+\ldots+(2\cdot 7-1)+(2(7+1)-1) & = & \\
(1+3+\ldots+(2\cdot 7-1)) \;+\; (2(7+1)-1) & = & \text{usando } P(7) \\
7^2 \quad + \quad 2\cdot 7+2-1 & = & \\
(7+1)^2 & &
\end{array}
$$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \;.\; a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \;.\; a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$
  - Hipótese: $\forall k \in \mathbb{N}, \quad k^3 + (k+1)^3 + (k+2)^3 = 9x,\ x \in \mathbb{Z}$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$
  - Hipótese: $\forall k \in \mathbb{N}, \quad k^3 + (k+1)^3 + (k+2)^3 = 9x,\ x \in \mathbb{Z}$
  - Passo
    $(k+1)^3+(k+2)^3+(k+3)^3 \qquad\qquad\qquad\qquad =$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$
  - Hipótese: $\forall k \in \mathbb{N}, \quad k^3 + (k+1)^3 + (k+2)^3 = 9x,\ x \in \mathbb{Z}$
  - Passo

$$
\begin{aligned}
(k+1)^3+(k+2)^3+(k+3)^3 &= \\
(k+1)^3+(k+2)^3+k^3+9k^2+27k+27 &=
\end{aligned}
$$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$
  - Hipótese: $\forall k \in \mathbb{N}, \quad k^3 + (k+1)^3 + (k+2)^3 = 9x,\ x \in \mathbb{Z}$
  - Passo

$$
\begin{array}{lll}
(k+1)^3+(k+2)^3+(k+3)^3 & = & \\
(k+1)^3+(k+2)^3+k^3+9k^2+27k+27 & = & \text{pela hipótese} \\
9x \qquad\qquad +9k^2+27k+27 & = &
\end{array}
$$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$
  - Hipótese: $\forall k \in \mathbb{N}, \quad k^3 + (k+1)^3 + (k+2)^3 = 9x,\ x \in \mathbb{Z}$
  - Passo

$$
\begin{array}{lll}
(k+1)^3+(k+2)^3+(k+3)^3 & = & \\
(k+1)^3+(k+2)^3+k^3+9k^2+27k+27 & = & \text{pela hipótese} \\
9x \qquad\qquad +9k^2+27k+27 & = & \\
9(x+k^2+3k+3) & = &
\end{array}
$$

Prova por Indução

Exemplo 2 — Indução do Tipo 1

- "A soma dos cubos de três naturais consecutivos é um múlt. de 9."
  - Definição: a é múltiplo de 9 $\iff \exists x \in \mathbb{Z} \,.\, a = 9x$
- reescrevendo: $\forall n \in \mathbb{N}, \quad n^3 + (n+1)^3 + (n+2)^3 = 9x,\ x \in \mathbb{Z}$
- Prova por Indução
  - Base: $0^3 + 1^3 + 2^3 \;=\; 0 + 1 + 8 \;=\; 9 \;= 9 \cdot 1$
  - Hipótese: $\forall k \in \mathbb{N}, \quad k^3 + (k+1)^3 + (k+2)^3 = 9x,\ x \in \mathbb{Z}$
  - Passo

$$
\begin{array}{lll}
(k+1)^3+(k+2)^3+(k+3)^3 & = & \\
(k+1)^3+(k+2)^3+k^3+9k^2+27k+27 & = & \text{pela hipótese} \\
9x \qquad\qquad +9k^2+27k+27 & = & \\
9(x+k^2+3k+3) & = & y = x+k^2+3k+3 \\
9y, \text{ com } y \in \mathbb{Z} & & \square
\end{array}
$$

Segundo Princípio da Indução Matemática

- Objetivo: o mesmo
- Motivo
  - há situações em que, para mostrar $P(k+1)$
    - não se pode depender única e exclusivamente de $P(k)$
    - pode ser necessário algum $P(i)$ com $0 \leq i \leq k$
- Solução
  - assumir que todos os anteriores são verdadeiros

Segundo Princípio da Indução Matemática

- Objetivo: o mesmo
- Motivo
  - há situações em que, para mostrar $P(k+1)$
    - não se pode depender única e exclusivamente de $P(k)$
    - pode ser necessário algum $P(i)$ com $0 \leq i \leq k$
- Solução
  - assumir que todos os anteriores são verdadeiros
- $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$
  - provavelmente, algum dos $P(i)$ será necessário
  - mas não se sabe qual, por isso se assume todos

Segundo Princípio da Indução Matemática

Variação

- Original
  - $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(0) \wedge P(1) \wedge \ldots \wedge P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$

Segundo Princípio da Indução Matemática

Variação

- Original
  - $$\frac{P(0) \qquad \forall k \in \mathbb{N}.P(0) \wedge P(1) \wedge \ldots \wedge P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$
- Generalização: para qualquer valor inicial $a \in \mathbb{N}$
  - $$\frac{P(a) \qquad \forall k \in \mathbb{N}.P(a) \wedge P(a+1) \wedge \ldots \wedge P(k) \Longrightarrow P(k+1)}{\forall n \in \mathbb{N}.P(n)}$$
- Também se pode generalizar para o conjunto $\mathbb{Z}$ e $a < 0$

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- "Todo inteiro positivo possui uma representação em binário."

