Fault Localization & Relevance Analysis

Numair Mansur, Christian Schilling, Matthias Heizmann

University of Freiburg, Germany

June 11, 2017

Definition 1 (Execution)**.** *Let π be an error trace of length n. An execution of π is a sequence of states $s_0, s_1 ... s_n$ 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 $s_0, s_1 ... s_j$ 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 exits an assume statement in the trace π at position j such that $s_j \not\models guard(\pi[j])$.*

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 $havoc(x)$ 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 predicate Q and an assignment statement of the form $x := t$ where x is a variable and t is an expression, we have:*

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

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 $P = \neg WP(False; \pi[i, n]) \cap SP(True; \pi[1, i-1])$ and $Q = \neg WP(False; \pi[i+1, n])$. The statement $\pi[i]$ is relevant iff:*

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

Proof. Let π' be the trace where the assignment statement $\pi[i]$ is replaced by a havoc statement.
"$\Rightarrow$"
If the assignment statement $\pi[i]$ is relevant then:

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

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

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

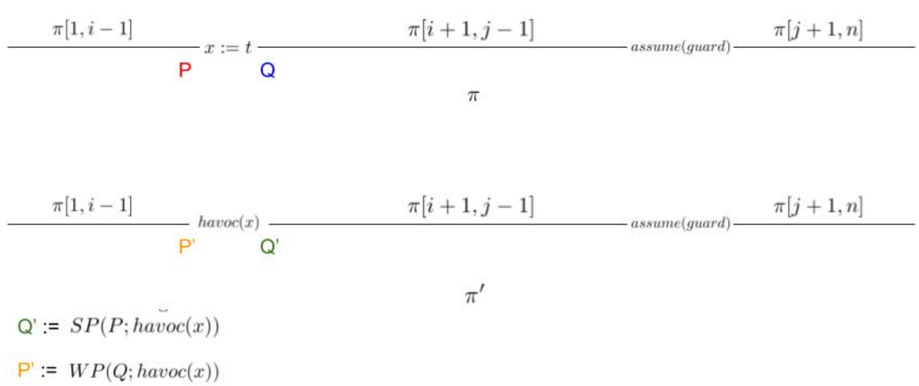
and also,

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

therefore:

$$P' \subseteq P$$

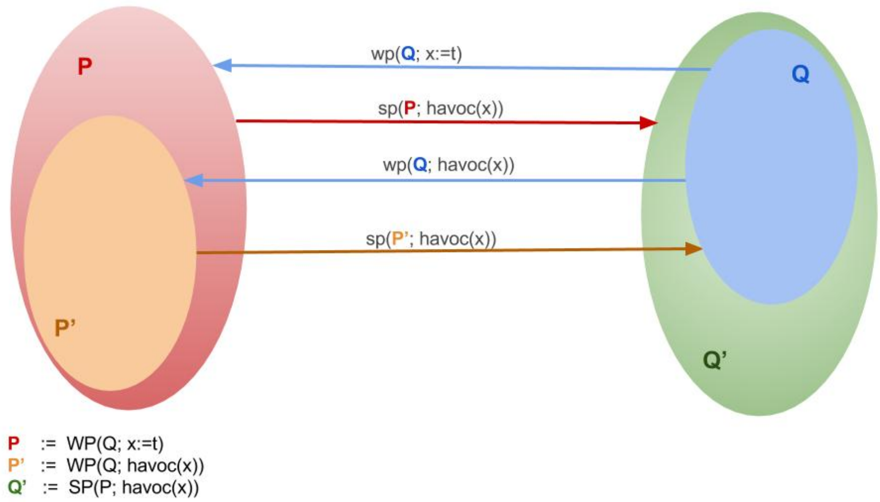
For simplicity in the proof, lets ignore the term $SP(True; \pi[1, i-1])$ from P and P'. We simplify P and P' to be $WP(Q; x := t)$ and $WP(Q; havoc(x))$ respectively.



Relevancy of $x := t$ implies that replacing it with $havoc(x)$ gives us strictly more blocking executions then 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 conculsions:



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

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

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:

$$P \not\Rightarrow P'$$

or

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

$\square$