MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira

Instituto de computação

UNICAMP

31 de julho de 2023

Informações preliminares

Apresentação do professor

- USP, Unicamp, Luxembourg, KU Leuven
- Professor do Instituto de Computação
- Departamento (área de concentração): Teoria da Computação
- Especialidade: Criptografia

Objetivos do curso

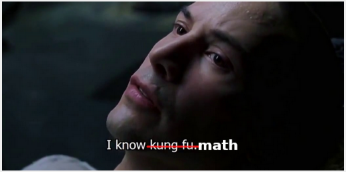
- Se familiarizar com provas matemáticas
- Aprender a provar formalmente
- Aprender técnicas de prova
- Aprender alguns tópicos comuns em ciência da computação

Página do curso

https://hilder-vitor.github.io/teaching/mc358.html

Aprendizado é uma tarefa ativa!

Não estamos na Matrix! O professor não vai inserir o conhecimento na sua cabeça.



Faça exercícios, revise as aulas, leia a bibliografia recomendada...

O que são provas matemáticas?

Muitas discussões têm o intuito de mostrar que algo está certo (ou errado).

Neste sentido, discussões são como provas matemáticas.

Mas por que algumas discussões são inconclusivas?

Axiomas

Discussões partem de pressupostos e, a partir deles, tentam chegar em uma conclusão.

Se não houver acordo sobre essa "base comum", fica difícil haver acordo sobre as conclusões.

Axiomas

Discussões partem de pressupostos e, a partir deles, tentam chegar em uma conclusão.

Se não houver acordo sobre essa "base comum", fica difícil haver acordo sobre as conclusões.

- Um cristão toma uma interpretação literal da bíblia e constrói um argumento.
- Quem não acredita na bíblia não vai ser convencido.

Axiomas

Discussões partem de pressupostos e, a partir deles, tentam chegar em uma conclusão.

Se não houver acordo sobre essa "base comum", fica difícil haver acordo sobre as conclusões.

- Um cristão toma uma interpretação literal da bíblia e constrói um argumento.
- Quem não acredita na bíblia não vai ser convencido.

Essas proposições que tomamos como verdade e que embasam os argumentos é o que chamamos de axiomas.

Definições

Por vezes, as discussões não chegam em lugar algum por falta de definições claras...

Por exemplo: Qual o *melhor* atacante brasileiro da história?

Sem a definir "melhor", não se pode chegar em nenhuma conclusão.

Definições

Por vezes, as discussões não chegam em lugar algum por falta de definições claras...

Por exemplo: Qual o *melhor* atacante brasileiro da história?

Sem a definir "melhor", não se pode chegar em nenhuma conclusão.

Provas matemáticas usam definições precisas das propriedades que queremos provar.

Dedução lógica

Além dos axiomas, é preciso também fixar as regras de inferência lógica.

Geralmente, esta parte é menos problemática...

As pessoas sabem as regras de dedução, mesmo que não se deem conta...

Além dos axiomas, é preciso também fixar as regras de inferência lógica.

Geralmente, esta parte é menos problemática...

As pessoas sabem as regras de dedução, mesmo que não se deem conta...

- *Modus ponens*: Se $((P \to Q)$ e $P)$, então Q.

Dedução lógica

Além dos axiomas, é preciso também fixar as regras de inferência lógica.

Geralmente, esta parte é menos problemática...

As pessoas sabem as regras de dedução, mesmo que não se deem conta...

- *Modus ponens*: Se $((P \to Q)$ e $P)$, então Q.
- *Modus tollens*: Se $((P \to Q)$ e $\bar{Q}$), então $\bar{P}$.

Dedução lógica

Além dos axiomas, é preciso também fixar as regras de inferência lógica.

Geralmente, esta parte é menos problemática...

As pessoas sabem as regras de dedução, mesmo que não se deem conta...

- *Modus ponens*: Se $((P \to Q)$ e $P)$, então Q.
- *Modus tollens*: Se $((P \to Q)$ e $\bar{Q}$ $)$, então $\bar{P}$.
- Lei do silogismo: Se $((P \to Q)$ e $(Q \to R))$, então $P \to R$.

