Notas de aula: Análise de Algoritmos
Centro de Matemática, Computação e Cognição
Universidade Federal do ABC
Profa. Carla Negri Lintzmayer

Conceitos matemáticos e técnicas de prova
(*Última atualização: 12 de fevereiro de 2019*)

Referências e materiais complementares desse tópico

PDF **O que é uma prova matemática**, do prof. Paulo Feofiloff, da USP.

PDF **Matemática discreta para computação**, dos profs. Anamaria Gomide e Jorge Stolfi, da Unicamp.

Livro Cormen, T. H.; Leiserson, C. E.; Rivest, R. L.; Stein, C.. Introduction to Algorithms. 2nd ed. MIT Press. 2002.
Capítulo 3.2, A, B, C.

Sumário

1 Lógica matemática

- Como ter certeza que nosso raciocínio é correto?
- Como transmitir aos outros essa certeza?
- Começamos por *axiomas*: fatos simples que todos concordam que são verdade.
- Desenvolvemos um raciocínio a partir deles usando regras de inferência.
- Usamos:
  - Proposições: sentenças declarativas que são verdadeiras ou falsas
  - Conectivos: conjunção $\wedge$, disjunção $\vee$, negação $\neg$, implicação $\Rightarrow$, equivalência $\Leftrightarrow$
  - Contrapositiva: $P \Rightarrow Q \rightsquigarrow \neg Q \Rightarrow \neg P$
  - Quantificadores: $\forall$, $\exists$

2 Miscelânea

- Conjuntos:
  - Notações básicas: $\in$, $\notin$, $\subset$, $\subseteq$, $\nsubseteq$
  - Conjuntos especiais: $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{R}$, $\emptyset$
  - Cardinalidade: $|A|$
  - Operações: $\cup$, $\cap$, $\setminus$
- Somatórios:
  - $a_1 + a_2 + \cdots + a_n = \sum_{k=1}^{n} a_k$ onde a_1, a_2, ..., a_n é uma sequência de n números
  - $\sum_{k=1}^{n}(ca_k + b_k) = c\sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$ para qualquer c real e quaisquer duas sequências de números
  - $\sum_{k=1}^{n} k = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$
  - $\sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}$ para $x \neq 1$
- Funções: dados dois conjuntos A e B, uma função f é uma relação binária em $A \times B$ tal que, para $a \in A$, existe exatamente um $b \in B$ tal que $(a, b) \in f$. Também escrevemos $f : A \to B$ e, se $(a, b) \in f$, escrevemos $b = f(a)$.
- Contagem:
  - Número de permutações de n elementos: $n!$
  - Número de permutações de k elementos de um conjunto de n elementos: $\dfrac{n!}{(n-k)!}$
  - Número de combinações de k elementos de um conjunto de n elementos: $\dfrac{n!}{k!(n-k)!}$
- Pisos e tetos:
  - $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
  - $\lceil n/2 \rceil + \lfloor n/2 \rfloor = n$ para qualquer inteiro n
- Exponenciais: para todo $a \geq 0$, m e n reais,
  - $a^0 = 1$, $a^1 = 1$, $a^{-1} = 1/a$
  - $(a^m)^n = (a^n)^m = a^{mn}$
  - $a^n a^m = a^{n+m}$
- Logaritmos: para todo $a > 0$, $b > 0$, $c > 0$ e n real,
  - $\log n = \log_2 n$
  - $\log_a^k n = (\log_a n)^k$
  - $a = b^{\log_b a}$
  - $\log_c(ab) = \log_c a + \log_c b$
  - $\log_b a^n = n \log_b a$
  - $\log_b a = \dfrac{\log_c a}{\log_c b}$
  - $a^{\log_b c} = c^{\log_b a}$

3 Prova ou demonstração

- Uma prova é uma argumentação precisa que procura convencer o leitor de que uma certa proposição, previamente enunciada, está correta.
- É uma história escrita em linguagem humana e feita de sentenças completas.
- É uma sequência de afirmações organizada da seguinte maneira:
  - cada afirmação é consequência simples das afirmações anteriores e das hipóteses da proposição em discussão
  - a última afirmação é a proposição que se deseja provar.
- Exemplo:

