Exploration of the scalability of LocFaults approach for error localization with While-loops programs
Mohammed Bekkouche

To cite this version:
Mohammed Bekkouche. Exploration of the scalability of LocFaults approach for error localization with While-loops programs. [Research Report] University of Nice-Sophia Antipolis, I3S/CNRS BP 121, 06903 Sophia Antipolis Cedex, France. 2015. <hal-01132781>

HAL Id: hal-01132781
https://hal.archives-ouvertes.fr/hal-01132781
Submitted on 18 Mar 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Exploration of the scalability of LocFaults approach for error localization with While-loops programs

Mohammed Bekkouche  
University of Nice-Sophia  
Antipolis, I3S/CNRS  
BP 121, 06903 Sophia  
Antipolis Cedex, France  
bekkouch@i3s.unice.fr

ABSTRACT
A model checker can produce a trace of counterexample, for an erroneous program, which is often long and difficult to understand. In general, the part about the loops is the largest among the instructions in this trace. This makes the location of errors in loops critical, to analyze errors in the overall program. In this paper, we explore the scalability capabilities of LocFaults, our error localization approach exploiting paths of CFG (Control Flow Graph) from a counterexample to calculate the MCDs (Minimal Correction Deviations), and MCSs (Minimal Correction Subsets) from each found MCD. We present the times of our approach on programs with While-loops unfolded $b$ times, and a number of deviated conditions ranging from 0 to $n$. Our preliminary results show that the times of our approach, constraint-based and flow-driven, are better compared to BugAssist, which is based on SAT and transforms the entire program to a Boolean formula, and further the information provided by LocFaults is more expressive for the user.

Categories and Subject Descriptors
D.3.3 [Language Constructs and features]: Constraints;  
D.2.5 [Testing and Debugging]: Debugging aids, Diagnostics, Error handling and recovery

General Terms
Verification, Algorithms, Experimentation

Keywords
Error localization, LocFaults, BugAssist, Off-by-one bug, Minimal Correction Deviations, Minimal Correction Subsets

1. INTRODUCTION
Errors are inevitable in a program, they can harm proper operation and have extremely serious financial consequences.

Thus it poses a threat to human well-being [17]. This link [3] cites recent stories of software bugs. Consequently, the debugging process (detection, localization and correction of errors) is essential. The location of errors is the step that costs the most. It consists of identifying the exact locations of suspicious instructions [18] to help the user to understand why the program failed, which facilitates him in the task of error correction. Indeed, when a program P is not conformed with its specification (P contains errors), a model checker can produce a trace of a counterexample, which is often long and difficult to understand even for experienced programmers. To solve this problem, we have proposed an approach [5] (named LocFaults) based on constraints that explores the paths of CFG (Control Flow Graph) of the program from the counterexample, to calculate the minimal subsets to restore the program’s compliance with its postcondition. Ensuring that our method is highly scalable to meet the enormous complexity of software systems is an important criterion for its quality [9].

Different statistical approaches for error localization have been proposed; e.g.: Tarantula [11] [10], Ochiai [1], AM-PLE [1], Pinpoint [6]. The most famous is Tarantula, which uses different metrics to calculate the degree of suspicion of each instruction in the program while running a battery of tests. The weakness of these approaches is that they require a lot of test cases, while our approach uses one counterexample. Another critical point in statistical approaches is that they require an oracle to decide if the result of a test case is correct or not. To overcome this problem, we consider the framework of Bounded Model Checking (BMC) which only requires a postcondition or assertion to check.

The idea of our approach is to reduce the problem of error localization to the one which is to compute a minimal set which explains why a CSP (Constraint Satisfaction Problem) is infeasible. The CSP represents the union of constraints of the counterexample, the program, and the assertion or the postcondition violated. The calculated set can be a MCS (Minimal Correction Subset) or a MUS (Minimal Unsatisfiable Subset). In general, test the feasibility of a CSP over a finite domain is a NP-complete problem (intractable)\(^1\), one of the most difficult NP problems. This means, explaining the infeasibility in a CSP is as hard or more (it can be classified as NP-hard problem).

\[^1\] If this problem could be solved in polynomial time, then all NP-complete problems would be too.
that satisfies all the constraints in \( C \) in Section 4. A brief description of our \texttt{LocFaults} treatment of erroneous loops, including the CSP.

