Feedback-Directed Instrumentation for Deployed JavaScript Applications

Magnus Madsen*  
University of Waterloo  
Waterloo, Ontario, Canada  
mmadsen@uwaterloo.ca

Frank Tip  
Samsung Research America  
Mountain View, CA, USA  
ftip@samsung.com

Esben Andreasen*  
Aarhus University  
Aarhus, Denmark  
esben@cs.au.dk

Koushik Sen  
EECS Department  
UC Berkeley, CA, USA  
ksen@cs.berkeley.edu

Anders Møller  
Aarhus University  
Aarhus, Denmark  
amoeller@cs.au.dk

ABSTRACT

Many bugs in JavaScript applications manifest themselves as objects that have incorrect property values when a failure occurs. For such errors, stack traces and log files are often insufficient for diagnosing problems. In such cases, it is helpful for developers to know the control flow path from the creation of an object to a crashing statement. Such crash paths are useful for understanding where the object originated and whether any properties of the object were corrupted since its creation.

We present a feedback-directed instrumentation technique for computing crash paths that allows the instrumentation overhead to be distributed over a crowd of users and to reduce it for users who do not encounter the crash. We implemented our technique in a tool, Crowdie, and evaluated it on 10 real-world issues for which error messages and stack traces are insufficient to isolate the problem. Our results show that feedback-directed instrumentation requires 5% to 25% of the program to be instrumented, that the same crash must be observed 3 to 10 times to discover the crash path, and that feedback-directed instrumentation typically slows down execution by a factor 2x–9x compared to 8x–90x for 25% of the program to be instrumented, that the same crash occurs. The technique relies on repeatable error reporting facilities, or in a bug reporting forum. Depending on the type of problem, additional information may be available along with failure reports. For example, log files may exist that contain a summary of an application’s execution behavior, or a dump of an application’s state at the time of a crash. However, such information is often of limited value, because the amount of information can be overwhelming (e.g., log files may span many megabytes, most of which is typically completely unrelated to the failure), or is woefully incomplete (e.g., a stack trace or memory dump usually provides little insight into how an application arrived in an erroneous state).

Many bugs that arise in JavaScript applications manifest themselves as objects that have incorrect property values when a failure occurs. This includes situations where an object is created with incorrect or missing property values, and where properties are corrupted after the object was created. In such cases, it is helpful for developers to know the control-flow path from the creation of the object of interest to the crashing statement. We will refer to such a path as a crash path. In the case studies reported on in this paper, we consider real-life bugs where the error message and stack trace provided with a bug report are insufficient to find and fix the underlying cause of a bug. In these case studies, information contained in the crash path provided crucial hints to developers in a debugging scenario. In principle, crash paths could be obtained by instrumenting applications so that control-flow is recorded as the program executes and exercising the application until the same failure is encountered. Unfortunately, such a “full instrumentation” approach tends to incur prohibitive runtime overhead and is indiscriminate in that much of the instrumentation occurs in regions of the code unrelated to the failure. Furthermore, in many cases, developers do not need an entire execution history as much of it tends to be unrelated to the bug being pursued.

In this paper, we present a feedback-directed technique for computing crash paths in scenarios where the same failure can be observed repeatedly. The technique relies on repeatedly deploying new versions of the application in which the amount of instrumentation is gradually increased to uncover successively longer suffixes of the crash path. This process continues until the complete crash path is found (i.e., the allocation site for the object of interest is found). We believe that our technique is particularly well-suited for a scenario where users collectively isolate crash paths associated with bugs in deployed software. In the scenario we envision, users

1. INTRODUCTION

Despite the best efforts of software engineers and testers, software shipped to end users still contains bugs, causing applications to crash or produce incorrect results. Failures that occur post-deployment are often reported via on-line error reporting facilities, or in a bug reporting forum. Depending on the type of problem, additional information may...

*The work of these authors was carried out during internships at Samsung Research America.

1E.g. Windows Error Reporting [22] or CrashReporter [5].
install applications from a central software repository (e.g., through an app store or a package manager). When a crash is encountered by a user, new versions of the application that contain additional instrumentation can be distributed to other users so that the effort of isolating crash paths is distributed over a user population. Furthermore, while our feedback-directed instrumentation approach occurs significant overhead, this tends to be up to an order of magnitude less than an approach where applications are fully instrumented. Similar crowdsourcing techniques for debugging were pioneered by Liblit et al. [18, 19] and by Orso et al. [10, 12], although they do not consider the specific problem of computing crash paths. We implemented the technique using Jalangi [28], and evaluated it on crashing executions of JavaScript applications available from GitHub. We report on instrumentation overhead and on the number of times that the same crash needs to be encountered to recover the complete crash path. In summary, the contributions are:

● We propose the notion of a crash path as a supplement to error messages and stack traces. A crash path records the path from the creation of an object of interest to a crashing statement.

● We present a technique for computing crash paths based on feedback-directed program instrumentation. This technique identifies increasingly longer suffixes of crash paths in successive executions of the application, by gradually increasing the amount of instrumentation.

● We implemented a prototype of our technique in a tool called CROWDIE and used it to debug 10 real-world issues previously reported on GitHub. Our case study shows that error messages and stack traces are insufficient to debug these issues, and that crash paths provide useful hints to developers debugging these issues.

● Our experimental evaluation shows that only 5% to 25% of the program is instrumented, that the same crash must be observed between 3 to 10 times to recover complete crash paths, and that the feedback-directed instrumentation has a typical slowdown of 2x–9x compared to 8x–90x with full instrumentation.

Furthermore, we argue informally that our technique is well-suited to a crowdsourcing scenario, where the effort of identifying crash paths is distributed over a user population.

2. MOTIVATING EXAMPLES

In this section, we look at two real-world bugs in popular JavaScript libraries. What these bugs have in common is that traditional debugging information (e.g., the error message, the line on which the crash occurs, and the stack trace) is insufficient to locate the root cause of the defect. We will show how, in each case, the crash path provides information that is vital for understanding and fixing the bug.

