DCC638 - Introdução à Lógica Computacional
2023.1

Introdução ao Curso

Área de Teoria DCC/UFMG

Introdução - O que é “lógica”?

- Vamos abrir o curso de Introdução à Lógica Computacional com uma pergunta:

O que é “lógica”*?*

Introdução - O que é "lógica"?

- Vamos abrir o curso de Introdução à Lógica Computacional com uma pergunta:

  O que é "lógica"*?*

  Algumas definições (mais ou menos) formais incluem:

  - *"A lógica (do grego antigo $\lambda o \gamma \iota \kappa \eta$) é o método de raciocínio conduzido ou avaliado de acordo com princípios estritos de validade."*
  - *"A lógica é o estudo sistemático das formas de inferência válidas, e das leis gerais da verdade."*
  - *"A lógica é o uso sistemático de técnicas matemáticas e simbólicas para determinar as formas de argumento dedutivo válido."*
  - ...

Introdução - O que é “lógica”?

- Nas definições acima, alguns termos merecem destaque:

  - **“raciocínio”**,
  - **“verdade”** e **“validade”**,
  - **“formas de inferência”** e **“argumento dedutivo”**,
  - **“técnicas matemáticas e simbólicas”**, e
  - **“princípios estritos”**, **“estudo sistemático”** e **“leis gerais”**.

- Neste curso vamos estudar estes termos com o devido cuidado.
- Mas podemos dizer que a intuição de “lógica” pode ser capturada informalmente como:

  “A lógica é o método de raciocinar de maneira estruturalmente válida.”

  É isso que vamos fazer neste curso: aprender a estruturar raciocínio de maneira válida, principalmente voltado para computação!

Objetivos e Programa da Disciplina

ILC: Objetivos

- Ao final deste curso, espera-se que o(a) estudante seja capaz de responder com propriedade as seguintes perguntas:

1. O que é a **lógica proposicional**, e como aplicá-la a problemas reais?
2. O que é a **lógica de predicados**, e como aplicá-la a problemas reais?
3. A partir de um conjunto de hipóteses, como realizar apenas **deduções válidas**?
4. Como **demonstrar formalmente a veracidade** de uma proposição matemática?
5. O que é o **conceito de recursão**, e como aplicá-lo a problemas reais?
6. Como a **lógica Booleana** é aplicada à base dos **circuitos digitais** que compõem os **computadores modernos**?

ILC: Programa

1. **Fundamentos das lógicas proposicional e de predicados.**
   - a) Conectivos lógicos (conjunção, disjunções inclusiva e exclusiva, negação, implicação, implicação dupla).
   - b) Tabelas da verdade.
   - c) Satisfatibilidade, tautologias, contradições.
   - d) Consequência lógica, equivalência lógica.
   - e) Predicados, quantificadores, e proposições quantificadas.
   - f) Regras de inferência.
   - g) Expressividade das lógicas proposicional e de predicados.

ILC: Programa

2. **Métodos de demonstração.**

    a) Demonstração direta, por contra-exemplo e por divisão em casos.
    b) Demonstração por contradição e por implicação contra-positiva.
    c) Demonstrações construtivas e não-construtivas.
    d) Automatização de demonstrações

ILC: Programa

2. **Métodos de demonstração.**
   a) Demonstração direta, por contra-exemplo e por divisão em casos.
   b) Demonstração por contradição e por implicação contra-positiva.
   c) Demonstrações construtivas e não-construtivas.
   d) Automatização de demonstrações

3. **Teoria de conjuntos e funções.**
   a) Conjuntos dos números naturais, inteiros, racionais e reais.
   b) Teoria de conjuntos elementar.
   c) Funções injetivas, sobrejetivas e bijetivas.
   d) Conjuntos enumeráveis e não-enumeráveis.
   e) Somatórios e produtórios.

ILC: Programma

4. **Indução e recursão.**

   a) Indução matemática fraca e forte.
   b) Princípio da boa ordenação.
   c) Relações de recorrência e recursão.
   d) Indução estrutural.

4. **Indução e recursão.**

   a) Indução matemática fraca e forte.
   b) Princípio da boa ordenação.
   c) Relações de recorrência e recursão.
   d) Indução estrutural.

