Introdução às Técnicas de Demonstração (2)

Matemática Discreta

Prof. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

30 de julho de 2020

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Objetivos

- Apresentar as técnicas de demonstração que faltam
- Discutir aplicações com base nos conectivos
- Exemplificar as técnicas estudadas

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Outline

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Anteriormente...

- Discutimos enunciados de generalização e de existência,
- Discutimos as técnicas relacionadas a quantificadores de variáveis e as técnicas de prova de condicionais.

Esta apresentação

- discutirá técnicas e requisitos para provar enunciados com outros conectivos lógicos ($\wedge, \vee, \leftrightarrow$), e
- inclui técnicas complementares relacionadas a generalizações com condicionais.

Samy Sá (samy@ufc.br)

Sobre Enunciados de Generalização...

Um enunciado de **Generalização de Condicional**

- Todas as variáveis quantificadas universalmente, e
- O conectivo principal na fórmula quantificada é o condicional.

De forma geral, expressamos como $\forall x[P(x) \rightarrow Q(x)]$, mas isto admite muitas variações.

- $\forall x[(P(x) \wedge R(x)) \rightarrow Q(x)]$
- $\forall x \forall y[P(x, y) \rightarrow Q(x, y)]$
- $\forall x \forall y[P(x) \wedge R(y) \rightarrow Q(x, y)]$
- $\forall x \forall y[P(x) \rightarrow Q(x, y)]$
- $\forall x \forall y[P(x, y) \rightarrow Q(y, x)]$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Sobre Enunciados de Generalização...

Um enunciado de **Generalização de Condicional**

- Todas as variáveis quantificadas universalmente, e
- O conectivo principal na fórmula quantificada é o condicional.

As técnicas já estudadas

- permitem provar **TODOS** os enunciados corretos;
- dependem das definições e estrutura de $P(x)$ e $Q(x)$.

Então:

1. **Os conectivos em $P(x)$ e $Q(x)$ também são relevantes**; e
2. **Algumas situações permitem provas mais simples.**

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Condicões Compostas por Conjunção

Normalmente, p/ provar $\forall x[P(x) \rightarrow Q(x)]$,

Prova
Seja c qualquer, precisamos provar que "$P(c) \rightarrow Q(c)$"...

Se $P(x)$ é uma **conjunção** $A(x) \wedge B(x)$, teremos um enunciado da forma

$$\forall x[(A(x) \wedge B(x)) \rightarrow Q(x)]$$

Então, similarmente, para provar o enunciado...

Prova
Seja c qualquer, precisamos provar que "$(A(c) \wedge B(c)) \rightarrow Q(c)$"...

Condicões Compostas por Conjunção

Normalmente, p/ provar $\forall x[(A(x) \wedge B(x)) \rightarrow Q(x)]$,

Prova

Seja c qualquer, precisamos provar que "$(A(c) \wedge B(c)) \rightarrow Q(c)$"...

Daí,

Por PROVA DIRETA:

1. assumiríamos $A(c) \wedge B(c)$ e
2. buscaríamos concluir $Q(c)$;

Este formato é favorável, pois nos permite usar $A(c), B(c)$ como duas hipóteses independentes.

Condicões Compostas por Conjunção

Normalmente, p/ provar $\forall x[(A(x) \wedge B(x)) \rightarrow Q(x)]$,

Prova

Seja c qualquer, precisamos provar que "$(A(c) \wedge B(c)) \rightarrow Q(c)$"...

Daí,

Por CONTRAPOSIÇÃO:

1. assumiríamos $\neg Q(c)$ e
2. buscaríamos concluir $\neg(A(c) \wedge B(c))$;

Este formato é desfavorável, pois nos dá como objetivo uma **disjunção**: $\neg(A(c) \wedge B(c)) \equiv \neg A(c) \vee \neg B(c)$ (por De Morgan).

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Alguns Padrões

Em geral, num condicional:

- Conjunção à esquerda favorece a prova direta;
- Conjunção à direita favorece a contraposição *;
- Disjunção à direita favorece a contraposição;
- Disjunção à esquerda favorece a prova direta*;

* aliada à *prova por casos*.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Alguns Padrões

Um condicional à direita de outro, permite trocar o primeiro condicional por uma conjunção.

$$
\begin{aligned}
A \rightarrow (B \rightarrow C) &\equiv A \rightarrow (\neg B \vee C) \\
&\equiv \neg A \vee (\neg B \vee C) \\
&\equiv (\neg A \vee \neg B) \vee C \\
&\equiv \neg(A \wedge B) \vee C \\
&\equiv (A \wedge B) \rightarrow C
\end{aligned}
$$

* Também admite aplicações aninhadas de técnicas p/ condicionais.

