Validation of Automation Systems using Temporal Logic Model Checking and Groebner Bases

Quoc-Nam Tran¹, Anjib Mulepati
Lamar University, U.S.A.

Abstract—Validation of an automation system is an important issue. The goal is to check if the system under investigation, modeled by a Petri net, never enters the undesired states. Usually, tools dedicated to Petri nets such as DESIGN/CPN are used to make reachability analysis. The biggest problem with this approach is that it is impossible to generate the full occurrence graph of the system because it is too large. In this paper, we show how computational methods such as temporal logic model checking and Groebner bases can be used to verify the correctness of the design of an automation system. We report our experimental results with two automation systems: the Automated Guided Vehicle (AGV) system and the traffic light system. Validation of these two systems ranged from 10 to 30 seconds on a PC depending on the optimizing parameters.

Keywords—Computational Intelligence, Temporal Logic Reasoning, Model Checking, Groebner Bases.

I. INTRODUCTION

VERIFYING the correctness of a design for an automation system is an important issue. The goal is to check if the system never enters the undesired states, i.e. the situations that should never happen. Usually, the system under investigation is modeled by means of a Petri net and tools dedicated to Petri nets such as DESIGN/CPN are used to make reachability analysis [27, 35]. The biggest problem with this approach is that it is impossible to generate the full occurrence graph of the system because it is too large.

In this paper, we show how computational methods such as temporal logic model checking and Groebner bases can be used to verify the correctness of the design of an automation system.

Temporal logic model checking is one of the formal verification techniques which can be used to verify the correctness of a finite state concurrent system. Model checking [1, 2, 9, 31] with temporal logic [36] and automata-theoretic techniques [28, 29, 30, 45, 46, 47, 48, 49] have the ability to discover subtle flaws resulting from improbable events. Model checking has several attractive features. Once the Kripke model of the system and the temporal logic specifications have been defined, the process is fully automated. If a computation that violates the specification is found in the Kripke model, it can be displayed to the designer to aid the debugging process. In addition, the model checker can formally verify if the specification holds [28, 32, 33]. Popularity of model checking has been increased due to being a fast and automatic method. Unlike other techniques, model checking can produce a counter example when there is fault in the system design. This automatic generation of counter examples can be used to pinpoint the bug in the design. In the paper we also show how the behavior of a system can be expressed in terms of algebraic equations and use Groebner bases to validate the system design.

We report our results with validating the correctness of two different systems: the Automated Guided Vehicle (AGV) system and the traffic light system using SMV model checker and reachability analysis on the Petri net using Groebner basis.

The paper is organized as follows. Section 2 present the formal logic, the model checking and Groebner basis verification methodology. Section 3 and 4 describe the AGV and traffic light verification problem respectively.

A. Temporal Logics

The first step in formal verification is the representation of formal specification of the design consisting of a description of the desired behavior. As sequential systems capture time-variant behavior, it is not possible to describe their properties completely in the framework of conventional propositional formulas. In a temporal logic, temporal operators are additionally provided, which can be used to express time-variant dependencies. A widely used specification language for designs is Temporal Logic [36], which is a modal logic (i.e. logic to reason about many possible worlds with their semantics based on Kripke structures).

In linear temporal logic (LTL), time is treated as if each moment has a unique possible future. (An alternative approach is to use branching time (CTL) [10].) Linear temporal formulas are constructed from a set $\varphi$ of atomic propositions using
usual Boolean connectives as well as temporal connectives \(X\) ("next"); \(G\) ("always"); \(F\) ("eventually"); and \(U\) ("until").

The semantics of LTL formulas are based on an appropriate Kripke structure of the form \(K = (\mathbb{N}, \leq, \pi)\), where \(\mathbb{N}\) is the set of natural numbers, \(\leq \subseteq \mathbb{N}^2\) is the standard linear order, and \(\pi : \mathbb{N} \rightarrow 2^\mathbb{N}\) is a function that defines what propositions are true at a certain time instant.

