Fault Localization & Relevance Analysis

(For the latest version: http://numairmansur.github.io/Error-Localization/project.pdf)

Numair Mansur

May 31, 2017

1 Introduction

The most tedious task in a programmer's routine is to spend time on debugging and to determine the cause of the error. Debugging can be made much simpler if we can determine automatically what program segments are actually responsible for the error. This process of automatically determining error locations is called **"Fault Localization"**.
Fault Localization encompasses the task of identification of the program statements that are **relevant** for the error trace and determining the variables whose values should be tracked in order to understand the cause of the error.
There can be many notions of error relevancy. During my master praktikum, I worked with and developed algorithm for two new relevancy criterion, which we called Flow-Sensitive and non Flow-Sensitive error relevancy. A part of this work will be to formalize these two new types of error relevancy. But first we need a basic formal definition to "relevancy", that is, what does it mean that a statement is relevant for an error. Surprisingly enough, I was unable to find a formal and a generally accepted definition of error relevancy in the literature. But this also makes sense because relevancy is not a well established concept and is a hard thing to define, let alone formally. Therefore, another aim of this project is to try to give a formal definition to error relevancy.

1.1 Relevant Work

In the paper Flow-Sensitive Fault Localization [1], the authors take into account the flow of the program while determining the statements that are relevant for the error. They do it by a new flow-sensitive encoding of error traces into trace formulas. After which, by identifying the irrelevant portions of the new trace formula, we can isolate the possible cause of the error. The result of a flow-sensitive fault localization not only explains why the error occurred, but also justifies why the statements leading to the error were executed [1].
In the Error invariants paper [2], the authors introduce a new concept in which for each position in an error trace they find a formula over program variables that over-approximates the reachable states at the given position while only

capturing the states that will still produce the error, if execution of the trace is continued from that position. We can find the relevant statements in the trace with the help of inductive error invariants. Inductive invariants are those error invariants that hold for consecutive positions in an error trace and hence characterize statements in the trace that are irrelevant for the trace [2].
In the paper Explaining inconsistent code [3] the authors use the idea presented in Error Invariants to find and explain inconsisitencies in a program using something called an "$ErrorInvariantAutomaton$". The error invariant automaton is an abstraction of the input code fragment that only mentions program statements and facts that are relevant for understanding the cause of the inconsistency.

2 Goals/Approach

2.1 Formalizations

During my Master Praktikum, I worked on a fault localization algorithm that find relevant statements in an error with respect to two error relevance criterion namely Flow Sensitive and Non-Flow Sensitive relevance criterion. I want to formalize these two notions of error relevance. There are also two sub categories in a relevance criteria which also need a formal definition.

(1) Predetermined input (which we called the UC case)
(2) Non-deterministic input (havoc).

Another task in this step would be to formalize our already implemented fault localization algorithm .

2.2 Performance Analysis of the Algorithm

I want to test the algorithm on big error traces and analyse its performance and find out where can the performance be improved. This might also require some modifications in the algorithm.

2.2.1 Non-Flow Sensitive Analysis

...

2.2.2 Flow-Sensitive Analysis

...

2.3 Security Bugs

We also discovered during my Praktikum that we may be able to perform a security analysis via our fault localization algorithm and distinguish security bugs in a program from all other bugs. I want to formalize what it means that a bug is a security bug and use the algorithm to precisely find them. I expect some modifications in our algorithm so that it can correctly classify an error as a security/non-security error. Following steps are expected to complete this task:
1) Analyse examples containing security bugs.
2) Formalize the definition of a security bug that satisfies all the examples.
3) Check if the formal definition fits correctly with the examples.
4) Modify our fault localization algorithm so that it models the definition correctly.

2.4 Verification of the results

I also want to make a mechanism to verify that what we are computing is correct that includes verifying the result of our fault localization algorithm and security bug analysis. For this task i plan to separately implement checks and compare it with our algorithms.

2.5 Broader analysis of the program

Currently we are doing the analysis only on the error trace (or counter example), i also want investigate how we can broaden our perspective from an error trace to a whole program. This may also give us some new definitions for relevance for example, statements that are directly responsible, statements that cause the execution of the directly responsible statements. As an example, consider the code below:

```

foo()
{
  int z;
  int x;
  if(x==0)
  {
    if(z==0)
    {
      y := 1;
    }
    else
    {
      while(true)
      {

      }
    }
    assert(false);
```

```
  }
}
```

π in this example is:

$$assume(x == 0); assume(z == 0); y = 1)$$

and our algorithm shows that none of the statements is relevant. But if we look at the program from a broader perspective then an error trace, we will notice that the value of z is relevant because if $z \neq 0$ then we would be stuck in a never ending loop and would not be able to reach the error. So we cannot say that $assume(z = 0)$ is irrelevant for the error.

