Semantic Fuzzing with Zest

Rohan Padhye  
University of California, Berkeley  
USA  
rohanpadhye@cs.berkeley.edu

Caroline Lemieux  
University of California, Berkeley  
USA  
clemieux@cs.berkeley.edu

Koushik Sen  
University of California, Berkeley  
USA  
ksen@cs.berkeley.edu

Mike Papadakis  
University of Luxembourg  
Luxembourg  
michail.papadakis@uni.lu

Yves Le Traon  
University of Luxembourg  
Luxembourg  
yves.letraon@uni.lu

ABSTRACT
Programs expecting structured inputs often consist of both a syntactic analysis stage, which parses raw input, and a semantic analysis stage, which conducts checks on the parsed input and executes the core logic of the program. Generator-based testing tools in the lineage of QuickCheck are a promising way to generate random syntactically valid test inputs for these programs. We present Zest, a technique which automatically guides QuickCheck-like random-input generators to better explore the semantic analysis stage of test programs. Zest converts random-input generators into deterministic parametric generators. We present the key insight that mutations in the untyped parameter domain map to structural mutations in the input domain. Zest leverages program feedback in the form of code coverage and input validity to perform feedback-directed parameter search. We evaluate Zest against AFL and QuickCheck on five Java programs: Maven, Ant, BCEL, Closure, and Rhino. Zest covers 1.03×–2.81× as many branches within the benchmarks’ semantic analysis stages as baseline techniques. Further, we find 10 new bugs in the semantic analysis stages of these benchmarks. Zest is the most effective technique in finding these bugs reliably and quickly, requiring at most 10 minutes on average to find each bug.

CCS CONCEPTS
• Software and its engineering → Software testing and debugging.

KEYWORDS
Structure-aware fuzzing, property-based testing, random testing

1 INTRODUCTION
Programs expecting complex structured inputs often process their inputs and convert them into suitable data structures before invoking the actual functionality of the program. For example, a build system such as Apache Maven first parses its input as an XML document and checks its conformance to a schema before invoking the actual build functionality. Document processors, Web browsers, compilers and various other programs follow this same check-then-run pattern.

In general, such programs have an input processing pipeline consisting of two stages: a syntax parser and a semantic analyzer. We illustrate this pipeline in Figure 1. The syntax parsing stage translates the raw input into an internal data structure that can be easily processed (e.g. an abstract syntax tree) by the rest of the program. The semantic analysis stage checks if an input satisfies certain semantic constraints (e.g. if an XML input fits a specific schema), and executes the core logic of the program. Inputs may be rejected by either stage if they are syntactically or semantically invalid. If an input passes both stages, we say the input is valid.

Automatically testing such programs is challenging. The difficulty lies in synthesizing inputs that (1) satisfy complex constraints on their structure and (2) exercise a variety of code paths in the semantic analysis stages and beyond. Random input generation is a popular technique for such scenarios because it can easily scale to execute a large number of test cases. Developers can write domain-specific generators from which random syntactically valid inputs—such as XML documents and abstract syntax trees—can be sampled. Popularized by QuickCheck [30], this approach has been adopted by many generator-based testing tools [16, 19, 32, 34, 38, 43, 49, 61]. QuickCheck-like test frameworks are now available in many programming languages such as Java [44], PHP [10], Python [11],
JavaScript [12], Scala [14], and Clojure [15]. Many commercial
black-box fuzzing tools, such as Peach [13], beSTORM [7], Cy-
berflood [9], and Codenomicon [8], also leverage generators for
network protocols or file formats. However, in order to effectively
exercise the semantic analyses in the test program, the generators
need to be tuned to produce inputs that are also semantically valid.
For example, the developers of CSmith [72], a tool that generates
random C programs for testing compilers, spent significant effort
manually tuning their generator to reliably produce valid C pro-
grams and to maximize code coverage in the compilers under test.

In this paper, we present Zest, a technique for automatically
guiding QuickCheck-like input generators to exercise various code
paths in the semantic analysis stages of programs. Zest incorporates
feedback from the test program in the form of semantic validity of
test inputs and the code coverage achieved during test execution.
The feedback is then used to generate new inputs via mutations.

Coverage-guided fuzzing (CGF) tools such as AFL [74] and lib-
Fuzzer [45] have gained a huge amount of popularity recently due
to their effectiveness in finding critical bugs and security vulnera-
ble in widely-used software systems. CGF works by randomly
mutating known inputs via operations such as bit flips and byte-
level splicing to produce new inputs. If the mutated inputs lead to
new code coverage in the test program, they are saved for subse-
quent mutation. Of course, such mutations usually lead to invalid
syntax. Naturally, most of the bugs found by these CGF tools lie
in the syntax analysis stage of programs. CGF tools often require
many hours or days of fuzzing to discover deeper bugs [47], which
makes them impractical for use in continuous integration systems
with limited testing time budgets.

Our proposed technique, Zest, adapts the algorithm used by CGF
tools in order to quickly explore the semantic analysis stages of
test programs. Zest first converts QuickCheck-like random-input
generators into deterministic parametric generators, which map a
sequence of untyped bits, called the “parameters”, to a syntactically
valid input. The key insight in Zest is that bit-level mutations on
these parameters correspond to structural mutations in the space
of syntactically valid inputs. Zest then apes a CGF algorithm on
the domain of parameters, in order to guide the test-input genera-
tion towards semantic validity and increased code coverage in the
semantic analysis stages.

We have integrated Zest into the open-source JQF frame-
work [60]: https://github.com/rohanpadhye/jqf. We evaluate Zest
on five real-world Java benchmarks and compare it to AFL [74]
and (a Java port of) QuickCheck [44]. Our results show that the
Zest technique achieves significantly higher code coverage in the
semantic analysis stage of each benchmark. Further, during our
evaluation, we find 10 new bugs in the semantic analysis stages of
our benchmarks. We find Zest to be the most effective technique
for reliably and quickly triggering these semantic bugs. For each
benchmark, Zest discovers an input triggering every semantic bug
in at most 10 minutes on average. Zest complements AFL, which is
best suited for finding syntactic bugs.

To summarize, we make the following contributions:

- We present an algorithm that combines parametric gener-
ators with feedback-directed parameter search, in order to
effectively explore the semantic analysis stages of programs.
- We evaluate our Java-based implementation of Zest against
AFL and QuickCheck on five real-world benchmarks to com-
pare their effectiveness in exercising code paths and discov-
ering new bugs within the semantic analysis stage.

