MC458 — Projeto e Análise de Algoritmos I

C.C. de Souza   C.N. da Silva   O. Lee

Antes de mais nada...

- Uma versão anterior deste conjunto de slides foi preparada por Cid Carvalho de Souza e Cândida Nunes da Silva para uma instância anterior desta disciplina.
- O que vocês tem em mãos é uma versão modificada preparada para atender a meus gostos.
- Nunca é demais enfatizar que o material é apenas um guia e não deve ser usado como única fonte de estudo. Para isso consultem a bibliografia (em especial o CLR ou CLRS).

Orlando Lee

Agradecimentos (Cid e Cândida)

- Várias pessoas contribuíram direta ou indiretamente com a preparação deste material.
- Algumas destas pessoas cederam gentilmente seus arquivos digitais enquanto outras cederam gentilmente o seu tempo fazendo correções e dando sugestões.
- Uma lista destes "colaboradores" (em ordem alfabética) é dada abaixo:
  - Célia Picinin de Mello
  - José Coelho de Pina
  - Orlando Lee
  - Paulo Feofiloff
  - Pedro Rezende
  - Ricardo Dahab
  - Zanoni Dias

Indução matemática

Demonstração por Indução

Na *Demonstração por Indução*, queremos demonstrar a validade de $P(n)$, uma propriedade P com um parâmetro natural n associado, para todo valor de n.

Demonstração por Indução

Na *Demonstração por Indução*, queremos demonstrar a validade de $P(n)$, uma propriedade P com um parâmetro natural n associado, para todo valor de n.

Exemplo:

A soma dos n primeiros naturais ímpares é n^2.

Na *Demonstração por Indução*, queremos demonstrar a validade de $P(n)$, uma propriedade P com um parâmetro natural n associado, para todo valor de n.

Exemplo:

A soma dos n primeiros naturais ímpares é n^2.

Há um número infinito de casos a serem considerados, um para cada valor de n. Demonstramos os infinitos casos de uma só vez:

Demonstração por Indução

Na *Demonstração por Indução*, queremos demonstrar a validade de $P(n)$, uma propriedade P com um parâmetro natural n associado, para todo valor de n.

Exemplo:

A soma dos n primeiros naturais ímpares é n^2.

Há um número infinito de casos a serem considerados, um para cada valor de n. Demonstramos os infinitos casos de uma só vez:

- **Base da Indução:** demonstramos $P(1)$.

Demonstração por Indução

Na *Demonstração por Indução*, queremos demonstrar a validade de $P(n)$, uma propriedade P com um parâmetro natural n associado, para todo valor de n.

Exemplo:

A soma dos n primeiros naturais ímpares é n^2.

Há um número infinito de casos a serem considerados, um para cada valor de n. Demonstramos os infinitos casos de uma só vez:

- **Base da Indução:** demonstramos $P(1)$.
- **Hipótese de Indução:** supomos que $P(n)$ é verdadeira.

Demonstração por Indução

Na *Demonstração por Indução*, queremos demonstrar a validade de $P(n)$, uma propriedade P com um parâmetro natural n associado, para todo valor de n.

Exemplo:

A soma dos n primeiros naturais ímpares é n^2.

Há um número infinito de casos a serem considerados, um para cada valor de n. Demonstramos os infinitos casos de uma só vez:

- **Base da Indução:** demonstramos $P(1)$.
- **Hipótese de Indução:** supomos que $P(n)$ é verdadeira.
- **Passo de Indução:** provamos que $P(n+1)$ é verdadeira, a partir da hipótese de indução.

Demonstração por Indução

Outra forma equivalente:

- **Base da Indução:** demonstramos $P(1)$.
- **Hipótese de Indução:** supomos que $P(n-1)$ é verdadeira.
- **Passo de Indução:** provamos que $P(n)$ é verdadeira, a partir da hipótese de indução.

Outra forma equivalente:

- **Base da Indução:** demonstramos $P(1)$.
- **Hipótese de Indução:** supomos que $P(n-1)$ é verdadeira.
- **Passo de Indução:** provamos que $P(n)$ é verdadeira, a partir da hipótese de indução.

Por razões didáticas, prefiro a segunda forma, mas ambas são equivalentes.

Demonstração por Indução

Às vezes queremos provar que uma proposição $P(n)$ vale para $n \geq n_0$ para algum n_0.

Demonstração por Indução

Às vezes queremos provar que uma proposição $P(n)$ vale para $n \geq n_0$ para algum n_0.

- **Base da Indução:** demonstramos $P(n_0)$.

Demonstração por Indução

Às vezes queremos provar que uma proposição $P(n)$ vale para $n \geq n_0$ para algum n_0.

- **Base da Indução:** demonstramos $P(n_0)$.
- **Hipótese de Indução:** supomos que $P(n-1)$ é verdadeira.

Demonstração por Indução

Às vezes queremos provar que uma proposição $P(n)$ vale para $n \geq n_0$ para algum n_0.

- **Base da Indução:** demonstramos $P(n_0)$.
- **Hipótese de Indução:** supomos que $P(n-1)$ é verdadeira.
- **Passo de Indução:** provamos que $P(n)$ é verdadeira, a partir da hipótese de indução.

Demonstração por Indução

Às vezes queremos provar que uma proposição $P(n)$ vale para $n \geq n_0$ para algum n_0.

- **Base da Indução:** demonstramos $P(n_0)$.
- **Hipótese de Indução:** supomos que $P(n-1)$ é verdadeira.
- **Passo de Indução:** provamos que $P(n)$ é verdadeira, a partir da hipótese de indução.

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos.

Exemplo 1

Prove que para naturais $x \geq 1$ e $n \geq 1$, $x^n - 1$ é divisível por $x - 1$.

Exemplo 1

Prove que para naturais $x \geq 1$ e $n \geq 1$, $x^n - 1$ é divisível por $x - 1$.

Prova:

Exemplo 1

Prove que para naturais $x \geq 1$ e $n \geq 1$, $x^n - 1$ é divisível por $x - 1$.

Prova:

- **Base:** $n = 1$. Temos que $x^n - 1 = x - 1$, que é obviamente divisível por $x - 1$. Isso encerra a demonstração da base da indução.

Exemplo 1

Prove que para naturais $x \geq 1$ e $n \geq 1$, $x^n - 1$ é divisível por $x - 1$.

Prova:

- **Base:** $n = 1$. Temos que $x^n - 1 = x - 1$, que é obviamente divisível por $x - 1$. Isso encerra a demonstração da base da indução.
- **Hipótese de indução:** suponha que $n \geq 2$ e que $x^{n-1} - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.

Exemplo 1 (cont.)

Exemplo 1 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $x^{n-1} - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.

Exemplo 1 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $x^{n-1} - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.
- **Passo de indução:** supondo a HI, mostraremos que $x^n - 1$ é divisível por $x - 1$, para todo natural $x \geq 1$.

Exemplo 1 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $x^{n-1} - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.
- **Passo de indução:** supondo a HI, mostraremos que $x^n - 1$ é divisível por $x - 1$, para todo natural $x \geq 1$.

  Primeiro reescrevemos $x^n - 1$ como

$$x^n - 1 = x(x^{n-1} - 1) + (x - 1).$$

Exemplo 1 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $x^{n-1} - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.
- **Passo de indução:** supondo a HI, mostraremos que $x^n - 1$ é divisível por $x - 1$, para todo natural $x \geq 1$.

