“Synthesizing Input Grammars”: A Replication Study

Bachir Bendrissou
CISPA Helmholtz Center For Information Security
Germany
bachir.bendrissou@cispa.de

Rahul Gopinath
CISPA Helmholtz Center For Information Security
Germany
rahul.gopinath@cispa.de

Andreas Zeller
CISPA Helmholtz Center For Information Security
Germany
zeller@cispa.de

Abstract
When producing test inputs for a program, test generators ("fuzzers") can greatly profit from grammars that formally describe the language of expected inputs. In recent years, researchers have studied means to recover input grammars from programs and their executions. The GLADE algorithm by Bastani et al., published at PLDI 2017, was the first black-box approach to claim context-free approximation of input specification for non-trivial languages such as XML, Lisp, URLs, and more.

Prompted by recent observations that the GLADE algorithm may show lower performance than reported in the original paper, we have reimplemented the GLADE algorithm from scratch. Our evaluation confirms that the effectiveness score (F1) reported in the GLADE paper is overly optimistic, and in some cases, based on the wrong language. Furthermore, GLADE fares poorly in several real-world languages evaluated, producing grammars that spend megabytes to enumerate inputs.

CCS Concepts: • Security and privacy → Software reverse engineering; • Software and its engineering → Software maintenance tools; Parsers.

Keywords: context-free grammar, inference, GLADE

1 Introduction
Generating test inputs for a program ("fuzzing") is much more effective if the fuzzer knows the input language of the program under test—that is, the set of valid inputs that actually leads to deeper functionality in the program. Input languages are typically characterized by context-free grammars, and the recent interest in fuzzing thus has fueled research in recovering input grammars from existing programs.

The GLADE algorithm by Bastani et al., published in “Synthesizing Input Grammars” at PLDI 2017 [6], automatically approximates an input grammar from a given program. In contrast to other approaches, GLADE does not make use of program code to infer input properties. Instead, it relies on feedback from the program whether a given input is valid or not, and synthesizes a multitude of trial inputs to infer the input grammar. GLADE claims substantial improvement over existing algorithms both in terms of accuracy as well as in terms of speed of inference. In particular, GLADE claims better performance over even the current best regular language inference techniques such as L-Star [4] and RPNI [20]. Further, GLADE claims to be able to recover the input grammar for complex languages such as Ruby, Python, and JavaScript in a couple of hours [6, Figure 6].

In recent work [18], however, Kulkarni, Lemieux, and Sen found that the F1 scores—a measure for the accuracy of the inferred grammar—produced by the GLADE tool were much lower than the scores reported in the GLADE paper, for instance XML (0.42 compared to 0.98) and Lisp (0.38 compared to 0.97) [18, Table I].

This observation prompted us to investigate the GLADE algorithm in detail. Given that the algorithm reported in the paper is the central contribution, we reimplemented the GLADE algorithm completely from scratch using the algorithm description given in the paper [6].

We call the implementation by Bastani et al. GLADE-I1, and we call our implementation GLADE-II to differentiate both where there is ambiguity. We used our implementation to evaluate synthesized grammars for programs given in the original paper [6]. These include URL, Grep, Lisp, and XML. We further evaluated GLADE-II on several other small grammars such as different parenthesis grammars, Ints, Decimals, and a few real-world complex grammars such as Lua,
Blackbox approaches, in contrast, extract grammars from the potential of grammars for producing syntactically valid mine if an input is valid or not. Clark’s algorithm [8] uses a membership queries, executing the program only to determine candidates for generalization.

1. The F1 score that we obtained from GLADE-II is much lower than the F1 scores reported by Bastani et al. This confirms the observation by Kulkarni et al. [18].
2. Bastani et al. use handwritten grammars for computing precision and recall. We found that the handwritten Grep grammar was far more permissive than the program, resulting in spurious results.
3. The precision scores of simple real-world grammars such as Decimals (0.84), and JSON (0.53) is lower than expected considering the high values reported by GLADE for other programs, and considering their simplicity.
4. The recall of JSON (0.79) is lower than expected considering the simplicity of its specification.
5. Similar to Grep, the XML grammar used by GLADE-I was more permissive than the actual XML specification.
6. GLADE is unable to learn and synthesize valid XML even when a correct XML grammar is used to learn from.
7. GLADE cannot learn trivial context-free languages such as \( a^nb^n \) or the language of palindromes.
8. The synthesized grammars are extremely large, often megabytes in size that enumerate inputs.