An LTL formula is interpreted over computations viewed as infinite sequences of truth assignments to the atomic propositions in \(\Sigma^\omega\) where \(\Sigma = 2^\mathbb{N}\) as follows:

1) \(\pi, i \models \varphi\) means that formula \(\varphi\) holds at the time \(i\) of the computation \(\pi\).
2) \(\pi, i \models p\) iff \(p \in \pi(i)\).
3) \(\pi, i \models X\varphi\) iff \(\pi, i+1 \models \varphi\).
4) \(\pi, i \models G\varphi\) iff \(\pi, j \models \varphi\) for all \(j \geq i\).
5) \(\pi, i \models F\varphi\) iff \(\exists j \geq i\) such that \(\pi, j \models \varphi\) and \(\pi, k \not\models \varphi\) for all \(k > j\).
6) \(\pi, i \models \varphi \lor \psi\) iff \(\exists j \geq i\) such that \(\pi, j \models \varphi\) or \(\pi, j \models \psi\).

Notice that operators \(G\) and \(F\) can be derived from \(X\) and \(U\) as \(F\varphi = \text{true} \lor U(\varphi \land \neg \varphi)\) and \(G\varphi = \neg F \lor \varphi\).

In LTL model checking, we assume that the specification is given in terms of properties expressed by LTL formulas. For example the formula \(G(request \rightarrow F\text{grant})\), which refers to the atomic propositions \(request\) and \(grant\), specifies that every state in the computation in which \(request\) holds is followed by some state in the future in which \(grant\) holds.

### B. Validity in Model Checking

Using temporal logic as a specification language for systems quite naturally leads to the idea of model checking. In fact, model checking has become one of the most actively studied automated formal verification techniques [9, 10, 37]. In model checking, an LTL specification is checked against a Kripke model of the finite state system (i.e. the implementation). Validity and satisfiability are defined as follows:

- \(\pi\) satisfies a formula \(\varphi\), denoted by \(\pi \models \varphi\), iff \(\pi, 0 \models \varphi\).
- \(\text{models}(\varphi) = \{\pi \in (2^\mathbb{N})^\omega : \pi \models \varphi\}\).
- \(\varphi\) is satisfiable iff \(\text{models}(\varphi) \neq \emptyset\) (non-emptiness).
- \(\varphi\) is valid iff \(\text{models}(\varphi) = (2^\mathbb{N})^\omega\) (universality).

### C. Model Checking

In model checking, the specification is expressed in temporal logic and the system is modeled as a finite state machine. For realistic designs, the number of states of the system can be very large, \(10^{30}\) or higher, and hence explicit traversal of the state space becomes infeasible. Perhaps the biggest hurdle for the practical use of model checking is the state explosion problem [44]. To relieve the state explosion problem, many approaches have been proposed.

Symbolic model checking using ordered binary decision diagrams (BDD) is a successful and widely used technique for verifying properties of concurrent hardware and software systems. In symbolic model checking, the state space is represented implicitly using symbolic means, and the propositional logic formulas are manipulated using BDDs [23]. Symbolic model checking succeeded in checking systems with unprecedented large state spaces.

Bounded model checking uses the same basic idea as symbolic model checking using BDD in that the state space of the system is represented implicitly by Boolean formulas. However, instead of manipulating the Boolean formulas using BDDs, the bounded model checker transforms the model and property specifications into a propositional satisfiability (SAT) problem. Given a system \(M\), a temporal logic formula \(\psi\) and a bound \(k\), a Boolean formula is constructed, which is satisfiable if and only if \(M\) has a counterexample of length \(k\) to \(\psi\). A SAT solver such as SATO or zChaff is used to perform the query. In BMC, the growth of the size of the Boolean formulas can be known in advanced, but predicting the running times of the SAT solver is difficult. BMC is particularly good at finding shallow counterexamples, and some industrial applications have been successful of BMC [3, 4, 13].

Other approaches to relieve the state explosion problem include the partial order methods [17, 26, 43, 50]; complete finite prefixes [21, 31]; compositional methods [12, 19, 25]; symmetry reduction [16, 20, 22, 24, 38]; and abstraction [11, 14, 15, 18].

