MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira

Instituto de computação

UNICAMP

16 de agosto de 2023

1 Prova por contrapositiva

2 Provas de equivalências

3 Perguntas, observações, comentários?

Prova por contrapositiva

Contrapositiva: visão geral

Vimos nas primeiras aulas que $p \to q$ é equivalente à $\neg q \to \neg q$.

- Se x é mamífero, então x tem pelos.
  - Ao vermos um animal que não tem pelos, já sabemos que ele não é mamífero.
- Se x é um pássaro, então x tem penas.
  - Ao vermos um animal que não tem penas, já sabemos que ele não é um pássaro.

Contrapositiva: visão geral

Vimos nas primeiras aulas que $p \rightarrow q$ é equivalente à $\neg q \rightarrow \neg q$.

- Se x é mamífero, então x tem pelos.
  - Ao vermos um animal que não tem pelos, já sabemos que ele não é mamífero.
- Se x é um pássaro, então x tem penas.
  - Ao vermos um animal que não tem penas, já sabemos que ele não é um pássaro.

Assim, para provar $p \Rightarrow q$, podemos provar $\neg q \Rightarrow \neg p$.

Prova por contrapositiva

Negamos a conclusão e tentamos demonstrar a negação da hipótese.

$$(H \Rightarrow C) \Leftrightarrow (\neg C \Rightarrow \neg H)$$

Depois de negarmos C, podemos seguir com uma prova direta (ou qualquer outra estratégia de prova).

Quando usar contrapositiva?
Às vezes é difícil extrair informação útil da hipótese. Então podemos tentar usar $\neg C$ como uma hipótese mais simples.

Primeiro exemplo: prova simples por contrapositiva

Teorema

Para todo $n \in \mathbb{Z}$, se $n^3 + 17$ é ímpar, então n é par.

Primeiro exemplo: prova simples por contrapositiva

Teorema

Para todo $n \in \mathbb{Z}$, se $n^3 + 17$ é ímpar, então n é par.

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?

Primeiro exemplo: prova simples por contrapositiva

Teorema

Para todo $n \in \mathbb{Z}$, se $n^3 + 17$ é ímpar, então n é par.

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?
- $n^3 + 17 = 2a + 1$ para algum $a \in \mathbb{Z}$.

Primeiro exemplo: prova simples por contrapositiva

Teorema

Para todo $n \in \mathbb{Z}$, se $n^3 + 17$ é ímpar, então n é par.

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?
- $n^3 + 17 = 2a + 1$ para algum $a \in \mathbb{Z}$.

O que queremos provar exatamente?

- $\exists b \in \mathbb{Z} : n = 2 \cdot b$.

Primeiro exemplo: prova simples por contrapositiva

Se tentarmos uma prova direta, temos

$$
\begin{aligned}
& n^3 + 17 = 2a + 1 \\
\Leftrightarrow\ & n^3 = 2a - 16 \\
\Leftrightarrow\ & n = \sqrt[3]{2(a-8)}
\end{aligned}
$$

Como continuar?

Primeiro exemplo: prova simples por contrapositiva

Em vez de uma prova direta, se usarmos a contrapositiva, temos

Para todo $n \in \mathbb{Z}$, se n é ímpar, então $n^3 + 17$ é par.

Primeiro exemplo: prova simples por contrapositiva

Em vez de uma prova direta, se usarmos a contrapositiva, temos

$$\text{Para todo } n \in \mathbb{Z}, \text{ se } n \text{ é ímpar, então } n^3 + 17 \text{ é par.}$$

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?

Primeiro exemplo: prova simples por contrapositiva

Em vez de uma prova direta, se usarmos a contrapositiva, temos

Para todo $n \in \mathbb{Z}$, se n é ímpar, então $n^3 + 17$ é par.

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?
- $n = 2a + 1$ para algum $a \in \mathbb{Z}$.

Primeiro exemplo: prova simples por contrapositiva

Em vez de uma prova direta, se usarmos a contrapositiva, temos

Para todo $n \in \mathbb{Z}$, se n é ímpar, então $n^3 + 17$ é par.

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?
- $n = 2a + 1$ para algum $a \in \mathbb{Z}$.

O que queremos provar exatamente?

