Introdução às Técnicas de Demonstração

Matemática Discreta

Prof. MSc. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

24 de julho de 2020

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

Objetivos

- Estabelecer onde havíamos parado a disciplina
- (Re)Introduzir os principais métodos prova
- Exemplificamos as técnicas estudadas

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

Outline

Anteriormente...

- Discutimos a terminologia de teoremas e demonstrações
- Diferenciamos provas formais e informais
- Discutimos algumas técnicas de demonstração e as exemplificamos

O propósito desta apresentação é destacar o que já foi visto e repassar os tópicos que devem precisar de maior atenção.

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

Anteriormente...

Cada técnica de demonstração, individualmente,

1. serve para demonstrar apenas alguns tipos de enunciados.
2. nos permite levantar uma ou mais hipóteses.
3. nos fornece um novo objetivo a ser demonstrado, sempre mais simples que o original.
4. deixa em aberto o caminho entre as novas hipóteses e novo objetivo.

Combinadas,

5. podem ser encadeadas, uma como parte da outra.
6. nos permitem demonstrar todo tipo de teorema.

Anteriormente...

As técnicas de demonstração, combinadas,

5. podem ser encadeadas, uma como parte da outra.
6. nos permitem demonstrar todo tipo de teorema.

Chamaremos as provas de passos intermediários de **sub-provas**.

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

Anteriormente...

Cada técnica de demonstração, individualmente,

1. serve para demonstrar apenas alguns tipos de enunciados.
2. nos permite levantar uma ou mais hipóteses.
3. nos fornece um novo objetivo a ser demonstrado.
4. deixa em aberto o caminho entre as novas hipóteses e novo objetivo.

Cada aplicação de uma técnica terá o seu próprio **escopo**.

- começa quando levantamos hipóteses criadas pela técnica;
- termina quando concluímos a prova do objetivo que ela criou.

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

Portanto...

Demonstrar um teorema (geralmente) envolve

1. analisar a estrutura da sua proposição,
2. identificar técnicas adequadas para provar a afirmação e escolher uma,
3. levantar **hipóteses** de acordo com a técnica escolhida,
4. * provar uma nova proposição (objetivo), criada pela técnica,
5. concluir que a proposição-**objetivo** segue das hipóteses.

O Item 1 é questão de interpretação de textos. Há algumas formas comuns como afirmações tendem a ser escritas em matemática que auxiliam nesta análise.

Portanto...

Demonstrar um teorema (geralmente) envolve

1. analisar a estrutura da sua proposição,
2. identificar técnicas adequadas para provar a afirmação e escolher uma,
3. levantar **hipóteses** de acordo com a técnica escolhida,
4. * provar uma nova proposição (objetivo), criada pela técnica,
5. concluir que a proposição-**objetivo** segue das hipóteses.

Os Items 3 a 5 serão a prova do teorema, da proposição original.

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

Portanto...

Demonstrar um teorema (geralmente) envolve

1. analisar a estrutura da sua proposição,
2. identificar técnicas adequadas para provar a afirmação e escolher uma,
3. levantar **hipóteses** de acordo com a técnica escolhida,
4. * provar uma nova proposição (objetivo), criada pela técnica,
5. concluir que a proposição-**objetivo** segue das hipóteses.

O * no Item 4 aponta uma abertura na prova. Esta parte é contextual, dependente do assunto do teorema. É nosso trabalho completá-la, re-aplicando o roteiro acima recursivamente.

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Universais (ou Generalizações)
- Existenciais

Algumas técnicas são orientadas ao tipo de enunciado:

- Prova de Generalização, Prova Existencial, Prova por Contra-Exemplo, Prova de Unicidade.

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

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Universais (ou Generalizações)

$$\forall x(P(x) \to Q(x))$$

"Todos os elementos do domínio que satisfazem à propriedade $P(x)$ devem satisfazer também à propriedade $Q(x)$."

- É o formato mais comum que teoremas assumem.
- Sempre condicionais, não admitem exceções.

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

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Universais (ou Generalizações)

$$\forall x(Par(x) \rightarrow QuadradoPar(x))$$

Variações

- "Para todo número, se este é par, então seu quadrado é par."
- "Para todo número par, seu quadrado é par."
- "Se um número é par, seu quadrado é par."
- "Para qualquer número par, seu quadrado é par."
- "Dado um número par, seu quadrado será par."
- "O quadrado de um inteiro par é par."

