BACHARELADO EM SISTEMAS DE INFORMAÇÃO

MATEMÁTICA DISCRETA

Aula 4 - Demonstrações matemáticas

Prof. Marcelo Gama

Universidade Federal Rural de Pernambuco - DM

25 de Agosto de 2011

Sumário

Objetos matemáticos

Em Matemática, os objetos podem ser de dois tipos: **primitivos** ou **definidos**.

Objetos (ou entes) primitivos

São aqueles que são aceitos pela experiência ou observação. Não são definidos!

Exemplos

- Ponto
- Reta
- Plano
- Conjunto

Objetos matemáticos

Em Matemática, os objetos podem ser de dois tipos: **primitivos** ou **definidos**.

Objetos (ou entes) definidos

São aqueles construidos a partir de outros objetos, sejam eles primitivos ou nao.

Exemplos

- Pontos colineares: Pontos que pertencem a uma mesma reta.
- Retas concorrentes: Duas retas que têm um único ponto em comum.
- Planos paralelos: Planos que não têm ponto em comum.
- Conjunto unitário: Tem apenas um elemento.
- Número primo: É aquele que têm apenas dois divisores positivos distintos.

Sumário

Sentenças matemáticas

São de três tipos: **demonstráveis**, **não demonstráveis** e **conjecturas**.

Sentenças não demonstráveis

São conhecidas por **axiomas** ou **postulados**. Estas são as afirmações mais básicas da matemática. A validade é aceita com base na observação. Não podem ser provadas!

Exemplos:

- **(Geometria)** Por dois pontos distintos passa uma única reta.
- **(Conjuntos)** Axioma da extensão: $(\forall x)(\forall A)(\forall B)((x \in A \leftrightarrow x \in B) \to A = B)$
- **(Aritmética)** Um elemento $\alpha \in \mathbb{N}$ é neutro para a adição quando $(\forall n \in \mathbb{N})(\alpha + n = n + \alpha = n)$.
- **(Combinatória)** $0! = 1$

Sumário

Sentenças matemáticas

São de três tipos: **demonstráveis**, **não demonstráveis** e **conjecturas**.

Sentenças demonstráveis

São aquelas cuja validade só é aceita por meio de uma justificativa, demonstração ou prova. São classificadas em

- Proposição
- Teorema
- Lema
- Corolário

Proposição

(Wikipedia) É uma sentença que não está associada a nenhuma outra sentença demonstrável, de simples prova e de importância matemática menor. (Subjetivo!)

Exemplos:

- A soma de dois inteiros ímpares é um inteiro par.
- A soma dos ângulos internos de um triângulo mede 180°.
- $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$
- $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

Sentenças matemáticas

Teorema

(Wikipedia) É uma sentença que não está associada a nenhuma outra sentença demonstrável, porém de grande importância matemática. (Subjetivo!)

Exemplos:

- **(Teorema de Pitágoras)** Em todo triângulo retângulo, o quadrado da medida da hipotenusa é igual à soma dos quadrados das medidas dos catetos.
- **(Teorema fundamental da aritmética)** Todo inteiro maior que 1 pode ser decomposto, de modo único, como produto de potências de números primos.
- **(Último teorema de Fermat)** Não existem inteiros positivos a, b, c tais que $a^n = b^n + c^n$ quando n é um inteiro maior que 2.

Lema

É uma proposição ou teorema, de menor importância, que serve para auxiliar na prova de outro teorema ou proposição.

Exemplo:

- **(Lema 1)** O quadrado de um inteiro positivo é um inteiro positivo.
- **(Lema 2)** O quadrado de um inteiro negativo é um inteiro positivo.
- **(Teorema)** O quadrado de todo inteiro não nulo é um inteiro positivo.

Corolário

(Wikipedia) É uma sentença que é **consequência imediata** de outra proposição ou teorema. Muitas vezes, tem suas provas omitidas por serem bastante simples.

Exemplo:

- **(Teorema)** Todo inteiro par é soma de dois inteiros ímpares.

$$par = mpar_1 + mpar_2$$

- **(Corolário)** Todo inteiro ímpar é soma de três inteiros ímpares.

$$mpar = par + 1 = \underbrace{mpar_1 + mpar_2}_{par} + \underbrace{mpar_3}_{1}$$

Sumário

Conjectura

(Wikipedia) Uma conjectura é uma idéia, fórmula ou frase, a qual não foi provada ser verdadeira (nem falsa).

Normalmente são formuladas com base em observações que indicam (mas não provam) sua veracidade.

Conjecturas mais conhecidas

- Hipótese de Riemann
- Hipótese do continuum
- Conjectura de Goldbach
- Conjectura dos primos gêmeos
- Problema P versus NP

Conjecturas: Hipótese de Riemann

Hipótese de Riemann (Georg F. Bernhard Riemann 1826-1866)

Trata-se da afirmação que as soluções complexas não triviais de uma certa equação (dada pela função zeta de Riemann) estão sobre a reta $x = 1/2$.

