



ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Doop-Soot: Parallel Fact Generation

Mouris Dimitris

Επιβλέπων: Smaragdakis Yannis, Associate Professor NKUA

ΑΘΗΝΑ

ΣΕΠΤΕΜΒΡΗΣ 2016

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Doop-Soot: Parallel Fact Generation

Mouris Dimitris

A.M.: 1115201200114

ΕΠΙΒΛΕΠΩΝ: Smaragdakis Yannis, Associate Professor NKUA

ΠΕΡΙΛΗΨΗ

Παραλληλοποίηση του Fact Generation του Doop. Το Doop χρησιμοποιείται για μπλαμπλαμπλ

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Τεκμηρίωση

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: static program analysis, doop: fact generation, soot, πτυχιακές εργασίες, τμήμα πληροφορικής και τηλεπικοινωνιών

Πανεπιστήμιο Αθηνών

ABSTRACT

Παραλληλοποίηση του Fact Generation του Doop. Το Doop χρησιμοποιείται για μπλαμπλαμπλαμπλ

SUBJECT AREA: Documentation

KEYWORDS: static program analysis, doop: fact generation, soot, undergraduate thesis, dept. of informatics

University of Athens

Αφιέρωση σε κάποιους.

ACKNOWLEDGEMENTS

blahblahblahblah

blahblahblahblah

blahblahblahblah

ΠΕΡΙΕΧΟΜΕΝΑ

PROLOGUE	11
1. INTRODUCTION	12
2. DOOP	13
2.1 Fact Generation	13
2.2 Doop-Nexgen Time Examples	13
3. SOOT	14
3.1 Bytecode To Jimple	14
3.2 Jimple Examples	14
3.2.1 Hello World	15
3.2.2 Inheritance Test	16
3.3 Compiling & Running Soot	18
4. FOUR APPROACHES	19
4.1 One Thread Per Method	19
4.2 One Thread Per Class	20
4.3 Fork-Join Framework	21
4.4 Multiple Classes Per Thread	23
5. LOCKING	24
5.1 Type Assigner	24
5.2 Fact Writer	24
5.2.1 CSVDatabase	24
5.2.2 Repesantation	24
5.3 Pack Manager	24
5.4 Shimple -ssa	25
6. TIME RESULTS	26
ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ	27

ABBREVIATIONS	28
REFERENCES	29

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1:	HelloWorld.java	15
Σχήμα 2:	HelloWorld.jimple	15
Σχήμα 3:	inheritanceTest.java	16
Σχήμα 4:	inheritanceTest.jimple	17
Σχήμα 5:	Compiling Soot	18
Σχήμα 6:	Generating Jimple from .class	18
Σχήμα 7:	Generating Jimple from .jar	18
Σχήμα 8:	Linear Fact Generation	19
Σχήμα 9:	One Thread Per Method	20
Σχήμα 10:	One Thread Per Class	21
Σχήμα 11:	Fork-Join Basic-Use	22
Σχήμα 12:	Fork-Join Framework	22
Σχήμα 13:	Multiple Classes Per Thread	23
Σχήμα 14:	JimpleBodyPack.java	24
Σχήμα 15:	CSVDatabase.java	24
Σχήμα 16:	Represantation.java	24
Σχήμα 17:	PackManager.java	25
Σχήμα 18:	Fact Generation Time Results	26

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1: Soot 2.5.0 times	13
---------------------------------------	----

PROLOGUE

Το παρόν έγγραφο δημιουργήθηκε στην Αθήνα, το 2016

blahblahblahblah

blahblahblahblah

1. INTRODUCTION

eisagwgh gia doop kai soot

2. DOOP

Doop is a framework for pointer, or points-to, analysis of Java programs. Doop implements a range of algorithms, including context insensitive, call-site sensitive, and object-sensitive analyses, all specified modularly as variations on a common code base. [1]

2.1 Fact Generation

Doop before running a pointer or points-to analysis, integrates with Soot to generate the facts. Facts are in Jimple (**J**ava **s**imple), a typed 3-address IR suitable for performing optimizations, it only has 15 statements.