  Teorema 1. *Se m e n são números inteiros pares, então $m + n$ é par.*

  Demonstração.
  1. Suponha que m é par (hipótese).
  2. Então existe inteiro r tal que $m = 2r$ (por definição de "par").
  3. Suponha que n é par (hipótese).
  4. Então existe inteiro s tal que $n = 2s$ (por definição de "par").
  5. Podemos escrever, portanto $m + n = 2r + 2s = 2(r + s)$ (usando 2 e 4 acima e álgebra).
  6. Então existe t tal que $m + n = 2t$ (tome, por exemplo, $t = r + s$).
  7. Logo, por definição, $m + n$ é par.

  □

- Terminologias:

  Teorema Uma afirmação devidamente demonstrada.

  Lema Um teorema que é demonstrado apenas para ajudar na prova de outro teorema.

  Corolário Um teorema que é consequência de um outro, cuja demonstração é relativamente simples.

  Conjectura Uma afirmação para a qual ainda não existe prova (mas em geral, há suspeita de que seja verdadeira). Ou provamos uma conjectura e ela se torna um teorema, ou a refutamos. Enquanto isso, ela está *em aberto*.

4 Métodos de prova

Prova direta Supomos que vale a hipótese e usamos uma sequência de deduções até chegar na conclusão.

Prova contrapositiva Para provar resultados do tipo $P \Rightarrow Q$, supomos que Q é falso e provamos que P é falso ($\neg Q \Rightarrow \neg P$).

Prova por contradição Supomos que a hipótese vale e que a conclusão não vale e usamos uma sequência de deduções que termina em uma contradição.

Prova por análise de casos Particionamos o universo de possibilidades em um número finito de casos e provamos a veracidade de cada um deles.

Prova por construção Alguns teoremas afirmam a existência de certos objetos. Um método para prová-lo é exibir um tal objeto.

Prova de afirmações "se e somente se" Para provar $A \Leftrightarrow B$, dividimos a demonstração em duas partes. A primeira prova "a ida" ($A \Rightarrow B$) e a segunda prova "a volta" ($B \Rightarrow A$).

Prova por contra-exemplo minimal Supomos que o resultado é falso e consideramos uma estrutura de "menor tamanho" possível em que o resultado é falso. Mostramos que existe uma estrutura menor em que o resultado é falso, obtendo contradição.

Prova por indução Seja $P(n)$ é uma sentença que depende de uma variável natural n. Provamos que $P(1)$ vale e que se $P(k)$ vale todo $1 \leq k < n$, então $P(n)$ vale.

4.1 Exemplo de prova direta

Teorema 2. *Se m e n são números inteiros pares, então $m + n$ é par.*

Demonstração.

1. Suponha que m é par (hipótese).
2. Então existe inteiro r tal que $m = 2r$ (por definição de "par").
3. Suponha que n é par (hipótese).
4. Então existe inteiro s tal que $n = 2s$ (por definição de "par").
5. Podemos escrever, portanto $m + n = 2r + 2s = 2(r + s)$ (usando 2 e 4 acima e álgebra).
6. Então existe t tal que $m + n = 2t$ (tome, por exemplo, $t = r + s$).
7. Logo, por definição, $m + n$ é par.

□

4.2 Exemplo de prova contrapositiva

Teorema 3. *Se m e n são números inteiros pares, então $m + n$ é par.*

Demonstração.

1. Vamos provar por contrapositiva que se $m + n$ é ímpar, então m é ímpar ou n é ímpar.
2. Suponha que $m + n$ é ímpar.
3. Então existe inteiro k tal que $m + n = 2k + 1$.
4. Se n é ímpar, então o resultado vale.
5. Assuma que n é par.
6. Então existe inteiro r tal que $n = 2r$.
7. Temos que $m = 2k + 1 - n = 2k + 1 - 2r = 2(k - r) + 1$.
8. Como $k - r$ é inteiro, então concluímos que m é ímpar.

□

4.3 Exemplo de prova por contradição

Teorema 4. *Se m e n são números inteiros pares, então $m + n$ é par.*

Demonstração.