- $\exists b \in \mathbb{Z} : n^3 + 17 = 2 \cdot b$.

Primeiro exemplo: prova simples por contrapositiva

Em vez de uma prova direta, se usarmos a contrapositiva, temos

Para todo $n \in \mathbb{Z}$, se n é ímpar, então $n^3 + 17$ é par.

Hipóteses:

- Quais são as hipóteses?
- O que podemos derivar imediatamente das hipóteses?
- $n = 2a + 1$ para algum $a \in \mathbb{Z}$.

O que queremos provar exatamente?

- $\exists b \in \mathbb{Z} : n^3 + 17 = 2 \cdot b$.

Agora podemos simplesmente substituir $n = 2a + 1$ em $n^3 + 17$ e verificar se o resultado é par.

Segundo exemplo: prova simples por contrapositiva

Teorema

Suponha $u \in \mathbb{Z}$. Se $u^2 - 6u + 7$ é par, então u é ímpar.

Segundo exemplo: prova simples por contrapositiva

Teorema

Suponha $u \in \mathbb{Z}$. Se $u^2 - 6u + 7$ é par, então u é ímpar.

Mise en place... (Hipóteses? Resultados diretos da hipótese? O que exatamente queremos provar?)

Segundo exemplo: prova simples por contrapositiva

Teorema

Suponha $u \in \mathbb{Z}$. Se $u^2 - 6u + 7$ é par, então u é ímpar.

Mise en place... (Hipóteses? Resultados diretos da hipótese? O que exatamente queremos provar?)

Parece difícil transformar $u^2 - 6u + 7 = 2a$ em $u = 2b + 1$...

Segundo exemplo: prova simples por contrapositiva

Teorema

Suponha $u \in \mathbb{Z}$. Se $u^2 - 6u + 7$ é par, então u é ímpar.

Prova por contrapositiva:

$$\text{Suponha } u \in \mathbb{Z}. \text{ Se } u \text{ é par, então } u^2 - 6u + 7 \text{ é ímpar}$$

Segundo exemplo: prova simples por contrapositiva

Teorema

Suponha $u \in \mathbb{Z}$. Se $u^2 - 6u + 7$ é par, então u é ímpar.

Prova por contrapositiva:

$$\text{Suponha } u \in \mathbb{Z}. \text{ Se } u \text{ é par, então } u^2 - 6u + 7 \text{ é ímpar}$$

Novo prato, nova *mise en place*... (Hipóteses? Resultados diretos da hipótese? O que exatamente queremos provar?)

Segundo exemplo: prova simples por contrapositiva

Teorema

Suponha $u \in \mathbb{Z}$. Se $u^2 - 6u + 7$ é par, então u é ímpar.

Prova por contrapositiva:

$$\text{Suponha } u \in \mathbb{Z}. \text{ Se } u \text{ é par, então } u^2 - 6u + 7 \text{ é ímpar}$$

Novo prato, nova *mise en place*... (Hipóteses? Resultados diretos da hipótese? O que exatamente queremos provar?)

Prova na lousa.

Terceiro exemplo: prova por contrapositiva

Prólogo: Dizemos que o resto da divisão de um inteiro n por um inteiro d é $r \in \mathbb{N}$ se existir $q \in \mathbb{Z}$ tal que

$$n = dq + r \wedge 0 \leq r < d.$$

Teorema

Seja n um inteiro cujo resto da divisão por 4 é igual a 2 ou a 3. Então, n não é um quadrado perfeito.

Terceiro exemplo: prova por contrapositiva

Prólogo: Dizemos que o resto da divisão de um inteiro n por um inteiro d é $r \in \mathbb{N}$ se existir $q \in \mathbb{Z}$ tal que

$$n = dq + r \wedge 0 \leq r < d.$$

Teorema

Seja n um inteiro cujo resto da divisão por 4 é igual a 2 ou a 3. Então, n não é um quadrado perfeito.

Prólogo: Dizemos que o resto da divisão de um inteiro n por um inteiro d é $r \in \mathbb{N}$ se existir $q \in \mathbb{Z}$ tal que

$$n = dq + r \wedge 0 \leq r < d.$$

Teorema

Seja n um inteiro cujo resto da divisão por 4 é igual a 2 ou a 3. Então, n não é um quadrado perfeito.