Petri nets (PN) provide a graphical and mathematical representation of many systems [34]. Formally we can define a Petri net as a bipartite directed graph represented by a quadruple \(PN = (P, T, I, O)\), where

- \(P = \{p_1, p_2, \ldots, p_n\}\) is a finite set of places,
- \(T = \{t_1, t_2, \ldots, t_m\}\) is a finite set of transitions,
- \(I : P \times T \rightarrow \{0, 1\}\) is an input function that defines the set of directed arcs from \(P\) to \(T\),
- \(O : T \times P \rightarrow \{0, 1\}\) is an output function that defines the set of directed arcs from \(T\) to \(P\),
- \(P \cup T \neq \emptyset\), \(P \cap T = \emptyset\).

Furthermore, a marking \(M\) of the Petri net assigns to each place a non-negative integer \(M(p_i)\), the number of tokens on that place. In the Petri net every marking \(M\) of Petri net can be associated with a polynomial \(\text{pol}(M) = \prod_{p} p^{M(p)}\) and each transition \(t\) of Petri net can be associated with a polynomial: \(\text{pol}(t) = \prod_{p} p^{\text{in}(p,t)} - \prod_{o} q^{\text{out}(o,t)}\).

Consider a set of polynomial \(P \subseteq K[X^\Delta]\). We say that two polynomials \(f\) and \(g\) of \(K[X^\Delta]\) are equivalent modulo \(P\) and write \(f \equiv_P g\) if their difference can be expressed in terms of \(P\), i.e. \(f - g = k_1p_1 + \ldots + k_np_n\) for some \(p_1, \ldots, p_n \in P, k_1, \ldots, k_n \in K[X^\Delta]\). Deciding \(f \equiv_P g\) can be made easy with Groebner Basis [5, 6, 7, 39, 40, 41, 42].

A polynomial \(g\) reduces to another polynomial \(h\) modulo some polynomial set \(F\), written as \(g \equiv_P h\), if and only if there exists \(f \in F, c = \text{lc}(g)/\text{lc}(f)\) and \(u = \text{lm}(g)/\text{lm}(f)\) such that \(h = g - c \cdot u \cdot f\) [8]. The new polynomial \(h\) is equivalent to \(g\) with respect to the ideal generated by \(F\). If a polynomial \(g\) can
be reduced to \( h \) by finitely many reduction steps w.r.t. \( F \) we write \( g \rightarrow_f^* h \). An \( h \) is said to be in reduced form if \( h \) cannot be reduced further w.r.t. \( F \), denoted by \( h_F \).

A given a finite set of polynomials \( G \) is a Groebner basis if and only if \( \forall g,h,k \text{ if } h \text{ and } k \text{ are normal form of } g \text{ modulo } G \) then \( h = k \), i.e. \( \forall g,h,k \) \( (h_F \leftarrow_f F \rightarrow_f^* g \rightarrow_f^* k_F) \Rightarrow (h = k) \).

The reachability test will answer whether we can reach some state in the Petri net. Formally, the reachability problem for a Petri net is given two markings, \( M_1 \) and \( M_2 \) of the same Petri net \( M \), to answer if \( M_2 \) is reachable from \( M_1 \). A Petri net is called reversible if a marking \( M_2 \) is reachable from another marking \( M_1 \) which implies that \( M_1 \) is reachable from \( M_2 \). We can apply the Groebner basis procedure to reversible Petri nets to solve the reachability problem [8].

Given a set of transitions, \( F = \{ \text{pol}(t) : t \in T \} \) where \( F \subseteq K[X^\Delta] \), we can compute \( G \), a Groebner Basis for \( F \). The new generated polynomials after the Groebner basis computation still corresponds to a Petri net because the generated polynomials are of the same form as the polynomials arising from the translation. Now, marking \( M_1 \) is reachable from marking \( M_0 \) if and only if \( \text{pol}(M_1) \rightarrow G \text{pol}(M_0) \).

### III. Automatic Guided Vehicle System

#### A. Problem Formulation

The objective of the problem is to check whether the paths followed by the five Automated Guided Vehicles (AGVs) modeled by the Petri Net as in Figure 1 [35] are collision free or not. The model consist of five different paths followed by vehicle A, B, D, E and F. Additionally there are three different workstations represented by W1, W2 and W3. Shaded rectangular depict the collision area for two vehicles i.e. two vehicles can’t be in this area simultaneously.

