ECEN689-602/CSCE689-603 Introduction to Formal Verification Fall 2021

Project Report Phase C

Submitted to the Faculty

Of

Texas A&M University

By

Team 6 I-Group Integration

Brent Arnold Basiano UIN: 130004869

Sri Hari Pada Kodi UIN: 932003040

Under the Guidance of

Professor Jiang Hu

Department of Electrical and Computer Engineering

November 2021

TABLE OF CONTENTS

LIST OF FIGURES

ECEN 689 - Introduction to Formal Verification

Phase C

Team 6 - I-Group

ABSTRACT:

Phase C is about verifying the properties of road grid with traffic system that we have designed in the Phase A. Here we have to verify the properties using the NuSMv model checker tool which the V-Group found out over the Phase B. Here the I-group is responsible for verifying the vehicle properties. There are in total 5 properties out of which 4 are pre-defined and 1 property is of our choice.

The properties that we, the I-group have to verify are as follows:

1. No vehicle takes any U-turn.
2. No vehicle enters an intersection at red light.
3. Every vehicle must visit all of points B, C and D.
4. There is no collision between any two vehicles.
5. Another property at your own choice.

BACKGROUND:

The project is to design a road system and verify its properties. All cars start in a common point in the road called point A which moves to other points labeled B, C, and D. The car must go to all the points in any order but must return to point A. For this project, two groups in a team deal with the road (I-Group) and vehicles (V-Group) separately. The project is also broken down to three phases. This report focuses on Phases C.

For phase C, the I-Group focused on verification of the vehicle properties using NuSMv model checking tool. We have applied the concept of modeling a concurrent system for the road grid with traffic system and obtained a transition system to verify the properties such as safety, mutual exclusion, liveliness et cetera that are defined above as vehicle properties. We have considered V-group system in the Phase A and thus verifying the vehicle properties.

PROCEDURES :

The system is a 3*3 road grid with traffic signal, with 4-two way intersections, 4-three way intersections, and 1-four way intersection. On a whole, a vehicle starts from the point labeled A and travels through the points B, C, and D and then returns to A in any order. Here we are considering the paths defined by V-group in the phase A to verify the vehicle group properties. There are total 30 slots between each segment, here segment means the path between 2 nodes (nodes are represented by circles in the figure 1).

