Model Checking

Модель Крипке для кофемашины DeLonge

Shurygin Anton Alexeevich

21 декабря 2023 г.

Введение

Последние несколько недель я только и существую с помощь кофемашины DeLonge. Поэтому я решил описать ее устройство, используя модель Крипке, поскольку пользовался ей достаточно.

Рис.: Вид спереди

Рис.: Вид сбоку

Введение

Определим множество предикатов нашей системы $P = s, h, w, g, m$

- s - start, флаг запуска кофемашины, работу от сети
- h - heated, флаг прогретости термопары кофемашины
- w - water, флаг гарантирующий необходимого количества воды для работы
- g - ground, флаг, гарантирующий свободное место в контейнере для гущи
- g - ground, флаг, гарантирующий использования молока

Введение

Определим множество состояний нашей системы S

- S_0 - кофемашина выключена
- S_1 - кофемашина подключена в сеть
- S_2 - кофемашина проверяет нынышнее значение воды
- S_3 - кофемашина проверяет заполненность контейнера для гущи
- S_4 - кофемашина в режиме ожидания
- S_5 - приготовить кофе с молоком
- S_6 - приготовить черный кофе
- S_7 - кофемашина запрашивает очистить бак с молоком
- S_8 - невалидное состояние, термпопара прогрелась до проверки количества воды

Алгоритм функционирования DeLonge

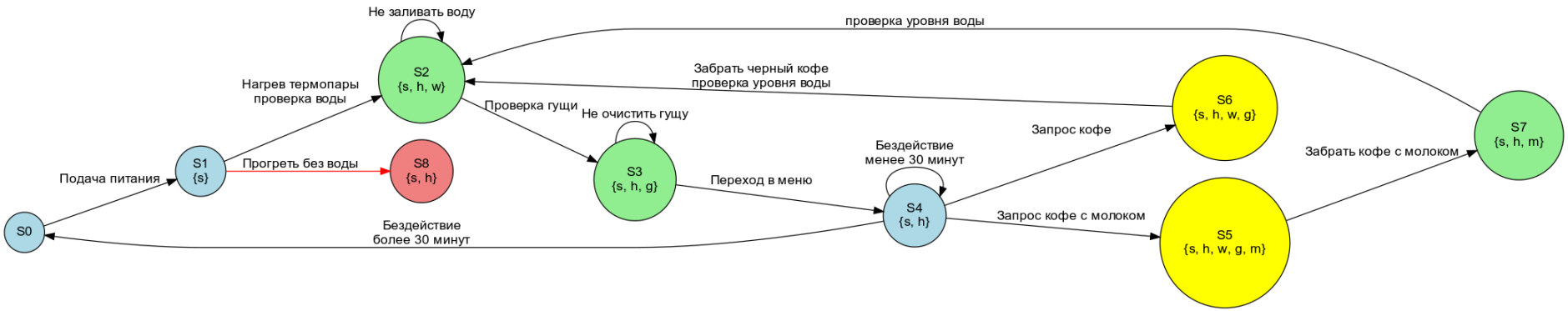

Рис.: Граф переходов между состояниями

Свойства safety

Свойства safety с использованием темпоральной логики LTL:

1. Требование безопасности: После включения (s) и нагрева термопары (h), должна произойти проверка воды (w). LTL: $G((s \wedge h) \rightarrow Fw)$
2. Проверка гущи (g) должна произойти только после проверки воды (w): LTL: $G((w \rightarrow Fg))$
3. Проверка гущи (g) должна произойти только после включения (s) и нагрева термопары (h): LTL: $G((s \wedge h) \rightarrow Fg)$
4. Если контейнер с гущей (g) пуст, то после запроса кофе (в состоянии s, h, g) должен произойти переход в меню в режим ожидания (в состояние s, h): LTL: $G(((s \wedge h \wedge w \wedge g \wedge m) \rightarrow F(s \wedge h \wedge w \wedge m)))$
5. Если кофемашина выключена (s), то не должно произойти запроса кофе с молоком: LTL: $G(s \rightarrow \neg F(s \wedge h \wedge w \wedge g \wedge m))$

Свойства liveness

Свойства liveness (живучести) в терминах темпоральной логики LTL:

1. После нагрева термопары, должна произойти проверка гущи: LTL: $G(h \rightarrow Fg)$
2. После запроса кофе кофе с молоком должна произойти очистка трубки с молоком: LTL: $G(((s \wedge h \wedge w \wedge g \wedge m) \rightarrow F(s \wedge h \wedge m))$

Нарушение свойства safety

На рис.5 указан красным цветом пример состояния, нарушающий одно свойство safety. Формализуем это как $G(h \rightarrow \neg w)$ означает буквально "всегда верно, что если термопара нагрета, то вода не проверяется". Это невалидное состояние, так как нагрев термопары в начале должен быть предшествовать проверке воды для корректной работы кофейной машины.