2 BACKGROUND

2.1 Generator-based testing

Generator-based testing tools [16, 30, 32, 34, 38, 43, 61, 72] allow
users to write generator programs for producing inputs that belong
to a specific type or format. These random-input generators are
non-deterministic, i.e., they sample a new input each time they are
executed. Figure 2 shows a generator for XML documents in the
junit-quickcheck [44] framework, which is a Java port of QuickCheck [30]. When generate() is called, the generator uses
the Java Standard library XML DOM API to generate a random
XML document. It constructs the root element of the document by
invoking genElement (Line 4). Then, genElement uses repeated
calls to methods of random to generate the element’s tag name
(Line 9), any embedded text (Lines 19, 20, and in genStr),
and the number of children (Line 13); it recursively calls genElement to
generate each child node. We omitted code to generate attributes,
but it can be done analogously.

Figure 3 contains a sample test harness method testProgram,
identified by the @Property annotation. This method expects a
test input xml of type XMLDocument; the @from annotation
indicates that inputs will be randomly generated using the
XMLGenerator.generate() API. When invoked with a generated
XML document, testProgram serializes the document (Line 3) and
invokes the readModel method (Line 9), which parses an input
string into a domain-specific model. For example, Apache Maven
parses pom.xml files into an internal Project Object Model (POM).
The model creation fails if the input XML document string does not
meet certain syntactic and semantic requirements (Lines 11, 13). If
the model creation is successful, the check at Line 4 succeeds and
the test harness invokes the method runModel at Line 5 to test one of
the core functionalities of the program under test.

An XML generator like the one shown in Figure 2 generates
random syntactically valid XML inputs; therefore Line 11 in Figure 3
will never be executed. However, the generated inputs may not be
semantically valid. That is, the inputs generated by the depicted
XML generator do not necessarily conform to the schema expected
by the application. In our example, the readModel method could
throw a ModelException and cause the assumption at Line 4 to fail.
If this happens, QuickCheck simply discards the test case and tries
again. Writing generators that produce semantically valid inputs
by construction is a challenging manual effort.

When we tested Apache Maven’s model reader for pom.xml files
using a generator similar to Figure 2, we found that only 0.09% of
the generated inputs were semantically valid. Moreover, even if
the generator manages to generate semantically valid inputs, it
may not generate inputs that exercise a variety of code paths in
the semantic analysis stage. In our experiments with Maven, the
QuickCheck approach covers less than one-third of the branches
Algorithm 1 Coverage-guided fuzzing.

Input: program \( p \), set of initial inputs \( I \)
Output: a set of test inputs and failing inputs

1. \( S \leftarrow I \)
2. \( F \leftarrow \emptyset \)
3. \( \text{totalCoverage} \leftarrow \emptyset \)
4. repeat
5. for input in \( S \) do
6. for \( 1 \leq i \leq \text{NUMCANDIDATES}(\text{input}) \) do
7. candidate \( \leftarrow \text{mutate}(\text{input}, S) \)
8. coverage, result \( \leftarrow \text{run}(p, \text{candidate}) \)
9. if result = \text{FAILURE} then
10. \( F \leftarrow F \cup \text{candidate} \)
11. else if coverage \( \subseteq \text{totalCoverage} \) then
12. \( S \leftarrow S \cup \{ \text{candidate} \} \)
13. \( \text{totalCoverage} \leftarrow \text{totalCoverage} \cup \text{coverage} \)
14. until given time budget expires
15. return \( S, F \)

on the base input (Line 7). These mutations may include operations that combine subsets of other inputs in \( S \). The given program is then executed with each newly generated input (Line 8). The result of a test execution can either be \text{SUCCESS} or \text{FAILURE}. If an input causes a test failure, it is added to the failure set \( F \) (Line 10).

The key to the CGF algorithm is that instead of treating the test program as a black-box as QuickCheck does, it instruments the test program to provide dynamic feedback in the form of code coverage for each run. The algorithm maintains in the variable \( \text{totalCoverage} \) the set of all \textit{coverage points} (e.g. program branches) covered by the existing inputs. If the successful execution of a generated input leads to the discovery of new coverage points (Line 11), then this input is added to the set \( S \) for subsequent fuzzing (Line 12) and the newly covered coverage points are added to \( \text{totalCoverage} \) (Line 13).

The whole process repeats until a time budget expires. Finally, CGF returns the generated corpus of test inputs \( S \) and failing inputs \( F \) (Line 15). CGF can either be used as a technique to discover inputs that expose bugs—in the form of crashes or assertion violations—or to automatically generate a corpus of test inputs that cover various program features.

A key limitation of existing CGF tools is that they work without any knowledge about the syntax of the input. State-of-the-art CGF tools \cite{25, 28, 45, 50, 63, 74} treat program inputs as sequences of bytes. This choice of representation also influences the design of their mutation operations, which include bit-flips, arithmetic operations on word-sized segments, setting random bytes to random or “interesting” values (e.g. 0, MAX_INT), etc. These mutations are tailored towards exercising various code paths in programs that parse inputs with a compact syntax, such as parsers for media file formats, decompression routines, and network packet analyzers. CGF tools have been very successful in finding memory-corruption bugs (such as buffer overflows) in the syntax analysis stage of such programs due to incorrect handling of unexpected inputs.

Unfortunately, this approach often fails to exercise the core functions of software that expects highly structured inputs. For example, when AFL \cite{74} is applied on a program that processes XML input data, a typical input that it saves looks like:

\[
\text{<a b>ac\&#84;以外>}
\]
which exercises code paths that deal with syntax errors. In this case, an error-handling routine for unmatched start and end XML tags. It is very difficult to generate inputs that will exercise new, interesting code paths in the semantic analysis stage of a program via these low-level mutations. Often, it is necessary to run CGF tools for hours or days on end in order to find non-trivial bugs, making them impractical for use in a continuous integration setting.

3 PROPOSED TECHNIQUE
Our approach, Zest, adds the power of coverage-guided fuzzing to generator-based testing. First, Zest converts a random-input generator into an equivalent deterministic parametric generator. Zest then uses feedback-directed parameter search to search through the parameter space. This technique augments the CGF algorithm by keeping track of code coverage achieved by valid inputs. This enables it to guide the search towards deeper code paths in the semantic analysis stage.