Loki Issue #0046. Loki is a database written in JavaScript. In issue #0046, entitled “Clearing collection breaks index”, a user reports that “after clearing a collection I wasn’t able to insert new objects without error.” Such a report is typically not enough for the developer to reproduce the bug and locate its cause. A stack trace, which may be sent automatically to the server when a crash occurs, may provide some hints but is also often insufficient. To keep

the example simple, imagine that we just try to execute the following four lines (example1.js) inspired by the text in the report, which happen to be enough to encounter the error:

```
1 var db = new loki('Example');
2 var col = db.addCollection(/* omitted */);
3 col.clear();
4 col.insert(/* omitted */);
```

Running this code makes Loki throw an exception with the following stack trace:

```
TypeError: undefined is not a function
  at Collection.add (loki.js:1789)
  at Collection.insert (loki.js:1661)
  at Object.<anonymous> (example1.js:4)
```

This stack trace tells us that the crash occurs at line 1789 in loki.js, which is executed due to the call col.insert on line 4. Line 1789 in loki.js looks as follows:

```
1789 this.idIndex.push(obj.id);
```

As there is only one function call on this line, one can infer that this.idIndex.push is undefined. From this, a developer may conclude that the value of this.idIndex or its push property is incorrect. To find the root cause of the crash we need to know what is the value of this.idIndex, and why the push property is undefined. Was it never set, or was it perhaps mistakenly overwritten?

We cannot answer these questions easily by inspecting the stack trace and source code. We could use a tool such as grep to search for this.idIndex, but such an approach is very crude and may match statements unrelated to the crash. What we want to know is (a) where was the object referred to by this.idIndex created, and (b) how was the push property of this object modified in the time between its creation and the crash. Our CROWDIE tool computes this information automatically. Applying CROWDIE to this program reveals that the object referred to by this.idIndex originates from line 1670 in loki.js:

```
1670 this.idIndex = {};
```

At this point, the root cause becomes clear: this line assigns the idIndex property with an empty object instead of an empty array. Arrays have a push method, whereas ordinary objects do not, which causes the expression this.idIndex.push to evaluate to undefined, and calling the push method on undefined results in the exception being thrown. CROWDIE also reveals that no writes to the push property of the object occur before the crash.

Upon realizing this problem, a project maintainer fixed the issue\(^2\) by assigning an array instead of an object to this.idIndex on line 1670 of loki.js.

To find this problem using CROWDIE, this.idIndex is designated as an object of interest. Then, CROWDIE produces the following crash path (shown simplified here; details of the path format are described in Section 3.1, and details about the actual path for this bug appear in Table 1):

```
Start(loki.js:1670) this.idIndex = {};
Return(example1.js:3) col.clear();
Call(example1.js:4) col.insert({ /* omitted */});
Call(loki.js:1661) this.add(doc);
Crash(loki.js:1789) this.idIndex.push(obj.id);
```

With this information, the developer would be able to quickly identify the buggy assignment on line 1670.

\(^2\)https://github.com/techfort/LokiJS/issues/46

\(^3\)Commit 5da46aeecda6046f738c6a612c2f181b21487108
Immutable Issue #0381. Immutable is a JavaScript collection library created by Facebook. In issue #0381, entitled “subCursor (cursor.cursor(‘a’)) returns improper type”, a user reports that the cursor method may return the wrong type of cursor. The following code fragment (example2.js), reported by the user, is a highly simplified version of the actual application code that triggers the bug:

```javascript
1 var data = Immutable.fromJS( {a: [1,2,3]});
2 var cursor = Cursor.from(data);
3 var deepCursor = cursor.cursor(‘a’);
4 assert(deepCursor instanceof IndexedCursor);
```

In this example, the stack trace only tells us that the assertion on line 4 fails:

```
Error:AssertionError
at Object.<anonymous> (example2.js:4)
```

We see that the value of deepCursor returned by the call to cursor cursor has the wrong type, causing the assertion to fail. However, it is not obvious whether the call Cursor from data on line 2 or the call cursor cursor(‘a’) on line 3 is at fault.

At this point, we ask CROWDIE to find where the erroneous deepCursor object was allocated and by what path it reached the assertion. In response, CROWDIE produces the following crash path:

```
Start(cursor.js:242) . . . new CursorClass(r,k,c,s);
Return(cursor.js:250) return makeCursor(
  Return(cursor.js:187) . . . subCursor(this, s);
  Return(example2.js:3) . . . cursor.cursor(‘a’);
  Crash(example2.js:4) assert(deepCursor . . .);
```

This crash path shows that the object was created on line 242 in function makeCursor in cursor.js, which looks as follows:

```javascript
236 function makeCursor(r, k, c, value) {
237 if (arguments.length < 4) {
238 value = r.getIn(k);
239 }
240 var s = value && value.size;
241 var CursorClass = Iterable.isIndexed(
242 value) ? IndexedCursor : KeyedCursor;
243 return new CursorClass(r, k, c, s);
244 }
```

Looking at this code, we see that an object with the wrong type could be allocated for two reasons: (1) function isIndexed is buggy, or (2) value somehow has an incorrect value. We also note that makeCursor implements overloading by checking the number of arguments on line 237.

