INE5403

FUNDAMENTOS DE MATEMÁTICA DISCRETA PARA A COMPUTAÇÃO

PROF. DANIEL S. FREITAS

UFSC - CTC - INE

1 - Lógica e Métodos de Prova

PROVA DE TEOREMAS

- Questões importantes na matemática:
  - quando um argumento matemático está correto?
  - métodos para construir argumentos matemáticos?

- **Teorema**: conjectura que se pode mostrar que é V.
  - “Proposições”, “fatos” ou “resultados”.

- **Prova**: seqüência de declarações (argumento) que mostra que um teorema é **V**

PROVA DE TEOREMAS & CC

- Métodos de prova também servem diretamente em CC:
  - correção de programas
  - segurança de sistemas operacional é seguro
  - inferências para IA
  - consistência das especificações de um sistema
  - correção de protocolos (de rede, de segurança)
  - prova de resultados teóricos em CC
  - (...)

PROVA DE TEOREMAS

- Objetivo da **Prova** ou **Demonstração**:
  - estabelecer a verdade de um teorema
- Construção de provas:
  - obter novas declarações a partir das já conhecidas

TEOREMAS NA LÓGICA PROPOSICIONAL

- Teoremas = tautologias
- Teorema mais comum: $p \longrightarrow q$
  - p e q são proposições compostas
  - p é a hipótese
  - q é a conclusão

TEOREMAS NA LÓGICA PROPOSICIONAL

- Técnicas usuais de prova:
  - tabelas-verdade:
    - inviáveis para muitas variáveis
  - dedução formal:
    - $p \longrightarrow q$ só será teorema se for tautologia
      - (sempre que p for V, q também deverá ser)
    - é possível deduzir q a partir de p

PROVAS

- Declarações em uma prova podem incluir:
  - hipóteses do teorema a ser provado
  - axiomas (ou postulados):
    - outras proposições que assume-se que são V
    - tautologias
    - “verdades evidentes”
  - teoremas já provados previamente
  - proposições derivadas através de regras de inferência

REGRAS DE INFERÊNCIA

- Regras de inferência:
  - “extraem conclusões” de afirmações prévias
  - “amarram” os passos de uma prova
- Justificam os passos usados para mostrar:
  - conclusão segue logicamente de hipóteses

- Regra fundamental: Modus Ponens

$$\begin{array}{ll} & p \\ & p \rightarrow q \\ \hline \therefore & q \end{array}$$

  - "se tanto uma implicação quanto sua hipótese são V, a conclusão desta implicação é V"
  - baseada na tautologia: $(p \wedge (p \rightarrow q)) \rightarrow q$

- **Exemplo:** Suponha que sejam verdadeiras:

  a implicação: “Se fizer sol hoje, eu irei à praia.”

  e a hipótese: “Hoje o dia está ensolarado.”

  - Então, por modus ponens, segue que é V a conclusão da implicação:

    “Eu irei à praia.” □

- **Exemplo:** Assuma que é V a implicação:

  "Se $n > 3$, então $n^2 > 9$".

  - Agora assuma que sabemos que n é maior que 3
  - Então, por modus ponens, segue que:

    "n^2 é maior do que 9." $\square$

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

- Outras regras de inferência:
  - tabela a seguir ($\Rightarrow$)
  - todas podem ser verificadas com tabelas-verdade

Regra	Tautologia	Nome
$\begin{array}{r} p \\ \hline \therefore\ p \lor q \end{array}$	$p \longrightarrow (p \lor q)$	**Adição**
$\begin{array}{l} p \land q \\ \hline \therefore\ p \end{array}$	$(p \land q) \longrightarrow p$	**Simplificação**
$\begin{array}{l} p \\ q \\ \hline \therefore\ p \land q \end{array}$	$((p) \land (q)) \longrightarrow (p \land q)$	**Conjunção**
$\begin{array}{l} p \\ p \longrightarrow q \\ \hline \therefore\ q \end{array}$	$[p \land (p \longrightarrow q)] \longrightarrow q$	**Modus Ponens**
$\begin{array}{l} \neg q \\ p \longrightarrow q \\ \hline \therefore\ \neg p \end{array}$	$[\neg q \land (p \longrightarrow q)] \longrightarrow \neg p$	**Modus Tollens**
$\begin{array}{l} p \longrightarrow q \\ q \longrightarrow r \\ \hline \therefore\ p \longrightarrow r \end{array}$	$[(p \longrightarrow q) \land (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$	**Silogismo hipotético**
$\begin{array}{l} p \lor q \\ \neg p \\ \hline \therefore\ q \end{array}$	$[(p \lor q) \land \neg p] \longrightarrow q$	**Silogismo disjuntivo**
$\begin{array}{l} p \lor q \\ \neg p \lor r \\ \hline \therefore\ q \lor r \end{array}$	$[(p \lor q) \land (\neg p \lor r)] \longrightarrow (q \lor r)$	**Resolução**

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

- **Exemplo 1(/3):** Determine qual regra de inferência é base para o argumento: "Está nublado agora. Portanto, ou está nublado ou está chovendo agora."
  - Sejam as proposições:

    p: "Está nublado agora."

    q: "Está chovendo agora."
  - Então este argumento tem a forma:

$$\begin{array}{rl} & p \\ \hline \therefore & p \vee q \end{array}$$

    - ou seja, usa a regra da adição. $\square$

- **Exemplo 2(/3):** "Está nublado e chovendo agora. Portanto, está nublado agora."
  - Proposições:

    p: "Está nublado agora."

    q: "Está chovendo agora."

  - Este argumento tem a forma:

$$\begin{array}{rl} & p \wedge q \\ \hline \therefore & p \end{array}$$

  - ou seja, usa a regra da simplificação. $\square$

Inferências na Lógica Proposicional

- **Exemplo 3(/3):** “Se chover hoje, então hoje nós não teremos churrasco. Se não tivermos churrasco hoje, então teremos churrasco amanhã. Portanto, se chover hoje, teremos churrasco amanhã.”

  p: “Vai chover hoje.”

  q: “Não teremos churrasco hoje.”

  r: “Teremos churrasco amanhã.”

  - Forma do argumento:

$$\begin{array}{rl} & p \longrightarrow q \\ & q \longrightarrow r \\ \hline \therefore & p \longrightarrow r \end{array}$$

  - ou seja, é um silogismo hipotético. $\square$

Argumentos válidos

- Um argumento tem forma válida se:
  - sempre que hipóteses são V, conclusão também é V
- Mostrar que q segue das hipóteses $p_1, p_2, \ldots, p_n$:
  - mesmo que mostrar que é V a implicação:

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \quad \longrightarrow \quad q$$

- Várias regras de inferência podem ser necessárias
  - argumento deve ser mostrado passo a passo
  - razão para cada passo deve ficar explícita.

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (1/9):** Mostre que as hipóteses "Não está fazendo sol esta tarde e está mais frio do que ontem", "Nós iremos nadar somente se fizer sol", "Se nós não formos nadar, então nós vamos velejar", e "Se nós formos velejar, então estaremos em casa no final da tarde." levam à conclusão: "Estaremos em casa no final da tarde."

p: "Está fazendo sol esta tarde."

q: "Está mais frio do que ontem."

r: "Nós iremos nadar."

s: "Nós iremos velejar."

t: "Estaremos em casa no final da tarde."