Alguns Padrões

Um condicional à esquerda de outro, favorece a prova direta *.

$(A \to B) \to C \equiv (\neg A \vee B) \to C$

* aliada à *prova por casos*.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Prova por CASOS

- Utilizada se há uma **disjunção** à esquerda do condicional;
- Divide-se a prova em duas ou mais partes, de acordo com a disjunção.

Exemplo

Teorema

Prove que "Se n é um inteiro, então $n^2 \geq n$*."*

Prova

Seja c qualquer, precisamos provar que "c é inteiro $\rightarrow c^2 \geq c$*". Por prova direta, suponha que c é inteiro. (... como continuar?)*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Prova por CASOS

Exemplo

Teorema
Prove que "Se n é um inteiro, então $n^2 \geq n$."

Prova
Seja c qualquer, precisamos provar que "c é inteiro $\rightarrow c^2 \geq c$". Por prova direta, suponha que c é inteiro. (... como continuar?)

Há uma complicação, pois $\geq$ é uma inequação e uma das operações envolvidas é a exponenciação. Precisaremos saber se c é negativo, mas só sabemos que c é inteiro. **Como resolver este impasse?**

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Teorema

Prove que "Se n é um inteiro, então $n^2 \geq n$."

Prova

Seja c qualquer, precisamos provar que "c é inteiro $\rightarrow c^2 \geq c$". Por prova direta, suponha que c é inteiro. (... como continuar?)

Como resolver este impasse? Trocaremos a condição "*c* é inteiro" da suposição por outro **equivalente** que use **disjunção**:

"*c* é inteiro negativo **ou** *c* é inteiro não-negativo".

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Teorema

Prove que "Se n é um inteiro, então $n^2 \geq n$*."*

Prova

Seja c qualquer, precisamos provar que

$$\text{“(}c \text{ é inteiro negativo} \lor c \text{ é inteiro não-negativo)} \rightarrow c^2 \geq c\text{”.}$$

Por PD, suponha que "c é inteiro negativo $\lor$ *c é inteiro não-negativo".*

Deste ponto em diante, procederemos POR CASOS.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Teorema

Prove que "Se n é um inteiro, então $n^2 \geq n$*."*

Prova

... ~~Suponha que c é um inteiro.~~

Caso 1*: Suponha que c é um inteiro negativo. (...)*

Caso 2*: Suponha que c é um inteiro não-negativo. (...)*

A prova fica dividida em duas, mas com hipóteses melhores.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Teorema

Prove que "Se n é um inteiro, então $n^2 \geq n$."

Prova

... Suponha que c é um inteiro.

Caso 1*: Suponha que c é um inteiro* ***negativo****. (...)*

~~***Caso 2****: Suponha que c é um inteiro* ***não-negativo****. (...)*~~

- ***Caso 2.1****: Suponha que c é um inteiro* ***positivo****. (...)*
- ***Caso 2.2****: Suponha que c é um inteiro* ***igual a zero****. (...)*

A prova fica dividida em três, mas com hipóteses melhores.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova por Casos

Teorema

Prove que "Se n é um inteiro, então $n^2 \geq n$."

Prova

Seja c qualquer, suponha que c é inteiro.

1. *Suponha que c é negativo, ou seja, $c < 0$. Neste caso, $c.c > 0.c$* *, *ou seja, $c^2 > 0$. Como $c^2 > 0$ e $c < 0$, temos $c^2 > c$. Portanto, $c^2 \geq c$* **
2. *Suponha que c é não-negativo, ou seja, $c \geq 0$.*
   - **2.1** *Suponha que $c > 0$ (i.e., $c \geq 1$). Neste caso, $c.c \geq 1.c$, ou seja, $c^2 \geq c$.*
   - **2.2** *Suponha que $c = 0$. Neste caso, $c.c = 0.c$, ou seja, $c^2 = 0$. Isso significa $c^2 = c$. Portanto, $c^2 \geq c$* **

Como concluímos $c^2 \geq c$ em todos os casos, vale para todo c inteiro. ■

* Se multiplicarmos cada lado de $x < y$ por $z < 0$, obteremos $xz > yz$: a multiplicação por um número negativo *inverte* a inequação. ** Para todo x, temos $x \geq y$ se e somente se $x > y$ ou $x = y$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova de Equivalência

Prova de EQUIVALÊNCIA

- Utilizada quando o conectivo principal é o $\leftrightarrow$;
- Divide-se a prova em duas partes: $\rightarrow$ e $\leftarrow$.

