



Matemática Discreta 1

Princípio da Indução Matemática

AULA 10

Professor: Luiz Augusto Laranjeira

luiz.laranjeira@gmail.com

5- Indução

Motivação

Imagine que Jorge está subindo uma escada infinitamente alta. Como poderá saber se conseguirá alcançar um degrau arbitrariamente alto?

Façamos as seguintes premissas:

- 1) Jorge pode subir no 1º degrau.
- 2) Uma vez que Jorge esteja em um degrau qualquer ele sempre consegue subir para o degrau seguinte.

Se estas duas premissas são verdadeiras pode-se demonstrar que Jorge conseguirá alcançar qualquer degrau da escada.

5- Indução

Seja $P(n)$ uma propriedade sobre os valores de n pertencentes a um domínio D , onde $D \subseteq \mathbb{N}$.

Para se provar que $P(n)$ é válido para qualquer n pertencente a D precisamos demonstrar que:

1) $P(n_1) \equiv V$ (n_1 tem a propriedade P , onde n_1 é o primeiro elemento de D)

2) $\forall n_k \in D, P(n_k) \rightarrow P(n_{k+1})$

Se um número (elemento) do domínio D tem a propriedade P , também a terá o próximo número (elemento) deste domínio



Indução

(Enunciado Alternativo)

- 1) $P(1) \equiv V$ (1 tem a propriedade P, onde 1 é o primeiro número de D)
- 2) $\forall k \in D, P(k) \rightarrow P(k+1)$
Se um número (elemento) do domínio D tem a propriedade P, também a terá o próximo número (elemento)



Princípio da Indução Matemática (PIM)

Se 1) $P(1) \equiv V$ ($P(1)$ é verdadeira)
 2) $(\forall k, k \geq 1) [P(k) \equiv V \Rightarrow P(k+1) \equiv V]$
Então 3) $P(n) \equiv V$ para $\forall n, n \in \mathbb{N}, n \geq 1$ (isto é, $D = \mathbb{N}$)

Princípio da Indução Forte (PIF)

Se 1) $P(1) \equiv V$ ($P(1)$ é verdadeira)
 2) $(\forall k, k \geq 1) [P(r) \equiv V \text{ (para } \forall r, 1 \leq r \leq k) \Rightarrow P(k+1) \equiv V]$
Então 3) $P(n) \equiv V$ para $\forall n, n \in \mathbb{N}, n \geq 1$ (isto é, $D = \mathbb{N}$)

$PIM \Rightarrow PIF \Rightarrow PBO(*) \Rightarrow PIM$

Estes princípios são, portanto equivalentes!

(*) Princípio da Boa Ordenação (PBO): toda coleção de números inteiros positivos que contenha pelo menos um elemento tem um mínimo.



Teorema: $D \subset \mathbb{N}$ satisfaz o PBO se todo $A \subset D \subset \mathbb{N}$, $A \neq \emptyset$, tem um **menor elemento**, ou seja, $\exists a \in A$ tal que $\forall x, x \in A, x \geq a$.

Demonstração:

Se $1 \in A$ então 1 é o menor elemento de A , pois $1 \leq n$ para $\forall n, n \in \mathbb{N}$ **cqd**

Para $1 \notin A$, definamos o conjunto $X = \{x \in \mathbb{N} \mid \forall k, k \in A, k > x\}$, $1 \in X$.

Se fosse verdade que $\forall x \in X \Rightarrow (x+1) \in X$ (por indução), teríamos $X = \mathbb{N}$ e $A = \emptyset$.

Mas isto não é verdade pois, por definição, $\forall k \in A$, temos $k \notin X$, e $A \neq \emptyset$.

Logo, existe (pelo menos um) $m \in X$ tal que $(m+1) \notin X$. Daí:

$$(m+1) \notin X \Rightarrow (m+1) \in A \quad (1)$$

$$m \in X \Rightarrow \forall x, x \in A, x > m \quad (2)$$

$$k \in A \Rightarrow k > m \quad (3)$$

Finalmente, de (1) e (3) vem que $k \in A \Rightarrow k > m \Rightarrow k \geq (m+1)$

Fazendo $a = (m+1)$ temos que para $x \in A \Rightarrow x > m, x \geq a$

cqd



Isto é óbvio, pois a hipótese do PIM é mais fraca do que a hipótese do PIF ou, em outras palavras, a hipótese do PIF inclui a hipótese do PIM (e ainda tem condições adicionais).



