

Course ISE 435: Distributed Algorithms in Network Communication

Recitation 4 Exercise Answers

Michael J. May

April 7, 2010

1 Exercise 1

Assume P_1 and P_2 are invariants of a system S . Prove that $(P_1 \vee P_2)$ and $(P_1 \wedge P_2)$ are invariants as well.

1.1 Answer

The definition of an invariant is that:

1. $\forall \gamma \in \mathcal{I} P(\gamma)$ (P holds initially)
2. $\{P\} \rightarrow \{P\}$, (no transition can invalidate P)

Given: So we have by the problem statement that P_1 and P_2 are true. Therefore:

1. $\forall \gamma \in \mathcal{I} P_1(\gamma)$
2. $\forall \gamma \in \mathcal{I} P_2(\gamma)$
3. $\{P_1\} \rightarrow \{P_1\}$
4. $\{P_2\} \rightarrow \{P_2\}$

To prove: We must prove the following properties then:

1. $\forall \gamma \in \mathcal{I} (P_1 \vee P_2)(\gamma)$
2. $\{P_1 \vee P_2\} \rightarrow \{P_1 \vee P_2\}$
3. $\forall \gamma \in \mathcal{I} (P_1 \wedge P_2)(\gamma)$
4. $\{P_1 \wedge P_2\} \rightarrow \{P_1 \wedge P_2\}$

Proof of $P_1 \vee P_2$ To prove the first property, begin by noting that for all initial states, since P_1 and P_2 are invariants, they are true in all initial states:

$$\forall \gamma \in \mathcal{I} (P_1(\gamma) \vee P_2(\gamma))$$

Since $P_1 = true \vee P_2 = true \implies (P_1 \vee P_2) = true$

For the second property, let us choose a c at random. Assume that c leads to some state d . There are four possibilities regarding the truth of the properties of P_1 and P_2 :

- $!P_1$ and P_2 - In this case, $P_1 \vee P_2 = true$. Since $\{P_2\} \rightarrow \{P_2\}$ by the definition, P_2 must be true in d . Since P_1 is false, by the definition we may have P_1 true or false in d (the implication is trivially true when P_1 is false). The resulting states from d can therefore be:

- $P_1 = true$ and $P_2 = true$.
- $P_1 = false$ and $P_2 = true$

In either case, $P_1 \vee P_2$ is true in d .

- P_1 and $!P_2$ - In this case $P_1 \vee P_2 = true$. It is parallel to the first case. Since $\{P_1\} \rightarrow \{P_1\}$ by the definition, P_1 must be true in d . Since P_2 is false, by the definition we may have P_2 true or false in d (the implication is trivially true when P_2 is false). The resulting states from d can therefore be:

- $P_1 = true$ and $P_2 = true$.
- $P_1 = true$ and $P_2 = false$

In either case, $P_1 \vee P_2$ is true in d .

- $!P_1$ and $!P_2$ - In this case $P_1 \vee P_2 = false$. Since it is false, the implication $\{P_1 \vee P_2\} \rightarrow \{P_1 \vee P_2\}$ for d is trivially true.
- P_1 and P_2 - In this case $P_1 \vee P_2 = true$. Since both are true in c , by the definition of the implication, there is only one possibility for d :

- $P_1 = true$ and $P_2 = true$.

In this case $P_1 \vee P_2$ is true in d .

Therefore we have shown that $\{P_1\} \rightarrow \{P_1\}$ and $\{P_2\} \rightarrow \{P_2\}$ imply that $\{P_1 \vee P_2\} \rightarrow \{P_1 \vee P_2\}$. Based on the above two proofs, we have shown that $P_1 \vee P_2$ is an invariant.

Proof of $P_1 \wedge P_2$ To prove the third property, begin by noting that for all initial states, since P_1 and P_2 are invariants, they are true in all initial states:

$$\forall_{\gamma \in \mathcal{I}} (P_1(\gamma) \vee P_2(\gamma))$$

Since $P_1 = true \vee P_2 = true \implies (P_1 \wedge P_2) = true$

For the fourth property, let us choose a c at random. Assume that c leads to some state d . There are four possibilities regarding the truth of the properties of P_1 and P_2 :

- $!P_1$ and P_2 - In this case, $P_1 \wedge P_2 = false$. Since it is false, the implication $\{P_1 \wedge P_2\} \rightarrow \{P_1 \wedge P_2\}$ for d is trivially true.
- P_1 and $!P_2$ - In this case, $P_1 \wedge P_2 = false$. Since it is false, the implication $\{P_1 \wedge P_2\} \rightarrow \{P_1 \wedge P_2\}$ for d is trivially true.
- $!P_1$ and $!P_2$ - In this case $P_1 \vee P_2 = false$. Since it is false, the implication $\{P_1 \vee P_2\} \rightarrow \{P_1 \vee P_2\}$ for d is trivially true.
- P_1 and P_2 - In this case $P_1 \vee P_2 = true$. Since both are true in c , by the definition of the implication, there is only one possibility for d :

- $P_1 = true$ and $P_2 = true$.

In this case $P_1 \wedge P_2$ is true in d .

Therefore we have shown that $\{P_1\} \rightarrow \{P_1\}$ and $\{P_2\} \rightarrow \{P_2\}$ imply that $\{P_1 \wedge P_2\} \rightarrow \{P_1 \wedge P_2\}$. Based on the above two proofs, we have shown that $P_1 \wedge P_2$ is an invariant.

2 Exercise 2

Give a transition system S and an assertion P such that P is always true in S but is not an invariant of S .

2.1 Answer

First let us define what is meant by an “always true” assertion:

An always true assertion is one which is true for all executions of the program, meaning there are no reachable states which violate the assertion.

An invariant poses a stronger requirement - that there aren't any transitions which violate the assertion, even if they are unreachable.

To show an example, we just need to find a case where an invariant is true in all reachable states, but contains an unreachable state where it is violated.

Example: Let the transition system consist of three states $k = 0$, $k = 1$, $k = 2$. For simplicity, let's just label the states by the value of k . Let $I = \{k = 0\}$. Let the transition relation $\rightarrow = \{k = 1\} \rightarrow \{k = 2\}$. Let's define an assertions $A = (k < 2)$.

Now, we can show that A is always true - there are no reachable executions in which A is violated.

However, A is not an invariant - the transition $\{k = 1\} \rightarrow \{k = 2\}$ violates the second condition of what an invariant is.