Matemática Discreta

Pedro Hokama

Fontes

- Gomide, Anamaria; Stolfi, Jorge. Elementos de Matematica Discreta para Computação.
- Rosen, Kenneth H. Discrete mathematics and its applications. McGraw-Hill Education, 8th Edition, 2019.

Métodos de Demonstração

Métodos de Demonstração

- **Demonstrações** são instrumentos usados por uma pessoa para convencer outras pessoas (ou a si mesma) de que uma afirmação é verdadeira.
- Toda demonstração precisa partir de
  - definições e afirmações básicas, chamadas **axiomas** ou **postulados** e
  - afirmações que foram previamente demonstradas.

- Para ser convincente, uma demonstração somente pode usar afirmações e regras de raciocínio que as duas partes consideram válidas.
  - equivalências e implicações lógicas.
  - regras de manipulação de fórmulas da álgebra e da teoria de conjuntos.

- Uma afirmação devidamente demonstrada é chamada de **teorema**
  - expressão grega que significa “verdade dos Deuses”.
- Um teorema que é demonstrado apenas para ajudar na prova de um outro teorema é chamado de **lema**.
- Um **corolário** de um teorema é outro teorema que é consequência do primeiro, e cuja demonstração é relativamente simples.

Definições

Uma demonstração também pode usar **definições**.

- Uma definição precisa ser **completa**, isto é, deve especificar todas as propriedades que identificam exatamente o conceito definido.
- Deve ser também **precisa**, de modo que o leitor não tenha dúvidas sobre seu significado.

- Por convenção, o termo definido é enfatizado por ocasião de sua definição. Por exemplo:

Definição 4.1: Um inteiro n é um **múltiplo** de um inteiro p se, e somente se, existe um inteiro q tal que $n = pq$.

Definição 4.1: Um inteiro n é um **múltiplo** de um inteiro p se, e somente se, existe um inteiro q tal que $n = pq$.

- Esta definição não deixa dúvidas: para quaisquer inteiros n e p, ela permite ao leitor decidir se n é ou não múltiplo de p.

- Criamos um novo predicado “é multiplo de”, em notação formal, podemos denotar por M.
- Então $M(n, p)$ é lido “n é multiplo de p”.
- a parte que vem depois do “se, e somente se” seria escrita formalmente “$(\exists q \in \mathbb{Z})\, n = pq$”.
- Depois de enunciarmos essa definição então, podemos tratar a fórmula abaixo como um axioma

$$(\forall n, p \in \mathbb{Z})\, M(n, p) \leftrightarrow (\exists q \in \mathbb{Z})\, n = pq$$

- Ou ainda supor que $M(n, p)$ é logicamente equivalente a $(\exists q \in \mathbb{Z})\, n = pq$

- O número π é um múltiplo de $\sqrt{17}$?
- essa frase não tem sentido: ela não é nem verdadeira nem falsa, e portanto não é uma proposição lógica (enquanto o conceito de “múltiplo” não for definido para números reais)

- Uma vez que um conceito foi definido, ele pode ser usado em outras definições:
  Definição 4.2: Um inteiro p **divide** um inteiro n (é um **divisor** de n) se, e somente se, n é múltiplo de p.
- Esta definição introduz um predicado “é divisor de” em termos do predicado “é multiplo de”. Formalmente podemos denotar esse predicado por D e introduzir o axioma:

$$(\forall n, p \in \mathbb{Z})\, D(p, n) \leftrightarrow M(n, p)$$

$$(\forall n, p \in \mathbb{Z})\ D(p, n) \leftrightarrow M(n, p)$$

Observe o uso do conectivo lógico “se e somente se” ($\leftrightarrow$) nestas definições. Este conectivo permite ao leitor decidir se uma entidade qualquer do domínio se enquadra **ou não** na definição.

- Portanto toda definição é se e somente se.

