

Математические методы верификации схем и программ

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

Семинар 2

Модели Крипке
LTL
Безопасность и живость
Справедливость

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

ВМК МГУ, 2023/2024, осенний семестр

Упражнение 1

Построить модель Крипке над заданным множеством атомарных высказываний для заданной системы

Система состоит из двух параллельно выполняющихся программ:

$x := 1; y := 2;$

$y := 1; x := 2;$

Программы выполняются на состоянии данных $[x/0, y/0]$

Атомарные высказывания: x/i и y/i , $i \in \{0, 1, -1, 2, -2, \dots\}$

Упражнение 1

Построить модель Крипке над заданным множеством атомарных высказываний для заданной системы

Система состоит из двух параллельно выполняющихся программ, каждая из которых имеет вид

$$x := x + x;$$

Программы выполняются на состоянии данных $[x/1]$ для общей переменной x

Атомарные высказывания: $x = i, \quad i \in \mathbb{Z}$

Упражнение 1

Построить модель Крипке над заданным множеством атомарных высказываний для заданной системы

Система состоит из двух параллельно выполняющихся программ, каждая из которых имеет вид

$$x := x + x;$$

Программы выполняются на состоянии данных $[x/1]$ для общей переменной x

Атомарные высказывания: $x = i, \quad i \in \mathbb{Z}$

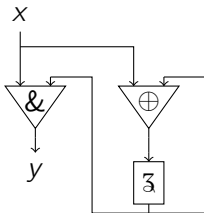
Усложнённый вариант: присваивание суммы реализовано как три атомарных действия:

1. получить значение левого аргумента суммы
2. получить значение правого аргумента суммы
3. сохранить сумму полученных значений в целевую переменную

Упражнение 1

Построить модель Крипке над заданным множеством атомарных высказываний для заданной системы

Система: схема из функциональных элементов с задержкой



Атомарные высказывания: $(i \in \{0, 1\})$

- ▶ x_i : входное значение x есть i
- ▶ y_i : выходное значение y есть i

Упражнение 1

Построить модель Крипке над заданным множеством атомарных высказываний для заданной системы

Система: головоломка про волка, козу и капусту

Гранулярность переходов:

1. посадка, плавание и высадка — одно атомарное действие
2. посадка, плавание и высадка — три атомарных действия
3. посадка каждого участника, плавание и высадка каждого участника — пять атомарных действий (три, если плывёт только лодочник)

Свобода действий участников: если кто-то может быть съеден, то он

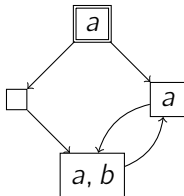
1. ... съедается немедленно
2. ... обязательно съедается при выполнении следующего перехода
3. ... может как быть съеден немедленно, так и не быть съеден

Атомарные высказывания:

- ▶ *wr, gr, cr*: волк/коза/капуста находятся на правом (целевом) берегу
- ▶ *ga, sa*: коза/капуста «живы» (не съедены)

Упражнение 2

Построить все вычисления и их трассы для следующей модели Крипке



Упражнение 3

Предложить ltl-формулу, выражающую следующее требование:

1. Процессы P_1 , P_2 не могут находиться в своих критических секциях одновременно

c_i — атомарное высказывание

“ P_i находится в своей критической секции”

2. Зелёный светофор рано или поздно станет жёлтым и до этого не будет красным

g , y , r — атомарные высказывания “светофор зелёный”, “светофор жёлтый” и “светофор красный” соответственно

3. Сообщение не может теряться бесконечно часто

$miss$ — атомарное высказывание “сообщение потеряно”

Упражнение 3

Предложить ltl-формулу, выражающую следующее требование:

4. Операция не может выполняться более трёх тактов подряд

p — атомарное высказывание

“операция выполняется на текущем такте”

