Математическая логика

mk.cs.msu.ru → Лекционные курсы → Математическая логика (318, 319/2, 241, 242)

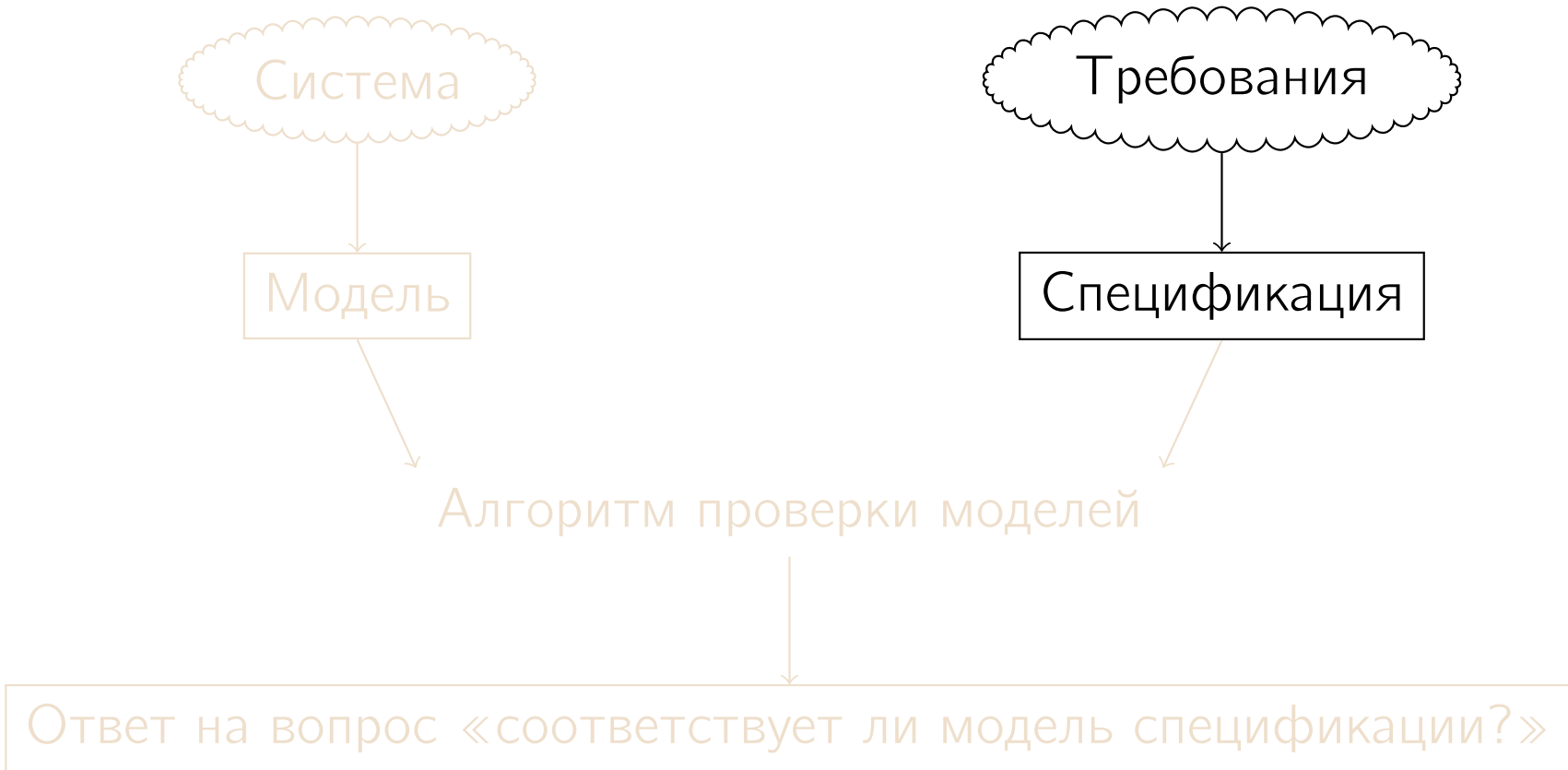
Блок 52

Спецификация систем
при помощи темпоральных логик

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

ВМК МГУ, 2025, февраль–май

Вступление


Система
Требования
Модель
Спецификация
Алгоритм проверки моделей
Ответ на вопрос «соответствует ли модель спецификации?»

