

# Математические методы верификации схем и программ

mk.cs.msu.ru → Лекционные курсы  
→ Математические методы верификации схем и программ

## Блок 18

Справедливость и CTL

Лектор:

**Подымов Владислав Васильевич**

E-mail:

**valdus@yandex.ru**

ВМК МГУ, 2022/2023, осенний семестр

# Напоминание

**Система переходов** над атомарными высказываниями AP и действиями Act — это модель Крипке, каждый переход которой помечен **действием**

**Безусловная справедливость**: действия заданного множества должны выполняться бесконечно часто

**Сильная справедливость**: если действия заданного множества могут выполняться бесконечно часто, то они должны выполняться бесконечно часто

**Слабая справедливость**: если действия заданного множества могут выполняться **почти всегда**, то они должны выполняться бесконечно часто

**Ограничения справедливости**  $\mathcal{F} = (\mathcal{F}_u, \mathcal{F}_s, \mathcal{F}_w)$ , где  $\mathcal{F}_u, \mathcal{F}_s, \mathcal{F}_w \subseteq 2^{\text{Act}}$  — это тройка семейств множеств, составляющих систему ограничений справедливости: каждое множество из  $\mathcal{F}_u$  — безусловной, каждое из  $\mathcal{F}_s$  — строгой, каждое из  $\mathcal{F}_w$  — слабой

## Напоминание

В LTL ограничения справедливости укладывались в рамки языка: если можно записать в виде формулы фразы «сейчас может выполняться действие множества  $A$ » и «сейчас было выполнено действие множества  $A$ », то ограничения справедливости можно было встроить в проверяемую формулу

В CTL так сделать нельзя — *из-за синтаксических ограничений на использование темпоральных операторов и, как будет показано дальше, невозможности записать на языке CTL словосочетание «почти всегда»*

Поэтому при внесении справедливости в CTL приходится изменять терминологический и алгоритмический фундамент: отношение выполнимости и алгоритм проверки выполнимости

# Напоминание

Отношение **выполнимости в ограничениях справедливости**  $\mathcal{F} \models_{\mathcal{F}}$  отличается от «обычного» отношения выполнимости для ctl-формул следующими пунктами:

- ▶  $M, s \models_{\mathcal{F}} \mathbf{A}\varphi \Leftrightarrow$  для любого  **$\mathcal{F}$ -справедливого** пути  $\pi$  в  $M$ , исходящего из  $s$ , верно  $M, \pi \models \varphi$
- ▶  $M, s \models_{\mathcal{F}} \mathbf{E}\varphi \Leftrightarrow$  существует  **$\mathcal{F}$ -справедливый** путь  $\pi$  в  $M$ , исходящий из  $s$  и такой что  $M, \pi \models \varphi$

## Напоминание

Алгоритм model checking в ограничениях справедливости  $\mathcal{F}$  может быть получен из базового внесением исправлений в процедуры  $Sat_{EX}$ ,  $Sat_{EU}$  и  $Sat_{EG}$ :

- ▶  $Sat_{EX}(M, \varphi)$ : множество  $Sat'(M, \varphi)$  следует заменить на  $Sat'(M, \varphi) \cap FairStates(M, \mathcal{F})$ 
  - ▶  $FairStates(M, \mathcal{F})$  — множество всех состояний  $M$ , из которых в  $M$  исходит хотя бы один  $\mathcal{F}$ -справедливый путь
- ▶  $Sat_{EU}(M, \varphi_1, \varphi_2)$ : множество  $Sat'(M, \varphi)$  следует заменить на  $Sat'(M, \varphi) \cap FairStates(M, \mathcal{F})$
- ▶  $Sat_{EG}(M, \varphi)$ : компоненты сильной связности следует заменить на  **$\mathcal{F}$ -справедливые компоненты сильной связности**, то есть такие, для которых возможен бесконечный обход, отвечающий  $\mathcal{F}$ -справедливому пути

Для самостоятельного размышления: а как вычислять  $FairStates(M, \mathcal{F})$  и справедливые компоненты сильной связности?