5. **Fundamentos de álgebra Booleana e circuitos digitais combinatórios.**

   a) Conversão entre bases numéricas.
   b) Álgebra Booleana e aritmética binária (incluindo leis de De Morgan e representação em complemento de dois).
   c) Portas lógicas.
   d) Formas normais conjuntiva e disjuntiva.
   e) Minimização de circuitos e mapas de Karnaugh.
   f) Completude de operadores.

Um exemplo de uso de lógica: Definindo números

O papel da lógica na definição de números

- Começamos com uma motivação natural para a lógica: definir os números.
- Definir números rigorosamente é essencial.

  Computadores, por exemplo, manipulam números o tempo todo, seguindo instruções.

  Tudo precisa ser rigorosamente definido para computadores funcionarem bem.
- Porém, quando os matemáticos tentaram definir rigorosamente o conceito de "número", muitas dificuldades surgiram.
  1. Como conseguir uma definição finita para um conjunto infinito (como o conjunto dos números naturais, ou o dos números reais)?
  2. Como demonstrar que sua definição está correta: que nenhum número "errado" está incluído nela, e que nenhum número "certo" está excluído?
- Para resolver estas dificuldades, muitas técnicas lógicas foram aprimoradas.

O papel da lógica na definição de números

- Aqui definiremos conjuntos de números importantes:
  - os números naturais $\mathbb{N}$,
  - os números inteiros $\mathbb{Z}$,
  - os números racionais $\mathbb{Q}$,
  - os números irracionais $\mathbb{I}$, e
  - os números reais $\mathbb{R}$.
- Para isto, vamos usar vários conceitos que veremos com cuidado neste curso:
  - conectivos lógicos para definir conjuntos,
  - definições recursivas,
  - uso de bases diferentes (decimal, binária) para representar números,
  - como representar somas com infinitos termos (somatórios), e
  - como demonstrar a veracidade de uma afirmação matemática.

Os números naturais

- O conjunto dos **números naturais** é o conjunto

$$\mathbb{N} = \{0, 1, 2, 3 \ldots\}.$$

Os números naturais

- O conjunto dos **números naturais** é o conjunto

$$\mathbb{N} = \{0, 1, 2, 3 \ldots\}.$$

  Alguns autores não consideram o número 0 (zero) como um número natural, definindo $\mathbb{N} = \{1, 2, 3, \ldots\}$.

- O conjunto dos números naturais $\mathbb{N}$ pode ser definido através de duas "observações auto-evidentes":

  N_1: 0 (zero) é um número natural, e

  N_2: cada número natural tem um sucessor.

Os números naturais

- Reescrevendo estas "observações auto-evidentes" de maneira mais formal, obtemos os seguintes **axiomas** para os naturais:

  N_1': $0 \in \mathbb{N}$, e

  N_2': se $k \in \mathbb{N}$, então $s(k) \in \mathbb{N}$,

  onde $s(\cdot)$ é a **função sucessor**: $s(k) = k + 1$.

- Exemplos:

  1. $0 \in \mathbb{N}$, por causa de (N_1').
  2. $s(0) \in \mathbb{N}$, por causa de (N_2'). Notação: $s(0) = 1$.
  3. $s(s(s(s(s(0))))) = 5 \in \mathbb{N}$.

- Para obter-se o número natural n, aplica-se (N_1') uma vez, e depois aplica-se (N_2') n vezes.

Números naturais na representação decimal e binária

- Números naturais podem ser escritos em função de potências de 10.

Números naturais na representação decimal e binária

- Números naturais podem ser escritos em função de potências de 10.
- $\boxed{\text{Exemplo 1}}$

$$237 \quad = \quad 2 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$$

Números naturais na representação decimal e binária

- Números naturais podem ser escritos em função de potências de 10.
- $\boxed{\text{Exemplo 1}}$

$$237 \quad = \quad 2 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$$

- Entretanto, não há nada de especial na escolha de potências de 10 para decompor os números naturais.

  Podemos representar os números naturais em potências de 2, por exemplo.
- $\boxed{\text{Exemplo 2}}$

$$\begin{aligned} 11101101_2 &= 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 128 + 1 \cdot 64 + 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 \\ &= 237 \end{aligned}$$

Os números inteiros

- O conjunto dos **números inteiros** é o conjunto

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

  O conjunto

$$\mathbb{Z}^+ = \{1, 2, 3, 4, 5, \ldots\}$$

  é o conjunto dos **números inteiros positivos**.