Comentários (Wikipedia):

- Tem intrigado os matemáticos há mais de 150 anos.
- É um dos poucos problemas não resolvidos daqueles chamados de problemas do milênio, propostos por Hilbert em 1900.
- É tão difícil que em 2000 o "Clay Mathematics Institute" ofereceu um prêmio de 1 milhão de dólares a quem prová-lo.

Conjecturas: Hipótese do continuum

Hipótese do continuum (George Cantor 1845-1918)

Não existe nenhum conjunto com mais elementos do que o conjunto dos números inteiros e menos elementos do que o conjunto dos números reais.

Conjecturas: Conjectura de Goldbach

Conjectura de Goldbach (Christian Goldbach 1690-1764)

Todo número par maior ou igual a 4 é a soma de dois primos.

Exemplos:

- $4 = 2 + 2$
- $8 = 5 + 3$
- $20 = 13 + 3$
- $100 = 21 + 79$
- $10000 = 59 + 9941$

Conjecturas: Primos gêmeos

Primos gêmeos

São dois números ímpares consecutivos onde ambos são números primos.

- **Exemplos:** 3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31, 71 e 73, $156733989 \cdot 2^{100007} - 1$ e $156733989 \cdot 2^{100007} + 1$, etc.

Conjectura dos primos gêmeos

Existem infinitos pares de primos gêmeos.

Algoritmos de tempo polinomial

Um algoritmo para resolver um certo problema é de tempo polinomial se o seu consumo de tempo, no pior caso, é limitado por uma função polinomial dos tamanhos das instâncias do problema.

Exemplo:

- Algoritmo bubblesort para ordenação: Tempo da ordem de n^2

Classe P

Chamamos de P a classe de problemas para os quais existe um algoritmo de tempo polinomial que o resolva.

Conjecturas: P versus NP

Problemas razoáveis

Um problema é razoável é possível verificar, em tempo polinomial, se uma suposta solução da instância é, de fato, uma solução.

Exemplo:

- Verificar se um dado x é solução da equação $ax^2 + bx + c = 0$

Classe NP

Chamamos de NP a classe dos problemas razoáveis.

$P \stackrel{?}{=} NP$

Todo problema cujas soluções podem ser verificadas por um algoritmo polinomial pode também ser resolvido por um algoritmo polinomial?

Fatos importantes

- O bom senso sugere que P é apenas uma pequena parte de NP.
- Ninguém conseguiu ainda encontrar um problema de NP que não esteja em P.
  (ou seja, um problema razoável para o qual não existe um algoritmo polinomial)
- O fato anterior sugere que $P = NP$.
- A maioria da comunidade científica acredita que $P \neq NP$.

Demonstração (ou prova)

É uma sucessão finita de argumentos, restritos às regras da lógica, mostrando que determinada afirmação é necessáriamente verdadeira quando se assumem certos axiomas.

Estrutura de uma demonstração

- **Hipóteses:** Conjunto de axiomas $H = \{H_1, H_2, \ldots, H_n\}$
- **Tese (T):** Conclusão à qual se deseja chegar
- **Prova:** Mostrar que vale a implicação lógica

$$H_1 \wedge H_2 \wedge \ldots \wedge H_n \Rightarrow T$$

Provas matemáticas

Métodos de prova matemática

Os métodos de provas matemáticas podem ser classificados em

- Prova direta
- Prova por contra-exemplo
- Prova pela contra-positiva
- Prova por redução ao absurdo (ou contradição)
- Prova por casos (ou por exaustão)
- Prova por indução

Sumário

Método direto

Partindo da hipótese H, usamos uma sequência de implicações lógicas até obter a tese T.

Exemplo: Se m e n são inteiros pares, então $m+n$ é um inteiro par.

- H: m e n são inteiros pares
- T: $m+n$ é um inteiro par

Prova.

$$\begin{aligned}
\overbrace{m \text{ e } n \text{ são inteiros pares}}^{H} &\Rightarrow (\exists a \in \mathbb{Z})(\exists b \in \mathbb{Z})(m = 2a \wedge n = 2b) \\
&\Rightarrow (\exists a \in \mathbb{Z})(\exists b \in \mathbb{Z})(m + n = 2a + 2b) \\
&\Rightarrow (\exists a \in \mathbb{Z})(\exists b \in \mathbb{Z})(m + n = 2(a + b)) \\
&\Rightarrow \underbrace{m + n \text{ é par}}_{T}
\end{aligned}$$

Sumário

Método do contra-exemplo

Mostramos com um exemplo (contra-exemplo), um caso em que a afirmação é falsa.

Exemplo: Para todo primo n, o inteiro $2^n - 1$ é um número primo.

