Especificação e Verificação de um Controlador de Semáforos

Trabalho de AMSR

FEUP/MRSC/AMSR
MPR

Problema a Resolver

» A concurso
- No *SDL '03 conference, Stuttgart, 2003*
- *SDL '03 design contest → to design a traffic light controller*
- `http://www.solinet.com/sdl_design_contest.htm`

» Mas, adaptado a AMSR ....
- Especificação em Promela
- Verificação usando o xspin
  - Software e documentação na página de AMSR

SDL '03 Design Contest

The challenge for the SDL '03 design contest is to **design a traffic light controller** with the following characteristics:

1. The traffic lights are located at a traffic intersection arranged as two roads crossing with one lane in each direction.
2. Each direction has a set of three lights with different colours: red means stop, green means go, the transitions for stop → go and go → stop are indicated by yellow. The lights at opposite sides of the intersection have the same colour.
3. Each set of three lights is a single unit with a control interface to select the colour red, yellow or green. Only one of the three lights is on at any time. (Note: The lights unit is not part of the controller.)

SDL '03 Design Contest

4. There are no lanes for turning, but turning left and right is allowed when green otherwise not (right turn on red not allowed).

5. Each lane arriving at the intersection has a single sensor, which has three states: waiting traffic, moving traffic and no traffic. Note: The sensor indicates the transition from one state to another and is not part of the controller.

6. The lights spend a maximum time in any state, i.e. traffic from the left or right will not be permanently blocked by continual traffic in the other directions.

SDL '03 Design Contest

7. If traffic is waiting in a red direction and the green direction is free of traffic, a transition will be initiated after a delay. If traffic arrives in the green direction during this time, the transition is deferred.
8. If one lane in a green direction has traffic congestion, the opposite direction has no traffic, and traffic is waiting in the red directions, then a transition will be initiated after a delay. If the congested traffic congestion in the green direction starts moving again during this time, the transition is deferred.
9. Traffic is not allowed to enter the intersection unless the exit is free. It is assumed the transition time is always greater than the time needed for traffic to cross the intersection.

Trabalho em AMSR

» Individual ou em grupo de 2 alunos

» O que deve ser feito

– Especificar o sistema em Promela

– Usando os mecanismos de verificação do XSPIN, demonstrar que:
  - o sistema é seguro (ex. há sempre uma direcção com vermelho)
  - o sistema projectado satisfaz todos os requisitos enunciados

Trabalho

» O que deve ser entregue
  – Um relatório (papel + pdf) que descreva
    - A solução proposta
    - A estratégia de verificação adoptada

  – Em anexo devem ser incluídos
    - A especificação do sistema em Promela
    - Os resultados de verificação obtidos
    - Os traços (sequências de eventos) relevantes

» Data de entrega do trabalho → 26 de Janeiro de 2002