Proposição: seja um conjunto A , $A \subset \mathbb{N}$, $A \neq \emptyset$, que satisfaz o Princípio da Indução Forte, então A satisfaz o Princípio da Boa Ordenação. Em outras palavras A tem um **mínimo**.

Demonstração:

Vamos supor que A não tenha um mínimo ($1 \notin A$, senão ele seria o mínimo). Seja $\bar{A} = \mathbb{N} - A$. Aplicando a hipótese 1 do PIF sobre \bar{A} temos que $1 \in \bar{A}$.

Supomos que $[1, x] \subseteq \bar{A}$. Então $\forall z \in A$, $z > x$ e, portanto, $z \geq x+1$. Daí, como $x+1 \in A$, teríamos que $x+1$ é o mínimo de A , o que é absurdo pois supusemos que A não tinha um mínimo. Portanto é necessário que $x+1 \in \bar{A}$.

Daí, aplicando a hipótese 2 do PIF a \bar{A} concluiríamos que $\bar{A} = \mathbb{N}$ e que $A = \emptyset$, o que é uma contradição, já que $A \neq \emptyset$. Então, A tem que ter um mínimo. **cqd**



Proposição: seja um conjunto $D \subset \mathbb{N}$, $D \neq \emptyset$, que satisfaz o Princípio da Boa Ordenação, então D satisfaz o Princípio da Indução Matemática, isto é:
Se $1 \in D$ ($1 = \min D$) e $\forall x \in \mathbb{N}$, $x \in D \Rightarrow x+1 \in D$, então $D = \mathbb{N}$.

Demonstração (por contradição):

Seja $T \subseteq D$ tal que:

- (1) $1 \in T$ ($1 = \min T$);
- (2) para $\forall x \in D$, $x \in T$
- (3) para $\forall x \in D$, $x \in T \Rightarrow x+1 \in T$.

Suponhamos porém que $T \neq D$ (T não satisfaz o PIM), isto é, \exists o conjunto $\bar{T} = D - T$, $\bar{T} \neq \emptyset$. Como $\bar{T} \subseteq D$, pelo PBO existe $m \in \bar{T}$, tal que $m = \min$ de \bar{T} .

É claro que $m \neq 1$, pois $1 \in T$. Dado que $m > 1$, então $m \geq 2$ e $m-1 \geq 1$. Como $m-1 < m$, $m-1 \notin \bar{T}$. Logo, $m-1 \in T$.

Pela proposição (3) temos que $(m-1)+1 \in T$, ou seja, $m \in T$. Chegamos a uma contradição pois, por hipótese, $m \in \bar{T}$ (isto é $m \notin T$). Logo, $\bar{T} = \emptyset$ e T satisfaz o PIM. Daí temos que $T = D = \mathbb{N}$. **cqd**



PBO \Rightarrow PIM **Verdadeiro**

PBO **Verdadeiro**

Então PIM **Verdadeiro**



Demonstrações por Indução

O que se quer demonstrar é $P(n) \equiv V$, onde $n \in D \subset \mathbb{N}$

- 1) Mostrar que $P(1) \equiv V$ **(base)**
- 2) Assumir que $P(k) \equiv V$ **(hipótese indutiva)**
- 3) Provar que $P(k) \rightarrow P(k+1)$ **(passo indutivo)**

Então, $P(k) \equiv V$ para $\forall k \in D$, $D = \mathbb{N}$



Exemplo 1

Prove que, dado um conjunto S com n elementos, o conjunto das partes de S , $\mathcal{P}(S)$, terá 2^n elementos.