3 Formalization of Relevancy Criterion

3.1 Error Relevancy

In a program containing a set of statements ST, let $\pi \in ST$ be a sequence of statements. Let ϕ be an assertion condition, such that if π is executed, the assertion condition ϕ is violated. We call this an error. It is possible that ϕ will not be violated after all possible executions of π. It will only be violated if we start the execution of π from a specific state which belongs to a set of states, which we call Error-Precondition EP.
A set of statements $REL \in P(\pi)$ is called relevant iff REL is a set which have a minimum size in $P(\pi)$ and the following property holds:
"If all the assignments in REL from π are replaced with a havoc statement to get a new path π' and if we now execute π' , starting from a state which is in EP, it is not guaranteed that the assertion condition ϕ is violated any more. i.e $\forall \psi \in EP$, the execution of π' is not guaranteed to violate ϕ".

[!!!!!] This definition only holds for our flow sensitive case, not for the non-flowsensitive case because for some non-flow relevant statements, changing them with a havoc still guarantees that we end up violating the assertion condition in the end

[[[REL must also represent a trace that is actually feasible [Define feasible trace here !]]]].

Consider the code below:

```

foo()
{
  x := 1;
  x--;
  x++;
  assert(x==0);
}
```

In the above example:
$\psi = True$
$\pi = \{x = 1, x--, x++\}$
$\phi \Rightarrow assume(x == 0)$

$$P(\pi) = \{\{x = 1\}, \{x--\}, \{x++\}, \{x = 1, x--\}, \{x = 1, x++\}, \{x--, x++\},$$
$$\{x = 1, x--, x++\}\}$$

$Rel = \{x++\}$ because if the statement in REL is replaced by a havoc statement in π to get a new path $\pi' = \{x = 1, x--, havoc(x)\}$ then there is no guarantee that the assertion condition ϕ is violated any more after the execution of π'.

Consider another example:

```

foo()
{
  x := 1;
```

```
  y := 1;
  y := 2;
  If ( y == 2 )
  {
    x := 0;
  }
  assert(x==1);
}
```

In this example:
$\pi = \{x = 1; y = 1; y = 2; x = 0\}$
$\phi = assume[x == 1]$
$REL = \{x = 0\}$
$\pi' = \{x = 1, y = 1, y = 2, havoc(x)\}$

3.2 Non-Flow Sensitive Relevance criteria

3.2.1 Preliminary definitions

Introduction:

Proof based fault localization techniques rely on encoding of an error trace into a so called error trace formula. A ***error trace formula*** is an unsatisfiable logical formula (or is it ? isn't it unsatisfiable together with the post condition). An error is observable by executing an error trace starting from a state that satisfies an ***error pre-condition***.
We will encode the (error?)trace into a so called extended trace formula which consists the error precondition, correctness assertion and the trace formula of the trace. When the extended trace formula is unsatisfiable, we say that the trace in the extended trace formula is an error trace and we say that we are seeing an "error".

Formal Setting:

We present programs and their control flow structure using *program automata*. Program automata provide a simple model of programs that abstracts from the syntactic constructs and semantics of specific programming languages. A program automaton is a finite automaton. A state in a program automaton corresponds to a program location and transitions between two states are labelled with program statements. That is, program automaton accepts a regular language of finite words over statements. Each word in this language corresponds to one control flow path. Not every path of a program automaton gives rise to a feasible execution [COME BACK TO FEASIBILITY OF AN EXECUTION].
Formally, let Σ be a fixed set of program statements. A program automaton A is a tuple $(Loc, \delta, l_0, l_{exit}, l_{error})$ where
- Loc is a finite set of locations.
- $\delta \subseteq Loc$ x Σ x Loc is a finite transition relation.
- l_0 is an initial location.
- l_{exit} is a set of exit locations.

