Escola de Engenharia de São Carlos
Universidade de São Paulo

TÉCNICAS DE DEMONSTRAÇÃO

Josimeire Maximiano dos Santos

Sistemas Lineares

EESC – USP 2017

Um pouco de Lógica...

Teoremas e Demonstrações Informais

- Os argumentos lógicos formais tem a forma $P \rightarrow Q$, onde P e Q podem representar proposições compostas.
  - Temos que demonstrar a validade do argumento.
- As vezes temos que provar argumentos que não são universalmente verdadeiros, sendo apenas em certos contextos.
  - Temos que provar que, se P é verdadeiro nesse contexto, Q também o é.
- Se pudermos provar essa condição, então $P \rightarrow Q$ torna-se um **teorema** sobre aquele assunto.
- Os teoremas podem ser enunciados e demonstrados de maneira menos formal do que usando argumentos da lógica formal.

Conectivos lógicos

- Conjunção ∧ (“e”)
- Disjunção ∨ (“ou”)
- Condicional →
- Negação ~

A	B	A ∧ B	A ∨ B	A → B	A ↔ B	~A
V	V	V	V	V	V	F
V	F	F	V	F	F	
F	V	F	V	V	F	V
F	F	F	F	V	V	

Tabela 1 – Resumo dos valores lógicos para todos os conectivos lógicos.

Expressão em português	Conectivo lógico
e; mas; também; além disso	$A \land B$
Ou	$A \lor B$
Se A, então B. A implica B. A, logo B. A só se B; A somente se B. B segue de A. A é uma condição suficiente para B; basta A para B. B é uma condição necessária para A.	$A \rightarrow B$
A se e somente se B. A é uma condição necessária e suficiente para B.	$A \leftrightarrow B$
Não A É falso que A … Não é verdade que A …	$\sim A$

Tabela 2 – Expressões comuns em português associadas a diversos conectivos lógicos.

Algumas definições...

- **Proposição:** conjunto de palavras ou símbolos que exprimem uma ideia com sentido completo e que se expressa através de sentenças, verdadeiras ou falsas.

- **Teorema:** proposição que é garantida por uma prova.

- Todo teorema é uma implicação da forma: **hipótese $\Rightarrow$ tese**

- Todo teorema cujo recíproco também é verdadeiro é uma equivalência:

hipótese $\Leftrightarrow$ tese

Algumas definições…

- **Corolário:** teorema que segue como consequência natural de um outro.

- **Lema:** teorema preparatório para a demonstração de um outro teorema.

- **Axioma:** proposição que se assume como verdadeira e que não precisa de prova.

- **Conjectura:** proposição que ainda não foi provada e nem refutada.

Provar ou Não Provar

- Ex. 01: Para um inteiro positivo n, **n!** é definido com sendo n(n-1)(n-2)...1. Prove ou encontre um contra-exemplo para a conjectura "para todo inteiro positivo **n, n! ≤ n²**.
- Testa-se alguns casos:

n	**n!**	**n^2**	**$n! \leq n^2$**
1	1	1	V
2	2	4	V
3	6	9	V

Os casos verdadeiros não provam a validade

- Até agora a conjectura foi sempre verdadeira. O caso seguinte:

n	**n!**	**n^2**	**$n! \leq n^2$**
4	24	16	F

Esse caso é suficiente para provar a falsidade

Demonstração exaustiva

- Encontrar um contra-exemplo pode não ser simples. Então o caminho para provar uma conjectura é usar métodos para demonstrá-la.
- Quando temos uma conjectura sobre uma coleção finita, ela pode ser provada verificando se ela é válida para cada elemento da coleção.
- Uma **demonstração por exaustão** significa que foram exauridos todos os casos possíveis.
- Ex.02: Provar a conjectura: "Se um inteiro entre 1 e 20 é divisível por 6, então também é divisível por 3."
  - Como existe um número finito de casos, a conjectura pode ser provada mostrando que é verdadeira para todos os inteiros de 1 a 20, por exemplo, usando uma tabela.

