Extending Bug Detector and Improving Analysis Performance in SAFE

Sooncheol Won
Programming Language Research Group
wonsch@kaist.ac.kr

KAIST Computer Science
PLRG Programming Language Research Group

Sukyoung Ryu
sryu.cs@kaist.ac.kr

Contributions

Bug Detection

1) First work to identify all 155 errors specified in ECMAScript
2) Extension of the SAFE bug detector to catch 129 out of 155 errors

Analysis

1) Significant speed up by multi-threading
2) High analysis coverage by a new worklist order algorithm
3) More speed up by combination of above two methods

Bug Detector

Error

Unhandled exception raised at runtime

```
var a = undefined;
var x = a.p;
```

Warning

Unexpected behaviors,

security or optimization problems

```
var a = new Array(16);
var x = -a[3];
```

Detects 6 Errors and 15 Warnings
Covers mistakes easily made by users

Example

```
* Bug Detector *
1) 3d-raytrace.js:118:19~118:23: [Warning]
    Trying to convert undefined to number. 'self[3]' can be undefined.
```

```
116: function invertMatrix(self) {
118:     var tx = -self[3]; // undefined
130: }
     ...
270: function Camera(origin, lookat, up) {
274:     var m = new Array(16);
         ...
278:     invertMatrix(m);
279:     m[3] = 0; m[7] = 0; m[11] = 0;
290: }
```

Bug Detector Extension

Bug definition : "An exception that stops the program execution."

	Range Error	Reference Error	Syntax Error	Type Error	URI Error	Total
ECMAScript	7	7	31	98	12	155
BugDetector	7	7	31	72	12	129

1) Semantics of CFG instructions is not one-to-one correspondence to AST's
2) Some built-in functions or internal functions are not yet modeled

Multi-threading

Iterations / Analysis time

Benchmark	Single-thread	Multi-threads	Reduced
crypto.js	330,855 / 80.37	353,593 / 20.26	74.8%
deltablue.js	95,561 / 21.78	144,567 / 8.44	61.2%
richards.js	13,102 / 4.47	13,092 / 3.23	27.7%
3d-cube.js	52,404 / 10.15	43,651 / 4.67	54.0%
3d-raytrace.js	22.919 / 6.69	41,456 / 4.71	29.6%
crypto-md5.js	28,937 / 7.15	14,947 / 3.42	52.1%
wikipedia.org	5,016 / 30.23	8,389 / 17.66	41.6%
soso.com	47,517 / 24.54	64,044 / 11.39	53.6%
directrev.com	34,137 / 43.34	34,024 / 17.74	59.1%
thepiratebay.sx	891 / 4.67	675 / 2.82	39.6%

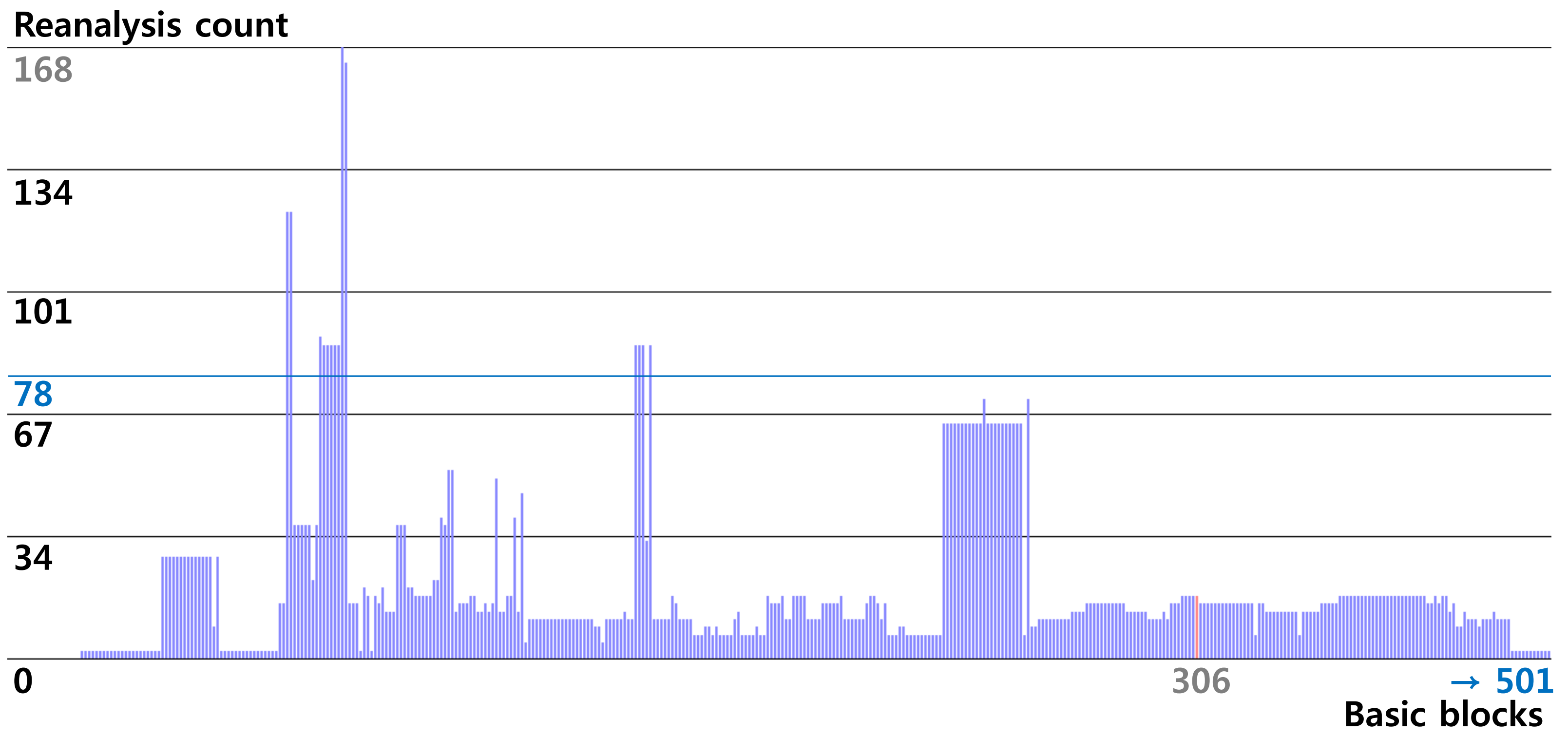
1) Shared data accesses
2) Reanalyzed basic blocks