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (2/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

  - Uma demonstração de que as hipóteses levam à conclusão:

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (3/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação

- **Exemplo 1 (4/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \longrightarrow p$	Hipótese

Argumentos válidos

- **Exemplo 1 (5/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \longrightarrow p$	Hipótese
4. $\neg r$	2, 3, Modus Tollens

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (6/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \longrightarrow p$	Hipótese
4. $\neg r$	2, 3, Modus Tollens
5. $\neg r \longrightarrow s$	Hipótese

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (7/9):**

Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \longrightarrow p$	Hipótese
4. $\neg r$	2, 3, Modus Tollens
5. $\neg r \longrightarrow s$	Hipótese
6. s	4, 5, Modus Ponens

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (8/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \longrightarrow p$	Hipótese
4. $\neg r$	2, 3, Modus Tollens
5. $\neg r \longrightarrow s$	Hipótese
6. s	4, 5, Modus Ponens
7. $s \longrightarrow t$	Hipótese

ARGUMENTOS VÁLIDOS

- **Exemplo 1 (9/9):**

  Hipóteses: $\neg p \wedge q, \quad r \longrightarrow p, \quad \neg r \longrightarrow s, \quad s \longrightarrow t$

  Conclusão: t

Passo	**Justificativa**
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \longrightarrow p$	Hipótese
4. $\neg r$	2, 3, Modus Tollens
5. $\neg r \longrightarrow s$	Hipótese
6. s	4, 5, Modus Ponens
7. $s \longrightarrow t$	Hipótese
8. t	6, 7, Modus Ponens $\square$

Argumentos válidos

- **Exemplo 2 (1/7):** Mostre que as hipóteses "Se você me enviar um email, eu termino de escrever o programa", "Se você não me enviar um email, então eu vou dormir cedo", e "Se eu for dormir cedo, então eu vou acordar revigorado." levam à conclusão: "Se eu não terminar de escrever o programa, vou acordar revigorado."

  p: "Você me envia um email."

  q: "Eu termino de escrever o programa."

  r: "Eu vou dormir cedo."

  s: "Eu vou acordar revigorado."

Hipóteses: $p \longrightarrow q$, $\neg p \longrightarrow r$ e $r \longrightarrow s$.

Conclusão desejada: $\neg q \longrightarrow s$ $(\Rightarrow)$

ARGUMENTOS VÁLIDOS

- **Exemplo 2 (2/7):**

  Hipóteses: $p \longrightarrow q, \quad \neg p \longrightarrow r, \quad r \longrightarrow s$

  Conclusão: $\neg q \longrightarrow s$

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese

- **Exemplo 2 (3/7):**

  Hipóteses: $p \longrightarrow q, \quad \neg p \longrightarrow r, \quad r \longrightarrow s$

  Conclusão: $\neg q \longrightarrow s$

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $\neg q \longrightarrow \neg p$	1, Contrapositiva

- **Exemplo 2 (4/7):**

  Hipóteses: $p \longrightarrow q, \quad \neg p \longrightarrow r, \quad r \longrightarrow s$

  Conclusão: $\neg q \longrightarrow s$

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $\neg q \longrightarrow \neg p$	1, Contrapositiva
3. $\neg p \longrightarrow r$	Hipótese

- **Exemplo 2 (5/7):**

  Hipóteses: $p \longrightarrow q, \quad \neg p \longrightarrow r, \quad r \longrightarrow s$

  Conclusão: $\neg q \longrightarrow s$

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $\neg q \longrightarrow \neg p$	1, Contrapositiva
3. $\neg p \longrightarrow r$	Hipótese
4. $\neg q \longrightarrow r$	2, 3, Silogismo Hipotético

ARGUMENTOS VÁLIDOS

- **Exemplo 2 (6/7):**

  Hipóteses: $p \longrightarrow q, \quad \neg p \longrightarrow r, \quad r \longrightarrow s$

  Conclusão: $\neg q \longrightarrow s$

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $\neg q \longrightarrow \neg p$	1, Contrapositiva
3. $\neg p \longrightarrow r$	Hipótese
4. $\neg q \longrightarrow r$	2, 3, Silogismo Hipotético
5. $r \longrightarrow s$	Hipótese

ARGUMENTOS VÁLIDOS

- **Exemplo 2 (7/7):**

  Hipóteses: $p \longrightarrow q, \quad \neg p \longrightarrow r, \quad r \longrightarrow s$

  Conclusão: $\neg q \longrightarrow s$

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $\neg q \longrightarrow \neg p$	1, Contrapositiva
3. $\neg p \longrightarrow r$	Hipótese
4. $\neg q \longrightarrow r$	2, 3, Silogismo Hipotético
5. $r \longrightarrow s$	Hipótese
6. $\neg q \longrightarrow s$	4, 5, Silogismo Hipotético $\square$

ARGUMENTOS VÁLIDOS

- Pode-se inserir uma tautologia em qualquer passo de uma prova.

ARGUMENTOS VÁLIDOS

- **Exemplo 3(a):** A proposição "Meu cliente é canhoto. Mas, se o diário não desapareceu, então meu cliente não é canhoto. Logo, o diário desapareceu." é válida?

p: "Meu cliente é canhoto."

q: "O diário desapareceu."

Argumento: $[p \wedge (\neg q \longrightarrow \neg p)] \longrightarrow q$

Argumentos válidos

- **Exemplo 3(a):**

Argumento: $[p \wedge (\neg q \longrightarrow \neg p)] \longrightarrow q$

Prova:

Passo	**Justificativa**
1. p	Hipótese
2. $\neg q \longrightarrow \neg p$	Hipótese
3. $(\neg q \longrightarrow \neg p) \longrightarrow (p \longrightarrow q)$	Tautologia

ARGUMENTOS VÁLIDOS

- **Exemplo 3(a):**

Argumento: $[p \wedge (\neg q \longrightarrow \neg p)] \longrightarrow q$

Prova:

Passo	**Justificativa**
1. p	Hipótese
2. $\neg q \longrightarrow \neg p$	Hipótese
3. $(\neg q \longrightarrow \neg p) \longrightarrow (p \longrightarrow q)$	Tautologia
4. $p \longrightarrow q$	2, 3, Modus Ponens

Argumentos válidos

- **Exemplo 3(a):**

Argumento: $[p \wedge (\neg q \rightarrow \neg p)] \rightarrow q$

Prova:

Passo	**Justificativa**
1. p	Hipótese
2. $\neg q \rightarrow \neg p$	Hipótese
3. $(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	Tautologia
4. $p \rightarrow q$	2, 3, Modus Ponens
5. q	1, 4, Modus Ponens $\square$

ARGUMENTOS VÁLIDOS

- **Exemplo 3(b):** A prova do exemplo anterior pode ser simplificada para:

Argumento: $[p \wedge (\neg q \longrightarrow \neg p)] \longrightarrow q$

Prova:

Passo	Justificativa
1. p	Hipótese
2. $\neg q \longrightarrow \neg p$	Hipótese
3. q	1, 2, Modus Tollens $\square$

ARGUMENTOS VÁLIDOS

- A validade da proposição depende apenas de sua forma lógica:
  - não tem a ver com o fato de seus componentes serem ou não realmente verdadeiros
  - no exemplo anterior, ainda não sabemos se o diário realmente desapareceu ou não...

ARGUMENTOS VÁLIDOS

- **Exemplo 4 (1/3):** “Se a taxa para importação diminuir, o comércio interno aumentará. A taxa federal de desconto diminuirá ou o comércio interno não irá aumentar. A taxa para importação vai diminuir. Portanto, a taxa federal de desconto vai diminuir.”

