PLRG
Programming Language
Research Group

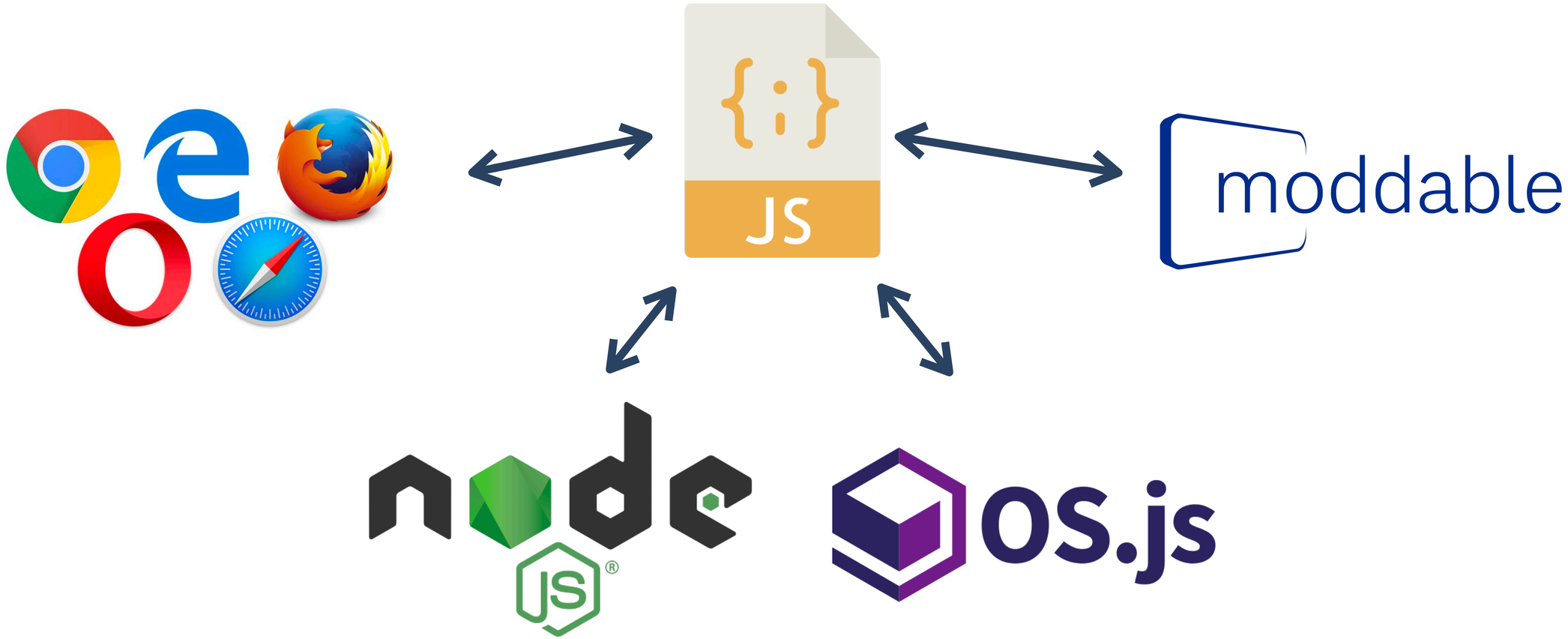
JEST: N+1-version Differential Testing of Both JavaScript Engines and Specification

The 43rd International Conference on
Software Engineering (ICSE'21)