- l_{error} is a set of error locations.
We interpret A as a finite automaton over alphabet Σ with initial state l_0 and final states l_{exit} or l_{error}. A *run* ρ of A is a finite sequence of locations and statements $l_0 st_0 l_1 .... st_{n-1} l_n$, such that for all $i \in [0, n)$, $(l_i, st_i, l_{i+1}) \in \delta$. A *trace* is a finite sequence of statements. We call $trace(\rho) = st_0 ... st_{n-1}$ the trace associated with ρ. A run is accepting if its final state is in l_{exit} or l_{error}. We call a word $\pi \in \Sigma^*$ a trace of A if $\pi = trace(\rho)$ for some accepting run ρ of A.
We present the semantics of program automata using formulas in first-order logic. Let X be a fixed set of program variables. A program state s is a function that assigns a value $s(x)$ to each program variable $x \in X$. A *state formula* F is a first-order constraint over free variables from X. We write $s \Rightarrow F$ to denote that a state s satisfies a state formula F.
For a variable $x \in X$ and $i \in N$, we denote by $x^{<i>}$ the variable which models the value of x in a state that is shifted i times into the future. We extend this shift function from variables to sets of variables, as expected, and we denote by X' the set of variables $X^{<1>}$. For a formula F with free variables from Y, we write $F^{<i>}$ for the formula obtained by replacing each occurance of a variable $y \in Y$ in F with the variable $y^{<i>}$. A *transition formula* T is a first order constraint over free variables from $X \cup X'$, where variables X' denote the values of the variables from X in the next state. That is, a transition formula T represents a binary relation on states. We write $s, s' \Rightarrow T$ to denote that states s and s' satisfy the transition formula T. We assume that every statement $st \in \Sigma$ has an associated transition formula $TF(\sigma)$ that provides the semantics of st. For example the transition formula of an assume statement can be defined as the $TF(assume(F)) \equiv F \bigwedge X = X'$, where $X = X'$ stands for the conjunction of equalities $x = x'$ for all $x \in X$.

st	T[st]
assignment statement ($x := e$)	$x' = e \bigwedge \{X \backslash x\} = \{X' \backslash x'\}$
assume statement ($assume(cond)$)	$cond \bigwedge X = X'$
havoc statement $havoc(vars)$	$vars' \bigwedge \{X \backslash vars\} = \{X' \backslash vars'\}$

For a trace $\pi \in \Sigma^*$ with $\pi = st_0 st_1 ..... st_n$, we define its *trace formula* $TF(\pi)$ as the conjunction of the shifted transition formulas of the statements in π

$$TF(\pi) = TF(st_0) \bigwedge TF(st_1)^{<1>} \bigwedge ..... \bigwedge TF(st_n)^{<n>}$$

An ***execution*** σ of a trace π of length n is a sequence of states $s_0 .... s_n$ such that for all $0 \leq i \leq n$, $s_i, s_{i+1} \Rightarrow T[\pi[i]]$. We denote by $Execs(\pi)$ the set of all executions of π. A trace is called feasible if its trace formula is satisfiable, otherwise we call it infeasible.
A program is safe if all the feasible traces in the corresponding program automata don't have an error state as the end state. If a program is not safe, an error can be witnessed along a trace.
Weakest Precondition Operator: For some given formula $R \in Preds(X)$,

and a program statement st, the weakest precondition operator $wp()$ returns the weakest formula that must be true such that if we execute st, R holds.

$$wp(T[st], R) \wedge T[st] \Rightarrow R$$

$wp(st, R)$ is a predicate that characterizes all pre-states of st from which no execution will go wrong and from which every execution ends in a state satisfying R.

Error-Precondition: In a trace π that ends in an error state, an error-precondition can be defined as the following:

$$error\ precondition : \neg wp(TF[\pi], False)$$

Error & Error Trace: For an unsafe program, with a trace $\pi = st_0; .....st_{n-1};$ whose corresponding run's last state is an error state, an error precondition Ψ, a state formula ϕ, such that $TF[\pi[n-1]] = \phi$, we say that there is an ***error*** in the program if the following conditions hold :

1) $\Psi \wedge TF(\pi[0, n-2])$ is satisfiable.

2) $\Psi \wedge TF(\pi[0, n-2]) \wedge \phi^{<n-1>}$ is un-satisfiable.

In this case π is called an ***error trace***. Hence for an error trace π, no execution of the trace π that starts in a state satisfying the error pre-condition Ψ ends in an exit state.

3.2.2 DEFINITIONS FOR SCREEN SHOT:

Let π be an error trace. An execution of a trace 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.
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 $s_j \not\Rightarrow guard(\pi[j])$.
Relevancy of an assignment statement x:=t
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 $\beta \subsetneq \beta'$.

