

INE5403

FUNDAMENTOS DE MATEMÁTICA DISCRETA PARA A COMPUTAÇÃO

PROF. DANIEL S. FREITAS

UFSC - CTC - INE

1 - LÓGICA E MÉTODOS DE PROVA

1.1) Lógica Proposicional

1.2) Lógica de Primeira Ordem

1.3) Métodos de Prova

PROVA DE TEOREMAS

- Questões importantes na matemática:
 - **quando** é que um argumento matemático está correto?
 - **que métodos** podem ser usados para construir argumentos matemáticos?
- Um **teorema** é uma declaração (conjectura) que se pode mostrar que é verdadeira.
 - Também chamados de “proposições”, “fatos” ou “resultados”.
- Mostra-se que um teorema é verdadeiro com uma **seqüência de declarações** que formam um **argumento** chamado de **prova**.

PROVA DE TEOREMAS & CC

- Os métodos de prova que veremos não servem apenas para provar teoremas matemáticos.
- Também possuem aplicações **diretas** em CC, como, por exemplo:
 - verificar a correção de programas
 - determinar se um sistema operacional é seguro
 - produzir inferências na área de Inteligência Artificial
 - mostrar a consistência das especificações de um sistema computacional
 - verificar a correção de protocolos (de rede, de segurança, etc...)
 - provar resultados teóricos em CC
 - (...)

PROVA DE TEOREMAS

- Objetivo da **Prova** ou **Demonstração**:
 - estabelecer a **verdade de um teorema**
- A construção de provas exige **métodos** que derivem novas declarações a partir daquelas já conhecidas.

TEOREMAS NA LÓGICA PROPOSICIONAL

- Na Lógica Proposicional, teoremas são **tautologias**.
- Teorema mais comum: $p \rightarrow q$
 - p e q são proposições compostas
 - p é a hipótese
 - q é a conclusão
- Técnicas usuais de prova:
 - **tabelas-verdade**
 - inviáveis para muitas variáveis proposicionais
 - **dedução** formal:
 - $p \rightarrow q$ só será teorema se for uma tautologia
 - (sempre que p for V, q também deverá ser)
 - neste caso, é possível **deduzir** q a partir de p

PROVAS

- As declarações utilizadas em uma prova podem incluir:
 - **axiomas** ou **postulados**:
 - proposições que assume-se que são verdadeiras
 - tautologias
 - “verdades evidentes”
 - **teoremas já provados** previamente
 - as **hipóteses** do teorema a ser provado
 - proposições **derivadas das anteriores** através de **regras de inferência**

REGRAS DE INFERÊNCIA

- **Regras de inferência:**
 - modos de “tirar conclusões” a partir de afirmações prévias
 - “amarram” os passos de uma prova
- **Justificam** os passos usados para mostrar que uma conclusão segue logicamente de um conjunto de hipóteses.

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

● Regra de inferência fundamental: **modus ponens**

● baseada na tautologia: $(p \wedge (p \rightarrow q)) \rightarrow q$

● escrita na forma:

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

● *hipóteses em uma coluna e conclusões sob uma barra*

● *o símbolo \therefore significa “portanto”*

● “se é conhecido que tanto uma implicação quanto sua hipótese são V, então a conclusão **desta implicação** é V”.

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

● Exemplo:

- Suponha que sejam verdadeiras:
 - a implicação: “Se fizer sol hoje, eu irei à praia.”
 - e a sua hipótese: “Hoje o dia está ensolarado.”
- Então, por modus ponens, segue que é verdadeira a conclusão da implicação:
 - “Eu irei à praia.”

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

● Exemplo:

- Assuma que é verdadeira a implicação:
 - “Se $n > 3$, então $n^2 > 9$ ”.
- Então, se soubermos que n é maior do que 3, segue, por modus ponens, que:
 - “ n^2 é maior do que 9.”

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

- Tabela a seguir (\Rightarrow):
 - outras importantes regras de inferência da Lógica Proposicional.
- Todas podem ser facilmente verificadas com tabelas-verdade.
- A seguir, exemplos de argumentos que utilizam estas regras.

Regra	Tautologia	Nome
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Adição
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplificação
$\frac{p}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunção
$\frac{p}{\therefore q}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus Ponens
$\frac{\neg q}{\therefore \neg p}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus Tollens
$\frac{p \rightarrow q}{\therefore p \rightarrow r}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Silogismo hipotético
$\frac{p \vee q}{\therefore q}$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Silogismo disjuntivo
$\frac{p \vee q}{\therefore q \vee r}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolução

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

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

- Solução:

- Sejam as proposições:

- p : “Está nublado agora.”