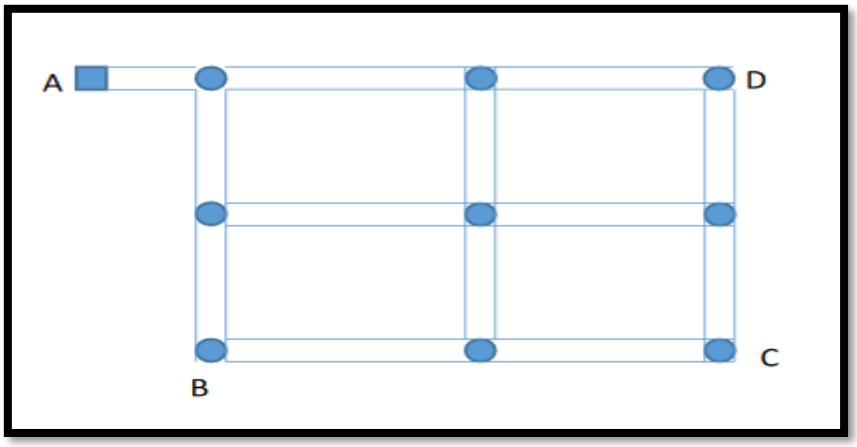

Figure 1. Road System

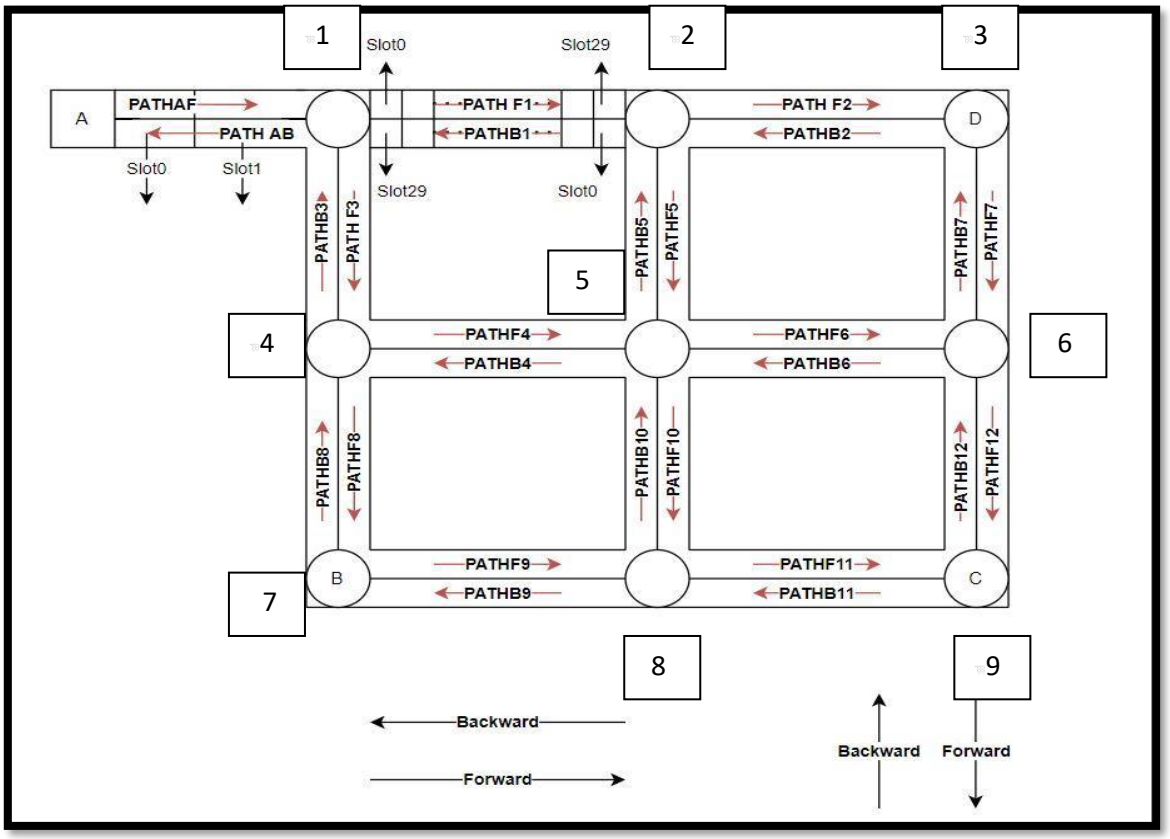

Figure 2: Directed Graph of the Road System

The vehicle movement in the grid showed in Figure 1 is implemented by the concept of directed graph with constraints such as PATH F1 (Forward path), PATH B1 (Backward path), slots (0 to 29) et cetera (refer to figure 2).

PROPERTY VERIFICATION:

1. NO VEHCILE TAKES ANY U-TURN:

A vehicle at any instant of time and position should not take a u-turn in the 3*3 road grid with traffic signal system.

Contextual explanation: Consider a vehicle is travelling in forward (ex: PATH F1) direction at any instant of time, either the vehicle should be moving in the same direction or it should stay in slot (i.e., should not move). It should not shift its direction and go in the reverse path (ex: PATH B1). This scenario can be better understood by a simple animated figure shown below.

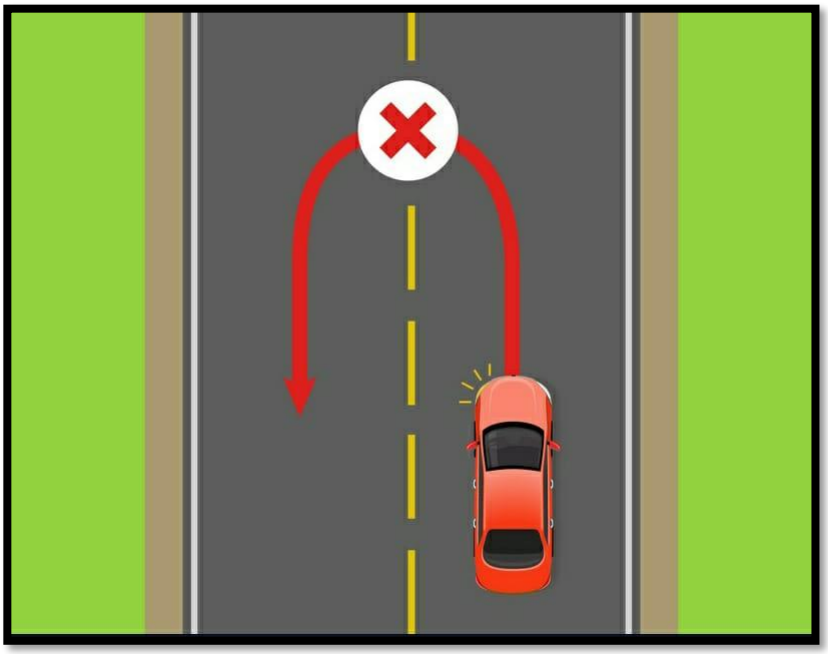

Figure 3: Animation showing there should be no u-turn

- Here the property of vehicle taking a u-turn is considered as something bad that should never happen for this system, hence this signifies the "**Safety**" property for the vehicle.

A simple state system explaining the property of **u-turn** not happening, that we are supposed to verify is as follows:

- Here we are considering the slots as transitions for better understanding.