Exemplo de conjunto $\mathcal{P}(S)$, o conjunto das partes do conjunto S :

$$\begin{aligned} S &= \{1, 2, 3\} & \mathcal{P}(S) &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} \\ \mathfrak{N}_{\mathcal{P}}(\mathcal{P}(S)) &= 2^n & \text{para } n = 3, \mathfrak{N}_{\mathcal{P}}(\mathcal{P}(S)) &= 2^3 = 8 \end{aligned}$$

$\mathcal{P}(S)$, o conjunto das partes do conjunto S (S tem n elementos)

$\mathfrak{N}_{\mathcal{P}}(\mathcal{P}(S)) = 2^n = \text{número de elementos do conjunto } \mathcal{P}(S)$



Exemplo 1 (cont.)

Prove que, dado um conjunto S com n elementos, o conjunto das partes de S , $\mathcal{P}(S)$, terá $\mathfrak{N}_p = 2^n$ elementos.

- (1) Para $n = 0$ ($S = \emptyset$), $\mathfrak{N}_p = 2^0 = 1$ $\mathcal{P}(S) = \{\emptyset\}$
Para $n = 1$, $\mathfrak{N}_p = 2^1 = 2$ $\mathcal{P}(S) = \{\emptyset, \{e_1\}\}$
- 2) Assumimos que para $n = k$, $\mathfrak{N}_p = 2^k$
- 3) Precisamos provar que para $n = k+1$, $\mathfrak{N}_p = 2^{k+1}$

Exemplo 1 (cont.)

$$\begin{array}{ll} (1) \text{ Para } n = 0 \ (S = \emptyset), \mathfrak{U}_p = 2^0 = 1 & \mathcal{P}(S) = \{\emptyset\} \\ \text{Para } n = 1, \mathfrak{U}_p = 2^1 = 2 & \mathcal{P}(S) = \{\emptyset, \{e_1\}\} \end{array}$$

2) Assumimos que, para $n = k$, $\mathfrak{U}_p = 2^k$

3) Precisamos provar que, para $n = k+1$, $\mathfrak{U}_p = 2^{k+1}$

O Triângulo de Pascal nos dá: $2^n = 1 + C_{n,1} + C_{n,2} + \dots + C_{n,n-1} + C_{n,n}$

De (2) vem: $\mathfrak{U}_p(k) = 2^k \quad (n = k)$

$$\mathfrak{U}_p(k) = 2^k = 1 + C_{k,1} + C_{k,2} + \dots + C_{k,k-1} + C_{k,k}$$

$$\mathfrak{U}_p(k+1) \quad (n = k+1)$$

$$\mathfrak{U}_p(k+1) = 1 + C_{k+1,1} + C_{k+1,2} + \dots + C_{k+1,k-1} + C_{k+1,k} + C_{k+1,k+1}$$

Exemplo 1 (cont.)

O Triângulo de Pascal nos dá: $2^k = 1 + C_{k,1} + C_{k,2} + \dots + C_{k,k-1} + C_{k,k}$

$$\mathfrak{N}_p(k) = 2^k = 1 + C_{k,1} + C_{k,2} + \dots + C_{k,k-1} + C_{k,k}$$

$$\mathfrak{N}_p(k+1) \quad (n = k+1)$$

$$\mathfrak{N}_p(k+1) = 1 + C_{k+1,1} + C_{k+1,2} + \dots + C_{k+1,k-1} + C_{k+1,k} + C_{k+1,k+1}$$

Usando a fórmula de Pascal: $C_{k+1,m} = C_{k,m} + C_{k,m-1}$

$$\mathfrak{N}_p(k+1) = 1 + C_{k,1} + 1 + C_{k,2} + C_{k,1} + \dots + C_{k,k-1} + C_{k,k-2} + C_{k,k} + C_{k,k-1} + C_{k+1,k+1}$$

E como $C_{k,k} = C_{k+1,k+1} = 1$, para $\forall k \in \mathbb{N}$, vem:

$$\mathfrak{N}_p = 1 + C_{k,1} + 1 + C_{k,2} + C_{k,1} + \dots + C_{k,k-1} + C_{k,k-2} + C_{k,k} + C_{k,k-1} + C_{k,k}$$

$$\mathfrak{N}_p = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} \quad \text{cqd}$$

Exemplo 1 (cont.)