- q : “Está chovendo agora.”

- Então este argumento tem **a forma**:

$$\therefore \frac{p}{p \vee q}$$

- Ou seja, este argumento **usa a regra da adição**. □

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

- **Exemplo 2(/3):** Determine qual regra de inferência é a base para o argumento: “Está nublado e chovendo agora. Portanto, está nublado agora.”

- Solução:

- Sejam as proposições:

- p : “Está nublado agora.”

- q : “Está chovendo agora.”

- Então este argumento tem **a forma**:

$$\therefore \frac{p \wedge q}{p}$$

- Ou seja, este argumento **usa a regra da simplificação**. □

INFERÊNCIAS NA LÓGICA PROPOSICIONAL

- **Exemplo 3(/3):** Determine qual regra de inferência é usada no argumento: “Se chover hoje, então hoje nós não teremos churrasco. Se não tivermos churrasco hoje, então teremos churrasco amanhã. Portanto, se chover hoje, então nós teremos churrasco amanhã.”

- Sejam as proposições:

- p : “Vai chover hoje.”

- q : “Não teremos churrasco hoje.”

- r : “Teremos churrasco amanhã.”

- Então este argumento tem **a forma**:

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

- Ou seja, este é um **silogismo hipotético**.



ARGUMENTOS VÁLIDOS

- Em Lógica Proposicional, um argumento tem uma forma **válida** se:
 - **sempre que** as hipóteses são V, a conclusão **também** é V

- Logo, mostrar que q segue logicamente das hipóteses p_1, p_2, \dots, p_n :

- é o mesmo que mostrar que é verdadeira a implicação:

$$p_1 \wedge p_2 \wedge \dots \wedge p_n \rightarrow q$$

- Quando há várias premissas, **várias regras de inferência** podem ser necessárias para mostrar que um argumento é válido.

- **Nota:**

- cada argumento deve ser mostrado **passo a passo**
- a **razão para cada passo** deve ser declarada **explicitamente**.

ARGUMENTOS VÁLIDOS

- **Exemplo 1(1/2):** **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:** “Nós estaremos em casa no final da tarde.”

- Sejam as proposições:

- 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.”

- Então as hipóteses são: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, e $s \rightarrow t$.

- E a conclusão é simplesmente: t . (\Rightarrow)

ARGUMENTOS VÁLIDOS

🔴 **Exemplo 1(2/2):** (Hipóteses: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$)
(Conclusão: t)

🟢 **Uma** demonstração de que as hipóteses levam à conclusão:

<i>Passo</i>	<i>Justificativa</i>
1. $\neg p \wedge q$	Hipótese
2. $\neg p$	1, Simplificação
3. $r \rightarrow p$	Hipótese
4. $\neg r$	2, 3, Modus Tollens
5. $\neg r \rightarrow s$	Hipótese
6. s	4, 5, Modus Ponens
7. $s \rightarrow t$	Hipótese
8. t	6, 7, Modus Ponens

ARGUMENTOS VÁLIDOS

- **Exemplo 2(1/2):** 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, então eu vou acordar revigorado.”
 - Sejam as proposições:
 - p : “Você me envia um email.”
 - q : “Eu termino de escrever o programa.”
 - r : “Eu vou dormir cedo.”
 - s : “Eu vou acordar revigorado.”
 - Então as hipóteses são: $p \rightarrow q$, $\neg p \rightarrow r$, e $r \rightarrow s$.
 - E a conclusão desejada é: $\neg q \rightarrow s$. (\Rightarrow)

ARGUMENTOS VÁLIDOS

● **Exemplo 2(2/2):** (Hipóteses: $p \rightarrow q$, $\neg p \rightarrow r$, $r \rightarrow s$)
(Conclusão: $\neg q \rightarrow s$)

● A seqüência a seguir mostra que as hipóteses levam à conclusão desejada:

<i>Passo</i>	<i>Justificativa</i>
1. $p \rightarrow q$	Hipótese
2. $\neg q \rightarrow \neg p$	1, Contrapositiva
3. $\neg p \rightarrow r$	Hipótese
4. $\neg q \rightarrow r$	2, 3, Silogismo Hipotético
5. $r \rightarrow s$	Hipótese
6. $\neg q \rightarrow s$	4, 5, Silogismo Hipotético

ARGUMENTOS VÁLIDOS

- Podemos 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. Portanto, o diário desapareceu.” é válida?