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- "Todo inteiro positivo possui uma representação em binário."
- reescrevendo
  - $\forall n > 0 \in \mathbb{N}$

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- "Todo inteiro positivo possui uma representação em binário."
- reescrevendo
  - $\forall n > 0 \in \mathbb{N}$
  - $\exists r \in \mathbb{N}$ (quantidade de bits)

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- "Todo inteiro positivo possui uma representação em binário."
- reescrevendo
  - $\forall n > 0 \in \mathbb{N}$
  - $\exists r \in \mathbb{N}$ (quantidade de bits)
  - $\exists b_{r-1}, b_{r-2}, ..., b_2, b_1, b_0 \in \{0, 1\}$ (os bits)

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- "Todo inteiro positivo possui uma representação em binário."
- reescrevendo
  - $\forall n > 0 \in \mathbb{N}$
  - $\exists r \in \mathbb{N}$ (quantidade de bits)
  - $\exists b_{r-1}, b_{r-2}, ..., b_2, b_1, b_0 \in \{0, 1\}$ (os bits)
  - $b_{r-1} \cdot 2^{r-1} + b_{r-2} \cdot 2^{r-2} + ... + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0 = n$

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- "Todo inteiro positivo possui uma representação em binário."
- reescrevendo
  - $\forall n > 0 \in \mathbb{N}$
  - $\exists r \in \mathbb{N}$ (quantidade de bits)
  - $\exists b_{r-1}, b_{r-2}, ..., b_2, b_1, b_0 \in \{0, 1\}$ (os bits)
  - $b_{r-1} \cdot 2^{r-1} + b_{r-2} \cdot 2^{r-2} + ... + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0 = n$

b_{r-1}	b_{r-2}	...	b_2	b_1	b_0
2^{r-1}	2^{r-2}	...	2^2	2^1	2^0

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- Exemplo: $n = 11$
  - $r = 4$
  - $b_3 = 1$
  - $b_2 = 0$
  - $b_1 = 1$
  - $b_0 = 1$
  - $1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 0 + 2 + 1 = 11 = n$
1	0	1	1

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- Prova por Indução
  - Base: Para $n = 1$, tem-se $r = 1$ e $b_0 = 1$
    $b_0 \cdot 2^0 = 1 \cdot 1 = 1 = n$

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- Prova por Indução
  - Base: Para $n = 1$, tem-se $r = 1$ e $b_0 = 1$
    $b_0 \cdot 2^0 = 1 \cdot 1 = 1 = n$
  - Hipótese
    - $\forall k > 0 \in \mathbb{N}$
    - $\exists r \in \mathbb{N}$
    - $\exists b_{r-1}, ..., b_1, b_0 \in \{0, 1\}$
    - $b_{r-1} \cdot 2^{r-1} + ... + b_1 \cdot 2^1 + b_0 \cdot 2^0 = k$

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- Prova por Indução (continuação)
  - Passo
    - Seja $k+1 \in \mathbb{N}$, com $k+1 > 1$
    - Pela Hipótese,
      todos números de 1 a k têm representações em binário
    - Escolhe-se um i entre eles, da seguinte forma

$$i = \begin{cases} \frac{k}{2} & \text{, se } k+1 \text{ é ímpar} \\ \\ \frac{k+1}{2} & \text{, se } k+1 \text{ é par} \end{cases}$$

    - Como $k+1 > 1$, tem-se $1 \leq i \leq k$
      portanto, i tem uma representação em binário

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- Prova por Indução (continuação)
  - Passo (continuação)
    - Seja a representação de i em binário
      r
      $b_{r-1}, ..., b_1, b_0$
      $b_{r-1} \cdot 2^{r-1} + ... + b_1 \cdot 2^1 + b_0 \cdot 2^0 = i$
    - Cria-se uma nova representação em binário
      Seja $a \in \{0, 1\}$ definido por $a = \begin{cases} 0 & \text{, se } k+1 \text{ é par} \\ 1 & \text{, se } k+1 \text{ é ímpar} \end{cases}$
      Cria-se $2 \cdot (b_{r-1} \cdot 2^{r-1} + ... + b_1 \cdot 2^1 + b_0 \cdot 2^0) + a \cdot 2^0$
      Que fica $b_{r-1} \cdot 2^r + ... + b_1 \cdot 2^2 + b_0 \cdot 2^1 + a \cdot 2^0$
      É uma representação de $r+1$ bits para o valor $2i + a$