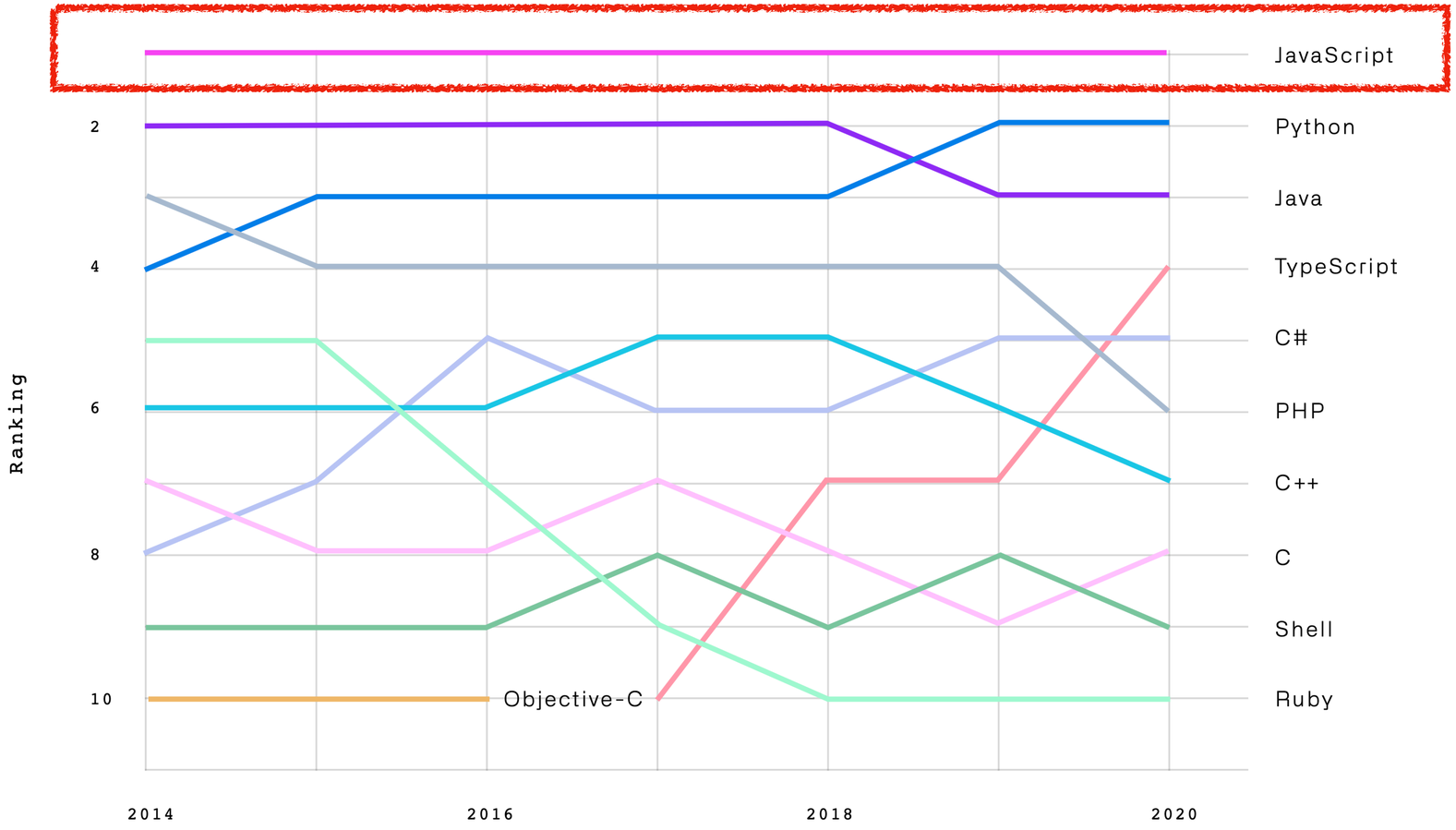
Jihyeok Park, Seungmin An, Donjun Youn,
Geyongwon Kim, Sukyoung Ryu

PLRG @ KAIST
May 28, 2021

JavaScript is Everywhere



JavaScript is Dominating



https://octoverse.github.com/

JavaScript Specification and Engines

ECMAScript

?