Mise en place...

Terceiro exemplo: prova por contrapositiva

Prólogo: Dizemos que o resto da divisão de um inteiro n por um inteiro d é $r \in \mathbb{N}$ se existir $q \in \mathbb{Z}$ tal que

$$n = dq + r \wedge 0 \leq r < d.$$

Teorema

Seja n um inteiro cujo resto da divisão por 4 é igual a 2 ou a 3. Então, n não é um quadrado perfeito.

Mise en place...

Contrapositiva

n é um quadrado perfeito $\Rightarrow$ o resto da divisão de n por 4 é 0 ou 1.

Terceiro exemplo: prova por contrapositiva

Prólogo: Dizemos que o resto da divisão de um inteiro n por um inteiro d é $r \in \mathbb{N}$ se existir $q \in \mathbb{Z}$ tal que

$$n = dq + r \wedge 0 \leq r < d.$$

Teorema

Seja n um inteiro cujo resto da divisão por 4 é igual a 2 ou a 3. Então, n não é um quadrado perfeito.

Mise en place...

Contrapositiva

n é um quadrado perfeito $\Rightarrow$ o resto da divisão de n por 4 é 0 ou 1.

Nova *mise en place*... (Hipóteses? Resultados diretos da hipótese? O que exatamente queremos provar?)

Provas de equivalências

Quando provamos $H \Rightarrow C$ dizemos que H implica C.
Ou seja, se H é verdade, então C é verdade, mas não podemos concluir nada quando H é falso.
Mas às vezes, duas proposições são equivalentes, i.e.,

$$H \Leftrightarrow C$$

Ou seja, tanto H implica C, quanto C implica H.
Por exemplo

Considere a equação $E : x^2 + bx + c = 0$, onde $b, c \in \mathbb{R}$.
E tem duas raízes reais diferentes $\Leftrightarrow b^2 - 4ac > 0$.

Como provar $H \Leftrightarrow C$

Duas possibilidades:

- Prove a "ida" e prove a "volta"
  - Duas provas separadas
  - Uma prova para $H \Rightarrow C$
  - Outra prova para $C \Rightarrow H$
  - Pode-se usar qualquer estratégia para cada prova
- Uma só prova
  - Cada passo da prova deve usar $\Leftrightarrow$ em vez de $\Rightarrow$.
  - Pode ser mais complicado.

Exemplo: prova de "se, e somente se"

Teorema

Dois inteiros a e b são ambos ímpares se, e somente se, $a \cdot b$ é ímpar.

Tentem provar.

Exemplo: prova de "se, e somente se"

Teorema

Dois inteiros a e b são ambos ímpares se, e somente se, $a \cdot b$ é ímpar.

Tentem provar.

Prova por partes:

- Provando $\Rightarrow$:
  - (a ímpar)$\wedge$(b ímpar) $\Rightarrow a \cdot b$ ímpar.
  - Prova direta.

Exemplo: prova de "se, e somente se"

Teorema

Dois inteiros a e b são ambos ímpares se, e somente se, $a \cdot b$ é ímpar.

Tentem provar.

Prova por partes:

- Provando $\Rightarrow$:
  - (a ímpar)$\wedge$(b ímpar) $\Rightarrow$ $a \cdot b$ ímpar.
  - Prova direta.
- Provando $\Leftarrow$:
  - $a \cdot b$ ímpar $\Rightarrow$ (a ímpar)$\wedge$(b ímpar).
  - Prova por contrapositiva.

Segundo exemplo de prova de equivalência

Teorema

$\forall x \in \mathbb{Z}\ (x$ é ímpar $\Leftrightarrow 5x + 8$ é ímpar$)$.

Segundo exemplo de prova de equivalência

Teorema

$\forall x \in \mathbb{Z}$ (x é ímpar $\Leftrightarrow 5x + 8$ é ímpar).

Tentem provar.

Segundo exemplo de prova de equivalência

Teorema

$\forall x \in \mathbb{Z}\ (x$ é ímpar $\Leftrightarrow 5x + 8$ é ímpar$)$.

Tentem provar.

Desta vez, é fácil fazer uma prova única usando o teorema do exemplo anterior.

Perguntas, observações, comentários?