  $\boldsymbol{p}$: “A taxa para importação vai diminuir.”

  $\boldsymbol{q}$: “O comércio interno vai aumentar.”

  $\boldsymbol{r}$: “A taxa federal de desconto vai diminuir.”

  Argumento: $[(\boldsymbol{p} \longrightarrow \boldsymbol{q}) \wedge (\boldsymbol{r} \vee \neg \boldsymbol{q}) \wedge \boldsymbol{p}] \longrightarrow \boldsymbol{r}$

ARGUMENTOS VÁLIDOS

- **Exemplo 4 (2/3):** “Se a taxa para importação diminuir, o comércio interno aumentará. A taxa federal de desconto diminuirá ou o comércio interno não irá aumentar. A taxa para importação vai diminuir. Portanto, a taxa federal de desconto vai diminuir.”

Argumento: $[(p \longrightarrow q) \wedge (r \vee \neg q) \wedge p] \longrightarrow r$

Prova:

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $r \vee \neg q$	Hipótese
3. p	Hipótese
4. q	1, 3, Modus Ponens

Argumentos válidos

- **Exemplo 4 (3/3):** "Se a taxa para importação diminuir, o comércio interno aumentará. A taxa federal de desconto diminuirá ou o comércio interno não irá aumentar. A taxa para importação vai diminuir. Portanto, a taxa federal de desconto vai diminuir."

Argumento: $[(p \longrightarrow q) \wedge (r \vee \neg q) \wedge p] \longrightarrow r$

Prova:

Passo	**Justificativa**
1. $p \longrightarrow q$	Hipótese
2. $r \vee \neg q$	Hipótese
3. p	Hipótese
4. q	1, 3, Modus Ponens
5. r	2, 4, Silogismo Disjuntivo $\square$

ARGUMENTOS VÁLIDOS

- **Exemplo 5(1/3):** “Você está a ponto de sair para o trabalho de manhã e descobre que está sem óculos. Você sabe os fatos a seguir. Onde estão os seus óculos?”

  1. Se meus óculos estão sobre a mesa da cozinha, então eu os vi no café da manhã.
  2. Eu estava lendo o jornal na sala ou na cozinha.
  3. Se eu estava lendo o jornal na sala, então meus óculos estão sobre a mesa de café.
  4. Eu não vi meus óculos no café da manhã.
  5. Se eu estava lendo meu livro na cama, então meus óculos estão sobre a mesinha de cabeceira.
  6. Se eu estava lendo o jornal na cozinha, então meus óculos estão sobre a mesa da cozinha.

ARGUMENTOS VÁLIDOS

- **Exemplo 5(2/3):** “Onde estão os seus óculos?”
  - Proposições simples (“idéias atômicas”):

    p: “Meus óculos estão sobre a mesa da cozinha”

    q: “Eu vi meus óculos no café da manhã”

    r: “Eu estava lendo o jornal na sala”

    s: “Eu estava lendo o jornal na cozinha”

    t: “Meus óculos estão sobre a mesa do café”

    u: “Eu estava lendo meu livro na cama”

    v: “Meus óculos estão sobre a mesinha de cabeceira”
  - Argumento:

    (a) $p \longrightarrow q$

    (b) $r \lor s$

    (c) $r \longrightarrow t$

    (d) $\neg q$

    (e) $u \longrightarrow v$

    (f) $s \longrightarrow p$

ARGUMENTOS VÁLIDOS

- **Exemplo 5(3/3):** "Onde estão os seus óculos?"

Argumento:

(a) $p \longrightarrow q$

(b) $r \vee s$

(c) $r \longrightarrow t$

(d) $\neg q$

(e) $u \longrightarrow v$

(f) $s \longrightarrow p$

Prova:

Passo	**Justificativa**
?	**?**

ARGUMENTOS VÁLIDOS

- **Exemplo 5(3/3):** "Onde estão os seus óculos?"

Argumento:

(a) $p \longrightarrow q$

(b) $r \vee s$

(c) $r \longrightarrow t$

(d) $\neg q$

(e) $u \longrightarrow v$

(f) $s \longrightarrow p$

Prova:

Passo	**Justificativa**
1. $\neg p$	a, d, Modus Tollens

Argumentos válidos

- **Exemplo 5(3/3):** "Onde estão os seus óculos?"

Argumento:

(a) $p \longrightarrow q$
(b) $r \vee s$
(c) $r \longrightarrow t$
(d) $\neg q$
(e) $u \longrightarrow v$
(f) $s \longrightarrow p$

Prova:

Passo	**Justificativa**
1. $\neg p$	a, d, Modus Tollens
2. $\neg s$	f, 1, Modus Tollens)

ARGUMENTOS VÁLIDOS

- **Exemplo 5(3/3):** “Onde estão os seus óculos?”

Argumento:

(a) $p \longrightarrow q$
(b) $r \vee s$
(c) $r \longrightarrow t$
(d) $\neg q$
(e) $u \longrightarrow v$
(f) $s \longrightarrow p$

Prova:

Passo	**Justificativa**
1. $\neg p$	a, d, Modus Tollens
2. $\neg s$	f, 1, Modus Tollens)
3. r	b, 2, Silogismo Disjuntivo

ARGUMENTOS VÁLIDOS

- **Exemplo 5(3/3):** "Onde estão os seus óculos?"

Argumento:

(a) $p \longrightarrow q$

(b) $r \vee s$

(c) $r \longrightarrow t$

(d) $\neg q$

(e) $u \longrightarrow v$

(f) $s \longrightarrow p$

Prova:

Passo	Justificativa
1. $\neg p$	a, d, Modus Tollens
2. $\neg s$	f, 1, Modus Tollens
3. r	b, 2, Silogismo Disjuntivo
4. t	c, 3, Modus Ponens $\square$

NOTA 1: USO DE TABELAS-VERDADE

- Uma demonstração por tabela-verdade seria possível para o exemplo anterior
  - mas exigiria a análise de $2^7 = 128$ possibilidades (!!)

- É melhor aplicar as regras de inferência
  - mesmo em um processo de tentativa e erro

NOTA 2: PREMISSAS FALSAS

- Argumento correto pode levar a conclusão incorreta
  - se uma ou mais premissas falsas forem usadas.
- **Exemplo:** Argumento válido por Modus Ponens:

  Se $\sqrt{\mathbf{2}} > \frac{\mathbf{3}}{\mathbf{2}}$, então: $(\sqrt{\mathbf{2}})^{\mathbf{2}} > (\frac{\mathbf{3}}{\mathbf{2}})^{\mathbf{2}}$

  - ora, “sabemos que”: $\sqrt{\mathbf{2}} > \frac{\mathbf{3}}{\mathbf{2}}$
  - consequentemente: $(\sqrt{\mathbf{2}})^{\mathbf{2}} > (\frac{\mathbf{3}}{\mathbf{2}})^{\mathbf{2}}$ (!!?)

