MC458 — Projeto e Análise de Algoritmos I

Cid Carvalho de Souza Cândida Nunes da Silva Orlando Lee

7 de março de 2016

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.
- Esses slides são o fruto de um trabalho colaborativo de vários professores.
- 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, "Cormen" e "Manber").

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.
- Eis a lista de "colaboradores" (em ordem alfabética):
  - 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.
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 verdadeiro.
- **Passo de Indução:** Provamos que $P(n+1)$ é verdadeiro, a partir da hipótese de indução.

Exemplo:

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

Demonstração por Indução

Outra forma equivalente:

- **Base da Indução:** Demonstramos $P(1)$.
- **Hipótese de Indução:** Supomos que $P(n-1)$ é verdadeiro.
- **Passo de Indução:** Provamos que $P(n)$ é verdadeiro, a partir da hipótese de indução.

Exemplo:

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

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 verdadeiro.
- **Passo de Indução:** Provamos que $P(n)$ é verdadeiro, a partir da hipótese de indução.

Exemplo:

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

Indução Fraca × Indução Forte

A *indução forte* difere da *indução fraca* (ou *simples*) apenas na suposição da hipótese.
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 verdadeiro, para todo $1 \leq k < n$.
- **Passo de Indução:** Provamos que $P(n)$ é verdadeiro, 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 $x - 1$.

Demonstração:

- A **base da indução** é, naturalmente, o caso $n = 1$. Temos que $x^n - 1 = x - 1$, que é obviamente divisível por $x - 1$. Isso encerra a demonstração da base da indução.

Exemplo 1 (cont.)

- A **hipótese de indução** é: Suponha que $x^n - 1$ seja divisível por $x - 1$ para todo natural $x \geq 1$.
- O **passo de indução** é: Supondo a h.i., mostraremos que $x^{n+1} - 1$ é divisível por $x - 1$, para todo natural $x \geq 1$.

  Primeiro reescrevemos $x^{n+1} - 1$ como

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

  Pela h.i., $x^n - 1$ 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. ■

Exemplo 2

Prove que todo natural $n \geq 8$ pode ser escrito como soma de 3's e 5's. (postagem de selos com valores 3 ou 5)

- A **base da indução** consiste nos seguintes casos:

$$\begin{aligned} 8 &= 3 + 5, \\ 9 &= 3 + 3 + 3 + 3, \\ 10 &= 5 + 5. \end{aligned}$$

  Isto completa a prova da base da indução.

  É necessário aumentar a base por causa do **passo de indução** feito a seguir.

Exemplo 2 (cont.)

- A **hipótese de indução (forte)** é: Para todo natural k tal que $8 \leq k < n$, temos que k pode ser escrito como uma soma de 3's e 5's.
- O **passo de indução** é: Supondo a h.i., mostraremos que n pode ser escrito como uma soma de 3's e 5's.

  Note que $n = (n - 3) + 3$.

  Como $n \geq 11$ temos que $n - 3 \geq 8$ e pela h.i., $(n - 3)$ pode ser escrito como uma soma de 3's e 5's.

  Portanto, n também pode e isto completa a prova por indução. ■

Exemplo 3

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

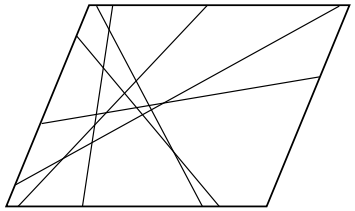
$$R_n = \frac{n(n+1)}{2} + 1.$$

Um conjunto de retas está em posição geral no plano se

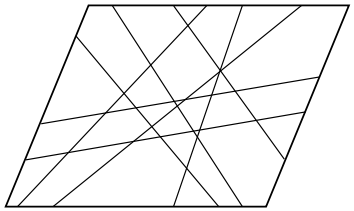
- todas as retas são concorrentes, isto é, não há retas paralelas e
- não há três retas interceptando-se no mesmo ponto.

Exemplo 3 (cont.)

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.)