3.2.3 Non-Flow Sensitive Relevancy

An assignment statement is relevant in a trace if the assigned value matters for the reachibility of the error. If we are reaching the error [what does reaching the error means?] for any possible value, then the assignment is irrelevant.
We can begin to formally define relevancy by first making the following three observations:
1) If we start the execution ***[What is an execution ?]*** of an error trace from a state satisfying the error-precondition Ψ, then we will always end up in an error state.
2) If we start the execution of an error trace from a state which is not in the the error-precondition, then we can get ***stuck*** during the execution of the error trace. Getting stuck means that one of the assume statments is blocking the execution of the trace and the guard in one of the assume statements is not satisfied.
[Also define formally what it means to get stuck and what is an execution of an error trace]
3) If we start the execution of an error trace from a state satisfying the error-precondition and we replace an assignment statement in the error trace with a havoc statement and we get stuck, then that statement is a ***relevant statement***.
Consider the error trace below:

```
y := 3;
x := 1;
assume( y==3 )
```

Which we obtain from the following program:

```
foo()
{
  y := 3;
  x := 1;
  assert(y !=3 );
}
```

If we replace $y := 3$ by $hacov(y)$, then y can non-deterministically be assigned any value and there will be an execution for which assumption in the end $[y == 3]$ will not be satisfied and we won't be able to satisfy the error state.
On the other hand changing the statement $x := 1$ to $havoc(x)$ will have no effect on the assumption in the end. Hence it is not relevant.
[define Guard in the definitions section]

Definition 1 (Restrictivness of a statement)**.** *Let pre be a state formula, π a trace and i a position such that $\pi[i]$ is an assume statement. We call the assume statement $\pi[i]$* restricitve *iff :*

$$Post(\pi[0, i-1], pre) \not\Rightarrow guard(\pi[i])$$

Definition 2 (Relevancy of a statement)**.** *Let π be an error trace 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 π' be the trace which is obtained by replacing $\pi[i]$ by havoc(x). Let Ψ be the error precondition of π. The assignment statement $\pi[i]$ is relevant *if there exists some assume statement at position $j > i$ in π' such that $\pi'[j]$ is restrictive for π' and Ψ.*

Examples:

1)

Consider an Error Trace:

```
[x = 0]
[y = 0][*]
assume(y == 0)
[x = 1][*]
assume(x != 0)
```

That we get from the following program:

```
foo()
{
  x := 0;
  y := 0;
  if(y == 0)
  {
    x := 1;
  }
  assert(x == 0);
}
```

From the three assignment statements, if we change $[y = 0]$ to $havoc(y)$, then $assume(y == 0)$ becomes restrictive. Hence $[y = 0]$ is relevant. Same is the case with $[x = 1]$.

But on the other hand, $x := 0$ is not relevant because changing this statemnet to havoc is not making any assume statement restrictive.

2)

Consider an error trace:

```
[y = 0]  [*]
[z = 0]  [*]
assume(y == 0)
[x = 1]  [*]
assume(z == 0)
[z = 1]
assume( x != 0)
```

That we get from the following program:

```
foo()
{
  y := 0;
  z := 0;
  if(y == 0)
  {
    x := 1;
    if(z == 0)
    {
      z := 1;
    }
```

```
  }
  else
  {
    y := 2;
  }
  assert(x == 0);
}
```

Following is the list of assignment statements and assume statements that are becoming restrictive if the assignment statements are changed to havoc().
There are four assignment statements in the trace. If we change $z = 1$ to $havoc(z)$ then no assume statement is becoming restrictive and hence it is not relevant.
If we change $x = 1$ to $havoc(x)$ then $assume!(x = 0)$ becomes restrictive.
If we change $z := 0$ to $havoc(z)$ then $assume(z == 0)$ is becoming restrictive.
If we change $y := 0$ to havoc(y) then $assume(y == 0)$ is becoming restrictive.

Algorithm:

Let π be an error trace of length n, $WP()$ the weakest pre-condition operator, $\pi[i]$ the ith statement of π. Let $P = \neg WP(False; \pi[i, n])$ and $Q = \neg WP(False; \pi[i + 1, n])$. Where n is the length of the error trace. A statement $\pi[i]$ in an error trace π is relevant with respect to the non-flow sensitive criteria $(*)$ if the conjunction of the the three formulas $(P, \pi[i], Q)$ is unsatisfiable and $\pi[i]$ is in the unsatisfiable core.