2. \textbf{DEFINITIONS}

In this paper, we explore the scalability of \texttt{LocFaults} on programs with While-loops unfolded \( b \) times, and a number of deviated conditions ranging from 0 to 3.

The contribution of our approach against BugAssist can be summarized in the following points:

* We do not transform the entire program in a system of constraints, but we use the CFG of the program to collect the constraints of the path of counterexample and paths derivatives thereof, assuming that at most \( k \) conditionals may contain errors. We calculate MCSs only on the path of counterexample and paths that correct the program;

* We do not translate the program instructions into a SAT formula, instead numerical constraints that will be handled by constraint solvers;

* We do not use MaxSAT solvers as black boxes, instead a generic algorithm to calculate MCSs by the use of a constraint solver;

* We limit the size of the generated MCSs and the number of deviated conditions;

* We can work together more solvers during the localization process and take the most efficient according to the category of CSP constructed. For example, if the CSP of the path detected is of type linear over integers, we use a MIP (Mixed Integer Programming) solver; if it is nonlinear, we use a CP (Constraint Programming) solver and/or as well as MINLP (Mixed Integer Nonlinear Programming).

Our practical experience has shown that all these restrictions and distinctions enable \texttt{LocFaults} to be faster and more expressive.

The paper is organized as follows. Section 2 introduces the definition of MUS and MCS. In Section 3, we define the problem \( \leq k\)-MCD. We explain a paper contribution for the treatment of erroneous loops, including the \texttt{Off-by-one} bug, in Section 4. A brief description of our \texttt{LocFaults} algorithm is provided in Section 5. The experimental evaluation is presented in Section 6. Section 7 talks about the conclusion and future work.

2. \textbf{DEFINITIONS}

In this section, we introduce the definition of an IIS/MUS and MCS.

\textbf{CSP}.

A CSP (Constraint Satisfaction Problem) \( P \) is defined as a triple \( < X, D, C > \), where:

* \( X \) a set of \( n \) variables \( x_1, x_2, ..., x_n \).

* \( D \) the tuple \( < D_{x_1}, D_{x_2}, ..., D_{x_n} > \). The set \( D_{x_i} \) contains the values of the variable \( x_i \).

* \( C=\{c_1, c_2, ..., c_n\} \) is the set of constraints.

A solution for \( P \) is an instantiation of the variables \( I \in D \) that satisfies all the constraints in \( C \). \( P \) is infeasible if it has no solutions. A sub-set of constraints \( C' \) in \( C \) is also said infeasible for the same reason except that it is limited to the constraints in \( C' \).

We denote as:

* \( \text{Sol}(< X, C', D >) = \emptyset \), to specify that \( C' \) has no solutions, so it is infeasible.

* \( \text{Sol}(< X, C', D >) \neq \emptyset \), to specify that \( C' \) has at least one solution, so it is feasible.

We say that \( P \) is linear and denote LP (Linear Program) iff all constraints in \( C \) are linear equations/inequalities, it is continuous if the domain all variables is real. If at least one of the variables in \( X \) is integer or binary (Special cases of an integer), and the constraints are linear, \( P \) is called a program linear mixed MIP (Mixed-integer linear program). If the constraints are nonlinear, we say that \( P \) is a program nonlinear NLP (NonLinear Program).

Let \( P = < X, D, C > \) an infeasible CSP, we define for \( P \):

\textbf{IS}.

An IS (Inconsistent Set) is an infeasible subset of constraints in the constraint set infeasible \( C \). \( C' \) is an IS iff:

* \( C' \subseteq C \).

* \( \text{Sol}(< X, C', D >) = \emptyset \).

\textbf{IIS or MUS}.

An IIS (Irreducible Inconsistent Set) or MUS (Minimal Unsatisfiable Subset) is an infeasible subset of constraints of \( C \), and all its strict subsets are feasible. \( C' \) is an IIS iff:

* \( C' \) is an IS.

* \( \forall C'' \subseteq C \). \( \text{Sol}(< X, C'', D >) \neq \emptyset \), (each of its parts contributes to the infeasibility), \( C'' \) is called irreducible.

\textbf{MCS}.

\( C' \) is a MCS(Minimal Correction Set) iff:

* \( C' \subseteq C \).