● Proposições simples:

● p : “Meu cliente é canhoto.”

● q : “O diário desapareceu.”

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

● Prova:

<i>Passo</i>	<i>Justificativa</i>
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

ARGUMENTOS VÁLIDOS

- **Exemplo 3(b):** Note que a prova do exemplo anterior pode ser **simplificada** com o uso da regra de inferência adequada:

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

- Prova:

<i>Passo</i>	<i>Justificativa</i>
1. p	Hipótese
2. $\neg q \rightarrow \neg p$	Hipótese
3. q	1, 2, Modus Tollens

ARGUMENTOS VÁLIDOS

- Note que a validade da proposição **depende apenas de sua forma lógica**:
 - não tem nada 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:** Verifi que a validade da proposição:

“Se a taxa para importação diminuir, o comércio interno aumentará. Ou 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.”

● Proposições simples:

● p : “A taxa para importação vai diminuir.”

● q : “O comércio interno vai aumentar.”


● r : “A taxa federal de desconto vai diminuir.”

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

● Prova:

<i>Passo</i>	<i>Justificativa</i>
1. $p \rightarrow q$	Hipótese
2. $r \vee \neg q$	Hipótese
3. p	Hipótese
4. q	1, 3, Modus Ponens
5. r	2, 4, Silogismo Disjuntivo

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 eu estava lendo o jornal 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?”

● **Solução:**

● **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) $p \rightarrow q$

(b) $r \vee s$

(c) $r \rightarrow t$

(d) $\neg q$

(e) $u \rightarrow v$

(f) $s \rightarrow p$

ARGUMENTOS VÁLIDOS

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

🔴 Solução:

🟢 Argumento:

(a) $p \rightarrow q$

(b) $r \vee s$

(c) $r \rightarrow t$

(d) $\neg q$

(e) $u \rightarrow v$

(f) $s \rightarrow p$

🟢 Prova:

<i>Passo</i>	<i>Justificativa</i>
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

NOTA 1: USO DE TABELAS-VERDADE

- Note que uma demonstração **por tabela-verdade** seria possível para o exemplo anterior.
- Mas exigiria a análise de $2^7 = 128$ possibilidades. (!!)
- Por isto, é melhor aplicar as regras de inferência (mesmo que seja um processo de tentativa e erro).

NOTA 2: PREMISSAS FALSAS

- Note que um argumento correto pode levar a uma conclusão incorreta se uma ou mais **premissas falsas** forem usadas.

- Exemplo:**

- O argumento:
 - Se $\sqrt{2} > \frac{3}{2}$, então: $(\sqrt{2})^2 > (\frac{3}{2})^2$.
 - Ora, sabemos que: $\sqrt{2} > \frac{3}{2}$.
 - Consequentemente: $2 = (\sqrt{2})^2 > (\frac{3}{2})^2 = \frac{9}{4}$
- tem um formato válido, baseado em Modus Ponens.
- No entanto, a conclusão deste argumento é **falsa**.
- Ocorre que a premissa “ $\sqrt{2} > \frac{3}{2}$ ”, usada neste argumento, é falsa
 - o que significa que a conclusão podia mesmo ser falsa.

NOTA 3: FALÁCIAS (1/4)

- **Nota 3:** Um erro comum em uma demonstração consiste na utilização de **falácias**.
 - Falácias **parecem-se** com regras de inferência, mas são **baseadas em contingências** em vez de tautologias.
- **Exemplo de falácia 1(/2):**
 - A proposição $[(p \rightarrow q) \wedge q] \rightarrow p$ é Falsa quando p é Falso e q é Verdadeiro.
 - Um erro comum consiste em tratá-la como uma tautologia.
 - Raciocínio conhecido como “**falácia de afirmar a conclusão**”.

NOTA 3: FALÁCIAS (2/4)

● **Exemplo:** Será que o argumento a seguir é válido?

“Se você resolver todos os problemas da lista de exercícios, então você vai aprender Matemática Discreta. Você aprendeu Matemática Discreta. Portanto, você resolveu **todos** os problemas da lista de exercícios.”