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

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Universais (ou Generalizações)

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

Variações

- "Para todo número, se este é par, então seu quadrado é par."
- "Para todo número par, seu quadrado é par."
- "Se um número é par, seu quadrado é par."
- "Para qualquer número par, seu quadrado é par."
- "Dado um número par, seu quadrado será par."
- "O quadrado de um inteiro par é par."

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

Enunciados de Generalização

Como interpretar?

- “O quadrado de um inteiro par é par.”

Procure os seguintes elementos:

1. Sempre há um condicional ($\rightarrow$) ou um bicondicional ($\leftrightarrow$)
2. O restante do texto é composto por afirmações menores.
    - Que partes do enunciado caracterizam objetos?
    - Que tipos de objetos são esses?
3. Algumas afirmações são **condições** (à priori) e outros são **conclusões** (à posteriori).

Obs.: É possível ter outros elementos no texto, mas estes da lista acima sempre existirão.

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

Enunciados de Generalização

Como interpretar?

- “O quadrado de um inteiro par é par.”

Procure os seguintes elementos:

1. Sempre há um condicional ($\rightarrow$) ou um bicondicional ($\leftrightarrow$)
   - Se não estiver explícito, assuma que é um condicional simples. Quando tiver os outros elementos da lista, re-avalie este item.

R.: $\rightarrow$

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

Enunciados de Generalização

Como interpretar?

- “O quadrado de um inteiro par é par.”

Procure os seguintes elementos:

1. O restante do texto é composto por afirmações menores.
   - Que partes do enunciado caracterizam objetos?
   - Que tipos de objetos são esses?

R.: “um inteiro par”, “o quadrado de(sse) um inteiro é par”.

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

Enunciados de Generalização

Como interpretar?

- "O quadrado de um inteiro par é par."

Procure os seguintes elementos:

1. Algumas afirmações são **condições** (à priori) e outros são **conclusões** (à posteriori).

Obs.: Neste enunciado, a descrição "um inteiro par" condiciona a descrição "o quadrado de(sse) um inteiro é par". Então temos que **SE** "um inteiro é par", **ENTÃO** "o quadrado desse inteiro é par".

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Existenciais

$$\exists x P(x)$$

"Alguns elementos do domínio satisfazem à propriedade $P(x)$."

- A propriedade $P(x)$ pode ser também uma fórmula com conectivos.
- O conectivo mais comum é a conjunção.
- Admitem exceções.

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

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Existenciais

$$\exists x(Primo(x) \land Par(x))$$

Variações

- "Existe um número primo par."
- "Algum número primo é par"
- "Existe um número que é primo e par"
- "Ao menos um número é simultaneamente primo e par."
- "Há números que são primos e pares"
- "Alguns números que são primos são pares"

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

Tipos de Enunciados de Teoremas

Há principalmente dois tipos de enunciados:

- Existenciais

$$\exists x(x \text{ é primo} \wedge x \text{ é par})$$

Variações

- "Existe um número primo par."
- "Algum número primo é par"
- "Existe um número que é primo e par"
- "Ao menos um número é simultaneamente primo e par."
- "Há números que são primos e pares"
- "Alguns números que são primos são pares"

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

Enunciados Existenciais

Como interpretar?

- “Algum número primo é par.”

Procure os mesmos elementos de antes.

1. Identifique partes do enunciado que descrevam objetos e que tipos de objetos são.
2. Quais deles são condições? Normalmente indicarão o domínio.

Obs.: Neste enunciado, a descrição “um inteiro par” condiciona a descrição “o quadrado de(sse) um inteiro é par”. Então temos que **SE** “um inteiro é par”, **ENTÃO** “o quadrado desse inteiro é par”.

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

Enunciados Existenciais

Como interpretar?

- "O quadrado de um inteiro par é par."

Procure os seguintes elementos:

1. Quantificadores para cada variável.
   - Se o condicional do enunciado tiver exceções, ele se tornará verdadeiro ou falso? Caso permaneça verdadeiro, o enunciado é existencial; caso falso, é universal.

R.: Se houver exceção entre a relação de condição e consequência estabelecida, a afirmação será falsa. Há penas uma variável, quantificada universalmente.

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

Enunciados Existenciais

Como interpretar?

- “Algum número primo é par.”

Procure os seguintes elementos:

1. Quantificadores para cada variável.
   - Se o condicional do enunciado tiver exceções, ele se tornará verdadeiro ou falso? Caso permaneça verdadeiro, o enunciado é existencial; caso falso, é universal.

R.: A palavra “algum” indica que basta um elemento do domínio satisfazer às propriedades. Isso significa que o enunciado admite exceções. A única variável existente é existencial.

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

Eu acho que o enunciado é falso ou verdadeiro?