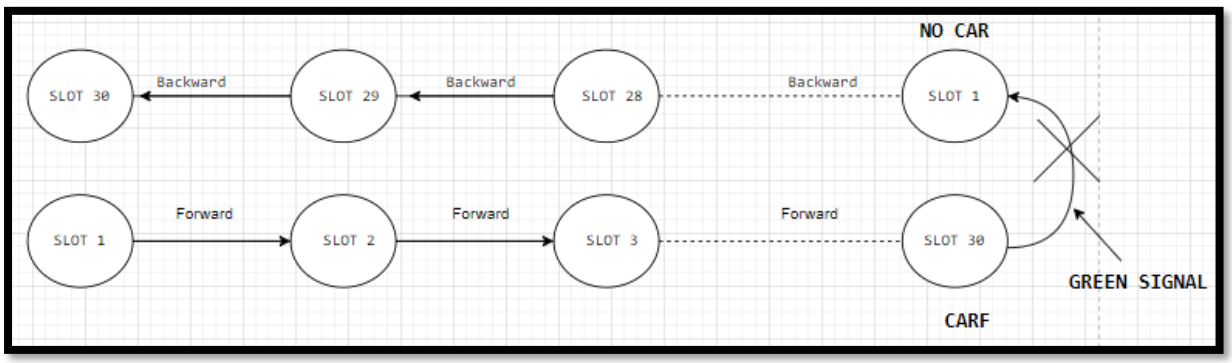

Figure 4: state system representation for property u-turn

Verification of state system explanation (theoretical):

Consider the segment between point 1 and 2 (from the Figure 2), here the vehicle is moving from slot 0 to slot 29. There are 2 possibilities for the u-turn to happen

a. One among them is, at the 29th slot (represented by SLOT 30 in Figure 4) if the signal is green and there is a vehicle at the first slot (**represented by SLOT 1 in Figure 4**) of backward path. There should be no u-turn, otherwise the collision takes place in the next state. This scenario of collision is covered in the 4th property.
b. The second scenario is, when the car in forward path is at the location of 29th slot (represented by SLOT 3 in Figure 4), the signal is green and there is no car in the first slot (represented by SLOT 4 in Figure 4) of the backward path. There should be no u-turn.

Verification of state system explanation (practical) using NUSMV model checking tool:

Using NUSMV we modeled the 3*3 road grid with traffic signal. For checking the **no vehicle turns u-turn** property here we are considering the instance from the above theoretical explanation i.e. segment between point 1 and 2 (from the Figure 2).

Using the **Linear Temporal Logic** concept we verified for the **Global** specification using the below condition. In the figure 5, **check_ltlspec** refers to checking Linear Temporal Logic, G refers to Global condition i.e., satisfies for each and every transition of the system. **F1** – Forward path, **B1** – Backward path, **L1** – traffic signal, **carF** – car in forward path, **no_car** – no car present in the slot.

```
NuSMV > go
NuSMV > check_ltlspec
-- specification  G (((F1 = carF & L1 = green) & B1 = no_car) -> !(B1 = carF))  is true
```

Figure 5: Output in NuSMV showing LTL spec verification for "G" is true for no u-turn

NuSMV model checking tool output explanation:

Here the output signifies that, for each and every transition when a car is moving in F1 direction and has green light i.e. L1 at the junction, and with empty slot at B1 direction. The next state of the car will never be B1 i.e. the car never takes a u-turn (i.e.! (B1 = carF)).

Symbols meanings:

a) **&** means **and**
b) **->** means **next state**
c) **!** means **negate** or **not**
d) **G** means **Global**

- Therefore the requirement of **no vehicle takes any u-turn** is satisfied globally (G) using the linear temporal logic (check_ltlspec) for the 3*3 road grid with traffic signal.

2. NO VEHICLE ENTERS AN INTERSECTION AT RED LIGHT.

A vehicle at any intersection in the 3*3 road grid with traffic signal system should not violate the red light.

Contextual explanation: Consider there are 4 vehicles at the 29^{th} slot of each segment at an intersection from all the directions. In this scenario only one vehicle should be allowed to move, rest all vehicles should not move i.e. at most 1 signal should be green at any intersection. This scenario is valid only when the vehicle which is having a red light in its path should not move.

Below is an animated figure of a 4-way intersection describing the situation of above scenario.

Figure 6: A 4-way intersection for visual understanding

- This situation is exhibiting "**safety**" property for vehicle which at any point of time in the 3*3 road grid with traffic signal does not break the red signal.