* \( \text{Sol}(< X, C' \setminus C', D >) \neq \emptyset \).

* \( \exists C'' \subseteq C' \) such as \( \text{Sol}(< X, C \setminus C'', D >) \neq \emptyset \).

3. \textbf{THE PROBLEM \( \leq k\)-MCD}

Given an erroneous program modeled in CFG\(^2 \) \( G = (C, A, E) \): \( C \) is the set of conditional nodes; \( A \) is the set of assignment blocks; \( E \) is the set of arcs, and a counterexample. A MCD (Minimal Correction Deviation) is a set \( D \subseteq C \) such as the propagation of the counterexample on all the instructions of \( G \) from the root, while having denied each condition\(^3 \) in \( D \), allows the output to satisfy the postcondition. It is called minimal (or irreducible) in the sense that no element can be removed from \( D \) without losing this property. In other

\(^2\) We use Dynamic Single Assignment (DSA) form [2] transformation that ensures that each variable is assigned only once on each path of the CFG.

\(^3\) The condition is denied to take the branch opposite to that where we had to go.
words, $D$ is a minimal program correctness in the set of conditions. The size of minimal deviation is its cardinal. The problem $\leq k$-MCD is to find all MCDs of size smaller or equal to $k$.

For example, the CFG of the program AbsMin (see fig. 2) has one minimal size deviation 1 for the counterexample $\{i = 0, j = 1\}$. Certainly, the deviation $\{0 \leq j_0 \land k_1 = 1 \land i_0 \neq j_0\}$ corrects the program, but it is not minimal; only one minimal correction deviation for this program is $\{k_1 = 1 \land i_0 \neq j_0\}$.

The table 1 summarizes the progress of LocFaults for the program AbsMin, with at most 2 conditions deviated from the following counterexample $\{i = 0, j = 1\}$.

We display the conditions deviated, if they are minimal deviation or non minimal, and the calculated MCSs from the constructed constraint system : see respectively the columns 1, 2 and 3. Column 4 shows the figure illustrating the path explored for each deviation. In the first and the third column we show in addition of the instruction, its line in the program. For example, the first line in the table shows that there is a single MCS found $\{(r_1 = i_0 - j_0 : 15)\}$ on the path of the counterexample.

### 4. ERROR LOCALIZATION IN LOOPS

As part of Bounded Model Checking (BMC) for programs, unfolding can be applied to the entire program or it can be applied to loops separately [9]. Our algorithm LocFaults [4] [5] for error localization is placed in the second approach: that is to say, we use a bound $b$ to unfold loops by replacing them with conditional statements nested of depth $b$. Consider for instance the program Minimum (see fig. 7), containing a single loop, that calculates the minimum in an array of integers. The effect on control flow graph of the program Minimum before and after unfolding is illustrated in Figures 7 and 8 respectively. The While-loop is unfolded 3 times, as 3 is the number of iterations needed for the loop to calculate the minimum value in an array of size 4 in the worst case.

LocFaults takes as input the CFG of the erroneous program, $CE$ a counterexample, $b_{med}$: a bound on the number of deviated conditions, $b_{med}$: a bound on the size of MCSs calculated. It allows to explore the CFG in depth by diverting at most $b_{med}$ conditions from the path of the counterexample:

* It propagates $CE$ on the CFG until the postcondition. Then it calculates the MCSs on the CSP of the path generated to locate errors on the path of counterexample.

* It seeks to enumerate the sets $\leq b_{med}$-MCD. For each found MCD, it calculates the MCSs on the path that arrives at the last deviated condition and allows to take the path of the deviation.

Among the most common errors associated with loops according to [14], the Off-by-one bug, i.e. loops that iterate one too many or one too few times. This may be due to improper initialization of the loop control variables, or an erroneous condition of the loop. The program Minimum presents a case of this type of error. It is erroneous because of its loop While, the falsified instruction is on the condition of the loop (line 9): the correct condition should be $(i < tab.length)$ (tab.length is the number of elements of the table tab). From the following counterexample
### Table 2: Paths and MCSs generated by LocFaults for the program Minimum.