3.1 Parametric Generators
Before defining parametric generators, let us return to the random XML generator from Figure 2. Let us consider a particular path through this generator, concentrating on the calls to nextInt, nextBool, and nextChar. The following sequence of calls will be our running example (some calls omitted for space):

\[
\text{Call} \rightarrow \text{result} \quad \text{Context}
\]

\[
\begin{array}{l}
\text{random.nextInt}(1, \text{MAX_STRLEN}) \rightarrow 3 \quad \text{Root: name length (Line 26)} \\
\text{random.nextChar()} \rightarrow 'f' \quad \text{Root: name[0] (Line 29)} \\
\text{random.nextChar()} \rightarrow 'o' \quad \text{Root: name[1] (Line 29)} \\
\text{random.nextChar()} \rightarrow 'o' \quad \text{Root: name[2] (Line 29)} \\
\text{random.nextInt(\text{MAX_CHILDREN})} \rightarrow 2 \quad \text{Root: # children (Line 13)} \\
\text{random.nextInt}(1, \text{MAX_STRLEN}) \rightarrow 3 \quad \text{Child 1: name length (Line 26)} \\
\vdots \\
\text{random.nextBool()} \rightarrow \text{False} \quad \text{Child 2: embed text? (Line 19)} \\
\text{random.nextBool()} \rightarrow \text{False} \quad \text{Root: embed text? (Line 19)} \\
\end{array}
\]

The XML document produced when the generator makes this sequence of calls looks like:

\[
x_1 = \langle \text{foo} \rangle \langle \text{bar} \rangle \text{Hello} \langle /\text{bar} \rangle \langle \text{baz} / \rangle / / \langle /\text{foo} \rangle.
\]

In order to produce random typed values, the implementations of random.nextInt, random.nextChar, and random.nextBool rely on a pseudo-random source of untyped bits. We call these untyped bits "parameters". The parameter sequence for the example above, annotated with the calls which consume the parameters, is:

\[
\sigma_1 = \begin{array}{cccccccc}
0000 & 0010 & 0110 & 0110 & \cdots & 0000 & 0000 & \cdot \\
\text{nextInt}(1, \ldots) \rightarrow 'f' & \text{nextChar()} \rightarrow 'o' & \text{nextBool()} \rightarrow \text{False}
\end{array}
\]

For example, here the function random.nextInt(a, b) consumes eight bit parameters as a byte, n, and returns \( n \% (b - a) + a \) as a typed integer. For simplicity of presentation, we show each random.nextXYZ function consuming the same number of parameters, but they can consume different numbers of parameters.

We can now define a parametric generator. A parametric generator is a function that takes a sequence of untyped parameters such as \( \sigma_1 \) —the parameter sequence— and produces a structured input, such as the XML \( x_1 \). A parametric generator can be implemented by simply replacing the underlying implementation of Random to consult not a pseudo-random source of bits but instead a fixed sequence of bits provided as the parameters.

While this is a very simple change, making generators deterministic and explicitly dependent on a fixed parameter sequence enables us to make the following two key observations:

1. **Every untyped parameter sequence corresponds to a syntactically valid input**—assuming the generator only produces syntactically valid inputs.

2. **Bit-level mutations on untyped parameter sequences correspond to high-level structural mutations in the space of syntactically valid inputs.**

Observation (1) is true by construction. The random.nextInt functions are implemented to produce correctly-typed values no matter what bits the pseudo-random source—or in our case, the parameters—provide. Every sequence of untyped parameter bits correspond to some execution path through the generator, and therefore every parameter sequence maps to a syntactically valid input. We describe how we handle parameter sequences that are longer or shorter than expected with the example sequences \( \sigma_3 \) and \( \sigma_4 \), respectively, below.

To illustrate observation (2), consider the following parameter sequence, \( \sigma_2 \), produced by mutating just a few bits of \( \sigma_1 \):

\[
\sigma_2 = \begin{array}{cccccccc}
0000 & 0010 & 0101 & 0111 & \cdots & 0000 & 0000 & \\
\text{nextChar()} \rightarrow 'W' & \text{nextChar()} \rightarrow 'W'
\end{array}
\]

As indicated by the annotation, all this parameter-sequence mutation does is change the value returned by the second call to random.nextChar() in our running example from ‘f’ to ‘W’. So the generator produces the following test-input:

\[
x_2 = \langle \text{Woo} \rangle \langle \text{bar} \rangle \text{Hello} \langle /\text{bar} \rangle \langle \text{baz} / \rangle / / \langle /\text{Woo} \rangle.
\]

Notice that this generated input is still syntactically valid, with "Woo" appearing both in the start and end tag delimiters. This is because the XML generator uses an internal DOM tree representation that is only serialized after the entire tree is generated. We get this syntactic-validity-preserving structural mutation for free, by construction, and without modifying the underlying generators.

Mutating the parameter sequence can also result in more drastic high-level mutations. Suppose that \( \sigma_1 \) is mutated to influence the first call to random.nextInt(\text{MAX_CHILDREN}) as follows:

\[
\sigma_3 = \begin{array}{cccccccc}
0000 & \cdots & 0000 & 001 & \cdots & 0000 & \\
\text{nextInt(\text{MAX CHILDREN})} \rightarrow 1
\end{array}
\]

Then the root node in the generated input will have only one child:

\[
x_3 = \langle \text{foo} \rangle \langle \text{bar} \rangle \text{Hello} \langle /\text{bar} \rangle \langle /\text{foo} \rangle
\]

(■ designates the absence of \( \langle \text{baz} / \rangle \)). Since the remaining values in the untyped parameter sequence are the same, the first child node in \( x_3 \) \( \langle \text{bar} \rangle \text{Hello} \langle /\text{bar} \rangle \) is identical to the one in \( x_1 \). The parametric generator thus enables a structured mutation in the DOM tree, such as deleting a sub-tree, by simply changing a few values in the parameter sequence. Note that this change results in fewer random.nextInt calls by the generator; the unused parameters in the tail of the parameter sequence will simply be ignored by the parametric generator.
The Zest algorithm, pairing parametric generators with feedback-directed parameter search. Additions to Algorithm 1 highlighted in grey.