The crash path produced by CROWDIE not only tells us that the object originated from line 242 but also provides information about the call stack when this object was created. This call stack can be obtained by observing that Return labels on the produced path must have had matching calls that occurred earlier. From this call stack, we learn that makeCursor was invoked by subCursor:

```javascript
249 function subCursor(cursor, k, value) {
250 return makeCursor(
251 cursor._rootData ,
252 newPath(cursor._keyPath , k),
253 cursor._onChange ,
254 value
255 );
```

Crucially, we observe that subCursor always passes four arguments to makeCursor on line 250 and that the fourth argument value is an argument to subCursor itself. Since it always passes four arguments, the condition on line 237 will always evaluate to false when called from subCursor. Furthermore, our tool tells us that subCursor, in turn, was called by KeyedCursorPrototype.cursor. The calling code of that function looks as follows:

```javascript
187 ..subCursor(this, s);
```

Here, we can see that subCursor is passed two arguments even though it has three parameters, so the third parameter will take on a default value of undefined. The subCursor function in turn calls makeCursor with this parameter, which checks if it received four arguments instead of checking if the fourth argument has the default value undefined! The core issue is thus that makeCursor implements an overloading check in a way that subCursor did not anticipate.

The fix6 for the issue is to change the overloading check on line 237 to value === undefined.

These examples demonstrate how CROWDIE can provide information that is vital for understanding and fixing bugs, especially in cases where the error message and stack trace of a crash provides insufficient information. Note that CROWDIE is not a fully automated debugging process: a nontrivial amount of human ingenuity may still be needed. However, in both cases, the crash path was sufficient to debug the issue. In particular, the (typically much longer) full execution path from the start of the application was not needed. Here, we have presented the crash paths as plain text, but we can imagine a scenario where IDEs naturally show the paths and allow the programmer to “jump” forwards and backwards through the statements on the path.

3. TECHNIQUE

A high-level architecture of the kind of system in which we envision our technique to be embedded is depicted in Figure 1. We assume a distribution model where users (shown on the left) install their applications through a central server (shown on the right). For example, in the case of client-side web applications the server is responsible for sending the JavaScript code to the users. As another example, in the case of a server-side application, the group of “users” may consist of a cluster of servers running the application. Finally, we envision that app stores for (mobile or non-mobile) devices could be extended with the techniques presented in this paper. To make this practical, an approach to feedback-directed instrumentation would be required that does not require pushing out new versions to users frequently. The latter could be accomplished by having selected parts of the instrumentation in an application be enabled or disabled based on an instrumentation policy that it periodically receives from the server.

The server in Figure 1 has several components, including an instrumentor component for instrumenting applications according to an instrumentation policy that specifies the functions that need to be traced. It also contains an analyzer component that decides which functions should be instrumented based on an analysis of traces of crashing executions that it receives from users and produces an instrumentation policy accordingly. In the scenario we envision, the instrumentation policy is updated repeatedly, each time the same failure is encountered.

---

4https://github.com/facebook/immutable-js/pull/381
5Commit 91af8fb4100ead6375ceba239ad624a4453684429

We define similar heuristics for other types of statements. For example, if the
statement has a suspicious operation [11], or a security policy violation. When this happens, the added instrumentation ensures that a crash path is recorded that reflects the set of functions specified in the instrumentation policy. This crash path identifies at least in what function the crash occurred and what local and global variables may be relevant to the crash (see Section 4 for more details). The instrumentation ensures that this crash path is uploaded to the analyzer component of the server, which in response updates the instrumentation policy accordingly. Note that, in general, the crash paths that users upload to the server are partial crash paths, in the sense that they may not contain the full flow of control from the allocation of an object to the point where the crash occurred. However, when the analyzer component determines that a bug was localized because the crash path is complete, the complete crash path is passed to the developer and all instrumentation is disabled for the entire user population.

Various features can be added to the architecture discussed above. For example, the server can be configured to trace multiple bugs concurrently, and these efforts can be crowdsourced over different subsets of the user population. Furthermore, the server can compare crash paths for different bugs that it is tracking concurrently, try to determine when they are duplicates, and prefer the shortest candidate.

### 3.1 Execution Paths

The grammar shown in Figure 2 defines the structure of execution paths constructed by our technique. An execution path \( p \in \text{Path} \) is a sequence of labels that are recorded during program execution. We capture intra-procedural control-flow using the three labels:

\[
\text{Intra} := \text{Branch}(s,c) \mid \text{Start}(s) \mid \text{Crash}(s)
\]

The \text{Branch}(s,c) label records the value of a conditional \( c \) in an if or while statement \( s \). The \text{Start}(s) label records that the object of interest originates from statement \( s \). The \text{Crash}(s) label records the statement \( s \) where the program crashed. We use heuristics to determine the object(s) of interest in an a crashing statement. For example, if the statement \( o.f() \) crashes because \( o.f \) is undefined then the object \( o \) is of interest. On the other hand, if the statement crashes because \( o.f \) is not a function then \( o.f \) is of interest.

We define similar heuristics for other types of statements.

We say that an execution path that begins with a \text{Start} label and ends with a \text{Crash} label is a crash path. Intuitively, a crash path identifies a statement where an object was created and a sequence of control-flow decisions leading to a crash where that object was somehow involved. A path that ends with the \text{Crash} label, but does not begin with the \text{Start} label is a partial crash path.

Inter-procedural control-flow is tracked using four labels:

\[
\text{Inter} := \text{Call}(s,f) \mid \text{Return}(s) \mid \text{Enter}(f) \mid \text{Exit}(f)
\]

The \text{Call}(s,f) label records a function invocation from call site \( s \) to function \( f \). The \text{Return}(s) label records the completion of a call at statement \( s \). The \text{Enter}(f) label records that the control-flow has entered function \( f \). The \text{Exit}(f) label records that the control-flow has left function \( f \).

Intuitively, the \text{call}/\text{return} labels represent a function invocation as seen from the caller, whereas the enter/exit labels represent a function invocation as seen from the callee. The reason for requiring both is that our technique does not instrument every function, and thus to observe whether or not calls are missing from a trace, we must record information inside both the caller and the callee. In particular, an execution path that has the labels

\[
\text{Call}(s,f) \rightarrow \text{Enter}(f) \rightarrow \text{Exit}(f) \rightarrow \text{Return}(s)
\]

is complete because it records the invocation of \( f \) from \( s \), the execution inside \( f \) and the return of control to \( s \). On the other hand, the execution path \text{Call}(s,f) \rightarrow \text{Return}(s), which lacks the \text{Enter} and \text{Exit} labels, records a call to an uninstrumented function \( f \) (if \( f \) was instrumented then its execution would have generated the appropriate enter/exit labels). We will discuss in Section 3.3 how this information is used to determine whether a crash path is complete.