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 equivilant(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 a statement st which is an assignment statement the following implication holds:*

$$WP(\neg Q, st) = \neg WP(Q, st)$$

Lemma 3. *For a predicate Q and an assignment statement of the form $x := t$ where x is the variable and t is the expression, the following implication holds:*

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

and by contraposition:

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

Lemma 4. *For predicates Q, Q' and P:*
If $Q \Rightarrow Q'$ and $P \not\Rightarrow WP(Q'; \pi)$, where π is a trace, then

$$P \not\Rightarrow WP(Q; \pi)$$

Proof. If $Q \Rightarrow Q'$, then $WP(Q; \pi) \Rightarrow WP(Q'; \pi)$.
If $P \not\Rightarrow WP(Q'; \pi)$ then certainly $P \not\Rightarrow WP(Q; \pi)$ since $WP(Q'; \pi)$ is stronger. □

Lemma 5 (nonempty post)**.** *If $P := WP(Q, x := t) \not\subseteq WP(Q, havoc(x))$ for some Q then $Q \subsetneq SP(P, havoc(x))$.*

Proof. We will show that $Q \equiv SP(P, x := t) \subseteq SP(P, havoc(x)) \not\subseteq Q$ from which it follows that the first inclusion is strict. The first inclusion is immediate from Lemma 3 (main document)[1]. By assumption $P \not\subseteq WP(Q, havoc(x))$, which by Lemma 1 (main document) is equivalent to the second part. □

Lemma 6 (restrictiveness)**.** *If the last statement of a trace π of length n is an assume statement and $P \Rightarrow WP(\bot, \pi)$, then $SP(P, \pi[0, j]) \not\Rightarrow guard(\pi[j])$ for some $1 \leq j \leq n$.*

Proof. Induction over n (length of π): For $n = 1$ we have $WP(\bot, \pi[0]) \equiv guard(\pi[1]) \Rightarrow \bot \equiv \neg guard(\pi[1])$. Now let $n > 1$ and let $Q := WP(\bot, \pi[1, n])$. By induction hypothesis $SP(Q, \pi[1, j]) \not\Rightarrow guard(\pi[j])$ for some j. If $\pi[0]$ is an assignment or havoc statement we just apply the hypothesis. If $\pi[0]$ is an assume statement then $P \equiv guard(\pi[1]) \Rightarrow Q$, so if $P \not\Rightarrow Q$ then $P \not\Rightarrow guard(\pi[1])$. □

Theorem 1 (Relevancy)**.** *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 $P = \neg WP(False, \pi[i, n])$ and $Q = \neg WP(False, \pi[i + 1, n])$. The statement $\pi[i]$ is relevant iff:*

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

Proof. Suppose we have an error trace π of length 2, where $\pi[0]$ is an assignment statement of the form $x := t$ and $\pi[1]$ is an assume statement where $guard(\pi[1])$ is the guard of the assume statement.
If we consider the assignment statment $\pi[0]$, P will be $\neg WP(\neg guard; x := t)$ and Q will be $guard(\pi[1])$.
" $\Rightarrow$ "
If the assignment statement $\pi[0]$ is relevant, then:

$$P \not\Rightarrow WP(Q, havoc(x)) \tag{1}$$

The relevancy of $\pi[0]$ implies that replacing $\pi[0]$ with $havoc(x)$ will result in the assume statement $\pi[1]$ getting restrictive.
i.e

$$SP(P; havoc(x)) \not\Rightarrow guard(\pi[1])$$

[1] We have to add it!

or by lemma(1)

$$P \not\Rightarrow WP(guard(\pi[1]); havoc(x))$$

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

" $\Leftarrow$ "

If

$$P \not\Rightarrow WP(Q, havoc(x)) \tag{2}$$

then the assignment statement $\pi[0]$ is relevant.
Substituting the values for P and Q

$$\neg WP(\neg guard(\pi[1]), x := t) \not\Rightarrow WP(guard(\pi[1]), havoc(x))$$

From lemma (2)

$$WP(guard(\pi[1]), x := t) \not\Rightarrow WP(guard(\pi[1]), havoc(x)) \tag{3}$$

From the "duality of WP and SP" (lemma 1), if in the above expression, we consider the right hand side of the implication as P, $guard(\pi[1])$ as Q and $havoc(x)$ as st, then we can write the above implication as:

$$SP(WP(guard(\pi[1]), x := t), havoc(x)) \not\Rightarrow guard(\pi[1]) \tag{4}$$

That means that from our supposed trace which contains one assignment statment and one assume statement with error precondition $WP(guard(\pi[1]), x := t)$, if we get a new trace where the assignment $x := t$ is replaced by $havoc(x)$, the strongest postcondition of the error precondition and $havoc(x)$ does not imply the guard of the assume statement. Which according to the definition of relevancy would mean that the statement $x := t$ is relevant.

