Математические методы верификации схем и программ

Лекторы:

Захаров Владимир Анатольевич

Подымов Владислав Васильевич

e-mail рассказчика:

valdus@yandex.ru

Осень 2017

Семинар 2

Модели Крипке

CTL, LTL

Безопасность и живость

Справедливость

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний

Система:

```
cobegin
  x := 1; y := 2
||
  y := 1; x := 2
coend
```

(начальное состояние данных: `x = 0, y = 0`)

Высказывания: `x =` i и `y =` i , $i \in \mathbb{Z}$

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний

Система: `cobegin x := x + x || x := x + x coend`

(начальное состояние данных: `x = 1`)

Высказывания: `x =` i , $i \in \mathbb{Z}$

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний

Система: `cobegin x := x + x || x := x + x coend`

(начальное состояние данных: `x = 1`)

Высказывания: `x =` i , $i \in \mathbb{Z}$

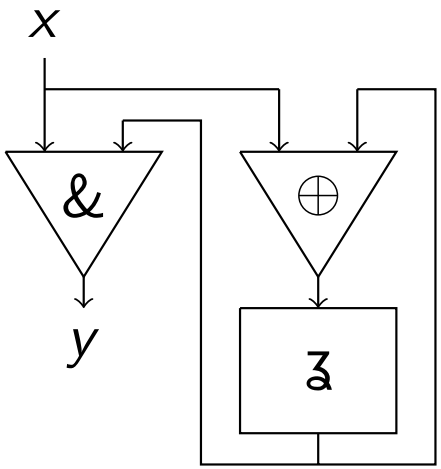
Усложнение: инструкция присваивания суммы реализована как 4 атомарных действия:

1. прочитать значение первого слагаемого
2. прочитать значение второго слагаемого
3. вычислить результат — сумму прочитанных значений
4. записать результат в целевую переменную

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний

Система: схема из функциональных элементов с задержкой



Высказывания: $(i \in \{0, 1\})$

- x_i: на вход x подано значение i
- y_i: на выходе y получено значение i

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний

Система: волк, коза, капуста и лодочник в задаче о переправе

Вариации:

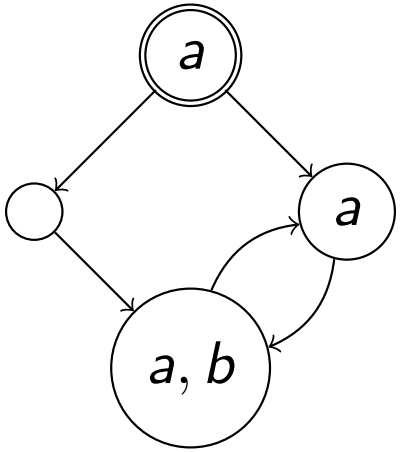
1. Все события (обед, посадка в лодку, переправа, высадка из лодки, ...) мгновенны, и при необходимых условиях могут как происходить, так и не происходить
2. Все события, кроме переправы, мгновенны; обед происходит немедленно при соблюдении необходимых условий
3. Все события, проме переправы, мгновенны; обед может как произойти, так и не произойти при соблюдении необходимых условий

Высказывания:

- *wr*, *gr*, *cr*: волк/коза/капуста находятся на правом берегу
- *wa*, *ga*, *ca*: волк/коза/капуста живы

Упражнение 2

Описать множество всех трасс заданной модели Крипке



S — состояние, помеченное множеством высказываний $\{S\}$

Переходы модели изображаются дугами

◎ — начальное состояние

Упражнение 3

Является ли множество P свойством

а) безопасности

б) живости

трасс над непустым множеством атомарных высказываний AP?

1. $P = AP^\omega$
2. $P = \emptyset$
3. $AP = \{a, b, c\}$, $P = \{a, b\}^\omega$
4. $AP = \{a, b\}$, $P = \{a\}^* \cdot \{b\} \cdot \{a\}^\omega$
5. $AP = \{a, b\}$, $P = \{a, b\}^* \cdot \{a\}^\omega$
6. $AP = \{a, b, c\}$, $P = \{a, b\}^* \cdot \{c\} \cdot \{a\}^\omega$
7. $AP = \{a, b\}$, $P = \{ab\}^\omega$

$X^\omega = \{w_1 w_2 w_3 \cdots \mid w_i \in X\}$
$X^* = \{w_1 w_2 \ldots w_k \mid w_i \in X,\ k \in \mathbb{N}_0\}$
$X \cdot Y = \{w_x w_y \mid w_x \in X,\ w_y \in Y\}$

Упражнение 4

Всегда ли верны следующие утверждения?

