

Projeto e Análise de Algoritmos*

Correção de algoritmos

Lehilton Pedrosa

Segundo Semestre de 2017

*Criado por C. de Souza, C. da Silva, O. Lee, F. Miyazawa et al.

Técnicas de demonstração

Demonstração Direta

A *demonstração direta* de uma implicação $p \Rightarrow q$ é uma sequência de passos lógicos (implicações):

$$p \Rightarrow p_1 \Rightarrow p_2 \Rightarrow \cdots \Rightarrow p_n \Rightarrow q,$$

que resultam, por transitividade, na implicação desejada. Cada passo da demonstração é um axioma ou um teorema demonstrado previamente.

Exemplo:

Provar que $\sum_{i=1}^k (2i - 1) = k^2$.

Demonstração pela Contrapositiva

A *contrapositiva* de $p \Rightarrow q$ é $\neg q \Rightarrow \neg p$.

A contrapositiva é equivalente à implicação original. A veracidade de $\neg q \Rightarrow \neg p$ implica a veracidade de $p \Rightarrow q$, e vice-versa.

A técnica é útil quando é mais fácil demonstrar a contrapositiva que a implicação original.

Para demonstrarmos a contrapositiva de uma implicação, podemos utilizar qualquer técnica de demonstração.

Exemplo:

Provar que se $2 \mid 3m$, então $2 \mid m$.

Demonstração por Contradição

A *Demonstração por contradição* envolve supor absurdamente que a afirmação a ser demonstrada é falsa e obter, através de implicações válidas, uma conclusão contraditória.

A contradição obtida implica que a hipótese absurda é falsa e, portanto, a afirmação é de fato verdadeira.

No caso de uma implicação $p \Rightarrow q$, equivalente a $\neg p \vee q$, a negação é $p \wedge \neg q$.

Exemplo:

$\sqrt{2}$ é irracional.

Demonstração por Casos

Na *Demonstração por Casos*, particionamos o universo de possibilidades em um conjunto finito de casos e demonstramos a veracidade da implicação para cada caso. Para demonstrar cada caso individual, qualquer técnica de demonstração pode ser utilizada.

Exemplo:

Provar que a soma de dois inteiros x e y de mesma paridade é sempre par.

Princípio da Indução

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:

Prove que 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:

Prove que 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:

Prove que todo inteiro $n \geq 2$ 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:

Prove que todo inteiro $n \geq 2$ pode ser fatorado como um produto de um ou mais primos.

Exemplo 1

Demonstre que, para inteiros $x \geq 1$ 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 .*
- ▶ O passo de indução é: *Supondo a h.i., vamos mostrar $x^{n+1} - 1$ é divisível por $x - 1$, para todo natural x .*
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

Demonstre que a equação

$$\sum_{i=1}^n (3 + 5i) = 2.5n^2 + 5.5n$$

vale para todo inteiro $n \geq 1$.

Demonstração:

- ▶ A base da indução é, naturalmente, o caso $n = 1$. Temos

$$\sum_{i=1}^1 (3 + 5i) = 8 = 2.5 \times 1^2 + 5.5 \times 1.$$

Portanto, a somatória tem o valor previsto pela fórmula fechada, demonstrando que a equação vale para $n = 1$.

Exemplo 2 (cont.)

- ▶ A hipótese de indução é: *Suponha que a equação vale para n .*
- ▶ O passo de indução é: *Supondo a h.i., vamos mostrar que a equação vale para o valor $n + 1$. O caminho é simples:*

$$\begin{aligned}\sum_{i=1}^{n+1} (3 + 5i) &= \sum_{i=1}^n (3 + 5i) + (3 + 5(n + 1)) \\ &= 2.5n^2 + 5.5n + (3 + 5(n + 1)) \text{ (pela h.i.)} \\ &= 2.5n^2 + 5.5n + 5n + 8 \\ &= 2.5n^2 + 5n + 2.5 + 5.5n + 5.5 \\ &= 2.5(n + 1)^2 + 5.5(n + 1).\end{aligned}$$

A última linha da dedução mostra que a fórmula vale para $n + 1$. A demonstração por indução está completa. ■

Exemplo 3

Demonstre que a inequação

$$(1 + x)^n \geq 1 + nx$$

vale para todo natural n e real x tal que $(1 + x) > 0$.

