

# Apresentação

Aula para disciplina de Métodos Formais

Gabriela Moreira

Departamento de Ciência da Computação - DCC  
Universidade do Estado de Santa Catarina - UDESC

26 de fevereiro de 2024



# Conteúdo

## Contexto

Sobre Métodos Formais  
Sobre Mim

## Plano de Ensino

Conteúdo  
Sistema de avaliação  
Bibliografia

## Recursos



# Outline

Contexto

Sobre Métodos Formais

Sobre Mim

Plano de Ensino

Conteúdo

Sistema de avaliação

Bibliografia

Recursos



# Essência

Métodos formais são técnicas, embasadas na matemática, que visam verificar que algum hardware/software faz o que se propõe.

As técnicas incluem dois componentes:

- Uma linguagem de especificação
- Um sistema de verificação



# Histórico da disciplina

- Lá por 2015~2017, ensinava-se uma linguagem chamada Z
- Em ~2018, ensinava-se Redes de Petri
- Desde 2019, o prof Cristiano assumiu a disciplina ensinando Coq
- Esse semestre, vou ensinar TLA+ (Temporal Logic of Actions+) e Quint



# Sobre Mim

## Academia:

- Ciência da Computação - UDESC - 2015-2019
  - **TCC:** Tradução automática de especificação formal modelada em TLA+ para linguagem de programação
- Computação Aplicada - UDESC - 2020-2022
  - **Dissertação:** Test Generation From TLA+ Specifications

## Indústria:

- Magrathea Labs (agora Trusted Health) - 2018-2021
  - Estágio (5 meses) + Engenheira de Software
- Informal Systems - 2021-presente
  - Engenheira de Pesquisa



# Meu envolvimento com Métodos Formais

- Aprendi TLA+ na graduação para fazer meu TCC, e continuei estudando TLA+ no mestrado
- Entrei na Informal Systems devido a pesquisa ativa (minha e deles) em TLA+
  - Muitos engenheiros com dificuldade em aprender e usar TLA+
  - Tinham a proposta de uma nova sintaxe para TLA+, que chamamos hoje de **Quint**
    - Sou a principal desenvolvedora dessa linguagem desde o início de 2022



# Outline

Contexto

Sobre Métodos Formais

Sobre Mim

Plano de Ensino

Conteúdo

Sistema de avaliação

Bibliografia

Recursos



# Vamos aprender TLA+ e Quint?

- TLA+ é uma linguagem de especificação bem estabelecida, e será nossa principal fundamentação teórica da disciplina
  - Alguns assuntos mais avançados vamos abordar somente em TLA+
- Quint é completamente opcional, vocês podem escolher fazer tudo em TLA+ se quiserem.
  - A linguagem e o ferramental de Quint pode facilitar bastante a vida de vocês.
  - Vamos conversar mais sobre isso no decorrer das aulas.

Os exemplos em aula poderão ser em qualquer uma das linguagens.

Minha expectativa é que vocês consigam entender especificações em ambas as linguagens, já que toda a base lógica para elas é a mesma - e a base lógica é a parte mais importante da disciplina.



# Plano de ensino

Disponível no SIGA (assim que for aprovado). Vamos ver juntos agora.





# Plano de ensino

Disponível no SIGA (assim que for aprovado). Vamos ver juntos agora.

## Objetivo Geral

Desenvolver habilidades para reconhecimento de cenários, em sistemas computacionais, onde o uso de métodos formais é apropriado; e para aplicação de métodos formais.

# Plano de ensino

Disponível no SIGA (assim que for aprovado). Vamos ver juntos agora.

## Objetivo Geral

Desenvolver habilidades para reconhecimento de cenários, em sistemas computacionais, onde o uso de métodos formais é apropriado; e para aplicação de métodos formais.

## Objetivo Específico

- Estimular o **senso de necessidade** de técnicas que auxiliem a garantir comportamentos em sistemas computacionais.
- Desenvolver a **capacidade de abstração** ao descrever comportamentos de sistemas em linguagens de especificação formal.
- Trabalhar técnicas de testes baseados em modelos para **conectar especificações com implementações**.

