CS611 Proof Paper 1

Anonymized

September 25, 2013

1 Introduction

I chose a proof of a lemma in the field of Model Checking. Some models and notations used in the proof are specific to this field, so I added explanation of those before getting into the actual proof.

1.1 Kripke Structure [2]

Let AP be a set of atomic propositions. A Kripke structure M over AP is a four tuple $M = (S, S_0, R, L)$ where

1. S is a finite set of states.
2. $S_0 \subseteq S$ is the set of initial states.
3. $R \subseteq S \times S$ is a transition relation that must be total, that is, for every state $s \in S$ there is a state $s' \in S$ such that $R(s, s')$.
4. $L : S \to 2^{AP}$ is a function that labels each state with the set of atomic propositions true in that state.

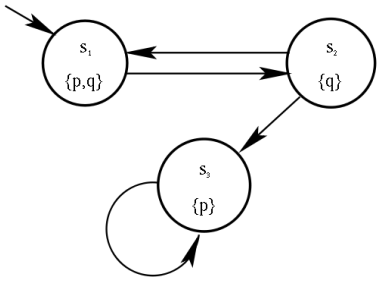

Figure 1: Example of a Kripke Model

Let me show you an example of a Kripke structure[1]. A set of atomic proposition is a boolean expression over variables, constants and predicate symbols, which defines a Kripke structure. In this example, the set of atomic propositions $AP = \{p, q\}$. p and q can model arbitrary boolean properties of the system that the Kripke structure is modeling. Figure 1 illustrates a Kripke structure $M = (S, S_0, R, L)$, where

1. $S = \{s_1 s_2, s_3\}$.
2. $S_0 = \{s_1\}$.
3. $R = \{(s_1, s_2), (s_2, s_1), (s_2, s_3), (s_3, s_3)\}$. The transition relation is total, meaning that all the transitions in the model represented by edges of the graph is listed. The direction of a transition represented by an arrow is important. $R(s_1, s_2)$ means there is a possible transition from the state s_1 to s_2.
4. $L = \{(s_1, \{p, q\}), (s_2, \{q\}), (s_3, \{p\})$. The function $L : S \to 2^{AP}$ creates an unique label for each state with using some atomic propositions that are true for the state out of a power set of atomic propositions. For example, for the state s_1, both p and q are true. So, that is the label for the state.

1.2 Symbols

- $\models$ (reads as "models"): This symbol takes three parameters, two on the left and the other on the right like this; $M, s \models f$. This means that a condition f holds for a state s in the Kripke structure M.
- **E** (reads as "exists"): This symbol is used with $\models$ to add a meaning. $M, s \models \mathbf{E}f$ means that there exists a path π from s such that $M, \pi \models f$. Please note that the condition f should be satisfied somewhere along the path π.
- **G** (reads as "globally"): This symbol is also used with $\models$ to add another meaning. $M, s \models \mathbf{G}f$ means for all $i \geq 0$, $M, \pi^i \models f$ where s is the first state of π. This means that the condition f should be satisfied through out the path π.

2 Original Proof[2]

Lemma $M, s \models \mathbf{EG}\ f_1$ iff the following two conditions are satisfied:

1. $s \in S'$.
2. There exists a path in M' that leads from s to some node t in a nontrivial strongly connected component C of the graph (S', R').

Proof Assume that $M, s \models \mathbf{EG}\ f_1$. Clearly $s \in S'$. Let π be an infinite path starting at s such that f_1 holds at each state on π. Since M is finite, it must be possible to write π as $\pi = \pi_0\pi_1$ where π_0 is a finite initial segment and π_1 is an infinite suffix of π with the property that each state on π_1 occurs infinitely often. Then, π_0 is contained in S'. Let C be the set of states in π_1. Clearly, C is contained in S'. We now show that there is a path within C between any pair of states in C. Let s_1 and s_2 be states in C. Pick some instance of s_1 on π_1. By the way in which π_1 was selected, we know that there is an instance of s_2 further along π_1. The segment from s_1 to s_2 lies entirely within C. This segment is a finite path from s_1 to s_2 in C. Thus, either C is a strongly connected component or it is contained within one. In either case, both conditions (1) and (2) are satisfied.

Next, assume that Conditions (1) and (2) are satisfied. Let π_0 be the path from s to t. Let π_1 be a finite path of length at least 1 that leads from t back to t. The existence of π_1 is guaranteed because t is a state in a nontrivial strongly connected component. All the states on the infinite path $\pi_=\pi_0\pi_1^\omega$ satisfy. Since π is also a possible path starting at s in M, we see that $M, s \models \mathbf{EG}\ f_1$. $\square$

3 Annotated Proof

3.1 Annotation

Lemma $M, s \models \mathbf{EG}\ f_1$ iff the following two conditions are satisfied:

1. $s \in S'$. This means that the start node should be in S' or modified Kripke structure.
2. There exists a path in M' that leads from s to some node t in a nontrivial strongly connected component C of the graph (S', R'). Trivial graph means there is only one state. Strongly connected graph means that from every node in the graph, any node can be visited. This does not mean a direct path from every node to every node. A node can be visited through other nodes.