Demonstração exaustiva

- Ex.03: Provar a conjectura: "Para qualquer inteiro **positivo menor ou igual a 5**, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro."
- Ex.04: Dê um contra-exemplo para a conjectura: "Para qualquer inteiro positivo, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro."

Demonstração Direta

- Uma demonstração ou prova é dita direta quando pressupões verdadeira a hipótese e, a partir desta, prova ser verdadeira a tese.
- Ex.05: Considere a seguinte conjectura: "A soma de dois números pares é um número par". Podemos efetuar a demonstração direta a partir dos seguintes passos:
  1. Reescrevendo na forma $P \rightarrow Q$: Se n e m são dois números pares quaisquer, então n+m é um número par.
  2. Lembrando que um numero par n pode ser definido por n=2r, onde r é um numero inteiro qualquer.
  3. Se n e m são pares, então existem r, s tais que: n=2r e m=2s, então: n+m=2r+2s => 2(r+s), como r+ s é um número natural, logo, n+m é um número par.

- Ex.06: Considere a seguinte conjectura: “O produto de dois números inteiros pares é um número par”. Faça a demonstração direta (informal) da mesma.

Contraposição

- Se a demonstração direta $P \to Q$, não foi atingida, pode-se tentar algumas variantes da técnica de demonstração direta.
- Se puder provar o teorema $Q' \to P'$, pode-se concluir que $P \to Q$, usando a tautologia $(Q' \to P') \to (P \to Q)$.
  - $Q' \to P'$ é a contrapositiva de $P \to Q$
- A técnica de provar $P \to Q$ através de uma demonstração direta de $Q' \to P'$ é chamada de **demonstração por contraposição.**
  - A tautologia $(Q' \to P') \to (P \to Q)$ vem da regra de inferência onde $P \to Q$ pode ser deduzida de $Q' \to P'$.

Contraposição

- Ex. 07: Prove o seguinte teorema ($n \in \mathbf{N}$):

$$n! > (n+1) \rightarrow n>2$$

- Por equivalência, pode-se demonstrar por contraposição, que:

$$n \leq 2 \rightarrow n! \leq (n+1)$$

- Testando a proposição para n=0, 1 e 2.

n	**n!**	**n+1**
0	1	1
1	1	2
2	2	3

Demonstração por absurdo

- Quando a demonstração de $P \rightarrow Q$, consiste em supor a hipótese P, supor a negação de Q e concluir uma contradição (em geral $Q \wedge Q'$), a demonstração é chamada de **por absurdo.**
- Lembrando que uma contradição é uma fbf cujo valor lógico é sempre Falso. Ela pode ser denotada por 0.
  - Por exemplo, a fbf $A \wedge A'$ tem sempre valor falso.
- Para provar $P \rightarrow Q$, podemos levar em conta a seguinte fbf: $(P \wedge Q' \rightarrow 0) \rightarrow (P \rightarrow Q)$.
  - Construindo a tabela verdade, concluímos a que a fbf é uma tautologia.
- Então se provarmos que $P \wedge Q' \rightarrow 0$, isto implicará em $P \rightarrow Q$

***fbf**: fórmula bem formulada, ié, expressão válida. Vem do inglês *well-formed formula*, com abreviação *wff, utilizada em alguns textos*.