2.2 Doop-Nexgen Time Examples

Soot 2.5.0	antlr.jar	hsqldb.jar	batik.jar
Fact Generation	1.16 min.	1.23 min.	2.26 min.
Total time	3.18 min.	3.21 min.	4.34 min.

Πίνακας 1: Soot 2.5.0 times

3. SOOT

Originally, Soot started off as a Java optimization framework. By now, researchers and practitioners from around the world use Soot to analyze, instrument, optimize and visualize Java and Android applications. [2]

3.1 Bytecode To Jimple

Soot is able to translate Java bytecode to a typed 3-address IR, Jimple. Jimple (Java Simple) is a very convenient IR for performing optimizations, it only has 15 statements.

First step is a naive translation to untyped Jimple with new local variables. Then Types are inferred to the untyped jimple. An important step is the linearization of expressions to statements only reference at most 3 local variables or constants. The local variables which start with a \$ sign represent stack positions and not local variables in the original program whereas those without \$ represent real local variables.

We now describe how Soot handles Java bytecode classes. In a typical case, Soot is launched by specifying the target directory as a parameter. This directory contains the code of the program to analyze, called Application Code (only Java bytecode in this example). First, the *main()* method of the Main class is executed and calls

Scene.loadNecessaryClasses(). This method loads basic Java classes and then loads specific Application classes by calling *loadClass()*. Then, *SootResolver.resolveClass()* is called. The resolver calls

SourceLocator.getClassSource() to fetch a reference to a *ClassSource*, an interface between the file containing the Java bytecode and Soot. In our case the class source is a *CoffiClassSource* because it is the coffi module which handles the conversion from Java bytecode to Jimple.

When the resolver has a reference to a class source, it calls *resolve()* on it. This method in turn calls

soot.coffi.Util.resolveFromClassFile() which creates a *SootClass* from the corresponding Java bytecode class. All source fields of Soot class' methods are set to refer to a *CoffiMethodSource* object. This object is used later to get the Jimple representation of the method. For instance, if during an analysis with Soot the analysis code calls

SootMethod.getActiveBody() and the Jimple code of the method was not already generated, *getActiveBody()* will call

CoffiMethodSource.getBody() to compute Jimple code from the Java bytecode. The Jimple code representation of the method can then be analyzed and/or transformed.

3.2 Jimple Examples

Below are two simple java programs along with their jimple translation. The first one is the classic HelloWorld, and the second is a simple inheritance test that depends on the user's input.

3.2.1 Hello World

```

1      public class helloWorld {
2          public static void main(String[] args) {
3              System.out.println("Hello, World");
4          }
5      }

```

Σχήμα 1: HelloWorld.java

```

1      public class helloWorld extends java.lang.Object {
2
3          public void <init>() {
4              helloWorld r0;
5              r0 := @this: helloWorld;
6              specialinvoke r0.<java.lang.Object: void <init>()>();
7              return;
8          }
9
10         public static void main(java.lang.String []) {
11             java.lang.String [] r0;
12             java.io.PrintStream $r1;
13             r0 := @parameter0: java.lang.String[];
14             $r1 = <java.lang.System: java.io.PrintStream out>;
15             virtualinvoke $r1.<java.io.PrintStream: void
16                 println (java.lang.String)>("Hello, World");
17             return;
18         }
19     }

```

Σχήμα 2: HelloWorld.jimple

3.2.2 Inheritance Test

```
1      public class inheritanceTest {
2
3          public static void main(String[] args) {
4              testA a;
5              if (args.length < 1) {
6                  a = new testA(5);
7              } else {
8                  a = new testB(5);
9              }
10             int result = a.getA();
11             System.out.println("the value of a is " + result);
12         }
13
14         public static class testA {
15             int a;
16
17             public testA(int a) {
18                 this.a = a;
19             }
20
21             public int getA() {
22                 return this.a;
23             }
24         }
25
26         public static class testB extends testA {
27             public testB(int a) {
28                 super(a+100);
29             }
30         }
31     }
32 }
```