Now we consider the case where the length of the trace is n and the first statment $\pi[0]$ of the trace π is an assignment statement. Let $\pi_s := \pi[1, n]$. If we consider the assignment statement $\pi[0]$, then $P := \neg WP(false; \pi)$, $Q := \neg WP(false, \pi_s)$. Let π' be the trace where the $\pi[0]$ is replaced with a havoc statement.
Let $P' := \neg WP(false; \pi') := WP(Q; havoc(x))$, and $Q' := SP(P; havoc(x))$.
Observe here that P can also be stated as $WP(Q; x := t)$
" $\Rightarrow$ "
If the assignment staement $\pi[0]$ is relevant, then:

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

i.e there exists some assume statement in the trace at position j, which is restrictive if we replace the assignment statement with a havoc statement.
i.e

$$SP(P; \pi'[0, j-1]) \not\Rightarrow guard(\pi'[j])$$

and consequently from lemma (1):

$$P \not\Rightarrow WP(guard(\pi'[j]); \pi'[0, j-1])$$

Or

$$P \not\Rightarrow WP(guard(\pi'[j]); \pi'[0], \pi'[1, j-1])$$

By the recursive definition of $WP()$

$$P \not\Rightarrow WP(WP(guard(\pi'[j]); \pi'[1, j-1]); \pi'[0]) \tag{5}$$

We also know that:

$$SP(Q; \pi'[1, j-1]) \Rightarrow guard(\pi'[j])$$

and consequently from lemma (1):

$$Q \Rightarrow WP(guard(\pi'[j]); \pi'[1, j-1]) \tag{6}$$

Let $WP(guard(\pi'[j]); \pi'[1, j-1]) := R$
Then (5) and(6)can be written as:

$$P \not\Rightarrow WP(R; \pi'[0])$$

$$Q \Rightarrow R$$

From Lemma (4)

$$P \not\Rightarrow WP(Q; havoc(x)) \tag{7}$$

" $\Leftarrow$ "
If

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

Then statement $x := t$ is relevant. By assumption and by definition of P:

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

By lemma (5) [DEFINE LEMMA 5 PLEASE !!!!] :

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

or

$$Q \subsetneq Q'$$

Let $R = Q' \setminus Q$ or $Q' = R \biguplus Q$ (disjoint union of R and Q).
Now we want to show a contradiction for the states in Q' but from

$$SP(X \cup Y; \pi) = SP(X; \pi) \cup SP(Y; \pi) \tag{8}$$

we can conclude that it suffices to show a contradiction for the states in R.
Let us assume that for all $1 \leq j \leq n$, statement $\pi'[j]$ is not restrictive. i.e

$$SP(Q'; \pi'[1, j-1]) \Rightarrow guard(\pi'[j]) \qquad \forall 1 \leq j \leq n$$

By equation (8) we can write:

$$SP(R; \pi'[1, j-1]) \Rightarrow guard(\pi'[j]) \qquad \forall 1 \leq j \leq n \tag{9}$$

We know that $R \Rightarrow \neg Q$ and hence

$$R \Rightarrow WP(false; \pi_s) \tag{10}$$

Considering (9) and (10) and lemma (6) we get a contradiction. That means that one of the assume statement is getting restrictive and hence the statement $x := t$ is relevant. $\square$

Algorithm 1: **nonFlow**(trace π)

Input: Trace π of length n.
Output: A list of relevant statements in the trace.

```
nonFlow(trace)
{
  formula wpList = [];
  relevantStatements =[];
  wpList.append(FALSE);
  for(i=n-1 to 0)
  {
    formula wp = WeakestPrecondition(last element of wpList, trace[
    i]);
    wpList.append(wp);
  }
  for(i=n-1 to 0)
  {
    formula pre = NEGATIVE(wpList[i+1])
    relevance = UNSATCORE(pre, trace[i],wpList[i]);
    if(relevance == "unsatisfiable" AND trace[i] is in
    unsatisfiable core)
    {
      relevantStatements.append(trace[i]);
    }

  }
  return(relevantStatements);
}
```