Our implementation GLADE-II and all experiments are available online for inspection and replication.

3 The GLADE Algorithm

GLADE [6] is a grammar inference algorithm. It infers the context-free grammar of a black-box oracle capable of saying yes or no to membership queries. It also bootstraps itself with a set of positive examples. The GLADE paper implies that it can produce the context-free grammar even if the positive examples given do not cover all “interesting behaviors”.

The GLADE algorithm starts with a seed input \( \alpha_{in} \). Such a single seed input (or a set of seed inputs) is a finite choice grammar [17] with high precision (because it will never generate an invalid input) but very low recall. From this, GLADE performs a series of precision-preserving generalization steps that attempts to increase the recall. Each step produces more and more general regular expressions.

While the algorithm attempts to preserve precision, doing so during transformations is hard. This is because we only have access to a membership oracle, and it is impossible to guarantee that precision is preserved without an infinite number of queries in general. Hence, GLADE uses a series of heuristic checks to ensure that the candidate is potentially precision preserving.

The GLADE algorithm has two main phases.

3.1 Phase I: Regular Expression Synthesis

In the first phase, the idea is to synthesize a representative regular expression. The algorithm first attempts to generalize substrings of the seed as repetition (rep) or alternation (alt). The seed input \( \alpha_{in} \) is first annotated as \([\alpha_{in}]_{rep}\). Then the following rules are followed to successively generalize the internal substrings.

- Given any partly annotated string \( P[\alpha]_{rep}Q \) such that \( P \) is the non annotated prefix, \( Q \) is the non annotated suffix, and the in between string \( \alpha \) is annotated with rep, we first find all decompositions of \( \alpha \) of the form \( \alpha_1\alpha_2\alpha_3 \) where \( \alpha_2 \neq \epsilon \). We then generate annotated strings \( Pa_x([\alpha_2]_{alt}) = [\alpha_3]_{rep}Q \) for every such decompositions of \( \alpha \). These along with the string \( PaQ \) becomes candidates for generalization.
3.2 Phase II: Infer Recursive Properties

The idea here is to infer recursive properties and transform the expression into a context-free grammar. The regular expression that was synthesized in Phase I is first translated into a context-free grammar. Next, each pair of nonterminals that were synthesized during Phase I corresponding to repetition is equated and checked whether the resulting language represents a valid generalization.

4 Evaluation

For evaluation, we wanted to ensure that the procedure we followed was the same as Bastani et al. except for the new implementation, and using the same grammar for precision and recall. Hence, the first set of subjects are the original four programs used by Bastani et al. for evaluation: URL, Lisp, Grep, and XML. Out of these, we used the URL, and Grep handwritten grammars as given by Bastani et al.\(^2\). We tried to check the accuracy, but could only evaluate that of the handwritten Grep grammar as this was the only binary available\(^3\). The XML and Lisp grammars were written as Java programs\(^4\). Since these are well known standard formats, we used external grammars for these.

Next, we wanted to extend our evaluation to a few simpler grammars so that we can understand the characteristics of the algorithm in detail. Hence, the second set includes a few simple grammars: Ints, Decimals, Floats, and JSON.

We then investigated GLADE behavior on a few parenthesis variants: Palindrome, Paren, Bool Add, TwoParen, TwoParenD, TwoAnyParenD, BinParen, and BinAnyParen.

Finally, we wanted to find the performance of GLADE on real-world complex grammars. Hence, the third set contained ANTLR grammars obtained from the ANTLR repository\(^5\): Lua, MySQL, Pascal, XPath, C, TinyC, Tiny, and Basic.

For the first, second, and third set of grammars, we produced 50 random inputs using the F1 fuzzer\(^6\). The random exploration depth was set to 100. For ANTLR grammars, the GLADE algorithm took an extremely large amount of time to learn. Hence, we limited both the seed set and the individual size. That is, for these, we only generated 10 seed inputs with a maximum random exploration depth of 20.

Note that GLADE claims not to require seed inputs that exercise all interesting behaviors. For ANTLR grammars, we used Grammarator\(^7\) as the input generator.

