

Error Localization & Relevance Analysis

Numair Mansur, Christian Schilling, Matthias Heizmann

University of Freiburg, Germany

Definition 1 (Execution). *Let π be an error trace of length n . An execution of π is a sequence of states $s_0, s_1 \dots s_n$ such that $s_i, s_{i+1} \models T$, where T is the transition formula of $\pi[i]$.*

Let ϵ represent the set of all possible executions of the error trace.

Definition 2 (Blocking Execution). *An execution of a trace π of size n is called a blocking execution if there exists a sequence of states $s_0, s_1 \dots s_j$ where $i < j \leq n$ such that $s_i, s_{i+1} \models T[i]$, where $T[i]$ is the transition formula of $\pi[i]$ and there exists an assume statement in the trace π at position j such that $s_j \not\models \text{guard}(\pi[j])$.*

Definition 3 (Relevancy of an assignment statement). *Let β represent the set of all blocking executions of a trace π . Let there be an assignment statement of the form $x := t$ at position i . Let π' represent the trace that we get after replacing $\pi[i]$ with a havoc statement of the form $\text{havoc}(x)$ and let β' represent the set of all blocking executions for π' .*

We say that the assignment statement $\pi[i]$ is relevant if the trace after the replacement has strictly more blocked executions than the trace before the replacement, i.e if $\beta \subsetneq \beta'$.

Lemma 1. *For a program statement st and predicates P and Q , where P is condition that is true before the execution of the statement and Q is a post condition, the following two implications are equivalent(also known as the duality of WP and SP):*

$$SP(P, st) \Rightarrow Q$$

$$P \Rightarrow WP(Q, st)$$

Lemma 2. *For a predicate Q and an assignment statement of the form $x := t$ where x is a variable and t is an expression, we have:*

$$WP(Q; \text{havoc}(x)) \subseteq WP(Q; x := t)$$

Lemma 3 (nonempty post). *If $P := WP(Q, x := t) \not\subseteq WP(Q, \text{havoc}(x))$ for some Q then $Q \subsetneq SP(P, \text{havoc}(x))$.*

Proof. We will show that $Q \equiv SP(P, x := t) \subseteq SP(P, \text{havoc}(x)) \not\subseteq Q$ from which it follows that the first inclusion is strict. The first inclusion is immediate from Lemma ???. By assumption $P \not\subseteq WP(Q, \text{havoc}(x))$, which by Lemma ?? is equivalent to the second part. \square

Theorem 1 (Relevancy of an assignment statement). *Let π be an error trace of length n and $\pi[i]$ be an assignment statement at position i having the form $x := t$, where x is a variable and t is an expression. Let P and Q be two predicates where $P = \neg WP(\text{False}; \pi[i, n]) \cap SP(\text{True}; \pi[1, i-1])$ and $Q = \neg WP(\text{False}; \pi[i+1, n])$. The statement $\pi[i]$ is relevant iff:*

$$P \not\Rightarrow WP(Q, \text{havoc}(x))$$

Proof. Let π' be the trace where the assignment statement $\pi[i]$ is replaced by a havoc statement.

Note that here we can also write P as $WP(Q; x := t) \cap SP(\text{True}; \pi[1, i-1])$. Let $Q' := SP(P; \text{havoc}(x))$ and $P' := WP(Q; \text{havoc}(x)) \cap SP(\text{True}; \pi[1, i-1])$. Since from lemma ?? , we know that