There is a very important modification applied to the Kripke structure in order to prove this lemma and the modification is applied as a presupposition. Since the lemma referring to a global condition of **G** , meaning that it only focuses on the states that satisfy the condition f_1, all other states can be disregarded. Therefore, a new Kripke structure of M' is obtained from M by deleting from S all of those states at which f_1 does not hold and restricting R and L accordingly. Thus, $M' = (S', R', L')$ where $S' = \{s \in S \mid M, s \models f_1\}$, $R' = R|_{S' \times S'}$, and $L' = L|_{S'}$. Note that R' may not be total in this case, but it does not affect the proof. An example of this is shown in Figure 2 and Figure 3. Whenever you see a notation about an original

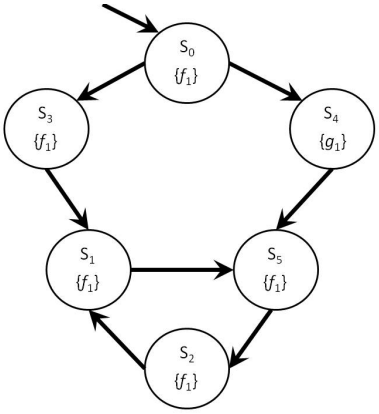

Figure 2: Kripke Structure M

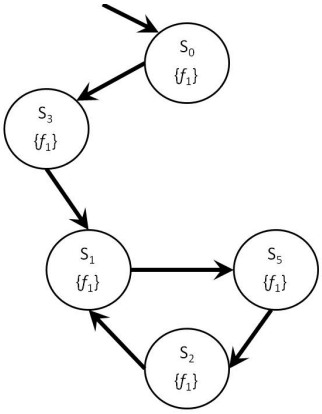

Figure 3: Modified Kripke Structure M'

Kripke structure of $M = (S, R, L)$, please refer to Figure 2. And also, whenever you see a notation about a modified Kripke structure of $M' = (S', R', L')$, please refer to Figure 3.

Proof Assume that $M, s \models \mathbf{EG}\ f_1$. Clearly $s \in S'$, or otherwise, the state should have been eliminated beforehand. Let π be an infinite path starting at s such that f_1 holds at each state on π. Since M is finite, it must be possible to write π as $\pi = \pi_0\pi_1$ where π_0 is a finite initial segment and π_1 is an infinite suffix of π with the property that each state on π_1 occurs infinitely often. Please look at Figure 2. In this model, s is s_0. s_0 and s_3 form π_0 and s_1, s_5, and s_2 form π_1 in the path of π. Now you can see how an infinitely long path can be formed with finite states. Then, π_0 is contained in S'. Let C be the set of states in π_1. In our case, s_1, s_5, and s_2 are in C. Clearly, C is contained in S'. We now show that there is a path within C between any pair of states in C. Let s_1 and s_2 be states in C. Pick some instance of s_1 on π_1. In our case, we just pick s_1 in our model. By the way in which π_1 was selected, we know that there is an instance of s_2 further along π_1. The segment from s_1 to s_2 lies entirely within C. This segment is a finite path from s_1 to s_2 in C. In our case, there are two steps from s_1 to s_2. Thus, either C is a strongly connected component or it is contained within one. In either case, both conditions (1) and (2) are satisfied.

Next, assume that Conditions (1) and (2) are satisfied. Please look at Figure 3. Conditions (1) and (2) mean that an initial state is chosen from S'. We pick s_0. Also, there is a state t somewhere in a strongly connected component C. We pick s_1 as t. Let π_0 be the path from s to t. In our case, that is from s_0 to s_1. Let π_1 be a finite path of length at least 1 that leads from t back to t, meaning s_1 to s_1. That has the length of three. The existence of π_1 is guaranteed because t is a state in a nontrivial strongly connected component. All the states on the infinite path $\pi_= \pi_0\pi_1^\omega$ satisfy. Since π is also a possible path starting at s in M, we see that $M, s \models \mathbf{EG}\ f_1$. $\square$

3.2 Plain English Translation

The most important part of this proof is to use both of the Kripke structures M and M' and go back and forth to connect the two statements in the lemma. It is easier to show the existence of a valid path in M' since the structure is simplified. Then, show that the same principle can be applied to the original M or vice versa. The original proof itself is very simple and self-explanatory, but figures may help to follow what is being explained in the proof instead of visualizing the models in mind. The key concept of this lemma is to understand the nature of a path that holds certain condition. A path has to be infinite, but the path is consist of finite states. So, basically, there should be a loop in the model. Another point is to find the connection from the valid start node to the loop part. Show these two points in both M and M'.

4 Analysis

4.1 Value of the Proof and Application

The essence of the model checking technique is to verify a system if it has a valid path from an initial state to a desired state automatically, meaning without any human assistance once the models are defined properly. This lemma tells what the required conditions are to do that. Application of this could be a navigation software. A user inputs the start and goal positions, and then the software returns a path or possibly multiple paths to navigate the user. To verify that the software works correctly, this lemma could be applied. The geographical information needs to be converted into a Kripke structure and some conditions are defined for a route. The software may generate multiple routes for the query, but the lemma can tell if there is a path that satisfies all the conditions throughout the path within the proposed routes.

4.2 Proof Strategy

The lemma has a form of P $\leftrightarrow$ Q where P is "$M, s \models \mathbf{EG}\ f_1$" and Q is "if given two conditions are satisfied". First, P $\rightarrow$ Q is proved by transforming P into Q. The key point is how to find a set that is equivalent to the set C defined in the second condition of the lemma. The other way around is also very straight forward. Q $\rightarrow$ P is proved by transforming Q into P. Again, the key point is to find a valid example within the given information and show that it satisfies the condition of the goal.

References

[1] Kripke structure (model checking) — Wikipedia, The Free Encyclopedia.

[2] Edmund M Clarke, Orna Grumberg, and Doron A Peled. *Model checking*. MIT press, 1999.