Further we have used model checking technique to verify whether the adding of new places as mentioned in [35] makes the design collision free or not.

To solve the problem using model checking, we use transitions as SMV processes. For each transition, one process was instantiated. Moreover, processes are run asynchronously, which means among all the modules instantiated, one is non-deterministically chosen, and the assignment statements declared in the process are executed in parallel. This is done by instantiating process with using process keyword. This approach seems elegant since only one process can run at a time and is determined non-deterministically.

- Places are represented by the variables and ASSIGN declaration specifies their initial values (Figure 2).

- Processes are nested, meaning five process modules for five AGVs, and in each AGV’s process there are processes for transitions. These transition processes are actually the instantiation of the process, differentiated by the number of parameters used which actually represent the number of input and output places (Figure 3). For example, \( t_2(in1,in2,out1,out2) \) represents a transition with two parameters, which is an instantiation of the process.
input places \( in_1 \) and \( in_2 \), and two output places \( out_1 \) and \( out_2 \).

-- Module for transition with 1 input and 1 output
MODULE t_1(in1, out1)
ASSIGN
next(in1) = case
  in1 >0: in1 - 1;
  1: in1;
  esac;
next(out1) = case
  out1 >0: out1 - 1 mod 11;
  1: out1;
  esac;
.....

-- Module for area A
MODULE proc_A(A02, A03, A05, A06, W12, W14)
VAR
t3: process t_3(A02, A03);
t4: process t_4(A03, A05);
t5: process t_5(A05, W14, A04, W12);
t6: process t_6(A04, A03);
t7: process t_7(A03, A06);
FAIRNESS running
.....

Figure 3. Module for Transitions of AVG

- Each AGV process has FAIRNESS running to make sure that every AGV process is executed infinitely often, so the system must make progress when possible.
- Finally, we have specification to check existence of the collision state. We check for the occurrence of one or more tokens in the places within collision area (Figure 4).

![Figure 4. Specification for AVG Model](image)

Verification done with SMV shows that there is a sequence of steps which leads to collision. This model can be made collision free by adding new places as shown in Table I and Figure 5 shows adding one of the new place Z1. New SMV program is written adding these new places (Figure 6) and this time verification shows that it's a collision free design.

![Figure 5. AGV with place Z1](image)

In Table II six different variable orders and their corresponding running times are shown.
running times are given. Among these Order 6 has least running time. An important notice in this result is that running time is greatly increased when the two variables W32 and W33 are not placed consecutively.

B. Verification with Groebner basis

1) AVG without places Z:

a) Scenario I: : Marking with polynomial \( \text{pol}(M_1) = a_{3b7d6e5f1w12w23w31w32} \)

- Initial state \( \text{pol}(M_0) = a_{6b8d4e1f3w12w23w32w33} \)
- Graded reverse lexicographic order: w33, w35, w32, w31, w23, w24, w12, w14, e10, f8, e5, b7, d6, d3, d, a3, f1, e1, e6, b8, d1, d4, a4, b13, b12, b11, b10, b14, e9, b9, b2, f7, f3, f2, e8, e7, e4, e3, e2, b6, b5, b4, b3, d2, d5, a5, a2, a6

Groebner Basis \( G = \{a2 - a6, a5 - a6, b4 - b3, b5 - b3, b6 - b3, e3 - e2, e4 - e2, e8 - e7, f3 - f2, f7 - f2, b2 - b3, b9 - b3, e9 - e7, b14 - b3, b10 - b3, b11 - b3, b12 - b3, b3 - b3, a4 - a6, d4 - d5, d1 - d2, b8 - b3, e6 - e7, e1 - e2, f1 - f2, a3 - a6, d2 - d3, d6 - d5, b7 - b3, e5 - e2, f8 - f2, e10 - e7, w12 a6 - w14 a6, w12 d2 - w14 d5, w32 d2 - w31 d5, w23 b3 - w24 b3, w24 e7 - w23 e2, w33 e7 - w33 e2, w14 d2 a6 - w14 d5 a6, w31 w12 d5 - w32 w14 d5, w35 w23 e2 - w33 w24 e2, w33 w32 f2 - w35 w31 f2, w32 w14 d5 a6 - w31 w14 d5 a6, w35 w31 f2 d2 - w33 w31 f2 d5, w33 w24 e2 b3 - w35 w24 e2 b3, w33 w31 f2 e2 d2 - w33 w31 f2 e7 d5, w33 w31 w14 f2 d5 a6 - w35 w31 w14 f2 d5 a6, w35 w32 w24 f2 e2 b3 - w35 w31 w24 f2 e2 b3\)

