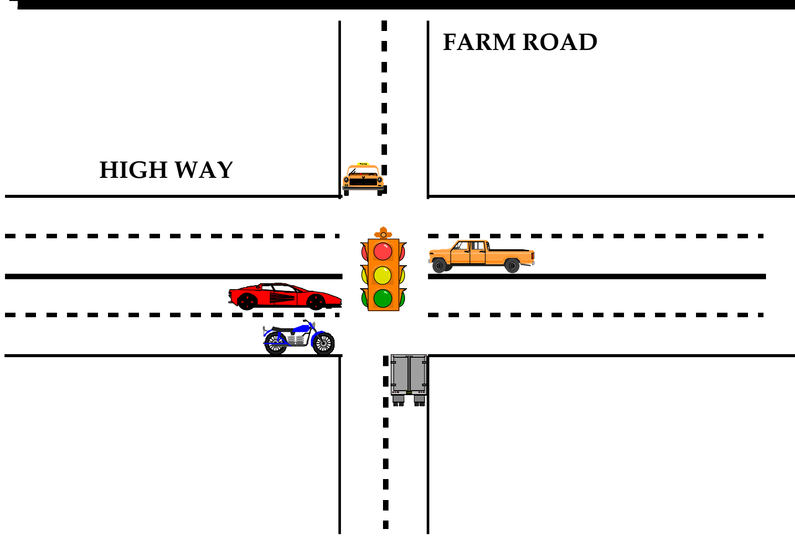
CTL Model Checking

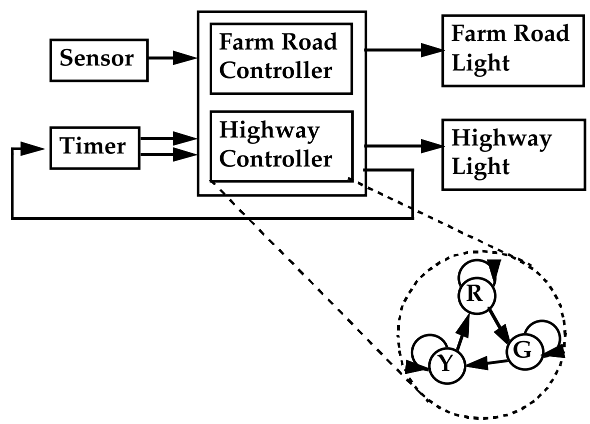
VIS - TTC

Presented by : Shaz Qadeer

Example System : Traffic Light Controller



Block Diagram of TLC



Example Properties for TLC

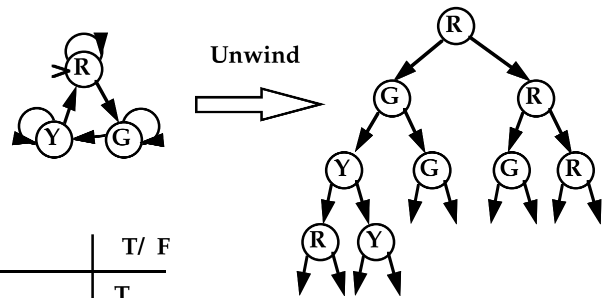
- **Invariant : It is never the case that both the highway and farm road have green simultaneously. The CTL formula saying this is**

  AG(!(hwy_light = green * farm_light = green))

- **If a car is waiting on the farm road, then eventually the farm road light turns green. The CTL formula saying this is**

  AG(car_waiting -> AF(farm_light = green))

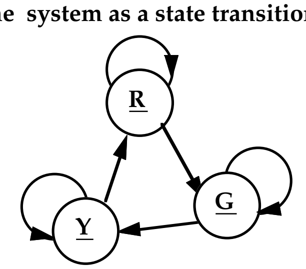
Branching View of Time



Formula	T/ F
E G (RED)	T
E (RED U GREEN)	T
AF (GREEN)	F
AGEF(GREEN)	T
A(RED U GREEN)	F

What is Model Checking?

