Математические методы верификации схем и программ

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

Блок 23

Справедливость и CTL

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2024/2025, 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 $\mathcal{F}_s$ — сильной, каждое из $\mathcal{F}_w$ — слабой

Напоминание

В LTL ограничения справедливости укладывались в рамки языка: если можно записать в виде формулы фразы «сейчас может выполниться действие множества A» и «сейчас было выполнено действие множества A», то ограничения справедливости можно 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 определения:

- $M, s \models_{\mathcal{F}} \mathbf{A}\varphi \Leftrightarrow$ для любого $\mathcal{F}$-справедливого пути π в M, исходящего из s, верно $M, \pi \models \varphi$

- $M, s \models_{\mathcal{F}} \mathbf{E}\varphi \Leftrightarrow$ существует $\mathcal{F}$-справедливый путь π в M, исходящий из s и такой что $M, \pi \models \varphi$

Напоминание

Алгоритм проверки моделей в ограничениях справедливости $\mathcal{F}$ может быть получен из базового внесением исправлений в процедуры $\mathfrak{P}_{\mathbf{EX}}$, $\mathfrak{P}_{\mathbf{EU}}$ и $\mathfrak{P}_{\mathbf{EG}}$:

- $\mathfrak{P}_{\mathbf{EX}}(M, \varphi)$: множество $\mathfrak{P}'_{sat}(M, \varphi)$ следует заменить на $\mathfrak{P}'_{sat}(M, \varphi) \cap \mathit{FairStates}(M, \mathcal{F})$
  - $\mathit{FairStates}(M, \mathcal{F})$ — множество всех состояний M, из которых в M исходит хотя бы один $\mathcal{F}$-справедливый путь
- $\mathfrak{P}_{\mathbf{EU}}(M, \varphi_1, \varphi_2)$: множество $\mathfrak{P}'_{sat}(M, \varphi_2)$ следует заменить на $\mathfrak{P}'_{sat}(M, \varphi_2) \cap \mathit{FairStates}(M, \mathcal{F})$
- $\mathfrak{P}_{\mathbf{EG}}(M, \varphi)$: н.к.с.с. следует заменить на $\mathcal{F}$-справедливые н.к.с.с., то есть такие, в которых есть бесконечный $\mathcal{F}$-справедливый путь

Для самостоятельного размышления:

а как вычислять $\mathit{FairStates}(M, \mathcal{F})$ и справедливые н.к.с.с.?