$$\mathfrak{N}_p(k+1) = 1 + C_{k+1,1} + C_{k+1,2} + \dots + C_{k+1,k-1} + C_{k+1,k} + C_{k+1,k+1}$$

Usando a fórmula de Pascal: $C_{k+1,m} = C_{k,m} + C_{k,m-1}$

$$\mathfrak{N}_p(k+1) = 1 + C_{k,1} + 1 + C_{k,2} + C_{k,1} + \dots + C_{k,k-1} + C_{k,k-2} + C_{k,k} + C_{k,k-1} + C_{k+1,k+1}$$

$$C_{k+1,1} = C_{k,1} + C_{k,1-1} = C_{k,1} + C_{k,0} = C_{k,1} + 1$$

E como $C_{k,k} = C_{k+1,k+1} = 1$, para $\forall k \in \mathbb{N}$, vem:

$$\mathfrak{N}_p = 1 + C_{k,1} + 1 + C_{k,2} + C_{k,1} + \dots + C_{k,k-1} + C_{k,k-2} + C_{k,k} + C_{k,k-1} + C_{k,k}$$

$$\mathfrak{N}_p = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} \quad \text{cqd}$$



Exemplo 2

Provar que $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$, $n \geq 1$



Exemplo 2

Provar que $1 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$, $n \geq 1$

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

$$3 = 2^2 - 1 = 4 - 1$$

$$3 = 3$$

2) Assumimos que $1 + 2 + 2^2 + \dots + 2^k = 2^{k+1} - 1$ ($n = k$)

3) Precisamos provar que

$$1 + 2 + 2^2 + \dots + 2^{k+1} = 2^{k+1+1} - 1 \quad (n = k+1)$$

ou seja

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



Exemplo 2 (cont.)

Dado que $1 + 2 + 2^2 + \dots + 2^k = 2^{k+1} - 1$ (hipótese indutiva)

Provar que $1 + 2 + 2^2 + \dots + 2^{k+1} = 2^{k+2} - 1$ (passo indutivo)

$$\begin{aligned} 1 + 2 + 2^2 + \dots + 2^{k+1} &= 1 + 2 + 2^2 + \dots + 2^k + 2^{k+1} \\ &= 2^{k+1} - 1 + 2^{k+1} \quad (\text{pela hipótese indutiva}) \\ &= 2(2^{k+1}) - 1 \\ &= 2^{k+1+1} - 1 \\ &= 2^{k+2} - 1 \end{aligned}$$



Exemplo 3

Provar que $1 + 2 + 3 + \dots + n = n(n+1) / 2$, $n \geq 1$



Exemplo 3

Provar que $1 + 2 + 3 + \dots + n = n(n+1) / 2$, $n \geq 1$

1) $1 = 1(1+1) / 2$

$$1 = 1 \cdot 2 / 2 = 2 / 2 = 1$$

$$1 = 1$$

2) Assumimos que $1 + 2 + 3 + \dots + k = k(k+1) / 2 = (k^2 + k) / 2$

3) Precisamos provar que

$$1 + 2 + 3 + \dots + (k+1) = (k+1)(k+2) / 2 = (k^2 + 3k + 2) / 2$$



Exemplo 3 (cont.)

Dado que $1 + 2 + 3 + \dots + k = (k^2 + k) / 2$ (hipótese indutiva)

Provar que $1 + 2 + 3 + \dots + (k+1) = (k^2 + 3k + 2) / 2$ (passo indutivo)

$$\begin{aligned} 1 + 2 + 3 + \dots + (k+1) &= 1 + 2 + 3 + \dots + k + (k+1) \\ &= (k^2 + k) / 2 + (k+1) \quad (\text{pela hipótese indutiva}) \\ &= (k^2 + k) / 2 + (2k + 2) / 2 \\ &= (k^2 + 3k + 2) / 2 \\ &= (k+1)(k+2) / 2 \end{aligned}$$



Exemplo 4

Provar que $2^{3n} - 1$ é divisível por 7, $n \geq 1$



Exemplo 4

Provar que $2^{3n} - 1$ é divisível por 7, $n \geq 1$

- 1) $2^{3 \cdot 1} - 1 = 8 - 1 = 7$ ($n = 1$) (base)
- 2) Assumimos que $2^{3k} - 1$ é divisível por 7 ($n = k$) (hip. Indutiva)
Isto é: $2^{3k} - 1 = 7m$
- 3) Precisamos provar que $2^{3(k+1)} - 1$ é divisível por 7 (passo indutivo)
Isto é: $2^{3(k+1)} - 1 = 7t$



Exemplo 4 (cont.)