Σχήμα 3: inheritanceTest.java

```

1      public class inheritanceTest extends java.lang.Object {
2
3          public void <init>() {
4              inheritanceTest r0;
5              r0 := @this: inheritanceTest;
6              specialinvoke r0.<java.lang.Object: void <init>()>();
7              return;
8          }
9
10         public static void main(java.lang.String []) {
11             java.lang.String [] r0;
12             int $i0, i1;
13             inheritanceTest$testA $r1, r2;
14             inheritanceTest$testB $r3;
15             java.io .PrintStream $r4;
16             java.lang.StringBuilder $r5, $r6, $r7;
17             java.lang.String $r8;
18             r0 := @parameter0: java.lang.String[];
19             $i0 = lengthof r0;
20             if $i0 >= 1 goto label1;
21             $r1 = new inheritanceTest$testA;
22             specialinvoke $r1.<inheritanceTest$testA: void <init>(int)>(5);
23             r2 = $r1;
24             goto label2;
25         label1:
26             $r3 = new inheritanceTest$testB;
27             specialinvoke $r3.<inheritanceTest$testB: void <init>(int)>(5);
28             r2 = $r3;
29         label2:
30             i1 = virtualinvoke r2.<inheritanceTest$testA: int getA()>();
31             $r4 = <java.lang.System: java.io.PrintStream out>;
32             $r5 = new java.lang.StringBuilder;
33             specialinvoke $r5.<java.lang.StringBuilder: void <init>()>();
34             $r6 = virtualinvoke $r5.<java.lang.StringBuilder:
35                 java.lang.StringBuilder append(java.lang.String)>("the value
36                 of a is ");
37             $r7 = virtualinvoke $r6.<java.lang.StringBuilder:
38                 java.lang.StringBuilder append(int)>(i1);
39             $r8 = virtualinvoke $r7.<java.lang.StringBuilder: java.lang.String
40                 toString()>();
41             virtualinvoke $r4.<java.io.PrintStream: void
42                 println (java.lang.String)>($r8);
43             return;
44         }
45     }

```

Σχήμα 4: inheritanceTest.jimple

3.3 Compiling & Running Soot

```

1      ant          /* To compile */
2      ant classesjar /* To generate the sootclasses jar file */
3      ant fulljar   /* To generate the complete soot jar file */

```

Σχήμα 5: Compiling Soot

```

1      (create a test.java)
2      javac test.java
3      java -cp ./lib/soot-trunk.jar soot.Main -f J -cp
        ./usr/lib/jvm/java-7-openjdk-amd64/jre/lib/rt.jar test

```

Σχήμα 6: Generating Jimple from .class

```

1      java -cp soot-trunk.jar soot.Main -f J -cp
        ./usr/lib/jvm/java-7-openjdk-amd64/jre/lib/rt.jar -process-dir
        pathtotest.jar

```

Σχήμα 7: Generating Jimple from .jar

4. FOUR APPROACHES

Abstract: Linear Fact Generation

```

1      public class FactGenerator {
2          /* ... */
3
4      public void generate(sootClass) {
5          if (c.hasSuperclass() && !c.isInterface())
6              _writer.writeDirectSuperclass(c, c.getSuperclass());
7          for(SootField f : c.getFields())
8              generate(f);
9          for(SootMethod m : c.getMethods()) {
10             Session session = new Session();
11             generate(m, session);
12         }
13     }
14
15     public void generate(SootMethod m, Session session) {
16         /* ... */
17
18         /* This instruction spends more than 80% of FG time */
19         m.retrieveActiveBody()
20
21         /* ... */
22     }
23
24     /* ... */
25 }

```

Σχήμα 8: Linear Fact Generation

4.1 One Thread Per Method

Our first approach to parallelize Fact Generation. Similar as the linear one, but instead of having a loop over all Soot Methods, we create a runnable for each one of them.

```

1      public class FactGenerator {
2          private ExecutorService MgExecutor = new ThreadPoolExecutor(8, 16, 0L,
3              TimeUnit.MILLISECONDS, new LinkedBlockingQueue<Runnable>());
4              /* ... */
5
6          public void generate(sootClass) {
7              if (c.hasSuperclass() && !c.isInterface())
8                  _writer.writeDirectSuperclass(c, c.getSuperclass());
9              for (SootField f : c.getFields())
10                  generate(f);
11              for (SootMethod m : c.getMethods()) {
12                  Session session = new Session();
13                  Runnable mg = new MethodGenerator();
14                  MgExecutor.execute(mg);
15              }
16          }
17
18      public class MethodGenerator {
19          public void run() {
20              generate(this.m, this.s)
21          }
22
23          /* ... */
24      }