Demonstração:

- ▶ A base da indução é, novamente, $n = 1$. Nesse caso, ambos os lados da inequação são iguais a $1 + x$, mostrando a sua validade. Isto encerra a prova do caso base.

Exemplo 3 (cont.)

- ▶ A hipótese de indução é: Suponha que a inequação vale para n , isto é, $(1+x)^n \geq 1+nx$ para todo real x tal que $(1+x) > 0$.
- ▶ O passo de indução é: Supondo a h.i., vamos mostrar que a inequação vale para o valor $n+1$, isto é, $(1+x)^{n+1} \geq 1+(n+1)x$ para todo x tal que $(1+x) > 0$. Novamente, a dedução é simples:

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x) \\ &\geq (1+nx)(1+x) \text{ (pela h.i. e } (1+x) > 0) \\ &= 1+(n+1)x+nx^2 \\ &\geq 1+(n+1)x \text{ (já que } nx^2 \geq 0)\end{aligned}$$

A última linha mostra que a inequação vale para $n+1$, completando a demonstração. ■

Exemplo 4

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

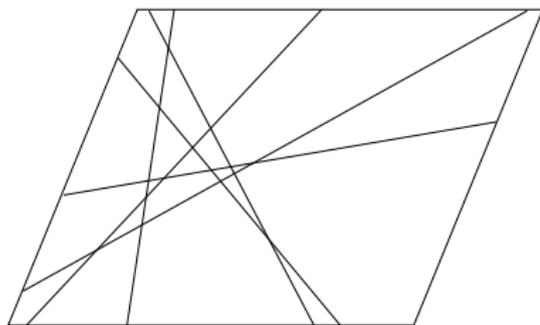
$$T_n = \frac{n(n+1)}{2} + 1.$$

Um conjunto de retas está em **posição geral** no plano se

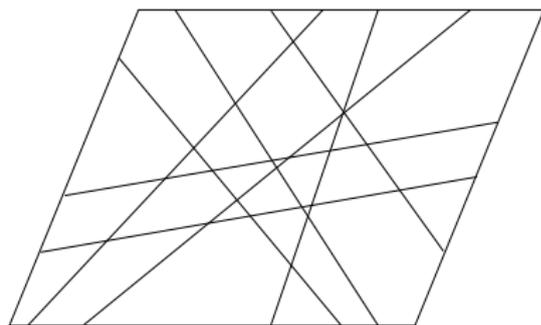
- ▶ todas as retas são concorrentes, isto é, não há retas paralelas e
- ▶ não há três retas interceptando-se no mesmo ponto.

Exemplo 4 (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 4 (cont.)

Demonstração: A ideia 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,

$$T_1 = (1 \times 2)/2 + 1 = 2.$$

Isto conclui a prova para $n = 1$.

Exemplo 4 (cont.)

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

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

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 4 (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, podemos escrever que

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

Isso conclui a demonstração. ■

Exemplo 5

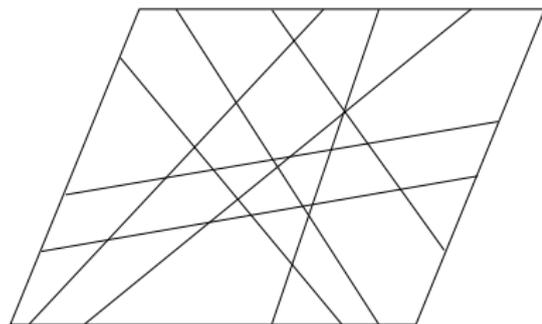
Definição:

Um conjunto de n retas no plano define regiões convexas cujas bordas são segmentos das n retas. Duas dessas regiões são *adjacentes* se as suas bordas se intersectam em algum segmento de reta não trivial, isto é contendo mais que um ponto.