  Primeiro reescrevemos $x^n - 1$ como

  $$x^n - 1 = x(x^{n-1} - 1) + (x - 1).$$

  Pela HI, $x^{n-1} - 1$ é divisível por $x - 1$. Portanto, o lado direito da equação acima é, de fato, divisível por $x - 1$.

Exemplo 1 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $x^{n-1} - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.
- **Passo de indução:** supondo a HI, mostraremos que $x^n - 1$ é divisível por $x - 1$, para todo natural $x \geq 1$.

  Primeiro reescrevemos $x^n - 1$ como

  $$x^n - 1 = x(x^{n-1} - 1) + (x - 1).$$

  Pela HI, $x^{n-1} - 1$ é divisível por $x - 1$. Portanto, o lado direito da equação acima é, de fato, divisível por $x - 1$.

A demonstração por indução está completa. ■

Indução Fraca × Indução Forte

A *indução forte* difere da *indução fraca* (ou *simples*) apenas na hipótese de indução.

Indução Fraca × Indução Forte

A *indução forte* difere da *indução fraca* (ou *simples*) apenas na hipótese de indução.

No caso da indução forte, devemos supor que a propriedade vale para todos os casos anteriores, não somente para o anterior, ou seja:

Indução Fraca × Indução Forte

A *indução forte* difere da *indução fraca* (ou *simples*) apenas na hipótese de indução.

No caso da indução forte, devemos supor que a propriedade vale para todos os casos anteriores, não somente para o anterior, ou seja:

- **Base da Indução:** demonstramos $P(1)$.

Indução Fraca $\times$ Indução Forte

A *indução forte* difere da *indução fraca* (ou *simples*) apenas na hipótese de indução.

No caso da indução forte, devemos supor que a propriedade vale para todos os casos anteriores, não somente para o anterior, ou seja:

- **Base da Indução:** demonstramos $P(1)$.
- **Hipótese de Indução Forte:** supomos que $P(k)$ é verdadeira, para todo $1 \leq k < n$.

Indução Fraca $\times$ Indução Forte

A *indução forte* difere da *indução fraca* (ou *simples*) apenas na hipótese de indução.

No caso da indução forte, devemos supor que a propriedade vale para todos os casos anteriores, não somente para o anterior, ou seja:

- **Base da Indução:** demonstramos $P(1)$.
- **Hipótese de Indução Forte:** supomos que $P(k)$ é verdadeira, para todo $1 \leq k < n$.
- **Passo de Indução:** provamos que $P(n)$ é verdadeira, a partir da hipótese de indução.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos.
(I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos.
(I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Base:** $n = 2$. A afirmação claramente é verdadeira.
  Isto conclui a prova para o caso base.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos. (I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Base:** $n = 2$. A afirmação claramente é verdadeira.
  Isto conclui a prova para o caso base.
- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos. (I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos. (I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.
- **Passo de indução:** supondo a HI, mostraremos que n pode ser escrito como um produto de primos.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos.
(I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.
- **Passo de indução:** supondo a HI, mostraremos que n pode ser escrito como um produto de primos.

  Se n é primo, então o resultado é óbvio.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos.
(I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.
- **Passo de indução:** supondo a HI, mostraremos que n pode ser escrito como um produto de primos.

  Se n é primo, então o resultado é óbvio. Suponha então que existem inteiros $a, b : 2 \leq a, b < n$ tais que $n = ab$.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos. (I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.
- **Passo de indução:** supondo a HI, mostraremos que n pode ser escrito como um produto de primos.

  Se n é primo, então o resultado é óbvio. Suponha então que existem inteiros $a, b : 2 \leq a, b < n$ tais que $n = ab$.

  Por HI tanto a quanto b podem ser escritos como produtos de primos.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos. (I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.
- **Passo de indução:** supondo a HI, mostraremos que n pode ser escrito como um produto de primos.

  Se n é primo, então o resultado é óbvio. Suponha então que existem inteiros $a, b : 2 \leq a, b < n$ tais que $n = ab$.

  Por HI tanto a quanto b podem ser escritos como produtos de primos. Logo n pode ser escrito como um produto de primos.

Exemplo 2

Exemplo:

Todo natural $n \geq 2$ pode ser fatorado como um produto de primos. (I.e., existem primos $p_1, p_2, \ldots, p_t$ tais que $n = p_1 p_2 \cdots p_t$.)

- **Hipótese de indução (forte):** suponha que $n \geq 3$ e que para todo $k : 2 \leq k < n$, o número k pode ser escrito como um produto de primos.
- **Passo de indução:** supondo a HI, mostraremos que n pode ser escrito como um produto de primos.

  Se n é primo, então o resultado é óbvio. Suponha então que existem inteiros $a, b : 2 \leq a, b < n$ tais que $n = ab$.

  Por HI tanto a quanto b podem ser escritos como produtos de primos. Logo n pode ser escrito como um produto de primos.

  Isto conclui a demonstração por indução. ■

Exemplo 3

Demonstre que o número R_n de regiões no plano criadas por n retas em posição geral é igual a

$$R_n = \frac{n(n+1)}{2} + 1.$$

Exemplo 3

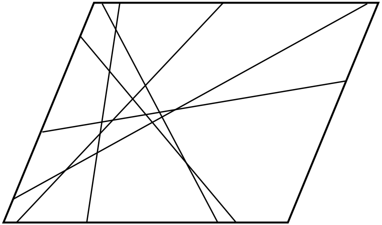
Demonstre que o número R_n de regiões no plano criadas por n retas em posição geral é igual a

$$R_n = \frac{n(n+1)}{2} + 1.$$

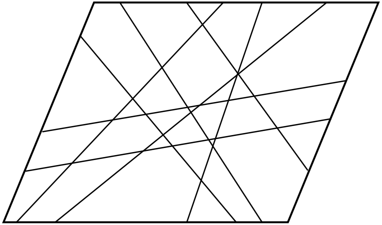
Um conjunto de retas está em posição geral no plano se

- todas as retas são concorrentes, isto é, não há retas paralelas e
- não há três retas interceptando-se no mesmo ponto.

Antes de prosseguirmos com a demonstração vejamos exemplos de um conjunto de retas que está em posição geral e outro que não está.



Em posição geral



Não estão em posição geral

Exemplo 3 (cont.)

Demonstre que o número R_n de regiões no plano criadas por n retas em posição geral é igual a

$$R_n = \frac{n(n+1)}{2} + 1.$$

Exemplo 3 (cont.)

Demonstre que o número R_n de regiões no plano criadas por n retas em posição geral é igual a

$$R_n = \frac{n(n+1)}{2} + 1.$$

- **Base:** $n = 1$. Uma reta sozinha divide o plano em duas regiões. De fato,

$$R_1 = \frac{1 \times 2}{2} + 1 = 2.$$

Exemplo 3 (cont.)

Demonstre que o número R_n de regiões no plano criadas por n retas em posição geral é igual a

$$R_n = \frac{n(n+1)}{2} + 1.$$

- **Base:** $n = 1$. Uma reta sozinha divide o plano em duas regiões. De fato,

$$R_1 = \frac{1 \times 2}{2} + 1 = 2.$$

Isto conclui a prova para $n = 1$.