Average : 49.3%

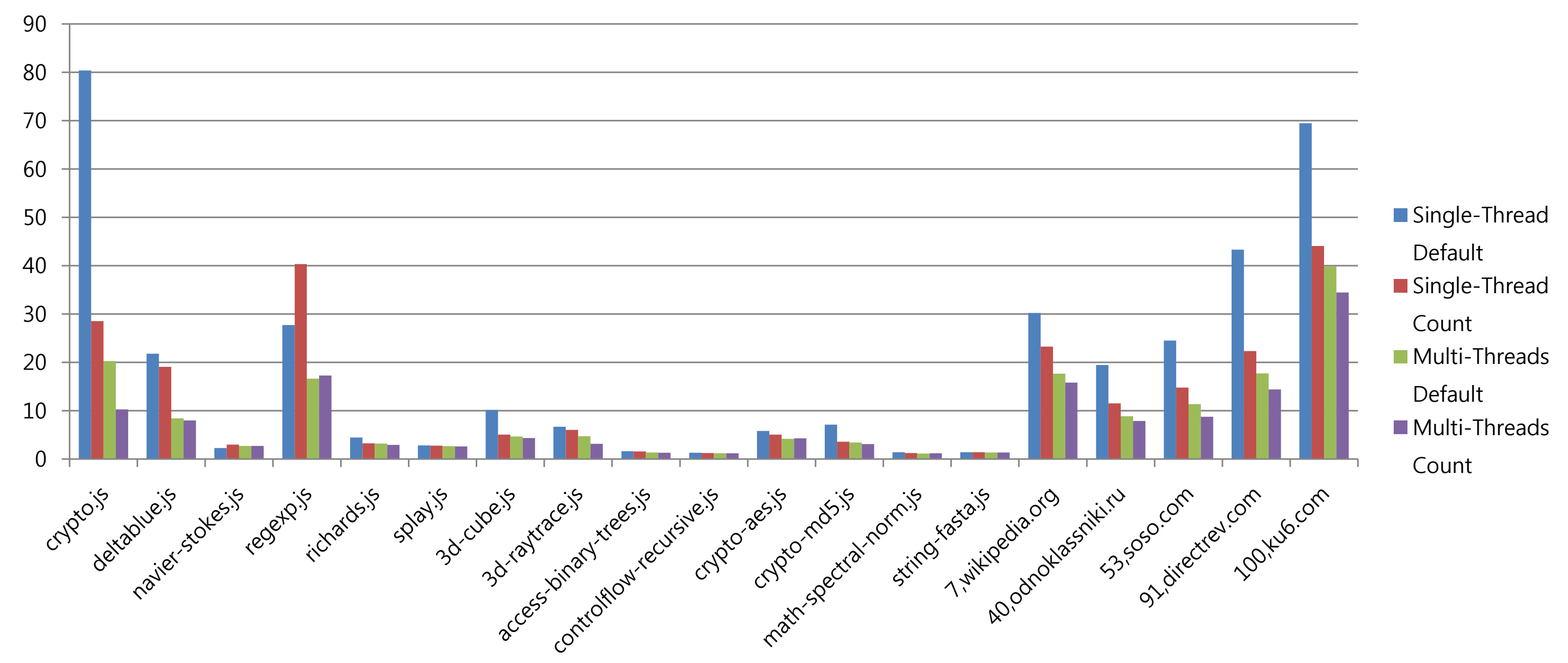
Analysis Performance Improvement

Maximizing Analysis Coverage

Default vs Count worklist order algorithm



Combination


crypto.js
deltablue.js
navier-stokes.js
regexp.js
richards.js
splay.js
3d-cube.js
3d-raytrace.js
access-binary-trees.js
controlflow-recursive.js
crypto-aes.js
crypto-md5.js
math-spectral-norm.js
string-fasta.js
7,wikipedia.org
40,odnoklassniki.ru
53,soso.com
91,directrev.com
100,ku6.com
Single-Thread Default
Single-Thread Count
Multi-Threads Default
Multi-Threads Count