Conformance

Conformance

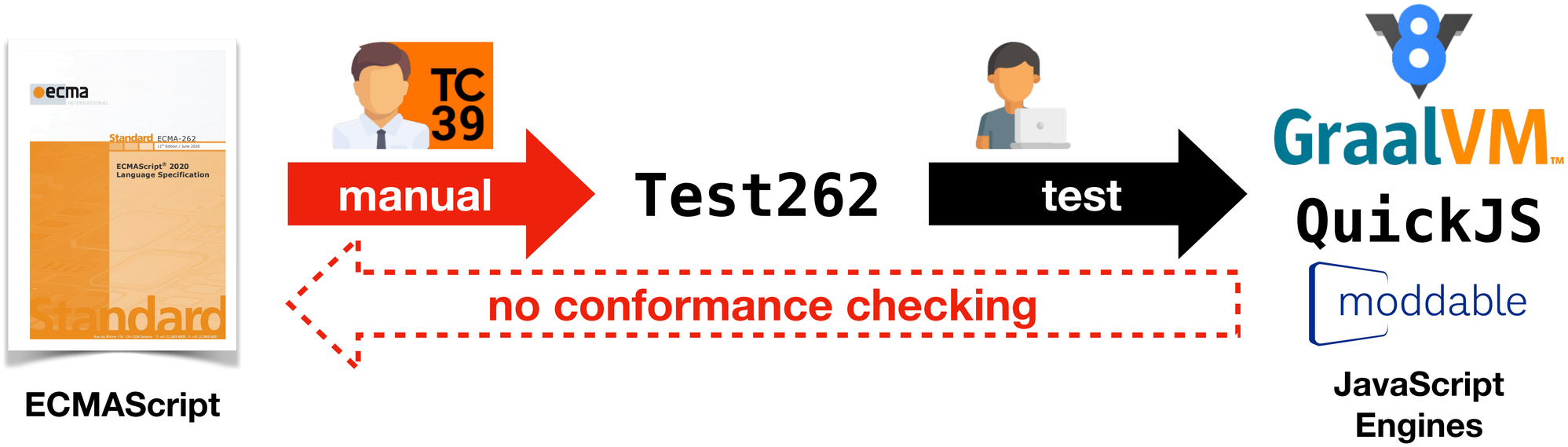
GraalVM

QuickJS

moddable

JavaScript Engines

Test262: JavaScript Conformance Tests



N+1-version Differential Testing

ECMAScript

Synthesize