- Represent the system as a state transition graph (the model) :



- Represent the property as a CTL formula

- Check that the model satisfies the property

Traces

- A trace is a sequence of states in the state transition graph starting from an initial state.
- A trace could be finite or infinite.
- Finite trace : red, red, green,yellow, red.
- CTL talks about infinite traces.
- Why are we concerned with infinite traces?
- Because we are concerned with eventualities - “eventually something good happens”.

CTL Formulae

- CTL = Computational Tree Logic
- Propositions refer to state variables e.g. hwy_light = red
- Propositions are the basic CTL formulae
- CTL operators: AX, AG, AU, AF, EX, EG, EU, EF
- Boolean operations: not, +, *, ->
- Any CTL operator applied to a CTL formula gives another CTL formula
- Any boolean combination of CTL formulas is a CTL formula

Examples of CTL formulae

- Propositions represented by small case alphabet e.g. p, q, r
- AGp
- E(p U q) (strong until)
- EF(p -> AGq) (same as EF(not(p) + AGq))
- AGEFp
- AG(not(AXp) + EFq)

Truth Value of CTL Formulae

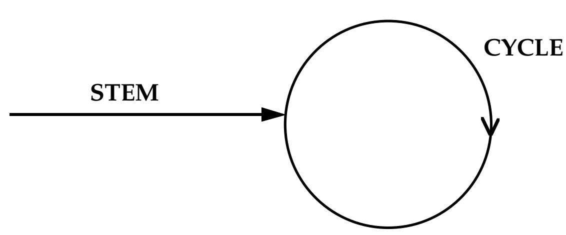
- A formula is either true or false in a state.
- A CTL formula is true for a design if it is true in all initial states of the state transition graph of the design.

Debug traces

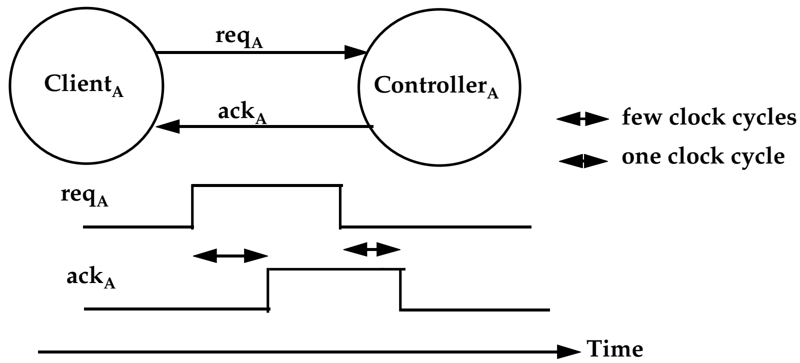
- If the property fails on the model, then the debug trace helps to figure out the problem.
- A debug trace is a witness to the negation of the CTL formula.
- Some properties have a finite debug trace; others have an infinite debug trace.
- AG(RED) has a finite debug trace : Red, Green. It is a witness to EF(not(RED)).
- AF(GREEN) has the infinite debug trace : Red, Red, Red...... It is a witness to EG(not(GREEN)).

Infinite Debug Traces

- An infinite debug trace is specified as a stem and a cycle.
- Both the stem and the cycle are finite sequences of states.



Example: Bus Arbiter



- AG(req_A -> A(req_A U ack_A))
- AG((req_A * ack_A) -> A(ack_A U not(req_A + EX(ack_A))))

CTL Model checking in VIS

- Create a description of your model in the form of a finite state machine (using Verilog).
- Prepare a list of properties you want to check.
- Translate them into CTL formulae and put them in a file.
- Use the VIS command "mc file.ctl".
- If some property fails, debug your design with the help of the error trace.
- At the end, you should feel more confident about your design.
- Onus on the designer to come up with a set of suitable properties.