<table>
<thead>
<tr>
<th>PATH</th>
<th>MCSs</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ ( c \in \mathbb{E} \colon</td>
<td>tab[0]</td>
</tr>
</tbody>
</table>

\{ \( \{ \( ( \{ i \colon tab[i] = 2 \} \land |tab[i]| = 2 \} \land |tab[2]| = 1 \) \} \land \( \{ tab[0][3] \) \( = \) \( 0 \), \( min_0 = tab[0][0] \), \( i_0 = 1 \), \( min_1 = tab[0][i], i_1 = i_0 + 1, min_2 = tab[0][i_1], i_2 = i_1 + 1 \) | \( \{ i_0 = 1 \), \( i_1 = i_0 + 1 \), \( i_2 = i_1 + 1 \) \} |

---

### Figure 7: The program Minimum and its normal CFG (non unfolded).

The postcondition is \( \{ \forall \text{ int } k \colon (k \geq 0 \land k < |tab.length|) ; tab[k] \geq min \} \). We show in table 2 erroneous paths generated (column PATH) and the MCSs calculated (column MCSs) for at most 1 condition deviated from the conduct of the counterexample. The first line concerns the path of counterexample; the second for the path obtained by deviating the condition \( \{ i_2 \leq tab[0].length - 1 \} \).

LocFaults identifies a single MCS on the path of counterexample that contains the constraint \( min_2 = tab[0][i_1] \), the instruction of the line 11 in the second iteration of the loop unfolded. With a deviated condition, the algorithm suspects the third condition of the unfolded loop \( i_2 < tab[0].length - 1 \); in other words, we need a new iteration to satisfy the postcondition.

This example shows a case of a program with an incorrect loop: the error is on the stopping criterion, it does not allow the program to iterate until the last element of the array input. LocFaults with its deviation mechanism is able to detect this type of error accurately. It provides the user not only suspicious instructions in the loop not unfolded on the original program, but also information about the iterations where they are in the unfolded loop. This information could be very useful for the programmer to understand the errors in the loop.

### 5. Algorithm

Our goal is to find MCDs of size less than a bound \( k \); in other words, we try to give a solution to the problem posed above (\( \leq k \cdot \text{MCD} \)). For this, our algorithm (named LocFaults) explores in depth the CFG and generates the paths where at most \( k \) conditions are deviated from the conduct of the counterexample.

To improve efficiency, our heuristic solution proceeds incrementally. It successively deviates from 0 to \( k \) conditions and search the MCSs for the corresponding paths. However, if in step \( k \) LocFaults deviates a condition \( c_i \) and that it has corrected the program, it does not explore in step \( k' \) with \( k' > k \) paths that involve a deviation from the condition \( c_i \). For this, we add the cardinality of the found minimum deviation \( k \) as information on the node of \( c_i \).

We will illustrate with an example of our approach, as seen in the graph in Figure 9. Each circle in the graph represents a conditional node visited by the algorithm. The example does not show the block of assignments because we want to
illustrate just how we find the minimal correction deviations of a bounded size as mentioned above. An arc connecting a condition $c_1$ to another $c_2$ illustrates that $c_2$ is reached by the algorithm. There are two ways related to the behavior of the counterexample, where LocFaults reaches the condition $c_2$:

1. by following the branch induced by the condition $c_1$;
2. by following the opposite branch.

The value of the label of arcs for case (1) (resp. (2)) is "next" (resp. "devie").

### 6. PRACTICAL EXPERIENCE

To evaluate the scalability of our method, we compared its performance with that of BugAssist\(^4\) on two sets benchmarks\(^5\).

- The first benchmark is illustrative, it contains a set of programs without loops;
- The second benchmark includes 19, 48 and 91 variations for respectively the programs BubbleSort, Sum and SquareRoot. These programs contain loops to study the scalability of our approach compared to BugAssist. To increase the complexity of a program, we increase the number of iterations in loops in the execution of each tool; we use the same bound of unfolding loops for LocFaults and BugAssist.

To generate the CFG and the counterexample, we use the tool CPBPV [8] (Constraint-Programming Framework for Bounded Program Verification). LocFaults and BugAssist work respectively on Java and C programs. For a fair comparison, we built two equivalent versions for each program:

- a version in Java annotated by a JML specification;
- a version in ANSI-C annotated by the same specification but in ACSL.