**Example I.** Consider the code fragment of Figure 3 and the execution path that is generated when \( f \) is invoked with the arguments \( x = 7, y = 8 \) and \( o = {} \) (the empty object): For this example, execution crashes when line 5 is reached, because \( o\.missingMethod \) has the value undefined at that point, and any attempt to call \( undefined \) as a function results in a crash. The full crash path\(^6\) is:

\[
\text{Start}(s_1) \rightarrow \text{Call}(s_7,f) \rightarrow \text{Enter}(f) \rightarrow \text{Branch}(s_3,\text{true}) \rightarrow \text{Branch}(s_4,\text{true}) \rightarrow \text{Crash}(s_5)
\]

**Example II.** In the example of Figure 3, the crash happened due to the arguments passed to \( f \) and a stack trace would contain all necessary information to debug the issue. However, this is not always the case as illustrated by the program of Figure 4. For this example, the crash path is:

\[
\text{Start}(s_9) \rightarrow \text{Branch}(s_{10},\text{true}) \rightarrow \text{Exit}(f) \rightarrow \text{Return}(s_{13}) \rightarrow \text{Branch}(s_{14},\text{true}) \rightarrow \text{Crash}(s_{15})
\]

---

\(^6\)We will use the notation \( s_l \) where \( l \) is some line number in this example and subsequent examples to identify the program construct at line \( l \).
includes two call labels, labeled \textbf{Enter} and \textbf{Exit}. Initially, the crash is observed from the function in which the crash occurs. Figure 6 illustrates this concept. Initially, the crash is observed from the function in which the crash occurs. The call labels since \textbf{Enter} and \textbf{Exit} are observed. In the fourth iteration, functions \texttt{g}, \texttt{h}, \texttt{j}, \texttt{k}, and \texttt{l} are instrumented. Now \texttt{j} is instrumented, and each object that is allocated inside a function is tagged with a special property recording where it was created. When the crash occurs, the instrumentation discovers that this property is set, and reports the crash path: \texttt{Start(j) \rightarrow Return(g) \rightarrow \cdots \rightarrow Call(k, m) \rightarrow Crash(s24)} (this path is highlighted in Figure 6 using dashed red lines). Note that the path does not include any control-flow that happened prior to entering \texttt{j}. In the end, \texttt{f}, \texttt{g}, \texttt{h}, \texttt{j}, \texttt{k}, \texttt{l}, and \texttt{m} have been instrumented, whereas function \texttt{i} and the top-level-code are left uninstrumented.

This feedback-directed process continues until the creation site of the object is discovered. In the worst case, the entire program may end up being instrumented, including functions whose execution was irrelevant to the observed crash (e.g., function \texttt{h} in the example). However, as we shall see in Section 5, it is often the case that only a small fraction of the code is instrumented in practice. A limitation of the technique is that it cannot locate the "source" of uninitialized variables and fields, since the absence of data flow cannot be attributed to any particular statement in the program.

### 3.2 Feedback-Directed Instrumentation

Figure 5 shows a small program that we will use to illustrate our feedback-directed instrumentation approach. In this example, the function \texttt{f} is called by top-level code and invokes \texttt{g}. This function, in turn, invokes \texttt{h}, \texttt{j}, and \texttt{k}. The call to \texttt{h} invokes \texttt{i}. Function \texttt{j} creates an empty object and assigns it to variable \texttt{x}. The call to \texttt{k} invokes \texttt{i} and \texttt{m}. Inside \texttt{m} a crash occurs due to a missing method on \texttt{x}.

Our goal is to discover the crash path beginning with the creation of the empty object inside \texttt{j} and ending with the crash inside \texttt{m}. We could discover such paths by instrumenting the entire program, but that would be costly. Instead, we propose to perform instrumentation of the program in a feedback-directed manner, where we gradually instrument more functions until the complete crash path is discovered.

The intuition behind our approach is that instrumentation is performed in a breadth-first manner starting backwards from the function in which the crash occurs. Figure 6 illustrates this concept. Initially, the crash is observed to occur inside \texttt{m}, which causes \texttt{m} to be instrumented. The next time the crash is seen, it is observed that \texttt{m} was called from \texttt{k}, so \texttt{k} is instrumented as well. Since \texttt{k} contains two call sites its execution will produce a path that includes two call labels, labeled \texttt{k1} and \texttt{k2} in Figure 6. In the third iteration, \texttt{k} and \texttt{m} are instrumented and calls from \texttt{g} to \texttt{k} and from \texttt{k} to \texttt{i} are observed. In the fourth iteration, \texttt{g}, \texttt{k}, \texttt{l}, and \texttt{m} are instrumented and calls to \texttt{h} and \texttt{j} are observed. In the fifth and final iteration, functions \texttt{f}, \texttt{g}, \texttt{h}, \texttt{j}, \texttt{k}, \texttt{l}, and \texttt{m} are instrumented. Now \texttt{j} is instrumented, and each object that is allocated inside a function is tagged with a special property recording where it was created. When the crash occurs, the instrumentation discovers that this property is set, and reports the crash path: \texttt{Start(j) \rightarrow Return(g) \rightarrow \cdots \rightarrow Call(k, m) \rightarrow Crash(s24)} (this path is highlighted in Figure 6 using dashed red lines). Note that the path does not include any control-flow that happened prior to entering \texttt{j}. In the end, \texttt{f}, \texttt{g}, \texttt{h}, \texttt{j}, \texttt{k}, \texttt{l}, and \texttt{m} have been instrumented, whereas function \texttt{i} and the top-level-code are left uninstrumented.