É comum encontrar definições que usam apenas a palavra “se” quando o autor na verdade quer dizer “se e somente se”. Ou ainda outras que não usam nenhuma delas. Por exemplo:

- **Definição 4.3:** Um inteiro n é **par** se ele é múltiplo de 2.
- **Definição 4.4:** Se um inteiro não é par, dizemos que ele é **ímpar**.
- **Definição 4.5:** Um **número primo** é um número inteiro maior que 1, que não tem nenhum divisor exceto 1 e ele mesmo.

Conjecturas

- Uma **conjectura** (ou **conjetura**) é uma afirmação para a qual ainda não existe prova. Em geral, este termo é usado quando se suspeita que a afirmação seja verdadeira.
- Se uma conjetura é finalmente demonstrada, ela se torna um teorema.

- Por outro lado, se for encontrada uma demonstração da negação da conjetura, dizemos que a mesma foi **refutada**.
- Enquanto nenhuma das duas coisas ocorre, diz-se que a conjetura continua **aberta**.

Conjectura de Fermat

Um exemplo famoso é a **conjectura de Fermat**:

- "se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas."
- Foi encontrada em um livro que pertenceu ao matemático Pierre de Fermat (1601–1665).

"se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas."

- Escreveu na margem "tenho uma linda demonstração, mas ela não cabe nesta margem."
- Apesar de inúmeros esforços por matemáticos de todo o mundo, a afirmação permaneceu como conjetura por mais de 300 anos.

- Em 1995, finalmente, o matemático inglês Andrew Wiles publicou uma demonstração com mais de 200 páginas.
- Hoje a conjetura é conhecida como **o último teorema de Fermat**.

Conjetura das quatro cores

Outro exemplo famoso é a **conjetura das quatro cores**:

- "todo mapa pode ser pintado com no máximo quatro cores, de modo que regiões vizinhas tenham cores diferentes."
- Enunciada em 1852 por Francis Guthrie (1831–1899).

- Foi provada em 1976 por Kenneth Appel e Wolfgang Haken, utilizando um computador.
- Em 1994 foi produzida uma prova simplificada por Paul Seymour, Neil Robertson, Daniel Sanders e Robin Thomas, mas ainda utilizando um computador.

- Há várias conjeturas famosas que ainda estão abertas. A **conjetura de Goldbach**, formulada pelo matemático alemão Christian Goldbach em 1742.
- **todo número inteiro par maior que 2 é a soma de dois números primos.**
- Testes com computadores mostram que esta afirmação é verdadeira para todos os inteiros pares entre 4 e 4×10^{18};
- mas obviamente estes testes não constituem uma prova.

- O monge e matemático francês Marin Mersenne (1585–1648) investigou os números $M_n = 2^n - 1$, onde n é um número primo.
- Ele observou que os números $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, e $M_7 = 127$ são primos; mas o número seguinte, $M_{11} = 2047$, não é primo ($2047 = 23 \times 89$).
- Ele conjecturou que M_n é primo para todo n em $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$

M_n é primo para todo n em $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$

- Em 1876 Edouard Lucas (1842–1891) provou que $M_{67} = 2^{67} - 1$ não era primo, e portanto a conjetura de Mersenne era falsa.
- Entretanto, sua prova não exibia os fatores de M_{67}, apenas provava que eles existiam.
- Em 1903, Frank Nelson Cole (1861–1926) apresentou uma palesta em uma conferência de matemática, com o título vago **On the Factorisation of Large Numbers**.

- Sem dizer nada, Cole primeiro escreveu $2^{67} - 1$ no quadro negro, e fez os cálculos à mão, obtendo o valor 147573952589676412927.
- Na outra metade do quadro, ele escreveu o produto $193707721 \times 761838257287$, e fez a multiplicação à mão, obtendo o mesmo resultado, e a plateia aplaudiu de pé.
- Depois ele contou que tinha levado três anos, trabalhando todos os domingos, para encontrar essa fatoração.

Métodos de demonstração

- Existem teoremas que tem muitas demonstrações diferentes.
- Qual é a melhor é, até certo ponto, uma questão de gosto, e depende para quem a demonstração é dirigida.