Test

test

test

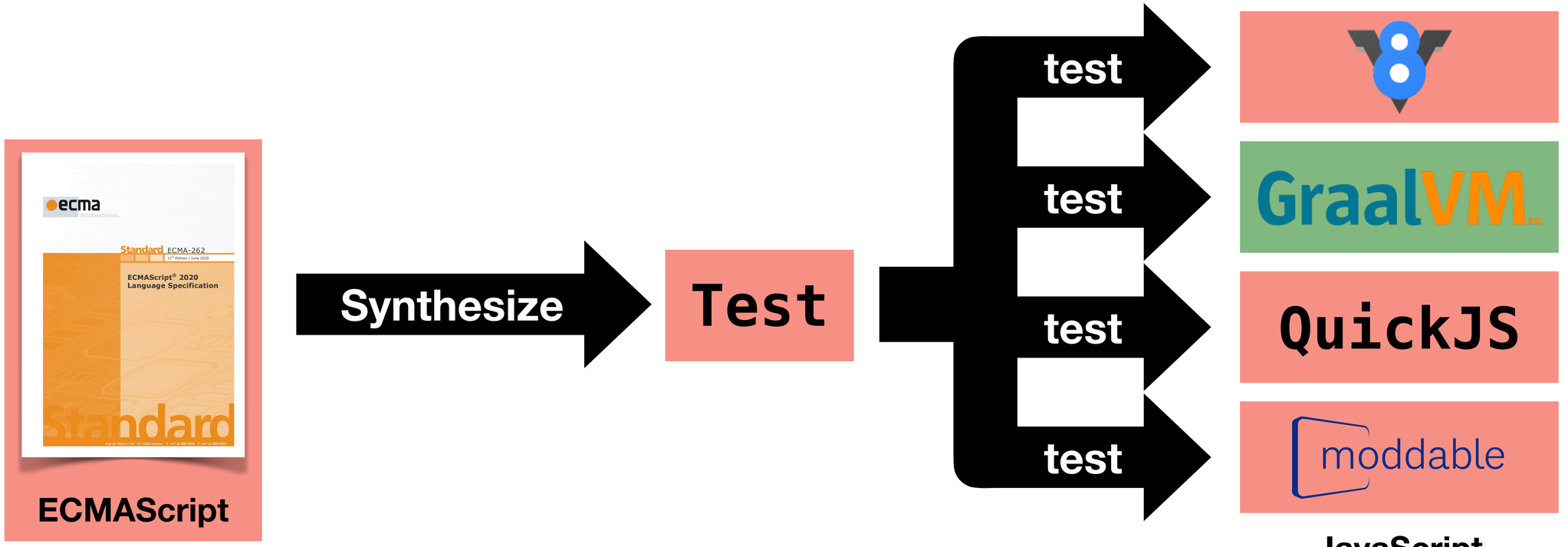
test

test

JavaScript Engines

An engine bug in

N+1-version Differential Testing

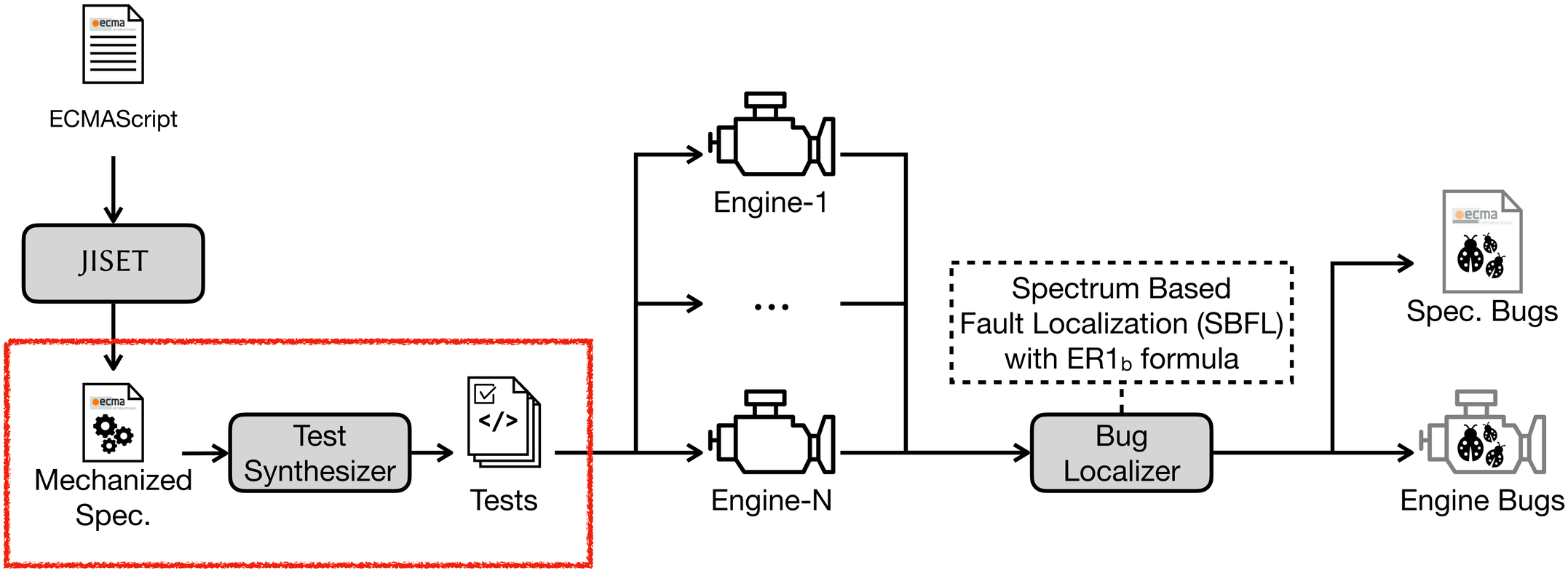


A <u>specification</u> bug in ECMAScript