1. Para fins de contradição, assuma que m e n são pares e que $m + n$ é ímpar.
2. Por definição, existem inteiros r e s tais que $m = 2r$ e $n = 2s$.
3. Também por definição, existe inteiro k tal que $m + n = 2k + 1$.
4. Logo, $2r + 2s = 2k + 1$, ou seja, $2(r + s - k) = 1$.
5. Mas isso é uma contradição, pois $r + s - k$ é um inteiro e 1 é ímpar.
6. Então $m + n$ deve ser par.

□

4.4 Exemplo de prova por contra-exemplo minimal

Teorema 5. *Se m e n são números inteiros pares, então $m + n$ é par.*

Demonstração.

1. Seja m o menor número par tal que $m + n$ é ímpar ($m \geq 2$).
2. Então existe inteiro k tal que $m + n = 2k + 1$.
3. Se tomarmos o número $m' = m-2$, temos que $m'+n = m-2+n = 2k+1-2 = 2(k-1)+1$
4. Mas então m não era o menor número par que somado com n dava um número ímpar.

□

4.5 Exemplo de prova por indução

Teorema 6. *Se m e n são números inteiros pares, então $m + n$ é par.*

Demonstração.

1. Supondo m e n pares, então existem inteiros r e s tais que $m = 2r$ e $n = 2s$, respectivamente.
2. Vamos provar por indução em r que $m + n$ é par.
3. Base: quando $r = 1$ temos $m = 2$ e $n + 2 = 2s + 2 = 2(s + 1)$ é par.
4. Hipótese: $n + m$ é par, onde $m = 2r'$, para $1 \leq r' < r$.
5. Passo: seja que $m = 2r$, com $r > 1$.
   - Note que $2r = 2r - 2 + 2 = 2(r - 1) + 2$.
   - Por hipótese de indução, $n + 2(r - 1)$ é par.
   - Então $n + 2(r - 1) = 2k$ para algum inteiro k.
   - Como $n + m = n + 2(r - 1) + 2 = 2k + 2 = 2(k + 1)$, temos que $n + m$ é par.

□

4.6 Exemplo de prova por análise de casos

Teorema 7. *Se p é um número primo, então $p^2 - 1$ é divisível por 3.*

Demonstração. Temos três casos a considerar, dependendo do resto da divisão de p por 3:

1. Resto 0. Então $p = 3k$, o que não é possível pois p não seria primo.
2. Resto 1. Então $p = 3k + 1$ e $p^2 - 1 = (3k + 1)^2 - 1 = 9k^2 + 6k = 3(3k^2 + 2k)$ é de fato divisível por 3.
3. Resto 2. Então $p = 3k + 2$ e $p^2 - 1 = 9k^2 + 12k + 3 = 3(3k^2 + 4k + 1)$ é de fato divisível por 3.

□

4.7 Exemplo de prova "se e somente se"

Teorema 8. *Os inteiros m e n são ambos ímpares se, e somente se, mn é ímpar.*

Demonstração. Ida: Se m e n são ímpares, então mn é ímpar.

1. Suponha que m e n são ímpares.
2. Então existem inteiros r e s tais que $m = 2r + 1$ e $n = 2s + 1$.
3. Assim, $mn = (2r + 1)(2s + 1) = 4rs + 2r + 2s + 1 = 2(2rs + r + s) + 1$, que é ímpar.

Volta: Se mn é ímpar, então m e n são ímpares.

1. Provaremos por contrapositiva que se m ou n são pares, então mn é par.
   (a) Se m é par, então existe inteiro r tal que $m = 2r$.
      - Então $mn = (2r)n = 2(rn)$ é par (pois rn é inteiro).
   (b) Se n é par, então existe inteiro s tal que $n = 2s$.
      - Então $mn = m(2s) = 2(ms)$ é par (pois ms é inteiro).

□

4.8 Exemplo de prova por construção

Teorema 9. *Para todo número natural n, se $2^n - 1$ é primo, então n é primo.*

Demonstração. Seja n natural. Vamos provar a contrapositiva: se n não é primo, então $2^n - 1$ não é primo.