This feedback-directed process continues until the creation site of the object is discovered. In the worst case, the entire program may end up being instrumented, including functions whose execution was irrelevant to the observed crash (e.g., function \texttt{h} in the example). However, as we shall see in Section 5, it is often the case that only a small fraction of the code is instrumented in practice. A limitation of the technique is that it cannot locate the "source" of uninitialized variables and fields, since the absence of data flow cannot be attributed to any particular statement in the program.

### 3.3 Algorithm

We now present a high-level description of our algorithm for feedback-directed instrumentation. A key challenge in computing crash paths in a feedback-directed manner is dealing with situations where fragments of a path are missing because functions are called that have not been instrumented yet. For example, assume we have a situation where an instrumented function \texttt{f} invokes an uninstrumented function \texttt{g}. This gives rise to a path like:

\[ \cdots \rightarrow \text{Call}(s, g) \rightarrow \text{Return}(s) \rightarrow \cdots \]

Note that, since \texttt{g} is not instrumented, no enter/exit labels are generated for it. Such a path is incomplete and indicates that \texttt{g} should be instrumented in the next iteration.

Figure 7 shows our algorithm as a function that takes one argument, \texttt{s}, the statement where the crash occurred. We maintain the last seen execution path in variable \texttt{p} and the set of instrumented functions in \texttt{I}. Initially, the path contains only the \texttt{Crash} label. We then repeatedly instrument and execute the program until a crash occurs. The outer
Figure 7: Pseudo-code for the algorithm.

```plaintext
Feedback-Directed-Instrumentation(s ∈ Stm)
1 var p: Path = Crash(s) // the current path
2 var l: P(Fun) = {s.fun} // instrumented functions
3 repeat
4   for each label l on path p
5     if instrument callee:
6       if l ∈ Call(s, f) do I = I ∪ {f}
7       // instrument caller:
8       if l ∈ Enter(c, f) do I = I ∪ {c}
9     repeatedly execute the program until a crash occurs
10    if p' is the path recorded in the last execution
11       if p' is a (partial) crashing path that matches p
12       p = p' // a longer path has been found
13 until p begins with a Start label and contains
14 return p // report the crashing path to the developer
```

Figure 8: An event-driven Node.js program.

```plaintext
var cache = {};
var net = require('net');
var server = net.createServer(function(c) {
  if (cache.data.length != 0) {
    c.write(cache.data);
  }
  return;
}
server.listen(80, function() {
  fs.readFile('a.txt', function(err, data) {
    cache.data = data;
  });
});
```

This allows the technique to trace control flow backwards through event listeners.

In general, many similar executions may exist in which event handlers are scheduled in different orders. In its current form, our technique does not attempt to identify and exploit similarities between executions. For example, consider a scenario where a failing execution involves a sequence of event handlers \( f,g \), and another involving a sequence \( f,h,g \), where event handler \( h \) is unrelated to the failure. In such cases, it may be preferable to focus only on the crash path for the former execution, because it omits information unrelated to the failure. In principle, our technique can be extended to give priority to executions in which the fewest number of event listeners is executed before a crash.
4. IMPLEMENTATION

We have implemented our technique using the Jalangi instrumentation framework [28] in a tool called CROWDIE.

**Overall Structure.** The implementation splits the technique into two phases. In the detection phase, the program is instrumented to assign every function object a unique identifier and a global error handler is installed. This handler catches any thrown exception that reaches the top-level and records in which function the exception was thrown. The detection phase also determines which event listeners (if any) were executed before the crash. The detection phase is run repeatedly until an exception is encountered. Its runtime overhead is negligible since only one instruction per function declaration is added. A separate isolation phase implements the feedback-directed technique of Section 3.3. Only the last 10,000 labels are tracked, to prevent the crash path from growing too large.

**Instrumentation Details.** Figure 9 presents some of the instrumentation rules used in our tool. Here, we aim to be informal and do not describe the finer details of the transformations used, and just sketch their overall structure. More details can be found in the original paper on the Jalangi instrumentation framework [28]. A conditional statement labeled $s$ is instrumented to record the Branch label (lines 38–41). Lines 42–43 show how a function call $s$ is instrumented to record Call and Return labels. Likewise, lines 44–47 show how a function declaration $f$ is instrumented to record the Enter and Exit labels. Finally, an object creation statement $s$ is instrumented to record the length of the path at the moment of creation (lines 48–50). This means that every object (created inside a function selected for instrumentation) knows its offset inside the path. In addition to these instrumentation steps, we assume that the program contains a special crash($o$) function call where $o$ is the object of interest. This call is intercepted by the instrumentation and generates the Crash($o$) label, but it also checks if $.path_offset$ is set to the object $o$. If so, the origin of $o$ has been found, and the Start label is inserted at the offset. If not, we have not yet instrumented the function in which the object was created and no Start label is generated.

**Other JavaScript Features.** Our tool implements the technique of Section 3.3 as well as the mechanisms related to event handling discussed in Section 3.4. Features such as exceptions, getters and setters, and native functions require additional support, and can be added with modest effort. Support for these features is in progress, but has not been needed in any of the case studies discussed in Section 5 (and we did not exclude any candidate programs due to lack of feature support).

5. EVALUATION

The evaluation of our technique aims to answer the following research questions:

Q1: How useful are the crash paths computed by our tool for understanding and fixing real bugs?

Q2: How many times must a crash be observed before the crash path has been found?

Q3: How much runtime overhead is incurred by users of our tool for computing crash paths?

The rationale behind Q1 is to determine whether the information computed by our tool is useful for debugging, particularly in cases where the information contained in error messages and stack traces is insufficient. The purpose of Q2 is to determine if the number of times that a bug needs to be encountered is reasonably low. This is relevant because if the same crash path needs to be encountered many times by different users, then the usefulness of the technique would be limited to bugs that occur very often. Lastly, Q3 aims to determine whether runtime overhead is acceptable.