● **Resposta:**

- Definindo as proposições:

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

q : “Você aprendeu Matemática Discreta.”

- Vemos que o argumento consiste em: se $p \rightarrow q$ e q , então p

- que é a “falácia de afirmar a conclusão”.

- De fato, é plenamente possível que você aprenda MD sem resolver **toda** a lista:

- você pode, por ex., ler o texto, assistir às aulas, resolver alguns (mas não todos) os problemas da lista, resolver **outros** exercícios, etc.

NOTA 3: FALÁCIAS (3/4)

● Exemplo de falácia 2(/2):

- A proposição $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ é Falsa quando p é Falso e q é Verdadeiro.
- Muitos argumentos incorretos a usam como regra de inferência.
 - Raciocínio conhecido como “**falácia de negar a hipótese**”.

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	Nota
$\frac{\forall x P(x)}{\therefore P(c)}$	<i>Instanciação Universal</i>	c específico
$\frac{P(c) \text{ para um } c \text{ arbitrário}}{\therefore \forall x P(x)}$	Generalização Universal	c arbitrário
$\frac{\exists x P(x)}{\therefore P(c) \text{ para algum elemento } c}$	<i>Instanciação Existencial</i>	c específico (mas não conhecido)
$\frac{P(c) \text{ para algum elemento } c}{\therefore \exists x P(x)}$	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:

● $\forall x(F(x) \rightarrow C(x))$

● $F(\text{Manoel})$

● Estabelecendo a conclusão a partir das premissas:

<i>Passo</i>	<i>Justificativa</i>
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

INFERÊNCIAS NA LÓGICA DE PREDICADOS (3/6)

● **Exemplo 2(1/2):** 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:

● $\exists x(P(x) \wedge \neg L(x))$

● Estabelecendo a conclusão a partir das premissas (\Rightarrow)

INFERÊNCIAS NA LÓGICA DE PREDICADOS (4/6)

Exemplo 2(2/2):

- Premissas: $\exists x(T(x) \wedge \neg L(x))$ e $\forall x(T(x) \rightarrow P(x))$
- Conclusão: $\exists x(P(x) \wedge \neg L(x))$
- Estabelecendo a conclusão a partir das premissas:

<i>Passo</i>	<i>Justificativa</i>
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)
9. $\exists x(P(x) \wedge \neg L(x))$	Generalização Existencial de (8)

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 em Matemática **omitem o quantificador** no momento de 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 números reais positivos, então $x^2 > y^2$ ”
 - é: “Para todos os números reais positivos x e y , se $x > y$, então $x^2 > y^2$ ”.
- Além disto, é comum que a lei de generalização universal seja usada sem menção explícita:
 - o primeiro passo da prova envolve a seleção de **um elemento geral** do UD
 - passos subsequentes mostram que este elemento tem a propriedade em questão
 - então, conclui-se que este teorema vale para **todos os elementos** do UD (generalização universal).

PROVANDO TEOREMAS MATEMÁTICOS

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

- Relembrando:

“ $p \rightarrow q$ só não é Verdadeiro quando p é V e q é F.”

- **Nota:**

- 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 $p \rightarrow q$:

1. assumir que p é verdadeiro
2. usar regras de inferência e teoremas já provados para mostrar que q também deve ser V.

● **Exemplo:** prove o teorema: “se n é ímpar, então n^2 é ímpar”

Prova:

- assuma a hipótese: n é ímpar
- então: $n = 2k + 1$, onde k é um inteiro
- segue que:

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

- portanto: n^2 é ímpar
- (1 a mais do que 2 vezes um inteiro)

□

PROVAS INDIRETAS

- **Princípio:** mostrar que a **contrapositiva** de $p \rightarrow q$:

$$\neg q \rightarrow \neg p$$

é Verdadeira, usando outras técnicas de demonstração.

- **Exemplo:** prove o teorema: “se $3n + 2$ é ímpar, então n é ímpar”

Prova:

- assuma que **a conclusão** desta implicação (n é ímpar) é F
- então: $n = 2k$, para algum k
- segue que: $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$
- 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.** □

PROVAS POR VÁCUO

- **Princípio:** $p \rightarrow q$ é Verdadeiro se p é Falso, de modo que:
 - pode-se provar $p \Rightarrow q$ estabelecendo que p é sempre falso.
- Usadas para provar casos especiais de teoremas do tipo $\forall n P(n)$.
- **Exemplo:** mostre que a proposição $P(0)$ é Verdadeira, onde $P(n)$ é “se $n > 1$, então $n^2 > n$ ”.

