Математические методы верификации схем и программ

Семинар 2

Модели Крипке, CTL, LTL, Безопасность, живость, справедливость

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний.

Система: **cobegin** p1 || p2 **coend**, где

p1:
```
x := 1;
y := 2
```

p2:
```
y := 1;
x := 2
```

Начальное состояние данных: $x = 0$, $y = 0$

Атомарные высказывания:

$$x = i, \qquad y = i \qquad (i \in \mathbb{Z})$$

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний.

Система: $\textbf{cobegin} \;\; \mathtt{x} := \mathtt{x} + \mathtt{x} \;\; || \;\; \mathtt{x} := \mathtt{x} + \mathtt{x} \;\; \textbf{coend}$

Начальное состояние данных: $x = 1$

Атомарные высказывания: $x = i \qquad (i \in \mathbb{Z})$

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: $x = 1$

Атомарные высказывания: $x = i \qquad (i \in \mathbb{Z})$

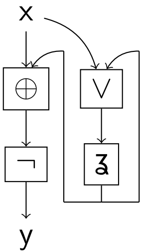
А если операция сложения не атомарна?

Построить модель в предположении, что присваивание $x := y + z$ реализуется как четыре неделимые команды работы с локальным стеком программы: положить в стек значение y; положить в стек значение z; выбрать из стека два верхних значения, сложить и положить результат в стек; выбрать значение из стека и загрузить в переменную

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний.

Система — схема из функциональных элементов с задержкой:



Атомарные предикаты: x_0, x_1, y_0, y_1, $\mathfrak{z}_0$, $\mathfrak{z}_1$

(*индекс — текущее значение переменной/задержки*)

Упражнение 1

Построить модель Крипке для заданной системы и заданного набора атомарных высказываний.

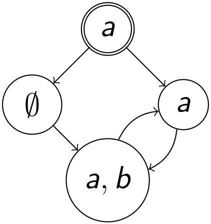
Система: волк, коза, капуста и лодочник в задаче о переправе

1. Лодочник переправляет мгновенно и может отдыхать на берегу сколько угодно, поедание не мгновенно
2. Лодочник переправляет дольше, чем происходит поедание, и не отдыхает на берегу
3. Лодочник переправляет дольше, чем происходит поедание, и может отдыхать на берегу

Атомарные предикаты: волк переправлен (wr), коза переправлена (gr), капуста переправлена (cr), коза жива (ga), капуста не съедена (ca)

Упражнение 2

Описать множество всех трасс заданной модели Крипке.



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

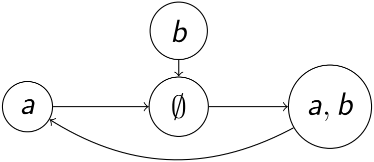
Упражнение 5

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

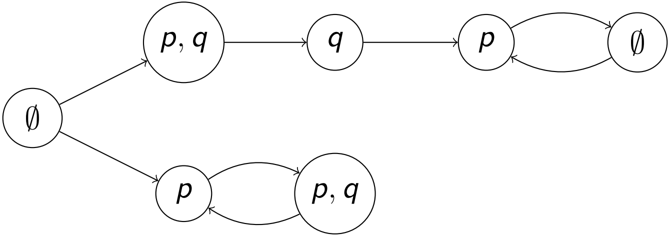
В каких состояниях приведённой ниже модели выполняется заданная LTL-формула?



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

Упражнение 6

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



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

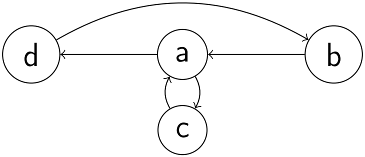
Упражнение 7

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

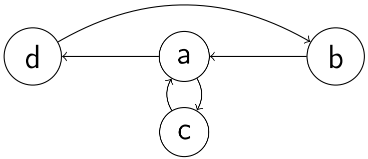
В каких состояниях приведённой ниже модели выполняется заданная CTL-формула?



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

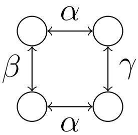
Будет ли верным для любых модели M и состояния s следующее утверждение:

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

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 $M, Fair \models \mathbf{AGF}a$?