**Algorithm 1**

**Input:** program \( p \), generator \( q \)

**Output:** a set of test inputs and failing inputs

1. \( S \leftarrow \{ \text{RANDOM} \} \)
2. \( \mathcal{F} \leftarrow \emptyset \)
3. \( \text{totalCoverage} \leftarrow \emptyset \)
4. \( \text{validCoverage} \leftarrow \emptyset \)
5. \( g \leftarrow \text{makeParametric}(q) \)
6. repeat
7. for param in \( S \) do
8. for \( 1 \leq i \leq \text{numCandidates}(\text{param}) \) do
9. candidate \( \leftarrow \text{mutate}(\text{param}, S) \)
10. input \( \leftarrow g(\text{candidate}) \)
11. \( \text{coverage}, \text{result} \leftarrow \text{run}(p, \text{input}) \)
12. if result = FAILURE then
13. \( \mathcal{F} \leftarrow \mathcal{F} \cup \text{candidate} \)
14. else if \( \text{coverage} \not\subseteq \text{totalCoverage} \) then
15. \( S \leftarrow S \cup \{ \text{candidate} \} \)
16. \( \text{totalCoverage} \leftarrow \text{totalCoverage} \cup \text{coverage} \)
17. \( \text{validCoverage} \leftarrow \text{validCoverage} \cup \text{coverage} \)
18. if result = VALID and \( \text{coverage} \not\subseteq \text{validCoverage} \) then
19. \( S \leftarrow S \cup \{ \text{candidate} \} \)
20. \( \text{validCoverage} \leftarrow \text{validCoverage} \cup \text{coverage} \)
21. until given time budget expires
22. return \( g(S), g(\mathcal{F}) \)

For our final example, suppose \( \sigma_1 \) is mutated as follows:
\[
\sigma_1' = 0000 \ 0000 \ 0011 \ldots \ 0000 \ 0001 \ 0000 \ 0000 \ .
\]
\( \text{nextInt}() \rightarrow 1 \)
\( \text{nextBool}() \rightarrow \) True

Notice that after this mutation, the last 8 parameters are consumed by \( \text{nextInt} \) instead of by \( \text{nextBool} \). But, note that \( \text{nextInt} \) still returns a valid typed value even though the parameters were originally consumed by \( \text{nextBool} \).

At the input level, this modifies the call sequence so that the decision to embed text in the second child of the document becomes True. Then, the last parameters are used by \( \text{nextInt} \) to choose an embedded text length of 1 character. However, one problem remains: to generate the content of the embedded text, the generator needs more parameter values than \( \sigma_1 \) contains. In Zest, we deal with this by appending pseudo-random values to the end of the parameter sequence on demand. We use a fixed random seed to maintain determinism. For example, suppose the sequence is extended as:
\[
\sigma_1'' = 0000 \ldots \ 0001 \ 0000 \ 0000 \ 0000 \ 0000 \ 0000 \ 0000 \ 0000 \ 0000 \ 0000 \ .
\]
\( \text{nextChar}() \rightarrow \text{H'} \)
\( \text{nextBool}() \rightarrow \) False

Then the parametric generator would produce the test-input:
\[
x_4 = \text{<foo>`<bar>`Hello</bar>`<baz>`<H'`<baz>`</foo>}
\]

### 3.2 Feedback-directed Parameter Search

Algorithm 2 shows the Zest algorithm, which guides parametric generators to produce inputs that get deeper into the semantic analysis stage of programs using feedback-directed parameter search. The Zest algorithm resembles Algorithm 1, but acts on parameter sequences rather than the raw inputs to the program. It also extends the CGF algorithm by keeping track of the coverage achieved by semantically valid inputs. We highlight the differences between Algorithms 2 and 1 in grey.

Like Algorithm 1, Zest is provided a program under test \( p \). Unlike Algorithm 1 which assumes seed inputs, the set of parameter sequences is initialized with a random sequence (Line 1). Additionally, Zest is provided a generator \( q \), which it automatically converts to a parametric generator \( g \) (Line 5). In an abuse of notation, we use \( g(S) \) to designate the set of inputs generated by running \( g \) over the parameter sequences in \( S \), i.e. \( g(S) = \{ g(s) : s \in S \} \).

Along with \( \text{totalCoverage} \), which maintains the set of coverage points in \( p \) covered by all \( g(S) \), Zest also maintains \( \text{validCoverage} \), the set of coverage points covered by the (semantically) valid inputs in \( g(S) \). This is initialized at Line 4.

New parameter sequences are generated using standard CGF mutations at Line 9; see Section 4 for details. New inputs are generated by running the sequences through the parametric generator (Line 10). The program \( p \) is then executed on each input. During the execution, in addition to code-coverage and failure feedback, the algorithm records in the variable \( \text{result} \) whether the input is valid or not. In particular, \( \text{result} \) can be any of \{VALID, INVALID, FAILURE\}. An input is considered invalid if it leads to a violation of any assumption in the test harness (e.g. Figure 3 at Line 4), which is how we capture application-specific semantic validity.

As in Algorithm 1, a newly generated parameter sequence is added to the set \( S \) at Lines 15–17 of Algorithm 2 if the corresponding input produces new code coverage. Further, if the corresponding input is valid and covers a coverage point that has not been exercised by any previous valid input, then the parameter sequence is added \( S \) and the cumulative valid coverage variable \( \text{validCoverage} \) is updated at Lines 18–20. Adding the parameter sequence to \( S \) under this new condition ensures that Zest keeps mutating valid inputs that exercise core program functionality. We hypothesize that this biases the search towards generating even more valid inputs and in turn increases code coverage in the semantic analysis stage.

As in Algorithm 1, the testing loop repeats until a time budget expires. Finally, Zest returns the corpus of generated test inputs \( g(S) \) and failing inputs \( g(\mathcal{F}) \).

### 4 IMPLEMENTATION

Zest is implemented on top of the open-source JQF platform \cite{JQF}, which provides a framework for specifying algorithms for feedback-directed fuzz testing of Java programs. JQF dynamically instruments Java classes in the program under test using the ASM bytecode-instrumentation framework \cite{ASM} via a javaagent. The instrumentation allows JQF to observe code coverage events, e.g. the execution of program branches and invocation of virtual method calls.