We use the same definitions of precision, recall, and the F1 score. We generate 1000 inputs from the synthesized grammar and check how many of them were recognized by the handwritten grammar for precision (P), and we generate 1000 inputs from the handwritten grammar and check how many were recognized by the synthesized grammar for recall (R). The F1 score is calculated as

\[
\text{F1} = \frac{2 \times P \times R}{P + R}
\]

We then investigated GLADE behavior on a few parenthesis variants: Palindrome, Paren, Bool Add, TwoParen, TwoParenD, TwoAnyParenD, BinParen, and BinAnyParen.

Finally, we wanted to find the performance of GLADE on real-world complex grammars. Hence, the third set contained ANTLR grammars obtained from the ANTLR repository\(^5\): Lua, MySQL, Pascal, XPath, C, TinyC, Tiny, and Basic.

For the first, second, and third set of grammars, we produced 50 random inputs using the F1 fuzzer\(^6\). The random exploration depth was set to 100. For ANTLR grammars, the GLADE algorithm took an extremely large amount of time to learn. Hence, we limited both the seed set and the individual size. That is, for these, we only generated 10 seed inputs with a maximum random exploration depth of 20.

\(^2\)https://github.com/obastani/glade-full/blob/master/data/handwritten/

\(^3\)https://github.com/obastani/glade-full/blob/master/data/prog

\(^4\)https://github.com/obastani/glade-full/blob/master/src/glade/constants/SyntheticGrammars.java

\(^5\)Only ASCII symbols were considered.
### Table 1. Glade-II Execution

<table>
<thead>
<tr>
<th>Grammar</th>
<th>LTime (s)</th>
<th>Seeds Len</th>
<th>σ</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>193</td>
<td>13.64</td>
<td>3.66</td>
<td>91,885</td>
</tr>
<tr>
<td>Lisp</td>
<td>1,463</td>
<td>13.93</td>
<td>13.20</td>
<td>81,769</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>5,840</td>
<td>16.44</td>
<td>13.15</td>
<td>129,362</td>
</tr>
<tr>
<td>XML</td>
<td>618</td>
<td>15.22</td>
<td>9.64</td>
<td>73,272</td>
</tr>
<tr>
<td>Greep</td>
<td>1,891</td>
<td>20.24</td>
<td>14.88</td>
<td>99,843</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grammar</th>
<th>LTime (s)</th>
<th>Seeds Len</th>
<th>σ</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ints</td>
<td>1</td>
<td>2.08</td>
<td>1.18</td>
<td>3,216</td>
</tr>
<tr>
<td>Decimals</td>
<td>15</td>
<td>3.72</td>
<td>2.20</td>
<td>21,292</td>
</tr>
<tr>
<td>Floats</td>
<td>16</td>
<td>5</td>
<td>2.45</td>
<td>22,827</td>
</tr>
<tr>
<td>JSON</td>
<td>7,398</td>
<td>24.04</td>
<td>45.78</td>
<td>172,163</td>
</tr>
</tbody>
</table>

### Table 2. Glade-II Scores

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
<th>Size (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>0.687</td>
<td>0.81</td>
<td>0.79</td>
<td>296</td>
</tr>
<tr>
<td>Lisp</td>
<td>0.378</td>
<td>0.55</td>
<td>0.63</td>
<td>638</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>0.55</td>
<td>0.96</td>
<td>0.7</td>
<td>976</td>
</tr>
<tr>
<td>XML</td>
<td>0.579</td>
<td>0.759</td>
<td>0.66</td>
<td>635</td>
</tr>
<tr>
<td>Greep</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
<th>Size (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ints</td>
<td>0.983</td>
<td>0.99</td>
<td>0.94</td>
<td>14</td>
</tr>
<tr>
<td>Decimals</td>
<td>0.848</td>
<td>0.92</td>
<td>0.74</td>
<td>74</td>
</tr>
<tr>
<td>Floats</td>
<td>0.914</td>
<td>0.984</td>
<td>0.95</td>
<td>71</td>
</tr>
<tr>
<td>JSON</td>
<td>0.531</td>
<td>0.797</td>
<td>0.64</td>
<td>594</td>
</tr>
</tbody>
</table>