Prova:

- $P(0)$ é a implicação: “se $0 > 1$, então $0^2 > 0$ ”
- uma vez que a hipótese é Falsa:
 - a implicação $P(0)$ é automaticamente Verdadeira. □

PROVAS TRIVIAIS

- **Princípio:** $p \rightarrow q$ é Verdadeiro 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:** Seja $P(n)$ dada por:

$P(n)$: “se a e b são inteiros positivos com $a \geq b$, então $a^n \geq b^n$ ”.

Mostre que a proposição $P(0)$ é Verdadeira.

Prova:

- $P(0)$ 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 Verdadeira. \square
- Note que a hipótese, “ $a \geq b$ ”, não é necessária.

ESTRATÉGIAS DE PROVA

- Primeiro, tentamos uma prova direta.
- Quando não há modo óbvio de seguir com uma prova direta, 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 número real que não é racional é chamado de **irracional**.

ESTRATÉGIAS DE PROVA

- **Exemplo:** Prove que a soma de dois números racionais é sempre racional.

Prova:

- 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 :
$$r + t = \frac{p}{q} + \frac{u}{v} = \frac{p \cdot v + q \cdot u}{q \cdot v}$$
- como $q \neq 0$ e $v \neq 0$, segue que $q \cdot v \neq 0$
- isto significa que $r + t$ é racional
- (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

Prova:

- 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^2 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:

- assumo 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:** 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, $2b^2 = a^2$
 - o que significa que a^2 é par
 - portanto: **a é par**
- então, $a = 2c$, para algum inteiro c
 - portanto: $2b^2 = 4c^2$ 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.** □

PROVAS POR CONTRADIÇÃO

- Contradição em provas indiretas:
 - mostrar que $p \rightarrow q$ é V demonstrando que $\neg q \rightarrow \neg p$ é V
 - usando contradição:
 - supor que $\neg q$ é V e que $\neg p$ é F
 - usar os passos da prova direta de $\neg q \rightarrow \neg p$ para mostrar que $\neg p$ deve ser V também
 - contradição! $(p \wedge \neg p)$

- **Exemplo 2:** Provar que: “Se $3n + 2$ é ímpar, então n é ímpar.”
 - vamos assumir que $3n + 2$ é ímpar e que n não é ímpar
 - mas já vimos que, se n é par, então $3n + 2$ é par
 - isto contradiz a hipótese de que $3n + 2$ é ímpar, completando a prova □

PROVAS POR CASOS

● **Princípio:** $p_1 \vee p_2 \vee \dots \vee p_n \rightarrow q$ é equivalente a:

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

● 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 $|xy| = |x||y|$.

Prova:

● 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. $p_1 \rightarrow q$ é V, pois:

● $xy \geq 0$ quando $x \geq 0$ e $y \geq 0$

● de modo que: $|xy| = xy = |x||y|$

2. $p_2 \rightarrow q$ é V, pois:

● se $x \geq 0$ e $y < 0$, então $xy \leq 0$

● de modo que: $|xy| = -xy = x \cdot (-y) = |x||y|$

3. $p_3 \rightarrow q$ é V, pois:

● se $x < 0$ e $y \geq 0$, então $xy \leq 0$

● de modo que: $|xy| = -xy = (-x) \cdot y = |x||y|$

4. $p_4 \rightarrow q$ é V, pois:

● se $x < 0$ e $y < 0$, então $xy > 0$

● de modo que: $|xy| = xy = (-x) \cdot (-y) = |x||y|$

□

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.”

Prova:

- 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 $p \rightarrow q$ e $q \rightarrow p$.
- O que já foi feito:
 - slide 43 (provas diretas)
 - slide 49 (estratégias de prova)



PROVANDO EQUIVALÊNCIAS

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

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

- Um modo de provar que eles são mutuamente equivalentes é usar a tautologia:

$$[p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1)]$$

- 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:

- Mostrar que são \forall as implicações: $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$ e $p_3 \rightarrow p_1$

- Mostrando $p_1 \rightarrow p_2$ (prova direta):

- n é par $\Rightarrow n = 2k \Rightarrow n - 1 = 2k - 1 = 2(k - 1) + 1$

- Mostrando $p_2 \rightarrow p_3$ (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 $p_3 \rightarrow p_1$ (prova indireta):

- ou seja, devemos provar que: “se n não é par, então n^2 não é par”

- já provado [slide 43 (provas diretas)] □

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:

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

- Uma vez que conseguimos apresentar um inteiro positivo com a característica descrita, a prova está concluída. □

PROVAS DE EXISTÊNCIA

- **Exemplo:** Mostre que **existem** números irracionais x e y tais que x^y é **racional**.