Fuzzing “guidances” can plug into JQF to provide inputs and register callbacks for listening to code coverage events. JQF originally shipped with AFLGuidance and NoGuidance, which we use in our evaluation in Section 5. AFLGuidance uses a proxy program to exchange program inputs and coverage feedback with the external AFL tool; the overhead of this inter-process communication...
is a negligible fraction of the test execution time. NoGuidance randomly provides inputs from junit-quickcheck [44] generators without using coverage feedback. We implement ZestGUI dance in JQF, which biases these generators using Algorithm 2.

junit-quickcheck provides a high-level API for making random choices in the generators, such as generating random integers, time durations, and selecting random items from a collection. All of these methods indirectly rely on the underlying JDK method java.util.Random.nextInt(int bits), which returns bits from a pseudo-random stream. Zest replaces this pseudo-random stream with store parameters, which are extended on-demand.

Since java.util.Random polls byte-sized chunks from its underlying stream of pseudo-random bits, Zest performs mutations on the parameter sequences (Algorithm 2, Line 9) at the byte-level. The basic mutation procedure is as follows: (1) choose a random number m of mutations to perform sequentially on the original sequence, (2) for each mutation, choose a random length ℓ of bytes to mutate and an offset k at which to perform the mutation, and (3) replace the bytes from positions [k, k + ℓ] with ℓ randomly chosen bytes. The random numbers m and ℓ are chosen from a geometric distribution, which mostly provides small values without imposing an upper bound. We set the mean of this distribution to 4, since 4-byte ints are the most commonly requested random value.

5 EVALUATION

We evaluate Zest by measuring its effectiveness in testing the semantic analysis stages of five benchmark programs. We compare Zest with two baseline techniques: AFL and junit-quickcheck (referred to as simply QuickCheck hereon). AFL is known to excel in exercising the syntax analysis stage via coverage-guided fuzzing of raw input strings. We use version 2.52b, with _FidgetyAFL_ configuration, which was found to match the performance of AFLFast [75].

QuickCheck uses the same generators as Zest but only performs random sampling without any feedback from the programs under test. Specifically, we evaluate the three techniques on two fronts: (1) the amount of code coverage achieved in the semantic analysis stage after a fixed amount of time, and (2) their effectiveness in triggering bugs in the semantic analysis stage.

_Benchmarks_. We use the following five real-world Java benchmarks as test programs for our evaluation:

(1) Apache Maven [3] (99k LoC): The test reads a pom.xml file and converts it into an internal Model1 structure. The test driver is similar to the one in Figure 3. An input is valid if it is a valid XML document conforming to the POM schema.

(2) Apache Ant [1] (223k LoC): Similar to Maven, this test reads a build.xml file and populates a Project object. An input is considered valid if it is a valid XML document and if it conforms to the schema expected by Ant.

(3) Google Closure [4] (247k LoC) statically optimizes JavaScript code. The test driver invokes the Compiler.compile() on the input with the _SIMPLE_OPTIMIZATIONS_ flag, which enables constant folding, function inlining, dead-code removal, etc. An input is valid if Closure returns without error.

(4) Mozilla Rhino [5] (89k LoC) compiles JavaScript to Java bytecode. The test driver invokes Context.compileString(). An input is valid if Rhino returns a compiled script.

(5) Apache’s Bytecode Engineering Library (BCEL) [2] (61k LoC) provides an API to parse, verify and manipulate Java bytecode. Our test driver takes as input a .class file and uses the Verifier API to perform 3-pass verifications of the class file according to the Java 8 specification [53]. An input is valid if BCEL finds no errors up to Pass 3A verification.

Experimental Setup. We make the following design decisions:

- **Duration**: We run each test-generation experiment for 3 hours. Researchers have used various timeouts to evaluate random test generation tools, from 2 minutes [37, 59] to 24 hours [25, 47]. We chose 3 hours as a middle ground. Our experiments justify this choice, as we found that semantic coverage plateaued after 2 hours in almost all experiments. Specifically, the number of semantic branches covered by Zest increased by less than 1% in the last hour of the runs.

- **Repetitions**: Due to the non-deterministic nature of random testing, the results may vary across multiple repetitions of each experiment. We therefore run each experiment 20 times and report statistics across the 20 repetitions.

- **Seeds and Dictionaries**: To bootstrap AFL, we need to provide some initial seed inputs. There is no single best strategy for selecting initial seeds [64]. Researchers have found success using varying strategies ranging from large seed corpora to single empty files [47]. In our evaluation, we provide AFL one valid seed input per benchmark that covers various domain-specific semantic features. For example, in the Closure and Rhino benchmarks, we use the entire React/JS library [6] as a seed. We also provide AFL with dictionaries of benchmark-specific strings (e.g. keywords, tag names) to inject into inputs during mutation. The generator-based tools Zest and QuickCheck do not rely on meaningful seeds.

- **Generators**: Zest and QuickCheck use hand-written input generators. For Maven and Ant, we use an XML document generator similar to Figure 2, of around 150 lines of Java code. It generates strings for tags and attributes by randomly choosing strings from a list of string literals scraped from class files in Maven and Ant. For Closure and Rhino, we use a generator for a subset of JavaScript that contains about 300 lines of Java code. The generator produces strings that are syntactically valid JavaScript programs. Finally, the BCEL generator (~500 LoC) uses the BCEL API to generate JavaClass objects with randomly generated fields, attributes and methods with randomly generated bytecode instructions. All generators were written by one of the authors of this paper in less than two hours each. Although these generators produce syntactically valid inputs, no effort was made to produce semantically valid inputs; doing so can be a complex and tedious task [72].

The generators, seeds, and dictionaries have been made publicly available at https://goo.gl/GfLRzA. All experiments are conducted on a machine with Intel(R) Core(TM) i7-5930K 3.50GHz CPU and 16GB of RAM running Ubuntu 18.04.