Demonstre que o número R_n de regiões no plano criadas por n retas em posição geral é igual a

$$R_n = \frac{n(n+1)}{2} + 1.$$

- **Base:** $n = 1$. Uma reta sozinha divide o plano em duas regiões. De fato,

  $$R_1 = \frac{1 \times 2}{2} + 1 = 2.$$

  Isto conclui a prova para $n = 1$.
- **Hipótese de indução:** suponha que $n \geq 2$ e que $R_{n-1} = \frac{(n-1)n}{2} + 1$.

Exemplo 3 (cont.)

Exemplo 3 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $R_{n-1} = \frac{(n-1)n}{2} + 1$.

Exemplo 3 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $R_{n-1} = \frac{(n-1)n}{2} + 1$.
- **Passo de indução:** supondo a HI, mostraremos que para n retas em posição geral vale que

$$R_n = \frac{n(n+1)}{2} + 1.$$

Exemplo 3 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $R_{n-1} = \frac{(n-1)n}{2} + 1$.
- **Passo de indução:** supondo a HI, mostraremos que para n retas em posição geral vale que

$$R_n = \frac{n(n+1)}{2} + 1.$$

Considere um conjunto L de n retas em posição geral no plano e seja r uma dessas retas. Então, as retas do conjunto $L' = L \setminus \{r\}$ obedecem à HI e, portanto, o número de regiões distintas do plano definidas por elas é $R_{n-1} = \frac{(n-1)n}{2} + 1$.

Exemplo 3 (cont.)

Exemplo 3 (cont.)

- Além disso, r intersecta as outras $n-1$ retas em $n-1$ pontos distintos. O que significa que, saindo de uma ponta de r no infinito e após cruzar as $n-1$ retas de L', a reta r terá cruzado n regiões, dividindo cada uma destas em duas outras.

Exemplo 3 (cont.)

- Além disso, r intersecta as outras $n-1$ retas em $n-1$ pontos distintos. O que significa que, saindo de uma ponta de r no infinito e após cruzar as $n-1$ retas de L', a reta r terá cruzado n regiões, dividindo cada uma destas em duas outras.
- Assim, temos que

$$R_n = R_{n-1} + n$$

Exemplo 3 (cont.)

- Além disso, r intersecta as outras $n-1$ retas em $n-1$ pontos distintos. O que significa que, saindo de uma ponta de r no infinito e após cruzar as $n-1$ retas de L', a reta r terá cruzado n regiões, dividindo cada uma destas em duas outras.
- Assim, temos que

$$\begin{aligned} R_n &= R_{n-1} + n \\ &= \frac{(n-1)n}{2} + 1 + n \text{ (pela HI)} \end{aligned}$$

Exemplo 3 (cont.)

- Além disso, r intersecta as outras $n-1$ retas em $n-1$ pontos distintos. O que significa que, saindo de uma ponta de r no infinito e após cruzar as $n-1$ retas de L', a reta r terá cruzado n regiões, dividindo cada uma destas em duas outras.
- Assim, temos que

$$\begin{aligned}
R_n &= R_{n-1} + n \\
&= \frac{(n-1)n}{2} + 1 + n \text{ (pela HI)} \\
&= \frac{(n-1)n}{2} + \frac{2n}{2} + 1
\end{aligned}$$

Exemplo 3 (cont.)

- Além disso, r intersecta as outras $n-1$ retas em $n-1$ pontos distintos. O que significa que, saindo de uma ponta de r no infinito e após cruzar as $n-1$ retas de L', a reta r terá cruzado n regiões, dividindo cada uma destas em duas outras.
- Assim, temos que

$$\begin{aligned} R_n &= R_{n-1} + n \\ &= \frac{(n-1)n}{2} + 1 + n \text{ (pela HI)} \\ &= \frac{(n-1)n}{2} + \frac{2n}{2} + 1 \\ &= \frac{n(n+1)}{2} + 1. \end{aligned}$$

Exemplo 3 (cont.)

- Além disso, r intersecta as outras $n-1$ retas em $n-1$ pontos distintos. O que significa que, saindo de uma ponta de r no infinito e após cruzar as $n-1$ retas de L', a reta r terá cruzado n regiões, dividindo cada uma destas em duas outras.
- Assim, temos que

$$\begin{aligned} R_n &= R_{n-1} + n \\ &= \frac{(n-1)n}{2} + 1 + n \text{ (pela HI)} \\ &= \frac{(n-1)n}{2} + \frac{2n}{2} + 1 \\ &= \frac{n(n+1)}{2} + 1. \end{aligned}$$

Isso conclui a demonstração. ■

Exemplo 4

Vejamos agora um exemplo onde a indução é aplicada de forma um pouco diferente.

Exemplo 4

Vejamos agora um exemplo onde a indução é aplicada de forma um pouco diferente.

Demonstre que a série S_n definida abaixo satisfaz

$$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} < 1,$$

para todo inteiro $n \geq 1$.

Exemplo 4

Vejamos agora um exemplo onde a indução é aplicada de forma um pouco diferente.

Demonstre que a série S_n definida abaixo satisfaz

$$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} < 1,$$

para todo inteiro $n \geq 1$.

Prova:

- **Base:** $n = 1$. A desigualdade se reduz a $\frac{1}{2} < 1$ e obviamente vale.

Exemplo 4

Vejamos agora um exemplo onde a indução é aplicada de forma um pouco diferente.

Demonstre que a série S_n definida abaixo satisfaz

$$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} < 1,$$

para todo inteiro $n \geq 1$.

Prova:

- **Base:** $n = 1$. A desigualdade se reduz a $\frac{1}{2} < 1$ e obviamente vale.
- **Hipótese de indução:** suponha que $n \geq 2$ e que $S_{n-1} < 1$.

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Pela definição de S_n, temos que

$$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^{n-1}} + \frac{1}{2^n} = S_{n-1} + \frac{1}{2^n}.$$

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Pela definição de S_n, temos que

  $$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^{n-1}} + \frac{1}{2^n} = S_{n-1} + \frac{1}{2^n}.$$

  Pela HI, $S_{n-1} < 1$. Entretanto, nada podemos dizer sobre S_n, já que não há nada que impeça que $S_{n-1} + \frac{1}{2^n}$ seja maior ou igual a 1.

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Pela definição de S_n, temos que

  $$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^{n-1}} + \frac{1}{2^n} = S_{n-1} + \frac{1}{2^n}.$$

  Pela HI, $S_{n-1} < 1$. Entretanto, nada podemos dizer sobre S_n, já que não há nada que impeça que $S_{n-1} + \frac{1}{2^n}$ seja maior ou igual a 1.

  Vamos manipular S_n de outra maneira.

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Então

$$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n}$$

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Então

$$\begin{aligned} S_n &= \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} \\ &= \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{n-1}}\right] \end{aligned}$$

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Então

$$\begin{aligned} S_n &= \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} \\ &= \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{n-1}}\right] \\ &= \frac{1}{2} + \frac{1}{2} \times S_{n-1} \end{aligned}$$

Exemplo 4 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n < 1$.

  Então

$$
\begin{aligned}
S_n &= \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} \\
&= \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{n-1}}\right] \\
&= \frac{1}{2} + \frac{1}{2} \times S_{n-1} \\
&< \frac{1}{2} + \frac{1}{2} \times 1 \text{ (pela HI)} \\
&= 1.
\end{aligned}
$$

Isto conclui a demonstração. ∎

Exemplo 5

Às vezes, parece que o passo de indução não funciona, não importa o que tentemos.

Prove que para todo natural $n \geq 1$ vale que

$$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2.$$

Exemplo 5

Às vezes, parece que o passo de indução não funciona, não importa o que tentemos.