Claramente, se $n = 0$ ou $n = 1$, a afirmação vale. Podemos supor então que $n > 1$ e n não é primo, ou seja, existem r e s maiores que 1 e menores que n tais que $n = rs$. Basta mostrar que existe algum inteiro x que divide $2^n - 1$, com $x \neq 1, 2^n - 1$.

Tome $x = 2^s - 1$ e $y = 1 + 2^s + 2^{2s} + \cdots + 2^{(r-1)s}$. Temos

$$\begin{aligned} xy &= (2^s - 1)(1 + 2^s + 2^{2s} + \cdots + 2^{(r-1)s}) \\ &= 2^s(1 + 2^s + 2^{2s} + \cdots + 2^{(r-1)s}) - (1 + 2^s + 2^{2s} + \cdots + 2^{(r-1)s}) \\ &= (2^s + 2^{2s} + \cdots + 2^{rs}) - (1 + 2^s + 2^{2s} + \cdots + 2^{(r-1)s}) \\ &= 2^{rs} - 1 \\ &= 2^n \ . \end{aligned}$$

Como $1 < s < n$ e $x = 2^s - 1$, então $2^1 - 1 < x < 2^n - 1$. Logo, x é divisor de $2^n - 1$ diferente de 1 e de $2^n - 1$ e, portanto, $2^n - 1$ não é primo. □

5 Indução

- Se $n \in \mathbb{N}$, então $n^2 + n + 41$ é primo?
  - Vale para $n = 1, 2, \ldots, 39$ mas $40^2 + 40 + 41 = 41^2$, que não é primo.
- Se n é inteiro positivo, então $991n^2 + 1$ não é quadrado perfeito?
  - Não vale para $x = 12055735790331359447442538767$ mas vale para todos os números $n < x$.
- A soma dos n primeiros números ímpares é n^2?
  - Note que $1 = 1^2$, $1+3 = 2^2$, $1+3+5 = 3^2$, $1+3+5+7 = 4^2$ e $1+3+5+7+9 = 5^2$, mas é possível que seja apenas uma coincidência.

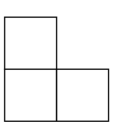
Teorema 10. *A soma dos n primeiros naturais ímpares é n^2.*

Demonstração.
- Vamos provar por indução em n.
- Base: quando $n = 1$, o primeiro natural ímpar é 1, que é igual a 1^2.
- Hipótese: a soma dos k primeiros naturais ímpares é k^2, para qualquer $1 \leq k < n$.
- Passo: vamos verificar se a soma dos n primeiros naturais ímpares $(1+3+5+\ldots+(2n-3)+(2n-1))$ é n^2.
  - Note que $1 + 3 + 5 + \ldots + (2n - 3) = (n - 1)^2$, por hipótese de indução.
  - Então

$$\begin{aligned} 1 + 3 + 5 + \ldots + (2n - 3) + (2n - 1) &= (n - 1)^2 + (2n - 1) \\ &= n^2 - 2n + 1 + 2n - 1 = n^2 \ . \end{aligned}$$

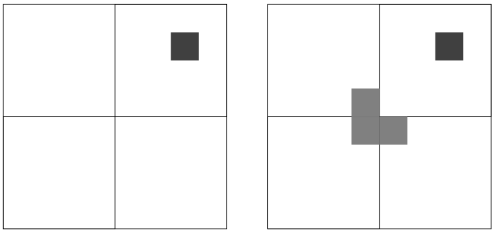
□

Teorema 11. *Seja n um inteiro positivo. Todo tabuleiro de damas de tamanho $2^n \times 2^n$ com um quadrado removido pode ser ladrilhado por triminós em forma de "L".*



Demonstração.
- Vamos provar por indução em n.