Syntax and Semantic Analysis Stages in Benchmarks. Zest is specifically designed to exercise the semantic analysis stages of
Semantic Fuzzing with Zest  
ISSTA ’19, July 15–19, 2019, Beijing, China

Table 1: Description of benchmarks with prefixes of class/package names corresponding to syntactic and semantic analyses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Syntax Analysis Classes</th>
<th>Semantic Analysis Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maven</td>
<td>3.5.2</td>
<td>org/codehaus/plexus/util/xml</td>
<td>org/apache/maven/model</td>
</tr>
<tr>
<td>Ant</td>
<td>1.10.2</td>
<td>com/sun/org/apache/xerces</td>
<td>org/apache/tools/ant</td>
</tr>
<tr>
<td>Closure</td>
<td>v20180204</td>
<td>com/google/javascript/jscmp/parsing</td>
<td>com/google/javascript/jscmp/[A-Z]</td>
</tr>
<tr>
<td>Rhino</td>
<td>1.7.8</td>
<td>org/mozilla/javascript/Parser</td>
<td>org/mozilla/javascript/(optimizer</td>
</tr>
<tr>
<td>BCEL</td>
<td>6.2</td>
<td>org/apache/bcel/classfile</td>
<td>org/apache/bcel/verifier</td>
</tr>
</tbody>
</table>

To evaluate Zest’s effectiveness in this regard, we manually identify the components of our benchmark programs which correspond to syntax and semantic analysis stages. Table 1 lists prefix patterns that we match on the fully-qualified names of classes in our benchmarks to classify them in either stage. Section 5.1 evaluates the code coverage achieved within the classes identified as belonging to the semantic analysis stage. Section 5.2 evaluates the bug-finding capabilities of each technique for bugs that arise in the semantic analysis classes. Section 6 discusses some findings in the syntax analysis classes, whose testing is outside the scope of Zest.

5.1 Coverage of Semantic Analysis Classes

Instead of relying on our own instrumentation, we use a third party tool, the widely used Eclemma-JaCoCo [42] library, for measuring code coverage in our Java benchmarks. Specifically, we measure branch coverage within the semantic analysis classes from Table 1; we refer to these branches as semantic branches for short.

To approximate the coverage of the semantic branches covered via the selected test drivers, we report the percentage of total semantic branches covered. Note, however, that this is a conservative, i.e. low, estimate. This is because the total number of semantic branches includes some branches not reachable from the test driver. We make this approximation as it is not feasible to statically determine the number of branches reachable from a given entry point, especially in the presence of virtual method dispatch. We expect the percent of semantic branches reachable from our test drivers to be much lower than 100%; therefore, the relative differences between coverage are more important than the absolute percentages.

Figure 4 plots the semantic branch coverage achieved by each of Zest, AFL, and QuickCheck on the five benchmark programs across the 3-hour-long runs. In the plots, solid lines designate means and shaded areas designate 95% confidence intervals across the 20 repetitions. Interestingly, the variance in coverage is quite low for all techniques except QuickCheck. Since AFL is initialized with valid seed inputs, its initial coverage is non-zero; nonetheless, it is quickly overtaken by Zest, usually within the first 5 minutes.

Zest significantly outperforms baseline techniques in exercising branches within the semantic analysis stage, achieving statistically significant increases for all benchmarks. Zest covers as much as 2.81× as many semantic branches covered by the best baseline technique for Maven (Figure 4a). When looking at our Javascript benchmarks, we see that Zest’s advantage over QuickCheck is more slight in Rhino (Figure 4b) than in Closure (Figure 4c). This may be because Closure, which performs a variety of static code optimizations on JavaScript programs, has many input-dependent paths. Rhino, on the other hand, directly compiles valid JavaScript to JVM bytecode, and thus has fewer input-dependent paths for Zest to discover through feedback-driven parameter search.

Note that in some benchmarks AFL has an edge in coverage over QuickCheck (Figure 4a, 4b, 4c), and vice-versa (Figure 4c, 4d). For BCEL, this may be because the input format is a compact syntax, on which AFL generally excels. The difference between the XML and JavaScript benchmarks may be related to the ability of randomly-sampled inputs from the generator to achieve broad coverage. It is much more likely for a random syntactically valid JavaScript program to be semantically valid than a random syntactically valid XML document to be a valid POM file, for example. The fact that

Figure 4: Percent coverage of all branches in semantic analysis stage of the benchmark programs. Lines designate means and shaded regions 95% confidence intervals.
Zest dominates the baseline approaches in all these cases suggests that it is more robust to generator quality than QuickCheck.

5.2 Bugs in the Semantic Analysis Classes

Each of Zest, AFL, and QuickCheck keep track of generated inputs which cause test failures. Ideally, for any given input, the test program should either process it successfully or reject the input as invalid using a documented mechanism, such as throwing a checked `ParseException` on syntax errors. Test failures correspond either to assertion violations or to undocumented run-time exceptions being thrown during test execution, such as a `NullPointerException`. Test failures can occur during the processing of either valid or invalid inputs; the latter can lead to failures within the syntax or semantic analysis stages themselves.

Across all our experiments, the various fuzzing techniques generated over 95,000 failing inputs that correspond to over 3,000 unique stack traces. We manually triaged these failures by filtering them based on exception type, message text, and source location, resulting in a corpus of what we believe are 20 unique bugs. We have reported each of these bugs to the project developers. At the time of writing, 5 bugs have been fixed, 10 await patches, and 5 reports have received no response.

We classify each bug as syntactic or semantic, depending on whether the corresponding exception was raised within the syntactic or semantic analysis classes, respectively (ref. Table 1). Of the 20 unique bugs we found, 10 were syntactic and 10 were semantic.

Here, we evaluate Zest in discovering semantic bugs, for which it is specifically designed. Section 6 discusses the syntactic bugs we found, whose discovery was not Zest’s goal.

Table 2 enumerates the 10 semantic bugs that we found across four of the five benchmark programs. The bugs have been given unique IDs—represented as circled letters—for ease of discussion. The table also lists the type of exception thrown for each bug. To evaluate the effectiveness of each of the three techniques in discovering these bugs, we use two metrics. First, we are interested in knowing whether a given technique reliably finds the bug across repeated experiments. We define reliability as the percentage of the 20 runs (of 3-hours each) in which a given technique finds a particular bug at least once. Second, we measure the mean time to find (MTF) the first input that triggers the given bug, across the repetitions in which it was found. Naturally, a shorter MTF is desirable. For each bug, we circle the name of the technique that is the most effective in finding that bug. We define most effective as the technique with either the highest reliability, or if there is a tie in reliability, then the shortest MTF.

The table indicates that Zest is the most effective technique in finding 8 of the 10 bugs; in the remaining two cases (§ and ⃝), Zest still finds the bugs with 100% reliability and in less than 20 seconds on average. In fact, Zest finds all the 10 semantic bugs in at most 10 minutes on average; 7 are found within the first 2 minutes on average. In contrast, AFL requires more than one hour to find 3 of the bugs (§, ⃝, ⃝), and simply does not find 5 of the bugs within the 3-hour time limit. This makes sense because AFL’s mutations on the raw input strings do not guarantee syntactic validity; it generates much fewer inputs that reach the semantic analysis stage. QuickCheck discovers 8 of the 10 semantic bugs, but since it relies on random sampling alone, its reliability is often low. For example, QuickCheck discovers ⃝ only 10% of the time, and ⃝ only 5% of the time; Zest discovers them 100% and 95% of the time, respectively. Overall, Zest is clearly the most effective technique in discovering bugs in the semantic analysis classes of our benchmarks.