### Table 3. Source Grammars

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Non-terminals</th>
<th>Rules</th>
<th>Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>13</td>
<td>119</td>
<td>73</td>
</tr>
<tr>
<td>Lisp</td>
<td>12</td>
<td>78</td>
<td>63</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>13</td>
<td>142</td>
<td>65</td>
</tr>
<tr>
<td>XML</td>
<td>12</td>
<td>140</td>
<td>65</td>
</tr>
<tr>
<td>Greep</td>
<td>12</td>
<td>155</td>
<td>91</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Non-terminals</th>
<th>Rules</th>
<th>Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ints</td>
<td>5</td>
<td>16</td>
<td>10</td>
</tr>
<tr>
<td>Decimals</td>
<td>7</td>
<td>19</td>
<td>11</td>
</tr>
<tr>
<td>Floats</td>
<td>10</td>
<td>27</td>
<td>14</td>
</tr>
<tr>
<td>JSON</td>
<td>27</td>
<td>159</td>
<td>101</td>
</tr>
</tbody>
</table>

### Table 4. Synthesized GLADE-II Grammars

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Non-terminals</th>
<th>Rules</th>
<th>Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>436</td>
<td>7,604</td>
<td>78</td>
</tr>
<tr>
<td>Lisp</td>
<td>923</td>
<td>15,928</td>
<td>63</td>
</tr>
<tr>
<td><strong>XML</strong></td>
<td>1,086</td>
<td>24,938</td>
<td>65</td>
</tr>
<tr>
<td>XML</td>
<td>693</td>
<td>16,282</td>
<td>69</td>
</tr>
<tr>
<td>Greep</td>
<td>993</td>
<td>54,756</td>
<td>91</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Non-terminals</th>
<th>Rules</th>
<th>Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ints</td>
<td>49</td>
<td>297</td>
<td>10</td>
</tr>
<tr>
<td>Decimals</td>
<td>194</td>
<td>1,252</td>
<td>19</td>
</tr>
<tr>
<td>Floats</td>
<td>260</td>
<td>1,524</td>
<td>14</td>
</tr>
<tr>
<td>JSON</td>
<td>1,418</td>
<td>10,727</td>
<td>114</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Non-terminals</th>
<th>Rules</th>
<th>Terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palindrome</td>
<td>46</td>
<td>89</td>
<td>44</td>
</tr>
<tr>
<td>Paren</td>
<td>1,635</td>
<td>3,549</td>
<td>3</td>
</tr>
<tr>
<td>Bool Add</td>
<td>1,097</td>
<td>2,224</td>
<td>9</td>
</tr>
<tr>
<td>TwoParenD</td>
<td>842</td>
<td>1,821</td>
<td>5</td>
</tr>
<tr>
<td>TwoAnyParenD</td>
<td>830</td>
<td>1,554</td>
<td>106</td>
</tr>
<tr>
<td>BinParen</td>
<td>1,188</td>
<td>2,625</td>
<td>12</td>
</tr>
<tr>
<td>BinAnyParen</td>
<td>3,514</td>
<td>7,260</td>
<td>120</td>
</tr>
<tr>
<td>Tiny</td>
<td>571</td>
<td>6,652</td>
<td>75</td>
</tr>
<tr>
<td>Lua</td>
<td>1,723</td>
<td>33,647</td>
<td>139</td>
</tr>
<tr>
<td>Pascal</td>
<td>2,975</td>
<td>41,648</td>
<td>134</td>
</tr>
<tr>
<td>MySQL</td>
<td>1,478</td>
<td>120,213</td>
<td>137</td>
</tr>
<tr>
<td>XPath</td>
<td>1,180</td>
<td>46,760</td>
<td>136</td>
</tr>
<tr>
<td>C</td>
<td>1,153</td>
<td>102,499</td>
<td>127</td>
</tr>
<tr>
<td>TinyC</td>
<td>2,294</td>
<td>30,126</td>
<td>162</td>
</tr>
<tr>
<td>Basic</td>
<td>1,298</td>
<td>13,683</td>
<td>135</td>
</tr>
</tbody>
</table>
The experiments were done on a machine with 8 Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz CPUs, with a memory of 16GB. The operating system was Ubuntu.

5 Discussion
There are several limitations with the GLADE paper.

5.1 Dependence on Seeds
In its discussion of relevant research, the GLADE paper [6] claims that some of the other grammar inference techniques rely on positive examples that exercise all interesting behaviors. One can wonder whether this implies that the seeds required by GLADE need not cover all interesting behaviors. In our evaluation, the performance of GLADE is strongly dependent on the features covered by seed inputs. A smaller number of seeds results in lower recall (less variety) but higher precision (less chance of making mistakes).

