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.

Métodos de Demonstração

- 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.

Definições

- Esta definição introduz um novo predicado “é multiplo de”, que, na notação formal, podemos denotar (por exemplo) 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)

Definições

- 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:

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

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).
- 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.

Conjectura de Fermat

- 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.

Conjecturas

- 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.

Conjecturas

- 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 $p \to q$.

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.

Método direto
Demonstração de implicações

- 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 $p \to q$,
  - então podemos considerar a proposição q demonstrada

Na prática, os passos são escritos de maneira mais abreviada:
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 $p \to q$.
- 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 $(\neg q) \to (\neg p)$.
- esta afirmação é logicamente equivalente a $p \to q$, que portanto também está provada.

Método da contrapositiva
Demonstração de implicações

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
Demonstração de implicações

- Também chamado de **prova indireta** ou **por contradição**
- Baseia-se na equivalência lógica entre a fórmula $(p \to q)$ e a fórmula $(p \wedge \neg q) \to \mathbf{F}$
- Queremos mostrar que $p \to q$
- 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 $(p \wedge \neg q) \to \mathbf{F}$, e portanto também a afirmação equivalente a $p \to q$.

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; vamos mostrar que estas suposições levam a uma contradição.
Pela definição de "par", 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.