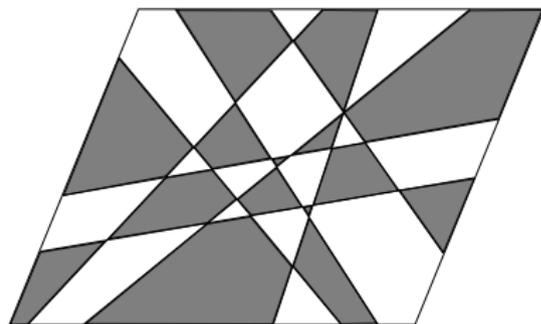
Uma *k -coloração* dessas regiões é uma atribuição de uma de k cores a cada uma das regiões, de forma que regiões adjacentes recebam cores distintas.

Exemplo 5 (cont.)

Veja exemplos dessas definições:



As regiões convexas



Uma 2-coloração do plano

Exemplo 5 (cont.)

Demonstre que para todo $n \geq 1$, existe uma 2-coloração das regiões formadas por n retas no plano.

Demonstração:

- ▶ A base da indução é, naturalmente, $n = 1$. Uma reta sozinha divide o plano em duas regiões. Atribuindo-se cores diferentes a essas regiões obtemos o resultado desejado.

Isto conclui a prova para $n = 1$.

Exemplo 5 (cont.)

- ▶ A hipótese de indução é: *Suponha que sempre existe uma 2-coloração das regiões formadas por n retas no plano.*
- ▶ O passo de indução é: *Supondo a h.i., vamos exibir uma 2-coloração para as regiões formadas por $n + 1$ retas no plano.*

A demonstração do passo consiste em observar que a adição de uma nova reta r divide cada região atravessada por r em duas, e definir a nova 2-coloração da seguinte forma: as regiões em um lado de r mantêm a cor herdada da hipótese de indução; as regiões no outro lado de r têm suas cores trocadas.

Como demonstrar que a 2-coloração obtida nesse processo obedece à definição?

Exemplo 6

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

Demonstre que a série S_n definida abaixo satisfaz

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

para todo inteiro $n \geq 1$.

Demonstração:

A base é $n = 1$, para a qual a inequação se reduz a $\frac{1}{2} < 1$, obviamente verdadeira.

Como **hipótese de indução**, supomos que $S_n < 1$ para um valor $n \geq 1$. Vamos mostrar que $S_{n+1} < 1$.

Exemplo 6 (cont.)

Pela definição de S_n , temos $S_{n+1} = S_n + \frac{1}{2^{n+1}}$.

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

A ideia aqui é manipular S_{n+1} um pouco mais:

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

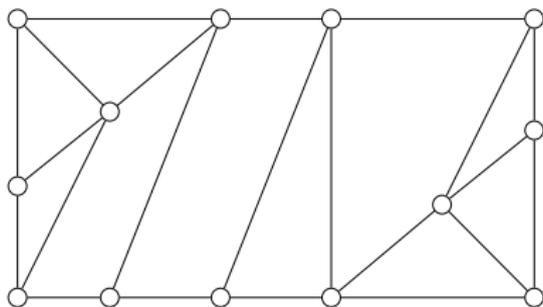
Isto conclui a demonstração. ■

Exemplo 7

Veremos a seguir um exemplo da aplicação de indução em Teoria dos Grafos.

Definição:

Um *grafo planar* é um grafo que pode ser desenhado no plano sem que suas arestas se cruzem. Um *grafo plano* é um desenho de grafo planar no plano, sem cruzamento de arestas (há inúmeros desenhos possíveis). Veja um exemplo de um grafo planar e um desenho possível dele no plano.



Exemplo 7 (cont.)

Definição:

- ▶ Um grafo plano define um conjunto F de *faces* no plano, que são as regiões contínuas **maximais** do desenho, livre de segmentos de retas ou pontos.
- ▶ Os *componentes* de um grafo são seus subgrafos maximais para os quais existe um caminho entre quaisquer dois de seus vértices.
- ▶ Dado um grafo plano G , com v vértices, e arestas, f faces e c componentes, a *Fórmula de Euler* (F.E.) é a equação

$$v - e + f = 1 + c.$$

Queremos demonstrar a Fórmula de Euler por indução.

Exemplo 7 (cont.)