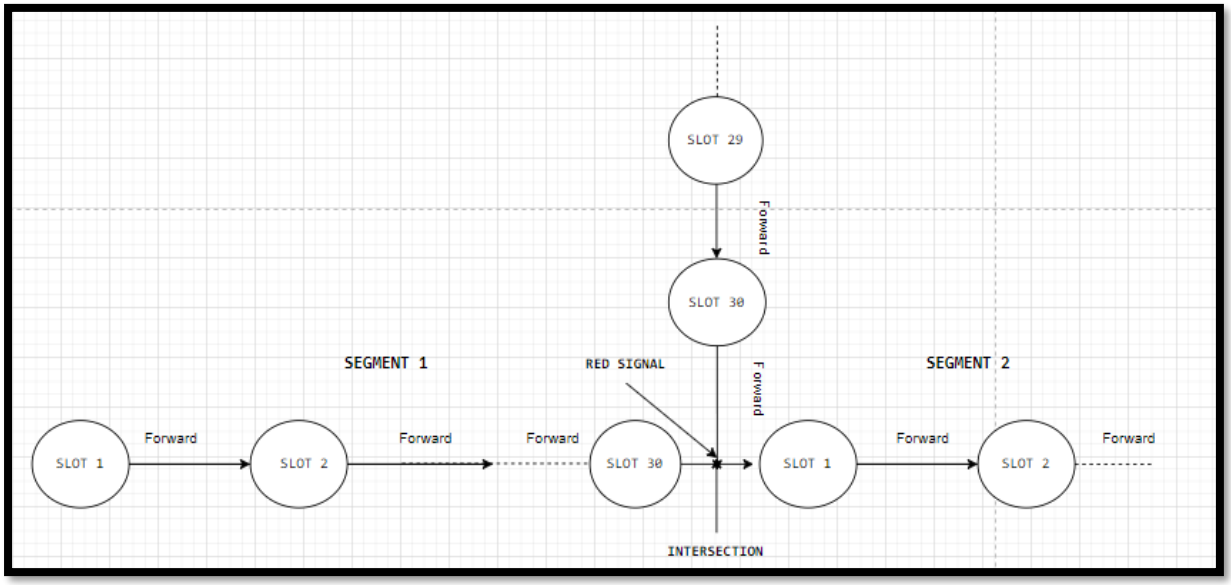

Figure 7: state system representation for property no vehicle at intersection while red light

Verification of state system explanation (theoretical):

Here let us consider a vehicle is at a 2-way intersection, the condition which is followed to satisfy our property is 'at most only 1 signal at an intersection is green'. Therefore when a car has red signal in its direction, it should stop even when there is no vehicle in the next slot or state. Refer to the above figure (Figure 7) for better understanding.

Verification of state system explanation (practical) using NUSMV model checking tool:

Using NUSMV we modeled the 3*3 road grid with traffic signal. For checking the **no vehicle entering an intersection at red signal property**, here we are considering the instance from the

above theoretical explanation i.e. vehicle traveling from SEGMENT 1 to SEGMENT 2 at a 2-way intersection (from the Figure 7). To verify the result we are also showing the signal property at the 2-way intersection for better understanding.

Using the **Linear Temporal Logic** concept we verified for the **Global** specification using the below condition. In the figure 8 & 9, **check_ltlspec** refers to checking Linear Temporal Logic, G refers to Global condition i.e., satisfies for each and every transition of the system.

Here the below output of NuSMV model checking tool shows that both the signals cannot be red at the same time. This means the property of "at most 1 signal green is obeyed here".

```
NuSMV > check_ltlspec -p "G (!(L1 = green) | !(L2 = green))
ignoring unbalanced quote ...
-- specification  G (!(L1 = green) | !(L2 = green))  is true
NuSMV >
```

Figure 8: Output in NuSMV showing LTL spec verification for "G" is true for signals at 2-way intersection

Now since the signal property stands true, we are verifying the property of **No vehicle enters an intersection at red light.**

```
NuSMV > go
NuSMV > check_ltlspec
-- specification  G (((F1 = carF & L1 = red) & (F2 = carF | F2 = no car)) -> !(F1 = no car))  is true
```

Figure 9: Output in NuSMV showing LTL spec verification for "G" is true for vehicle enters an intersection at red light

NuSMV model checking tool output explanation:

Here the output signifies that, for each and every transition when a vehicle **carF** is at the **29th** slot of the **first segment F1** and the **signal L1** is **red** and at the **second segment**, whether the slot 1 **F2** is having a **car** or **no car**, the vehicle **carF** will not go the slot 1 or next state (i.e. F1 = car means car is present at F1).

Symbols meanings:

a) **&** means **and**
b) **->** means **next state**
c) **!** means **negate** or **not**
d) **G** means **Global**

carF -> car moving in forward path

no car -> no car is present at a slot

F1 -> forward path for segment 1

F2 -> forward path for segment 2

- Therefore the requirement of **No vehicle enters an intersection at red light** is satisfied globally (G) using the linear temporal logic (check_ltlspec) for the 3*3 road grid with traffic signal.

3. **EVERY VEHICLE MUST VISIT ALL OF POINTS B, C and D.**

Any vehicle entering into the 3*3 road grid with traffic signal system should travel covering the points B, C and D.

Contextual explanation: In the phase A of the project, the vehicle group defined 5 paths for a vehicle to travel covering all the points B, C and D. For simplicity we are verifying the system for those properties using the NuSMv model checking tool. Here consider a vehicle is at point 4 (refer to the numbering in the Figure 10) it should cover point B (point 7 in Figure 10), point 9, point C (point 9 in Figure 10), point 6, point D (point 3 in the Figure 10) to verify the property.

Here the vehicle should cover 5 traffic signals and 5 segments at least to cover the points B, C and D and come out. Here we are verifying the system for 2 cases i.e. B->C->D and D->B->C.

- Here the vehicle is travelling across all the 3 points B, C and D. Similarly for D, C and B. Hence the vehicle is satisfying the "**Liveness**" property for the 3*3 road grid with traffic signal system.