An <u>engine</u> bug in GraalVM

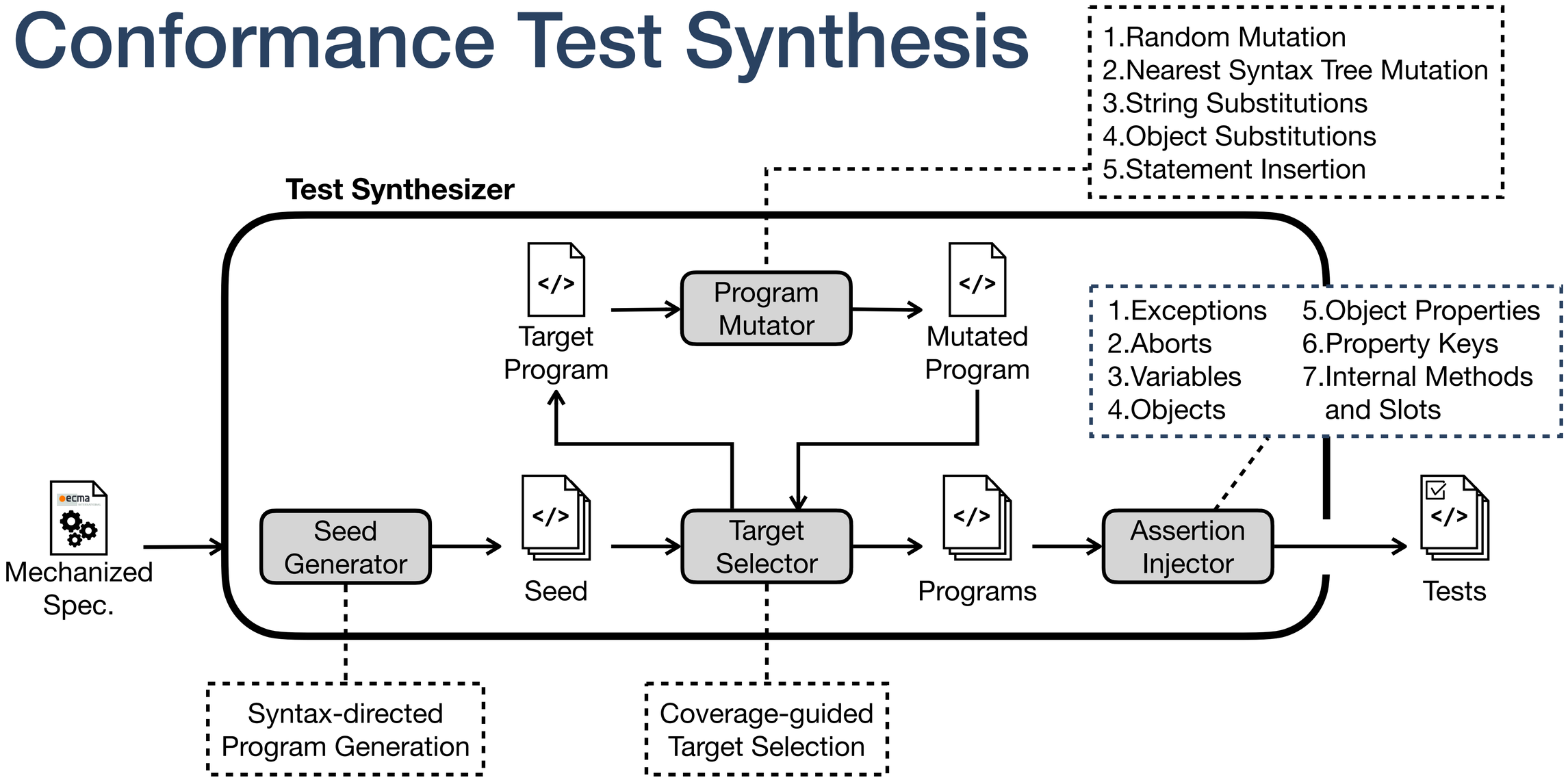
JEST

JavaScript Engines and Specification Tester



[ASE'20] Park et al, “JISET: Javascript IR-based Semantics Extraction Toolchain”