Prove que para todo natural $n \geq 1$ vale que

$$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2.$$

Prova:

- **Base:** $n = 1$. A desigualdade se reduz a $1 \leq 2$ e obviamente vale.

Exemplo 5 (cont.)

Exemplo 5 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $S_{n-1} \leq 2$.

Exemplo 5 (cont.)

- **Hipótese de indução:** suponha que $n \geq 2$ e que $S_{n-1} \leq 2$.

  Pela definição de S_n, temos que

  $$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(n-1)^2} + \frac{1}{n^2} = S_{n-1} + \frac{1}{n^2}.$$

  Como no exemplo anterior, usar a HI diretamente não nos permite concluir nada.

  Aqui não parece fácil manipular a expressão para obter uma forma melhor de aplicar a HI.

Exemplo 5 (cont.)

É necessário **fortalecer** a **hipótese de indução**!

Exemplo 5 (cont.)

É necessário **fortalecer** a **hipótese de indução**!

- **Hipótese de indução (fortalecida):** suponha que

$$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Exemplo 5 (cont.)

É necessário **fortalecer** a **hipótese de indução**!

- **Hipótese de indução (fortalecida):** suponha que

$$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

- Esta ideia aparentemente contra-intuitiva segue de um fenômeno bastante comum em matemática: muitas vezes é mais fácil provar um resultado mais forte do que o resultado que desejávamos.

Exemplo 5 (cont.)

É necessário **fortalecer** a **hipótese de indução**!

- **Hipótese de indução (fortalecida):** suponha que

$$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

- Esta ideia aparentemente contra-intuitiva segue de um fenômeno bastante comum em matemática: muitas vezes é mais fácil provar um resultado mais forte do que o resultado que desejávamos.
- Polya chamava isso de paradoxo do inventor.

Exemplo 5 (cont.)

É necessário **fortalecer** a **hipótese de indução**!

- **Hipótese de indução (fortalecida):** suponha que

$$S_n = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

- Esta ideia aparentemente contra-intuitiva segue de um fenômeno bastante comum em matemática: muitas vezes é mais fácil provar um resultado mais forte do que o resultado que desejávamos.
- Polya chamava isso de paradoxo do inventor.
- Obviamente para isto funcionar, é necessário que o resultado fortalecido seja verdadeiro!

Exemplo 5 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n \leq 2 - \frac{1}{n}$.

Exemplo 5 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n \leq 2 - \frac{1}{n}$.

$$\begin{aligned} S_n &= \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(n-1)^2} + \frac{1}{n^2} \\ &\leq 2 - \frac{1}{n-1} + \frac{1}{n^2} \text{ (pela HI)} \\ &\leq 2 - \frac{1}{n}, \end{aligned}$$

Exemplo 5 (cont.)

- **Passo de indução:** supondo a HI, mostraremos que $S_n \leq 2 - \frac{1}{n}$.

$$\begin{aligned} S_n &= \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(n-1)^2} + \frac{1}{n^2} \\ &\leq 2 - \frac{1}{n-1} + \frac{1}{n^2} \text{ (pela HI)} \\ &\leq 2 - \frac{1}{n}, \end{aligned}$$

onde a última desigualdade segue do fato que

$$\frac{1}{n-1} - \frac{1}{n} = \frac{1}{(n-1)n} > \frac{1}{n^2}.$$

Isto completa a prova por indução. ■

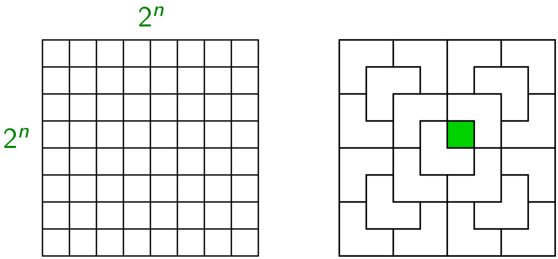
Exemplo 6

Um bilionário (que chamaremos de Bill para manter seu anonimato) ajudou financeiramente a UNICOMP várias vezes.

Exemplo 6

Um bilionário (que chamaremos de Bill para manter seu anonimato) ajudou financeiramente a UNICOMP várias vezes.

Para retribuir tanta generosidade, a UNICOMP decidiu construir um grande pátio de dimensões $2^n \times 2^n$ e cobri-lo com ladrilhos em forma de L (um quadrado 2×2 com uma casa removida). Uma das casas centrais ficará livre para que uma estátua de Bill seja colocada ali.



Exemplo 6 (cont.)

Prove que para todo natural $n \geq 1$ é sempre possível cobrir um quadrado de dimensões $2^n \times 2^n$ com ladrilhos em forma de L deixando uma casa central livre.

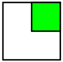
Prova:

Exemplo 6 (cont.)

Prove que para todo natural $n \geq 1$ é sempre possível cobrir um quadrado de dimensões $2^n \times 2^n$ com ladrilhos em forma de L deixando uma casa central livre.

Prova:

- O **caso base** é $n = 1$. A figura abaixo mostra uma solução.



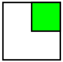
- **Hipótese de indução:** suponha que $n \geq 2$ e que é possível cobrir um quadrado $2^{n-1} \times 2^{n-1}$ deixando uma casa central livre.

Exemplo 6 (cont.)

Prove que para todo natural $n \geq 1$ é sempre possível cobrir um quadrado de dimensões $2^n \times 2^n$ com ladrilhos em forma de L deixando uma casa central livre.

Prova:

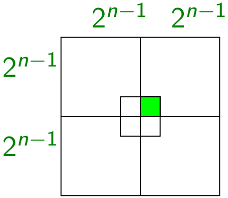
- O **caso base** é $n = 1$. A figura abaixo mostra uma solução.



- **Hipótese de indução:** suponha que $n \geq 2$ e que é possível cobrir um quadrado $2^{n-1} \times 2^{n-1}$ deixando uma casa central livre.
- **Passo de indução:** supondo a HI, mostraremos que é possível cobrir um quadrado $2^n \times 2^n$ deixando uma casa central livre.

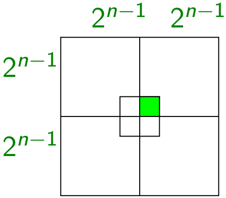
Exemplo 6 (cont.)

- Um quadrado $2^n \times 2^n$ pode ser dividido em 4 quadrados $2^{n-1} \times 2^{n-1}$ como na figura seguinte.



Exemplo 6 (cont.)

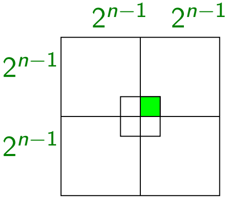
- Um quadrado $2^n \times 2^n$ pode ser dividido em 4 quadrados $2^{n-1} \times 2^{n-1}$ como na figura seguinte.



- Observando a figura, a ideia óbvia é aplicar a HI em cada um dos 4 quadrados $2^{n-1} \times 2^{n-1}$ e completar com um azulejo nas três casas centrais.

Exemplo 6 (cont.)

- Um quadrado $2^n \times 2^n$ pode ser dividido em 4 quadrados $2^{n-1} \times 2^{n-1}$ como na figura seguinte.