- Portanto, na demonstração por absurdo, assume-se o oposto do que se quer provar, ao chegar a uma contradição, a prova é finalizada.
- Ex.10: Demonstrar por absurdo a proposição: "Se um número somado a ele mesmo é igual a ele mesmo, então esse número é 0".
  - Representando x por um numero qualquer.
  - A hipótese é $x+x=x$ e a conclusão é $x=0$.
  - Para demonstrar por absurdo, supomos que $x+x=0$ e $x\neq 0$. Então $2x=x$ e $x\neq 0$.
  - Dividindo ambos os lados da eq. $2x=x$, obtem-se $2=1$, uma contradição, que buscamos.
  - Portanto, $(x+x=x) \rightarrow (x=0)$

Resumo das Técnicas de Demonstração

Técnica	Abordagem para provar $P \rightarrow Q$	Observações
Exaustão	Demonstre $P \rightarrow Q$ para todos os casos possíveis	Pode ser usada para provar um número finito de casos.
Direta	Suponha P, deduza Q	Abordagem padrão – o que se deve tentar em geral.
Contraposição	Suponha Q′, deduza P′	Use a técnica se Q′ parece dar mais munição que P.
Por Absurdo	Suponha $P \wedge Q'$, deduza uma contradição	Use essa técnica quando Q disser que alguma coisa não é verdade.

Para complementar...

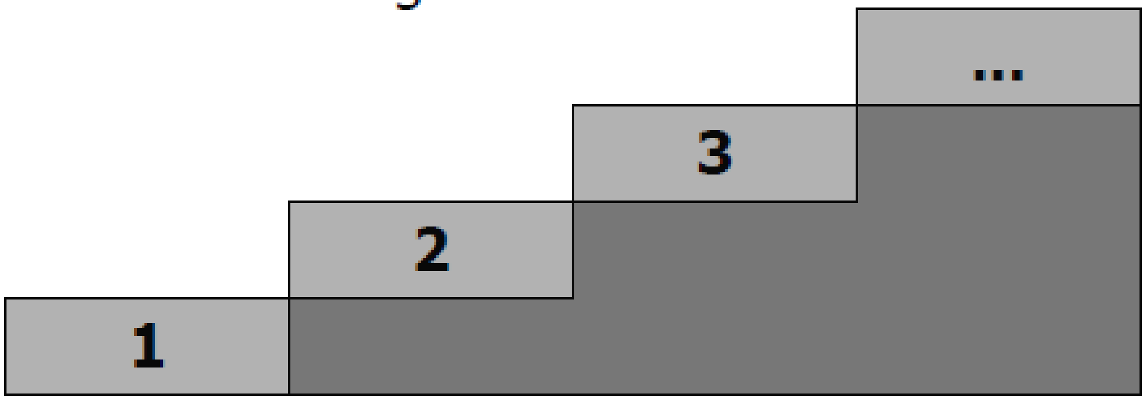
INDUÇÃO MATEMÁTICA

PRIMEIRO PRINCÍPIO DE INDUÇÃO

PRIMEIRO PRINCÍPIO DE INDUÇÃO

- Imagine que você está subindo uma escada infinitamente alta. Como você será capaz de saber se será capaz de chegar a um degrau arbitrariamente alto?
  - Você pode inicialmente fazer as seguintes hipóteses sobre a sua capacidade de subir:
  1. Você consegue alcançar o primeiro degrau.
  2. Uma vez chegado a um degrau, você sempre será capaz de chegar ao próximo.
  - Se a proposição 1 e o condicional 2 são verdadeiros, então, pela proposição 1, você consegue chegar no primeiro degrau e, portanto, pela 2, consegue chegar no segundo. Novamente pela 2, consegue chegar no terceiro.
  - Mais uma vez, pela 2, chega no quarto degrau e assim por diante.
  - Você poderá subir tão alto quanto quiser.

- Nesse caso, ambas as hipóteses são necessárias. Se apenas a primeira fosse V, não teríamos a garantia de passar do primeiro degrau.
  - Se apenas a 2ª fosse V, poderíamos não ser capazes de começar nunca.
- Numerando os degraus...



- Seja uma propriedade de que cada número que identifica o degrau possa ter.
  - Ao invés de chegar a um degrau arbitrário, podemos buscar um número inteiro positivo que tenha essa propriedade.