NOTA 2: PREMISSAS FALSAS

- Argumento correto pode levar a conclusão incorreta
  - se uma ou mais premissas falsas forem usadas.
- **Exemplo:** Argumento válido por Modus Ponens:

  Se $\sqrt{\mathbf{2}} > \frac{\mathbf{3}}{\mathbf{2}}$, então: $(\sqrt{\mathbf{2}})^{\mathbf{2}} > (\frac{\mathbf{3}}{\mathbf{2}})^{\mathbf{2}}$

  - ora, "sabemos que": $\sqrt{\mathbf{2}} > \frac{\mathbf{3}}{\mathbf{2}}$
  - consequentemente: $(\sqrt{\mathbf{2}})^{\mathbf{2}} > (\frac{\mathbf{3}}{\mathbf{2}})^{\mathbf{2}}$ (!!?)
  - No entanto, a conclusão deste argumento é falsa
    - ocorre que a premissa "$\sqrt{\mathbf{2}} > \frac{\mathbf{3}}{\mathbf{2}}$" é falsa
    - logo, a conclusão podia mesmo ser falsa. □

NOTA 3: FALÁCIAS (1/4)

- Erro comum em demonstrações: utilização de falácias.
  - Falácias parecem-se com regras de inferência
  - mas: são baseadas em contingências

- **Exemplo 1:** a proposição $[(p \rightarrow q) \wedge q] \rightarrow p$
  - é F quando p é F e q é V
  - Erro comum: tratá-la como tautologia
    - falácia de "afirmar a conclusão".

NOTA 3: FALÁCIAS (2/4)

- **Exemplo:** "Se você resolver todos os problemas da lista de exercícios, então você vai aprender Matemática Discreta. Você aprendeu Matemática Discreta. Logo, você resolveu todos os problemas da lista de exercícios."
  - Proposições:

    p: "Você resolveu todos os problemas da lista de exercícios."

    q: "Você aprendeu Matemática Discreta."
  - Vemos que o argumento consiste em:

    se $p \longrightarrow q$ e q, então p ("falácia de afirmar a conclusão")
  - É plenamente possível aprender MD sem resolver toda a lista:
    - você pode, por ex., resolver alguns (mas não todos) os problemas da lista, resolver outros exercícios, etc.

NOTA 3: FALÁCIAS (3/4)

- **Exemplo 2:** a proposição $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$
  - é F quando p é F e q é V
  - Falácia de "negar a hipótese"
  - Muitos argumentos incorretos a usam como regra

NOTA 3: FALÁCIAS (4/4)

- **Exemplo:** Assuma que é correto que: “Se você resolver todos os problemas da lista de exercícios, então você vai aprender Matemática Discreta.”
  - Então, “Se você não resolveu todos os problemas da lista”,
  - será que é correto concluir que: “você não aprendeu MD”??

- **Resposta:**
  - “Falácia de negar a hipótese”.
  - É possível que você tenha aprendido MD mesmo que você não tenha resolvido todos os problemas da lista...

INFERÊNCIAS NA LÓGICA DE PREDICADOS (1/6)

Regra de Inferência	Nome	Observação
$\dfrac{\forall x P(x)}{\therefore\ P(c)}$	*Instanciação* Universal	c específico
$\dfrac{P(c) \text{ para um } c \text{ arbitrário}}{\therefore\ \forall x P(x)}$	Generalização Universal	c arbitrário
$\dfrac{\exists x P(x)}{\therefore\ P(c) \text{ para algum elemento } c}$	*Instanciação* Existencial	c específico (não conhecido)
$\dfrac{P(c) \text{ para algum elemento } c}{\therefore\ \exists x P(x)}$	Generalização Existencial	c específico e conhecido

INFERÊNCIAS NA LÓGICA DE PREDICADOS (2/6)

- **Exemplo 1:** Mostre que as premissas "Todos nesta turma de Fundamentos já cursaram Cálculo" e "Manoel é um estudante nesta turma" implicam na conclusão "Manoel já cursou Cálculo".
  - Declarações básicas:

    $F(x)$: "x está nesta turma de Fundamentos"

    $C(x)$: "x já cursou Cálculo"
  - Premissas:

    $\forall x(F(x) \rightarrow C(x))$

    F(Manoel)

Inferências na Lógica de Predicados (2/6)

- **Exemplo 1:**
  - Premissas: $\forall x(F(x) \rightarrow C(x))$

    F(Manoel)
  - Estabelecendo a conclusão a partir das premissas:

Passo	**Justificativa**
1. $\forall x(F(x) \rightarrow C(x))$	Premissa
2. F(Manoel) $\rightarrow C$(Manoel)	Instanciação universal de (1)

Inferências na Lógica de Predicados (2/6)

- **Exemplo 1:**
  - Premissas: $\forall x(F(x) \rightarrow C(x))$

    F(Manoel)
  - Estabelecendo a conclusão a partir das premissas:

Passo	**Justificativa**
1. $\forall x(F(x) \rightarrow C(x))$	Premissa
2. F(Manoel) $\rightarrow C$(Manoel)	Instanciação universal de (1)
3. F(Manoel)	Premissa

Inferências na Lógica de Predicados (2/6)

- **Exemplo 1:**
  - Premissas: $\forall x(F(x) \rightarrow C(x))$

    $F(\text{Manoel})$
  - Estabelecendo a conclusão a partir das premissas:

Passo	**Justificativa**
1. $\forall x(F(x) \rightarrow C(x))$	Premissa
2. $F(\text{Manoel}) \rightarrow C(\text{Manoel})$	Instanciação universal de (1)
3. $F(\text{Manoel})$	Premissa
4. $C(\text{Manoel})$	(2), (3), Modus Ponens $\square$

- **Exemplo 2 (1/10):** Mostre que as premissas “Tem um estudante nesta turma que não leu o livro-texto” e “Todos nesta turma se saíram bem na primeira prova” implicam na conclusão “Alguém que se saiu bem na primeira prova não leu o livro-texto”.
  - Declarações básicas:
    $T(x)$: “x está nesta turma”
    $L(x)$: “x leu o livro-texto”
    $P(x)$: “x se saiu bem na primeira prova”
  - Premissas: $\exists x(T(x) \wedge \neg L(x))$
    $\forall x(T(x) \rightarrow P(x))$
  - Conclusão: $\exists x(P(x) \wedge \neg L(x))$

INFERÊNCIAS NA LÓGICA DE PREDICADOS (4/6)

- **Exemplo 2 (2/10):**

Premissas: $\exists x(T(x) \land \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

Conclusão: $\exists x(P(x) \land \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \land \neg L(x))$	Premissa

INFERÊNCIAS NA LÓGICA DE PREDICADOS (4/6)

- **Exemplo 2 (3/10):**

Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

Conclusão: $\exists x(P(x) \wedge \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \wedge \neg L(x))$	Premissa
2. $T(a) \wedge \neg L(a)$	Instanciação existencial de (1)

- **Exemplo 2 (4/10):**

Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

Conclusão: $\exists x(P(x) \wedge \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \wedge \neg L(x))$	Premissa
2. $T(a) \wedge \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)

INFERÊNCIAS NA LÓGICA DE PREDICADOS (4/6)

- **Exemplo 2 (5/10):**

  Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

  Conclusão: $\exists x(P(x) \wedge \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \wedge \neg L(x))$	Premissa
2. $T(a) \wedge \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)
4. $\forall x(T(x) \rightarrow P(x))$	Premissa

Inferências na Lógica de Predicados (4/6)

- **Exemplo 2 (6/10):**

  Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

  Conclusão: $\exists x(P(x) \wedge \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \wedge \neg L(x))$	Premissa
2. $T(a) \wedge \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)
4. $\forall x(T(x) \rightarrow P(x))$	Premissa
5. $T(a) \rightarrow P(a)$	Instanciação Universal de (4)

- **Exemplo 2 (7/10):**

Premissas: $\exists x(T(x) \land \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