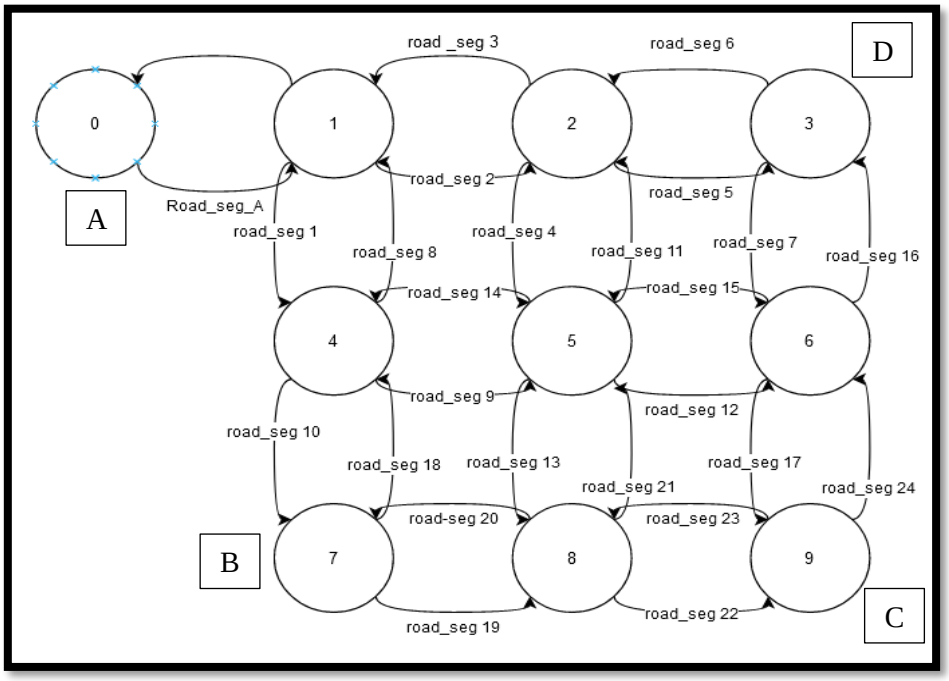

Figure 10: Directed graph of road system with points B, C and D

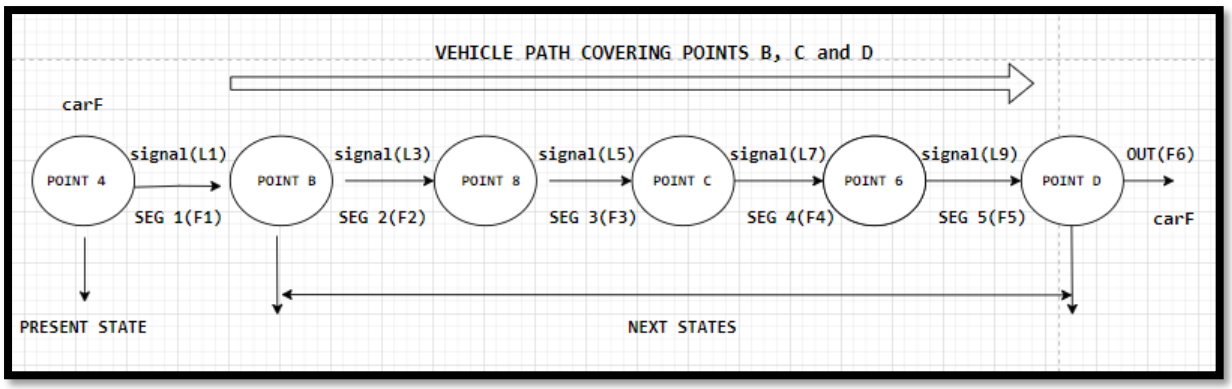

Figure 11: state system for vehicle covering the points B, C and D

Verification of state system explanation (theoretical):

Here let us consider a vehicle is at point 4 in Figure 11 (for clear understanding follow the Figure 10: Directed graph). So, the vehicle should cover point B, point 8, point C, point 6, point D (next states). Condition followed by the vehicle here is the signals in the path should be green at the intersections. The vehicle here goes through 5 segments to cover the points B, C and D (segments are listed in Figure 11). The vehicle follows the same process for the path covering D, C and B points respectively.

Verification of state system explanation (practical) using NUSMV model checking tool:

Using NUSMV we modeled the 3*3 road grid with traffic signal. For checking the **every vehicle must visit all of points B, C and D** property, here we are considering the instance from the above theoretical explanation i.e. vehicle traveling from SEGMENT 1 to SEGMENT 5 and coming out covering B, C and D points.

Using the **Linear Temporal Logic** concept we verified for the **Global** specification using the below condition. In the figure 12, **check_ltlspec** refers to checking Linear Temporal Logic, G refers to Global condition i.e., satisfies for each and every transition of the system.

```
NuSMV > go
NuSMV > check_ltlspec
-- specification  G ((((((L1 = green & L3 = green) & L5 = green) & L7 = green) & L9 = green) & (((((F1 = carF -> F1 = no_car) & (F2 = carF -> F2 = no_car)) & (F3 = carF
 -> F3 = no_car)) & (F4 = carF -> F4 = no_car)) & (F5 = carF -> F5 = no_car))) ->  F F6 = carF)  is true
-- specification  G ((((((L2 = green & L4 = green) & L6 = green) & L8 = green) & L10 = green) & (((((B6 = carB -> B6 = no_car) & (B5 = carB -> B5 = no_car)) & (B4 = car
B -> B4 = no_car)) & (B3 = carB -> B3 = no_car)) & (B2 = carB -> B2 = no_car))) ->  F B1 = carB)  is true
NuSMV >
```