```

Σχήμα 9: One Thread Per Method

4.2 One Thread Per Class

We observed that some threads did not have much work to do, and finishing instantly. All those new allocations and assignments were an overhead. So, in this approach we tried to feed the threads more and we create a new thread for each class, not for each method.

```

1      public class FactGenerator {
2          private ExecutorService CgExecutor = new ThreadPoolExecutor(8, 16, 0L,
3              TimeUnit.MILLISECONDS, new LinkedBlockingQueue<Runnable>());
4              /* ... */
5
6          public void generate(sootClass) {
7              Runnable cg = new ClassGenerator();
8              CgExecutor.execute(cg);
9          }
10     }
11
12     public class ClassGenerator {
13         public void run() {
14             if (c.hasSuperclass() && !c.isInterface())
15                 _writer.writeDirectSuperclass(c, c.getSuperclass());
16             for(SootField f : c.getFields())
17                 generate(f);
18             for(SootMethod m : c.getMethods()) {
19                 Session session = new Session();
20                 Runnable mg = new MethodGenerator();
21                 MgExecutor.execute(mg);
22                 generate(m, session);
23             }
24         }
25         /* ... */
26     }

```

Σχήμα 10: One Thread Per Class

4.3 Fork-Join Framework

The fork/join framework is an implementation of the `ExecutorService` interface that helps you take advantage of multiple processors. It is designed for work that can be broken into smaller pieces recursively. The goal is to use all the available processing power to enhance the performance of your application.

The center of the fork/join framework is the `ForkJoinPool` class, an extension of the `AbstractExecutorService` class. `ForkJoinPool` implements the core work-stealing algorithm and can execute `ForkJoinTask` processes.

The idea of using the fork/join framework is to write code that performs a segment of the work. The basic structure should be like the following pseudocode. [3]

```

1      if (my portion of the work is small enough) {
2          do the work directly
3      } else {
4          split my work into two pieces
5          invoke the two pieces and wait for the results
6      }

```

Σχήμα 11: Fork-Join Basic-Use

```

1      public class FactGenerator {
2          private ForkJoinPool classGeneratorPool = new ForkJoinPool();
3          /* ... */
4          public void generate(sootClass) {
5              if (c.hasSuperclass() && !c.isInterface())
6                  _writer.writeDirectSuperclass(c, c.getSuperclass());
7              for(SootClass i : c.getInterfaces())
8                  _writer.writeDirectSuperinterface(c, i);
9              for(SootField f : c.getFields())
10                 generate(f);
11              if (c.getMethods().size() > 0) {
12                  ClassGenerator classGenerator = new ClassGenerator(_writer,
13                      _ssa, c, 0, c.getMethods().size());
14                  classGeneratorPool.invoke(classGenerator);
15              }
16          }
17      }
18
19      public class ClassGenerator {
20          /* ... */
21          public void compute() {
22              List<SootMethod> sootMethods = _sootClass.getMethods();
23              /* if (my portion of the work is small enough) */
24              if (_to - _from < threshold) {
25                  for (int i = _from ; i < _to ; i++) {
26                      SootMethod m = sootMethods.get(i);
27                      Session session = new Session();
28                      generate(m, session);
29                  }
30              } else { /* split work*/
31                  int half = (_to - _from)/2;
32                  ClassGenerator c1 = new ClassGenerator(_writer, _ssa,
33                      _sootClass, _from, _from + half);
34                  ClassGenerator c2 = new ClassGenerator(_writer, _ssa,
35                      _sootClass, _from + half, _to);
36                  invokeAll(c1, c2);
37              }
38          }
39          /* ... */
40      }