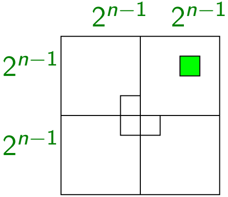
- Observando a figura, a ideia óbvia é aplicar a HI em cada um dos 4 quadrados $2^{n-1} \times 2^{n-1}$ e completar com um azulejo nas três casas centrais.
- O problema é que a HI diz que é possível cobrir cada quadrado $2^{n-1} \times 2^{n-1}$ deixando livre uma casa central e não a dos cantos como queremos. E agora?

Exemplo 6 (cont.)

Vamos **fortalecer** a **hipótese de indução**!

Vamos **fortalecer** a **hipótese de indução**!

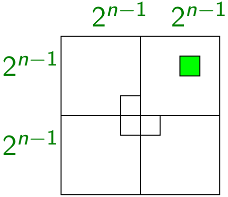
- **Hipótese de indução:** suponha que $n \geq 2$ e que é possível cobrir um quadrado $2^{n-1} \times 2^{n-1}$ deixando livre **qualquer casa desejada**.



Exemplo 6 (cont.)

Vamos **fortalecer** a **hipótese de indução**!

- **Hipótese de indução:** suponha que $n \geq 2$ e que é possível cobrir um quadrado $2^{n-1} \times 2^{n-1}$ deixando livre **qualquer casa desejada**.

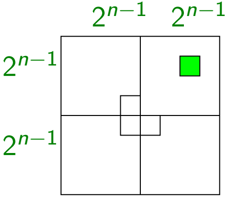


- Agora o **passo de indução** funciona perfeitamente. Para cada um dos quadrados $2^{n-1} \times 2^{n-1}$ que não contém a casa livre original escolhemos um canto conveniente para ser livre. Aplicamos a HI para cada um dos 4 quadrados.

Exemplo 6 (cont.)

Vamos **fortalecer** a **hipótese de indução**!

- **Hipótese de indução:** suponha que $n \geq 2$ e que é possível cobrir um quadrado $2^{n-1} \times 2^{n-1}$ deixando livre **qualquer casa desejada**.



- Agora o **passo de indução** funciona perfeitamente. Para cada um dos quadrados $2^{n-1} \times 2^{n-1}$ que não contém a casa livre original escolhemos um canto conveniente para ser livre. Aplicamos a HI para cada um dos 4 quadrados.

  Colocamos então mais um azulejo nas três casas centrais do quadrado de dimensão $2^n \times 2^n$. Isto completa a prova. ■

Algumas armadilhas - redução $\times$ expansão

Algumas armadilhas - redução $\times$ expansão

- A demonstração do passo da indução simples supõe a proposição válida para um $n-1$ (resp., n) e mostra-se que é válida para n (resp., $n+1$).

Algumas armadilhas - redução $\times$ expansão

- A demonstração do passo da indução simples supõe a proposição válida para um $n - 1$ (resp., n) e mostra-se que é válida para n (resp., $n + 1$).
- Portanto, devemos sempre partir de um caso geral n e **reduzi-lo** ao caso $n - 1$. Às vezes porém, parece mais fácil pensar no caso $n - 1$ e **expandi-lo** para o caso geral n.

Algumas armadilhas - redução $\times$ expansão

- A demonstração do passo da indução simples supõe a proposição válida para um $n-1$ (resp., n) e mostra-se que é válida para n (resp., $n+1$).
- Portanto, devemos sempre partir de um caso geral n e **reduzi-lo** ao caso $n-1$. Às vezes porém, parece mais fácil pensar no caso $n-1$ e **expandi-lo** para o caso geral n.
- O perigo do procedimento de expansão é que ele não seja suficientemente geral, de forma que obtenhamos a implicação, a partir do caso $n-1$, para um caso **geral** n.

Algumas armadilhas - redução $\times$ expansão

- A demonstração do passo da indução simples supõe a proposição válida para um $n-1$ (resp., n) e mostra-se que é válida para n (resp., $n+1$).
- Portanto, devemos sempre partir de um caso geral n e **reduzi-lo** ao caso $n-1$. Às vezes porém, parece mais fácil pensar no caso $n-1$ e **expandi-lo** para o caso geral n.
- O perigo do procedimento de expansão é que ele não seja suficientemente geral, de forma que obtenhamos a implicação, a partir do caso $n-1$, para um caso **geral** n.
- As conseqüências de um lapso como esse podem ser a obtenção de uma estrutura de tamanho n fora da hipótese de indução, ou a prova da proposição apenas para casos particulares de estruturas de tamanho n.

Algumas armadilhas - redução $\times$ expansão

Eis um exemplo de "prova" de um resultado falso.

Todo grafo simples com $n \geq 2$ vértices tal que cada vértice tem grau pelo menos 1 é conexo.

Algumas armadilhas - redução × expansão

Eis um exemplo de "prova" de um resultado falso.

Todo grafo simples com $n \geq 2$ vértices tal que cada vértice tem grau pelo menos 1 é conexo.

- **Base:** $n = 2$. Claramente o resultado vale.

Algumas armadilhas - redução $\times$ expansão

Eis um exemplo de "prova" de um resultado falso.

Todo grafo simples com $n \geq 2$ vértices tal que cada vértice tem grau pelo menos 1 é conexo.

- **Base:** $n = 2$. Claramente o resultado vale.
- **Hipótese de indução:** suponha que $n \geq 2$ e que o resultado vale para todo grafo com n vértices.

Algumas armadilhas - redução $\times$ expansão

Eis um exemplo de "prova" de um resultado falso.

Todo grafo simples com $n \geq 2$ vértices tal que cada vértice tem grau pelo menos 1 é conexo.

- **Base:** $n = 2$. Claramente o resultado vale.
- **Hipótese de indução:** suponha que $n \geq 2$ e que o resultado vale para todo grafo com n vértices.
- **Passo de indução:** mostraremos que o resultado vale para todo grafo com $n + 1$ vértices que satisfaz a hipótese.

Algumas armadilhas - redução $\times$ expansão

Eis um exemplo de "prova" de um resultado falso.

> Todo grafo simples com $n \geq 2$ vértices tal que cada vértice tem grau pelo menos 1 é conexo.

- **Base:** $n = 2$. Claramente o resultado vale.
- **Hipótese de indução:** suponha que $n \geq 2$ e que o resultado vale para todo grafo com n vértices.
- **Passo de indução:** mostraremos que o resultado vale para todo grafo com $n + 1$ vértices que satisfaz a hipótese.
- Seja G um grafo com n vértices que satisfaz a hipótese. Pela HI, G é conexo.

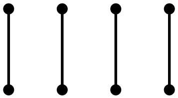
Eis um exemplo de "prova" de um resultado falso.

Todo grafo simples com $n \geq 2$ vértices tal que cada vértice tem grau pelo menos 1 é conexo.

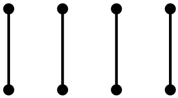
- **Base:** $n = 2$. Claramente o resultado vale.
- **Hipótese de indução:** suponha que $n \geq 2$ e que o resultado vale para todo grafo com n vértices.
- **Passo de indução:** mostraremos que o resultado vale para todo grafo com $n + 1$ vértices que satisfaz a hipótese.
- Seja G um grafo com n vértices que satisfaz a hipótese. Pela HI, G é conexo.