- Em geral, quanto mais curta a prova, melhor;
- mas há outros critérios, como a facilidade de compreensão, a simplicidade dos passos, etc..
- Para convencer outras pessoas, devemos cuidar para que a demonstração seja, além de correta, também simples, clara e objetiva, tanto quanto possível.

Demonstração de implicações

- Muitas vezes temos que provar implicações da forma $p \to q$,
- **se** p é verdadeira, **então** q também é.
- A afirmação p é chamada de **hipótese**, **premissa** ou **condição**.
- A afirmação q é chamada de **tese** ou **conclusão**.

Método direto

Demonstração de implicações

- Supomos que a hipótese p é verdadeira.
- Usamos uma sequência de proposições que são consequências lógicas das anteriores,
- até obter a tese q.
- Esta sequência de passos prova a implicação $p \rightarrow q$.

Teorema 4.1: Se m e n são inteiros pares, então $m + n$ é par.

Prova:

1. Suponha que m é par. (Hipótese.)
2. Suponha que n é par. (Hipótese.)
3. Existe um inteiro r tal que $m = 2r$. (Definição de "par").
4. Existe um inteiro s tal que $n = 2s$. (Definição de "par").
5. $m + n = 2r + 2s = 2(r + s)$. (De 3 e 4, por álgebra.)
6. Seja $t = r + s$. (Introdução de variável.)
7. Existe um inteiro t tal que $m + n = 2t$. (De 6.)
8. $m + n$ é par. (Definição de "par", dada 6. Tese.)

Fim.

- Cada um dos passos da prova é um raciocínio simples o bastante para ser aceito como válido pelo leitor.
- Cada passo deveria ser uma aplicação de uma **regra de inferência**, tirada de uma lista fixa de regras que todos aceitam como válidas e fundamentais.
- Uma das regras comumente aceitas, por exemplo, é a regra de **modus ponens**
  - se já demonstramos que uma proposição p é verdade,
  - e que $p \rightarrow q$,
  - então podemos considerar a proposição q demonstrada

Na prática, os passos são escritos mais abreviados:

Teorema 4.1: Se m e n são inteiros pares, então $m + n$ é par.

Prova:

Suponha que m e n são inteiros pares. Por definição de número "par", existem inteiros r e s tais que $m = 2r$ e $n = 2s$. Logo $m + n = 2r + 2s = 2(r + s)$. Como $r + s$ é inteiro, concluímos que o inteiro $m + n$ é par, pela definição. Isto prova que, se m e n são pares, $m + n$ é par.

Fim

Exercícios

- Demonstre que o produto de um inteiro par por um inteiro ímpar é par.
- Demonstre que se r é um número racional diferente de zero, então $\frac{1}{r}$ é racional.
- Demonstre que, para quaisquer conjuntos A, B, C e D, as seguintes afirmações são sempre verdadeiras
  - Se $x \in A$, $(A \setminus B) \subseteq (C \cap D)$ e $x \notin D$, então $x \in B$.
  - Se B e C são disjuntos, $A \subseteq C$ e $x \in A$, então $x \notin B$.
  - Se $x \in C$ e $(A \cap C) \subseteq B$, então $x \notin (A \setminus B)$.

Método da contrapositiva

Demonstração de implicações

- Queremos provar que $p \rightarrow q$.
- Supomos que a negação da tese $\neg q$ é verdadeira.
- Procuramos uma sequência de deduções lógicas que termina com a negação da hipótese $\neg p$.
- Ou seja, provamos que $(\neg q) \rightarrow (\neg p)$.
- esta afirmação é logicamente equivalente a $p \rightarrow q$, que portanto também está provada.

Teorema 4.2: Se n^2 é um inteiro par, então n é par.
Prova:
Suponha que n é ímpar. Pela definição de "ímpar", existe um inteiro k tal que $n = 2k + 1$. Portanto $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
Como $2k^2 + 2k$ é um inteiro, pela definição de "ímpar" concluímos que n^2 é impar.
Pela regra da contrapositiva, isto prova que, se n^2 é um inteiro par, então n é um inteiro par.
Fim.

- Demonstre que, para todo inteiro n, se $n^3 + 5$ é impar, então n é par.