Resultados conhecidos

Proposições que já foram demonstradas podem ser usadas para derivar novos resultados.

Esses são chamados de lemas, teoremas e corolários.

Preparando uma demonstração

Ingredientes

- Axiomas
- Definições
- Teoremas, lemas, corolários
- Regras de inferência lógica

Preparando uma demonstração

Ingredientes

- Axiomas
- Definições
- Teoremas, lemas, corolários
- Regras de inferência lógica

Modo de preparo

Veremos técnicas de prova nas próximas aulas...

Conjuntos

Assumir proposições como verdadeiras (axiomas) é um risco.
Quanto mais complexa for a proposição, maior o risco.

Assumir proposições como verdadeiras (axiomas) é um risco.
Quanto mais complexa for a proposição, maior o risco.

- Prova que $\frac{de^x}{dx} = e^x$ assume existência de $\mathbb{R}$.

Assumir proposições como verdadeiras (axiomas) é um risco.
Quanto mais complexa for a proposição, maior o risco.

- Prova que $\frac{de^x}{dx} = e^x$ assume existência de $\mathbb{R}$.
- É possível construir $\mathbb{R}$ a partir de $\mathbb{Q}$.

Uma formalização para toda a matemática

Assumir proposições como verdadeiras (axiomas) é um risco.
Quanto mais complexa for a proposição, maior o risco.

- Prova que $\frac{de^x}{dx} = e^x$ assume existência de $\mathbb{R}$.
- É possível construir $\mathbb{R}$ a partir de $\mathbb{Q}$.
- $\mathbb{Q}$ a partir de $\mathbb{Z}$...

Uma formalização para toda a matemática

A teoria dos conjuntos nos dá um conjunto mínimo de axiomas simples, dos quais podemos deduzir todos os resultados da matemática.

Uma formalização para toda a matemática

A teoria dos conjuntos nos dá um conjunto mínimo de axiomas simples, dos quais podemos deduzir todos os resultados da matemática.

ZFC: Zermelo–Fraenkel and Choice:

- Nove axiomas propostos por Zermelo e Fraenkel.
- Mais o axioma da escolha (axiom of choice).
- Axiomas simples como
  - O conjunto vazio, $\emptyset$, existe.
  - Dois conjuntos são iguais se têm os mesmos elementos.
  - A união de conjuntos, $A \cup B$, existe.
  - Dados conjuntos A e B, existe um conjunto $C = \{A, B\}$.
  - ...

Números naturais: construção de von Neumann

$$
\begin{aligned}
0 &= \{\} &&= \varnothing \\
1 &= \{0\} &&= \{\varnothing\} \\
2 &= \{0, 1\} &&= \{\varnothing, \{\varnothing\}\} \\
3 &= \{0, 1, 2\} &&= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\
&\vdots
\end{aligned}
$$

Números naturais: construção de von Neumann

$$
\begin{aligned}
0 &= \{\} &&= \varnothing \\
1 &= \{0\} &&= \{\varnothing\} \\
2 &= \{0,1\} &&= \{\varnothing,\{\varnothing\}\} \\
3 &= \{0,1,2\} &&= \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\} \\
& \vdots
\end{aligned}
$$

Note que $a \leq b$ no sentido usual significa agora $a \subseteq b$.

Conjuntos: resumo das propriedades e notações básicas

- $A \subseteq B$: subconjunto (A pode ser igual a B)
- $A \subset B$: subconjunto estrito (A contido em B, mas $A \neq B$)
- $A \cup B$: união
- $A \cap B$: intersecção
- $|A|$: cardinalidade do conjunto A ($\#$ elmts se A é finito)
- $A - B$ ou $A \setminus B$: diferença de conjuntos
  - conjunto dos elementos de A que não estão em B
  - $A - B = \{x : x \in A \text{ e } x \notin B\}$
- $A \Delta B$: diferença simétrica
  - conjunto dos elementos que estão em A ou em B, mas não em ambos
  - $A \Delta B = (A \cup B) - (A \cap B)$
- $A \times B$: produto cartesiano (pares (a, b) com $a \in A$ e $b \in B$)

Perguntas, observações, comentários?