- Normal form of \( M_1 - M_0 \) with respect to Groebner Basis G is \(-w35 w31 f2 w24 b3 w14 a2 d3 w24 + w31 w14 d5 a2 w35 w24 b2 e8 which is not equal to zero.

Thus this state is not reachable.

This is also not reachable since normal form of \( M_2 - M_0 \) with respect to Groebner Basis G is \(-w35 w31 f2 w24 b3 w14 a2 d3 w24 + w31 w14 d5 a2 w35 w24 b2 e8 which is not equal to zero.

Thus this state is not reachable. This is true because B vehicle can move to collision area if and only if there is token at z1, z2 and z3 and also remove token from these places if it moves to collision area i.e. z1, z2 and z3 control the vehicle B.

b) Scenario II: : Marking with polynomial \( \text{pol}(M_2) = a_{3b7d6e5f1w12w23w33w35} \)

Normal form of \( M_2 - M_0 \) with respect to Groebner Basis G is \(-w35 w31 f2 w24 b3 w14 a2 d3 w24 + w31 w14 d5 a2 w35 w24 b2 e8 which is not equal to zero.

Thus this state is not reachable.

Interestingly these are the only two states which are not reachable in this original AGV Petri net.

C. AGV with places Z

1) AVG without places Z:

2) AVG with places Z

- Initial state \( \text{pol}(M_0) = a_{6b8d4e1f3w12w23w32w33} \)
- Graded reverse lexicographic order: w33, w35, w32, w31, w23, w24, w12, w14, b9, b2, e10, f8, f1, e7, e2, e5, b7, d1, d6, d4, d3, a4, a3, e1, f7, f2, e6, b8, b2, d5, a5, a2, b13, b11, f3, a6, b14, e9, e4, b6, b4, b12, b10, e8, e3, b5, b3, z2, z1, z4, z3.

- Groebner Basis \( G = \{b4 - b3, b6 - b5, e4 - e3, e9 - e8, b11 - b10, b13 - b12, a5 - a2, f7 - f2, b9 - b2, -e2 + e3 z3, b10 z3 - b2, b7 z3 - b5, e10 z3 - e8, -e7 + e8 z4, -f2 + f3 z4, e5 - e3, f4 - z3, f1 - z4, f2, f8 z4 - f2, b3 z1 - b2, b14 z1 - b12, a6 z1 - a2, -a2 + a3 z1, a4 z1 - a2, b5 z2 - b3, b12 z2 - b10, -d2 + d3 z2, d4 z2 - d5, d5 + d6 z2, d1 z2 - d2, d6 z3 - d4 z3, d1 z3 - d3 z3, b10 z5 - b12 z5, b5 z5 - d4 z3, d2 z2 - d3 z3, f3 - f3 e3, f8 e3 - f3 e3, b7 e8 - e10 b5, a3 z10 - a6 b10, a4 z10 - a6 b10, ...

Normal form of \( M_1 - M_0 \) with respect to Groebner Basis G is \(-w35 w31 f3 e3 b3 w14 a2 d3 w24 + w31 w14 d5 a2 w35 w24 b2 e8 which is not equal to zero.

Thus this state is not reachable. This is true because token of route E can’t be in collision area if both places Z3 and Z4 do not have the token.