5.2 Reporting of Results
The F1 score as given in Figure 4 is never explicitly specified in figures. The most important information—precision and recall of the synthesized grammars—are never reported separate from F1.

5.3 Evaluation Results
The F1 score we obtain that is listed in Table 2 is much lower than the F1 score as given in Figure 4 is never explicitly specified in figures. The most important information—precision and recall of the synthesized grammars—are never reported separate from F1.

5.4 Practicality of the Inferred Grammars
One of the strong claims of GLADE is that the recovered grammar can be immediately used for fuzzing. However, we found that the size of the grammar generated is extremely large. For example, learning Grep resulted in a 2 MB grammar. The problem with such large grammars is that it is essentially enumerative. It cannot be feasibly used for parsing existing seed files as the parsers we tried to use gave up on such large grammars. Even grammar-based generators tend to have trouble using such large grammars. This is especially noticeable when considering the original grammars. For example, Palindrome resulted in a 13 KB grammar, while the actual grammar contains a single nonterminal and five rules.

The biggest surprise comes from the parenthesis languages. These are trivial languages with less than five nonterminal symbols. It should be trivial for GLADE to recover their grammar. However, GLADE fares poorly in most both in terms of accuracy (F1) and on the size of the grammars recovered, thousands of nonterminal symbols, and hundreds of kilobytes in size. On inspection, the GLADE recovered grammar was strongly enumerating rather than abstracting.

5.5 Insights about the GLADE Algorithm
During our implementation of GLADE algorithm and the subsequent evaluation, we found a number of insights about the GLADE algorithm, and why it has problems with some of the languages. These we describe in detail below.

1. The GLADE algorithm cannot learn a valid XML representation. Even in the paper [6], the regular expression synthesized \(-\langle a(>\langle a/>\langle)</a>\rangle\ast\ast\ast\) does not always produce valid XML inputs as it lacks a root element.
2. The heuristic checks specified by Bastani et al. is insufficient even for XML which drove their design [6, Section 8]. For example, given a seed \(<ab>\), the first generalization is \(<a*b/>\) and the second generalization is \(<a*b/>\). The second generalization is imprecise because we can only construct \(</\). However, it is accepted because the two required checks \(<a/>\) and \(<abb/>\) pass [6, Section 4.3 Check Construction].
3. Merging can incur loss of precision. Consider, for example, TwoAnyParenD. We start with a seed input \([()1\), which is generalized to \([>()\ast]*\). During Phase II, \(>()\ast\) and \(1\ast\) are hence checked for unification. To verify the new generalization, GLADE constructs two checks \([6, Section 5.3 Check Construction] – [111]

Table 5. GLADE Learning Accuracy (F1 Score)

<table>
<thead>
<tr>
<th>Grammar</th>
<th>Language</th>
<th>GLADE-I F1</th>
<th>GLADE-II F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Regular</td>
<td>0.92</td>
<td>0.81</td>
</tr>
<tr>
<td>Lisp</td>
<td>Context-Free</td>
<td>0.97</td>
<td>0.55</td>
</tr>
<tr>
<td>XML</td>
<td>Context-Free</td>
<td>0.98</td>
<td>0.7</td>
</tr>
<tr>
<td>Grep</td>
<td>Regular</td>
<td>0.93</td>
<td>1.00</td>
</tr>
</tbody>
</table>

As the actual F1 score was not reported by Bastani et al. [6], we estimated it from the graph [6, Figure 4(b)].

The handwritten grammar used for computing precision is much more permissive than the actual Grep grammar. Hence, the high F1 score.

\[\text{ Bastani et al. [6, Section 7 Limitations] incorrectly claims that it is valid XML subset.} \]
and \([ \emptyset \emptyset \emptyset ]\). Since both are valid, the new generalization is accepted. However, the resulting grammar can now produce \([ \emptyset \emptyset \emptyset ]\) which is invalid.

4. In Phase II, only repetitions are considered for unification. These are, however, insufficient in many cases. Consider XML, and seed input \(\langle b\rangle h1\langle b\rangle\). GLADE never learns about \(\langle b\rangle b h1\langle b\rangle\) because \(\langle b\rangle h1\langle b\rangle\) is not a repetition. We found the same issue in Palindrome where the grammar is exclusively made up of concrete enumerations.

