Improving Error Discovery Using Guided Model Checking

Neha Shyam Rungta
Brigham Young University - Provo

Follow this and additional works at: https://scholarsarchive.byu.edu/etd

Part of the Computer Sciences Commons

BYU ScholarsArchive Citation
Rungta, Neha Shyam, "Improving Error Discovery Using Guided Model Checking" (2006). All Theses and Dissertations. 782.
https://scholarsarchive.byu.edu/etd/782
This thesis has been read by each member of the following graduate committee and by majority vote has been found to be satisfactory.

Date

__________________________

Eric G. Mercer, Chair

Date

__________________________

Michael D. Jones

Date

__________________________

Kevin D. Seppi
As chair of the candidate’s graduate committee, I have read the thesis of Neha S. Rungta in its final form and have found that (1) its format, citations, and bibliographical style are consistent and acceptable and fulfill university and department style requirements; (2) its illustrative materials including figures, tables, and charts are in place; and (3) the final manuscript is satisfactory to the graduate committee and is ready for submission to the university library.

Date

Eric G. Mercer
Chair, Graduate Committee

Accepted for the
Department

Parris K. Egbert
Graduate Coordinator

Accepted for the
College

Thomas W. Sederberg
Associate Dean, College of Physical and Mathematical Sciences
ABSTRACT

IMPROVING ERROR DISCOVERY USING GUIDED MODEL CHECKING

Neha S. Rungta
Department of Computer Science
Master of Science

State exploration in directed software model checking is guided using a heuristic function to move states near errors to the front of the search queue. Distance heuristic functions rank states based on the number of transitions needed to move the current program state into an error location. Lack of calling context information causes the heuristic function to underestimate the true distance to the error; however, inlining functions at call sites in the control flow graph to capture calling context leads to exponential growth in the computation. This paper presents a new algorithm that implicitly inlines functions at call sites to compute distance data with unbounded calling context that is polynomial in the number of nodes in the control flow graph. The new algorithm propagates distance data through call sites during a depth-first traversal of the program. We show in a series of benchmark examples that the new heuristic function with unbounded distance data is more efficient than the same heuristic function that inlines functions up to a certain depth.
I am greatly thankful and indebted to my advisor, Dr. Eric G Mercer for his assistance, guidance, patience, and encouragement throughout the development of this work. Whenever I presented him with an idea, his ability to quickly find errors, and instinctively take the idea to the next level has contributed immensely to the success and completion of this work. I would also like to thank Dr. Mike Jones for always taking the time to provide constructive feedback and comments. I express my sincere gratitude to him for it.

Among my current and past co-workers, I would like to thank Joel Self for fixing and patching our code base, sometimes even at the cost of delaying his own research. His efforts have helped me immensely in gathering experimental results for my research. I thank Peter Lamborn for introducing me to guided heuristics and mentoring me in the early stages of my research. I am grateful to all my other lab-mates especially Rahul Kumar, Joseph Edelman and Tonglaga Bao for their kindness and support. I would like to extend my heartfelt thanks to my friends Devlin Daley and Terry Wilcox for always being there for me. Their support and friendship has meant a lot to me in the past four years.

Finally, I express my sincere thanks to my family: Shyam, Kusum, Vandana, and Hemant Rungta for their love, support, and sacrifice which made it possible for me to achieve this success.
Contents

1 Introduction 1
   1.1 Motivating Example 3

2 Thesis Statement 9

3 Full Context Aware (FCA) Algorithm 11

4 EFSM with FCA 19

5 Results 23

6 Conclusion and Future Work 29
List of Figures

1.1 A program and analysis demonstrating underestimation in the EFSM heuristic due to bounded calling context. (a) A program with a nested call depth of four. (b) An one-bounded CFG for the program that inlines procedures at call sites. (c) The run-time stack for a given state of the program. ....................................................... 4

1.2 Pseudo-code for the EFSM algorithm. ....................................................... 6

3.1 Execution of the FCA on a set of CFGs. (a) A set of two CFGs for a software artifact. (b) The CFG for sub1 annotated with $d_{end}$ and $d_{error}$ data. (c) Distance matrix $L$ for main before and after shortest-path analysis. (d) The CFG for main annotated with $d_{end}$ and $d_{error}$ data. 17

3.2 Pseudo-code for the FCA algorithm. ....................................................... 18

4.1 The CFGs for the program in Fig. 1.1(a) annotated with context aware distances after running the FCA algorithm. ....................................................... 20
## List of Tables

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Time taken in seconds for static analysis</td>
<td>24</td>
</tr>
<tr>
<td>5.2</td>
<td>Total number of states generated before error discovery</td>
<td>25</td>
</tr>
<tr>
<td>5.3</td>
<td>Total running time before error discovery</td>
<td>26</td>
</tr>
<tr>
<td>5.4</td>
<td>Scalability across different threads</td>
<td>27</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Multi-core processor design and hyper-threading create a need for techniques to validate concurrent interactions in threaded software artifacts. Traditional validation techniques based on test vector generation generally break down in the presence of concurrency since they cannot control scheduling decisions imposed by the operating system when running the input vectors. As a consequence, the validation is not effective in discovering subtle race or deadlock conditions that often lead to unexpected program behavior. Model checking is particularly effective in finding errors in deep execution traces because it considers all possible thread schedules in its analysis. Model checking has the potential to aid software validation if it can be effectively applied to real software artifacts.

State explosion is inherent in model checking, and it is especially problematic in software model checking because of the size and complexity of typical software artifacts. The process of model checking systematically explores the behavior space of the program in some way. There are several different tools and approaches to address the state explosion problem in software model checking, and the work in this paper specifically focuses on directed model checking.

Directed model checking guides the search into areas of the state space where
errors are more likely to exist. It aims to find a property violation before computation resources are exhausted. Directed model checking uses a heuristic function to rank successor states during state space exploration. The search order follows the ranking of states on the search frontier using a priority queue rather than a search stack. An accurate heuristic function reduces the number of states generated before error discovery without dramatically decreasing the frequency of state generation.

Early heuristics use notions from circuit design technology for computing the distance estimate. For example, hamming distance heuristics use the explicit state representation to estimate a bit-wise distance between the current state and an error state \[9\]. Current heuristic functions for directed software model checking are broadly classified into two categories: property based heuristics and structural heuristics. A property based heuristic function tries to estimate the number of changes in the program values needed to violate a property, while structural heuristics consider the structure of either the actual program or its resulting transition system to compute the heuristic estimate. Examples of property based heuristics are in \[10, 11\]. The work in this paper focuses on structural heuristics.

The notion of structural heuristics is introduced in \[12\]. The heuristics in \[12\] exploit the structural properties of thread interdependencies specific to only Java programs to find concurrency errors. Distance heuristic functions \[13, 14, 15\] are structural heuristics that compute the minimal number of transitions required to reach an error location from the current state in the control flow representation of the artifact. These heuristic functions have been shown to be effective in driving threads into race and deadlock conditions.

The extended-FSM (EFSM) distance heuristic combines statically computed distance estimates from the structure of the software artifact with the dynamic call trace in the run-time stack extracted from the state representation of the software artifact to improve the accuracy of the heuristic values \[15\]. The heuristic function
is based on the following notion: at a given program location, the program is either
going to reach a return point for the callee without encountering an error and return
to the caller; or it encounters an error before it reaches the return point and does not
return to the caller. The algorithm to compute the EFSM distance heuristic uses a
graph with bounded calling context to compute the distances in the forward direction.
To build such a graph, procedures are inlined at call sites up to the depth of the user
specified bound. Although the EFSM heuristic function reduces the number of states
before error discovery in various examples, it is not an efficient heuristic function
because the time required to construct the bounded graph increases exponentially
with the bound; thus, the heuristic function does not scale well to programs with
deeply nested function calls where large bounds are required for accurate heuristic
estimates.

This paper presents a new full context aware (FCA) algorithm that implicitly
inlines functions at call sites to compute distance data with unbounded calling context
that is polynomial in the number of nodes in the control flow graph (CFG) for the soft-
ware artifact. The new algorithm computes full context information for non-recursive
programs with resolved function pointers, and works by propagating distance data
through call sites during a depth-first traversal of the program’s CFG. We show, in a
series of benchmark examples, that a new heuristic function, e-FCA that is based on
the EFSM heuristic but uses the FCA for forward distance estimates, generates fewer
states and decreases total running time compared to the EFSM heuristic function
that uses the inlined bounded calling context information [15].

1.1 Motivating Example

We demonstrate with an example how the accuracy of the EFSM heuristic in [15]
relies on the bounded calling context used while computing the static shortest-path
distances for the forward analysis. A program with a maximum possible call depth
Figure 1.1: A program and analysis demonstrating underestimation in the EFSM heuristic due to bounded calling context. (a) A program with a nested call depth of four. (b) An one-bounded CFG for the program that inlines procedures at call sites. (c) The run-time stack for a given state of the program.
of four is presented in Fig. 1.1(a) where an error location, 0b, is reachable from the main procedure only after making a call to procedures x and y. Procedures x and y both make calls to procedure f which in turn calls procedure g. In our program, the EFSM heuristic function tries to accurately estimate the minimal number of transitions required to reach the error location from the current program location. For example, from line 01 of main, it computes the number of instructions that need to be executed in order for the program state to reach the error location in line 0b of main. Ideally, the heuristic computation needs to account for the fact that the true execution flow of the program moves through procedures x and y before reaching the error.

The EFSM heuristic inlines procedures at call sites up to a bounded depth to capture partial context information. It does this by constructing a k-bounded CFG in a depth-first traversal of the program, where k is the specified bound. Each node in a k-bounded CFG is a location in the program with up to k entries for the partial call trace of length k used to arrive at that location. A one-bounded CFG for the program in Fig. 1.1(a) is shown in Fig. 1.1(b), where boxes represent call sites, circle nodes are return points or arbitrary program instructions, and the diamond shape nodes represent the error locations in the artifact. Each node, regardless of its type, has a program location identifier to map it back to the original program followed by a return address indicated by the RA label. There is a single return address in each node for this example because the k-bound of the graph is one. Returning to our example, procedures x, y, and f have enough context information to be uniquely inlined at their call sites; however, procedure g is not fully inlined at its call sites because unlike procedure f that is called from two unique call sites: locations 03 and 05, while procedure g is invoked two times from the same call site: location 07. In Fig. 1.1(b), the node q4, an rts (return) instruction, is at program location 0a in procedure g. The return instruction can transfer control to any node that is at
Figure 1.2: Pseudo-code for the EFSM algorithm.

location 08 in procedure \( f \). The edges from the \( q_4 \) node show that there are two possible return points: nodes \( q_5 \) and \( q_{10} \). Both are at location 08, and both are an invocation of \( f \). Without a \( k \)-bound of at least two, there is not enough context to create a unique invocation in the graph of the partial call trace, \( f \rightarrow g \), for both the \( x \) and \( y \) origins. The missing context leads to an underestimation of the final estimate in a shortest-path analysis because the shortest-path analysis uses the \( x \) invocation to get to procedure \( f \) but returns to the \( y \) invocation.

The EFSM heuristic function in [15] uses the calling context in the run-time stack present in the state of the program to recapture part of the missing calling context in the \( k \)-bounded CFG. There is no additional overhead in maintaining the run-time stack of the program because at any point in the program, the model checker has a complete snapshot of the actual state of the program including its entire run-time stack. The concrete run-time stack reflects the complete call trace from the top-most procedure of the artifact to the current program location which can be used in conjunction with the \( k \)-bounded graph to produce an accurate distance estimate. This is done by unrolling the run-time stack, and at each stack frame, considering the case that the program moves forward to encounter an error without returning from the current stack frame, or it returns from the current stack frame and then moves forward to encounter an error. The heuristic function minimizes over each of these
scenarios as it moves through stack frames.

In Fig. 1.1(c), we present an example of a run-time stack from the concrete state of the program in the model checker. The current stack frame is for procedure g shown at the bottom of the run-time stack since it grows downward. The return address for the current procedure in the run-time stack is location 08 in procedure f. The current program location is 09 in the procedure g. The EFSM heuristic function, shown in Fig. 1.2, takes the current program location (pc) and combines it with the first k return locations (ret_locs) from the run-time stack (rstack) to identify the node (n) corresponding to the current program state in the k-bounded CFG (lines 3-4). The corresponding node in the one-bounded graph for the current program state of Fig. 1.1(b) is q3 since it is at program location 09 with a return address of 08. The heuristic function in Fig. 1.2 now computes a distance estimate in the forward direction within the scope of the current stack frame (line 6). It requests a distance estimate on the k-bounded graph to all possible errors \( n_e \in \text{Errors} \) in the forward direction using a shortest-path analysis \( \text{FSM}(n, n_e) \) assuming the current procedure does not return from the current stack frame \( \text{in\_scope}(n_e, n) = \text{true} \). In our example, the error is not reachable from procedure g without moving through its return point so the shortest-path analysis returns \( \infty \). The heuristic function in Fig. 1.2 then makes a note of this distance (line 6) and then computes the shortest distance to the previous call frame through the return statement of the current procedure (lines 7-8). It finally simulates returning from the current call frame by making the first return location its current program location (line 9).

Continuing with the concrete example in Fig. 1.1(c), after returning from procedure g, the EFSM heuristic function combines the new current program location, now 08, and the return location, 04, to find the next node in the k-bounded CFG. This corresponds to node q5 in the one-bounded graph in Fig. 1.1(b). The heuristic function requests another forward estimate which is still \( \infty \). It then considers the
cost of returning from the stack frame. The algorithm in Fig. 1.2 repeats this process until it runs out of stack frames in the run-time stack (line 2), and it then reports the distance estimate to the nearest error computed during the analysis (line 11). The key observation in this example is that the call site for procedure g is resolved using the run-time stack, and the EFSM heuristic reports the correct distance value from node $q_3$ to the error location. This does not, however, completely remove the underestimation in other distance estimates.

When the program execution is at the topmost level of the call structure or has a shallow call depth, the heuristic estimate computation is reduced to a shortest-path analysis on the $k$-bounded CFG. Returning to our example, suppose the concrete state in the model checker has a single frame in the run-time stack showing the current location to be node $q_0$. A request for the distance estimate in the forward direction returns a distance of seven which is the shortest-path to the error node $q_{12}$ from node $q_0$ in the one-bounded CFG. The missing context information at depths greater than one is needed to resolve the unique call sites leading to node $q_4$, and it causes the shortest-path analysis to choose a path that is not consistent with the actual program execution from node $q_0$.

The cost of building the $k$-bounded graph is exponential in the nested call depth due to inlining. The cost of doing the shortest-path analysis is also very expensive since it is run several times to account for the scoping check on the path to the error. For the EFSM heuristic to be accurate, it needs full calling context, but for it to be efficient in runtime, it needs a small $k$-bound. The goal of this work is to produce an efficient estimate in terms of its accuracy and computational overhead.
Chapter 2

Thesis Statement

The full context aware algorithm implicitly inlines functions at call sites to compute distance data with unbounded calling context that is polynomial in the number of nodes in the CFG. We demonstrate with a series of benchmark examples that a heuristic function using unbounded distance data computed by the FCA is more efficient than existing heuristic functions.
Chapter 3

Full Context Aware (FCA) Algorithm

The FCA algorithm is an interprocedural control flow analysis technique that implicitly constructs call traces to compute static lower-bounds on distance estimates to return locations of the procedures and nearest error locations in a software artifact using shortest-path analysis and depth-first traversal. The FCA algorithm uses the reverse invocation order to summarize the shortest-path analysis in all the callees of a given procedure. It then propagates the summarized distance information of the callees back to the given procedure. The input to the algorithm is a set of CFGs with a single CFG for each method or procedure in the artifact. Fig. 3.1(a) is an example of the input for a program with two procedures main and sub1. Each CFG has a single start node and end node. A call node is represented as a box in the CFG. The label in the call node identifies the start node for the target CFG of the call. The diamond shape nodes represent error nodes in the program. These are most often critical sections or assertion points in the software artifact. We associate values with each CFG node for the distance to the end node \(d_{\text{end}}\) and the distance to the nearest error node \(d_{\text{error}}\).
The FCA algorithm uses a depth-first traversal to build a distance matrix for a given CFG to use in a shortest-path analysis to compute \(d_{\text{end}}\) and \(d_{\text{error}}\) for each node. We associate with each individual CFG a distance matrix, \(L\), that is defined over the number of nodes in the CFG. \(L\) is initialized with entries along the diagonal set to zero and all other entries set to \(\infty\). Edge costs in \(L\) are added as the depth-first traversal moves through nodes in the CFG. The depth-first traversal begins at the start node of the top-level method in the software artifact. In our example, the traversal starts at node \(m_1\), updates the \((m_1, m_2)\) entry in \(L\) to add the cost of the \(m_1 \rightarrow m_2\) edge, and then visits \(m_2\). The distance between two immediate successors in a CFG is one for all nodes except the successors of call nodes. The distance to the immediate successor of a call node needs to reflect the cost of moving through the target CFG of the call.

The depth-first traversal moves to the start node of the target CFG at a call node, and when the traversal returns, it then explores the immediate successor of the call node in the current CFG. The distance to the immediate successor of the call node relies on the analysis of the target CFG to account for the cost of moving through the target CFG without encountering an error. The distance to the immediate successor of the call node is the \(d_{\text{end}}\) value stored in the start node of its target CFG plus two: one to move to the start node of the target CFG and one to return from the end node of the target CFG. Fig. 3.1(b) shows the \(d_{\text{end}}\) and \(d_{\text{error}}\) values in the \texttt{sub1} CFG when the traversal returns to \(m_2\) after analyzing \texttt{sub1}. Recall that call node \(m_2\) points to the \(s_1\) start node. The \(d_{\text{end}}\) value for \(s_1\) is three. This reflects the number of program steps required in \texttt{sub1} to reach its \(s_4\) end node. The traversal updates the \((m_2, m_3)\) entry in \(L\) by setting the \(m_2 \rightarrow m_3\) edge to five (three plus two), and continues the traversal by visiting node \(m_3\). The top matrix in Fig. 3.1(c) is the final \(L\) matrix for \texttt{main}. The matrix includes all the edges in the \texttt{main} CFG with the cost of moving through \texttt{sub1} included in the row for \(m_2\). Note that the matrix excludes the row for
since the end node has no successors in the traversal. The $L$ matrix provides the requisite data to derive $d_{end}$ and $d_{error}$ values for the CFG nodes.

The FCA algorithm computes $d_{end}$ for each node in the current CFG with a shortest-path analysis using the distance matrix when the traversal is ready to backtrack out of the start node. Recall that $L$ only includes nodes in the immediate CFG since call nodes move to the immediate successor in the CFG with the cost of moving through the target CFG. The bottom matrix in Fig. 3.1(c) is the final $L$ matrix for main after the shortest-path analysis. Each $d_{end}$ value for the CFG of main is set to its corresponding entry in the $m_4$ column of $L$ after the shortest-path analysis. This is the shortest-path through the CFG to the end node $m_4$ including the cost of function calls.

The nearest error distance values are computed by minimizing over distances to error locations in the current CFG and distances to error locations reachable from the target CFGs of call nodes. In the discussion, $N_{error}$ and $N_{call}$ denote the sets of error locations and call nodes respectively for a given CFG. We use the results of the shortest-path analysis in the distance matrix, $L$, to compute distances to the nearest error location. For convenience, a global array, $D_{error}(n)$ is used to store the distance to the nearest error, $d_{error}$, for node $n$ in a CFG. The equations for computing $d_{error}$ for a given node $n$ are

$$d_{local} = \min_{n_e \in N_{error}} (L(n, n_e))$$

$$d_{nonlocal} = \min_{n_c \in N_{call}} (L(n, n_c) + D_{error}(n_{start}') + 1)$$

$$d_{error} = \min(d_{local}, d_{nonlocal})$$

$$D_{error}(n) = d_{error}$$

where $n$ is the current node being analyzed and a call node $n_c$ points to the start node $n_{start}'$ of its target CFG.
The $d_{\text{local}}$ value in Equation 3.1 is the distance to the nearest error in the immediate CFG. This error is reachable without having to move into a different CFG through a call node. The value is taken directly from the shortest-path analysis results in the distance matrix ($L(n, n_e)$ is the shortest-path from node $n$ to node $n_e$ in the current CFG).

The $d_{\text{nonlocal}}$ value in Equation 3.2 is the distance to the nearest error through a call node of the immediate CFG. This error is only reachable by moving into a different CFG through a call node. The equation computes the transitive distance of first moving forward to the call node and then moving from the start node of the target CFG to the error. In the equation for the $n_c$ call node, $n_{\text{start}}'$ is the start node of its target CFG. The value stored in $D_{\text{error}}(n_{\text{start}}')$ is computed prior by virtue of the depth-first traversal. The traversal only triggers the distance analysis when it is ready to backtrack out of a start node to resolve call dependencies in the computation. The final $d_{\text{error}}$ value for node $n$ in Equation 3.3 is either local to the CFG or reached through a call node in the CFG.

Fig. 3.1(d) shows the end results of the FCA algorithm for main. Fig. 3.1(b) and Fig. 3.1(d) give the complete view of the final analysis. For Fig. 3.1(d), the path to the end node for $m_1$ bypasses the $m_2$ call node for a distance of two, which is the number of edges in the path $m_1 \rightarrow m_3 \rightarrow m_4$. An error location is only reachable through the target CFG of the call node $m_2$. The nearest error for $m_1$ is three which represents the path $m_1 \rightarrow m_2 \rightarrow s_1 \rightarrow s_2$ in the CFGs. An error location cannot be reached from node $m_4$.

The FCA algorithm lower-bounds all distance estimates by assuming shortest-paths through CFGs. From this, the $d_{\text{error}}$ and $d_{\text{end}}$ data by themselves form an admissible and consistent distance estimate similar to the finite state machine (FSM) distance heuristic in [13]. Regardless of the true path of execution, the length of that path is at least that of the shortest-path through the CFG. An example is seen in
Fig. 3.1(d) where the algorithm bypasses the $m_2$ call node to reach the $m_4$ end node. If the true path of execution follows $m_2$, then the actual distance is strictly larger than the reported distance. This lower-bound also appears in all iterative constructs of the CFG.

The pseudo-code for the FCA algorithm is presented in Fig. 3.2. In Fig. 3.2 a CFG is a tuple $\langle N, E, n_{\text{start}}, n_{\text{end}}, N_{\text{call}}, N_{\text{error}} \rangle$ where $N$ is set of uniquely labeled nodes, $E \subseteq N \times N$ is the set of edges, $n_{\text{start}} \in N$ is a unique start node, $n_{\text{end}} \in N$ is a unique end node, $N_{\text{call}} \subseteq N$ is a set of call nodes, and $N_{\text{error}} \subseteq N$ is a set of error nodes. $D_{\text{end}}$ and $D_{\text{error}}$ are global arrays that store distances to the end node and nearest error node respectively for $X = |\bigcup_{1 \leq i \leq m} N_i|$ nodes where $m$ is the number of procedures in the artifact. Note that the $d_{\text{error}}$ and $d_{\text{end}}$ values stored in $D_{\text{error}}$ and $D_{\text{end}}$ arrays are the same $d_{\text{error}}$ and $d_{\text{end}}$ values annotated on the CFGs. The function $\text{Target}$ takes a call node as input and returns the target CFG of the call node. Finally, the function $\text{succ}(n_x) = \{n_y \in N \mid (n_x, n_y) \in E\}$, which means the $\text{succ}$ function returns a set containing all the immediate successors of the input node, $n_x$.

In Fig. 3.2 the $\text{compute\_distances}$ function initializes a distance matrix $L$ (line 4) for the input CFG and calls the $\text{traverse\_CFG}$ function (line 5). The $\text{traverse\_CFG}$ function uses a depth-first traversal to add edge costs between successors of the CFG in the distance matrix $L$ (lines 26-28). If the traversal encounters a call node (line 19), the algorithm makes a mutually recursive call to $\text{compute\_distances}$ with the target CFG of the call node (line 21). When the execution returns, it adds the edge cost to the immediate successor of the call node taking into account the cost of moving through the target CFG without encountering an error (line 22). For all other nodes, the distance between two immediate successors in a CFG is one (line 24). After the traversal of the CFG is done, the algorithm returns the distance matrix $L$ (line 29), and the flow of execution returns to the $\text{compute\_distances}$ function where the FCA
algorithm computes the all-pairs shortest-path on the distance matrix $L$ (line 6). For each node in the CFG, it adds the corresponding $d_{\text{end}}$ and $d_{\text{error}}$ values to the global arrays $D_{\text{end}}$ and $D_{\text{error}}$ (lines 7-16). The $d_{\text{error}}$ value is computed by minimizing over distances to error locations in the current CFG ($d_{\text{local}}$) and distances to error locations reachable from the target CFGs of call nodes ($d_{\text{nonlocal}}$).

The initial traversal and the final algorithm to propagate the $d_{\text{end}}$ and $d_{\text{error}}$ values are linear in the number of nodes in the artifact since the traversal reuses the information from the secondary analysis if it encounters the same CFG numerous times from different call nodes in the artifact. The complexity of the secondary analysis is $O(X^3)$, where $X$ is the total number of nodes in the artifact because an all-pairs shortest-path algorithm is run once for every reachable CFG in the artifact. Hence, the complexity of the FCA algorithm is polynomial in time and space with regards to the total number of nodes in the CFGs as a result of the shortest-path analysis.
Distance Matrix for **main**

<table>
<thead>
<tr>
<th></th>
<th>(m_1)</th>
<th>(m_2)</th>
<th>(m_3)</th>
<th>(m_4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m_1)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>∞</td>
</tr>
<tr>
<td>(m_2)</td>
<td>∞</td>
<td>0</td>
<td>5</td>
<td>∞</td>
</tr>
<tr>
<td>(m_3)</td>
<td>1</td>
<td>∞</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Shortest-path Analysis

<table>
<thead>
<tr>
<th></th>
<th>(m_1)</th>
<th>(m_2)</th>
<th>(m_3)</th>
<th>(m_4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m_1)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>(m_2)</td>
<td>6</td>
<td>0</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>(m_3)</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 3.1: Execution of the FCA on a set of CFGs. (a) A set of two CFGs for a software artifact. (b) The CFG for sub1 annotated with \(d_{\text{end}}\) and \(d_{\text{error}}\) data. (c) Distance matrix \(L\) for main before and after shortest-path analysis. (d) The CFG for main annotated with \(d_{\text{end}}\) and \(d_{\text{error}}\) data.
```plaintext
procedure compute_distances(N, E, n_start, n_end, N_error, N_call)
1: /* Visited is global variable initialized to ∅ */
2: if n_start ∉ Visited then
3:   Visited = Visited ∪ {n_start}
4: /* L : N × N → N ∪ {∞}, entries along the diagonal are set to 0, while all other entries are set to ∞ */
5:   L = traverse_CFG(n_start, N_call, L)
6:   L = compute_all_pairs_shortest_distance(L)
7: for each n ∈ N do
8:   d_end = L(n, n_end)
9: /* D_end, a global array of size X is initialized to 0 */
10:  D_end(n) = d_end
11:  d_local = min_n ∈ N_error {L(n, n_e)}
12:  ⟨N', E', n'_start, n'_end, N'_error, N'_call⟩ = Target(n_k)
13:  d_nonlocal = min_n ∈ N_call {L(n, n_k) + d_error(n'_start) + 1}
14:  d_error = min(d_local, d_nonlocal)
15: /* D_error, a global array of size X is initialized to 0 */
16:  D_error(n) = d_error
17: return
18:
procedure traverse_CFG(n_x, N_call, L)
19: if n_x ∈ N_call then
20:   ⟨N', E', n'_start, n'_end, N'_error, N'_call⟩ = Target(n_x)
21:   compute_distances(N', E', n'_start, n'_end, N'_error, N'_call)
22:   d_succ = D_end(n'_start) + 2
23: else
24:   d_succ = 1
25: /* Conditional branches have multiple successors */
26: for each n'_x ∈ succ(n_x) do
27:   L(n_x, n'_x) = d_succ
28: L = traverse_CFG(n'_x, N_call, L)
29: return L
```

Figure 3.2: Pseudo-code for the FCA algorithm.
Chapter 4

EFSM with FCA

The FCA is a forward analysis algorithm which is run once statically. The FCA cannot resolve the non-determinism arising from the end nodes in the CFGs of the program. For example, in Fig. 1.1(a) there are two calls to procedure $f$. The CFG of $f$ does not contain any information about where the flow of execution returns when it exits procedure $f$. The only information present in the nodes of the CFGs are the distance values to the end ($d_{end}$) of the CFGs and the distance values to error locations ($d_{error}$) in the forward direction without executing the end of the CFGs. We dynamically recreate the call trace based on the values of the run-time stack like the EFSM heuristic to compute true successors of end nodes for a particular program execution path.

For the program shown in Fig. 1.1(a), the CFGs for each procedure annotated with $d_{error}$ and $d_{end}$ values after executing the FCA computation are shown in Fig. 4.1. Now let us consider a concrete example of how the EFSM is combined with the FCA to compute accurate heuristic estimates. Suppose the values on the return stack are: $\langle x_2, m_2 \rangle$ where the $x_2$ is the first return location encountered on exiting the current stack frame, and $m_2$ is the next return location. The current location of the program is $f_1$ in procedure $f$. The heuristic function in the EFSM requests a distance estimate
Figure 4.1: The CFGs for the program in Fig. 1(a) annotated with context aware distances after running the FCA algorithm.

After noting the value of $d_{\text{error}}$ at node $f_1$, the heuristic function uses the value of $d_{\text{end}}$ to compute the distance to the end node of procedure $f$. It requires this value to estimate the distance to the previous call frame. The algorithm to compute the heuristic estimate has an accumulator variable, path, that keeps track of the cost incurred in backtracking through the call frames. In Fig. 4.1, the value of $d_{\text{end}}$ is three; the heuristic function adds one to it to account for the return and sets path equal to four. Next, the heuristic simulates returning from the current call frame by making the first value on the return stack, $x_2$, its current program location like the EFSM algorithm. The value of $d_{\text{error}}$ on node $x_2$ is $\infty$ showing that the error is still not reachable. Since $x_2$ is an end node, the value of $d_{\text{end}}$ is zero, and the heuristic function increments path by one for the return, changing the value of path to five. The heuristic function repeats the process of unrolling the stack by moving to node $m_2$, where the value of $d_{\text{error}}$ is seven. It adds this value to path to get the
final value of twelve as the estimate of the distance to the error. At all points of forward computation to find the error location, and while going to the end node, the heuristic function has access to unbounded context information from the FCA algorithm resulting in a better lower-bound on the true estimate of the distance to the error which is also admissible and consistent.