IV. TRAFFIC LIGHT SYSTEM

A. Problem Formulation

The objective of this problem is to verify that traffic light system at a busy intersection works correctly. The complete structure of this intersection is shown in Figure 7. On each direction we have five lanes, right two lanes are for incoming traffics and left three for outgoing traffic from that direction. Among three lanes on the left hand side, rightmost lane is to turn left, middle one to go straight and leftmost can be used either to go straight or turn right. Incoming vehicles are sensed by the sensor and controlled by the traffic lights. Vehicles are allowed to continue at the junction if it is safe to do so i.e. there is no possibility of collision with the vehicle from opposite direction. Further we also have four buttons for pedestrians on each of the four directions. When a pedestrian presses the button, lights must be set in a way such that it is safe for the pedestrian to cross the road.
To solve this problem the whole program is divided into three modules, for straight lane (Figure 9), for left turn lane and for pedestrian. The following approach is taken to simulate lane activities (Figure 9):

- For each lane four states are defined: *idle* (no vehicle), *entering* (vehicle sensed), *critical* (request is pending) and *exiting* (successfully crossed).
- Initially lane is in *idle* state
- If vehicle arrive sensor will be activate, set the request and change state to *entering*.
- After being in *entering* state try to get lock on the lane if
  - none of the opposite lanes have set it.
  - none of opposite lanes have requested and
  - none of pedestrian on the way have requested.
- After gaining lock check if all other opposite lane has not requested (same condition as for gaining lock). If so enter the *critical* state and set the go status.
- Once done, free the lock if pair lanes are also done and set off the go status.

```
-- Module for the straight lane.
MODULE s_straightLane (lock:in, request:in, rel:in, start:in, rel:in, go:out, stop:out)
VAR
   -- Possible state of the lane
   state: (idle, entering, critical, exiting);
   lock: boolean;

ASSUMPTION
   --Initially no vehicle so state is idle
   state = idle;
   rel = true;
   start = false;
   go = false;
   lock = false;

SPEC
   -- Set next state
   NEXT(state, lock, rel, start, go) =
     if state = idle then
       if lock = true then
         state = entering
       else
         state = idle;
     else
       if state = entering then
         if rel = true then
           state = critical
         else
           state = exiting;
     end

   -- Set go to avoid collision
   NEXT(assumption, lock, rel, start, go) =
     if lock = true then
       state = critical
     else
       state = exit;
     end

   -- When the request is made
   NEXT(request, lock, rel, start, go) =
     if request = true then
       state = entering
     else
       state = idle;
     end

   -- When the lock is set
   NEXT(lock, lock, rel, start, go) =
     if lock = true then
       state = entering
     else
       state = idle;
     end

   -- Define actions
   ASSUMPTION =
     state = idle;
     rel = false;
     start = false;
     lock = false;
     go = false;

   SPEC =
     state = critical;
     rel = false;
     start = false;
     lock = false;
     go = true;

   POSTCONDITION =
     start = false;
     rel = true;
     state = critical;
     lock = true;

   -- If vehicle enter the lane
   NEXT(request, lock, rel, start, go) =
     if request = true then
       state = entering
     else
       state = idle;
     end

   -- When the lock is set
   NEXT(lock, lock, rel, start, go) =
     if lock = true then
       state = critical
     else
       state = exit;
     end

   -- Set go to avoid collision
   NEXT(assumption, lock, rel, start, go) =
     if lock = true then
       state = critical
     else
       state = exit;
     end

-- Set go to avoid collision
START
   state = idle;
   rel = true;
   request = true;
   start = false;
   lock = false;
   go = false;
```

Figure 8. Traffic Light Petri Net

Figure 7. Traffic System

Figure 9. SMV Code for Straight Lane

Figure 10. SMV Code for Left Turn Lane
Similarly, pedestrian module as shown in Figure 11 is written to simulate pedestrian activity. Following is an outline of steps done to do so (Figure 11):

- Three states of pedestrian are defined as follows: idle (no request), press (requested) and exiting (successfully granted).
- The initially state is idle.
- State changes to press as soon as a sensor senses the request.
- Crossing is allowed if all incoming lanes (there will be four lanes to check each time) had not requested.