Вступление

Оказалось, что в качестве основы модели распределённой системы
можно выбрать модели Крипке:
интерпретацию формул модальной логики

Тогда естественно возникает вопрос:
а нельзя ли в качестве основы языка спецификаций
выбрать язык модальных формул?

При положительном ответе можно будет использовать
все факты, относящиеся к модальным формулам
и их выполнимости в тех или иных моделях

Вступление

Основные препятствия на пути к использованию модальных формул в качестве спецификаций:

- Техническое: когда язык спецификаций выбран, следует строго, чётко и разумно (*адекватно*) поставить задачу проверки соответствия модели и спецификации
- Описательное: если язык спецификаций оказался слишком невыразительным, то требуется найти достаточно выразительное расширение этого языка
- Алгоритмическое: если эффективная проверка соответствия модели и спецификации оказалась невозможной, то требуется найти достаточно эффективно анализируемое сужение этого языка

CTL: синтаксис и семантика

Синтаксис формул CTL над множеством атомарных высказываний AP задаётся БНФ

$$\begin{aligned} \Phi &::= \mathbb{t} \mid p \mid (\Phi \,\&\, \Phi) \mid (\Phi \vee \Phi) \mid (\neg\Phi) \mid (\Phi \to \Phi) \\ &\quad \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi &::= (\mathbf{F}\Phi) \mid (\mathbf{G}\Phi) \mid (\mathbf{X}\Phi) \mid (\Phi\mathbf{U}\Phi), \end{aligned}$$

где

- Φ — формула CTL, или, по-другому, формула состояния,
- φ — формула пути и
- $p \in \mathrm{AP}$

Для двух видов формул соответственно определяется два вида выполнимости:

- Выполнимость формулы состояния Φ в заданном состоянии s СП M: $M, s \models \Phi$
- Выполнимость формулы пути φ на заданном бесконечном пути π в СП M: $M, \pi \models \varphi$

CTL: синтаксис и семантика

Синтаксис формул CTL над множеством атомарных высказываний AP задаётся БНФ

$$\begin{array}{rcl} \Phi & ::= & \mathbb{t} \mid p \mid (\Phi \,\&\, \Phi) \mid (\Phi \vee \Phi) \mid (\neg\Phi) \mid (\Phi \to \Phi) \\ & \mid & (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi & ::= & (\mathbf{F}\Phi) \mid (\mathbf{G}\Phi) \mid (\mathbf{X}\Phi) \mid (\Phi\mathbf{U}\Phi), \end{array}$$

Приоритеты операций: $\neg$, **A**, **E**, **F**, **G** и **X**; затем **U**;
затем остальные операции с обычными приоритетами

Символ $\mathbb{t}$, связки $\&$, $\vee$, $\neg$, $\to$ и атомарное высказывание p имеют «привычный» содержательный смысл

Буквы **A** и **E** — это кванторы пути:

- «$\mathbf{A}\varphi$» = «для любого бесконечного пути, исходящего из текущего состояния, верно φ» и
- «$\mathbf{E}\varphi$» = «существует бесконечный путь, исходящий из текущего состояния и такой что для него верно φ»

CTL: синтаксис и семантика

Синтаксис формул CTL над множеством атомарных высказываний AP задаётся БНФ

$$\begin{aligned} \Phi &::= \mathbb{t} \mid p \mid (\Phi \,\&\, \Phi) \mid (\Phi \vee \Phi) \mid (\neg\Phi) \mid (\Phi \to \Phi) \\ &\quad \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi) \\ \varphi &::= (\mathbf{F}\Phi) \mid (\mathbf{G}\Phi) \mid (\mathbf{X}\Phi) \mid (\Phi\mathbf{U}\Phi), \end{aligned}$$