Demonstração: A idéia que queremos explorar para o passo de indução é a seguinte: supondo que a fórmula vale para n, adicionar uma nova reta em posição geral e tentar assim obter a validade de $n+1$.

- A **base da indução** é, naturalmente, $n = 1$. Uma reta sozinha divide o plano em duas regiões. De fato,

$$R_1 = (1 \times 2)/2 + 1 = 2.$$

Isto conclui a prova para $n = 1$.

Exemplo 3 (cont.)

- A **hipótese de indução** é: Suponha que $R_n = n(n+1)/2 + 1$.
- O **passo de indução é:** Supondo a h.i., mostraremos que para $n+1$ retas em posição geral vale que

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

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

Exemplo 3 (cont.)

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

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

Isso conclui a demonstração. ■

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 $n \geq 1$.

Demonstração:

- A **base da indução** é $n = 1$, para a qual a desigualdade se reduz a $\frac{1}{2} < 1$, obviamente verdadeira.
- A **hipótese de indução** é: Suponha que $S_n < 1$.

Exemplo 4 (cont.)

- O **passo de indução** é: Supondo a h.i., mostraremos que $Sn + 1 < 1$.

Pela definição de S_n, temos que

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

Pela hipótese de indução, $S_n < 1$. Entretanto, nada podemos dizer acerca de S_{n+1} em conseqüência da hipótese, já que não há nada que impeça que $S_{n+1} \geq 1$.

É preciso manipular S_{n+1} de outra maneira.

Exemplo 4 (cont.)

- O **passo de indução** é: Supondo a h.i., mostraremos que $Sn + 1 < 1$.

Então

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

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

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

Demonstração:

- A **base da indução** é $n = 1$ e o resultado é óbvio.

Exemplo 5 (cont.)

- A **hipótese de indução** é: Suponha que $S_n \leq 2$.

  Pela definição de S_n, temos que

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

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

  Além disso, não parece fácil manipular a expressão para obter uma forma melhor de aplicar a h.i.

Exemplo 5 (cont.)

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

- A **hipótese de indução** é: 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.)

- O **passo de indução** é: Supondo a h.i., mostraremos que $S_{n+1} \leq 2$.

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

  onde a última desigualdade segue do fato de que

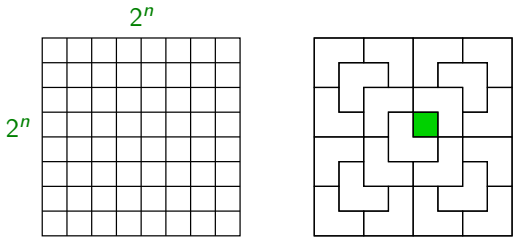
$$\frac{1}{n} - \frac{1}{n+1} = \frac{1}{n(n+1)} > \frac{1}{(n+1)^2}.$$

  Isto completa a prova por indução. ■

Exemplo 6

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

Para retribuir tanta generosidade, a UNICOMP decidiu construir um grande pátio de dimensões $2^n \times 2^n$ e cobri-lo com azulejos 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 azulejos em forma de L deixando uma casa central livre.

Demonstração:

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

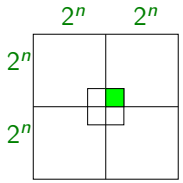
Isto completa a prova do caso base.

Exemplo 6 (cont.)

- A **hipótese de indução** é: É possível cobrir um quadrado $2^n \times 2^n$ deixando uma casa central livre.
- O **passo de indução** é: Supondo a h.i., mostraremos que é possível cobrir quadrado $2^{n+1} \times 2^{n+1}$ deixando uma casa central livre.
- Um quadrado $2^{n+1} \times 2^{n+1}$ pode ser dividido em 4 quadrados $2^n \times 2^n$ como na figura seguinte.

Exemplo 6 (cont.)