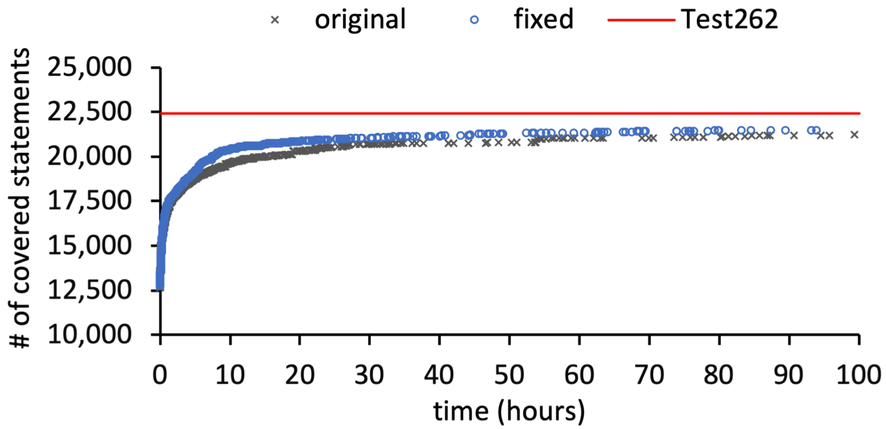
Conformance Test Synthesis



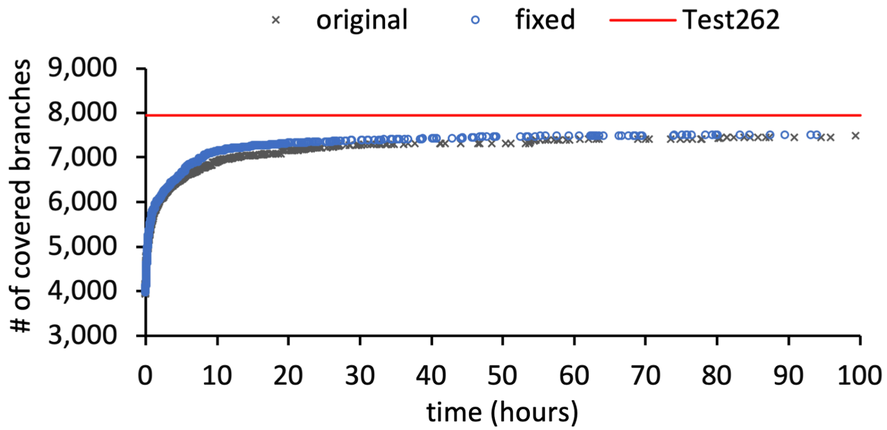
Evaluation

- **JavaScript Specification**
  - ECMAScript 2020 (ES11) - released in June 2020
- **JavaScript Engines**
  - V8 - v8.3 by Google
  - GraalJS - v20.1.0 by Oracle
  - QuickJS - 2020-04-12 by Fabrice Bellard
  - Moddable XS - v10.3.0 by Moddable Tech Inc.

RQ1: Coverage of Synthesized Tests



(a) Statement coverage



(b) Branch coverage

- 1,700 **Synthesized Tests in** 100 hours
- **Syntax Coverage:** 97.79% (397 / 406)
- **Semantics Coverage**
  - Statement: 86.67% (21,230 / 24,495)
  - Branch: 77.95% (7,480 / 9,596)

RQ2: Bug Detection in JavaScript Engines

TABLE II: The number of engine bugs detected by JEST

Engines	Exc	Abort	Var	Obj	Desc	Key	In	Total
V8	0	0	0	0	0	2	0	2
GraalJS	6	0	0	0	2	8	0	16
QuickJS	3	0	1	0	0	2	0	6
Moddable XS	12	0	0	0	3	5	0	20
Total	21	0	1	0	5	17	0	44

```
function f (... { x = x }) { return x; } var y = f();
```

QuickJS initializes 'x' with '`undefined`' instead of throwing a '`ReferenceError`'

```
try { ++undefined; } catch(e) { }
```

GraalJS crashes with an exception '`java.lang.IllegalStateException`'