Exemplo

Teorema

Prove que "Se n é inteiro, então n é ímpar ***se e somente se*** *n^2 é ímpar".*

$$\forall n[Impar(n) \leftrightarrow Impar(n^2)]$$

Prova

Seja c qualquer, precisamos provar que $Impar(c) \leftrightarrow Impar(c^2)$.

($\Rightarrow$) *Prova-se que $Impar(c) \rightarrow Impar(c^2)$; e que*

($\Leftarrow$) *Prova-se que $Impar(c^2) \rightarrow Impar(c)$.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Técnicas Complementares p/ $\forall x[P(x) \rightarrow Q(x)]$

Prova EXAUSTIVA

- Possível apenas para domínio **finito**;
- Demonstra-se a propriedade para cada elemento do domínio, **um por vez**.

Exemplo

Teorema

Prove que "se n é um inteiro positivo com $n \leq 4$, então $(n+1)^3 \geq 3^n$".

Prova

Como o domínio é finito, utilizaremos uma prova exaustiva. Ou seja, verificaremos que a propriedade $(n+1)^3 \geq 3^n$ vale para $n = 1, 2, 3$ e 4. (CONTINUA...)

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Técnicas Complementares p/ $\forall x[P(x) \rightarrow Q(x)]$

Prova EXAUSTIVA

Exemplo

Teorema

Prove que "se n é um inteiro positivo com $n \leq 4$, então $(n+1)^3 \geq 3^n$".

Prova

Como o domínio é finito, utilizaremos uma prova exaustiva. Ou seja, verificaremos que a propriedade $(n+1)^3 \geq 3^n$ vale para $n = 1, 2, 3$ e 4.

- *Para $n = 1$, teremos $(1+1)^3 \geq 3^1$, o que resulta em $8 \geq 3$;*
- *Para $n = 2$, teremos $(2+1)^3 \geq 3^2$, o que resulta em $27 \geq 9$;*
- *Para $n = 3$, teremos $(3+1)^3 \geq 3^3$, o que resulta em $64 \geq 27$;*
- *Para $n = 4$, teremos $(4+1)^3 \geq 3^4$, o que resulta em $125 \geq 81$.* ■

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Técnicas Complementares p/ $\forall x[P(x) \to Q(x)]$

Prova EXAUSTIVA

- Possível apenas para domínio **finito**;
- Demonstra-se a propriedade para cada elemento do domínio, **um por vez**.

Observações

- Pode ser útil, mas só se o domínio for pequeno.
- Pode ser usada mesmo que não haja condicional.
- É um caso particular extremo da *Prova por Casos* (apresentada mais à frente).

Técnicas Complementares p/ $\forall x[P(x) \to Q(x)]$

Prova por VACUIDADE

- Utilizada quando $P(x)$ é *necessariamente* falsa;
- Demonstra-se $\forall x \neg P(x)$, então conclui-se $\forall x[P(x) \to Q(x)]$.

Exemplo

Teorema
Prove que "Todo elemento do conjunto vazio é um número natural".

Este enunciado é uma Generalização de Condicional.

$$\forall x[x \in \emptyset \to x \in \mathbb{N}]$$

Técnicas Complementares p/ $\forall x[P(x) \to Q(x)]$

Prova por VACUIDADE

Exemplo

Teorema
Prove que "Todo elemento do conjunto vazio é um número natural".

$$\forall x[x \in \emptyset \to x \in \mathbb{N}]$$

Este enunciado é uma Generalização de Condicional. Seguindo os métodos anteriores, aplicaríamos a Prova de Generalização.

Prova
*Seja c qualquer, precisamos provar que $c \in \emptyset \to c \in \mathbb{N}$. Observe que $c \in \emptyset$ **é falso**, pois o conjunto é vazio! Por **vacuidade**, $c \in \emptyset \to x \in \mathbb{N}$ é verdadeiro.*

Técnicas Complementares p/ $\forall x[P(x) \rightarrow Q(x)]$

Prova por VACUIDADE

- Utilizada quando $P(x)$ é *necessariamente* falsa;
- Demonstra-se $\forall x \neg P(x)$, então conclui-se $\forall x[P(x) \rightarrow Q(x)]$.