  Acrescente um novo vértice v. Como v deve ter grau pelo menos 1, devemos ligá-lo a pelo menos um vértice de G. O grafo resultante G' tem $n + 1$ vértices e satisfaz a hipótese. Como G é conexo, claramente G' é conexo. ■

- O resultado é claramente falso. Considere o grafo

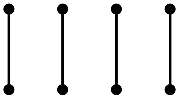


- O resultado é claramente falso. Considere o grafo



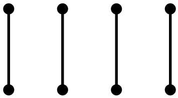
- Mas então onde está o erro?

- O resultado é claramente falso. Considere o grafo



- Mas então onde está o erro?
- Este grafo não pode ser obtido pelo método construtivo descrito.

- O resultado é claramente falso. Considere o grafo



- Mas então onde está o erro?
- Este grafo não pode ser obtido pelo método construtivo descrito.
- Ou seja, o método não consegue construir todos os grafos que satisfazem a hipótese (todo vértice tem grau ≥ 1).

Algumas armadilhas - outros passos mal dados

O que há de errado com a demonstração da seguinte proposição, claramente falsa?

Proposição. Em um conjunto de n cavalos, todos têm a mesma cor.

O que há de errado com a demonstração da seguinte proposição, claramente falsa?

Proposição. Em um conjunto de n cavalos, todos têm a mesma cor.

Prova:

Algumas armadilhas - outros passos mal dados

O que há de errado com a demonstração da seguinte proposição, claramente falsa?

Proposição. Em um conjunto de n cavalos, todos têm a mesma cor.

Prova:

- **Base:** $n = 1$. A afirmação é claramente verdadeira.

O que há de errado com a demonstração da seguinte proposição, claramente falsa?

Proposição. Em um conjunto de n cavalos, todos têm a mesma cor.

Prova:

- **Base:** $n = 1$. A afirmação é claramente verdadeira.
- **Hipótese de indução**: suponha que $n \geq 2$ e que em um conjunto de $n - 1$ cavalos, todos têm a mesma cor.

Algumas armadilhas - outros passos mal dados

- **Passo de indução:** Mostraremos que em um conjunto de n cavalos, todos têm a mesma cor.

Algumas armadilhas - outros passos mal dados

- **Passo de indução:** Mostraremos que em um conjunto de n cavalos, todos têm a mesma cor.
- Sejam $C_1, C_2, \ldots, C_n$ os n cavalos do conjunto. Pela HI os $n-1$ primeiro cavalos $C_1, C_2, \ldots, C_{n-1}$ têm a mesma cor. Do mesmo modo, os $n-1$ últimos cavalos $C_2, \ldots, C_{n-1}, C_n$ têm a mesma cor. Como C_2 está em ambos os conjuntos, segue que todos os n cavalos têm a mesma cor, completando a demonstração. $\blacksquare$

Algumas armadilhas - outros passos mal dados

- **Passo de indução:** Mostraremos que em um conjunto de n cavalos, todos têm a mesma cor.
- Sejam $C_1, C_2, \ldots, C_n$ os n cavalos do conjunto. Pela HI os $n-1$ primeiro cavalos $C_1, C_2, \ldots, C_{n-1}$ têm a mesma cor. Do mesmo modo, os $n-1$ últimos cavalos $C_2, \ldots, C_{n-1}, C_n$ têm a mesma cor. Como C_2 está em ambos os conjuntos, segue que todos os n cavalos têm a mesma cor, completando a demonstração. $\blacksquare$

  Certo?

Algumas armadilhas - outros passos mal dados

- **Passo de indução:** Mostraremos que em um conjunto de n cavalos, todos têm a mesma cor.
- Sejam $C_1, C_2, \ldots, C_n$ os n cavalos do conjunto. Pela HI os $n-1$ primeiro cavalos $C_1, C_2, \ldots, C_{n-1}$ têm a mesma cor. Do mesmo modo, os $n-1$ últimos cavalos $C_2, \ldots, C_{n-1}, C_n$ têm a mesma cor. Como C_2 está em ambos os conjuntos, segue que todos os n cavalos têm a mesma cor, completando a demonstração. $\blacksquare$

  Certo?

Errado!

O argumento no passo de indução funciona para todo $n \geq 3$. Mas no caso $n = 2$ ele falha, porque neste caso, o cavalo C_2 não está em ambos os conjuntos de $n-1$ cavalos.

Invariantes de laço e indução matemática

Um invariante de um laço de um algoritmo é uma propriedade que é satisfeita pelas variáveis do algoritmo em toda iteração do laço executada pelo algoritmo.

Invariantes de laço e indução matemática

Um invariante de um laço de um algoritmo é uma propriedade que é satisfeita pelas variáveis do algoritmo em toda iteração do laço executada pelo algoritmo.

- Usados em provas de corretude de algoritmos.

Invariantes de laço e indução matemática

Um invariante de um laço de um algoritmo é uma propriedade que é satisfeita pelas variáveis do algoritmo em toda iteração do laço executada pelo algoritmo.

- Usados em provas de corretude de algoritmos.
- Tipicamente um algoritmo é composto de vários laços executados em sequência.

Invariantes de laço e indução matemática

Um invariante de um laço de um algoritmo é uma propriedade que é satisfeita pelas variáveis do algoritmo em toda iteração do laço executada pelo algoritmo.

- Usados em provas de corretude de algoritmos.
- Tipicamente um algoritmo é composto de vários laços executados em sequência.
- Para cada laço pode-se obter um invariante que, uma vez provado, garanta o funcionamento correto daquela parte *específica* do algoritmo.

Invariantes de laço e indução matemática

Um invariante de um laço de um algoritmo é uma propriedade que é satisfeita pelas variáveis do algoritmo em toda iteração do laço executada pelo algoritmo.

- Usados em provas de corretude de algoritmos.
- Tipicamente um algoritmo é composto de vários laços executados em sequência.
- Para cada laço pode-se obter um invariante que, uma vez provado, garanta o funcionamento correto daquela parte *específica* do algoritmo.
- A corretude do algoritmo como um todo fica provada se for provado que os invariantes de todos os laços estão corretos.

Invariantes de laço e indução matemática

Um invariante de um laço de um algoritmo é uma propriedade que é satisfeita pelas variáveis do algoritmo em toda iteração do laço executada pelo algoritmo.

- Usados em provas de corretude de algoritmos.
- Tipicamente um algoritmo é composto de vários laços executados em sequência.
- Para cada laço pode-se obter um invariante que, uma vez provado, garanta o funcionamento correto daquela parte *específica* do algoritmo.
- A corretude do algoritmo como um todo fica provada se for provado que os invariantes de todos os laços estão corretos.
- O difícil é encontrar o invariante que leva à prova da corretude do algoritmo.

Invariantes de laço e indução matemática

Exemplo: usando *invariante de laços*, provaremos a corretude de um algoritmo que calcula a potência a^d onde a é um real e d é um natural.

Invariantes de laço e indução matemática

Exemplo: usando *invariante de laços*, provaremos a corretude de um algoritmo que calcula a potência a^d onde a é um real e d é um natural.