Figure 12: Output in NuSMV showing LTL spec verification for "G" is true for vehicle covering paths in order BCD and DCB

NuSMV model checking tool output explanation:

Case 1 (B->C->D) explanation from NuSMV model checker output: Here the output signifies that, for each and every transition when vehicle is at point 4 from figure 10, then for next state **F1 = carF** (car is at point B from figure 10) and **L1 = green** as signal for corresponding 2-way intersection. Next state is the next segment **F2 = carF** (car is at point 8 from figure 10) and **L3 = green** as signal for corresponding 3-way intersection, next state is the next segment **F3 = carF** (car is at point C from figure 10) and **L5 = green** as signal for corresponding 2-way intersection, next state is the next segment **F4 = carF** (car is at point 6 from figure 10) and **L7 = green** as signal for corresponding 3-way intersection, next state is the next segment **F5 = carF** (car is at point D from figure 10) and **L9 = green** as signal for corresponding 2-way intersection. Thus covering all the carF will be at **F6** (F **F6 = carF** means Final state of system at which vehicle is present).

Case 2 (D->C->B) explanation from NuSMV model checker output: Here the output signifies that, for each and every transition when vehicle is at point 2 from figure 10, then for next state **B6 = carB** (car is at point D from figure 10) and **L2 = green** as signal for corresponding 2-way intersection. Next state is the next segment **B5 = carB** (car is at point 6 from figure 10) and **L4 = green** as signal for corresponding 3-way intersection, next state is the next segment **B4 = carB** (car is at point C from figure 10) and **L6 = green** as signal for corresponding 2-way intersection, next state is the next segment **B3 = carB** (car is at point 8 from figure 10) and **L8 = green** as signal for corresponding 3-way intersection, next state is the next segment **B2 = carB** (car is at point B from figure 10) and **L10 = green** as signal for corresponding 2-way intersection. Thus covering all the carF will be at **B1** (F **B1 = carB** means Final state of system at which vehicle is present).

Symbols meanings:

a) **&** means **and**
b) **->** means **next state**
c) **!** means **negate** or **not**
d) **G** means **Global**

carF -> car moving in forward path; carB -> car moving in backward path; no car -> no car is present at a slot; L1, L2,…L10 -> signals; F1……F6 & B1……B6 -> paths forward & backward.

- Therefore the requirement of **every vehicle must visit all of points B, C and D** is satisfied globally (G) using the linear temporal logic (check_ltlspec) for the 3*3 road grid with traffic signal.

4. **THERE IS NO COLLISION BETWEEN ANY 2 VEHICLES.**

At any point of time in 3*3 road grid with traffic signal system, there should never be collision between any 2 vehicles.

Contextual explanation:

In the phase A of the project, the vehicle group defined 30 vehicles for the entire 3*3 road grid with traffic signal system. We are considering all the 30 vehicles to verify the property of "**no collision between any 2 vehicles**". For that, we are here considering a segment in the road system and inserting 30 vehicles into that path. Here we are verifying the property for the segment present between point 1 and 2 (refer to Figure 10) for proper visualization. Below is an animated figure of a vehicle collision describing the situation of above scenario.

Figure 13: Collision of 2 vehicles

- Here the property of vehicles having any collision is considered as something bad that should never happen for this system, hence this signifies the "**Safety**" property for the vehicle.

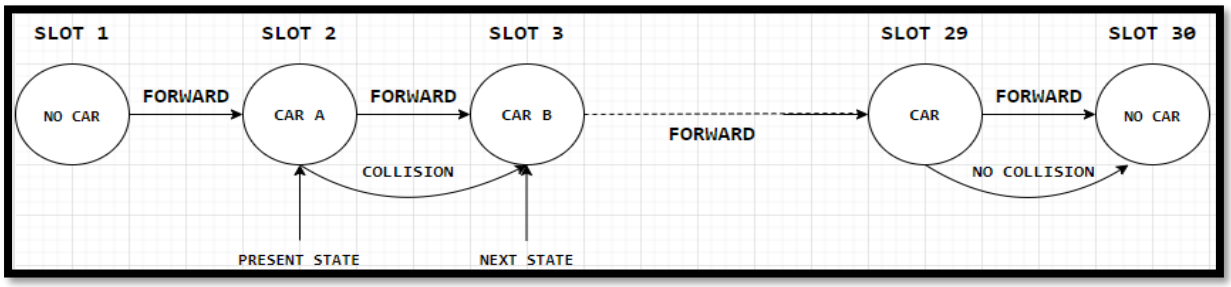

Figure 14: state system for collision of 2 vehicles

Verification of state system explanation (theoretical):

Here we are considering a road segment between points 1 and 2 (refer to the figure 10), there are total 30 slots with vehicles assigned randomly in those slots (refer to figure 14). Now consider a slot where there is a vehicle as a present state, the condition that the system should follow is, check if there is vehicle in the next slot or not, if there is no vehicle then the present state vehicle will move to the next slot or state, else if there is vehicle in the next slot (carB) then the present state vehicle (carA) should not go to next state.

Verification of state system explanation (practical) using NUSMV model checking tool:

Using NUSMV we modeled the 3*3 road grid with traffic signal. For checking the collision between any two vehicles, here we are assigning the slots with Boolean values i.e. if car is present means slot value is 1 (carA or carB) else the value of vehicle is 0.