- O conjunto dos números inteiros $\mathbb{Z}$ pode ser definido como sendo o conjunto de todos os números naturais e seus negativos:

$$\mathbb{Z} = \{x \mid x \in \mathbb{N} \quad \text{ou} \quad -x \in \mathbb{N}\}.$$

Os números reais

- Outro conjunto importante é o conjunto dos **números reais** $\mathbb{R}$.
- Exemplos:
  1. $\pi = 3.14159265359\ldots$
  2. $\sqrt{2} = 1.41421356237\ldots$
  3. 2
  4. -4.5
- Um **número real** pode ser definido como uma soma ponderada infinita de potências de 10:

$$d_k \quad d_{k-1} \quad \cdots \quad d_1 \quad d_0 \quad . \quad d_{-1} \quad d_{-2} \quad d_{-3} \quad \cdots \quad = \quad \sum_{i=-\infty}^{\infty} d_i \cdot 10^i$$

Os números reais

- Outro conjunto importante é o conjunto dos **números reais** $\mathbb{R}$.
- Exemplos:
  1. $\pi = 3.14159265359\ldots$
  2. $\sqrt{2} = 1.41421356237\ldots$
  3. 2
  4. -4.5
- Um **número real** pode ser definido como uma soma ponderada infinita de potências de 10:

$$d_k \quad d_{k-1} \quad \cdots \quad d_1 \quad d_0 \quad . \quad d_{-1} \quad d_{-2} \quad d_{-3} \quad \cdots \quad = \quad \sum_{i=-\infty}^{\infty} d_i \cdot 10^i$$

$\boxed{\text{Exemplo 3}}$

$$\begin{aligned} \pi &= 3 \cdot 10^0 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 1 \cdot 10^{-3} + 5 \cdot 10^{-4} + \ldots \\ &= 3 + 0.1 + 0.04 + 0.001 + 0.0005 + \ldots \end{aligned}$$

Os números racionais

- O próximo conjunto de interesse é o dos **números racionais** $\mathbb{Q}$.
- Um número **racional** é um numero real x tal que existam $p, q \in \mathbb{Z}$, com $q \neq 0$, tais que

$$x = \frac{p}{q}.$$

Note sempre podemos usar a **representação simplificada** de racional, em que $\text{mdc}(p, q) = 1$.

- Exemplos:

1. $\frac{17}{34} = \frac{-9}{-18} = \frac{1}{2} = 0.5$
2. $\frac{-1}{3} = \frac{1}{-3} = -\frac{1}{3} = -0.333333\ldots$

- **Teorema.** Um número real é racional se, e somente se, há periodicidade na sua representação decimal.

Exemplos:

1. $1/5 = 0.2\,000\,000\,000\ldots$
2. $1/7 = 0.\,142857\,142857\ldots$

Os números irracionais

- O conjunto dos **números irracionais** são os números reais não-racionais:

$$\mathbb{I} \quad = \quad \mathbb{R} - \mathbb{Q} \quad = \quad \{x \mid x \in \mathbb{R} \quad \text{e} \quad x \notin \mathbb{Q}\}$$

- O seguinte resultado mostra que existe pelo menos um número irracional.

- **Teorema.** $\sqrt{2}$ não é racional.

Os números irracionais

- O conjunto dos **números irracionais** são os números reais não-racionais:

$$\mathbb{I} \quad = \quad \mathbb{R} - \mathbb{Q} \quad = \quad \{x \mid x \in \mathbb{R} \quad \text{e} \quad x \notin \mathbb{Q}\}$$

- O seguinte resultado mostra que existe pelo menos um número irracional.

- **Teorema.** $\sqrt{2}$ não é racional.

  Demonstração.

  Por contradição: Suponha que $\sqrt{2}$ é racional.

Os números irracionais

- O conjunto dos **números irracionais** são os números reais não-racionais:

$$\mathbb{I} \quad = \quad \mathbb{R} - \mathbb{Q} \quad = \quad \{x \mid x \in \mathbb{R} \quad \text{e} \quad x \notin \mathbb{Q}\}$$

- O seguinte resultado mostra que existe pelo menos um número irracional.

- **Teorema.** $\sqrt{2}$ não é racional.

  Demonstração.

  Por contradição: Suponha que $\sqrt{2}$ é racional.