Now let us explain the specification give for the verification. Specification is shown in Figure 12. Two sets of specification are given, one to check for mutual exclusion i.e. when any one lane or one side pedestrian is in go state no other opposite lane be in go state too. This ensures that no collisions or hit will ever occur. Other set of specifications ensure that no process can block other process from getting the request.

### For Mutual Exclusion

<table>
<thead>
<tr>
<th>SPEC</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{SPEC}<em>{\text{id}}(\text{MP-Do})) (\text{SPEC}</em>{\text{Do-Do}}) (\text{SPEC}<em>{\text{MP-ID}}) (\text{SPEC}</em>{\text{MP-MD}}) (\text{SPEC}<em>{\text{MD-ID}}) (\text{SPEC}</em>{\text{MD-MD}})</td>
<td></td>
</tr>
<tr>
<td>(\text{SPEC}<em>{\text{MD-ID}}) (\text{SPEC}</em>{\text{MD-MD}}) (\text{SPEC}<em>{\text{MD-MD}}) (\text{SPEC}</em>{\text{MD-ID}}) (\text{SPEC}<em>{\text{MD-MD}}) (\text{SPEC}</em>{\text{MD-ID}})</td>
<td></td>
</tr>
</tbody>
</table>

---

Figure 12. Specification for Traffic Light Verification

1) **Verification with Model Checking:** Following observation (Figure 13) is made while verifying the model. All the specification comes to be true so no counter example is given which means that the desire properties are fulfilled by the model.

![Figure 13. Traffic Light Problem Verification Result](image.png)

2) **Verification with Groebner Basis:** Now, further verification can be done with the help of Petri Net and Groebner basis. Petri Net for this traffic problem can be defined in terms of traffic lights. Here six traffic lights will be enough to simulate, four lights for each left turn and one light for each horizontal and vertical lane. Pedestrian lights can share same transition as of horizontal and vertical lanes. For example North to South pedestrian light will be identical to light for North-South lane.

**Scenario I:** Lights for both North-East turn and South-West turn is green \(\text{pol}(M_1) = R1G2R3R4G5R6\)

- Initial state \(\text{pol}(M_0) = SR1R2R3R4R5R6\)
- Graded reverse lexicographic order: R1, R2, R3, R4, R5, R6, G4, O1, G2, O2, O4, G3, O3, G6, O6, G5, G1, O5, S.
- Groebner Basis $G = [G5 - O5, G6 - O6, G3 - O3, G2 - O2, O1 - G1, G4 - O4, S R6 - O6, S R5 - O5, -O4 + S R4, -O3 + S R3, -O2 + S R2, S R1 - G1, R5 G1 - R1 O5, R5 O6 - R6 O5, R1 O6 - R6 G1, R6 O3 - R3 O6, R5 O3 - R3 O5, R1 O3 - R3 G1, R6 O4 - R4 O6, R5 O4 - R4 O5, R3 O4 - R4 O3, R1 O4 - R4 G1, R6 O2 - R2 O6, R5 O2 - R2 O5, R4 O2 - R2 O4, R3 O2 - R2 O3, R1 O2 - R2 G1]

- Normal form of $M_1 - M_0$ with respect to Groebner Basis $G$ is $R6 G1 R2 O5 R3 R4 - R6 O5 R1 R2 R3 R4$ which is not equal to zero. Thus this state is not reachable which must be true to ensure safety at the crossroad.

**Scenario II:** Lights for both North-South and East-West lane are green $pol(M_2) = G1R2R3G4R5R6$

The normal form of $M_2 - M_0$ with respect to Groebner Basis $G$ and with same graded reverse lexicographic order as above is $R6 G1 R2 O5 R3 R4 - R6 O5 R1 R2 R3 R4$ which is not equal to zero. Thus this state is also unreachable.

**V. Conclusion**

We have shown that computational methods like model checking and Groebner bases can be used to verify the correctness of an automation system by specifying the desired properties in the CTL form and verifying the corresponding temporal formula. The benefit of using SMV for model checking is its feature of giving counter example in the case of fault in the system. This feature not only helps to catch the bug but also helps to rectify the fault in the design. We also use algorithms from the field of computer algebra particularly theory of Groebner basis is used on Petri Net to test the reachability problem.

**REFERENCES**