Буквы **F**, **G**, **X**, **U** — это темпоральные операторы:

- «$\mathbf{F}\varphi$» = «когда-нибудь, рано или поздно, станет верно φ»
- «$\mathbf{G}\varphi$» = «всегда будет верно φ»
- «$\mathbf{X}\varphi$» = «в следующем состоянии будет верно φ» (neXt step)
- «$\varphi\mathbf{U}\psi$» = «когда-нибудь станет верно ψ,
  а пока оно не стало верным, обязательно верно φ» (Until)

Согласно синтаксису, кванторы пути и темпоральные операторы встречаются в формулах только в парах: снаружи квантор, внутри оператор

То есть: **AG**, **EG**, **AF**, **EF**, **AX**, **EX**, **A**(. . . U . . .), **E**(. . . U . . .)

CTL: синтаксис и семантика

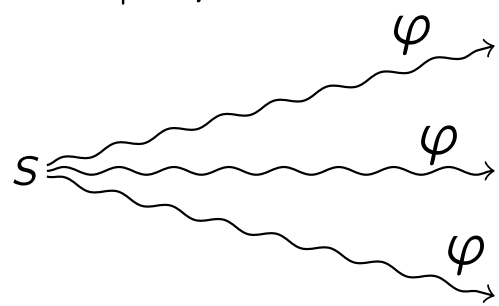
Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π задатся следующими правилами:

- Соотношение $M, s \models \mathbb{t}$ верно всегда
- $M, s \models p$, где $p \in \mathrm{AP} \quad \Leftrightarrow \quad p \in L(s)$
- $M, s \models \Phi \,\&\, \Psi \quad \Leftrightarrow \quad M, s \models \Phi$ и $M, s \models \Psi$
- $M, s \models \Phi \vee \Psi \quad \Leftrightarrow \quad M, s \models \Phi$ или $M, s \models \Psi$
- $M, s \models \neg\Phi \quad \Leftrightarrow \quad M, s \not\models \Phi$
- $M, s \models \Phi \to \Psi \quad \Leftrightarrow \quad M, s \not\models \Phi$ или $M, s \models \Psi$

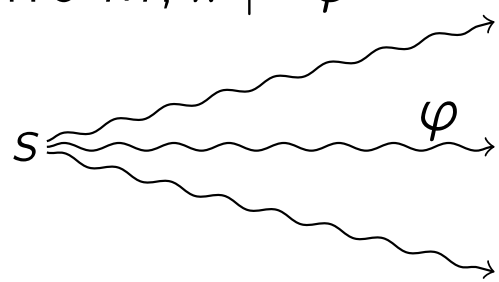
CTL: синтаксис и семантика

Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π задатся следующими правилами:

- $M, s \models \mathbf{A}\varphi \quad \Leftrightarrow \quad$ для любого бесконечного пути π в M, исходящего из s, верно $M, \pi \models \varphi$



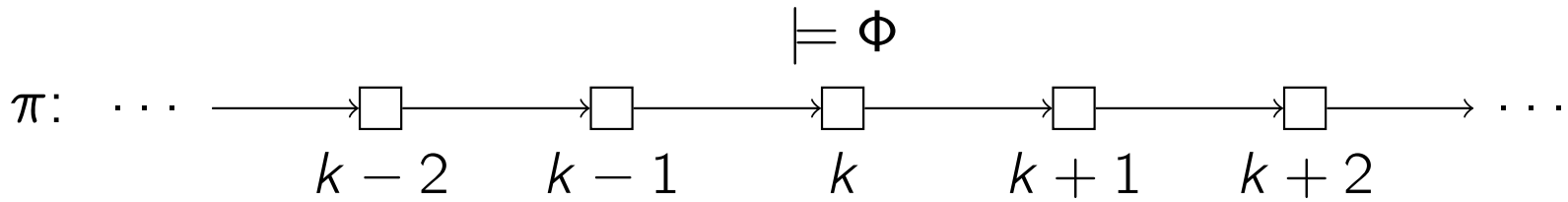
- $M, s \models \mathbf{E}\varphi \quad \Leftrightarrow \quad$ существует бесконечный путь в M, исходящий из s и такой что $M, \pi \models \varphi$