- ▶ Há várias possibilidades para se fazer indução neste caso. No livro de U. Manber encontra-se uma indução em duas variáveis, a chamada *indução dupla*, primeiro em v depois em f . Além disso, lá a Fórmula de Euler está descrita diferentemente, sem especificar o número de componentes. Isso torna a indução um pouco mais complicada.
- ▶ Nossa formulação é mais geral simplificando a demonstração. Esse um fenômeno comum em matemática: formulações mais poderosas quase sempre resultam em demonstrações mais simples.
- ▶ Vamos demonstrar a F.E. por indução em e , o número de arestas do grafo plano G .

Exemplo 7 (cont.)

Demonstração:

- ▶ A base da indução é $e = 0$. Temos $f = 1$ e $c = v$ e

$$v - e + f = v + 1 = 1 + c$$

como desejado. Isso demonstra a base.

- ▶ A hipótese de indução é: *Suponha que a F.E. vale para todo grafo com $e - 1$ arestas.*
- ▶ Seja G um grafo plano com e arestas, v vértices, f faces e c componentes. Seja a uma aresta qualquer de G . A remoção de a de G cria um novo grafo plano G' com $v' = v$ vértices e $e' = e - 1$ arestas, f' faces e c' componentes. A remoção de a de G pode ou não ter desconectado um componente de G . Caso tenha, $c' = c + 1$ e $f' = f$ (por quê?). Caso contrário, teremos $c' = c$ e $f' = f - 1$ (por quê?).

Exemplo 7 (cont.)

- ▶ No caso em que houve a criação de novo componente, temos

$$\begin{aligned}v - e + f &= v' - (e' + 1) + f' \\ &= 1 + c' - 1 \text{ (pela h.i.)} \\ &= c' \\ &= 1 + c.\end{aligned}$$

- ▶ Caso contrário obtemos

$$\begin{aligned}v - e + f &= v' - (e' + 1) + (f' + 1) \\ &= v' - e' + f' \\ &= 1 + c' \text{ (pela h.i.)} \\ &= 1 + c.\end{aligned}$$

Em ambos casos obtemos o resultado desejado.



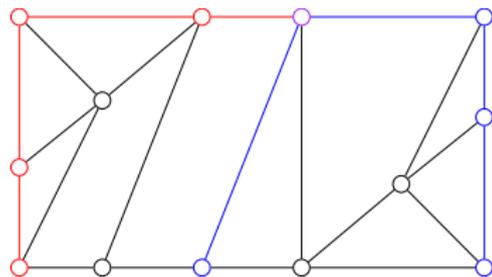
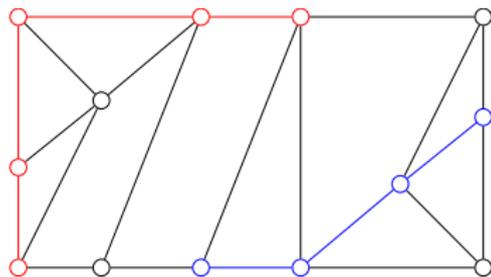
Exemplo 8

Este é um exemplo de indução forte. Antes algumas definições:

- ▶ Seja G um grafo não direcionado. O **grau** de um vértice v de G é o número de arestas incidentes a v , onde laços (arestas cujos extremos coincidem) são contados duas vezes.
- ▶ Um vértice é **ímpar** (**par**) se o seu grau é ímpar (par).
O número de vértices ímpares em um grafo é sempre par (por quê?).

Exemplo 8 (cont.)

Dois caminhos em G são **aresta-disjuntos** se não têm arestas em comum. Veja exemplos de caminhos aresta-disjuntos em um grafo:



Exemplo 8 (cont.)

Teorema:

Seja G um grafo (não direcionado) conexo e I o conjunto de vértices ímpares de G . Então é possível encontrar alguma partição de I em $|I|/2$ pares e caminhos aresta-disjuntos cujos extremos são os vértices de cada par.

Demonstração: A demonstração é por indução no número de arestas de G . Seja e esse número.

- ▶ A base da indução trata do caso $e = 0$, ou seja, de um grafo sem arestas e com um único vértice (pois G é conexo). Neste caso, $|I| = 0$ e o teorema é trivialmente verdadeiro.