Both versions have the same numbers of lines of instructions, including errors. The precondition specifies the counterexample used for the program.

To calculate the MCSs, we used IBM ILOG MIP\(^6\) and CP\(^7\) solvers of CPLEX. We adapted and implemented the algorithm of Lifiton and Sakallah [15], see alg. 1. This implementation takes as input the infeasible set of constraints corresponding to the identified path (C), and $b_{mcs}$: the bound on the size of calculated MCSs. Each constraint $c_i$ in the system built $C$ is augmented by an indicator $y_i$ for giving $y_i \rightarrow c_i$ in the new system of constraints $C'$. Assign to $y_i$ the value True implies the constraint $c_i$; however, assign to $y_i$ value False implies the removal of the constraint $c_i$. A MCS is obtained by seeking an assignment that satisfies the constraint system with a minimal set of constraints indicators affected with False. To limit the number of constraints indicators that can be assigned with False, we use the constraint $\text{AtMost}(-y_1, -y_2, ..., -y_n, k)$ (see the line 5), the created system is noted in the algorithm $C'_b$ (line 5). Each iteration of the WHILE-loop (lines 6 - 19) is allowed to find all MCSs of size $k$, $k$ is incremented by 1 after each iteration. After finding each MCS (lines 8 - 13), a blocking constraint is added to $C'_b$ and $C'$ to prevent finding this new MCS in the next iterations (lines 15 - 16). The first loop (lines 4 - 19) is iterated until all MCSs of $C$ are generated ($C'$ becomes infeasible); it can also stop if the MCSs of size smaller or equal to $b_{mcs}$ are obtained ($k > b_{mcs}$).

\(^4\)The tool BugAssist is available at: [http://bugassist.mpi-sws.org/](http://bugassist.mpi-sws.org/)
\(^5\)The source code for all programs is available at: [http://www.i3s.unice.fr/~bekkouch/Benchs_Mohammed.html](http://www.i3s.unice.fr/~bekkouch/Benchs_Mohammed.html)
BugAssist uses the tool CBMC [7] to generate the faulty trace and input data. For Max-SAT solver, we used MSUnCore2 [16].

The experiments were performed with a processor Intel Core i7-3720QM 2.60 GHz with 8 GO of RAM.

6.1 Benchmark without loops

This part serves to illustrate the improvement in LocFaults to reduce the number of subsets of suspects instructions provided to the user: at a given step of the algorithm, the node in the CFG of the program that allows detect a MCD will be marked by the cardinality of the latter; in the next steps, the algorithm will not allow scanning an adjacency list of this node.

Our results8 show that LocFaults misses errors only for TritypeKO6. While BugAssist misses errors for AbsMinusKO2, AbsMinusKO3, AbsMinusV2KO2, TritypeKO, TriPerimetreKO, TriMultPerimetreKO and one of two errors in TritypeKO5. The times 9 of our tool are better compared to BugAssist for programs with numerical calculation; they are close for the rest of programs.

We randomly take three programs as examples. And we consider the implementation of two versions of our algorithm with and without marking nodes named respectively LocFaultsV1 and LocFaultsV2.

- Tables 3 and 4 show respectively the suspects sets and times of LocFaultsV1;
- Tables 5 and 6 show respectively the suspects sets and times of LocFaultsV2.

In tables 3 and 5, we display the list of calculated MCSs and MCDs. The line number corresponding to the condition

is underlined. Tables 4 and 6 give calculation times: P is the pretreatment time which includes the translation of Java program into an abstract syntax tree with JDT tool (Eclipse Java development tools), as well as the construction of CFG; L is the time of the exploration of CFG and calculation of MCSs.

LocFaultsV2 has significantly reduced the deviations generated and the time summing exploration of the CFG and calculation of MCSs by LocFaultsV1, without losing the error; the localizations provided by LocFaultsV2 are more relevant. The eliminated lines of the table 5 are colored blue in the table3. The improved time are shown in bold in the table 4. For example, for the program TritypeKO2, at step 1 of the algorithm, LocFaultsV2 marks the node of condition 26, 35 and 53 (from the counterexample, the program becomes correct by deviating each of these three conditions). This allows, at step 2, to cancel the following deviations: {26, 32, 35}, {29, 35}, {32, 35}. Always in step 2, LocFaultsV2 detects two minimal correction deviations more: {29, 35}, {32, 44}, the nodes 57 and 44 will be marked (the value of the mark is 2). At step 3, no deviation is selected; for example, {29, 32, 44} is not considered because its cardinal is strictly superior to the mark value of the node 44.