$$WP(Q; \text{havoc}(x)) \subseteq WP(Q; x := t)$$

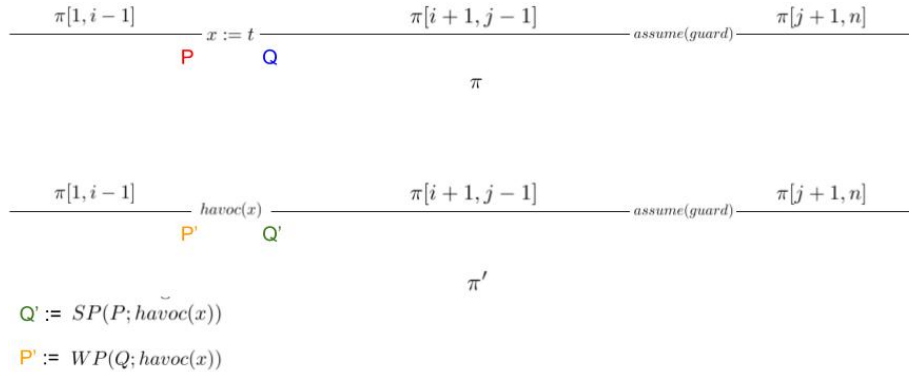
and also,

$$WP(Q; \text{havoc}(x)) \cap SP(\text{True}; \pi[1, i-1]) \subseteq WP(Q; x := t) \cap SP(\text{True}; \pi[1, i-1])$$

therefore:

$$P' \subseteq P$$

For simplicity in the proof, let's ignore the term $SP(\text{True}; \pi[1, i-1])$ from P and P' . We simplify P and P' to be $WP(Q; x := t)$ and $WP(Q; \text{havoc}(x))$ respectively.



" \Rightarrow "

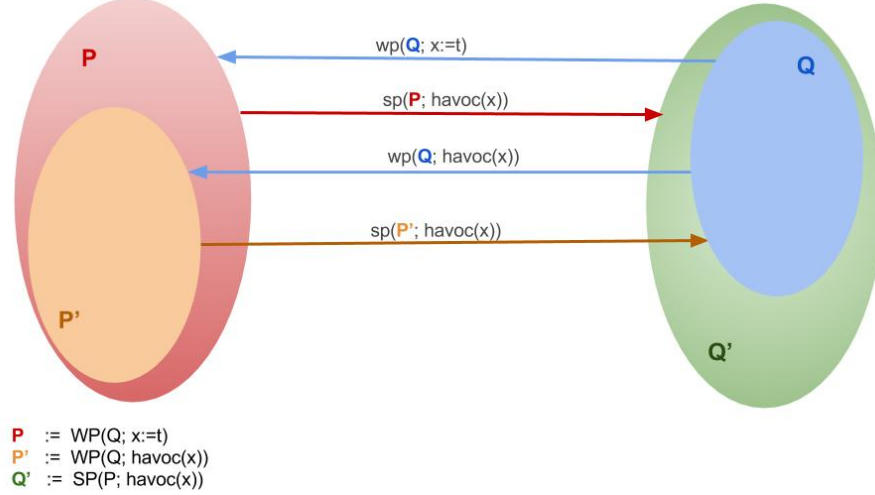
If the assignment statement $\pi[i]$ is relevant then:

$$P \not\Rightarrow WP(Q, \text{havoc}(x))$$

Relevancy of $x := t$ implies that replacing it with $\text{havoc}(x)$ gives us strictly more blocking executions than before. Therefore

$$Q \subsetneq Q'$$

Lets look at the following diagram to help us see the states a little better and come to the following conclusions:



$$SP(P; havoc(x)) = Q'$$

$$SP(P'; havoc(x)) = Q$$

and we know that $Q \subsetneq Q'$. This means that $\exists S \in P \setminus P'$, such that there is a transition from S to Q' if we execute $havoc(x)$. The existence of the state S means:

$$P \not\approx P'$$

or

$$P \not\approx WP(Q; havoc(x))$$

" \Leftarrow " [under construction. Please don't read now]

If

$$P \not\approx WP(Q; havoc(x))$$

then the assignment statement $x := t$ is relevant.

By the definition of P :

$$WP(Q; x := t) \not\approx WP(Q; havoc(x))$$

By lemma ??:

$$Q \subsetneq SP(Q; havoc(x))$$

or

$$Q \subsetneq Q'$$

Let $R = Q' \setminus Q$ or $Q' = R \uplus Q$ (disjoint union of R and Q).

Now if we can show that there are states in R such that there is a blocking execution from those states. Then that would mean that replacing the assignment with havoc have introduced some new blocking executions.

□