Exemplo 8 (cont.)

- ▶ A hipótese de indução (forte) é:

Suponha que para todos os grafos conexos com menos que e arestas vale o resultado do enunciado do teorema.

Vamos mostrar que o resultado vale para todo grafo conexo com e arestas.

- ▶ Seja então G um grafo qualquer com e arestas. Se $I = \emptyset$ não há nada que provar. Caso contrário existe pelo menos um par u, v de vértices de I . Como G é conexo, existe um caminho π em G cujos extremos são u, v .
- ▶ Seja G' o grafo obtido removendo-se de G as arestas de π . O grafo G' tem menos que e arestas e dois vértices ímpares a menos.
- ▶ Embora seja tentador aplicar a h.i. a G' , nada garante que G' seja conexo. Se não for, a h.i. não se aplica.

Exemplo 8 (cont.)

- ▶ É possível consertar a situação mudando a hipótese para:
Suponha que para todos os grafos com menos que e arestas vale o seguinte: é possível encontrar alguma partição de V em $|V|/2$ pares, cada par na mesma componente, e os caminhos entre esses pares.

Veja que removemos a restrição de conexidade, fortalecendo a hipótese.

- ▶ Com essa nova hipótese, a demonstração é a mesma. Aqui escolhemos x e y na mesma componente para garantir a existência do caminho π . Agora podemos aplicar a h.i. a G' : os caminhos de G' e π são todos aresta-disjuntos e formam o conjunto de caminhos desejados para G . ■

Exercício: Demonstre esse mesmo teorema usando indução fraca

Exemplo 9

Este é um exemplo de **indução reversa**, cujo princípio pode ser enunciado da seguinte forma:

Suponha que

- ▶ *a proposição $P(n)$ vale para um subconjunto infinito dos números naturais, e*
- ▶ *se $P(n)$ vale para n então $P(n - 1)$ também vale.*

Então $P(n)$ vale para todo natural n .

Você consegue ver por que esse é um processo indutivo igualmente legítimo?

Exemplo 9 (cont.)

Teorema:

Se x_1, x_2, \dots, x_n são todos números reais positivos, então

$$(x_1 x_2 \dots x_n)^{\frac{1}{n}} \leq \frac{x_1 + x_2 + \dots + x_n}{n}.$$

Demonstração: Em dois passos:

1. Vamos mostrar que a inequação vale para todos os valores de n que são potências 2, isto é $n = 2^k$, para k inteiro ≥ 0 . Faremos esse passo por indução simples em k . Esse é o conjunto infinito de valores da indução reversa.
2. Mostraremos que se a inequação é verdadeira para n , então é verdadeira para $n - 1$.

Exemplo 9 (cont.)

- ▶ Se $n = 2^0 = 1$, então o teorema vale trivialmente.
- ▶ Se $n = 2^1 = 2$, a inequação também é válida já que

$$\sqrt{x_1 x_2} \leq \frac{x_1 + x_2}{2}$$

pode ser verificada tomando-se o quadrado dos dois lados.

$$\begin{aligned}\sqrt{x_1 x_2} &\leq (x_1 + x_2)/2 && \Leftrightarrow \\ x_1 x_2 &\leq (x_1^2 + 2x_1 x_2 + x_2^2)/4 && \Leftrightarrow \\ 2x_1 x_2 &\leq x_1^2 + x_2^2 && \Leftrightarrow \\ 0 &\leq x_1^2 - 2x_1 x_2 + x_2^2 && \Leftrightarrow \\ 0 &\leq (x_1 - x_2)^2\end{aligned}$$

Exemplo 9 (cont.)

(h.i.) Vamos supor agora que a inequação vale para $n = 2^k$, para k .

Considere $2n = 2^{k+1}$ e reescreva o lado esquerdo da inequação como

$$(x_1 x_2 \dots x_{2n})^{\frac{1}{2n}} = \sqrt{(x_1 x_2 \dots x_n)^{\frac{1}{n}} (x_{n+1} x_{n+2} \dots x_{2n})^{\frac{1}{n}}}.$$

Tome $y_1 = (x_1 x_2 \dots x_n)^{\frac{1}{n}}$ e $y_2 = (x_{n+1} x_{n+2} \dots x_{2n})^{\frac{1}{n}}$. Portanto

$$(x_1 x_2 \dots x_{2n})^{\frac{1}{2n}} = \sqrt{y_1 y_2} \leq \frac{y_1 + y_2}{2}$$

pelo caso $n = 2$ já demonstrado.