5.1 Experimental Methodology

CROWDIE produces information that is intended to assist developers with debugging, but manual effort remains required in diagnosing the problem. Therefore, we opt for an evaluation based on case studies, in which we apply our tool to 10 real bugs in open source programs taken from GitHub. For these programs, we compute crash paths with our tool, manually inspect these crash paths to determine whether they are helpful (Q1), and measure various aspects of the tool’s execution behavior to answer Q2 and Q3.

**Selection Criteria.** We chose subject programs by looking at bug reports for popular JavaScript projects on GitHub. These applications had to satisfy some limitations of our implementation: (a) the program did not make use of eval, and (b) the program was runnable on Node.js version 0.12. Furthermore, we required that the reported bug could be reproduced with modest effort, and that the reported issue had an identifiable place in the source code where the problem was observable (i.e., a crash caused by an exception being thrown, an assertion failure, or an incorrect returned value). Lastly, we excluded “easy bugs” where the bug was local to the same function in which the crash occurred, i.e., situations where the line number in an error message or in a stack trace would suffice to diagnose the problem quickly.

**Subject Programs and Issues.** For triggering the bug of interest we use small bug triggering examples provided in the bug reports, as seen twice in Section 2. This creates a much simpler scenario than the one CROWDIE is intended to be used in, but no bug reports describe a complete scenario where the bug is encountered in a production environment. Each bug reporter has spent time manually creating these.
small examples before the reporting the bug. CROWDIE could potentially alleviate the need for this manual work.

The leftmost four columns of Table 1 identify the selected subject programs and their associated bug reports (all taken from GitHub). Each row in the table corresponds to one bug report and one debugging scenario. The Program column shows the name of the application/library, the Issue column shows the number assigned to the bug report. The Lines and Functions columns show the number of lines in the source code (including whitespace and comments) and the total number of function declarations, respectively.

 AlaSQL is a JavaScript SQL database. Buckets is a data structure library. Esprima is a JavaScript parser. Immutable is a collection library. Loki is a JavaScript database. Redis is a Redis client for JavaScript. The bugs include corrupted, incorrect control-flow due to argument passing, but multiple labels can be present on each of the 54 source code lines in 24 functions corresponding to 25% of the total number functions in the program. Finally, the crash path contained 219 labels distributed over 54 source code lines in 24 functions corresponding to only 16% of the total number of functions. Looking at 219 labels might seem like a daunting task for a programmer, but multiple labels can be present on each of the 54 source code lines, e.g., in the case of loops, and some labels are implied by others, e.g., implied by others, e.g.,

Process. In the case studies, we used the following 5-step process for diagnosing a bug report using our tool: (1) run the program and observe that a crash occurs; (2) manually identify the function and line which caused the crash; (3) manually select a subset of relevant local and global variables related to the function and line of interest (frequently only a single variable was selected). In the fully automated scenario the variables would be selected by heuristics, as discussed earlier; (4) run our tool with the given line and variables as input to compute a crash path; (5) manually understand and debug the issue using the computed crash path. In some cases, the crash was caused by an exception that was thrown from a generic error handling function. In such cases, we followed the above steps, except that we focused on the previous function on the call stack.

5.2 Experiments

We now discuss the results obtained by running our tool.

Quantitative Results: Instrumentation and Paths. The columns under the header Instrumentation in Table 1 show some key characteristics of our feedback-directed instrumentation method. The column Iterations shows the number of times the same bug had to occur for the technique to find the complete crash path. Moreover, the column Functions shows the number of functions instrumented by the technique in its final iteration, both as an absolute number and as a percentage of the total number of functions. For example, for Esprima issue #0560, 7 executions were required before the complete crash path was found plus one execution to detect the crash in the first place.

The columns under the header Recorded Path report characteristics of the complete crash path found by the technique. Here, the column Length reports the length of the crash path (i.e., the total number of labels), and the column Func. counts the number of functions on the crash path. Regarding the last metric, recall that a function might be instrumented although it is not on the crash path, so it is interesting to see whether the technique instruments many functions unnecessarily. Returning to Esprima issue #0560, during the last iteration 37 functions were instrumented corresponding to 25% of the total number functions in the program. Finally, the crash path contained 219 labels distributed over 54 source code lines in 24 functions corresponding to only 16% of the total number of functions. Looking at 219 labels might seem like a daunting task for a programmer, but multiple labels can be present on each of the 54 source code lines, e.g., in the case of loops, and some labels are implied by others, e.g., Call/Enter. Thus, the programmer has to look at significantly fewer statements/labels.

<table>
<thead>
<tr>
<th>Program and Issue</th>
<th>Instrumentation</th>
<th>Recorded Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>Issue</td>
<td>Lines</td>
</tr>
<tr>
<td>AlaSQL (v0.0.36)</td>
<td>#0092</td>
<td>12,561</td>
</tr>
<tr>
<td>Bucket-JS (v1.81)</td>
<td>#0006</td>
<td>2,393</td>
</tr>
<tr>
<td>Esprima (v2.1)</td>
<td>#0299</td>
<td>4,410</td>
</tr>
<tr>
<td>Esprima (v1.2)</td>
<td>#0560</td>
<td>3,762</td>
</tr>
<tr>
<td>Esprima (v2.2)</td>
<td>#1042</td>
<td>5,314</td>
</tr>
<tr>
<td>Immutable (v3.6.2)</td>
<td>#0381</td>
<td>5,147</td>
</tr>
<tr>
<td>Immutable (v3.7.3)</td>
<td>#0489</td>
<td>4,935</td>
</tr>
<tr>
<td>Loki (v1.0)</td>
<td>#0042</td>
<td>2,599</td>
</tr>
<tr>
<td>Loki (v1.0)</td>
<td>#0046</td>
<td>2,599</td>
</tr>
<tr>
<td>Redis (v0.7.1)</td>
<td>#0067</td>
<td>1,529</td>
</tr>
</tbody>
</table>

Table 1: Summary of main results from the case study.