RQ3: Bug Detection in ECMAScript

TABLE III: Specification bugs in ECMAScript 2020 (ES11) detected by JEST

Name	Feature	#	Assertion	Known	Created	Resolved	Existed
ES11-1	Function	12	Key	O	2019-02-07	2020-04-11	429 days
ES11-2	Function	8	Key	O	2015-06-01	2020-04-11	1,776 days
ES11-3	Loop	1	Exc	O	2017-10-17	2020-04-30	926 days
ES11-4	Expression	4	Abort	O	2019-09-27	2020-04-23	209 days
ES11-5	Expression	1	Exc	O	2015-06-01	2020-04-28	1,793 days
ES11-6	Object	1	Exc	X	2019-02-07	2020-11-05	637 days

```
@@ -12789,7 +12789,7 @@ <h1>Runtime Semantics: PropertyDefinitionEvaluation</h1>
12789  12789          1. Let _propKey_ be the result of evaluating |PropertyName|.
12790  12790          1. ReturnIfAbrupt(_propKey_).
12791  12791          1. If IsAnonymousFunctionDefinition(|AssignmentExpression|) is *true*, then
12792        -          1. Let _propValue_ be NamedEvaluation of |AssignmentExpression| with argument _propKey_.
       12792  +       1. Let _propValue_ be ? NamedEvaluation of |AssignmentExpression| with argument _propKey_.
12793  12793          1. Else,
12794  12794            1. Let _exprValueRef_ be the result of evaluating |AssignmentExpression|.
12795  12795            1. Let _propValue_ be ? GetValue(_exprValueRef_).
```

https://github.com/tc39/ecma262/pull/2130/files

RQ4: Accuracy of Bug Localization

- **64 out of 71 bugs are semantics bugs**

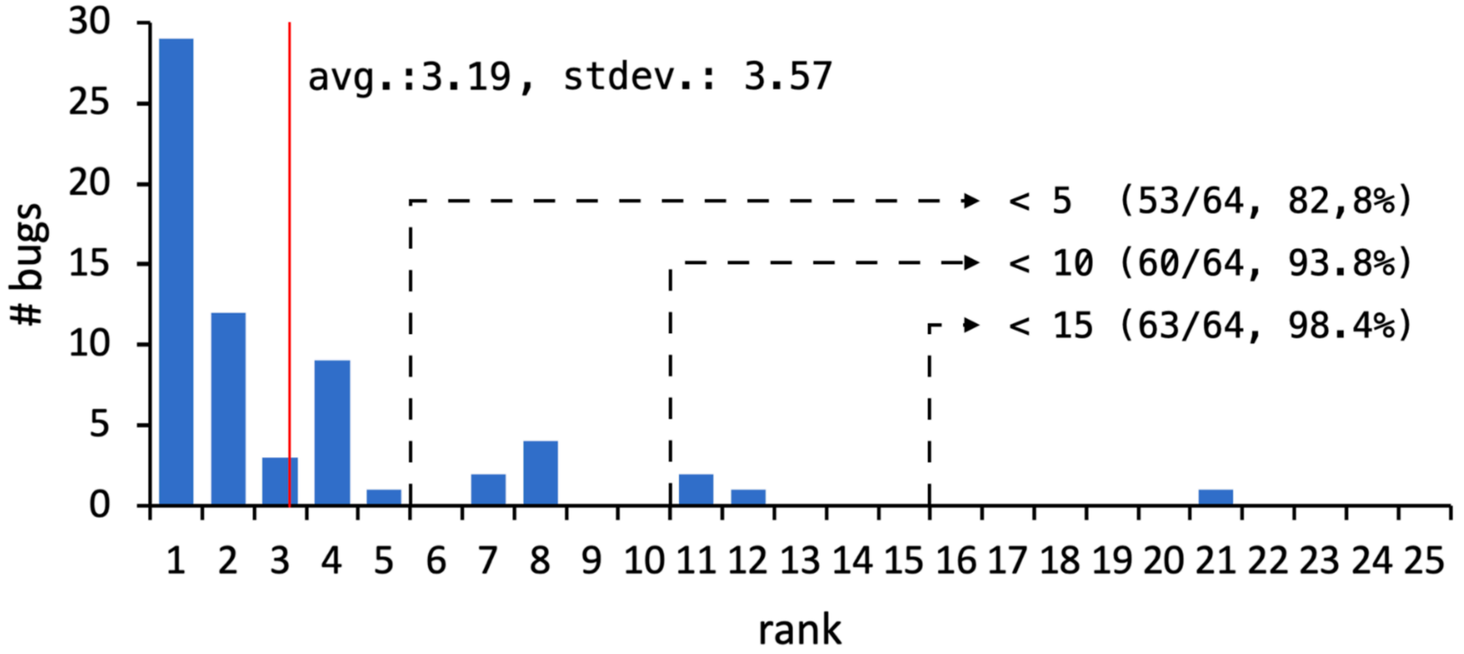
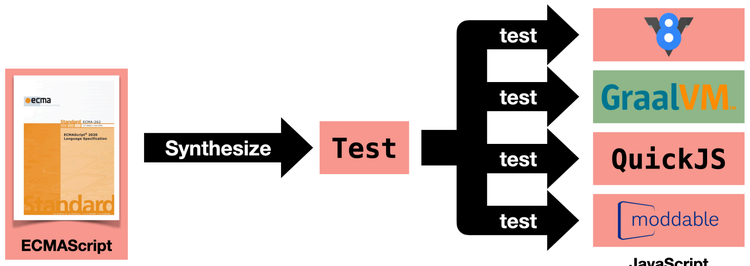