- Usando a notação P(n) para dizer que o inteiro positivo n tem a propriedade P.
- Por analogia, vamos usar a mesma "técnica" usada para subir a escada, para provar que, qualquer que seja o inteiro positivo n, temos P(n).
  - Precisamos provar as proposições:
  1. P(1) - (1 tem a propriedade P)
  2. Para qualquer inteiro positivo k, $P(k) \rightarrow P(k+1)$ – Se qualquer número tem a propriedade P, o próximo também tem.
- Se pudermos provar ambas as proposições 1 e 2, então P(n) é válida para qualquer inteiro positivo n.
- O fundamento para argumentos desse tipo é o **primeiro princípio de indução matemática.**

Primeiro Princípio de Indução

1. **P(1)**
2. **$(\forall k)$ [P(k) verdade $\rightarrow$ P(k+1) verdade]**

P(n) é verdade para todo inteiro positivo n

- O primeiro princípio de indução matemática é um condicional, com uma conclusão na forma "P(n) é verdade para todo inteiro positivo n".
  - A técnica da indução se mostra mais apropriada para provarmos que alguma coisa é verdade para todo inteiro positivo n (conjunto dos números naturais).

1. $P(1)$
2. $(\forall k)$ [$P(k)$ verdade $\rightarrow$ $P(k+1)$ verdade]

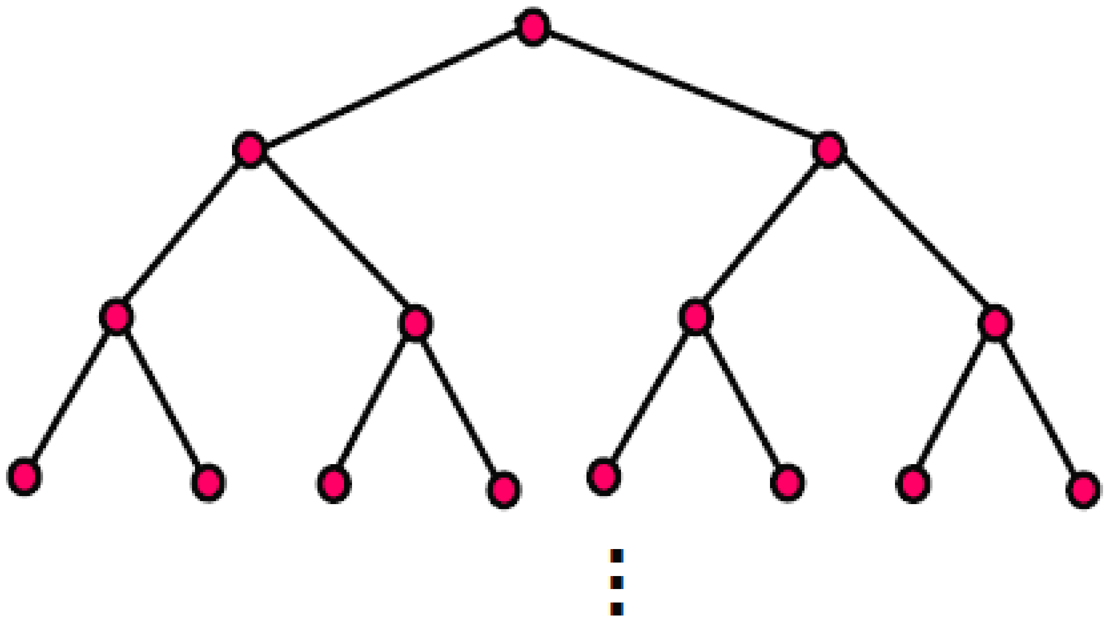
- Para mostrar que a conclusão dessa condicional é verdadeira, precisamos provar que as hipóteses 1 e 2 são.
  - Para provar a proposição 1, basta mostrar que o número 1 tem a propriedade P, o que pode ser trivial (**Base da Indução**).
  - A proposição 2 é um condicional que tem que ser válido para todo k (**Passo da Indução**).
  - Para provar essa condicional, suponha que P(k) (**Hipótese da Indução**) é verdade para um inteiro positivo k e mostre que, baseado nesta hipótese, que p(k+1) é verdade.