<table>
<thead>
<tr>
<th>Program and Issue</th>
<th>Performance benchmarks</th>
<th>Unit tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlaSQL (v0.0.36)</td>
<td>#0092</td>
<td>14</td>
</tr>
<tr>
<td>Esprima (v2.1)</td>
<td>#0299</td>
<td>7</td>
</tr>
<tr>
<td>Esprima (v1.2)</td>
<td>#0560</td>
<td>7</td>
</tr>
<tr>
<td>Esprima (v2.2)</td>
<td>#1042</td>
<td>7</td>
</tr>
<tr>
<td>Immutable (v3.6.2)</td>
<td>#0381</td>
<td>6</td>
</tr>
<tr>
<td>Immutable (v3.7.3)</td>
<td>#0489</td>
<td>6</td>
</tr>
<tr>
<td>Loki (v1.0)</td>
<td>#0042</td>
<td>9</td>
</tr>
<tr>
<td>Loki (v1.0)</td>
<td>#0046</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 2: Summary of performance results.
Quantitative Results: Performance. Column Func. under the heading Instrumentation in Table 1 shows the number (and percentage) of functions instrumented in the final iteration by the feedback-directed technique. Only between 2% and 31% of functions are ultimately instrumented, suggesting good potential for performance improvement compared to full instrumentation.

To measure actual impact on runtime performance we exercised the programs using benchmarks and unit tests available in the source repositories. Table 2 shows the results.

Starting with the performance benchmarks, the row for AlaSQL issue #0092 shows that the benchmark program contained 14 different executions and the original program took 95 seconds to execute them all. Using our feedback-directed approach, 34 functions are instrumented (see Table 1), resulting in a total running time of 188 seconds, i.e., a slowdown by a factor 2x. In contrast, running the benchmark with full instrumentation took 1929 seconds, i.e., a factor 20x overhead. Continuing, AlaSQL’s unit test suite comprises 415 individual tests which took 15 seconds to run originally; this was 3x slower with feedback-directed instrumentation, and 11x slower with full instrumentation. For the three Esprima issues there is negligible difference in performance between feedback-directed and full instrumentation. For the remaining 5 programs there are significant differences ranging from 1.1x to 121x.

In general, the performance benchmarks show a larger performance difference than the unit tests when comparing partial and full instrumentation. We postulate this is because the unit tests cover a broad range of functionality and exercise the code more evenly (including the instrumented code), whereas the benchmark programs presumably exercise only performance critical components of the code that may avoid instrumentation with our technique.

We investigated why our technique worked so poorly for Esprima. We found that Esprima is divided into two components; a lexer and a parser. In each case, an unexpected token was generated by the lexer, and then caused a crash in the parser. The problem was not the actual token itself, but the control-flow that followed. Regardless, this architecture and the tight connectedness of the parser itself meant that large parts of the program were ultimately instrumented.

The Buckets and Redis programs were not included in Table 2 since they had no performance benchmark suites.

In summary, if we exclude the best and worst running times for both techniques, then feedback-directed instrumentation has a typical overhead of between 2x–9x compared to an overhead of 8x–90x for full instrumentation.

Usefulness. We previously discussed two of our case studies in Section 2 that illustrated how it can be useful to know: (1) where an object was allocated, (2) what the call stack looked like during that allocation and (3) what properties were not written since that allocation. Space limitations keep us from discussing the remaining 8 case studies in detail, but they cover similar, and more complex, issues. In each case, the crash path provides crucial information about a property of interest. In each case, some amount of human ingenuity remains necessary but we believe that the crash paths computed by CROWDIE would be helpful for developers. In particular, the size of the code base that developers need to consider is greatly reduced by allowing them to focus on only the source lines in the crash path; these reductions can be seen in Table 1. A detailed analysis of each of these case studies can be found in a technical report [20].

5.3 Summary of Results

We can now answer the research questions stated earlier.

Q1. The crash paths computed by CROWDIE can provide useful assistance to developers, but by themselves are not a panacea: some amount of human ingenuity remains necessary to complete the debugging task.

Q2. In our case studies, between 4 and 9 iterations (executions) were needed to discover the crash path. This is a relatively low number, suggesting that our technique may be generally useful for widely deployed software, except for bugs that are very rarely encountered.

Q3. The typical runtime overhead of the feedback-directed instrumentation in CROWDIE ranges from 2x–9x. While this is often dramatically better than the overhead of full instrumentation (8x–90x), work remains to be done on making the instrumentation more efficient. Furthermore, as the results for Esprima suggest, the architecture of certain applications may make them unsuitable candidates for the technique.

5.4 Threats to Validity

We selected our subject programs based on issues reported on GitHub. While these programs are widely used, they may not be representative of all programs and likewise the reported bugs that we investigated may not be representative either. Furthermore, we selected bug reports that involved crashes (thrown exceptions, assertions errors, ...) but not every bug necessarily manifests itself as a crash. When we debugged these issues we had no prior knowledge of the program. Thus, it is possible that a developer familiar with source code might have debugged the program differently. On the other hand, the debugging scenario we faced, with no prior knowledge of the codebase, is the hardest possible.

Another valid concern is that the experiments are all based on small snippets of code that trigger the bugs. These scenarios may differ from real-life deployment scenarios, for which the results could be very different from the ones we report here. These more complex scenarios might require longer crash paths and make CROWDIE more expensive to use, but extra complexity will also make the partial instrumentation of CROWDIE even more tractable compared to naive full instrumentation.

6. RELATED WORK

Numerous techniques have been developed to support debugging. A key property of our approach is that it helps obtaining critical information about failures that occur in deployed JavaScript programs. This setting is particularly well suited for crowdsourced analysis that collects data from user executions, since it is easy to deploy new instrumentation policies. Although we focus on errors that manifest as uncaught exceptions in the JavaScript programs, our technique works more generally, for example, also when debugging assertion failures, errors related to suspicious coercions and other bad coding practices [11], or DOM-related faults [26].