Conclusão: $\exists x(P(x) \land \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \land \neg L(x))$	Premissa
2. $T(a) \land \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)
4. $\forall x(T(x) \rightarrow P(x))$	Premissa
5. $T(a) \rightarrow P(a)$	Instanciação Universal de (4)
6. $P(a)$	(3), (5), Modus Ponens

INFERÊNCIAS NA LÓGICA DE PREDICADOS (4/6)

- **Exemplo 2 (8/10):**

  Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

  Conclusão: $\exists x(P(x) \wedge \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \wedge \neg L(x))$	Premissa
2. $T(a) \wedge \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)
4. $\forall x(T(x) \rightarrow P(x))$	Premissa
5. $T(a) \rightarrow P(a)$	Instanciação Universal de (4)
6. $P(a)$	(3), (5), Modus Ponens
7. $\neg L(a)$	Simplificação de (2)

- **Exemplo 2 (9/10):**

Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

Conclusão: $\exists x(P(x) \wedge \neg L(x))$

Passo	**Justificativa**
1. $\exists x(T(x) \wedge \neg L(x))$	Premissa
2. $T(a) \wedge \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)
4. $\forall x(T(x) \rightarrow P(x))$	Premissa
5. $T(a) \rightarrow P(a)$	Instanciação Universal de (4)
6. $P(a)$	(3), (5), Modus Ponens
7. $\neg L(a)$	Simplificação de (2)
8. $P(a) \wedge \neg L(a)$	Conjunção de (6) e (7)

Inferências na Lógica de Predicados (4/6)

- **Exemplo 2 (10/10):**

Premissas: $\exists x(T(x) \land \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$

Conclusão: $\exists x(P(x) \land \neg L(x))$

Passo	Justificativa
1. $\exists x(T(x) \land \neg L(x))$	Premissa
2. $T(a) \land \neg L(a)$	Instanciação existencial de (1)
3. $T(a)$	Simplificação de (2)
4. $\forall x(T(x) \rightarrow P(x))$	Premissa
5. $T(a) \rightarrow P(a)$	Instanciação Universal de (4)
6. $P(a)$	(3), (5), Modus Ponens
7. $\neg L(a)$	Simplificação de (2)
8. $P(a) \land \neg L(a)$	Conjunção de (6) e (7)
9. $\exists x(P(x) \land \neg L(x))$	Generalização Existencial de (8) $\square$

INFERÊNCIAS NA LÓGICA DE PREDICADOS (5/6)

- **Nota 1:** É comum que apareçam tanto uma regra de inferência proposicional quanto uma para quantificadores.
- Por exemplo, Instanciação Universal e Modus Ponens são frequentemente usadas juntas:
  - combinando $\forall x(P(x) \rightarrow Q(x))$ e $P(c)$,
    - onde c é um elemento do UD
  - obtemos que $Q(c)$ é Verdadeiro.

INFERÊNCIAS NA LÓGICA DE PREDICADOS (6/6)

- **Nota 2:** Muitos teoremas omitem o quantificador ao definir que uma propriedade vale para todos os elementos de um conjunto.

- Por exemplo, o real significado de:
  - "Se $x > y$, onde x e y são reais positivos, então $x^2 > y^2$"
  - é: "Para todos os reais positivos x e y, se $x > y$, então $x^2 > y^2$".

- É comum a lei de generalização universal ser usada implicitamente:
  - no início da prova, seleciona-se um elemento geral do UD
  - passos subseqüentes mostram que este elemento tem a propriedade em questão
  - conclui-se que o teorema vale para todos os elementos do UD.

PROVA DE TEOREMAS MATEMÁTICOS

- Tarefa difícil.
- Veremos uma “bateria” de diferentes métodos.
- Relembrando:

  “$p \longrightarrow q$ só não é V quando p é V e q é F.”
- Observações úteis:
  - o inteiro n é par se existe um inteiro k tal que $n = 2k$
  - o inteiro n é ímpar se existe um inteiro k tal que $n = 2k + 1$

PROVAS DIRETAS

- **Princípio**: para provar $p \longrightarrow q$:
  1. assumir que p é verdadeiro
  2. usar regras de inferência e teoremas já provados para mostrar que q também deve ser V.

PROVAS DIRETAS

- **Princípio**: para provar $p \longrightarrow q$:
  1. assumir que p é verdadeiro
  2. usar regras de inferência e teoremas já provados para mostrar que q também deve ser V.

- **Exemplo:** "se n é ímpar, então n^2 é ímpar"
  - assuma a hipótese: n é ímpar
  - então: $n = 2k + 1$
  - segue que:

    $$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

  - portanto: n^2 é ímpar $\square$

PROVAS INDIRETAS

- **Princípio**: mostrar que a contrapositiva de $p \longrightarrow q$ é V, usando outras técnicas de demonstração.

- **Exemplo:** "se $3n + 2$ é ímpar, então n é ímpar"
  - assuma que a conclusão desta implicação é F
  - então: $n = 2k$, para algum k
  - daí: $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$

Provas Indiretas

- **Princípio**: mostrar que a contrapositiva de $p \longrightarrow q$ é V, usando outras técnicas de demonstração.

- **Exemplo:** "se $3n + 2$ é ímpar, então n é ímpar"
  - assuma que a conclusão desta implicação é F
  - então: $n = 2k$, para algum k
  - daí: $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$
  - de modo que: $3n + 2$ é par
  - logo, uma vez que a negação da conclusão implica que a hipótese é F, a implicação original é V. $\square$

PROVAS POR VÁCUO

- **Princípio**: $p \longrightarrow q$ é V se p é F, de modo que:
  - prova-se $p \Rightarrow q$ estabelecendo que p é sempre F
- Provam casos especiais de teoremas do tipo $\forall n P(n)$.

PROVAS POR VÁCUO

- **Princípio**: $p \longrightarrow q$ é V se p é F, de modo que:
  - prova-se $p \Rightarrow q$ estabelecendo que p é sempre F
- Provam casos especiais de teoremas do tipo $\forall n P(n)$.

- **Exemplo:** mostre que a proposição $P(0)$ é V, aonde $P(n)$ é "se $n > 1$, então $n^2 > n$".
  - $P(0)$ é a implicação: "se $0 > 1$, então $0^2 > 0$"
  - uma vez que a hipótese é F:
    - a implicação $P(0)$ é automaticamente V. $\square$

PROVAS TRIVIAIS

- **Princípio**: $p \longrightarrow q$ é V se q é V, de modo que:
  - pode-se provar $p \Rightarrow q$ apenas estabelecendo que q é sempre V
- Importantes quando casos especiais de teoremas precisam ser provados (por ex.: em provas por casos e na indução matemática).

PROVAS TRIVIAIS

- **Princípio**: $p \rightarrow q$ é V se q é V, de modo que:
  - pode-se provar $p \Rightarrow q$ apenas estabelecendo que q é sempre V
- Importantes quando casos especiais de teoremas precisam ser provados (por ex.: em provas por casos e na indução matemática).
- **Exemplo:** Mostre que a proposição $P(0)$ é Verdadeira em:

  $P(n)$: "se a e b são inteiros positivos com $a \geq b$, então $a^n \geq b^n$"
  - $P(0)$ é: "se $a \geq b$, então $a^0 \geq b^0$"
  - uma vez que $a^0 = b^0 = 1$, a conclusão de $P(0)$ é V $\square$
    - (a hipótese, "$a \geq b$", não é necessária)

ESTRATÉGIAS DE PROVA

- Primeiro, tentamos uma prova direta.
- Quando não há modo óbvio de seguir, às vezes uma prova indireta funciona tranquilamente...
- **Nota**:
  - O número real r é **racional** se existem inteiros p e q, com $q \neq 0$, tais que $r = p/q$.
  - Um real que não é racional é chamado de **irracional**.