Primeiro Princípio de Indução - Resumo

1. Passo 1 – Prove a base da indução P(1) (ou o menor inteiro positivo em questão.
2. Passo 2 – Suponha P(k)
3. Passo 3 – Prove P(k+1)

Demonstração por Indução Matemática

- Ex. 01:Suponha a árvore genealógica de uma família cuja característica fundamental é que cada casal tem sempre dois filhos e que cada um desses filhos também tem dois filhos. A árvore é ilustrada abaixo:



Geração	Descendentes
1	$2^1=2$
2	$2^2=4$
3	$2^3=8$
...	...

- Há de se perceber que a geração n contém 2^n descendentes. Precisamos demonstrar essa propriedade.
- Formalmente, se denotarmos por P(n) o número de descendentes em cada geração, nossa conjectura é que:

$$P(n) = 2^n$$

- Vamos usar a indução para provar que a conjectura está correta.

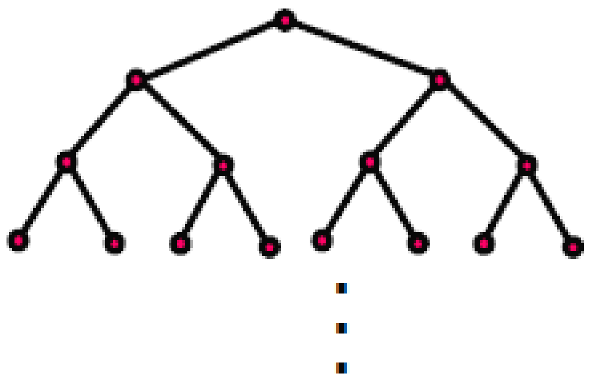
1. O passo básico é estabelecer P(1), que é a equação:

$$P(1) = 2^1 = 2$$

2. Isso é verdadeiro pois o primeiro elemento da genealogia teve 02 filhos.
3. Supondo agora que a conjectura está correta para uma geração arbitrária k, $k \geq 1$:

$P(k) = 2^k$ Vamos mostrar que $P(k+1) = 2^{k+1}$

- Vamos mostrar que $P(k+1) = 2^{k+1}$
- Nessa família, cada descendente tem 2 filhos, de modo que o número de descendentes na geração k+1 será o dobro da geração k.
  - Ou seja $P(k+1) = 2P(k)$
- Pela hipótese de indução:



$$P(k) = 2^k$$

$$\boxed{P(k+1) = 2P(k) = 2(2^k) = 2^{k+1}}$$

$$\boxed{\text{De fato, } P(k+1) = 2^{k+1}}$$

- Ex. 02: Sejam as seguintes definições:

$$2^0 = 1 = 2^1 - 1$$
$$2^0 + 2^1 = 1 + 2 = 3 = 2^2 - 1$$
$$2^0 + 2^1 + 2^2 = 1 + 2 + 4 = 7 = 2^3 - 1$$
$$2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = 15 = 2^4 - 1$$

- No exemplo acima o padrão mais geral parece com:

$$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$$

- Mas, não podemos afirmar que este padrão será sempre verdadeiro para todos os valores de *n* a menos que provemos.
- Prove que para todo número inteiro positivo n,

$$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1.$$

- Ex. 02: $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$.
- Pelo princípio da indução:

$P(1)$ é a equação $1 + 2 = 2^{1+1}$ ou $3=2^2-1$ (**base da indução**)

- Supondo $P(k)$ como **hipótese de indução**:

$1 + 2 + 2^2 + \ldots + 2^k = 2^{k+1} - 1$

- Provar que $P(k+1)$ é verdadeira:

$1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} = 2^{k+1+1} - 1$

Considerando a soma à esquerda $\underbrace{1 + 2 + 2^2 + \ldots + 2^k} + 2^{k+1}$

Usando a hipótese de indução: $1 + 2 + 2^2 + \ldots + 2^k = 2^{k+1} - 1$

em $p(k+1)$:

$= 2^{k+1} - 1 + 2^{k+1}$

$=2(2^{k+1}) - 1$

$= 2^{k+1+1} - 1$

Portanto $P(k+1)$: $1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} = 2^{k+1+1} - 1$

- Ex. 03: Demonstre que, para qualquer n, $2^n > n$.