- H: n é primo
- T: $2^n - 1$ é primo

Prova (da falsidade). Tomando $n = 11$, temos

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

Portanto, a afirmação é falsa para $n = 11$.

Sumário

Provas matemáticas

Método da contra-positiva

A contra-positiva de uma condicional $P \rightarrow Q$ é dada por $\neg Q \rightarrow \neg P$.

- Uma condicional e sua contra-positiva são equivalentes.
  (Prove isto usando tabela-verdade.)

Exemplo: Se $15x^3 - 9x^2 + 27x - 5 \geq 0$, então $x \geq 0$.

- H: $5x^3 - 9x^2 + 2x - 5 \geq 0$ T: $x \geq 0$

Contra-positiva: Se $x < 0$, então $5x^3 - 9x^2 + 2x - 5 < 0$.

- H: $x < 0$ T: $15x^3 - 9x^2 + 27x - 5 < 0$

Prova

$$x < 0 \Rightarrow 15x^3 < 0, -9x^2 < 0, 27x < 0, -5 < 0 \Rightarrow 5x^3 - 9x^2 + 2x - 5 < 0$$

Método da contra-positiva

A contra-positiva de uma condicional $P \to Q$ é dada por $\neg Q \to \neg P$.

- Uma condicional e sua contra-positiva são equivalentes. (Prove isto usando tabela-verdade.)

Exemplo: Se $15x^3 - 9x^2 + 27x - 5 \geq 0$, então $x \geq 0$.

- H: $5x^3 - 9x^2 + 2x - 5 \geq 0$ T: $x \geq 0$

Contra-positiva: Se $x < 0$, então $5x^3 - 9x^2 + 2x - 5 < 0$.

- H: $x < 0$ T: $15x^3 - 9x^2 + 27x - 5 < 0$

Prova

$x < 0 \Rightarrow 15x^3 < 0, -9x^2 < 0, 27x < 0, -5 < 0 \Rightarrow 5x^3 - 9x^2 + 2x - 5 < 0$

Método da contra-positiva

A contra-positiva de uma condicional $P \to Q$ é dada por $\neg Q \to \neg P$.

- Uma condicional e sua contra-positiva são equivalentes.
  (Prove isto usando tabela-verdade.)

Exemplo: Se $15x^3 - 9x^2 + 27x - 5 \geq 0$, então $x \geq 0$.

- H: $5x^3 - 9x^2 + 2x - 5 \geq 0$ $\quad$ T: $x \geq 0$

Contra-positiva: Se $x < 0$, então $5x^3 - 9x^2 + 2x - 5 < 0$.

- H: $x < 0$ $\quad$ T: $15x^3 - 9x^2 + 27x - 5 < 0$

Prova

$$x < 0 \Rightarrow 15x^3 < 0, -9x^2 < 0, 27x < 0, -5 < 0 \Rightarrow 5x^3 - 9x^2 + 2x - 5 < 0$$

Sumário

Método da contradição

Este método baseia-se no seguinte fato:

- $((P \wedge \neg Q) \to F) \to (P \to Q)$ (Prove isto usando tabela-verdade.)
- Interpretando: Se $P \wedge \neg Q$ leva a uma contradição, então $P \to Q$.

Exemplo: Se m e n são pares, então $m + n$ é par.

- H: m e n são pares $\qquad T$: $m + n$ é par.

Assumimos H e $\neg T$, ou seja, m e n são pares, mas $m + n$ é ímpar.
Existem inteiros a, b, c tais que $m = 2a$, $n = 2b$, $m + n = 2c + 1$. Então

$$\begin{aligned} m + n = 2c + 1 \quad &\Rightarrow \quad 2a + 2b = 2c + 1 \\ &\Rightarrow \quad 2a + 2b - 2c = 1 \\ &\Rightarrow \quad 2(a + b - c) = 1 \\ &\Rightarrow \quad a + b - c = 1/2 \end{aligned}$$

Temos uma contradição:

$a + b - c = 1/2$ nunca irá ocorrer, pois $a + b - c$ é um número inteiro!

Conclusão: $H \rightarrow T$, ou seja,

Se m e n são pares, então $m + n$ é par.

Sumário

Prova por casos

Dividimos a prova em um número finito de casos que cobrem todas as possibilidades.

Exemplo: O quadrado de qualquer inteiro é maior ou igual a zero.

Prova. Temos três casos a considerar sobre um dado inteiro n:

1. $n > 0$: Nesse caso, $n^2 = n \cdot n = (+n) \cdot (+n) > 0$
2. $n < 0$: Nesse caso, $n^2 = n \cdot n = (-n) \cdot (-n) > 0$
3. $n = 0$: Nesse caso, $n^2 = 0^2 = 0 \cdot 0 = 0$

Em qualquer caso, $n^2 \geq 0$.

Sumário

Provas matemáticas

Prova por indução

Teremos um tópico específico apenas sobre esse método!