Санкт-Петербургский Государственный Политехнический Университет

Курсовая работа
Разработка контроллера светофоров и его верификация

Выполнил: студент гр. 63504-12 Лукашин А.А.

Руководитель: ст. преподаватель Шошмина И.В.

2013

Введение

- Верификация (model checking) – это набор формальных приемов и методов подтверждения того, что разрабатываемая система удовлетворяет формальным установленным требованиям
- От программных систем все в большей степени каждодневно зависят жизнь и здоровье людей, однако программирование до сих пор остается единственной областью инженерной деятельности, где разработчик фактически не может гарантировать качество своей работы
- Системы для формальной верификации ПО все чаще применяются в промышленной разработке

Описание модели

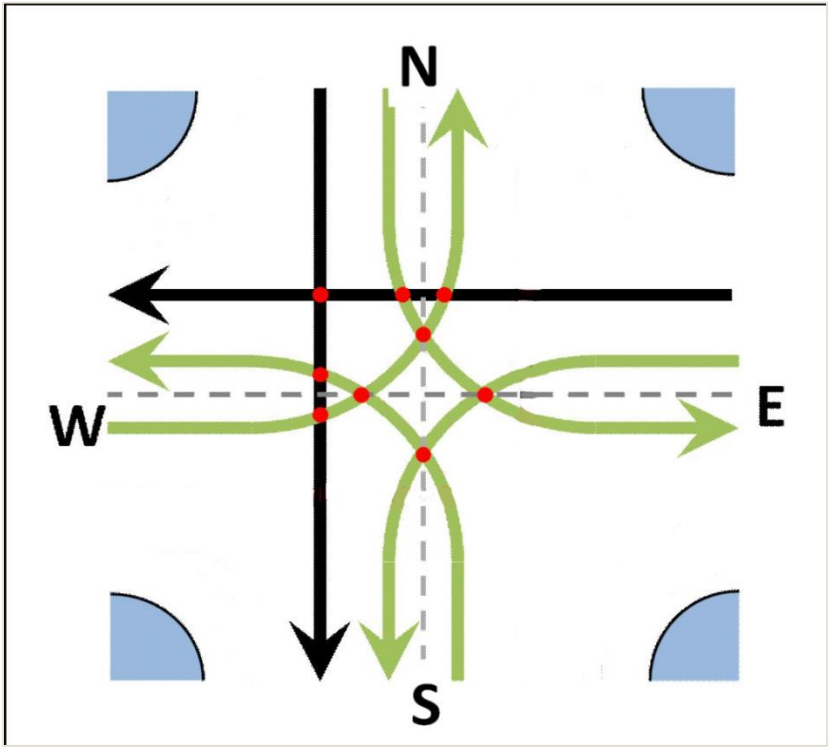
- В данной курсовой работе рассматривается модель контроллера управления движением на дорожном перекрестке. Необходимо описать модель и проверить ее корректность при выполнении следующих условий:
  - Каждое направление контролирует отдельный светофор
  - Поведение светофоров описывается параллельными процессами
  - Необходимо моделировать появление машин
  - Алгоритм управления движением не должен определяться заранее заданным порядком переключения светофоров
  - В системе для каждого из направлений присутствуют датчики, фиксирующие наличие автомобилей.

Цель и задачи работы

- Целью данной работы является изучение механизмов верификации в среде SPIN на учебной модели «Контроллер светофоров»
- В рамках достижения заданной цели можно выделить следующие задачи:
  - Разработать описание заданной модели на языке Promela
  - Описать правила корректного функционирования системы в виде LTL формул
    - Safety
    - Liveness
    - Fairness
  - Провести верификацию для каждого правила

Вариант

- Вариант (1, 12, 15)
- Пересечения: {(NS, WN), (NE, EW),(SW,ES)}



Основная идея реализации

- Каждый контроллер светофора описывается отдельным процессом
- Сигнал светофора может быть двух видов: красный (запрещающий движение) – зеленый (разрешающий движение)
- Датчик движения определяет наличие машины перед светофором
- Появление машин (траффик) генерируется внешним, по отношению к контроллерам, процессом
- Появление машин происходит по всем направлениям независимо друг от друга (нет заранее определенной очередности возникновения машин на направлениях)

Пересечения – разделяемый ресурс

- Разделяемые ресурсы (конкурентные пересечения) описываются каналами единичной емкости и принимающие элементы типа **bool**
- Захват ресурсы означает получение из канала значения **true**
- Некоторые каналы задают не одно пересечение, а несколько
- В системе присутствуют следующие каналы:
  - **chan NS_WN_EW = [1] of {bool};**
  - **chan NS_WN_SW = [1] of {bool};**
  - **chan NE_WN_EW = [1] of {bool};**
  - **chan NE_ES = [1] of {bool};**
  - **chan ES_SW = [1] of {bool};**

Проверяемые свойства

- Безопасность
  - Никогда не будет такой ситуации, что на данном направлении будет гореть зеленый свет, и на всех, пересекающих это направление дорогах, тоже будет зеленый
  - Пример: {[] !pNS_S} при:

    pNS_S (NS@green && WN@green && SW@green && EW@green)
- Живость и справедливость
  - При наличии ожидающих автомобилей на каком-либо направлении ему обязательно представится возможность проехать (возможно, через какое-то время), при ограничении, что в каждом направлении не движется непрерывный поток автомобилей
  - Пример: **pNS_S (NS@green && WN@green && SW@green && EW@green)** при:
    - **pNS_F ((NS@green) && gen_t@NSTrue)**
    - **qNS_L (NS@green)**
    - **pNS_L (gen_t@NSTrue && (NS@red))**

Результаты и выводы

- Модель удовлетворяет всем свойствам корректности для заданных направлений
- Были исследованы возможности системы верификации SPIN
- Были изучены основы построения моделей на языке Promela и описания свойств модели с помощью LTL
- Полученные знания могут применяться при разработке систем и ПО

Спасибо за внимание