To calculate the heuristic estimate for a concurrent program with multiple threads, the approach presented in [13] computes the distance to the nearest error location for each thread and sums up the individual estimates to create a final heuristic value. To ensure underestimation of the distance to the error, we modify the number of individual estimates summed together based on the property being verified. For example, the heuristic estimate for a mutex violation is the sum of distances in two threads which have the shortest paths to the critical section compared to all the other threads. Now, consider the property which is a check to see if any thread reaches a certain location in the program, like an assert statement. In such a case, the heuristic estimate is the smallest distance in the set of estimated distances from the current location to the desired location for each thread. Another useful property checked in concurrent programs is whether two or more threads are deadlocked. In this case, we take the summation of the distances from the current state to the error state for two or more threads that can lead to a deadlock state. From this point forward in the presentation we refer to the combination of the FCA and EFSM approaches as the e-FCA heuristic function.
Chapter 5

Results

We implemented the e-FCA heuristic function in the gnu-debugger based model checker Estes, and executed it on a benchmark set consisting of programs with concurrency errors. The results show that the e-FCA heuristic reduces the total number of states generated and also decreases the total running time before error discovery compared to the FSM and EFSM distance heuristics.

We focus specifically on three classical concurrency problems in our benchmark suite:

- **Dining Philosophers**
- **Barbershop**
- **Hyman’s mutual exclusion principle**

The results presented are from a Pentium III 1.5 Ghz processor with 2 GB of RAM and are run on Estes, with a 6.1.1 version of the gnu debugger, using the m68hc11 backend simulator. We report the wall clock time for the time taken to do the static analysis and for the total running time of the program before error discovery, as well as the total states generated before error discovery.

For the benchmarks, we add procedures containing nested function calls that
Table 5.1: Time taken in seconds for static analysis

<table>
<thead>
<tr>
<th>Name</th>
<th>T</th>
<th>M</th>
<th>k</th>
<th>FSM</th>
<th>EFSM</th>
<th>FCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyman</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Hyman</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>Hyman</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>27</td>
<td>0</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>76</td>
<td>0</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>76</td>
<td>0</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>146</td>
<td>0</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>147</td>
<td>0</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>41</td>
<td>0</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

do not affect the property being verified to the base implementation of the concurrent programs. We then randomly insert calls to these procedures throughout the programs to derive examples with varying call structures and call depths in order to test the accuracy and efficiency of the e-FCA in computing context aware distances.

To measure the accuracy of the e-FCA heuristic function we compare the e-FCA to the shortest-path analysis (FSM) and the EFSM distance heuristic. We also compare it with random search and an exhaustive depth-first search (DFS). We use best-first search rather than $A^*$ to decrease the number of states expanded before error discovery; although best-first does not guarantee a shortest error trace like the $A^*$ search.

In our experiments, the length of the error traces generated by the best-first search are comparable to that of $A^*$. The results of the analyses are shown in Table 5.1, Table 5.2, Table 5.3, and Table 5.4. In Table 5.1, Table 5.2, and Table 5.3 the first column (Name), shows the concurrent program being verified; if the program is model checked at the C-level, where a single C instruction is considered atomic, a letter C is appended to the end of the program name. Otherwise, the program is model checked.
Table 5.2: Total number of states generated before error discovery

<table>
<thead>
<tr>
<th>Name</th>
<th>T</th>
<th>M</th>
<th>k</th>
<th>DFS</th>
<th>Rand</th>
<th>FSM</th>
<th>EFSM</th>
<th>e-FCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyman</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6,478</td>
<td>15,800</td>
<td>10,227</td>
<td>7,160</td>
<td>3,817</td>
</tr>
<tr>
<td>Hyman</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>16,190</td>
<td>59,796</td>
<td>41,791</td>
<td>21,909</td>
<td>13,529</td>
</tr>
<tr>
<td>Hyman</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>40,471</td>
<td>91,947</td>
<td>123,743</td>
<td>59,951</td>
<td>38,745</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>157,436</td>
<td>475,184</td>
<td>53,897</td>
<td>4,594</td>
<td>1,626</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>19,769</td>
<td>11,497</td>
<td>18,148</td>
<td>1036</td>
<td>415</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>452,092</td>
<td>54,725</td>
<td>13,830</td>
<td>3,816</td>
<td></td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>157,818</td>
<td>95,009</td>
<td>8,575</td>
<td>3,348</td>
<td>1,015</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>*</td>
<td>999,480</td>
<td>186,419</td>
<td>36,467</td>
<td>13,696</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>548,127</td>
<td>173,494</td>
<td>42,107</td>
<td>10,224</td>
<td>3,655</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>334,198</td>
<td>400,474</td>
<td>55,876</td>
</tr>
<tr>
<td>D-phil C</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>*</td>
<td>370,656</td>
<td>861,319</td>
<td>142,350</td>
<td>14,755</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>*</td>
<td>442,285</td>
<td>82,333</td>
<td>21,465</td>
<td>3,298</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>*</td>
<td>939,828</td>
<td>73,940</td>
<td>75,635</td>
<td>13,118</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>378,632</td>
<td>388,161</td>
<td>66,608</td>
</tr>
</tbody>
</table>

at the assembly-level where a single assembly-level instruction is considered atomic.
The next column (T) indicates the number of threads in the program, the column (M)
shows the maximum possible call depth of the program, and the column (k) is the
value of the bound picked for the EFSM heuristic.