# Conteúdo programático I

- Introdução: Programação e matemática não são a mesma coisa
- Estruturas de Kripke
- Linguagens de especificação formal
- Lógica Temporal
- Exemplo com semáforos
- Motivação para o uso de métodos formais
- Lógica Temporal de Ações: TLA+ e Quint
- Formulas temporais em TLA+ e Quint
- Métodos formais no design de protocolos
- Especificações para sistemas distribuídos
- Exemplo sobre a efetivação em duas fases (two phase commit)



# Conteúdo programático II

- Verificação vs testes
- Testes baseados em modelos
- Outros métodos formais
- Métodos formais no ciclo de desenvolvimento de software
- Model checking
- Refinamento
- Model values e conjuntos de simetria



# Metodologia

A disciplina será desenvolvida através de aulas expositivo-dialogadas, com exercícios e trabalhos práticos, e seminários. O conteúdo da disciplina poderá ser ministrado na modalidade de ensino a distância em até 20% do total de sua Carga Horária (MEC PORTARIA No 4.059, DE 10 DE DEZEMBRO DE 2004 publicado no DOU de 13/12/2004, Seção 1, p. 34).

# Do desempenho do aluno

A qualidade do desempenho do aluno será avaliada com base em:

- 1 Uma prova individual (P) - 30%
- 2 Dois trabalhos práticos (T1 e T2) - 25% cada
- 3 Um seminário (S) - 20%

Assim, a Média Semestral (MS) será calculada pela fórmula

$$MS = (30 * P + 25 * T1 + 25 * T2 + 20 * S)/100$$



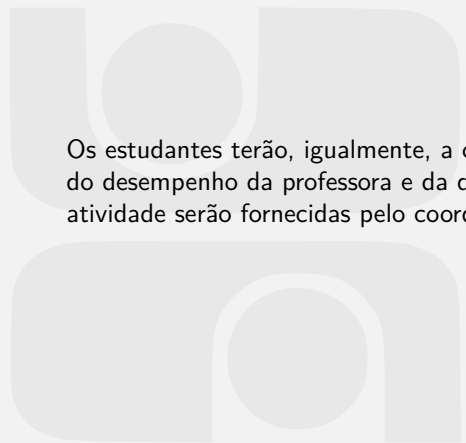


# Exame

Caso o discente não obtenha média MS igual ou superior a 7,0, um exame escrito será aplicado objetivando aferir o conhecimento teórico do estudante. Não há recuperação das provas por não comparecimento, exceto nos casos previstos no regulamento da UDESC na resolução 0392015 - CONSEPE.



# Do desempenho da disciplina e da professora



Os estudantes terão, igualmente, a oportunidade de fazer uma avaliação do desempenho da professora e da disciplina. As informações sobre esta atividade serão fornecidas pelo coordenador do curso.



# Bibliografia básica

BAIER, C.; KATOEN, J.-P. **Principles of model checking**. Cambridge, MA: The MIT Press, 2008.

LAMPORT, L. **Specifying systems: The tla+ language and tools for hardware and software engineers**. Boston: Addison-Wesley, 2002.

MONIN, J. F.; HINCHEY, M. G. **Understanding formal methods**. Berlin, Heidelberg: Springer-Verlag, 2001.



## Bibliografia complementar

KONNOV, I.; KUKOVEC, J. **Tla+ language reference manual**.

Disponível em: <<https://apalache.informal.systems/docs/lang/index.html#tla-language-reference-manual->>.

LAMPORT, L. **A science of concurrent programs**. 2024. Disponível em: <<https://lamport.azurewebsites.net/tla/science.pdf>>.



# Outline

Contexto

Sobre Métodos Formais

Sobre Mim

Plano de Ensino

Conteúdo

Sistema de avaliação

Bibliografia

Recursos



# Recursos

- ① Aulas em HTML no meu site: [bugarela.com/mfo](http://bugarela.com/mfo)
  - Todo o conteúdo dos slides
- ② Toda a bibliografia tem disponível online gratuitamente
- ③ Páginas web relevantes
  - TLA+: <https://lamport.azurewebsites.net/tla/tla.html>
  - Quint: <https://github.com/informalsystems/quint>
- ④ Pesquisa de opinião: querem usar o moodle?

# Apresentação

Aula para disciplina de Métodos Formais

Gabriela Moreira

Departamento de Ciência da Computação - DCC  
Universidade do Estado de Santa Catarina - UDESC

26 de fevereiro de 2024