Using the **Linear Temporal Logic** concept we verified for the **Global** specification using the below condition. In the **figure 15, check_ltlspec** refers to checking Linear Temporal Logic, **G** refers to Global condition i.e., satisfies for each and every transition of the system.

```
NuSMV > go
NuSMV > check_ltlspec
-- specification  G carA != carB  is true
-- specification  G carA = carB  is false
-- as demonstrated by the following execution sequence
Trace Description: LTL Counterexample
Trace Type: Counterexample
  -> State: 1.1 <-
    carA = 15
    carB = -1
  -> State: 1.2 <-
    carA = 16
    carB = 0
  -> State: 1.3 <-
    carA = 17
    carB = 1
  -> State: 1.4 <-
    carA = 18
    carB = 2
```

Figure 15: Output in NuSMV showing LTL spec verification for "G" for both cases of collision and no collision

NuSMV model checking tool output explanation:

Here the carA and carB are present slot vehicle and vehicle in the next slot respectively. For the property to satisfy the value of carA and carB should never be same since both carA and

carB are assigned with the same Boolean value of 1. And value 1 refers to the slot with a vehicle, so if both are having vehicles at their slots respectively then there should be no movement in the vehicle i.e., carA and carB should not be equal i.e. **carA != carB** (**refer to figure 15**) is **True** for the 3*3 road grid with traffic signal system. When both are equal i.e. **carA = carB** there occurs collision which is showed in the counter example (**refer to figure 15**) as a **False** condition.

Symbols meanings:

a) **&** means **and**
b) = checking for the condition whether they are equal
c) **!** means **negate** or **not**
d) **G** means **Global**
e) **carA is vehicle in present slot (or state)**
f) **carB is vehicle in next slot (or state)**

- Therefore the requirement of "**no collision between any 2 vehicles**" is satisfied globally (G) using the linear temporal logic (check_ltlspec) for the 3*3 road grid with traffic signal.

5. **ANOTHER PROPERTY AT YOUR OWN CHOICE (AT MOST ONE VEHICLE INSERTION AT POINT A).**

At any point of time in 3*3 road grid with traffic signal system, there can enter **at most one vehicle at a time from the point A.** N number of vehicles can enter the road system but in a sequential manner and not parallel.

Contextual explanation:

The last property which we are going to verify is, in a 3*3 road grid with traffic signal system at most 1 vehicle can enter at a time. The distance between points 0 and 1 has only 2 paths one for vehicle moving from 0-1 (forward path) and other for the vehicle moving 1-0 (backward path). Below is the animated image showing the cars in a queue for both entering and leaving grid. Here the property that we are focused is only, **there can enter at most one vehicle at a time from the point A.** Below is a animated image of the vehicles going to and fro into the point A for proper visualization.

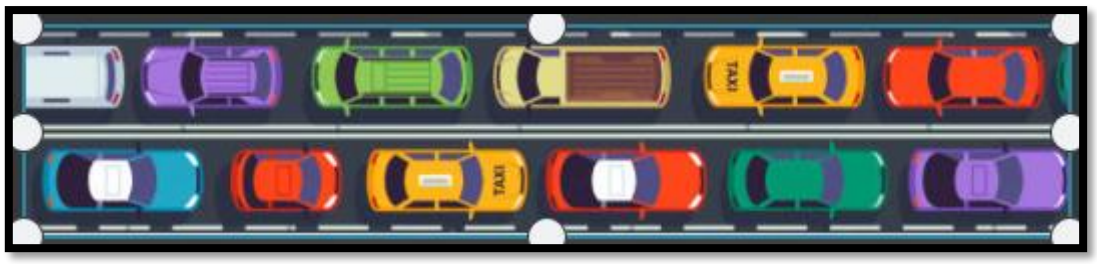

Figure 16: Vehicles entering (forward path) and leaving (backward path) at point A (refer to Figure 10 directed graph)

- Here the property of vehicles entering first slot of road segment 0 at point A (refer to the figure 10) is at most one i.e. at any instant of time no two vehicles can stay in a single slot 1 if that happens it is exhibiting bad behavior, hence this signifies the **"Safety"** property for the vehicle.