The static analysis time reported in Table 5.1 is the time taken in seconds
during the period after the execution of the program starts and before the model
checking run begins. The FCA analysis takes negligible amount of time. The average
time taken by the FCA to complete static analysis (0.65 secs) is less than the average
time (1 secs) taken by the FSM, even though the FSM does not consider calling
context of the program at all. As we increase the k-bound for the EFSM distance
heuristic, the cost to construct the inlined graph and do a shortest path analysis for
checking whether the error is in scope grows exponentially. The high overhead of
static analysis with larger k-bounds forces us to pick a bound of either one or zero for
the EFSM distance heuristic in order to finish static analysis within a few minutes.
In spite of picking low bounds of k for the EFSM computation, the time taken by
Table 5.3: Total running time before error discovery

<table>
<thead>
<tr>
<th>Name</th>
<th>T</th>
<th>M</th>
<th>k</th>
<th>DFS</th>
<th>Rand</th>
<th>FSM</th>
<th>EFSM</th>
<th>e-FCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyman</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Hyman</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>7</td>
<td>28</td>
<td>17</td>
<td>21</td>
<td>5</td>
</tr>
<tr>
<td>Hyman</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>17</td>
<td>42</td>
<td>49</td>
<td>56</td>
<td>16</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>71</td>
<td>318</td>
<td>31</td>
<td>79</td>
<td>1</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>12</td>
<td>10</td>
<td>14</td>
<td>77</td>
<td>0</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>*</td>
<td>292</td>
<td>28</td>
<td>155</td>
<td>3</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>102</td>
<td>75</td>
<td>5</td>
<td>149</td>
<td>1</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>*</td>
<td>730</td>
<td>113</td>
<td>27</td>
<td>8</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>299</td>
<td>159</td>
<td>31</td>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>*</td>
<td>*</td>
<td>178</td>
<td>388</td>
<td>32</td>
</tr>
<tr>
<td>D-phil</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>294</td>
<td>680</td>
<td>136</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>*</td>
<td>282</td>
<td>41</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>*</td>
<td>576</td>
<td>38</td>
<td>47</td>
<td>7</td>
</tr>
<tr>
<td>Barbers</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>*</td>
<td>237</td>
<td>252</td>
<td>38</td>
<td></td>
</tr>
</tbody>
</table>

EFSM to complete static analysis is significantly higher compared to the FCA. Note that even with a bound of zero, the EFSM dynamically recreates the call trace of the program; hence, it has more context than the FSM distance heuristic.

For each model, we report the total number of states enumerated before finding the error state and total running time to find the error in Table 5.2 and Table 5.3 respectively. The ‘*’ symbol in Table 5.2 and Table 5.3 shows that after generating a million states, the error state was still not found, and at that point, the search was terminated. For the random search, the heuristic value is set to a random value and the numbers reported for the total number of states and total running time numbers are averaged over 10 model checking runs.

The e-FCA gains a significant reduction in total states generated compared to the other heuristics and search techniques as shown in Table 5.2. In Table 5.2, we can see that DFS, an exhaustive search is mostly ineffective in finding the error. In seven out of fourteen examples it is unable to find the error within a million states; however, sometimes DFS happens to find the error quickly by chance as seen in the Hyman
examples. In some cases, the EFSM generates more states than the FSM distance heuristic before finding the error. Our experiments with different $k$-bounds show that for some programs, the improvement in error discovery by the EFSM heuristic with increasing context is not always monotonic. For such programs, the EFSM heuristic does not perform well until the context information reaches a certain threshold.

The e-FCA also obtains a significant decrease in the total running time compared to the other search techniques as shown in Table 5.3. The state reduction achieved by the EFSM is not enough to compensate for the high cost of static analysis causing its total running time to increase dramatically compared to the e-FCA. While computing the heuristic estimate, the EFSM faces an additional overhead cost of extracting the call trace in the run-time stack from the start of the program to its current point. The e-FCA faces the same overhead of extracting the run-time stack; however, this cost is very effectively mitigated by the significant reduction in the states generated and low cost of static analysis resulting in a substantial decrease in the total running time of the e-FCA before error discovery.

We test the scalability of the e-FCA heuristic function by instrumenting our implementation of the barbershop problem to allow a variable number of threads.
(between 5 and 51). Additionally, we implement three versions of the problem with varying maximum possible call depths of two, five, and nine. The total number of states and total running time before error discovery for these examples are presented in Table 5.4. The first column (T) in Table 5.4 indicates the number of threads created for the particular example. From the barbershop example, it seems that the e-FCA scales to multiple threads with a high degree of nested function calls. DFS and random search do not find the error in a million states for even the smallest model. The FSM distance heuristic and EFSM distance heuristic, with small k-bounds, do not find the error in a million states for most of the models. With a slightly higher k-bound the EFSM heuristic does not finish static analysis in 1 hour for any of the examples.
Chapter 6

Conclusion and Future Work

In this paper we present the FCA algorithm that computes full context aware distances for a CFG in a non-recursive program with resolved function pointers by implicitly inlining function calls. It propagates context information through call nodes, start nodes, and end nodes of the CFG and annotates the nodes in the CFG with context sensitive distances to end nodes and error locations in the forward direction. We then present a new heuristic function, e-FCA which combines the unbounded distance data computed by the FCA algorithm with the dynamic recreation of the run-time stack from the EFSM heuristic function. The e-FCA heuristic function computes more accurate heuristic estimates compared to other distance heuristic functions.

In some cases, the e-FCA heuristic function underestimates the true distance to the error locations because it does not consider the feasibility of the execution paths. Resolving the feasiblity of all execution paths is not possible statically; however, while model checking, as the variables are assigned dynamic values, we can determine the infeasible execution paths. In future work we plan on pruning these infeasible execution paths before computing the heuristic estimate to overcome the underestimation arising due to the path-insensitive computation of the e-FCA.
Bibliography