Taking example number 2 from above with the following error trace:

```
y := 0; [*]
z := 0; [*]
assume (y == 0);
x := 1; [*]
assume (z == 0);
z := 1;
assume !(x == 0);
```

In the above trace, for $i = 4$,

$\psi = \neg WP(False, \pi[4,7]) \implies z = 0$
$\pi[4] \implies x = 1$
$\phi = WP(False, \pi[5,7]) \implies x = 0 \vee \neg(z = 0)$

The formula $(\psi, \pi[4], \neg\phi)$ is unsatisfiable and $\pi[4]$ is in the unsatisfiable core. Hence $\pi[4]$ is relevant with respect to Non-Flow Sensitive relevance criterion and we therefore label it with a $[*]$.

3.2.4 Security Error/non-determinisitic assignment Relevancy (golden frame case):

A statement can be called a security error relevant(or a non-determinisitc assignment relevant) statement if it is a non-deterministic assignment statement and relevant for the reachability of the error.

Definition 3 (Relevancy of a statement)**.** *Let π be a feasible error trace and $\pi[i]$ be a $Havoc$ statement at position i having the form $havoc(x)$, where x is a variable. Let $x := t$ be an assignment statement where x is the same variable as in $havoc(x)$ and t is an expression. The havoc statement $\pi[i]$ is relevant if there exists an assignemnt $x := t$ such that if we replace the havoc in π with $x := t$ to get a new trace π', then the following implication holds:*

$$SP(true; \pi') \Rightarrow false$$

Algorithm

Let π be an error trace of length n, $WP()$ the weakest pre-condition operator, $\pi[i]$ the ith statement of π. Let $P = \neg WP(False, \pi[i, n])$ and $Q = WP(False, \pi[i+1, n])$, where n is the length of the error trace. A *havoc* statement $\pi[i]$ in an error trace π is relevant with respect to the non-flow sensitive criteria (@) if the conjunction of the the three formulas $(\psi, \pi[i], \neg\phi)$ is satisfiable.

Theorem 2 (Security Error Relevancy)**.** *Let π be an error trace of length n and $\pi[i]$ be a non-deterministic assignment statement at position i having the form $havoc(x)$, where x is a variable. Let P and Q be two predicates where $P = \neg WP(False, \pi[i, n])$ and $Q = \neg WP(False, \pi[i+1, n])$. The statement $\pi[i]$ is relevant iff:*

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

Proof:

Suppose we have an error trace of length 2 where $\pi[0]$ is a *havoc* statement of the form $havoc(x)$, where x is a variable and $\pi[1]$ an assume statement where $guard(\pi[1])$ is the guard of the assume statetment.
" $\Rightarrow$ "
If the *havoc* statement is relevant, then:

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

For the initial case P, will be $\neg WP(\neg guard, havoc(x))$, which is the error pre-condition of the trace and Q will be $guard$.
Hence we have to show the following:

$$\neg WP(\neg guard, havoc(x)) \not\Rightarrow WP(guard, havoc(x)) \tag{11}$$

We can show that the above implication does not hold, by showing that the right hand side is false and the left hand side is not.
If the statement is relevant, then

$$SP(true, \pi') \Rightarrow false$$

Which in the case of a trace of length 2 is equivalent to

$$SP(true, x := t) \Rightarrow \neg guard$$

By Lemma(1)

$$true \Rightarrow WP(\neg guard, x := t)$$

negating both sides

$$\neg WP(\neg guard, x := t) \Rightarrow false$$

By lemme(2)

$$WP(guard, x := t) \Rightarrow false$$

Hence,

$$WP(guard; x := t) = false$$

Lemma (3) states

$$WP(guard, havoc(x)) \Rightarrow WP(guard; x := t)$$

$$WP(guard; havoc(x)) \Rightarrow false$$

Since only false implies false, we get the result that

$$WP(guard, havoc(x)) = false$$

Which is the right hand side of the implication in (?). Since the left hand side of the implication in (?) is the error precondtion of a feasible error trace, it can not be empty or false.
Hence the implication in (?) does not hold.
" $\Leftarrow$ "
If

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

Then the statement $havoc(x)$ is relevant. Where P is $\neg WP(\neg guard; havoc(x))$ and Q is $guard$.
To show that a *havoc* statement is relevant we have to show that there exists an assignment $x := t$ which makes the error trace infeasible. That would imply that there exists a transition that ends up in the state $\neg guard$.
By definition of the $WP()$ operator.