Exemplo 9 (cont.)

Além disso, podemos aplicar a h.i. a y_1 e y_2 , obtendo

$$y_1 \leq \frac{x_1 + x_2 + \dots + x_n}{n},$$

$$y_2 \leq \frac{x_{n+1} + x_{n+2} + \dots + x_{2n}}{n}.$$

Substituindo esses dois valores na inequação acima obtemos o resultado desejado para $2n$.

$$\begin{aligned} (x_1 x_2 \dots x_{2n})^{\frac{1}{2n}} &= \sqrt{y_1 y_2} \\ &\leq \frac{y_1 + y_2}{2} \\ &= \frac{x_1 + x_2 + \dots + x_n}{2n} + \frac{x_{n+1} + x_{n+2} + \dots + x_{2n}}{2n} \end{aligned}$$

Exemplo 9 (cont.)

Vamos agora utilizar o princípio de indução reversa. Suponha que o resultado vale para n e vamos mostrar que vale para $n - 1$.

Dados $n - 1$ números positivos x_1, x_2, \dots, x_{n-1} , defina

$$z := \frac{x_1 + x_2 + \dots + x_{n-1}}{n - 1}.$$

Por h.i., o teorema aplica-se a $x_1, x_2, \dots, x_{n-1}, z$. Portanto

$$\begin{aligned} (x_1 x_2 \dots x_{n-1} z)^{\frac{1}{n}} &\leq \frac{x_1 + x_2 + \dots + x_{n-1} + z}{n} \\ &= z. \end{aligned}$$

Exemplo 9 (cont.)

Então

$$(x_1 x_2 \dots x_{n-1} z)^{\frac{1}{n}} \leq z.$$

Elevando ambos os lados à potência $\frac{n}{n-1}$ obtemos

$$(x_1 x_2 \dots x_{n-1} z)^{\frac{1}{n-1}} \leq z^{\frac{n}{n-1}}.$$

Finalmente, multiplicando por $z^{-\frac{1}{n-1}}$ ambos os lados, obtemos

$$(x_1 x_2 \dots x_{n-1})^{\frac{1}{n-1}} \leq z = \frac{x_1 + x_2 + \dots + x_{n-1}}{n-1},$$

o que prova a asserção para $n-1$, completando a demonstração. ■

Algumas armadilhas - redução \times 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 problema do procedimento de expansão é que ele não é suficientemente geral, de forma que obtenhamos a implicação, a partir do caso $n - 1$, para um caso **geral** n .

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 demonstração de correção

Ordena-Por-Inserção

```
ORDENA-POR-INserÇÃO( $A, n$ )
1  para  $j \leftarrow 2$  até  $n$  faça
2      chave  $\leftarrow A[j]$ 
3       $\triangleright$  Insere  $A[j]$  no subvetor ordenado  $A[1..j - 1]$ 
4       $i \leftarrow j - 1$ 
5      enquanto  $i \geq 1$  e  $A[i] >$  chave faça
6           $A[i + 1] \leftarrow A[i]$ 
7           $i \leftarrow i - 1$ 
8       $A[i + 1] \leftarrow$  chave
```

Até agora:

- ▶ vimos que o algoritmo **para**
- ▶ e analisamos sua **complexidade de tempo**

O que falta fazer?

- ▶ Verificar se ele produz uma **resposta correta**.

Invariantes de laço e provas de correção

- ▶ **Definição:** um **invariante de um laço** é uma **propriedade** que é satisfeita pelas variáveis do algoritmo a cada execução completa do laço.
- ▶ Ele deve ser escolhido de modo que, ao término do laço, tenha-se uma propriedade útil para mostrar a correção do algoritmo.
- ▶ A prova de correção de um algoritmo normalmente requer que sejam encontrados e provados invariantes dos vários laços que o compõem.
- ▶ Em geral, é **mais difícil** descobrir um **invariante apropriado** do que mostrar sua validade se ele for dado de bandeja...