Dado que $2^{3k} - 1 = 7m$ (hipótese indutiva)

Provar que $2^{3(k+1)} - 1 = 7t$ (passo indutivo)

$$\begin{aligned} 2^{3(k+1)} - 1 &= 8 \cdot 2^{3k} - 1 \\ &= 8(7m + 1) - 1 && \text{(pela hipótese indutiva)} \\ &= 8(7m) + 8 - 1 \\ &= 7(8m) + 7 \\ &= 7(8m + 1) \\ &= 7t \end{aligned}$$



Exemplo 5

Provar que $x^n - 1$ é divisível por $x - 1$, $x \neq 1$



Exemplo 5

Provar que $x^n - 1$ é divisível por $x - 1$, $x \neq 1$

1) $x^1 - 1 = x - 1$ que é divisível por $x - 1$ $(n = 1)$ (base)

2) Assumimos que $x^k - 1$ é divisível por $x - 1$ $(n = k)$

Isto é: $x^k - 1 = (x - 1)m$

3) Precisamos provar que $x^{k+1} - 1$ é divisível por $x - 1$

Isto é: $x^{k+1} - 1 = (x - 1)t$



Exemplo 5 (cont.)

Dado que $x^k - 1 = (x - 1)m$ (hipótese indutiva)

Provar que $x^{k+1} - 1 = (x - 1)t$ (passo indutivo)

$$\begin{aligned}x^{k+1} - 1 &= x \cdot x^k - 1 \\&= x \cdot x^k - 1 - x + x \\&= x \cdot x^k - x + x - 1 \\&= x(x^k - 1) + (x - 1) \\&= x \cdot (x - 1)m + (x - 1) \quad (\text{pela hipótese indutiva}) \\&= (x - 1) [xm + 1] \\&= (x - 1)t\end{aligned}$$



Exemplo 5 (cont.)

Dado que $x^k - 1 = (x - 1)m$ (hipótese indutiva)

Provar que $x^{k+1} - 1 = (x - 1)t$ (passo indutivo)

$$\begin{aligned}x^{k+1} - 1 &= x \cdot x^k - 1 & x^k &= (x - 1)m + 1 \text{ (Hip Ind)} \\&= x \cdot [(x - 1)m + 1] - 1 \\&= x(x - 1)m + (x - 1) \\&= (x - 1) [xm + 1] \\&= (x - 1)t\end{aligned}$$



Exemplo 6

Provar por indução que $n^2 > 3n$, $n \geq 4$

Exemplo 6

Provar por indução que $n^2 > 3n$, $n \geq 4$

- 1) Para $n=4$ temos: $4^2 > 3 \cdot 4$ ou $16 > 12$ (base)
- 2) Assumimos que $k^2 > 3k \rightarrow 3k < k^2$ (hipótese indutiva)
- 3) Precisamos provar que $(k+1)^2 > 3(k+1)$ (passo indutivo)

$$\begin{aligned}(k+1)^2 &= k^2 + 2k + 1 \\ &> 3k + 2k + 1 && \text{(pela hipótese indutiva)} \\ &> 3k + 8 + 1 && \text{(dado que } k > 4\text{)} \\ &> 3k + 9 \\ &> 3k + 3 \\ &> 3(k+1)\end{aligned}$$



Exercício 1:

Provar que $(1 + x)^n > 1 + x^n$ $n > 1, \quad x \neq 0$



Exercício 1:

Provar que:

$$(1 + x)^n > 1 + x^n \quad n, x \in \mathbb{N}, \quad n > 1, \quad x \neq 0$$

$$1) (1 + x)^2 = 1 + 2x + x^2 > 1 + x^2 \quad (n = 2)$$

$$2) (1 + x)^k > 1 + x^k \quad (n = k)$$

$$3) \text{ Precisamos provar que } (1 + x)^{k+1} > 1 + x^{k+1} \quad (n = k+1)$$



Exercício 1 (cont.)