Estratégias de Prova

- **Exemplo:** Prove que a soma de dois números racionais é sempre racional:
  - tentando uma prova direta...
  - sejam r e t números racionais
  - então, existem inteiros:

    p e q, com $q \neq 0$, tais que: $r = p/q$

    u e v, com $v \neq 0$, tais que: $t = u/v$
  - daí, adicionando r e t:

    $$r + t = \frac{p}{q} + \frac{u}{v} = \frac{p.v + q.u}{q.v}$$
  - como $q \neq 0$ e $v \neq 0$, segue que $q.v \neq 0$
  - isto significa que $r + t$ é racional $\square$
    - (nossa tentativa direta deu certo...)

ESTRATÉGIAS DE PROVA

- **Exemplo:** Prove que se n é um inteiro e n^2 é ímpar, então n é ímpar:
  - tentando uma prova direta:
    - n^2 é ímpar $\Rightarrow$ $\exists k$ tal que $n^2 = 2k + 1$
    - será que isto serve para mostrar que n é ímpar??
    - ora, resolvendo para n, obtemos: $\pm\sqrt{2k+1}$
    - o que não é muito útil...
  - prova indireta:
    - assumimos que n não é ímpar
    - então $n = 2k$
    - elevando os dois lados ao quadrado: $n^2 = 4k^2 = 2(2k^2)$
    - o que implica que n^2 é par. $\square$

OUTRAS TÉCNICAS

- **Provas por contradição**:
  - assuma que $p \rightarrow q$ seja F
    - isto é: que p seja V e q seja F
  - com regras de inferência, derive uma contradição desta hipótese.
    - $r \wedge \neg r$, por exemplo
- **Exemplo 1:** Prove que $\sqrt{2}$ é irracional.

PROVAS POR CONTRADIÇÃO

- **Exemplo 1 (1/4):** Provar que p: "$\sqrt{2}$ é irracional" é V.
  - assuma que $\neg p$ é V, ou seja: $\sqrt{2}$ é racional
    - logo, existem inteiros a e b tais que $\sqrt{2} = a/b$
    - onde a e b não têm fatores em comum

PROVAS POR CONTRADIÇÃO

- **Exemplo 1 (2/4):** Provar que p: "$\sqrt{2}$ é irracional" é V.
  - assuma que $\neg p$ é V, ou seja: $\sqrt{2}$ é racional
    - logo, existem inteiros a e b tais que $\sqrt{2} = a/b$
    - onde a e b não têm fatores em comum
  - mas, como $\sqrt{2} = a/b$, segue que $2 = a^2/b^2$
    - logo, $2b^2 = a^2$, ou seja, a^2 é par
    - logo: a é par

Provas por contradição

- **Exemplo 1 (3/4):** Provar que p: "$\sqrt{2}$ é irracional" é V.
  - assuma que $\neg p$ é V, ou seja: $\sqrt{2}$ é racional
    - logo, existem inteiros a e b tais que $\sqrt{2} = a/b$
    - onde a e b não têm fatores em comum
  - mas, como $\sqrt{2} = a/b$, segue que $2 = a^2/b^2$
    - logo, $2b^2 = a^2$, ou seja, a^2 é par
    - logo: a é par
  - então, $a = 2c$, para algum inteiro c
    - logo: $2b^2 = 4c^2$ de modo que $b^2 = 2c^2$
    - ou seja: b^2 é par e b é par também
    - contradição: assumimos que a e b não tinham fatores em comum

PROVAS POR CONTRADIÇÃO

- **Exemplo 1 (4/4):** Provar que p: "$\sqrt{2}$ é irracional" é V.
  - assuma que $\neg p$ é V, ou seja: $\sqrt{2}$ é racional
    - logo, existem inteiros a e b tais que $\sqrt{2} = a/b$
    - onde a e b não têm fatores em comum
  - mas, como $\sqrt{2} = a/b$, segue que $2 = a^2/b^2$
    - logo, $2b^2 = a^2$, ou seja, a^2 é par
    - logo: a é par
  - então, $a = 2c$, para algum inteiro c
    - logo: $2b^2 = 4c^2$ de modo que $b^2 = 2c^2$
    - ou seja: b^2 é par e b é par também
    - contradição: assumimos que a e b não tinham fatores em comum
  - portanto: p é que é V. $\square$

Provas por casos

- **Princípio**: $p_1 \vee p_2 \vee \ldots \vee p_n \rightarrow q$ é equivalente a:

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$$

  - ou seja: provar cada um dos $p_i \rightarrow q$ individualmente

- **Exemplo:** Use a prova por casos para mostrar que $|xy| = |x||y|$, onde x e y são reais.

- **Nota:**
$$|x| = x, \quad \text{se } x \geq 0$$
$$|x| = -x, \quad \text{se } x \leq 0$$

PROVAS POR CASOS

- **Exemplo (1/2):** Mostre que $|xy| = |x||y|$.
  - Sejam:
    - p: "x e y são números reais"
    - q: "$|xy| = |x||y|$"
  - Note que p é equivalente a $p_1 \vee p_2 \vee p_3 \vee p_4$, onde:
    - p_1: "$x \geq 0 \ \wedge \ y \geq 0$"
    - p_2: "$x \geq 0 \ \wedge \ y < 0$"
    - p_3: "$x < 0 \ \wedge \ y \geq 0$"
    - p_4: "$x < 0 \ \wedge \ y < 0$"

PROVAS POR CASOS

- **Exemplo (2/2):** Mostre que $|xy| = |x||y|$.

  4 casos para provar:

  1. $p_1 \longrightarrow q$ é V, pois:
     - $xy \geq 0$ quando $x \geq 0$ e $y \geq 0$
     - de modo que: $|xy| = xy = |x||y|$
  2. $p_2 \longrightarrow q$ é V, pois:
     - se $x \geq 0$ e $y < 0$, então $xy \leq 0$
     - de modo que: $|xy| = -xy = x.(-y) = |x||y|$
  3. $p_3 \longrightarrow q$ é V, pois:
     - se $x < 0$ e $y \geq 0$, então $xy \leq 0$
     - de modo que: $|xy| = -xy = (-x).y = |x||y|$
  4. $p_4 \longrightarrow q$ é V, pois:
     - se $x < 0$ e $y < 0$, então $xy > 0$
     - de modo que: $|xy| = xy = (-x).(-y) = |x||y|$ $\square$

PROVANDO EQUIVALÊNCIAS

- Provas de teoremas que são bicondicionais.
- Usar a tautologia: $(p \leftrightarrow q) \Leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$
- Ou seja, "p se e somente se q" pode ser provada ao serem provadas as implicações:
  - "se p, então q"
  - "se q, então p"

Provando equivalências

- **Exemplo:** Prove o teorema: "O inteiro n é ímpar sse n^2 é ímpar."
  - Teorema da forma: "p sse q", aonde:
    - p é dado por: "n é ímpar"
    - q é dado por: "n^2 é ímpar"
  - Temos que provar $p \longrightarrow q$ e $q \longrightarrow p$.
  - O que já foi feito:
    - $\longrightarrow$: provas diretas
    - $\longleftarrow$: estratégias de prova $\square$

PROVANDO EQUIVALÊNCIAS

- Pode-se ter que mostrar que várias proposições são equivalentes:

  $$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n$$

- Prova-se que são mutuamente equivalentes usando a tautologia:

  $$[p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n] \;\leftrightarrow\; [(p_1 \rightarrow p_2) \wedge \cdots \wedge (p_n \rightarrow p_1)]$$

  - Muito mais eficiente do que provar todos contra todos...
  - Qualquer encadeamento de declarações é igualmente válido.