5. The character generalization [6, Section 5.3 Check Construction] can produce generalizations that do not preserve precision. Consider the Grep grammar. We use \(a\) as a seed input. GLADE now constructs the check – \([\emptyset]\) – which passes, producing \([\emptyset a\] as a generalization for the first index. Next, GLADE constructs the check – \(aa\) – which passes, resulting in \([\emptyset a\] as a generalization for the second index, and the new generalized language \([a[\emptyset]](\emptyset)a\]. However, this language loses precision because it can produce \([a\] which is invalid.

6 Threats to Validity

We acknowledge that our evaluation of the GLADE algorithm is subject to the following threats.

**Defects in the implementation.** One of the largest threats to our evaluation is the possibility that (1) we misunderstood some parts of the GLADE paper and/or (2) we implemented the algorithm incorrectly. Given that this is a software program, this is a possibility that cannot be completely mitigated. We have tried to reduce the possible bugs as much as possible by carefully documenting our code, reviewing our code multiple times, investigating how simple grammars that exercised each feature of the GLADE algorithm behaved, and investigating a sample of inputs that reduced the precision or recall of the synthesized grammar.

**GLADE algorithm vs. tool.** For investigating GLADE, we also considered the GLADE tool supplied for replication. However, the GLADE tool does not support extraction or inspection of the inferred grammars, and we found it prohibitively hard to extract the GLADE algorithm code, as it is deeply entangled with code for custom serialization and custom input generation provided with GLADE. However, we note that our implementation achieves better F1 scores than Kulkarni et al. [18] (who used the GLADE tool) for JSON (0.64 > 0.59), XML (0.66 > 0.42), and Lisp (0.55 > 0.38). While the evaluation of Kulkarni achieved higher precision for TinyC (0.47 < 0.60), we note that the recall which is an indication of the amount of actual abstraction is surprisingly low (0.17).

**Defects in the input generator.** Another threat is that (1) our input generator is faulty (generates invalid strings) or that it is biased (generates a skewed distribution of inputs). We have tried to mitigate it by using off-the-shelf fuzzers such as the F1 fuzzer [13] and Grammarinator [15]. Further, we have checked that the strings that the fuzzers generate are parsed by the same grammar.

**Defects in the parser.** Another threat is the possibility that our parser may be defective, rejecting valid inputs or accepting invalid inputs. We have mitigated this by using an off-the-shelf well tested textbook parser [22].

7 Questions and Answers

Given that this is a replication study, questions may arise about our procedure. Let us address the most important ones.

1) Why do we not use GLADE-I [2]?

Our focus is to replicate the GLADE paper, not its implementation, as we see the paper as the definite, archived, and cited reference. ACM defines [1] replicability as: “For computational experiments, this means that an independent group can obtain the same result using artifacts which they develop completely independently.” Hence, we independently implemented the same algorithm. We note that our effort was prompted by the discovery that some of the GLADE F1 scores failed the reproducibility test for XML and Lisp when attempted by other researchers [18] using the same artifacts from GLADE-I (Section 6).

2) Is this a complete replication of the GLADE paper?

We attempt to replicate only what we consider to be the main result of the paper, which is the high accuracy achieved in F1 scores while learning different grammars. In particular, we do not replicate the evaluation of L-Star or RPNI. Secondly, we do not replicate the fuzzing experiments.

3) How do we know that the language \(a^n b^n\) could not be learned by GLADE?

Note that \(a^n b^n\) can equivalently be defined as:
\[\langle S \rangle ::= (\langle S\rangle \langle S\rangle) | \epsilon\]

We evaluated Palindrome (Figure 1) which is a trivial extension of the language \(a^n b^n\). Palindrome is defined as:
\[\langle S \rangle ::= (\langle S\rangle \langle S\rangle) | (\langle S\rangle \langle S\rangle) | \langle S\rangle \langle S\rangle | \langle S\rangle \langle S\rangle | \epsilon\]

That is, Palindrome contains three pairs of parenthesis rather just one pair. We analyzed different variations of the same language with different pairs, and found that the particular pattern—nesting nonterminals without repetition—is not learnable by GLADE.

4) How representative of real-world grammars are JSON and Decimals?

We argue that both grammars are representative and simple: Representativeness. Decimals numbers are a common component in almost all programming languages. JSON is
one of the most popular data-interchange formats, similar to XML and Lisp S-Expressions. Hence, we believe that both the Decimals and JSON grammars are representative of the real world.