Exemplo de invariante

ORDENA-POR-INSERÇÃO(A, n)

```
1  para  $j \leftarrow 2$  até  $n$  faça
2      chave  $\leftarrow A[j]$ 
3       $\triangleright$  Insere  $A[j]$  no subvetor ordenado  $A[1..j - 1]$ 
4       $i \leftarrow j - 1$ 
5      enquanto  $i \geq 1$  e  $A[i] > \textit{chave}$  faça
6           $A[i + 1] \leftarrow A[i]$ 
7           $i \leftarrow i - 1$ 
8       $A[i + 1] \leftarrow \textit{chave}$ 
```

Invariante principal de ORDENA-POR-INSERÇÃO: (i1)

No começo de cada iteração do laço **para** das linha 1–8, o subvetor $A[1 \dots j - 1]$ está ordenado.

Correção de algoritmos por invariantes

A estratégia “típica” para mostrar a correção de um algoritmo iterativo através de invariantes segue os seguintes passos:

1. Mostre que o invariante **vale** no início da **primeira iteração** (trivial, em geral)
2. Suponha que o invariante **vale** no início de uma **iteração qualquer** e prove que ele **vale** no início da **próxima iteração**
3. Conclua que se o algoritmo **para** e o invariante **vale** no início da **última iteração**, então o algoritmo é **correto**.

Note que (1) e (2) implicam que o invariante vale no início de qualquer iteração do algoritmo. Isto é similar ao método de **indução matemática** ou **indução finita**!

Correção da ordenação por inserção

Vamos verificar a **correção do algoritmo de ordenação por inserção** usando a técnica de **prova por invariantes de laços**.

Invariante principal: (i1)

No começo de cada iteração do laço **para** das linhas 1–8, o subvetor $A[1 \dots j - 1]$ está ordenado.

1						j				n
20	25	35	40	44	55	38	99	10	65	50

- ▶ Suponha que o invariante vale.
- ▶ Então a correção do algoritmo é “evidente”. **Por quê?**
- ▶ No início da última iteração temos $j = n + 1$. Assim, do invariante segue que o (sub)vetor $A[1 \dots n]$ está ordenado!

Melhorando a argumentação

ORDENA-POR-INSERÇÃO(A, n)

```
1  para  $j \leftarrow 2$  até  $n$  faça
2      chave  $\leftarrow A[j]$ 
3      ▷ Insere  $A[j]$  no subvetor ordenado  $A[1..j - 1]$ 
4       $i \leftarrow j - 1$ 
5      enquanto  $i \geq 1$  e  $A[i] > \textit{chave}$  faça
6           $A[i + 1] \leftarrow A[i]$ 
7           $i \leftarrow i - 1$ 
8       $A[i + 1] \leftarrow \textit{chave}$ 
```

Um invariante mais preciso: ($i1'$)

No começo de cada iteração do laço **para** das linhas 1–8, o subvetor $A[1 \dots j - 1]$ é uma permutação ordenada do subvetor original $A[1 \dots j - 1]$.

Esboço da demonstração de (i1')

1. Validade na primeira iteração: neste caso, temos $j = 2$ e o invariante simplesmente afirma que $A[1 \dots 1]$ está ordenado, o que é evidente.
2. Validade de uma iteração para a seguinte: segue da discussão anterior. O algoritmo **empurra** os elementos maiores que a **chave** para seus lugares corretos e ela é colocada no **espaço vazio**.

Uma demonstração mais formal deste fato exige invariantes auxiliares para o laço interno **enquanto**.

3. Correção do algoritmo: na última iteração, temos $j = n + 1$ e logo $A[1 \dots n]$ está ordenado com os **elementos originais** do vetor. Portanto, o algoritmo é **correto**.

Invariantes auxiliares

No início da linha 5 valem os seguintes invariantes:

- (i2) $A[1 \dots i]$, *chave* e $A[i + 2 \dots j]$ contém os elementos de $A[1 \dots j]$ antes de entrar no laço que começa na linha 5.
- (i3) $A[1 \dots i]$ e $A[i + 2 \dots j]$ são crescentes.
- (i4) $A[1 \dots i] \leq A[i + 2 \dots j]$
- (i5) $A[i + 2 \dots j] > \textit{chave}$.