- Universal, Verdadeiro: **Prova de Generalizações**
- Universal, Falso: **Prova por Contra-Exemplo**
- Existencial, Verdadeiro: **Prova Existencial**
  - Construtiva ou
  - Não-Construtiva
- Existencial, Falso: **Prova de Generalizações**

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

Eu acho que o enunciado é falso ou verdadeiro?

- Existencial, Falso: **Prova de Generalizações**

Ex.: "Existe um número par cujo quadrado é ímpar."

$$\exists x(x \text{ é par} \land x^2 \text{ é ímpar})$$

Parece falso, não é mesmo?

Vamos negar esta frase...
Não existe nenhum número par cujo quadrado seja ímpar.

$$\neg\exists x(x \text{ é par} \land x^2 \text{ é ímpar})$$

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

Eu acho que o enunciado é falso ou verdadeiro?

- Existencial, Falso: **Prova de Generalizações**

Ex.: "Existe um número par cujo quadrado é ímpar."

$$\exists x(x \text{ é par} \wedge x^2 \text{ é ímpar})$$

Parece falso, não é mesmo?

Vamos negar esta frase... E reescrevê-la:
Para todo número par, seu quadrado não é ímpar.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

Eu acho que o enunciado é falso ou verdadeiro?

Desenvolvimento completo a partir da negação:

Ex.: “Não existe nenhum número par cujo quadrado é ímpar.”

$$\begin{aligned}
&\neg\exists x(x \text{ é par} \wedge x^2 \text{ é ímpar})\\
&\equiv \forall x \neg(x \text{ é par} \wedge x^2 \text{ é ímpar})\\
&\equiv \forall x(\neg x \text{ é par} \vee \neg x^2 \text{ é ímpar})\\
&\equiv \forall x(x \text{ é par} \rightarrow \neg x^2 \text{ é ímpar})\\
&\equiv \forall x(x \text{ é par} \rightarrow x^2 \text{ é par})
\end{aligned}$$

Equiv.: “Para todo número par, seu quadrado é par.”

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

Prova de Generalizações

Por exemplo, no enunciado (decodificado anteriormente)

- "O quadrado de um inteiro par é par."

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

temos o quantificador universal.

Portanto, para demonstrar que o enunciado é verdadeiro, precisaremos da **Prova de Generalizações**.

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

Prova de Generalizações

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow$ c^2 é par"
   - Este item é deixado em aberto pela generalização
   - Demanda a aplicação de outra técnica
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Prova de Existenciais

Por exemplo, no enunciado (decodificado anteriormente)

- "Algum número primo é par."

$$\exists x(x \text{ é primo} \wedge x \text{ é par})$$

temos o quantificador existencial.

Portanto, para demonstrar que o enunciado é verdadeiro, precisaremos da **Prova Existencial**.

Prova de Existenciais

Teo. Demonstre que algum número primo é par.

$$\exists x(x \text{ é primo} \wedge x \text{ é par})$$

1. (**Construtiva**) O número 2 é primo e é par.

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

Prova de Existenciais

Teo. Demonstre que algum número primo é par.

$$\exists x(x \text{ é primo} \land x \text{ é par})$$

1. (**Não Construtiva**)
    - Por contradição, suponha que não existe nenhum número primo par. Isso significaria que todos os números primos são ímpares.
    - Considere agora um número par como, por exemplo, o número 42.
    - Pela nossa suposição, 42 não é primo, ou seja, 42 é composto (um produto de números primos).
    - Como todos os primos são ímpares, temos um produto de números ímpares que resulta em um número par (Absurdo!).
    - Logo, deve existir ao menos um número primo par.

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

Tipos de Enunciados

Estas técnicas são as únicas associadas a quantificadores.

- Prova de Generalizações
- Prova de Existenciais
- Prova por Contra-Exemplo

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

Prova de Condicionais

Vimos que

- O formato mais comum é o de generalização $\forall x P(x) \rightarrow Q(x)$.
- Sempre há um condicional numa generalização.

Conclusão: Será comum precisarmos provar condicionais.

Técnicas:

1. Prova Direta
2. Prova por Contraposição
3. Prova por Contradição (ou Redução ao Absurdo)

Samy Sá (samy@ufc.br)

Prova de Condicionais

Por exemplo, o enunciado (decodificado anteriormente)

- "O quadrado de um inteiro par é par."

$$\forall x(Par(x) \rightarrow Par(x^2))$$

tem um conectivo condicional.