-

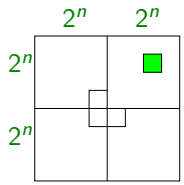


- Observando a figura, a ideia óbvia é aplicar a h.i. em cada um dos 4 quadrados $2^n \times 2^n$ e completar com um azulejo nas três casas centrais.
- O problema é que a h.i. diz que é possível cobrir cada quadrado $2^n \times 2^n$ deixando livre uma casa central e não a dos cantos como queremos agora.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

Exemplo 6 (cont.)

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

- A **hipótese de indução** é: É possível cobrir um quadrado $2^n \times 2^n$ deixando livre **qualquer casa desejada**.



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

  Colocamos então mais um azulejo nas três casas centrais do quadrado de dimensão $2^{n+1} \times 2^{n+1}$. Isto completa a prova. ■

Algumas armadilhas - redução × expansão

- A demonstração do passo da indução simples supõe a proposição válida para um $n-1$ e mostra que é válida para n.
- 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 a prova da proposição para casos particulares de estruturas de tamanho n e não todos, como se espera.

Algumas armadilhas - redução × expansão

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

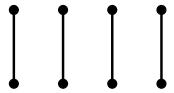
Prove que todo grafo simples com $n \geq 2$ vértices e tal que cada vértice tem grau pelo menos 1 é conexo.

- O **caso base** é $n = 2$ e claramente o resultado vale.
- A **hipótese de indução** é: O resultado vale para todo grafo com n vértices.
- O **passo de indução** é: 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 h.i., 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. ■

Algumas armadilhas - redução × expansão

- 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.

Algumas armadilhas - outros passos mal dados

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

Proposição:

Considere n retas no plano, concorrentes duas a duas. Então existe um ponto comum a todas as n retas.

Demonstração:

- A base da indução é o caso $n = 1$, claramente verdadeiro.
- Para o caso $n = 2$, também é fácil ver que a proposição é verdadeira.
- Considere a proposição válida para $n - 1$, $n > 2$, e considere n retas no plano concorrentes duas a duas.

Algumas armadilhas - outros passos mal dados

Pela h.i., todo subconjunto de $n - 1$ das n retas têm um ponto em comum. Sejam S_1, S_2 dois desses subconjuntos, distintos entre si.

A interseção $S_1 \cap S_2$ contém $n - 2$ retas. Portanto, o ponto em comum às retas de S_1 tem que ser igual ao ponto em comum às retas de S_2, senão duas retas distintas de $S_1 \cap S_2$ se tocariam em mais que um ponto, o que não é possível.

Portanto, a asserção vale para n, completando a demonstração.
Certo?

Errado!

O argumento no passo de indução funciona para todo $n > 2$, exceto $n = 3$. pois nesse caso $S_1 \cap S_2$ contém apenas uma reta. Não é possível concluir a validade para $n = 3$. De fato, a afirmação não vale para $n \geq 3$.

Invariantes de laço e indução matemática

Definição:

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.

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

Invariantes de laço e indução matemática

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

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 3 temos que $a^d = y^n x$.

Invariantes de laço e indução matemática

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

Invariante: No início de cada iteração da linha 3 temos que $a^d = y^n x$.

Vamos provar por indução no número de iterações que o invariante vale. O invariante vale no início da primeira iteração pois $y = a$, $n = d$ e $x = 1$.

Suponha então que ele vale no início de alguma iteração e mostraremos que ele vale no início da próxima.

Invariantes de laço e indução matemática

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

Invariante: No início de cada iteração da linha 3 temos 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 h.i. temos que $a^d = y^n x$. Assim, $a^d = (y^2)^{2k} yx = y^{n'} x'$ e o invariante vale.

Invariantes de laço e indução matemática

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

Invariante: No início de cada iteração da linha 3 temos 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 h.i. temos que $a^d = y^n x$. Assim, $a^d = (y^2)^{2k} x = y^{n'} x'$ e o invariante vale.

Invariantes de laço e indução matemática

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

Invariante: No início de cada iteração da linha 3 temos que $a^d = y^n x$.

Assim, o invariante vale. Note que quando o algoritmo para, temos $n = 0$ e portanto $x = a^d$.