<table>
<thead>
<tr>
<th>Program</th>
<th>LocFaultsV2</th>
<th>LocFaultsV1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>P</td>
<td>L</td>
</tr>
<tr>
<td>TritypeKO2</td>
<td>0.471</td>
<td>0.291</td>
</tr>
<tr>
<td>TritypeKO4</td>
<td>0.476</td>
<td>0.294</td>
</tr>
<tr>
<td>TriPerimetreKO</td>
<td>0.487</td>
<td>0.309</td>
</tr>
</tbody>
</table>

Table 4: Computation time, for the results without marking of nodes in the CFG

<table>
<thead>
<tr>
<th>Program</th>
<th>LocFaultsV2</th>
<th>LocFaultsV1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>P</td>
<td>L</td>
</tr>
<tr>
<td>TritypeKO2</td>
<td>0.496</td>
<td>0.292</td>
</tr>
<tr>
<td>TritypeKO4</td>
<td>0.481</td>
<td>0.286</td>
</tr>
<tr>
<td>TriPerimetreKO</td>
<td>0.485</td>
<td>0.304</td>
</tr>
</tbody>
</table>

Table 6: Computation time, for the results with marking of nodes in the CFG

6.2 Benchmarks with loops

These benchmarks are used to measure the scalability of LocFaults compared to BugAssist for programs with loops, depending on the increase of unfolding b. We took three programs with loops : BubbleSort, Sum, and SquareRoot. We have caused the Off-by-one bug in each of them. The benchmark for each program is created by increasing the number of unfolding b. b is equal to the number of iterations through the loop in the worst case. We also vary the number of deviated conditions for LocFaults from 0 to 3.

We used the MILP solver of CPLEX for BubbleSort. For Sum and SquareRoot, we collaborate the two solvers of CPLEX (CP and MIP) during the localization process. Indeed, during the collection of constraints, we use a variable to keep the information on the type of building CSP. When LocFaults detects an erroneous path10 and prior to the calculation of MCSs, it takes the good solver depending on the type of CSP corresponding to this path: if it is non-linear, it uses the CP OPTIMIZER solver; otherwise it uses the MIP solver.

10An erroneous path is the one on which we identify MCSs.
### Table 3: MCs and deviations identified by LocFaults for programs without loops, without marking of nodes in the CFG

<table>
<thead>
<tr>
<th>Program</th>
<th>Counterexample</th>
<th>Errors (LocFaults)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>(5)</td>
<td>1, 4</td>
</tr>
<tr>
<td>(b)</td>
<td>(6)</td>
<td>2, 2</td>
</tr>
</tbody>
</table>

### Table 4: MCs and deviations identified by LocFaults for programs without loops, with marking of nodes in the CFG

<table>
<thead>
<tr>
<th>Program</th>
<th>Counterexample</th>
<th>Errors (LocFaults)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)</td>
<td>(5)</td>
<td>1, 4</td>
</tr>
<tr>
<td>(b)</td>
<td>(6)</td>
<td>2, 2</td>
</tr>
</tbody>
</table>
For each benchmark, we presented an extract of the table containing the computation time\(^\text{11}\) (columns \(P\) and \(L\) show respectively the time of pretreatment and calculating of MCs), and the graph which corresponds to the time of calculation of MCs.

### 6.2.1 BubbleSort benchmark

BubbleSort is an implementation of the bubble sort algorithm. This program contains two nested loops; its average complexity is \(O(n^2)\), where \(n\) is the size of the table sorted: the bubble sort is considered among the worst sort algorithms. The erroneous statement in the program causes the program to sort input array by considering only its \(n - 1\) first elements. The malfunction of BubbleSort is due to the insufficient number of iterations performed by the loop. This is due to the faulty initialization of the variable \(i\): \(i = \text{tab.length} - 1\); the instruction should be \(i = \text{tab.length}\).