PROVANDO EQUIVALÊNCIAS

- **Exemplo:** Mostre que as afirmações a seguir são equivalentes:

  p_1: n é um inteiro par

  p_2: $n - 1$ é um inteiro ímpar

  p_3: n^2 é um inteiro par

Prova (1/3):

- Mostrar que são V as implicações: $p_1 \longrightarrow p_2$, $p_2 \longrightarrow p_3$ e $p_3 \longrightarrow p_1$
- Mostrando $p_1 \longrightarrow p_2$ (prova direta):
  - n é par $\Rightarrow$ $n = 2k$ $\Rightarrow$ $n - 1 = 2k - 1 = 2(k-1) + 1$

PROVANDO EQUIVALÊNCIAS

- **Exemplo:** Mostre que as afirmações a seguir são equivalentes:

  p_1: n é um inteiro par

  p_2: $n - 1$ é um inteiro ímpar

  p_3: n^2 é um inteiro par

Prova (2/3):

- Mostrar que são V as implicações: $p_1 \longrightarrow p_2$, $p_2 \longrightarrow p_3$ e $p_3 \longrightarrow p_1$
- Mostrando $p_1 \longrightarrow p_2$ (prova direta):
  - n é par $\Rightarrow$ $n = 2k$ $\Rightarrow$ $n - 1 = 2k - 1 = 2(k-1) + 1$
- Mostrando $p_2 \longrightarrow p_3$ (prova direta):
  - $n - 1$ é ímpar $\Rightarrow$ $n - 1 = 2k + 1$ $\Rightarrow$ $n = 2k + 2$
  - logo: $n^2 = (2k+2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$ (par)

PROVANDO EQUIVALÊNCIAS

- **Exemplo:** Mostre que as afirmações a seguir são equivalentes:

  p_1: n é um inteiro par

  p_2: $n - 1$ é um inteiro ímpar

  p_3: n^2 é um inteiro par

Prova (3/3):

- Mostrar que são V as implicações: $p_1 \longrightarrow p_2$, $p_2 \longrightarrow p_3$ e $p_3 \longrightarrow p_1$
- Mostrando $p_1 \longrightarrow p_2$ (prova direta):
  - n é par $\Rightarrow$ $n = 2k$ $\Rightarrow$ $n - 1 = 2k - 1 = 2(k-1) + 1$
- Mostrando $p_2 \longrightarrow p_3$ (prova direta):
  - $n - 1$ é ímpar $\Rightarrow$ $n - 1 = 2k + 1$ $\Rightarrow$ $n = 2k + 2$
  - logo: $n^2 = (2k+2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$ (par)
- Mostrando $p_3 \longrightarrow p_1$ (prova indireta):
  - ou seja, devemos provar que: “se n não é par, então n^2 não é par”
  - já provado (provas diretas) $\square$

Teoremas com Quantificadores

- Muitos teoremas são propostos como proposições que envolvem quantificadores.
- Veremos alguns dos métodos mais importantes para provar teoremas deste tipo.

PROVAS DE EXISTÊNCIA

- Muitos teoremas são asserções de que existem objetos de um tipo em particular:
  - ou seja, são proposições da forma: $\exists x P(x)$

- Modos de provar estes teoremas:
  - Provas **construtivas**: encontrar elemento a tal que $P(a)$ é V
  - Provas **não-construtivas**: mostrar que a negação da proposição implica em uma contradição.

PROVAS DE EXISTÊNCIA

- **Exemplo:** Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas formas diferentes.

Solução:

- Após uma busca computacional, descobrimos que:

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \qquad \square$$

PROVAS DE EXISTÊNCIA

- **Exemplo:** Mostre que existem números irracionais x e y tais que x^y é racional.
  - Sabemos que $\sqrt{2}$ é irracional.
  - Agora considere o número $\sqrt{2}^{\sqrt{2}}$:
    - se ele for racional, já temos x e y irracionais com x^y racional

PROVAS DE EXISTÊNCIA

- **Exemplo:** Mostre que existem números irracionais x e y tais que x^y é racional.
  - Sabemos que $\sqrt{2}$ é irracional.
  - Agora considere o número $\sqrt{2}^{\sqrt{2}}$:
    - se ele for racional, já temos x e y irracionais com x^y racional
    - mas se ele for irracional, podemos re-escolher x e y como:

$$x = \sqrt{2}^{\sqrt{2}} \quad \text{e} \quad y = \sqrt{2}$$

$$\Rightarrow x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$$

PROVAS DE EXISTÊNCIA

- **Exemplo:** Mostre que existem números irracionais x e y tais que x^y é racional.
  - Sabemos que $\sqrt{2}$ é irracional.
  - Agora considere o número $\sqrt{2}^{\sqrt{2}}$:
    - se ele for racional, já temos x e y irracionais com x^y racional
    - mas se ele for irracional, podemos re-escolher x e y como:

      $$x = \sqrt{2}^{\sqrt{2}} \quad \text{e} \quad y = \sqrt{2}$$

      $$\Rightarrow x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$$
  - Um dos dois casos demonstra o que foi pedido. $\square$
- Prova não-construtiva: mostramos que existe um par de números com a propriedade, mas não sabemos qual dos dois é o certo. (!)

PROVAS DE UNICIDADE

- Alguns teoremas afirmam que um elemento com a propriedade especificada existe e é único.
  - Ou seja: existe exatamente um elemento com esta propriedade.
- Logo, uma prova de unicidade tem duas partes:
  1. **Existência:** mostra-se que um elemento x com a propriedade desejada existe.
  2. **Unicidade:** mostra-se que, se $y \neq x$, então y não possui a propriedade desejada.
     - Nenhum outro elemento tem esta propriedade.
- Mesmo que provar: $\exists x(P(x) \land \forall y(y \neq x \rightarrow \neg P(y)))$

PROVAS DE UNICIDADE

- **Exemplo:** Mostre que todo inteiro tem uma única inversa aditiva.
  - Se p é um inteiro, $p + q = 0$ para o inteiro $q = -p$.
    - Logo: existe um inteiro q tal que $p + q = 0$.

PROVAS DE UNICIDADE

- **Exemplo:** Mostre que todo inteiro tem uma única inversa aditiva.
  - Se p é um inteiro, $p + q = 0$ para o inteiro $q = -p$.
    - Logo: existe um inteiro q tal que $p + q = 0$.
  - Agora, seja um inteiro $r \neq q$ tal que $p + r = 0$.
    - Então: $p + q = p + r$.
    - Só que, subtraindo p de ambos os lados, segue que: $q = r$
      - o que contradiz a hipótese $q \neq r$
    - Logo, só existe um único inteiro q tal que $p + q = 0$. $\square$

CONTRA-EXEMPLOS

- Podemos mostrar que uma declaração do tipo $\forall x P(x)$ é falsa com um contra-exemplo.
  - Ou seja, um exemplo de x para o qual $P(x)$ é falsa.

- Procuramos um contra-exemplo sempre que encontramos uma declaração do tipo $\forall x P(x)$ que:
  - acreditamos ser falsa,
  - tenha resistido a muitas tentativas de prova...