- $WP(guard, havoc(x)) \rightarrow$ Set of states from which all transitions end up in $gurad$.
- $WP(\neg guard, havoc(x)) \rightarrow$ Set of states from which all transitions end up in $\neg guard$.

- $\neg WP(guard, havoc(x)) \rightarrow$ Set of states from which there exists atleast one transition that ends up in $\neg guard$.
- $\neg WP(\neg guard, havoc(x)) \rightarrow$ Set of states from which there exists atleast one transition that ends up in $guard$.

We know that

$$\neg WP(\neg guard; havoc(x)) \not\subseteq WP(guard; havoc(x))$$

The left hand side of the above inequality represent the set of states from which there is atleast one transition that goes to $guard$ and a transition that go to $\neg guard$. And the right hand side represents the set of states from which all transisitons go to $guard$.
Since the left hand side is the error precondition, the above inequality shows that there exist a state in the error precondition, which is not in the set represented by the right hand side and from which there exists a transition that ends up in $\neg guard$ making the error trace infeasible if we replace the error trace with that transition.

3.3 Flow Sensitive Relevance criteria

The definition of relevancy is actually similar to the non-flow sensitive case. The only thing different is that now we take branches in the trace into account. If there is a branch in the error trace, the relevancy of the statements inside the error trace will only be calculated if the branch as a whole is relevant to the error. We see that we can get slightly different results from the Non-Flow Sensitive case because it is possible that a statement might be relevant with respect to non-flow sensitive case but it lies inside a branch which is not relevant.
When we say that a branch $\pi[i, j]$ must be relevant to the error, we mean that the branch is reduced to a transition formula which we call a "$MarkhorFormula$" and it's relevancy is calculated in the same way as we did for a statement in the non-flow sensitive case (by checking if the conjunction of $(\psi, \pi[i], \neg\phi)$ is unsatisfiable and the statement is in the unsatisfiable core).

3.3.1 Markhor Formula

.
.
.

4 Performance Analysis

4.1 Non-Flow Sensitive Fault Localization:

I think our algorithm is more effected not by the size of the trace, but the size of the formulas in the trace. That's why, sometimes even for small traces, the

non-flow sensitive analysis is fast but it takes very long for flow-sensitive analysis to run, not because of the size of the trace , but the complexity of the formulas in it.
Therefore there might not be much we can do to increase the performance of non-flow sensitive analysis because there are not many steps involved and the formulas we compute here (wp, pre) are our most basic requirement to compute the relevance of a statement and their calculation cannot be further simplified.

5 Security Errors

A very interesting problem that we might be able to solve via our fault localization algorithm is to distinguish security error from all other kinds of errors. According to our current definition an error is a security error iff an input statement (network/user) can cause the program execution to reach the error. Following are the (current) criterion for a security error.
1. There is some reachable location where the program reads input.
2. There is some input value, such that continuing from this location we definitely reach the error
3. There is some input that continuing from this location we do not reach the error.
From condition 2 and 3 we can deduce that the input is somehow relevant for the error.
For example:

```
foo()
{
  int y;
  int x;
  x := 1;
  y := user_input();
  if(y==2)
  {
    y := y+1;
  }
  assert(y != 3);
}
```

In the above example, the input statement $y := user_input()$ determines if we reach the error state or not. Hence there is a security error in this program.

References

[1] J. Christ, E. Ermis, M. Schaf, and T. Wies. Flow-sensitive fault localization. In VMCAI, volume 7737, pages 189–208, Berlin, Heidelberg, 2013. Springer

[2] E.Ermis, M. Schaf, and T. Wies. Error Invariants. In FM'12, pages 338–353. Springer, 2012.

[3] M. Schaf, D. Schawrtz, T. Wies. Explaining Inconsistent Code. In Joint meeting of the European Software Engineering conference and the Symposium on the Foundations of Software Engineering, ESEC/FSE'13, pages: 521 - 531, Saint Petersburg, Russian Federation. August 18-26,2013

[4] https://courses.cs.washington.edu/courses/cse503/06sp/correctness2.pdf