Table 7: Computation time for benchmark BubbleSort

<table>
<thead>
<tr>
<th>Programs</th>
<th>(b)</th>
<th>LocFaults</th>
<th>BugAssist</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(P)</td>
<td>(L)</td>
</tr>
<tr>
<td>V0</td>
<td>4</td>
<td>0.011</td>
<td>0.081</td>
</tr>
<tr>
<td>V1</td>
<td>5</td>
<td>0.511</td>
<td>0.888</td>
</tr>
<tr>
<td>V2</td>
<td>6</td>
<td>1.968</td>
<td>1.575</td>
</tr>
<tr>
<td>V3</td>
<td>7</td>
<td>4.154</td>
<td>0.904</td>
</tr>
<tr>
<td>V4</td>
<td>8</td>
<td>8.542</td>
<td>6.509</td>
</tr>
<tr>
<td>V5</td>
<td>9</td>
<td>1.457</td>
<td>18.79</td>
</tr>
<tr>
<td>V6</td>
<td>10</td>
<td>9.341</td>
<td>25.745</td>
</tr>
<tr>
<td>V7</td>
<td>11</td>
<td>0.918</td>
<td>69.895</td>
</tr>
</tbody>
</table>

Table 8: MCD and MCSs calculated by LocFaults for SquareRoot.

<table>
<thead>
<tr>
<th>(n)</th>
<th>MCD</th>
<th>MCSs</th>
</tr>
</thead>
<tbody>
<tr>
<td>(9 : 2)</td>
<td>[5, 9]</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>(9 : 3)</td>
<td>[7, 9 : 4]</td>
<td>({9 : 5})</td>
</tr>
<tr>
<td>(9 : 4)</td>
<td>(\emptyset)</td>
<td>[9 : 5, 9 : 6]</td>
</tr>
</tbody>
</table>

The times of LocFaults and BugAssist for the benchmark BubbleSort are presented in the table 7. The graph illustrates the increase in times of different versions of LocFaults and of BugAssist depending on the number of unfolding given in Figure 10.

The runtime of LocFaults and of BugAssist grows exponentially with the number of unfoldings; the times of BugAssist are always the greatest. We can consider that BugAssist is ineffective for this benchmark. The different versions of LocFaults (with at most 3, 2, 1, and 0 conditions deviated) remain usable up to a certain unfolding. The number of unfolding beyond which growth time of BugAssist becomes prohibitory is lower than that of LocFaults, that of LocFaults with at most 2 conditions deviated which is also lower than that of LocFaults with at most 1 conditions deviated. The times of LocFaults with at most 1 and 0 conditions deviated are almost the same.

### 6.2.2 SquareRoot and Sum benchmarks

The program SquareRoot (see fig. 11) permits to find the integer part of the square root of the integer 50. An error is injected at the line 13, which leads to return the value 8; while the program must return 7. This program has been used in the paper describing the approach BugAssist, it contains a linear numerical calculation in its loop and nonlinear in its postcondition.

![Figure 11: The program SquareRoot](https://example.com/square_root_program.png)

With an unwinding limit of 50, BugAssist calculates for this program the following suspicious instructions: \(\{9, 10, 11, 13\}\). The time of localization is 36, 16s and the pretreatment time is 0, 12s.

LocFaults displays a suspicious instruction by indicating both its location in the program (instruction line), the line of the condition and the iteration of each loop leading to this instruction. For example, \(\{9 : 2.11\}\) corresponds to the instruction that is on line 11 in the program, the latter is in a loop whose line of the stop condition is 9 and the iteration number is 2. The sets suspected by LocFaults are provided in the table 8.
The pretreatment time is 0.769s. The time during the exploration of the CFG and the calculation of MCSs is 1.299s. We studied the times of LocFaults and BugAssist of values of val ranging from 10 to 100 (the number of unfolding b used is equal to val), to study the combinatorial behavior of each tool for this program.