Case studies. In Ant, ⃝ is triggered when the input `build.xml` document contains both an `<augment>` element and a `<target>` element inside the root `<project>` element, but when the `<augment>` element is missing an id attribute. This incomplete semantic check leads to an `IllegalStateException` for a component down the pipeline which tries to configure an Ant task. Following our bug report, this issue has been fixed starting Ant version 1.10.6.

In Rhino, ⃝ is triggered by a semantically valid input. Rhino successfully validates the input JavaScript program and then compiles it to Java bytecode. However, the compiled bytecode is corrupted, which results in a `VerifyError` being generated by the JVM. AFL does not find this bug at all. The Rhino developers confirmed the bug, though a fix is still pending.

In Closure, ⃝ is an NPE that is triggered in its dead-code elimination pass when handling arrow functions that reference undeclared variables, such as "x => y". The generator-based techniques always find this bug and within just 8.8 seconds on average, while AFL requires more than 90 minutes and only finds it in 20% of the runs. The Closure developers fixed this issue after our report.

�� is a bug in Closure’s semantic analysis of variable declarations. The bug is triggered when a new variable is declared after a break statement. Although everything immediately after a break statement is unreachable code, variable declarations in JavaScript are hoisted and therefore cannot be removed. Zest is the only technique that discovered this bug. A sample input Zest generated is:

```
while ((l_0)){
        while ((l_0)){
            if ((l_0)){ break;;var l_0;continue }
                break;var l_0 }
          }
        }
```

�� was the most elusive bug that we encountered. Zest is the only technique that finds it and it does so in only one of the 20 runs. An exception is triggered by the following input:

```
((o_0) => (((o_0) *= (o_0))
        < ((i_1) &= ((o_0){{((undefined)[((i_1, o_0, a_2) => {
            if ((i_1)) { throw {{{false},o_0, a_2})
        }()})()})})))(()((y_3)))~~((new null){{true,undefined})}))
```

The issue is perhaps rooted in Closure’s attempt to compile-time evaluate `undefined[undefined]`(...). The developers acknowledged the bug but have not yet published a fix. These complex examples demonstrate both the power of Zest’s generators, which reduce the search space to syntactically valid inputs, as well as the effectiveness of its feedback-directed parameter search.

6 DISCUSSION AND THREATS TO VALIDITY

Zest and QuickCheck make use of generators for synthesizing inputs that are syntactically valid by construction. By design, these tools do not exercise code paths corresponding to parse errors in the syntax analysis stage. In contrast, AFL performs mutations directly on raw input strings. Byte-level mutations on raw inputs usually
Table 2: The 10 new bugs found in the semantic analysis stages of benchmark programs. The tools Zest, AFL, and QuickCheck (QC) are evaluated on the mean time to find (MTF) each bug across the 20 repeated experiments of 3 hours each as well as the reliability of this discovery, which is the percentage of the 20 repetitions in which the bug was triggered at least once. For each bug, the highlighted tool is statistically significantly more effective at finding the bug than unhighlighted tools.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Exception</th>
<th>Tool</th>
<th>Mean Time to Find (shorter is better)</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>ant B</td>
<td>IllegalStateException</td>
<td>Zest</td>
<td>(99.45 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(1208.0 sec)</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(6396.5 sec)</td>
<td>10%</td>
</tr>
<tr>
<td>closure C</td>
<td>NullableException</td>
<td>Zest</td>
<td>(8.8 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(5496.25 sec)</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(8.8 sec)</td>
<td>100%</td>
</tr>
<tr>
<td>closure D</td>
<td>RuntimeException</td>
<td>Zest</td>
<td>(460.42 sec)</td>
<td>60%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(5496.25 sec)</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(8.8 sec)</td>
<td>100%</td>
</tr>
<tr>
<td>closure U</td>
<td>NullableException</td>
<td>Zest</td>
<td>(534.0 sec)</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(18.6 sec)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(9.65 sec)</td>
<td>100%</td>
</tr>
<tr>
<td>rhino G</td>
<td>NullableException</td>
<td>Zest</td>
<td>(8.25 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(5343.0 sec)</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(9.65 sec)</td>
<td>100%</td>
</tr>
<tr>
<td>rhino F</td>
<td>NullableException</td>
<td>Zest</td>
<td>(18.6 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(9.85 sec)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(9.85 sec)</td>
<td>100%</td>
</tr>
<tr>
<td>rhino H</td>
<td>ClassCastException</td>
<td>Zest</td>
<td>(245.18 sec)</td>
<td>85%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(362.43 sec)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(362.43 sec)</td>
<td>35%</td>
</tr>
<tr>
<td>rhino J</td>
<td>Verifier</td>
<td>Zest</td>
<td>(94.75 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(229.5 sec)</td>
<td>0%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(229.5 sec)</td>
<td>80%</td>
</tr>
<tr>
<td>bcel O</td>
<td>ClassFormatException</td>
<td>Zest</td>
<td>(19.5 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(5.85 sec)</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(142.1 sec)</td>
<td>100%</td>
</tr>
<tr>
<td>bcel N</td>
<td>AssertionViolatedException</td>
<td>Zest</td>
<td>(19.32 sec)</td>
<td>95%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AFL</td>
<td>(1082.22 sec)</td>
<td>90%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QC</td>
<td>(15.0 sec)</td>
<td>5%</td>
</tr>
</tbody>
</table>

lead to inputs that do not parse. Consequently, AFL spends most of its time testing error paths within the syntax analysis stages.

In our experiments, AFL achieved the highest coverage within the syntax analysis classes of our benchmarks (ref. Table 1), 1.1×-1.6× higher than Zest’s syntax analysis coverage. Further, AFL discovered 10 syntactic bugs in addition to the bugs enumerated in Table 1: 3 in Maven, 6 in BCEL, and 1 in Rhino. These bugs were triggered by syntactically invalid inputs, which the generator-based tools do not produce. Zest does not attempt to target these bugs; rather, it is complementary to AFL-like tools.