Dado que $(1 + x)^k > 1 + x^k$ (hipótese indutiva)

Provar que $(1 + x)^{k+1} > 1 + x^{k+1}$ (passo indutivo)

$$(1 + x)^{k+1} = (1 + x)(1 + x)^k$$

$$(1 + x)^{k+1} > (1 + x)(1 + x^k) \quad (\text{pela hipótese indutiva})$$

$$> (1 + x^k) + x(1 + x^k)$$

$$> 1 + x^k + x + x^{k+1}$$

$$> 1 + x^{k+1} + x^k + x$$

$$> 1 + x^{k+1}$$



Atenção!!!

Na tentativa de provar por indução se provarmos que $P(k+1)$ é verdadeiro sem utilizar o fato de que $P(k)$ é verdadeiro teremos feito uma **prova direta** de $P(k+1)$, onde $k+1$ é arbitrário.



Exercício 2

Provar por indução o teorema de DeMoivre:

$$(\cos \theta + i \operatorname{sen} \theta)^n = \cos n\theta + i \operatorname{sen} n\theta, \quad n \geq 1, \quad i^2 = -1$$

Dica! Lembrar das fórmulas trigonométricas de adição:

$$\begin{aligned}\cos (\alpha + \beta) &= \cos \alpha \cos \beta - \operatorname{sen} \alpha \operatorname{sen} \beta \\ \operatorname{sen} (\alpha + \beta) &= \operatorname{sen} \alpha \cos \beta + \cos \alpha \operatorname{sen} \beta\end{aligned}$$



Exercício 3

Provar que $(\cos \theta + i \sen \theta)^n = \cos n\theta + i \sen n\theta$, $n \geq 1$, $i^2 = -1$

$$\text{Para } n=1, \quad (\cos \theta + i \sen \theta)^1 = \cos \theta + i \sen \theta$$

$$\text{Para } n=k, \quad (\cos \theta + i \sen \theta)^k = \cos k\theta + i \sen k\theta$$

$$\text{Para } n = k+1 \quad (\cos \theta + i \sen \theta)^{k+1} = \cos (k+1)\theta + i \sen (k+1)\theta$$

Usando as fórmulas trigonométricas de adição, temos:

$$\cos (k+1)\theta = \cos (k\theta + \theta) = \cos k\theta \cos \theta - \sen k\theta \sen \theta$$

$$\sen (k+1)\theta = \sen (k\theta + \theta) = \sen k\theta \cos \theta + \cos k\theta \sen \theta$$



Exercício 2

Provar que $(\cos \theta + i \sen \theta)^n = \cos n\theta + i \sen n\theta$

Dado que $(\cos \theta + i \sen \theta)^k = \cos k\theta + i \sen k\theta$

Provar que $(\cos \theta + i \sen \theta)^{k+1} = \cos (k+1)\theta + i \sen (k+1)\theta$

$$\begin{aligned}(\cos \theta + i \sen \theta)^{k+1} &= (\cos \theta + i \sen \theta) (\cos \theta + i \sen \theta)^k \\&= (\cos \theta + i \sen \theta) (\cos k\theta + i \sen k\theta) \\&= \cos k\theta \cos \theta + i \sen k\theta \cos \theta + i^2 \sen k\theta \sen \theta + i \cos k\theta \sen \theta \\&= \cos k\theta \cos \theta + i \sen k\theta \cos \theta - \sen k\theta \sen \theta + i \cos k\theta \sen \theta \\&= (\cos k\theta \cos \theta - \sen k\theta \sen \theta) + i (\sen k\theta \cos \theta + \cos k\theta \sen \theta) \\&= \cos (k\theta + \theta) + i \sen (k\theta + \theta) \\&= \cos (k+1)\theta + i \sen (k+1)\theta\end{aligned}$$