```

Σχήμα 12: Fork-Join Framework

4.4 Multiple Classes Per Thread

Similar as the second approach, but insted of having one thread per class, now we have one thread per multiple classes. Some threads in the previous approaches did not have much work to do.

```

1      public class Driver {
2          public Driver(ThreadFactory factory, boolean ssa, int totalClasses) {
3              _factory = factory;
4              _ssa = ssa;
5              _classCounter = 0;
6              _sootClasses = new ArrayList<>();
7              _totalClasses = totalClasses;
8              _cores = Runtime.getRuntime().availableProcessors();
9              _executor = new ThreadPoolExecutor(_cores/2, _cores, 0L,
              TimeUnit.MILLISECONDS, new
              LinkedBlockingQueue<Runnable>());
10         }
11
12         public void doInParallel(List<SootClass> sootClasses) {
13             for(SootClass c : sootClasses)
14                 generate(c);
15             _executor.shutdown();
16             _executor.awaitTermination(Long.MAX_VALUE,
              TimeUnit.NANOSECONDS);
17         }
18
19         void generate(SootClass _sootClass) {
20             _classCounter++;
21             _sootClasses.add(_sootClass);
22             if ((_classCounter % _classSplit == 0) || (_classCounter +
              _classSplit-1 >= _totalClasses)) {
23                 Runnable runnable = _factory.newRunnable(_sootClasses);
24                 _executor.execute(runnable);
25                 _sootClasses = new ArrayList<>();
26             }
27         }
28     }
29
30     public class ThreadFactory {
31         /* ... */
32         public Runnable newRunnable(List<SootClass> sootClasses) {
33             if (_makeClassGenerator)
34                 return new FactGenerator(_factWriter, _ssa, sootClasses);
35             else
36                 return new FactPrinter(_ssa, _toStdout, _outputDir, _printWriter,
              sootClasses);
37         }
38     }

```

Σχήμα 13: Multiple Classes Per Thread

5. LOCKING

Threads and locks blah blah blah

5.1 Type Assigner

Lock before applying Type Assigner, unlock afterwards.

```

1      lock.lock();
2      PackManager.v().getTransform("jb.tr").apply(b);
3      lock.unlock();

```

Σχήμα 14: JimpleBodyPack.java

5.2 Fact Writer

5.2.1 CSVDatabase

Lock files, to prevent more than one threads to write to the same file.

```

1      synchronized(predicateFile) {
2          Writer writer = getWriter(predicateFile);
3          addColumn(writer, arg, shouldTruncate);
4          for (Column col : args)
5              addColumn(writer.append(SEP), col, shouldTruncate);
6          writer.write(EOL);
7      }

```

Σχήμα 15: CSVDatabase.java

5.2.2 Representantion

Lock files, to prevent more than one threads to write to the same file.

```

1      public synchronized String signature(SootMethod);
2      public synchronized String handler(SootMethod, Trap, Session);
3      public synchronized String compactMethod(SootMethod);

```

Σχήμα 16: Representantion.java

5.3 Pack Manager

Lock before retrieving Class Hierarchy Analysis, unlock afterwards.