Prova por Indução

Exemplo 3 — Indução do Tipo 2

- Prova por Indução (continuação)
  - Passo (continuação)
    - Como
      $$i = \begin{cases} \frac{k}{2} & \text{, se } k+1 \text{ é ímpar} \\ \\ \frac{k+1}{2} & \text{, se } k+1 \text{ é par} \end{cases}$$
      $$a = \begin{cases} 0 & \text{, se } k+1 \text{ é par} \\ 1 & \text{, se } k+1 \text{ é ímpar} \end{cases}$$
    - Se $k+1$ é par, $2i + a = 2 \cdot \frac{k+1}{2} + 0 = k+1$
    - Se $k+1$ é ímpar, $2i + a = 2 \cdot \frac{k}{2} + 1 = k+1$
    - Portanto, a representação em binário
      $b_{r-1} \cdot 2^r + \ldots + b_1 \cdot 2^2 + b_0 \cdot 2^1 + a \cdot 2^0$
      representa $k+1$
      o que prova que $k+1$ tem representação em binário □

Indução Estrutural

- Objetivo
  - provar propriedades sobre conjuntos de estruturas
    - geralmente definidos indutivamente
    - são enumeráveis
- Inspiração
  - Indução Matemática
- Diferenças
  - Pode ter mais de uma Base
  - Pode ter mais de um Passo
    - conseqüentemente, pode ter mais de uma hipótese

Indução Estrutural

Exemplo

- Seja L a linguagem gerada pela gramática
  - $(\{S\}, \{1, +, -, \times, \div, (,)\}, P, S)$ onde
  - $P = \{\ S \ \rightarrow \ 1 \ \mid \ 111 \ \mid \ (S + S) \ \mid \ (S \times S - S \div S)\ \}$

Indução Estrutural

Exemplo

- Seja L a linguagem gerada pela gramática
  - $(\{S\}, \{1, +, -, \times, \div, (,)\}, P, S)$ onde
  - $P = \{\ S \ \rightarrow \ 1 \ \mid \ 111 \ \mid \ (S + S) \ \mid \ (S \times S - S \div S)\ \}$
- Exemplos de palavras da linguagem L
  - 1, 111, $(1 + 1)$, $(1 + 111)$, $(1 \times 111 - 1 \div 111)$
  - $((1 + 1) + (111 + 111))$, $(1 + ((111 \times (111 + 1) - 111 \div 1) + 1))$

Indução Estrutural

Exemplo

- Seja L a linguagem gerada pela gramática
  - $(\{S\}, \{1, +, -, \times, \div, (,)\}, P, S)$ onde
  - $P = \{\ S \ \rightarrow\ 1 \mid 111 \mid (S + S) \mid (S \times S - S \div S)\ \}$
- Exemplos de palavras da linguagem L
  - 1, 111, $(1 + 1)$, $(1 + 111)$, $(1 \times 111 - 1 \div 111)$
  - $((1 + 1) + (111 + 111))$, $(1 + ((111 \times (111 + 1) - 111 \div 1) + 1))$

- Provar
  - Todas palavras de L têm tamanho ímpar.
  - $\forall w \in L\ .\ tam(w)$ é ímpar

Indução Estrutural

Exemplo

- Prova por Indução Estrutural
  - Bases
    - $tam(1) = 1$, que é ímpar
    - $tam(111) = 3$, que é ímpar

Indução Estrutural

Exemplo

- Prova por Indução Estrutural
  - Bases
    - $tam(1) = 1$, que é ímpar
    - $tam(111) = 3$, que é ímpar
  - Hipótese
    - $\forall w \in L \; . \; tam(w)$ é ímpar
  - Passo
    - Seja $w \in L$ com $w \neq 1$ e $w \neq 111$.
    - Portanto,
      w é da forma $(w_1 + w_2)$ ou
      w é da forma $(w_1 \times w_2 - w_3 \div w_4)$
      onde $w_1, w_2, w_3, w_4 \in L$

Indução Estrutural

Exemplo

- Prova por Indução Estrutural (continuação)
  - Passo (continuação)
    - Se w é da forma $(w_1 + w_2)$, então
      $tam(w) = tam(w_1) + tam(w_2) + 3$
      Como, por hipótese, $tam(w_1)$ e $tam(w_2)$ são ímpares,
      $tam(w) = (2k_1 + 1) + (2k_2 + 1) + 3 = 2(k_1 + k_2 + 2) + 1$,
      portanto, ímpar
    - Se w é da forma $(w_1 \times w_2 - w_3 \div w_4)$, então
      $tam(w) = tam(w_1) + tam(w_2) + tam(w_3) + tam(w_4) + 5$
      Como, por hipótese, $tam(w_1)$, $tam(w_2)$, $tam(w_3)$ e $tam(w_4)$
      são ímpares,
      $tam(w) = (2k_1 + 1) + (2k_2 + 1) + (2k_3 + 1) + (2k_4 + 1) + 5 =$
      $2(k_1 + k_2 + k_3 + k_4 + 4) + 1$, portanto, ímpar $\square$

Técnicas de Demonstração
Lógica Matemática

Marnes Augusto Hoff
marnes.hoff@gmail.com
http://www.nyx.net/~mhoff

11 de Março de 2008