Solução:

- 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: $\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$

PROVAS DE UNICIDADE

- **Exemplo:** Mostre que todo inteiro tem uma única inversa aditiva.

Solução:

- 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 $p + q = 0$. □

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”.

Solução:

- Possível com os 6 primeiros inteiros positivos:

$$\begin{array}{lll} 1 = 0^2 + 0^2 + 1^2 & 2 = 0^2 + 1^2 + 1^2 & 3 = 1^2 + 1^2 + 1^2 \\ 4 = 0^2 + 0^2 + 2^2 & 5 = 0^2 + 1^2 + 2^2 & 6 = 1^2 + 1^2 + 2^2 \end{array}$$

- **Porém**, não conseguimos fazer o mesmo com 7:
 - os únicos quadrados que poderíamos usar são: 0, 1 e 4 (aqueles que não excedem 7)
 - uma vez que não há maneira de combinar estes 3 números para somar 7, concluimos que 7 é mesmo um contra-exemplo.
- E a declaração acima é falsa. □

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 exemplos 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??

● **Solução:**

- 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.
- A conclusão deve seguir logicamente dos passos que a precederam.
 - 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

1. $a = b$

2. $a^2 = ab$

3. $a^2 - b^2 = ab - b^2$

4. $(a - b)(a + b) = b(a - b)$

5. $a + b = b$

6. $2b = b$

7. $2 = 1$

Justificativa

Dado

Multiplicando os 2 lados de (1) por a

Subtraindo b^2 dos 2 lados de (2)

Fatorando ambos os lados de (3)

Dividindo ambos os lados de (4) por $a - b$

Substituindo a por b em (5) (pois $a = b$)

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

1. $a = b$

2. $a^2 = ab$

3. $a^2 - b^2 = ab - b^2$

4. $(a - b)(a + b) = b(a - b)$

5. $a + b = b$

6. $2b = b$

7. $2 = 1$

Justificativa

Dado

Multiplicando os 2 lados de (1) por a

Subtraindo b^2 dos 2 lados de (2)

Fatorando ambos os lados de (3)

Dividindo ambos os lados de (4) por $a - b$

Substituindo a por b em (5) (pois $a = b$)

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 (1)

● Exemplo 2: O que está errado com esta “prova”?

“Teorema:” Se n^2 é positivo, então n é positivo.

“Prova:”

- *suponha que n^2 é positivo,*
- *uma vez que a implicação “Se n é positivo, então n^2 é positivo” é verdadeira, podemos concluir que n é positivo.*

● “Solução:”

- Falácia de afirmar a conclusão:
 - sejam $P(n)$: “ n é positivo” e $Q(n)$: “ n^2 é positivo”
 - esta “prova” conclui $P(n)$ a partir de $Q(n)$ e $\forall n(P(n) \rightarrow Q(n))$
- Contra-exemplo: $n = -1$.

ERROS COMUNS EM PROVAS (1)

● Exemplo 3: O que está errado com esta “prova”?

“Teorema:” Se n não é positivo, então n^2 não é positivo.

“Prova:”

- *suponha que n não é positivo,*
- *uma vez que a implicação “Se n é positivo, então n^2 é positivo” é verdadeira, podemos concluir que n^2 não é positivo.*

● “Solução:”

- Falácia de negar a hipótese:
 - sejam $P(n)$: “ n é positivo” e $Q(n)$: “ n^2 é positivo”
 - esta “prova” conclui $\neg Q(n)$ a partir de $\neg P(n)$ e de $\forall n(P(n) \rightarrow Q(n))$
- Contra-exemplo: $n = -1$.

ERROS COMUNS EM PROVAS (2)

- Um erro comum de assumir hipóteses não justificadas 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 $p_1 \rightarrow q$:*

- *quando x é positivo, x^2 é positivo, pois é o produto de dois positivos*

- *provando $p_2 \rightarrow q$:*

- *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.

- **Solução:**

- Nada na prova permite concluir 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 consequência 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...