Invariantes (i2) a (i5)
+condição de parada na linha 5
+atribuição da linha 7

} \implies invariante (i1')

Demonstração? Mesma que antes.

Correção do Mergesort

```
MERGE-SORT( $A, p, r$ )  
1  se  $p < r$   
2    então  $q \leftarrow \lfloor (p + r)/2 \rfloor$   
3        MERGE-SORT( $A, p, q$ )  
4        MERGE-SORT( $A, q + 1, r$ )  
5        INTERCALA( $A, p, q, r$ )
```

O algoritmo está correto?

A correção do algoritmo **Mergesort** apoia-se na correção do algoritmo **Intercala** e pode ser demonstrada **por indução** em $n := r - p + 1$.

Invariante principal de Intercala:

No começo de cada iteração do laço das linhas 7–12, vale que:

1. $A[p \dots k - 1]$ está ordenado,
2. $A[p \dots k - 1]$ contém todos os elementos de $B[p \dots i - 1]$ e de $B[j + 1 \dots r]$,
3. $B[i] \geq A[k - 1]$ e $B[j] \geq A[k - 1]$.

Exercício. Prove que a afirmação acima é de fato um invariante de INTERCALA.

Exercício. (fácil) Mostre usando o invariante acima que INTERCALA é correto.

Outro exemplo:

Usando *invariante de laços*, provamos a correção de um algoritmo que converte um número inteiro para a sua representação binária.

CONVERTE-BINÁRIO(n)

- 1 \triangleright na saída, b contém a representação binária de n
- 2 $t \leftarrow n$;
- 3 $k \leftarrow -1$;
- 4 enquanto $t > 0$ faça
- 5 $k \leftarrow k + 1$;
- 6 $b[k] \leftarrow t \bmod 2$;
- 7 $t \leftarrow t \operatorname{div} 2$;
- 8 retorne b .

Invariante:

Ao entrar no laço 4–7, o inteiro m representado pelo subvetor $b[0 \dots k]$ é tal que $n = t \cdot 2^{k+1} + m$.

Demonstração: seja $j = k + 1$ ($j = \#$ execuções da linha 4)

Deseja-se provar por indução em j que $n = t \cdot 2^j + m$.

Base da indução: $j = 0$. Trivial, pois antes de fazer o laço, $m = 0$ (subvetor vazio de b) e $n = t$ pela linha 2.

Hipótese de indução: no início da execução da linha 4 na j^{a} iteração, tem-se que $n = t(j) \cdot 2^j + m(j)$, sendo $m(j) = \sum_{i=0}^{j-1} 2^i \cdot b[i]$.

Invariantes de laço e indução matemática

Passo de indução: antes da execução da linha 4 na $(j + 1)^a$ iteração, deve valer que $n = t(j + 1).2^{j+1} + m(j + 1)$, com $m(j) = \sum_{i=0}^j 2^i . b[i]$.

Pelas linhas 6 e 7, respectivamente, tem-se que:

$$t(j + 1) = t(j) \operatorname{div} 2 \quad \text{e} \quad m(j + 1) = [t(j) \operatorname{mod} 2].2^j + m(j).$$

Caso $t(j) = 2p$ (par):

$$\begin{aligned} t(j + 1).2^{j+1} + m(j + 1) &= p.2^{j+1} + m(j) = 2p.2^j + m(j) \\ &= t(j).2^j + m(j) = n \quad (\text{HI}) \end{aligned}$$

Caso $t(j) = 2p + 1$ (ímpar):

$$\begin{aligned} t(j + 1).2^{j+1} + m(j + 1) &= p.2^{j+1} + m(j) + 2^j = (2p + 1).2^j + m(j) \\ &= t(j).2^j + m(j) = n \quad (\text{HI}) \quad \blacksquare \end{aligned}$$

O algoritmo está correto pois, ao término do laço, $t = 0$ e passa-se da linha 4 direto para a linha 8. Pelo invariante, neste momento $n = m$.