1. Base da indução: $P(1) = 2^1 = 2$, então $2 > 1$ (verdadeira)
2. Hipótese da indução: supondo que para algum k inteiro positivo, $P(k)$: $2^k > k$ é verdadeira.
3. Passo da indução: Provar que para $P(k+1)$: $2^{k+1} > k+1$ é verdadeira.
4. Como $P(k)$: $2^k > k$ e $P(k+1)$: $2^{k+1} > k+1$, então, à esquerda da desigualdade temos que:

$2^{k+1} = 2^k.2^1$

Pela hipótese de indução $2^k > k$ (x2) $= 2^k.2^1 > k.2$

$2^{k+1} > k.2$, como $k.2 = k+k$, e $k+k \geq k+1$,

Ou seja,

$\mathbf{2^{k+1} > k+1}$

- O primeiro passo de uma demonstração por indução não é necessariamente obrigado ser P(1). Podemos começar por P(0) ou por outro valor.
  - O mesmo princípio se aplica, independente do grau que se começa a subir.
- Ex. 04: Prove que $n^2 > 3n$, para $n \geq 4$.
  - Nesse caso, é melhor começar a base da indução em P(4).

1. Base da indução - P(4): $4^2 > 3(4)$ é verdadeira
2. Hipótese da indução - $\mathbf{k^2 > 3k}$, para $k \geq 4$
3. Queremos mostrar que $\mathbf{(k+1)^2 > 3(k+1)}$

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

$> 3k + 2k + 1$ (pela hipótese da indução)

$\geq 3k + 8 + 1$ (pois $k \geq 4$)

$> 3k + 3 = 3(k+1)$

Portanto P(k+1): $(k+1)^2 > 3(k+1)$

- Ex. 05: Prove por indução que a soma dos n primeiros números naturais é dada por $P(n) = n\,(n+1)\,/\,2$
- Temos: $P(n) = 1 + 2 + 3 + 4 + \ldots + n = n(n + 1)\,/\,2$

1. Base da indução: $P(1) = 1\,(1 + 1)\,/\,2 = 1$
2. Hipótese da indução: $P(k)$: $1 + 2 + 3 + \ldots + k = k(k + 1)/2$
3. Devemos mostrar quer

$P(k+1) = 1+2+3+ \ldots + k + (k + 1)=[(k+1)(k+1+1)]/2$

Usando a hipótese de indução, vamos substituir na expressão acima, o valor de P(k), teremos:

$P(k + 1) = k\,(k + 1)\,/\,2 + (k + 1) =[(k+1)(k+1+1)]/2$

Desenvolvendo o lado esquerdo, fica:

$P(k +1) = [k(k+1)/2]+(k+1) = [k\,(k + 1) + 2(k + 1)]\,/\,2$

$= [(k + 1)\,(k + 2)]\,/\,2 = (k+1)\,[(k+1) + 1]\,/\,2$

que é a mesma fórmula para (k+1).

Logo, $P(n) = n\,(n+1)\,/\,2$ é verdadeira para todo n natural.

Referências

BISPO, C. A. F.; CASTANHEIRA, L. B.; SOUZA FILHO, O. M. **Introdução à Lógica Matemática**. Cengage Learning, 2011.

GERSTING, J. L. **Fundamentos Matemáticos para a Ciência da Computação – Um tratamento moderno de Matemática Discreta**. 5ª Edição. Rio de Janeiro: LTC, 2008.

IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar,** vol. 1. 9ª edição, Editora Atual. São Paulo, 2013.