**Simplicity.** The Decimals grammar is a regular grammar containing only 19 rules, and 7 nonterminals (Table 3). JSON is an LL(1) grammar that is a heavily reduced subset of the actual JSON specification. It contains only 27 nonterminals and 159 rules. We believe that regular grammars containing 11 rules should be considered simple by any definition, and LL(1) grammars are one of the simplest grammar classes under the Context-Free Grammar umbrella.

5) Does your implementation of GLADE include the optimizations from original GLADE implementation?
The only optimization mentioned in the GLADE paper [6] is multiple-inputs optimization, which enables GLADE to learn from multiple seed inputs. We have implemented that.

6) Is there a potential for non-determinism in the GLADE learning?
As far as we are aware, there is no potential for non-determinism in the GLADE implementation. We contacted the GLADE authors regarding our implementation. The only advice was to be careful about the order in which the alternatives were tried. We followed their advice and have implemented it exactly as the paper mentions. If there are any avenues of non-determinism influencing the grammar learning by GLADE, the GLADE paper does not mention it.

7) Why do you not evaluate Learning Highly Recursive Input Grammars [18] as well?
Our focus is on replication of GLADE. We do not claim that our research is much more than that. Hence, evaluation of Learning Highly Recursive Input Grammars is out of scope for this study.

8) How dependent is GLADE on the seed selection?
The GLADE paper uses ambiguous language in this regard. It says that it can produce the context-free grammar even if the positive examples given do not cover all “interesting behaviors”. However, the paper does not provide a definition of behavior. Hence, we would not know how to validate (or invalidate) this claim.

9) What is going wrong with GLADE and how can it be addressed?
This paper is a pure replication study of the GLADE paper. Hence, a detailed analysis of what is going wrong with GLADE, and how to overcome it is out of scope for this study.

8 Conclusion
Recovering input grammars for existing programs is an important, yet challenging problem. The GLADE algorithm by Bastani et al. is the first published approach that is set to recover general context-free grammars using membership queries alone. Having reimplemented the GLADE algorithm, we find that the accuracy of the inferred context-free grammars is much lower than originally reported, a discrepancy recently also reported for the original GLADE tool [18]. Our investigation details more issues with the GLADE algorithm; notably, we show that its inferred grammars can be extremely large and enumerative, indicating low usability for practical tasks such as parsing or producing inputs with general fuzzers. Prospective users should also evaluate other grammar mining approaches, such as the “blackbox” and “whitebox” approaches listed in Section 2.

Should the GLADE issues have been caught by the PLDI 2017 reviewers? In total, replicating and evaluating GLADE took us more than six person-months; we cannot expect from reviewers to spend all this time checking a paper. We hope, however, that future authors search for and report weaknesses just as they do for strengths, and that future reviewers appreciate honesty just as they appreciate success.

Replication studies are still rare in our field. Indeed, it is much more work to replicate a piece of research, especially from a paper, than to implement a new alternative from scratch (for which one may also get more credits). That extra effort comes from the required quality assurance: Does the reimplementaion really exactly reflect the algorithm(s) as stated in the paper? Of course, such quality assurance would be expected from any piece of research; yet, it is the authors of the replication study that would be challenged with such questions, not so much the authors of the original paper. As a community, we need to further encourage replication and reuse of research results—by making tools and data available, usable, understandable, and extensible. Such standards must become the norm, not the exception.

Our annotated reimplementaion GLADE-II and all experimental data is available at:
https://doi.org/10.5281/zenodo.6326396
A Appendix

\[
(S) ::= \langle S \rangle '1' | \langle S \rangle '0' | \langle S \rangle '1' | \langle S \rangle '0' | \langle S \rangle '1' | \langle S \rangle '0' | \epsilon
\]

Figure 1. Palindrome

\[
\langle S \rangle ::= \langle PS \rangle
\]
\[
\langle PS \rangle ::= \langle P \rangle \langle PS \rangle | \langle P \rangle
\]
\[
\langle P \rangle ::= \langle '1' \rangle | \langle '0' \rangle
\]

Figure 2. Paren

\[
\langle S \rangle ::= \langle S \rangle '+' \langle S \rangle | \langle '1' \rangle \langle S \rangle '1' | \langle '0' \rangle \langle D \rangle
\]
\[
\langle D \rangle ::= 1 | 0
\]