Record and replay techniques. The ability to record and replay failing executions is valuable for debugging, as demonstrated by, e.g., Narayanasamy et al. [23]. We argue that knowing the part of the execution history that we call
the crash path is often sufficient for the developer to debug the crash, and is cheaper to produce in a JavaScript setting. The BugRedux framework by Jin and Orso [12] gathers partial execution traces from deployed programs and then uses symbolic execution to synthesize reproducible failures. SymCrash [8] instead uses dynamic symbolic execution and more selective instrumentation. We avoid the need for symbolic execution by the use of iterative instrumentation. Some techniques utilize static analysis to reduce the instrumentation overhead [24, 31], however, the dynamic language features in JavaScript are known to cause considerable challenges for static analysis [3].

One challenge to dynamic analysis of deployed JavaScript applications is that instrumenting JavaScript programs is known to incur a large runtime overhead. Techniques that attempt to reduce the overhead by only logging sources of nondeterminism, as e.g. Chronicler [6], are difficult to apply to JavaScript. Even though our implementation uses the state-of-the-art Jalangi infrastructure [28], we observe a substantial runtime overhead when full instrumentation is enabled, which necessitates the more selective instrumentation. Several other tools described in the literature are capable of recording live executions, which can subsequently be analyzed by the developers when debugging. Mughot [21] is capable of capturing events using unmodified browsers. Similarly, WaRR [4] and, more recently, Timelapse and Dolos [7] can in principle provide full information about failing executions. Ripley [30] instruments JavaScript applications to enable replaying executions on the server with the purpose of ensuring computational integrity, and DoDOM [27] performs replaying to infer DOM invariants, not to aid debugging of crashes that users encounter. However, we have seen no concrete usage of these tools in real-world debugging. We believe that record/replay tools usually require that the record and replay environments, which include browser configuration, browser state, persistent data (e.g., cookies), network speed, processor speed, and operating system configuration, to be exactly same. Such a requirement is too strict and difficult to reproduce in real-world scenarios where an application can be run by any user under any possible environment. CrowdIE does not suffer from such limitations because it does not aim to faithfully replay a buggy execution—it simply tries to collect a relevant portion of the control-flow path using lightweight and targeted instrumentation.

Fault localization techniques. Several automated fault localization techniques [13, 14, 18] rely on statistical data from user executions collected in order to assist developers with debugging. Such information may be useful for debugging, but it does not provide the crash paths that we argue are valuable when debugging. For future work, it will be interesting to perform a direct experimental comparison with such techniques. Liblit et al. [19] interestingly note that “the stack contains essentially no information about the bug’s cause” in half of the bugs considered in their experiments, which aligns well with our observation that more information about the failing executions is often needed. The Holmes tool [9] localizes faults using path profiles, which are constructed by iteratively instrumenting and re-deploying programs similar to our technique. Unlike crash paths, path profiles only provide statistical information about intra-procedural and acyclic paths. The AutoFLox tool by Ocariza et al. [25] performs fault localization for JavaScript under the assumption that a complete failing execution is known, unlike our technique that aims to automatically find the crash path. Our algorithm for finding crash paths is also related to algorithmic program debugging [29] but does not require guidance by the programmer or by formal specifications.

Dynamic program slicing. Our notion of crash paths is related to the use of dynamic slicing for debugging [1, 2, 17, 32]. Such techniques typically compute slices backwards, which resembles our construction of crash paths, but usually assuming that a complete execution trace is already known. Although many variations of dynamic slicing have been proposed, they generally differ from our notion of crash path, which comprises a path from the creation of an object of interest to a crashing statement, without including all dependencies earlier in the execution. In principle, slicing may be applied subsequently to the crash path to filter away instructions that are likely irrelevant.

Other crowdsourced analysis techniques. Crowdsourced analysis has also been suggested for other debugging scenarios. For example, Kerschbaum et al. [16] use crowdsourced analysis to test for information flow vulnerabilities by letting different users track different information flows so that a crowd of users can achieve high coverage of all information flows without imposing unacceptable performance overhead on any single user. Likewise, Kasikci et al. [15] test potential data races by distributing them over a set of users by giving each user an instrumented version of an application where the purpose of the added instrumentation code is to confirm whether the potential race happens in practice. To lower the overhead, instrumentation is enabled probabilistically. In contrast, we enable instrumentation only when a crash occurs, then increase instrumentation until a crash path is discovered, and finally disable the instrumentation.

7. CONCLUSIONS AND FUTURE WORK

Many bugs manifest themselves as objects that have incorrect property values when a failure occurs. For such bugs, error messages and stack traces often provide insufficient information for diagnosing the problem. We have proposed the notion of a crash path, which reflects the control flow from the allocation of a selected object of interest to the crashing statement, and argue that this often provides useful information for debugging such problems.

In principle, crash paths can be computed by executing a fully instrumented version of a program, but this incurs prohibitive runtime overhead. Therefore, we have developed a feedback-directed instrumentation technique for computing crash paths that we envision to be deployed in a crowdsourced deployment scenario. We implemented the technique in a tool called CrowdIE, and evaluated it in 10 case studies by using it to debug real-world issues reported on GitHub for which error messages and stack traces are insufficient to find and fix the bugs. In these case studies, the feedback-directed technique requires the same crash to be encountered 3 to 10 times, and the runtime overhead generally compares favorably to that of full instrumentation.

We envision several directions for future work, including achieving a deeper understanding in which situations the feedback-directed technique is useful, and reducing instrumentation overhead. We also plan to explore alternative instrumentation strategies and the use of more detailed instrumentation once a complete crashing path has been identified in order to prune irrelevant statements from the path.
References