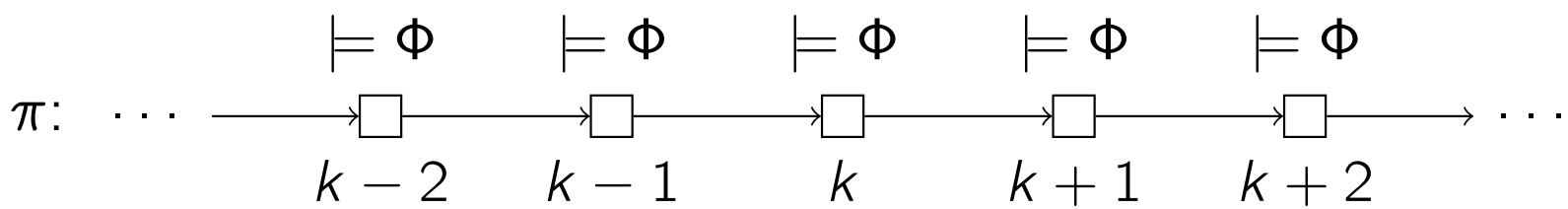
CTL: синтаксис и семантика

Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π задатся следующими правилами:

- $M, \pi \models \mathbf{F}\Phi \quad \Leftrightarrow \quad$ существует номер k, $k \geq 1$, такой что $M, \pi[k] \models \Phi$
  - $\pi[i]$ — i-е состояние пути π при нумерации с единицы



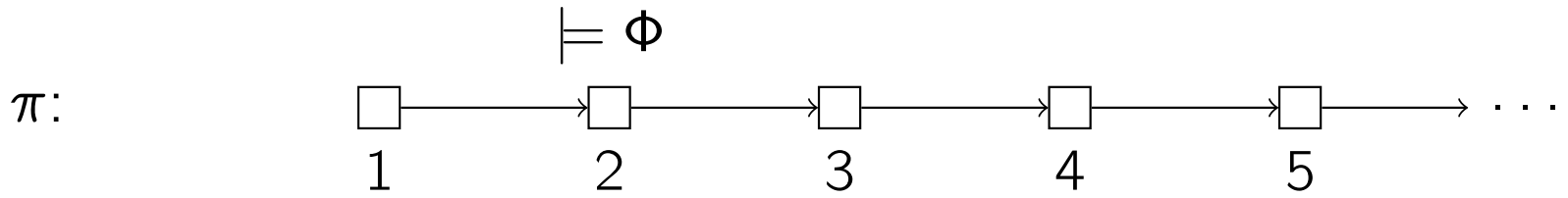
- $M, \pi \models \mathbf{G}\Phi \quad \Leftrightarrow \quad$ для любого номера k, $k \geq 1$, верно $M, \pi[k] \models \varphi$



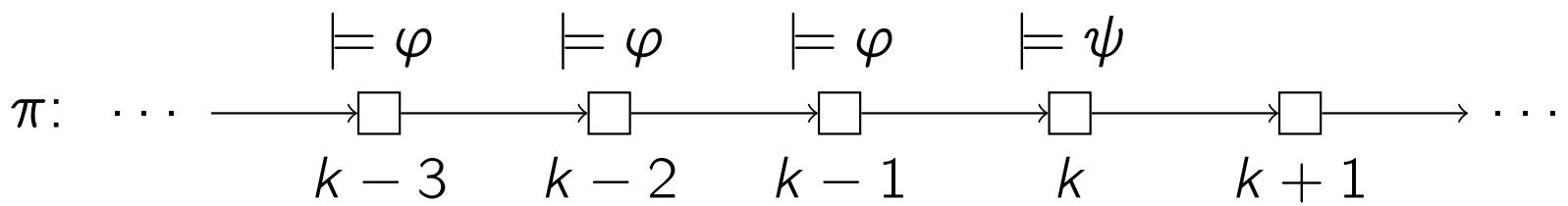
CTL: синтаксис и семантика

Отношения выполнимости формул для СП $M = (S, S_0, \mapsto, L)$, состояния s и бесконечного пути π задатся следующими правилами:

- $M, \pi \models \mathbf{X}\Phi \quad \Leftrightarrow \quad M, \pi[2] \models \Phi$



- $M, \pi \models \Phi\mathbf{U}\Psi \quad \Leftrightarrow \quad$ существует номер k, $k \geq 1$, такой что
  - $M, \pi[k] \models \Psi$ и
  - для любого номера m, такого что $1 \leq m < k$, верно $M, \pi[m] \models \Phi$



CTL: постановка задачи проверки моделей

Формула CTL Φ выполняется на СП M ($M \models \Phi$),
если она выполняется в любом начальном состоянии системы M

Задача проверки моделей для CTL формулируется так:
для заданной **конечной** системы переходов M
и заданной формулы Φ CTL
проверить справедливость соотношения $M \models \Phi$

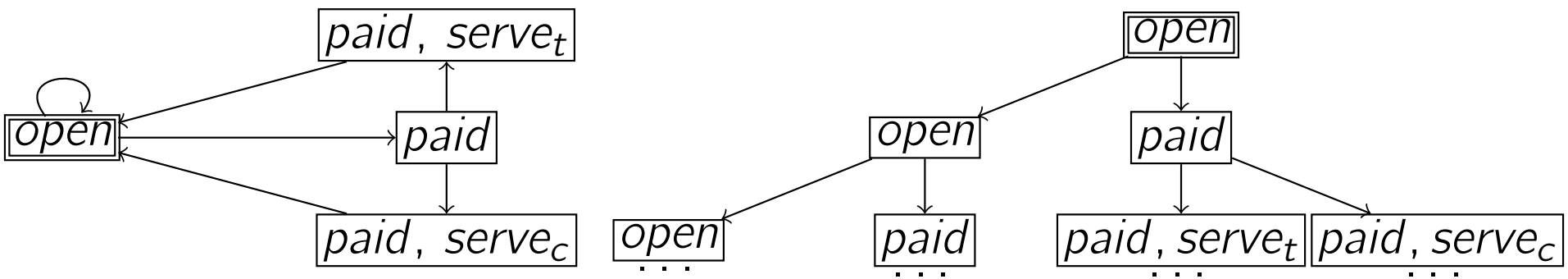
CTL: постановка задачи проверки моделей

В блоке 45 рассказывалось, что формулы CTL интерпретируются на рефлексивно-транзитивных замыканиях особых бесконечных деревьев

Такое бесконечное дерево можно понимать
как развёртку системы переходов:

- Корень — это выбранное начальное состояние
- Вершина развёртки отвечает конечному пути в СП
  и размечена теми же атомарными высказываниями,
  что и последняя вершина пути
- Дуга $v_1 \to v_2$ в развёртке означает,
  что путь v_1 можно продолжить до пути v_2, добавив один переход

Например, ниже изображены СП и фрагмент её развёртки



CTL: постановка задачи проверки моделей

Примеры спецификаций на языке CTL для кофейного автомата:

- В самом начале работы автомата приёмник монет открыт, в нём нет монеты, и автомат ничего не выдаёт:
$$open \,\&\, \neg paid \,\&\, \neg serve_t \,\&\, \neg serve_c$$
- Нельзя сделать так, чтобы автомат выдал напиток, не имея монеты в приёмнике:
$$\neg \mathbf{EF}(\neg paid \,\&\, (serve_c \vee serve_t))$$
- Если в приёмнике есть монета, то рано или поздно он выдаст напиток ...
$$\mathbf{AG}(paid \to \mathbf{AF}(serve_c \vee serve_t))$$
- ... но этот напиток не обязан быть чаем ...
$$\mathbf{EF}(paid \,\&\, \mathbf{EG} \neg serve_t)$$
- ... но при желании можно, опустив монету в приёмник, получить чай
$$\mathbf{AG}(\neg paid \to \mathbf{AX}(paid \to \mathbf{EF} serve_t))$$