Dica: $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Método de redução ao absurdo

- Também chamado de **prova indireta** ou **por contradição**
- Baseia-se na equivalência lógica entre a fórmula $(p \rightarrow q)$ e a fórmula $(p \wedge \neg q) \rightarrow \mathbf{F}$

- Queremos mostrar que $p \rightarrow q$
- Supomos que tanto a hipótese p quanto a **negação** da tese $\neg q$ são verdadeiras
- Procuramos uma sequência de deduções lógicas que termina com uma contradição (uma afirmação com valor lógico **F**).
- Isto prova a afirmação $(p \wedge \neg q) \rightarrow \mathbf{F}$, e portanto também a afirmação equivalente a $p \rightarrow q$.

Teorema 4.3: Se m e n são inteiros pares, então $m + n$ é um inteiro par.
Prova:
Suponhamos que m e n são inteiros pares e $m + n$ é um inteiro ímpar; e isso leva a uma contradição.
Por definição existem r e s inteiros tais que $m = 2r$ e $n = 2s$. Pela definição de "ímpar", existe um inteiro j tal que $m + n = 2j + 1$. Logo $2r + 2s = 2j + 1$, ou seja, $r + s - j = 1/2$. Isto é falso pois $r + s - j$ é um inteiro.
Esta contradição prova que, se m e n são inteiros pares, $m + n$ é um inteiro par. **Fim.**

Exercícios

1. Demonstre que a soma de um número racional com um número irracional é um número irracional.
2. Demonstre que o número $\sqrt{2}$ é irracional.
3. Sejam x, y, z números reais. Demonstre que pelo menos um deles é maior ou igual à média aritmética dos três.

Implicação com tese conjuntiva

- Queremos provar que $p \to (q \wedge r)$
- Que é logicamente equivalente à $(p \to q) \wedge (p \to r)$
- Basta provar cada uma separadamente.

Teorema 4.4: Se 6 divide um inteiro n, então 2 divide n e 3 divide n.

Prova:

Se 6 divide n então existe um inteiro k tal que $n = 6k$. Então, $n = 2(3k)$, logo 2 divide n. Temos também que $n = 3(2k)$, logo 3 divide n. Portanto 2 divide n e 3 divide n.

Fim.

Implicação com hipótese disjuntiva

- Queremos provar $(p \vee q) \to r$
- Equivale à $(p \to r) \wedge (q \to r)$
- Basta provar cada uma dessas partes.

Teorema 4.5: Para quaisquer inteiros m e n, se m for par ou n for par, então mn é par.

Prova:

Sejam m e n inteiros quaisquer. Temos dois casos:

- Caso 1: m é par. Pela definição, existe um inteiro q tal que $m = 2q$. Nesse caso, $mn = (2q)n = 2(nq)$, e portanto mn é par.
- Caso 2: n é par. Pela definição, existe um inteiro r tal que $n = 2r$. Nesse caso $mn = m(2r) = 2(mr)$, e portanto mn é par.

Portanto, se m é par ou n é par, mn é par. **Fim.**

Demonstrações de afirmações “se e somente se”

Outro tipo comum de teorema tem a forma $p \leftrightarrow q$, ou seja, “p vale se e somente se q vale.”

- Equivalente à $(p \rightarrow q) \wedge (q \rightarrow p)$
- Dividimos a demostração em duas partes.
  - (1) prova que $p \rightarrow q$ (ida);
  - (2) prova que $q \rightarrow p$ (volta);

Teorema 4.7: Os inteiros x e y são ambos ímpares se, e somente se, o produto xy é ímpar.

Prova:

Sejam x e y inteiros quaisquer.

- Parte (1) ($\rightarrow$): provaremos que, se x e y são ímpares, então xy é ímpar.Se x e y são ímpares, por definição existem inteiros r e s tais que $x = 2r + 1$ e $y = 2s + 1$. Portanto $xy = (2r + 1)(2s + 1) = 2(rs + r + s) + 1$. Como $rs + r + s$ é um inteiro, concluímos que xy é ímpar.