$\textsc{Potencia}(a, d)$ $\quad \triangleright$ devolve a^d

$\quad y \leftarrow a$, $n \leftarrow d$, $x \leftarrow 1$
$\quad$ **enquanto** $n > 0$ **faça**
$\quad\quad$ **se** n é ímpar **então** $x \leftarrow xy$
$\quad\quad$ $n \leftarrow \lfloor n/2 \rfloor$
$\quad\quad$ $y \leftarrow y^2$
$\quad$ **devolva** x

```
POTENCIA(a, d)      ▷ devolve a^d
    y ← a, n ← d, x ← 1
    enquanto n > 0 faça
        se n é ímpar então x ← xy
        n ← ⌊n/2⌋
        y ← y²
    devolva x
```

$a = 2, d = 11$

y	n	x

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
  y ← a, n ← d, x ← 1
  enquanto n > 0 faça
      se n é ímpar então x ← xy
      n ← ⌊n/2⌋
      y ← y²
  devolva x
```

$a = 2, d = 11$

y	n	x
2	11	1

POTENCIA(a, d) ▷ devolve a^d

```
y ← a, n ← d, x ← 1
enquanto n > 0 faça
    se n é ímpar então x ← xy
    n ← ⌊n/2⌋
    y ← y²
devolva x
```

$a = 2, d = 11$

y	n	x
2	11	1
4	5	2

Invariantes de laço e indução matemática

Potencia(a, d) ▷ devolve a^d

$y \leftarrow a$, $n \leftarrow d$, $x \leftarrow 1$
enquanto $n > 0$ **faça**
  se n é ímpar **então** $x \leftarrow xy$
  $n \leftarrow \lfloor n/2 \rfloor$
  $y \leftarrow y^2$
devolva x

$a = 2, d = 11$

y	n	x
2	11	1
4	5	2
16	2	8

Invariantes de laço e indução matemática

```
POTENCIA(a, d)      ▷ devolve a^d
    y ← a, n ← d, x ← 1
    enquanto n > 0 faça
        se n é ímpar então x ← xy
        n ← ⌊n/2⌋
        y ← y^2
    devolva x
```

$a = 2, d = 11$

y	n	x
2	11	1
4	5	2
16	2	8
256	1	8

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
y ← a, n ← d, x ← 1
enquanto n > 0 faça
    se n é ímpar então x ← xy
    n ← ⌊n/2⌋
    y ← y²
devolva x
```

$a = 2, d = 11$

y	n	x
2	11	1
4	5	2
16	2	8
256	1	8
262144	0	2048

Invariantes de laço e indução matemática

```
POTENCIA(a, d)      ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

$a = 2, d = 11$

y	n	x
2	11	1
4	5	2
16	2	8
256	1	8
262144	0	2048

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

POTENCIA(a, d) ▷ devolve a^d

1 $y \leftarrow a$, $n \leftarrow d$, $x \leftarrow 1$
2 **enquanto** $n > 0$ **faça**
3   **se** n é ímpar **então** $x \leftarrow xy$
4     $n \leftarrow \lfloor n/2 \rfloor$
5     $y \leftarrow y^2$
6 **devolva** x

$a = 2, d = 11$

y	n	x
2	11	1
4	5	2
16	2	8
256	1	8
262144	0	2048

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Note que quando o algoritmo para, temos $n = 0$ e o invariante implica que $a^d = x$. Isto mostra que o algoritmo funciona.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1  y ← a, n ← d, x ← 1
2  enquanto n > 0 faça
3      se n é ímpar então x ← xy
4      n ← ⌊n/2⌋
5      y ← y^2
6  devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Provaremos o invariante por indução no número de iterações.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Provaremos o invariante por indução no número de iterações.

Base: O invariante claramente vale no início da primeira iteração pois $y = a$, $n = d$ e $x = 1$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1    y ← a, n ← d, x ← 1
2    enquanto n > 0 faça
3        se n é ímpar então x ← xy
4        n ← ⌊n/2⌋
5        y ← y^2
6    devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Hipótese de indução: Suponha que o invariante vale no início de **alguma iteração**.

Invariantes de laço e indução matemática

```
Potencia(a, d)    ▷ devolve a^d
1  y ← a, n ← d, x ← 1
2  enquanto n > 0 faça
3      se n é ímpar então x ← xy
4      n ← ⌊n/2⌋
5      y ← y^2
6  devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Hipótese de indução: Suponha que o invariante vale no início de **alguma iteração**.

Passo de indução: Mostraremos que o invariante vale no início da **próxima iteração**.

Invariantes de laço e indução matemática

```
Potencia(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

No início da próxima iteração o valor de y será $y' = y^2$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

No início da próxima iteração o valor de y será $y' = y^2$.

Se n é par $(n = 2k)$ então o valor de n na próxima iteração é $n' := k$ e o valor de x será $x' = x$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

No início da próxima iteração o valor de y será $y' = y^2$.

Se n é par $(n = 2k)$ então o valor de n na próxima iteração é $n' := k$ e o valor de x será $x' = x$.

Por HI temos que $a^d = y^n x$. Assim, $a^d = y^n x = (y^2)^k x = (y')^{n'} x'$ e o invariante vale na próxima iteração. ■

Invariantes de laço e indução matemática

Potencia(a, d) ▷ devolve a^d

1 $y \leftarrow a$, $n \leftarrow d$, $x \leftarrow 1$
2 **enquanto** $n > 0$ **faça**
3   **se** n é ímpar **então** $x \leftarrow xy$
4     $n \leftarrow \lfloor n/2 \rfloor$
5     $y \leftarrow y^2$
6 **devolva** x

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

Invariantes de laço e indução matemática

POTENCIA(a, d) $\triangleright$ devolve a^d

1 $y \leftarrow a$, $n \leftarrow d$, $x \leftarrow 1$
2 **enquanto** $n > 0$ **faça**
3   **se** n é ímpar **então** $x \leftarrow xy$
4     $n \leftarrow \lfloor n/2 \rfloor$
5     $y \leftarrow y^2$
6 **devolva** x

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

No início da próxima iteração o valor de y será $y' = y^2$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1   y ← a, n ← d, x ← 1
2   enquanto n > 0 faça
3       se n é ímpar então x ← xy
4       n ← ⌊n/2⌋
5       y ← y^2
6   devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

No início da próxima iteração o valor de y será $y' = y^2$.

Se n é ímpar ($n = 2k + 1$) então o valor de n na próxima iteração é $n' := k$ e o valor de x será $x' = xy$.

Invariantes de laço e indução matemática

```
POTENCIA(a, d)    ▷ devolve a^d
1  y ← a, n ← d, x ← 1
2  enquanto n > 0 faça
3      se n é ímpar então x ← xy
4      n ← ⌊n/2⌋
5      y ← y^2
6  devolva x
```

Invariante:

No início de cada iteração da linha 2 vale que $a^d = y^n x$.

No início da próxima iteração o valor de y será $y' = y^2$.

Se n é ímpar ($n = 2k + 1$) então o valor de n na próxima iteração é $n' := k$ e o valor de x será $x' = xy$.

Por HI temos que $a^d = y^n x$. Assim, $a^d = y^n x = (y^2)^k yx = (y')^{n'} x'$ e o invariante vale na próxima iteração.

- No caso de algoritmos mais complicados, com laços encaixados, para provar formalmente a correção deste, é necessário demonstrar invariantes auxiliares (para cada laço).

Invariantes de laço e indução matemática

- No caso de algoritmos mais complicados, com laços encaixados, para provar formalmente a correção deste, é necessário demonstrar invariantes auxiliares (para cada laço).
- Além disso, deve-se ter um invariante principal (do laço principal) que implica na corretude do algoritmo.

Invariantes de laço e indução matemática

- No caso de algoritmos mais complicados, com laços encaixados, para provar formalmente a correção deste, é necessário demonstrar invariantes auxiliares (para cada laço).
- Além disso, deve-se ter um invariante principal (do laço principal) que implica na corretude do algoritmo.
- Os invariantes auxiliares podem/devem ser usados para provar o invariante principal.

Invariantes de laço e indução matemática

Eis um exemplo bem simples:

O algoritmo FIND recebe uma matriz real $A[1\,..\,m, 1\,..\,n]$ e um real x e devolve (i) índices i, j tais que $A[i,j] = x$ ou (ii) FALSE, se tais índices não existirem.