  Neste caso, sabemos que existem números $p, q \in \mathbb{Z}$, com $\text{mdc}(p, q) = 1$, tais que $\sqrt{2} = p/q$.

Os números irracionais

- O conjunto dos **números irracionais** são os números reais não-racionais:

$$\mathbb{I} \quad = \quad \mathbb{R} - \mathbb{Q} \quad = \quad \{x \mid x \in \mathbb{R} \quad \text{e} \quad x \notin \mathbb{Q}\}$$

- O seguinte resultado mostra que existe pelo menos um número irracional.

- **Teorema.** $\sqrt{2}$ não é racional.

  Demonstração.

  Por contradição: Suponha que $\sqrt{2}$ é racional.

  Neste caso, sabemos que existem números $p, q \in \mathbb{Z}$, com $\mathrm{mdc}(p, q) = 1$, tais que $\sqrt{2} = p/q$.

  Elevando os dois lados da equação acima ao quadrado, obtemos $2 = p^2/q^2$, ou seja, $p^2 = 2q^2$.

Os números irracionais

- **Demonstração (Continuação).**

  Note que $2q^2$ é par, portanto pela igualdade acima p^2 também tem que ser par. Isto implica que p deve ser par.

- **Demonstração (Continuação).**

  Note que $2q^2$ é par, portanto pela igualdade acima p^2 também tem que ser par. Isto implica que p deve ser par.

  Agora, já que p é par, existe algum $r \in \mathbb{Z}$ tal que $p = 2r$. Isso implica que $2q^2 = p^2 = (2r)^2 = 4r^2$, o que resulta em $q^2 = 2r^2$. Note que então q^2 é par, portanto q deve ser par.

- **Demonstração (Continuação).**

  Note que $2q^2$ é par, portanto pela igualdade acima p^2 também tem que ser par. Isto implica que p deve ser par.

  Agora, já que p é par, existe algum $r \in \mathbb{Z}$ tal que $p = 2r$. Isso implica que $2q^2 = p^2 = (2r)^2 = 4r^2$, o que resulta em $q^2 = 2r^2$. Note que então q^2 é par, portanto q deve ser par.

  Mas se ambos p e q são pares, isto contradiz a suposição de que o $mdc(p, q) = 1$: <u>encontramos uma contradição.</u>

  <u>Conclusão:</u> não existem $p, q \in \mathbb{Z}$, com $q \neq 0$ e $\mathrm{mdc}(p, q) = 1$, tais que $\sqrt{2} = p/q$, portanto <u>$\sqrt{2}$ não é racional</u>.

  $\square$

Observações sobre os números racionais e irracionais

- Alguns fatos interessantes sobre racionais e irracionais:
    a) O conjunto dos números reais é a união dos racionais e irracionais: $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$.
    b) Entre dois números racionais quaisquer sempre existe um número irracional.
    c) Entre dois números irracionais quaisquer sempre existe um número racional.
    d) A soma de dois números racionais é sempre um número racional.
    e) A soma de um racional e um irracional é sempre um número irracional.
    f) A soma de dois números irracionais é mais complicada: não se sabe se o número $\pi + e$, onde e é a constante de Euler, é racional ou irracional!

Uma última questão “complicada”

- Vamos fechar com uma questão mais “complicada” sobre os números.

  A seguinte afirmação é verdadeira ou é falsa?

  > *“O conjunto $\mathbb{Z}$ dos inteiros é “maior” que o conjunto $\mathbb{N}$ dos naturais.”*

Uma última questão "complicada"

- Vamos fechar com uma questão mais "complicada" sobre os números.

  A seguinte afirmação é verdadeira ou é falsa?

  "O conjunto $\mathbb{Z}$ dos inteiros é "maior" que o conjunto $\mathbb{N}$ dos naturais."

  Há duas possibilidades:

  - Se a afirmação for <u>verdadeira</u>, então existe um infinito "maior" que o outro!
  - Mas se ela for <u>falsa</u>, então é possível um conjunto ter o mesmo "tamanho" que de um de seus subconjuntos próprios (ou seja, $\mathbb{Z}$ ter o mesmo "tamanho" que seu subconjunto próprio $\mathbb{N}$)!

  Dilemas como este, em que nossa intuição não é de muita ajuda, dependem de métodos lógicos cuidadosos para serem resolvidos.