5. Система постоянно сигнализирует об ошибке, пока не станет исправной

ok — атомарное высказывание *“система исправна”*

err — атомарное высказывание *“система сигнализирует об ошибке”*

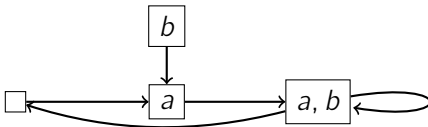
6. Кто много тренируется, тот рано или поздно достигнет совершенства

t — атомарное высказывание *“он тренируется”*

p — атомарное высказывание *“он достиг совершенства”*

Упражнение 4

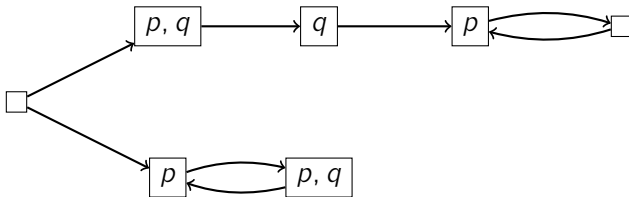
Какие состояния заданной модели Крипке можно объявить начальными так, чтобы на модели была выполнена заданная ltl-формула?



- ▶ a
- ▶ $\mathbf{XX}a$
- ▶ $\mathbf{G}a$
- ▶ $\mathbf{GF}a$
- ▶ $\mathbf{FG}a$
- ▶ $\neg b \mathbf{U} a \ \& \ b$
- ▶ $a \mathbf{U} \neg a$

Упражнение 4

Какие состояния заданной модели Крипке можно объявить начальными так, чтобы на модели была выполнена заданная ltl-формула?



► $F(\mathbf{X}p\mathbf{UG}\neg q)$

Упражнение 5

Является ли заданное множество трасс над непустым множеством AP

- а) свойством безопасности?
- б) свойством живости?

1. $(2^{AP})^\omega$
2. \emptyset
3. $\{\emptyset, \{a\}\}^\omega$ для $AP = \{a, b\}$
4. $\{\emptyset, \{a\}\}^* \cdot \{\emptyset\}^\omega$ для $AP = \{a\}$
5. $\{\emptyset\}^* \cdot \{\{a\}\} \cdot \{\emptyset\}^\omega$ для $AP = \{a\}$
6. $\{\emptyset\{a\}\}^\omega$ для $AP = \{a\}$
7. $\{\emptyset, \{a\}, \{b\}\}^* \cdot \{\{a, b\}\} \cdot \{\emptyset\}^\omega$ для $AP = \{a, b\}$

Упражнение 6

Справедливо ли следующее утверждение для **любых** свойств трасс P_1 и P_2 ?

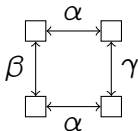
1. Если P_1 и P_2 — свойства безопасности, то $P_1 \cap P_2$ — свойство безопасности
2. Если P_1 и P_2 — свойства безопасности, то $P_1 \cup P_2$ — свойство безопасности
3. Если P_1 и P_2 — свойства живости, то $P_1 \cap P_2$ — свойство живости
4. Если P_1 и P_2 — свойства живости, то $P_1 \cup P_2$ — свойство живости

Упражнение 7

Какие пути следующей системы переходов **не** являются

- а) безусловно A -справедливыми
- б) сильно A -справедливыми
- в) слабо A -справедливыми

для заданного множества действий A ?



- 1. $A = \emptyset$
- 2. $A = \{\alpha\}$
- 3. $A = \{\beta\}$
- 4. $A = \{\gamma\}$
- 5. $A = \{\alpha, \beta\}$
- 6. $A = \{\beta, \gamma\}$
- 7. $A = \{\alpha, \beta, \gamma\}$

Упражнение 8

Построить все ограничения справедливости $\mathcal{F} = (\mathcal{F}_u, \mathcal{F}_s, \mathcal{F}_w)$, для которых верно соотношение $TS, \mathcal{F} \models \mathbf{GF}a$

TS :