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

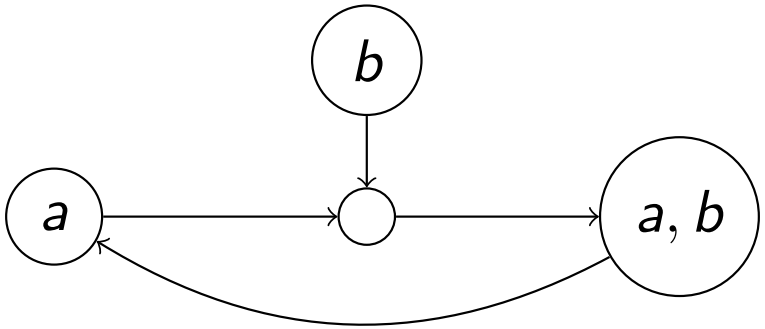
Упражнение 5

Записать формулу логики LTL, адекватно формализующую следующее высказывание:

1. Кто много тренируется, тот обязательно достигнет совершенства
2. Если лифт отправился, то он обязательно остановится, и во время движения двери не откроются
3. Два процесса никогда не займут критическую секцию одновременно
4. Сообщение может быть потеряно в канале связи лишь конечное число раз
5. Приём и обработка сообщения обязательно чередуются
6. Операция выполняется процессором ровно 4 такта
7. Как только система сломалась, она начнёт бесконечно часто сигнализировать о неисправности, пока её питание не отключат

Упражнение 6

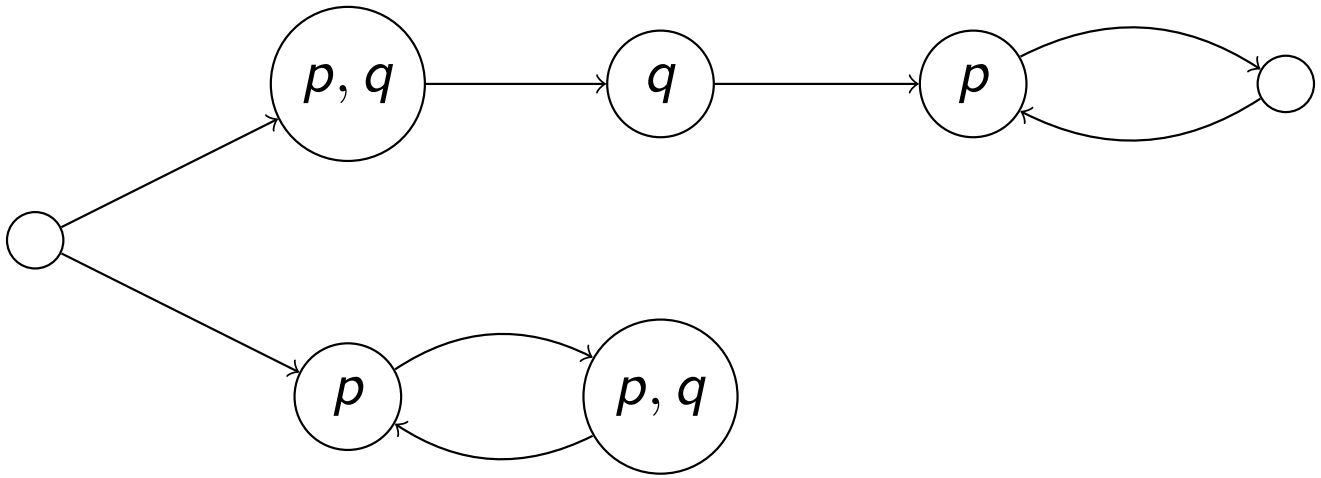
В каких состояниях приведённой ниже модели выполняется заданная LTL-формула?



- $\mathbf{AX}a$
- $\mathbf{AXXX}a$
- $\mathbf{AG}a$
- $\mathbf{AGF}a$
- $\mathbf{AFG}a$
- $\mathbf{AG}(b\mathbf{U}a)$
- $\mathbf{AF}(a\mathbf{U}b)$

Упражнение 6

В каких состояниях приведённой ниже модели выполняется заданная LTL-формула?



- $\mathbf{AF}(\mathbf{X}p\mathbf{UG}\neg q)$

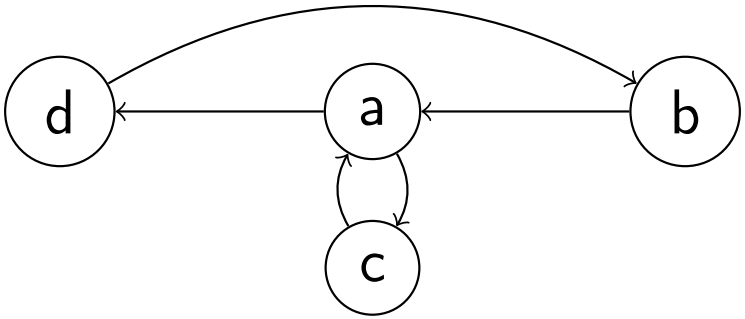
Упражнение 7

Записать формулу логики CTL, адекватно формализующую следующее высказывание:

1. Если постоянно запрашивать вход в критическую секцию, то когда-нибудь доступ в неё будет получен
2. Между приёмом и обработкой сообщения оно никогда не удаляется
3. Когда компьютер запущен, всегда есть возможность его выключить
4. Если компьютер сломался, то это навсегда
5. Если когда-нибудь я захочу всё бросить, то всегда смогу это сделать на следующий день
6. Если когда-нибудь обнаружится, что я не сдал сессию, то меня обязательно вышвырнут на следующий день

Упражнение 8

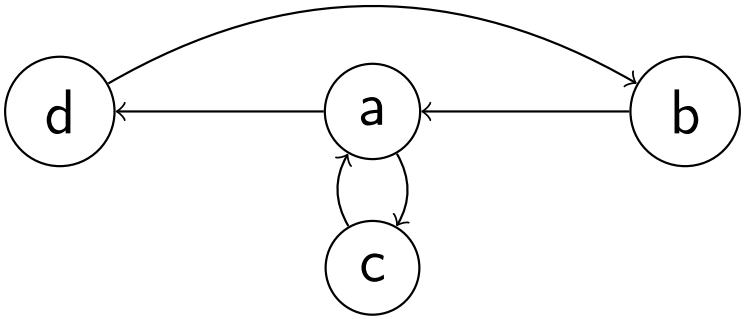
В каких состояниях приведённой ниже модели выполняется заданная CTL-формула?



1. $\mathbf{AGAF}a$
2. $\mathbf{EF}b$
3. $\mathbf{AF}b$
4. $\mathbf{EG}b$
5. $\mathbf{EG}\neg b$

Упражнение 8

В каких состояниях приведённой ниже модели выполняется заданная CTL-формула?



1. $\mathbf{EX}d$
2. $\mathbf{AX}d$
3. $\mathbf{E}(c\mathbf{U}\neg c)$
4. $\mathbf{A}(\neg c\mathbf{UEF}c)$
5. $\mathbf{A}(b\mathbf{UA}(a\mathbf{U}d))$

Упражнение 9

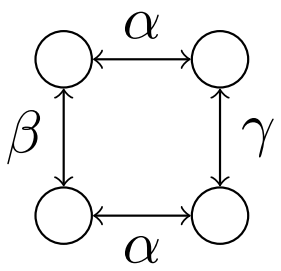
Верно ли, что для любой модели Крипке M и любого состояния s этой модели верно следующее утверждение:

$$\text{если } M, s \models \varphi, \text{ то } M, s \models \psi \quad ?$$

1. $\varphi = \mathbf{AFAG}p$, $\psi = \mathbf{AFG}p$
2. $\varphi = \mathbf{AFG}p$, $\psi = \mathbf{AFAG}p$
3. $\varphi = \mathbf{AFEG}p$, $\psi = \mathbf{AFG}p$
4. $\varphi = \mathbf{AFG}p$, $\psi = \mathbf{AFEG}p$
5. $\varphi = \mathbf{AGAF}p$, $\psi = \mathbf{AGF}p$
6. $\varphi = \mathbf{AGF}p$, $\psi = \mathbf{AGAF}p$
7. $\varphi = \mathbf{AGEF}p$, $\psi = \mathbf{AGF}p$
8. $\varphi = \mathbf{AGF}p$, $\psi = \mathbf{AGEF}p$

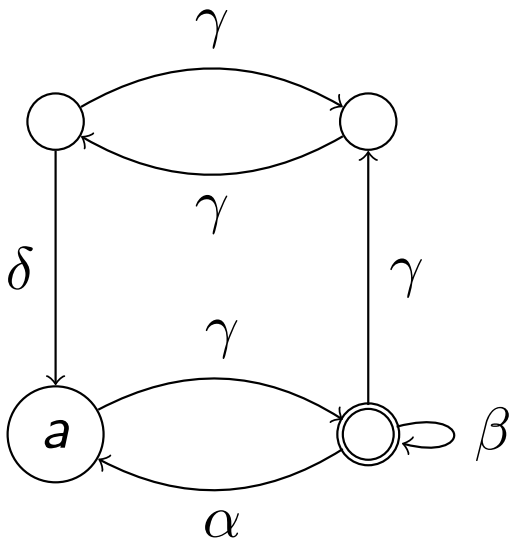
Упражнение 10

Какие пути приведённой ниже модели M **не** входят в множество $Tr(M, Fair)$ для ограничений справедливости $Fair = (WeakFair, StrongFair)$?



1. $WeakFair = \emptyset$, $StrongFair = \emptyset$;
2. $WeakFair = \{\alpha\}$, $StrongFair = \emptyset$;
3. $WeakFair = \{\alpha, \beta\}$, $StrongFair = \emptyset$;
4. $WeakFair = \{\alpha\}$, $StrongFair = \{\beta\}$;
5. $WeakFair = \emptyset$, $StrongFair = \{\alpha, \beta\}$;
6. $WeakFair = \emptyset$, $StrongFair = \{\alpha, \beta, \gamma\}$;

Упражнение 11

Описать всевозможные условия справедливости $Fair = (WeakFair, StrongFair)$, для которых будет верно соотношение $M, Fair \models \mathbf{AGF}a$

M: