

# Checando propriedades com Lógica Temporal II

Aula para disciplina de Métodos Formais

Gabriela Moreira

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

11 de março de 2024



# Conteúdo

Revisão & Cheatsheet

Exemplos

Exercício prático

Tipos de propriedades



# Outline

Revisão & Cheatsheet

Exemplos

Exercício prático

Tipos de propriedades

□ ou **G**: *Globally*, sempre

**G**  $\phi$ :  $\phi$  deve ser verdadeiro por toda a execução a partir de agora.

**G**  $\phi$  é verdadeiro num momento  $t$  se...

...  $\phi$  é verdadeiro em **todos** os momentos  $t' \geq t$ .

Exemplo: Comida sacia a fome.



## ◇ ou **F**: Finally, eventualmente, no Futuro

**F**  $\phi$ : eventualmente (na execução a partir de agora),  $\phi$  deve ser verdadeiro.

**F**  $\phi$  é verdadeiro num momento  $t$  se...

...  $\phi$  é verdadeiro em **algum** o momento  $t' \geq t$ .

Exemplo: Eventualmente, terei fome.



○ ou **X**:  $Ne(x)t$ , próximo

**X**  $\phi$ :  $\phi$  deve ser verdadeiro no próximo estado.

**F**  $\phi$  é verdadeiro num momento  $t$  se...

...  $\phi$  é verdadeiro no momento  $t + 1$ .

Exemplo: Logo após comer, tenho sede.



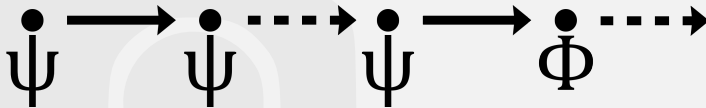
# U: Until, até

$\psi \text{ U } \phi$ :  $\psi$  deve ser verdade até que  $\phi$  seja verdade, sendo que  $\phi$  deve ser verdade no presente ou no futuro.

$\psi \text{ U } \phi$  é verdadeiro num momento  $t$  se...

... $\phi$  é verdadeiro em algum momento  $t' \geq t$  e, para todo tempo  $t''$  (tal que  $t \leq t'' < t'$ ),  $\psi$  é verdadeiro.

Exemplo: Eu tenho fome até eu comer alguma coisa.



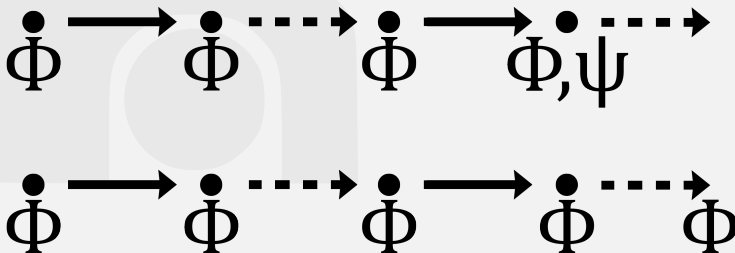
## R: *Release*, libera

$\psi$  **R**  $\phi$ :  $\phi$  deve ser verdade até e incluindo o momento que  $\psi$  se torna verdadeiro. Se  $\psi$  nunca ficar verdadeiro,  $\phi$  deve permanecer verdadeiro para sempre.

$\psi$  **R**  $\phi$  é verdadeiro num momento  $t$  se...

...  $\phi$  é verdadeiro em todos os momentos  $t' \geq t$  até e incluindo o momento  $t''$  onde  $\psi$  também é verdadeiro. Alternativamente, pode ser que  $\psi$  nunca seja verdadeiro, e nesse caso  $\phi$  deve ser verdadeiro para todo momento  $t' \geq t$ .

Exemplo: Ao comer chocolate, deixo de ter vontade de comer doce.







# Outline

Revisão & Cheatsheet

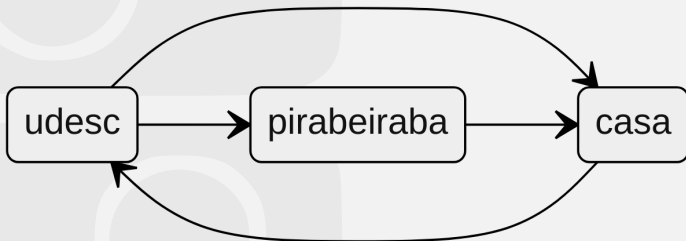
**Exemplos**

Exercício prático

Tipos de propriedades

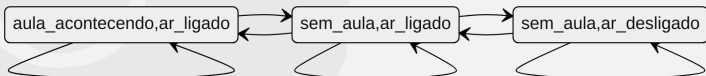
# Ônibus

Normalmente, Joãozinho pega ônibus pra udesc e de volta pra casa. Às vezes, Joãozinho erra o ônibus e vai parar em Pirabeiraba.



- $F \text{ casa: true}$

# Ar condicionado da sala de aula



- `aula_acontecendo -> sem_aula V ar_ligado: true`
- `aula_acontecendo -> ar_ligado U sem_aula: false`, porque podemos ficar em aula pra sempre :)



# Outline

Revisão & Cheatsheet

Exemplos

**Exercício prático**

Tipos de propriedades



# Exercício prático

Vamos escrever um avaliador de operadores para operadores temporais

- Isso não é um *model checker*, porque não vamos considerar todas as possíveis execuções de um sistema
- Dado uma única execução e uma fórmula temporal, a fórmula é verdadeira para essa execução?



# Outline

Revisão & Cheatsheet

Exemplos

Exercício prático

Tipos de propriedades



# Propriedades

Propriedades podem ser propriedades de **segurança** (*safety properties*), **vivacidade** (*liveness properties*) ou uma combinação das duas.

# Segurança

*“Algo ruim **não** acontece”*

Descreve algo específico. Basta esse algo acontecer uma única vez para que a propriedade seja violada.

## Exemplos:

- “O saque não deve ser autorizado, a menos que uma senha correta tenha sido digitada”
- “Dois processos não devem estar na seção crítica ao mesmo tempo”
- “Ao receber um saque, eu fico com mais dinheiro do que eu tinha antes”



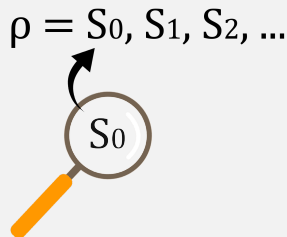
# Segurança - Invariantes

Invariantes são um tipo de propriedade de segurança.

Uma invariante é uma propriedade sobre um **estado**, *não sobre uma execução*. Uma invariante não consegue “ver além” de um único estado.

Uma **execução** satisfaz uma invariante sse cada estado da execução satisfaz a invariante.

Uma **estrutura de Kripke** satisfaz uma invariante sse cada estado alcançável satisfaz a invariante.





# Vivacidade

*“Algo bom eventualmente acontece”*

## **Exemplos:**

- “Se um processo pediu pra entrar na seção crítica, ele eventualmente deve conseguir”
- “Cada sinaleiro deve sempre eventualmente ficar verde”

# Vivacidade - propriedade de persistência

*“Eventualmente, algo é satisfeito pra sempre”*

$\diamond \square F$

## Exemplos:

- Ao entrar na faculdade, eventualmente vou ter um diploma
- Eventualmente estaremos mortos
- Eventualmente teremos cabelos brancos ou calvice



# Fairness (razoabilidade)

Propriedades de razoabilidade (*Fairness properties*)

- Razoabilidade incondicional (*Unconditional fairness*): “Algo acontece com frequência infinita”

# Fairness (razoabilidade)

Propriedades de razoabilidade (*Fairness properties*)

- Razoabilidade incondicional (*Unconditional fairness*): “Algo acontece com frequência infinita”
  - Razoabilidade **forte** (*Strong fairness*): “Algo acontece com frequência infinita **se é habilitado com frequência infinita**”

# Fairness (razoabilidade)

## Propriedades de razoabilidade (*Fairness properties*)

- Razoabilidade incondicional (*Unconditional fairness*): “Algo acontece com frequência infinita”
  - Razoabilidade **forte** (*Strong fairness*): “Algo acontece com frequência infinita **se é habilitado com frequência infinita**”
  - Razoabilidade **fraca** (*Weak fairness*): “Algo acontece com frequência infinita **se é continuamente habilitado a partir de um certo momento**”

# Fairness (razoabilidade)

Propriedades de razoabilidade (*Fairness properties*)

- Razoabilidade incondicional (*Unconditional fairness*): “Algo acontece com frequência infinita”
  - Razoabilidade **forte** (*Strong fairness*): “Algo acontece com frequência infinita **se é habilitado com frequência infinita**”
  - Razoabilidade **fraca** (*Weak fairness*): “Algo acontece com frequência infinita **se é continuamente habilitado a partir de um certo momento**”

Vamos ver isso com mais precisão na Lógica Temporal das Ações (TLA).

# Fairness (razoabilidade)

Propriedades de razoabilidade (*Fairness properties*)

- Razoabilidade incondicional (*Unconditional fairness*): “Algo acontece com frequência infinita”
  - Razoabilidade **forte** (*Strong fairness*): “Algo acontece com frequência infinita **se é habilitado com frequência infinita**”
  - Razoabilidade **fraca** (*Weak fairness*): “Algo acontece com frequência infinita **se é continuamente habilitado a partir de um certo momento**”

Vamos ver isso com mais precisão na Lógica Temporal das Ações (TLA).

Usamos essas propriedades como **pré-condições** para descartar execuções não realistas.

- $WF(...) \rightarrow F$
- $SF(...) \rightarrow F$





# Tarefa de casa

Ler página 10 de <https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf>



# FIM

## Checando propriedades com Lógica Temporal II

Aula para disciplina de Métodos Formais

Gabriela Moreira

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

11 de março de 2024