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

Prova de Generalizações (*)

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow$ c^2 é par"
   - Este item é deixado em aberto pela generalização
   - Demanda a aplicação de outra técnica
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Prova Direta

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow c^2$ é par"
   - **2.1** Por PROVA DIRETA, suponha que c é par.
   - **2.2** Então existe $k \in \mathbb{Z}$ tal que $c = 2k$ (definição).
   - **2.3** Logo, $c^2 = 4k^2 = 2.(2k^2)$, um número par.
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Comparação entre as Técnicas

Para provar $P(c) \rightarrow Q(c)$:

- Prova Direta:
  - **SUPONHA** $P(c)$, **ALCANCE/CONCLUA** $Q(c)$.

- Prova por Contraposição:
  - **SUPONHA** $\neg Q(c)$, **ALCANCE/CONCLUA** $\neg P(c)$.

- Prova Contradição (ou Redução ao Absurdo, R.A.A.):
  - **SUPONHA** $P(c) \wedge \neg Q(c)$, **ALCANCE/CONCLUA** $\perp$.

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

Prova por Contraposição

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x (x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow$ c^2 é par"
   - **2.1** Por CONTRAPOSIÇÃO, suponha que c^2 é ímpar.
   - **2.2** Por ser ímpar, c^2 não é divisível por 2 (deixaria resto 1). Isso significa que a fatoração de c^2 só tem números ímpares.
   - **2.3** Além disso, os fatores de c precisam estar entre os fatores de c^2. Isso nos diz que c só tem fatores ímpares.
   - **2.4** Logo, c é ímpar.
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Prova por Contradição

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow c^2$ é par"
   - **2.1** Por CONTRADIÇÃO, suponha que c é par, mas c^2 é ímpar.
   - **2.2** Então existem $k \in \mathbb{Z}$ tal que $c = 2k$ (definição de par) e $j \in \mathbb{Z}$ tal que $c^2 = 2j + 1$ (definição de ímpar).
   - **2.3** Temos que, $c^2 = c.c = 2k.2k = 4k^2$. Logo, $4k^2 = 2j + 1$.
   - **2.4** Isolando j, encontraremos que $j = \frac{4k^2-1}{2}$, que não é inteiro.
   - **2.5** Absurdo, pois j deveria ser inteiro.
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

Prova por Contradição

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow c^2$ é par"
   - **2.1** Por CONTRADIÇÃO, suponha que c é par, mas c^2 é ímpar.
   - **2.2** Então existem $k \in \mathbb{Z}$ tal que $c = 2k$ (definição de par) e $j \in \mathbb{Z}$ tal que $c^2 = 2j + 1$ (definição de ímpar).
   - **2.3** Temos que, $c^2 = c.c = 2k.2k = 4k^2$. Logo, $4k^2 = 2j + 1$.
   - **2.4** Isolando j, encontraremos que $j = \frac{4k^2-1}{2}$, que **não é inteiro**.
   - **2.5** Absurdo, pois j deveria ser inteiro.
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Prova por Contradição

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \rightarrow x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\rightarrow c^2$ é par"
   - **2.1** Por CONTRADIÇÃO, suponha que c é par, mas c^2 é ímpar.
   - **2.2** Então existem $k \in \mathbb{Z}$ tal que $c = 2k$ (definição de par) e $j \in \mathbb{Z}$ tal que $c^2 = 2j + 1$ (definição de ímpar).
   - **2.3** Temos que, $c^2 = c.c = 2k.2k = 4k^2$, que é par.
   - **2.4** Absurdo, pois assumimos que c^2 seria ímpar.
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Prova por Contradição

Teo. Demonstre que o quadrado de um inteiro par é par.

$$\forall x(x \text{ é par} \to x^2 \text{ é par})$$

1. (**Instanciação**) Seja c um inteiro qualquer.
2. (**Desenvolvimento**) Provaremos que: "c é par $\to$ c^2 é par"
   - **2.1** Por CONTRADIÇÃO, suponha que c é par, mas c^2 **é ímpar**.
   - **2.2** Então existem $k \in \mathbb{Z}$ tal que $c = 2k$ (definição de par) e $j \in \mathbb{Z}$ tal que $c^2 = 2j + 1$ (definição de ímpar).
   - **2.3** Temos que, $c^2 = c.c = 2k.2k = 4k^2$, que **é par**.
   - **2.4** Absurdo, pois assumimos que c^2 seria ímpar.
3. (**Generalização**) Como provamos a propriedade para um inteiro qualquer, a propriedade vale para todos os inteiros.

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

Prova de Condicionais

Estas técnicas são as mais comumente usadas para condicionais.

- Prova Direta
- Prova por Contraposição
- Prova por Contradição