CONTRA-EXEMPLOS

- **Exemplo:** Mostre que é falsa a declaração:

  "Todo inteiro positivo é igual à soma dos quadrados de três inteiros".

  - Possível com os 6 primeiros inteiros positivos:

$$\mathbf{1 = 0^2 + 0^2 + 1^2} \qquad \mathbf{2 = 0^2 + 1^2 + 1^2} \qquad \mathbf{3 = 1^2 + 1^2 + 1^2}$$
$$\mathbf{4 = 0^2 + 0^2 + 2^2} \qquad \mathbf{5 = 0^2 + 1^2 + 2^2} \qquad \mathbf{6 = 1^2 + 1^2 + 2^2}$$

CONTRA-EXEMPLOS

- **Exemplo:** Mostre que é falsa a declaração:

  "Todo inteiro positivo é igual à soma dos quadrados de três inteiros".

  - Possível com os 6 primeiros inteiros positivos:

    $$1 = 0^2 + 0^2 + 1^2 \qquad 2 = 0^2 + 1^2 + 1^2 \qquad 3 = 1^2 + 1^2 + 1^2$$
    $$4 = 0^2 + 0^2 + 2^2 \qquad 5 = 0^2 + 1^2 + 2^2 \qquad 6 = 1^2 + 1^2 + 2^2$$

  - Porém, não conseguimos fazer o mesmo com 7:
    - os únicos quadrados que poderíamos usar são: 0, 1 e 4 (aqueles que não excedem 7)
    - e não há maneira de combinar estes 3 números para somar 7

  - Logo, a declaração acima é falsa. $\square$

CONTRA-EXEMPLOS

- Um erro comum é achar que (apenas) um ou mais exemplos são suficientes para concluir que uma declaração é verdadeira.

- **Atenção**: não importa quantos exempos indiquem que $P(x)$ é V:
  - a quantificação $\forall x P(x)$ ainda pode ser falsa...

CONTRA-EXEMPLOS

- **Exemplo:** Será que é verdade que todo inteiro positivo é a soma de 18 inteiros elevados à quarta potência??
  - Observa-se que todos os inteiros até 78 podem mesmo ser escritos desta maneira (!!).
  - Daí, se decidíssemos que já havíamos verificado o suficiente, chegaríamos a uma conclusão errada, pois:
    - 79 não é a soma de 18 quartas potências. □

Erros comuns em provas (1)

- Mais comuns: erros em aritmética ou álgebra básica.
- Cada passo de uma prova matemática deve ser correto.
- Muitos erros resultam da inclusão de passos que não seguem logicamente dos anteriores.

ERROS COMUNS EM PROVAS (1)

- **Exemplo 1:** O que está errado com a "prova" abaixo para 1=2?

"Prova:" (a e b são dois inteiros positivos iguais)

Passo	**Justificativa**
1. $a = b$	Dado
2. $a^2 = ab$	Multiplicando os 2 lados de (1) por a
3. $a^2 - b^2 = ab - b^2$	Subtraindo b^2 dos 2 lados de (2)
4. $(a - b)(a + b) = b(a - b)$	Fatorando ambos os lados de (3)
5. $a + b = b$	Dividindo ambos os lados de (4) por $a - b$
6. $2b = b$	Substituindo a por b em (5) (pois $a = b$)
7. $2 = 1$	Dividindo ambos os lados de (6) por b

ERROS COMUNS EM PROVAS (1)

- **Exemplo 1:** O que está errado com a “prova” abaixo para 1=2?

  “Prova:” (a e b são dois inteiros positivos iguais)

Passo	**Justificativa**
1. $a = b$	Dado
2. $a^2 = ab$	Multiplicando os 2 lados de (1) por a
3. $a^2 - b^2 = ab - b^2$	Subtraindo b^2 dos 2 lados de (2)
4. $(a - b)(a + b) = b(a - b)$	Fatorando ambos os lados de (3)
5. $a + b = b$	Dividindo ambos os lados de (4) por $a - b$
6. $2b = b$	Substituindo a por b em (5) (pois $a = b$)
7. $2 = 1$	Dividindo ambos os lados de (6) por b

- **“Solução:”**
  - Todos os passos são válidos, com exceção do passo 5, em que houve uma divisão por zero.

ERROS COMUNS EM PROVAS (2)

- Um erro comum ocorre em provas por casos, aonde nem todos os casos são considerados...

ERROS COMUNS EM PROVAS (2)

- **Exemplo:** O que está errado com esta "prova"?

  "Teorema:" Se x é um número real, então x^2 é um real positivo.

  "Prova:"

  - *sejam:*
    - p_1: "x é positivo"
    - p_2: "x é negativo"
    - q: "x^2 é positivo"
  - *provando* $p_1 \longrightarrow q$:
    - *quando* x *é positivo,* x^2 *é positivo, pois é o produto de dois positivos*
  - *provando* $p_2 \longrightarrow q$:
    - *quando* x *é negativo,* x^2 *é positivo, pois é o produto de dois negativos*

- **"Solução:"** o suposto "teorema" é falso, pois está faltando o caso:
  - p_3: "$x = 0$"

ERROS COMUNS EM PROVAS (3)

- Erro particularmente desagradável: falácia chamada de “usar a questão”.
- Consiste em basear um ou mais passos de uma prova na verdade daquilo que está sendo provado.
  - Ou seja: provar uma declaração usando ela mesma (ou uma outra equivalente a ela).
  - Também chamada de **raciocínio circular**.

ERROS COMUNS EM PROVAS (3)

- **Exemplo:** O argumento a seguir supostamente mostra que n é um inteiro par sempre que n^2 é um inteiro par. Será que está correto??
  - Suponha que n^2 é par.
  - Então $n^2 = 2k$ para algum inteiro k.
  - Seja $n = 2l$ para algum inteiro l.
  - Isto mostra que n é par.

Erros comuns em provas (3)

- **Exemplo:** O argumento a seguir supostamente mostra que n é um inteiro par sempre que n^2 é um inteiro par. Será que está correto??
  - Suponha que n^2 é par.
  - Então $n^2 = 2k$ para algum inteiro k.
  - Seja $n = 2l$ para algum inteiro l.
  - Isto mostra que n é par.

- **Solução:**
  - Nada na prova permite concluir que n possa ser escrito como $2l$.
  - Isto é equivalente ao que está sendo provado ("n é par").
  - *Note que o resultado em si é correto: apenas o método de prova está errado.*

Erros comuns: comentários finais

- Cometer erros em provas é parte do processo de aprendizagem.
- Quando cometer um erro que seja encontrado por outros, certifique-se de não cometê-lo de novo.
- Mesmo matemáticos profissionais cometem erros em provas.
- Diversas provas incorretas enganaram muitas pessoas durante anos antes que erros sutis fossem encontrados nelas...
- Note que não existe um algoritmo para provar teoremas.
- A construção de provas deve ser aprendida através da experiência.
- Ainda veremos muitas provas ao longo deste curso...

NOTA: TIPOS DE TEOREMAS

- **Lema**: teorema simples usado na prova de outros teoremas.
  - Teoremas complicados são mais fáceis de provar quando sub-divididos em uma série de lemas a serem provados individualmente.
- **Corolário**: proposição que é conseqüência imediata de um teorema recém provado.
- **Conjectura**: declaração cujo valor-verdade não é conhecido.
  - Se for encontrada uma prova para a conjectura, ela se torna um teorema.

MÉTODOS DE PROVA

- Final deste item.

- **Dica**: fazer exercícios sobre Métodos de Prova...