- Base: quando $n = 1$, o tabuleiro 2×2 certamente pode ser coberto por um triminó, independente de onde está o quadrado removido.
- Hipótese: todo tabuleiro de tamanho $2^k \times 2^k$ com um quadrado removido pode ser ladrilhado por triminós, para $1 \leq k < n$.
- Passo: suponha que temos um tabuleiro $2^n \times 2^n$ com um quadrado removido.
  - Podemos dividir o tabuleiro em 4 subtabuleiros menores de tamanho $2^{n-1} \times 2^{n-1}$ cada.
  - Suponha, s.p.g., que o quadrado removido do tabuleiro original está no subtabuleiro superior esquerdo.
  - Por hipótese, o subtabuleiro superior esquerdo pode ser ladrilhado.
  - Escolhemos quadrados específicos para remover nos outros três subtabuleiros (as casas centrais)[1].



  - Por hipótese, podemos cobrir os outros três subtabuleiros.
  - Os quadrados removidos podem ser ladrilhados por um triminó extra.
  - Então o tabuleiro original pode ser totalmente ladrilhado.

□

Teorema 12. *Para todo natural $n \geq 1$, vale que $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} < 1$.*

Demonstração.
- Vamos provar por indução em n.
- Base: quando $n = 1$, a soma é $\frac{1}{2}$, que é obviamente menor do que 1.
- Hipótese: $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^k} < 1$ para todo $1 \leq k < n$.
- Passo: vamos verificar se $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n}$ é menor do que 1.
  - Note que
$$\frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{n-1}}\right)$$
  - Por hipótese, $\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{n-1}} < 1$.
  - Então
$$\frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{n-1}}\right) < \frac{1}{2}$$
  - Assim,
$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n} < \frac{1}{2} + \frac{1}{2} = 1 \ .$$

□

[1] Por que fizemos isso? Por que não podemos simplesmente usar a hipótese nos outros três subtabuleiros, que são menores do que o tabuleiro inicial?

6 Exercícios

1. Escreva explicitamente os elementos dos seguintes conjuntos:

   (a) $A = \{x \colon x \in \mathbb{Z} \text{ e } x^2 - 2x + 1 \leq 0\}$

   (b) $B = \{x \colon x \in \mathbb{Z}, 2 \leq x \leq 20 \text{ e } x \text{ é primo}\}$

2. Considere o conjunto $A = \{\emptyset, \{2, 3\}, \{2, 4\}, \{2, 4, 7\}\}$. Escreva quais são os elementos de A e escreva **todos** os subconjuntos de A.

3. Prove que para todos os números reais a e b, se $a < b$ e $b < 0$, então $a^2 > b^2$.

4. Prove que se x, y e z são números reais, então pelo menos um deles é maior ou igual à média aritmética dos três.

5. Prove que para todo n natural, $2^n > n$.

6. Prove que $2^{2n} - 1 = 4^n - 1$ é divisível por 3 para todo $n \geq 1$.

7. Prove que $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$ para todo $n \geq 1$.

8. Seja (a_n) uma sequência de números reais positivos tal que $a_1 = 1$ e $a_1^3 + a_2^3 + \ldots + a_n^3 = (a_1 + a_2 + \ldots + a_n)^2$, para todo $n \geq 1$. Mostre que $a_n = n$ para todo $n \geq 1$.

9. Encontre o erro da prova por indução a seguir:

   Teorema 13. *Em um conjunto de n cavalos, todos têm a mesma cor.*[2]

   Demonstração.
   - Vamos provar por indução em n.
   - Base: para $n = 1$, obviamente o resultado vale.
   - Hipótese de indução: suponha que em todo conjunto com k cavalos, para $1 \leq k < n$, todos têm a mesma cor.
   - Passo: considere um conjunto $C = \{c_1, c_2, \ldots, c_n\}$ com n cavalos.
     - Podemos escrever $C = C' \cup C''$ onde $C' = \{c_1, \ldots, c_{n-1}\}$ e $C'' = \{c_2, \ldots, c_n\}$.
     - Por hipótese de indução, todos os cavalos de C' têm a mesma cor.
     - Da mesma forma, todos os cavalos de C'' têm a mesma cor.
     - Como $c_2 \in C'$ e $c_2 \in C''$, então os cavalos de C' têm a mesma cor dos cavalos de C''.
     - Concluímos que todos os cavalos em C têm a mesma cor.

   □

[2] Falso.