Fig. 5: Ranks of algorithms that caused the bugs detected by JEST

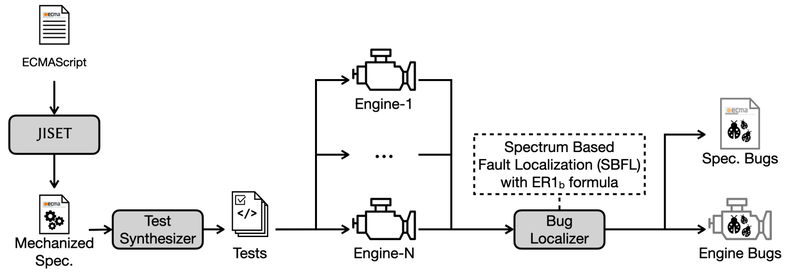
N+1-version Differential Testing



A specification bug in ECMAScript
An engine bug in GraalVM

JEST

JavaScript **E**ngines and **S**pecification **T**ester



[ASE'20] Park et al, "JISET: Javascript IR-based Semantics Extraction Toolchain"

RQ2: Bug Detection in JavaScript Engines

TABLE II: The number of engine bugs detected by JEST

Engines	Exc	Abort	Var	Obj	Desc	Key	In	Total
V8	0	0	0	0	0	2	0	2
GraalJS	6	0	0	0	2	8	0	16
QuickJS	3	0	1	0	0	2	0	6
Moddable XS	12	0	0	0	3	5	0	20
Total	21	0	1	0	5	17	0	44

```
function f (... { x = x }) { return x; } var y = f();
```

QuickJS initializes 'x' with 'undefined' instead of throwing a 'ReferenceError'

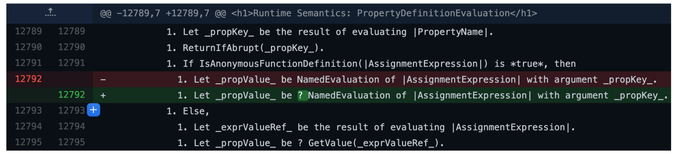
```
try { ++undefined; } catch(e) { }
```

GraalJS crashes with an exception 'java.lang.IllegalStateException'

RQ3: Bug Detection in ECMAScript

TABLE III: Specification bugs in ECMAScript 2020 (ES11) detected by JEST

Name	Feature	#	Assertion	Known	Created	Resolved	Existed
ES11-1	Function	12	Key	O	2019-02-07	2020-04-11	429 days
ES11-2	Function	8	Key	O	2015-06-01	2020-04-11	1,776 days
ES11-3	Loop	1	Exc	O	2017-10-17	2020-04-30	926 days
ES11-4	Expression	4	Abort	O	2019-09-27	2020-04-23	209 days
ES11-5	Expression	1	Exc	O	2015-06-01	2020-04-28	1,793 days
ES11-6	Object	1	Exc	X	2019-02-07	2020-11-05	637 days



https://github.com/tc39/ecma262/pull/2130/files