Zest assumes the availability of QuickCheck-like generators to exercise the semantic analysis classes and to find semantic bugs. Although this is no doubt an additional cost, the effort required to develop a structured-input generator is usually no more than the effort required to write unit tests with hand-crafted structured inputs, which is usually an accepted cost. In fact, due to the growing popularity of generator-based testing tools like Hypothesis [11], ScalaCheck [14], PropEr [61], etc. a large number of off-the-shelf or automatically synthesized type-based generators are available. The Zest technique can, in principle, work with any such generator. When given a generator, Zest excels at exercising semantic analyses and is very effective in discovering semantic bugs.

We did not evaluate how Zest’s effectiveness might vary depending on the quality of generators, since we hand-wrote the simplest generators possible for our benchmarks. However, our results suggest that Zest’s ability to guide generation towards paths deep in the semantic analysis stage make its performance less tied to generator quality than pure random sampling as in QuickCheck.

The effectiveness of CGF tools like AFL is usually sensitive to the choice of seed inputs [47]. Although the relative differences
between the performance of Zest and AFL will likely vary with this choice, the purpose of our evaluation was to demonstrate that focusing on feedback-directed search in the space of syntactically valid inputs is advantageous. No matter what seed inputs one provides to conventional fuzzing tools, the byte-level mutations on raw inputs will lead to an enormous number of syntax errors. We believe that approaches like Zest complement CGF tools in testing different components of programs.

7 RELATED WORK

A lot of research has gone into automated test-input generation techniques, as surveyed by Anand et al. [17].

Randoop [59] and EvoSuite [36] generate JUnit tests for a particular class by incrementally trying and combining sequences of calls. During the generation of sequence of calls, both Randoop and EvoSuite take some form of feedback into account. These tools produce unit tests by directly invoking methods on the component classes. In contrast, Zest addresses the problem of generating inputs when given a test driver and an input generator.

UDITA [38] allows developers to write random-input generators in a QuickCheck-like language. UDITA then performs bounded-exhaustive enumeration of the paths through the generators, along with several optimizations. In contrast, Zest relies on random mutations over the entire parameter space but uses code coverage and input-validity feedback to guide the parameter search. It would be interesting to see if UDITA’s search strategy could be augmented to selectively adjust bounds using code coverage and validity feedback; however, we leave this investigation as future work.

Targeted property-testing [54, 55] guides input generators used in property testing towards a user-specified fitness value using techniques such as hill climbing and simulated annealing. GödelTest [35] attempts to satisfy user-specified properties on inputs. It performs a meta-heuristic search for stochastic models that are used to sample random inputs from a generator. Unlike these techniques, Zest relies on code coverage feedback to guide input generation towards exploring diverse program behaviors.

In the security community, several tools have been developed to improve the effectiveness of coverage-guided fuzzing in reaching deep program states [24, 28, 50, 52, 63]. AFLGo [24] extends AFL to direct fuzzing towards generating inputs that exercise a program point of interest. It relies on call graphs obtained from whole-program static analysis, which can be difficult to compute precisely in our ecosystem. Zest is purely a dynamic analysis tool. FairFuzz [50] modifies AFL to bias input generation towards branches that are rarely executed, but does not explicitly identify parts of the program that perform the core logic. In Zest, we bias input generation towards validity no matter how frequently the semantic analysis stage is exercised.

Zest generates inputs that are syntactically valid by construction (assuming suitable generators), but uses heuristics to guide input generation towards semantic validity. Unlike Zest, symbolic execution tools [18, 21, 27, 29, 31, 39, 40, 46, 51, 65, 69] methodically explore the program under test by capturing path constraints and can directly generate inputs which satisfy specific path constraints. Symbolic execution can thus precisely produce valid inputs exercising new behavior. The cost of this precision is that it can lead to the path explosion problem for larger programs. Hybrid techniques that combine symbolic execution with coverage-guided fuzzing have been proposed [26, 57, 68, 73]. These hybrid techniques could be combined with Zest to solve for parameter sequences that satisfy branch constraints which Zest may not cover on its own.

Grammar-based fuzzing [23, 32, 39, 56, 67] techniques rely on context-free grammar specifications to generate structured inputs. CSmith [72] generates random C programs for differential testing of C compilers. LangFuzz [43] generates random programs using a grammar and by recombining code fragments from a codebase. These approaches fall under the category of generator-based testing, but primarily focus on tuning the underlying generators rather than using code coverage feedback. Zest is not restricted to context-free grammars, and does not require any domain-specific tuning.

Several recently developed tools leverage input format specifications (either grammars [20, 71], file formats [62], or protocol buffers [66]) to improve the performance of CGF. These tools develop mutations that are specific to the input format specifications, e.g. syntax-tree mutations for grammars. Zest’s generators are arbitrary programs; therefore, we perform mutations directly on the parameters that determine the execution path through the generators, rather than on a parsed representation of inputs.

There has also been some recent interest in automatically generating input grammars from existing inputs, using machine learning [41] and language inference algorithms [22]. Similarly, DILFAZE [53] infers device driver interfaces from a running kernel to bootstrap subsequent structured fuzzing. These techniques are complementary to Zest—the grammars generated by these techniques could be transformed into parametric generators for Zest.

Finally, validity feedback has been useful in fuzzing digital circuits that have constrained interfaces [48], as well as in generating seed inputs for conventional fuzzing [70].

8 CONCLUSION

We presented Zest, a technique that incorporates ideas from coverage-guided fuzzing into generator-based testing. We showed how a simple conversion of random-input generators into parametric input generators enables an elegant mapping from low-level mutations in the untyped parameter domain into structural mutations in the syntactically valid input domain. We then presented an algorithm that combined code coverage feedback with input-validity feedback to guide the generation of test inputs. On 5 real-world Java benchmarks, we found that Zest achieved consistently higher branch coverage and had better bug-finding ability in the semantic analysis stage than baseline techniques. Our results suggest that Zest is highly effective at testing the semantic analysis stage of programs, complementing tools such as AFL that are effective at testing the syntactic analysis stage of programs.

ACKNOWLEDGMENTS

We would like to thank Kevin Laeufer and Michael Dennis for their helpful feedback during the development of this project, as well as Benjamin Brock and Rohan Bavishi for their invaluable comments on the paper draft. This research is supported in part by gifts from Samsung, Facebook, and Futurewei, and by NSF grants CCF-1409872 and CNS-1817122.