Observações

- Usada normalmente como atalho quando **percebe-se** que $\forall x \neg P(x)$ num condicional do tipo $\forall x[P(x) \rightarrow Q(x)]$.
- Pode ser muito útil em algumas situações de *prova por casos*.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Técnicas Complementares p/ $\forall x[P(x) \rightarrow Q(x)]$

Prova TRIVIAL

- Utilizada quando $Q(x)$ é *necessariamente* verdadeira;
- Demonstra-se $\forall x Q(x)$, então conclui-se $\forall x[P(x) \rightarrow Q(x)]$.

Exemplo

Teorema

Prove que "Todo número primo é par ou ímpar".

Este enunciado é uma Generalização de Condicional.

$$\forall x[Primo(x) \rightarrow (Par(x) \vee Impar(x))]$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Técnicas Complementares p/ $\forall x[P(x) \to Q(x)]$

Prova TRIVIAL

Exemplo

Teorema

Prove que "Todo número primo é par ou ímpar".

$$\forall x[Primo(x) \to (Par(x) \vee Impar(x))]$$

Este enunciado é uma Generalização de Condicional. Seguindo os métodos anteriores, aplicaríamos a Prova de Generalização.

Prova

Seja c qualquer, precisamos provar que $Primo(c) \to Par(c) \vee Impar(c)$. *Observe que* $Par(c) \vee Impar(c)$ ***é verdadeiro*** *para todo c inteiro, o que é requerido de todo número primo. Logo,* $Primo(c) \to Par(c) \vee Impar(c)$ *é (trivialmente) verdadeiro.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Técnicas Complementares p/ $\forall x[P(x) \rightarrow Q(x)]$

Prova TRIVIAL

- Utilizada quando $Q(x)$ é *necessariamente* verdadeira;
- Demonstra-se $\forall x Q(x)$, então conclui-se $\forall x[P(x) \rightarrow Q(x)]$.

Observações

- Usada normalmente como atalho quando **percebe-se** que $\forall x Q(x)$ num condicional do tipo $\forall x[P(x) \rightarrow Q(x)]$.
- Pode ser muito útil em algumas situações de *prova por casos*.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova de Unicidade

Prova de UNICIDADE

- Utilizada para enunciados do tipo "existe um único";
- Tem duas partes: um existencial e uma generalização.

Exemplo

Teorema
"Existe um único primo par."

$$\exists n((Primo(n) \land Par(n)) \land \forall m((Primo(m) \land m \neq n) \rightarrow \neg Par(m)))$$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova de Unicidade

Prova de UNICIDADE

- Utilizada para enunciados do tipo "existe um único";
- Tem duas partes: um existencial e uma generalização.

Exemplo

Teorema
*"**Existe um** único **primo par.**"*
$\exists n((Primo(n) \wedge Par(n)) \wedge \forall m((Primo(m) \wedge m \neq n) \rightarrow \neg Par(m)))$

Note semelhanças:

Teorema
*"**Existe um primo par.**"*
$\exists n((Primo(n) \wedge Par(n)))$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova de Unicidade

Prova de UNICIDADE

- Utilizada para enunciados do tipo "existe um único";
- Tem duas partes: um existencial e uma generalização.

Exemplo

Teorema
*"Existe um **único** primo par."*
$\exists n((Primo(n) \wedge Par(n)) \wedge \forall m((Primo(m) \wedge m \neq n) \rightarrow \neg Par(m)))$

Note semelhanças:

Teorema
*"**Existe um primo par.**"*
$\exists n((Primo(n) \wedge Par(n)))$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Prova de Unicidade

Prova de UNICIDADE

- Utilizada para enunciados do tipo "existe um único";
- Tem duas partes: um existencial e uma generalização.

Exemplo

Teorema
"Existe um único primo par."
$\exists n((Primo(n) \wedge Par(n)) \wedge \forall m((Primo(m) \wedge m \neq n) \rightarrow \neg Par(m)))$

Prova

1. *Prova-se que* $\exists n[Primo(n) \wedge Par(n)]$*; e que*
2. *Prova-se que* $\forall m[(Primo(m) \wedge m \neq n) \rightarrow \neg Par(m)]$.