- Parte (2) ($\leftarrow$): provaremos que, se xy é ímpar, então x e y são ambos ímpares. Ou seja (pela contrapositiva), que se x é par ou y é par, então xy é par. Temos dois casos (não exclusivos):
  - Caso (a): x é par. Neste caso existe um inteiro r tal que $x = 2r$. Portanto $xy = (2r)y = 2(ry)$. Como ry é inteiro, concluímos que xy é par.
  - Caso (b): y é par. Então existe um inteiro s tal que $y = 2s$. Portanto $xy = x(2s) = 2(xs)$. Como xs é inteiro, concluímos que xy é par.

Fim.

Regras para quantificadores universais

Instanciação universal

- Se provarmos que $(\forall x \in D)\, P(x)$,
- podemos afirmar $P(c)$ para qualquer elemento c do domínio D.
- “para todo inteiro x maior que 5, $2^x > x^2$”, podemos imediatamente concluir que $2^{418} > 418^2$.
- Esta regra é chamada de **instanciação universal**.

Generalização universal

- Agora suponha que desejamos provar $(\forall x \in D)\, P(x)$
- começar supondo que x é um elemento de D escolhido arbitrariamente
- Se, com essa suposição, conseguirmos provar a afirmação $P(x)$, provamos que o teorema original é verdadeiro.
- Este último passo é chamado de **generalização universal** ou **suspensão do quantificador universal**.

Teorema 4.10: Para quaisquer números reais x e y, $(x+y)^2 - (x-y)^2 = 4xy$.

Prova:

Sejam x e y dois números reais quaisquer.

Pelo teorema do binômio, temos

$(x+y)^2 = x^2 + 2xy + y^2$, e $(x-y)^2 = x^2 - 2xy + y^2$.

Portanto,

$(x+y)^2-(x-y)^2 = (x^2+2xy+y^2)-(x^2-2xy+y^2) = 4xy$.

Fim.

Demonstração por vacuidade

Lembre-se que se E é o conjunto vazio, a afirmação $(\forall x \in E)\, Q(x)$ é verdadeira, qualquer que seja o predicado Q. Esta afirmação é verdadeira **por vacuidade**.

- Queremos demostrar $(\forall x \in D)\, P(x)$ para um domínio arbitrário D.
- Mostrar que ela é equivalente a outra afirmação $(\forall x \in E)\, Q(x)$
- Então mostrar que E é vazio.

Teorema: Para todo número inteiro x, se $x^2 = 5$ então x é par.

- $(\forall x \in \mathbb{Z})\, Q(x) \rightarrow P(x)$
- $Q(x)$ significa "$x^2 = 5$", e $P(x)$ é "x é par".
- $E = \{\forall x \in \mathbb{Z} : Q(x)\}$
- equivale à $(\forall x \in E)\, P(x)$.
- ou seja, E é o conjunto dos inteiros cujo quadrado é 5.
- Como E é vazio, a afirmação é verdadeira por vacuidade.

Regras para quantificadores existenciais

- Se provamos que $(\exists x \in D)\, P(x)$,
- podemos supor, dali em diante, que a variável x é um dos elementos cuja existência é afirmada.
- Esta regra é chamada de **instanciação existencial**.
- Exemplo: Considere as seguintes premissas: “Um aluno desse curso não estudou” e “Todos os alunos desse curso foram aprovados” podemos concluir que "Algum aluno não estudou e foi aprovado".

Demonstrações construtivas

- Agora suponha que queremos provar que $(\exists x \in D)\, P(x)$.
- Exibimos um elemento específico a do domínio D (explicitamente, ou através de uma construção algorítmica)
- $P(a)$ é verdadeira, para esse elemento.
- **Demonstração construtiva**

Demonstrações construtivas

Teorema 4.11: Existem três números inteiros positivos tais que $x^2 + y^2 = z^2$.
Prova:
Sejam $x = 3$, $y = 4$, e $z = 5$. Como
$x^2 + y^2 = 3^2 + 4^2 = 25 = 5^2 = z^2$, a afirmação é verdadeira.
Fim.