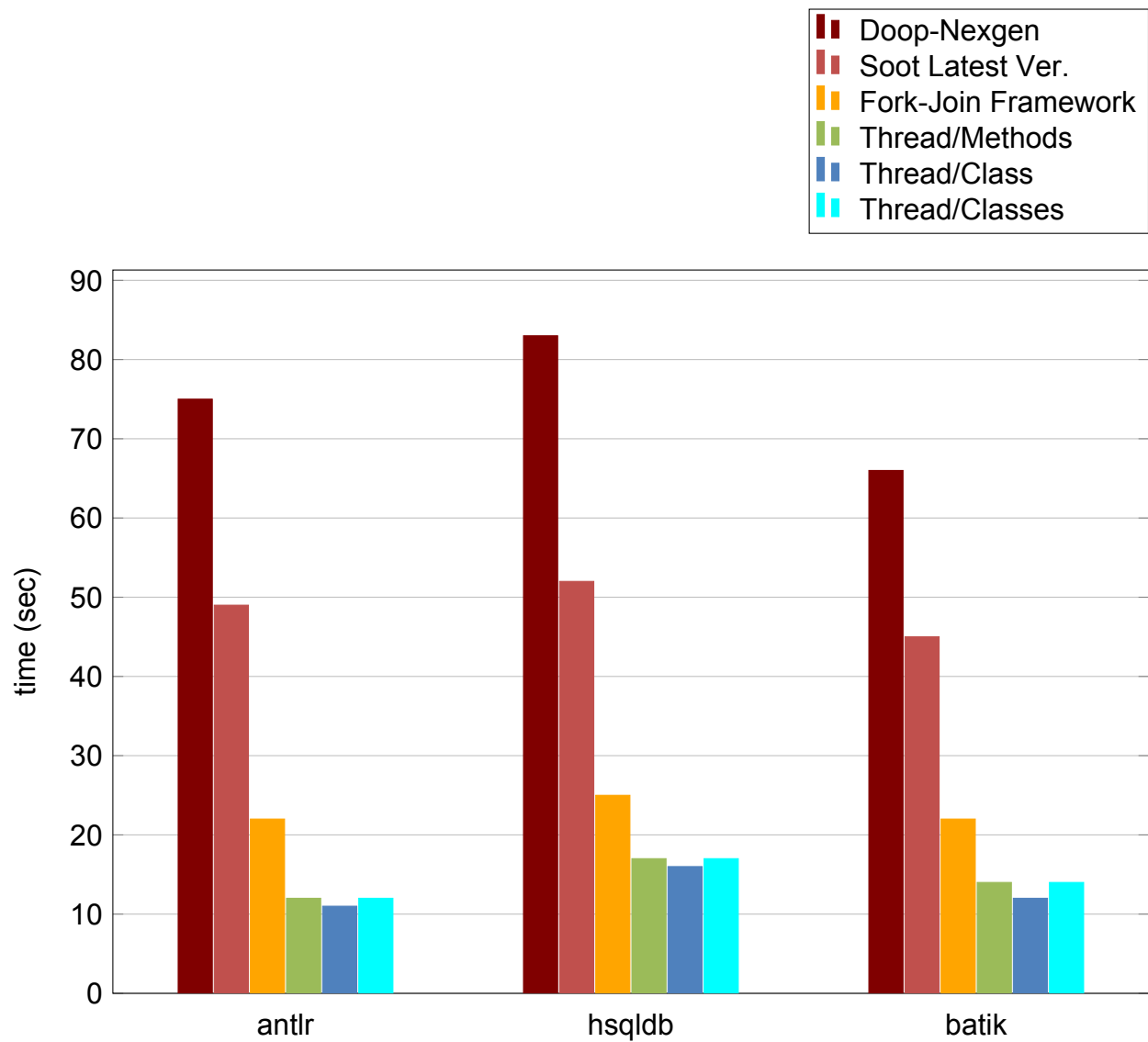
```
1      lock.lock();
2      p.add(new Transform("cg.cha", CHATransformer.v()));
3      p.add(new Transform("cg.spark", SparkTransformer.v()));
4      p.add(new Transform("cg.paddle", PaddleHook.v()));
5      lock.unlock();
```

Σχήμα 17: PackManager.java

5.4 Shimple -ssa

Synchronize all Shimple-Body-creation methods.

6. TIME RESULTS



Σχήμα 18: Fact Generation Time Results

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ακολουθεί δείγμα πίνακα ορολογίας.

κλάση	class
εντολή	command
περιβάλλον	environment

ABBREVIATIONS

NP	Non-deterministic polynomial time
----	-----------------------------------

REFERENCES

- [1] "Doop: Framework for Java Pointer Analysis" [Online] Available: <http://doop.program-analysis.org/>
- [2] "Sable: Soot" [Online] Available: <https://sable.github.io/soot/>
- [3] "Oracle Java Fork/Join Framework" [Online] Available: <https://docs.oracle.com/javase/tutorial/essential/concurrency/forkjoin.html>