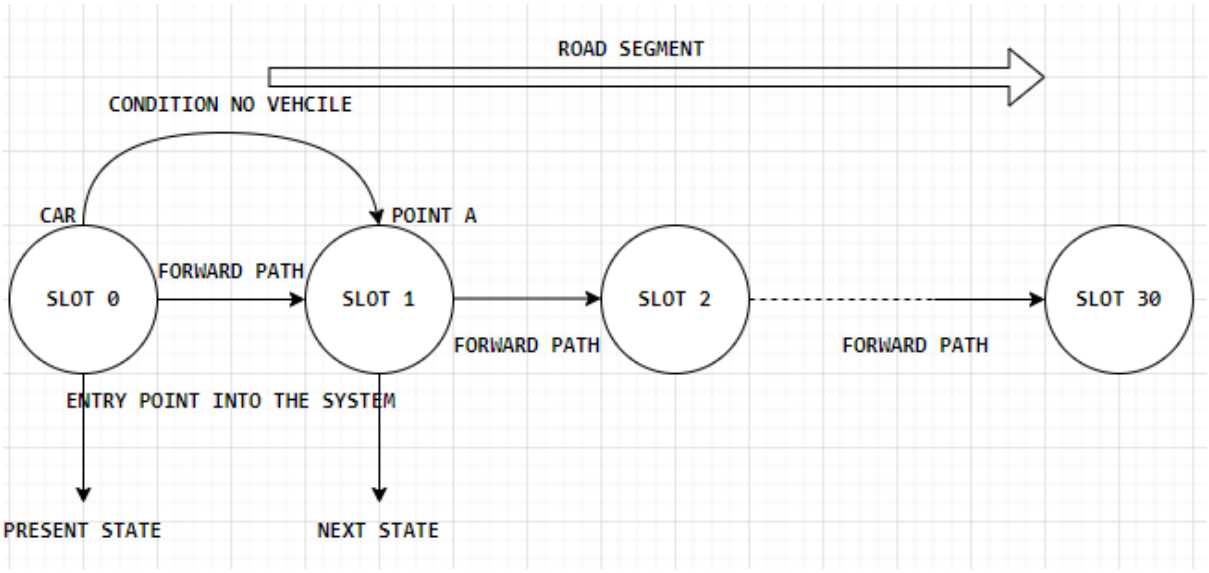

Figure 17: state system for vehicle insertion into the point A

Verification of state system explanation (theoretical):

Here we are considering a road segment between points 0 and 1 (refer to the figure 10), there are total 30 slots within the segment from point A to point 1. Here a vehicle at slot 0 i.e. slot before entering the 3*3 road grid with traffic signal, it should check if there is vehicle in the next segment. If there is no vehicle then the car can enter into slot 1 of road segment and continue to move in forward path else if vehicle is present at slot 1 then the vehicle at slot 0 before road segment should not move.

Verification of state system explanation (practical) using NUSMV model checking tool:

Using NUSMV we modeled the 3*3 road grid with traffic signal. For checking the vehicle insertion property we are considering

here a total number of 200 cars, the condition for vehicle getting inserted into the road segment is no vehicle should be present at the slot 1 of the road system at point A. We are assigning a counter for number of cars entering and showing the result.

Using the **Linear Temporal Logic** concept we verified for the **Global** specification using the below condition. In the **figure 18, check_ltlspec** refers to checking Linear Temporal Logic, **G** refers to **Global condition** i.e., satisfies for each and every transition of the system.

```
NuSMV > go
NuSMV > check_ltlspec
-- specification  G !(pointA_state >= 2)  is true
```

```
-> State: 1.2 <-
  pointA_state = 1
  car_count = 199
-> State: 1.3 <-
  pointA_state = 0
  car_count = 199
-> State: 1.4 <-
  pointA_state = 1
  car_count = 198
-> State: 1.5 <-
  pointA_state = 0
  car_count = 198
```

Figure 18: Output in NuSMV showing LTL spec verification for "G" for insertion of vehicle at point A of the road system

```
NuSMV > go
NuSMV > check_ltlspec
-- specification  G pointA_state >= 2  is false
-- as demonstrated by the following execution sequence
Trace Description: LTL Counterexample
Trace Type: Counterexample
  -> State: 1.1 <-
    pointA_state = 0
    car_count = 200
  -> State: 1.2 <-
    pointA_state = 1
    car_count = 199
  -> State: 1.3 <-
    pointA_state = 0
  -> State: 1.4 <-
    pointA_state = 1
    car_count = 198
```

Figure 19: Output in NuSMV showing LTL spec verification for "G" for insertion of vehicle at point A of the road system (counter example)

NuSMV model checking tool output explanation:

Here both the **figures 18** and **19** are showing the output for the **insertion of vehicles** at **pointA** with **example** and a **counter example.** As discussed above here we are considering **200 vehicles** and entering them sequentially at pointA whilst verifying the condition whether a vehicle is present at the slot or next state of the road segment. Here the output (**for figure 18**) says that !**(pointA_state >=2)** is **true** means **number of vehicles at pointA_state is always less than 2 and the car_count decrement is by 1 vehicle for each state.** And for counter example part the output (**for figure 19**) says that **pointA_state >=2** is **false** and all the states and **car_count** is represented respectively.

Symbols meanings:

a) = checking for the condition whether they are equal
b) **!** means **negate** or **not**
c) **G** means **Global**
d) **pointA_state means state of the first slot of segment 1**
e) **car_count** means the counter assigned to **number of vehicles.**

- Therefore the requirement of "**at most one vehicle insertion at point A**" is satisfied globally (G) using the linear temporal logic (check_ltlspec) for the 3*3 road grid with traffic signal.

CONCLUSION:

For phase C, all the properties defined for the I-group is verified and corresponding results are displayed in the above section for the 3*3 road grid with traffic signal. Here are the properties are verified using the NuSMV model checking tool. The conditions that we verified for the above properties satisfies globally (G) using the Linear Temporal Logic (check_ltspec). Here all the vehicle properties defined and verified are for the system designed by I-group and V-group on a whole considering both the phase A and phase B of the project.