```
FIND(A, m, n, x)
    para i ← 1 até m faça
        para j ← 1 até n faça
            se  A[i, j] = x então devolva i, j
    devolva FALSE
```

Invariantes de laço e indução matemática

Eis um exemplo bem simples:

O algoritmo FIND recebe uma matriz real $A[1 \,..\, m, 1 \,..\, n]$ e um real x e devolve (i) índices i, j tais que $A[i,j] = x$ ou (ii) FALSE, se tais índices não existirem.

FIND(A, m, n, x)
1 **para** $i \leftarrow 1$ **até** m **faça**
2   **para** $j \leftarrow 1$ **até** n **faça**
3   **se** $A[i,j] = x$ **então devolva** i, j
4 **devolva** FALSE

- Convenciona-se que quando o laço na linha 1 para, temos $i = m + 1$.

Invariantes de laço e indução matemática

Eis um exemplo bem simples:

O algoritmo FIND recebe uma matriz real $A[1\,..\,m, 1\,..\,n]$ e um real x e devolve (i) índices i, j tais que $A[i,j] = x$ ou (ii) FALSE, se tais índices não existirem.

FIND(A, m, n, x)

1 **para** $i \leftarrow 1$ **até** m **faça**
2   **para** $j \leftarrow 1$ **até** n **faça**
3   **se** $A[i,j] = x$ **então devolva** i, j
4 **devolva** FALSE

- Convenciona-se que quando o laço na linha 1 para, temos $i = m + 1$.
- Analogamente, quando o laço na linha 2 para, temos $j = n + 1$.

Invariantes de laço e indução matemática

$\textsc{Find}(A, m, n, x)$

para $i \leftarrow 1$ **até** m **faça**
  para $j \leftarrow 1$ **até** n **faça** $\triangleright$ procura x em $A[i, 1\,..\,n]$
    se $A[i, j] = x$ **então devolva** i, j
devolva FALSE

Observações:

$\text{FIND}(A, m, n, x)$
```
para i ← 1 até m faça
    para j ← 1 até n faça ▷ procura x em A[i, 1 . . n]
        se A[i, j] = x então devolva i, j
devolva FALSE
```

Observações:

- O algoritmo FIND sempre para.

Invariantes de laço e indução matemática

FIND(A, m, n, x)
1 **para** $i \leftarrow 1$ **até** m **faça**
2   **para** $j \leftarrow 1$ **até** n **faça** $\triangleright$ procura x em $A[i, 1..n]$
3   **se** $A[i, j] = x$ **então devolva** i, j
4 **devolva** FALSE

Observações:

- O algoritmo FIND sempre para.
- Se FIND para na linha 3 então obviamente ele devolve a resposta correta.

Invariantes de laço e indução matemática

```
FIND(A, m, n, x)
1   para i ← 1 até m faça
2       para j ← 1 até n faça    ▷ procura x em A[i, 1 . . n]
3           se A[i, j] = x então devolva i, j
4   devolva FALSE
```

Observações:

- O algoritmo FIND sempre para.
- Se FIND para na linha 3 então obviamente ele devolve a resposta correta.
- O que precisamos é de um invariante para mostrar que se FIND para na linha 4, então a resposta está correta.

Invariantes de laço e indução matemática

FIND(A, m, n, x)

1 **para** $i \leftarrow 1$ **até** m **faça**
2 **para** $j \leftarrow 1$ **até** n **faça** $\triangleright$ procura x em $A[i, 1 \mathinner{..} n]$
3 **se** $A[i, j] = x$ **então devolva** i, j
4 **devolva** FALSE

Invariante principal:

No início de cada iteração da linha 1, vale que x não está nos vetores $A[1, \cdot], A[2, \cdot], \ldots, A[i-1, \cdot]$.

Invariantes de laço e indução matemática

```
FIND(A, m, n, x)
1   para i ← 1 até m faça
2      para j ← 1 até n faça ▷ procura x em A[i, 1 . . n]
3         se  A[i, j] = x então devolva i, j
4   devolva FALSE
```

Invariante principal:

No início de cada iteração da linha 1, vale que x não está nos vetores $A[1,\cdot], A[2,\cdot], \ldots, A[i-1,\cdot]$.

É fácil ver agora que se FIND para na linha 4 ($i = m + 1$) e o invariante vale, então o algoritmo devolve a resposta correta.

Invariantes de laço e indução matemática

FIND(A, m, n, x)
1 **para** $i \leftarrow 1$ **até** m **faça**
2   **para** $j \leftarrow 1$ **até** n **faça** $\triangleright$ procura x em $A[i, 1\,..\,n]$
3   **se** $A[i,j] = x$ **então devolva** i, j
4 **devolva** FALSE

Invariante principal:

No início de cada iteração da linha 1, vale que x não está nos vetores $A[1,\cdot], A[2,\cdot], \ldots, A[i-1,\cdot]$.

Invariantes de laço e indução matemática

FIND(A, m, n, x)
1 **para** $i \leftarrow 1$ **até** m **faça**
2 **para** $j \leftarrow 1$ **até** n **faça** $\triangleright$ procura x em $A[i, 1 \mathinner{..} n]$
3 **se** $A[i, j] = x$ **então devolva** i, j
4 **devolva** FALSE

Invariante principal:

No início de cada iteração da linha 1, vale que x não está nos vetores $A[1, \cdot], A[2, \cdot], \ldots, A[i-1, \cdot]$.

Invariante auxiliar:

No ínicio de cada iteração da linha 2, vale que $x \notin A[i, 1 \mathinner{..} j-1]$.

- No exemplo visto, os invariantes não são difíceis de adivinhar. Além disso, são simples de verificar.

- No exemplo visto, os invariantes não são difíceis de adivinhar. Além disso, são simples de verificar.
- Em outros casos, os invariantes podem não ser nada óbvios pois o algoritmo pode ser muito complicado, ou o invariante é baseado em alguma propriedade matemática não trivial.

Invariantes de laço e indução matemática

- No exemplo visto, os invariantes não são difíceis de adivinhar. Além disso, são simples de verificar.
- Em outros casos, os invariantes podem não ser nada óbvios pois o algoritmo pode ser muito complicado, ou o invariante é baseado em alguma propriedade matemática não trivial.
- Uma vez adivinhados os invariantes, em geral, não é muito difícil verificar a validade deles. Às vezes, pode ser necessário colocar mais invariantes para facilitar a prova.

Invariantes de laço e indução matemática

- No exemplo visto, os invariantes não são difíceis de adivinhar. Além disso, são simples de verificar.
- Em outros casos, os invariantes podem não ser nada óbvios pois o algoritmo pode ser muito complicado, ou o invariante é baseado em alguma propriedade matemática não trivial.
- Uma vez adivinhados os invariantes, em geral, não é muito difícil verificar a validade deles. Às vezes, pode ser necessário colocar mais invariantes para facilitar a prova.
- Deve-se dizer que o processo de verificar a validade de um invariante pode ser técnico e tedioso...