Teorema do deserto de primos: Para todo número inteiro positivo n, existe uma sequência de n números inteiros consecutivos que não são primos.

Prova: Seja n um inteiro positivo, e seja $x = (n+1)! + 2$. Observe que

$$\begin{aligned} 2 \text{ divide } x &= (n+1)! + 2, && (1)\\ 3 \text{ divide } x+1 &= (n+1)! + 3, && (2)\\ &\ldots && (3)\\ n+1 \text{ divide } x+(n-1) &= (n+1)! + n + 1. && (4) \end{aligned}$$

Logo todos os inteiros $x + i$ com $0 \leq i < n$ são não primos; e eles formam uma sequência de n inteiros consecutivos.

Fim.

Exercício:

- Existem 100 inteiros consecutivos que não são quadrados perfeitos.

Demonstrações não construtivas

- Em alguns casos, é possível demonstrar a existência de um elemento que satisfaz uma dada condição mesmo sem exibir explicitamente tal elemento.
- Uma demonstração deste tipo é chamada de **demonstração não construtiva**

Teorema 4.14: Existem dois números reais irracionais x e y tais que x^y é racional.

Prova:

Sabemos que número $\sqrt{2}$ é irracional. Se $(\sqrt{2})^{\sqrt{2}}$ for racional, a afirmação está satisfeita tomando-se $x = \sqrt{2}$ e $y = \sqrt{2}$. Por outro lado, se $(\sqrt{2})^{\sqrt{2}}$ for irracional, podemos tomar $x = (\sqrt{2})^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$ que é racional.

Fim.

Demonstração de existência e unicidade

- Queremos provar $(\exists! x \in D)\, P(x)$
- Logicamente equivalente à
  $((\exists x \in D)\, P(x)) \wedge ((\forall x \in D)(\forall y \in D)\, ((P(x) \wedge P(y)) \rightarrow x = y))$

Portanto, uma demonstração de existência e unicidade pode ser dividida em duas partes:

- **Existência:** prova-se-se que existe pelo menos um x em D que satisfaz $P(x)$.
- **Unicidade:** supõe-se que y também é um elemento de D que satisfaz $P(y)$, e prova-se que ele é igual ao x.

Teorema: Mostre que se a e b são números reais e $a \neq 0$, então existe um único número real r tal que $ar + b = 0$

Prova: Note que o número real $r = -b/a$ é uma solução para $ar + b = 0$. Suponha então que s é um número real, tal que $as + b = 0$. Então $ar + b = as + b$. Subtraindo b dos dois lados e dividindo por a (que é diferente de 0), encontramos que $r = s$.

Demonstração de falsidade por contra-exemplo

- Demonstrações de existência são usadas, em particular, para refutar conjeturas da forma $(\forall x \in D)\, P(x)$; pois a negação desta afirmação é $(\exists x \in D)\, \neg P(x)$.
- Neste caso dizemos que o elemento x de D que comprovadamente não satisfaz $P(x)$.
- Portanto mostra a falsidade da conjetura

Considere a seguinte afirmação: “Para todo primo n, o inteiro $2^n - 1$ é primo.” Esta afirmação não é verdadeira, basta ver que o número $n = 11$ é um contra-exemplo, pois
$P(11) = 2^{11} - 1 = 2047 = 23 \times 89$.

Exercícios:
Demonstre (por meio de contra-exemplos) que as seguintes conjeturas são falsas:

- Todo inteiro positivo é soma dos quadrados de três inteiros.
- Se n é um número inteiro e $4n$ é par, então n é par.
- O produto de dois números irracionais é um número irracional.

Prove (ou mostre contra exemplos) de que as seguintes proposições são equivalentes

a) $(\forall x \in D)\, P(x) \vee Q(x)$ e
$((\forall x \in D)\, P(x)) \vee ((\forall x \in D)\, Q(x))$.

b) $(\exists x \in D)\, P(x) \wedge Q(x)$ e
$((\exists x \in D)\, P(x)) \wedge ((\exists x \in D)\, Q(x))$.