



Курсовая работа

Разработка контроллера светофоров и его верификация

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

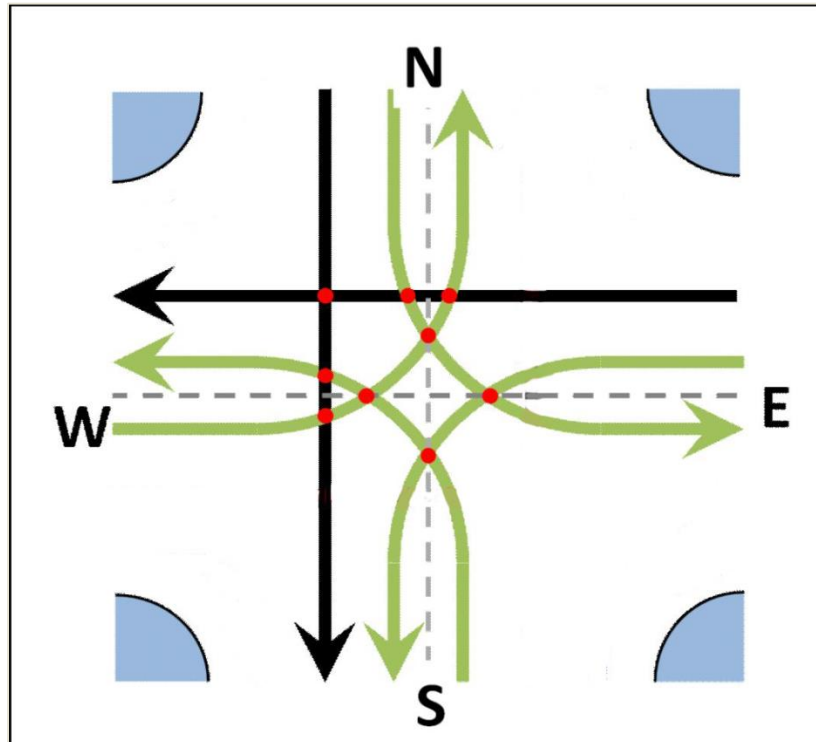
Руководитель: ст. преподаватель Шошмина И.В.

- Верификация – это проверка модели (алгоритма, системы) на корректность работы, с учетом заданных правил.
- Наблюдается устойчивая тенденция к усилению требований к корректности создаваемого ПО
- Системы для верификации ПО все чаще применяются в промышленной разработке
- В данной курсовой работе рассматривается модель управления движением на перекрестке:
 - Каждое направление контролируется своим светофором.
 - Машины появляются на всех направлениях независимо
 - Возможно одновременное движение по непересекающимся направлениям

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



Основная идея реализации

- Каждое пересечение является разделяемым ресурсом (канал единичной глубины)
- Захват (получение из канала значения true) всех необходимых пересечений гарантирует безопасный проезд
- После окончания трафика ресурс освобождается (канал заполняется значение true)
- Контроллер, диагностировавший наличие машин, ожидает освобождения требуемых пересечений
- Непересекающиеся направления не блокируются

Описание модели

- Каждый контроллер светофора является отдельным процессом
- Сигнал светофора может быть двух видов: красный – зеленый
- Состояние светофора описывается глобальными переменными
- Датчики движения также являются глобальными переменными
- Движение (трафик машин) генерируется внешним, по отношению к контроллерам, процессом. Направления выбираются случайным образом

- **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:
 - $pNS_S (NS_L == Green \ \&\& \ WN_L == Green \ \&\& \ SW_L == Green \ \&\& \ EW_L == Green)$

- **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: $\{[] \langle \rangle !pNS_F \rightarrow ([] \langle \rangle (!pNS_F) \ \&\& \ (pNS_L \rightarrow (\langle \rangle qNS_L)))\}$ при:
 - $pNS_F ((NS_L == Green) \ \&\& \ NS_S)$
 - $pNS_L (NS_S \ \&\& \ (NS_L == Red))$
 - $qNS_L (NS_L == Green)$

- 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

Список использованных материалов

- Ю.Г. Карпов, И.В. Шошмина Верификация распределенных систем – СПб.: Издательство Политехнического университета, 2011
- Thomas Wahl – Fairness and Liveness URL: <http://www.ccs.neu.edu/home/wahl/Publications/fairness.pdf>
- Concurrent programming lab2 URL: http://www2.compute.dtu.dk/courses/02158/sol_cplab2.html
- Andrew Ireland - Distributed Systems Programming (F21DS1) SPIN: Formal Analysis I URL: <http://www.macs.hw.ac.uk/~air/dsp-spin/lectures/lec-6-spin-2.pdf>
- AG-Wehrheim – Verification with SPIN URL: http://www.cs.uni-paderborn.de/fileadmin/Informatik/AG-Wehrheim/Lehre/SS09/Model_Checking/Slides/11May09.pdf

Спасибо за внимание

10

Спасибо за внимание