<table>
<thead>
<tr>
<th>Programs</th>
<th>b</th>
<th>LocFaults</th>
<th>BugAssist</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0</td>
<td>10</td>
<td>1.000</td>
<td>0.067</td>
</tr>
<tr>
<td>V10</td>
<td>10</td>
<td>0.721</td>
<td>0.543</td>
</tr>
<tr>
<td>V20</td>
<td>10</td>
<td>0.731</td>
<td>1.117</td>
</tr>
<tr>
<td>V30</td>
<td>10</td>
<td>0.760</td>
<td>1.220</td>
</tr>
<tr>
<td>V40</td>
<td>10</td>
<td>0.760</td>
<td>1.281</td>
</tr>
<tr>
<td>V50</td>
<td>10</td>
<td>0.734</td>
<td>1.294</td>
</tr>
<tr>
<td>V60</td>
<td>10</td>
<td>0.741</td>
<td>1.320</td>
</tr>
<tr>
<td>V70</td>
<td>10</td>
<td>0.760</td>
<td>1.400</td>
</tr>
<tr>
<td>V80</td>
<td>10</td>
<td>0.744</td>
<td>1.400</td>
</tr>
<tr>
<td>V90</td>
<td>10</td>
<td>0.760</td>
<td>1.510</td>
</tr>
</tbody>
</table>

Table 9: The computation time for the benchmark SquareRoot

<table>
<thead>
<tr>
<th>Programs</th>
<th>b</th>
<th>LocFaults</th>
<th>BugAssist</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0</td>
<td>6</td>
<td>0.760</td>
<td>0.427</td>
</tr>
<tr>
<td>V10</td>
<td>6</td>
<td>0.766</td>
<td>0.543</td>
</tr>
<tr>
<td>V20</td>
<td>6</td>
<td>1.117</td>
<td>1.117</td>
</tr>
<tr>
<td>V30</td>
<td>6</td>
<td>1.220</td>
<td>1.220</td>
</tr>
<tr>
<td>V40</td>
<td>6</td>
<td>1.349</td>
<td>1.349</td>
</tr>
<tr>
<td>V50</td>
<td>6</td>
<td>1.400</td>
<td>1.400</td>
</tr>
<tr>
<td>V60</td>
<td>6</td>
<td>1.439</td>
<td>1.439</td>
</tr>
<tr>
<td>V70</td>
<td>6</td>
<td>1.499</td>
<td>1.499</td>
</tr>
<tr>
<td>V80</td>
<td>6</td>
<td>1.552</td>
<td>1.552</td>
</tr>
<tr>
<td>V90</td>
<td>6</td>
<td>1.605</td>
<td>1.605</td>
</tr>
</tbody>
</table>

Table 10: The computation time for the benchmark Sum

The program Sum takes a positive integer n from the user, and it calculates the value of \( \sum_{i=1}^{n} i \). The precondition specifies that sum. The error in Sum is in the condition of its loop. It causes to calculate the sum \( \sum_{i=1}^{n-1} i \) instead of \( \sum_{i=1}^{n} i \). This program contains linear numerical instructions in the core of the loop, and a nonlinear postcondition.

The results in time for SquareRoot and Sum benchmarks are shown in the tables respectively 9 and 10. We also designed the graph that corresponds to the result of each benchmark, see respectively the graphs in Figure 12 and 13. The execution time of LocFaults grows rapidly; the times of LocFaults are almost constant. The times of LocFaults with at most 0, 1, and 2 conditions deviated are similar to those of LocFaults with at most 3 conditions deviated.

7. CONCLUSION

The method LocFaults detects the suspicious subsets by analyzing the paths of the CFG to find the MCDs and MCSs from each MCD; it uses constraint solvers. The method BugAssist calculates the merger of MCSs of the program by transforming the whole program into a Boolean formula; it uses Max-SAT solvers. Both methods work by starting from a counterexample. In this paper, we presented an exploration of scalability of LocFaults, particularly on the treatment of loops with the Off-by-one bug. The first results show that LocFaults is more effective than BugAssist on programs with loops. The times of BugAssist rapidly increase with the number of unfolding.

As part of our future work, we plan to validate our results on programs with more complex loops. We envisage to compare the performance of LocFaults with existing statistical methods. To improve our tool, we develop an interactive ver-
sion that provides the suspect subsets, one after the other: we want to take advantage of the user’s knowledge to select the conditions that should be deviated. We also reflect on how to extend our method to treat numerical instructions with calculation on floating-point.

8. ACKNOWLEDGMENTS

Thanks to Bertrand Neveu for his careful reading and helpful comments on this paper. Thanks to Michel Rueher and Hélène Collavizza for their interesting remarks. Thanks to You Li for his remarks on English mistakes.

9. REFERENCES