Figure 3. Bool Add

\[
\langle S \rangle ::= \langle '1' \rangle \langle S \rangle '1' | \langle '0' \rangle \langle D \rangle
\]
\[
\langle D \rangle ::= 1 | 1 \langle D \rangle
\]

Figure 5. TwoParenD

\[
\langle S \rangle ::= \langle D \rangle
\]
\[
| \langle '1' \rangle \langle S \rangle '1' \langle S \rangle
\]
\[
| \langle '0' \rangle \langle S \rangle '0' \langle S \rangle
\]
\[
| \langle '1' \rangle \langle S \rangle '1' \langle S \rangle
\]
\[
\langle D \rangle ::= \epsilon | 1 | 1 \langle D \rangle
\]

Figure 6. TwoAnyParenD

\[
\langle S \rangle ::= \langle PS \rangle
\]
\[
\langle PS \rangle ::= \langle P \rangle \langle PS \rangle | \langle P \rangle
\]
\[
\langle P \rangle ::= \langle '1' \rangle \langle '0' \rangle | \langle '0' \rangle \langle OS \rangle
\]
\[
\langle OS \rangle ::= \langle '1' \rangle | \langle '0' \rangle \langle OS \rangle
\]

Figure 7. BinParen

\[
\langle S \rangle ::= \langle PS \rangle \langle DigitNZ \rangle \langle DigitZs \rangle | \langle '0' \rangle
\]
\[
\langle DigitNZ \rangle ::= \epsilon | \langle DigitZ \rangle \langle DigitZs \rangle
\]
\[
\langle DigitZ \rangle ::= \langle '0' \rangle | \langle DigitNZ \rangle
\]
\[
\langle DigitNZ \rangle ::= [1-9]
\]

Figure 8. BinAnyParen

\[
\langle START \rangle ::= \langle INTEGER \rangle
\]
\[
\langle INTEGER \rangle ::= \langle DigitNZ \rangle \langle DigitZs \rangle | \langle '0' \rangle
\]
\[
\langle DigitZs \rangle ::= \epsilon | \langle DigitZ \rangle \langle DigitZs \rangle
\]
\[
\langle DigitZ \rangle ::= \langle '0' \rangle | \langle DigitNZ \rangle
\]
\[
\langle DigitNZ \rangle ::= [1-9]
\]

Figure 9. Integer grammar

\[
\langle START \rangle ::= \langle DECNUM \rangle
\]
\[
\langle DECNUM \rangle ::= \langle INT \rangle '.' \langle DEC \rangle
\]
\[
\langle DEC \rangle ::= \langle DigitNZ \rangle \langle DigitNZ \rangle | \langle '0' \rangle
\]
\[
\langle INT \rangle ::= \langle DigitNZ \rangle \langle DigitZs \rangle | \langle '0' \rangle
\]
\[
\langle DigitZs \rangle ::= \epsilon | \langle DigitZ \rangle \langle DigitZs \rangle
\]
\[
\langle DigitZ \rangle ::= \langle '0' \rangle | \langle DigitNZ \rangle
\]
\[
\langle DigitNZ \rangle ::= [1-9]
\]

Figure 10. Decimal grammar

\[
\langle START \rangle ::= \langle FLOAT \rangle
\]
\[
\langle FLOAT \rangle ::= \langle INT \rangle '.' \langle EXT \rangle | \langle 'E' \rangle \langle INT \rangle '.'
\]
\[
\langle EXT \rangle ::= \langle DEC \rangle | \langle DEC \rangle \langle LETTER \rangle \langle OP \rangle \langle INT \rangle | \langle DEC \rangle \langle LETTER \rangle \langle OP \rangle \langle INT \rangle
\]
\[
\langle DEC \rangle ::= \langle DigitZs \rangle \langle DigitNZ \rangle | \langle '0' \rangle
\]
\[
\langle INT \rangle ::= \langle DigitNZ \rangle \langle DigitZs \rangle | \langle '0' \rangle
\]
\[
\langle OP \rangle ::= '+' | '-'
\]
\[
\langle LETTER \rangle ::= 'E' | 'e'
\]
\[
\langle DigitZs \rangle ::= \epsilon | \langle DigitZ \rangle \langle DigitZs \rangle
\]
\[
\langle DigitZ \rangle ::= \langle '0' \rangle | \langle DigitNZ \rangle
\]
\[
\langle DigitNZ \rangle ::= [1-9]
\]

Figure 11. Float grammar
References


