ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Doop-Soot: Parallel Fact Generation

Μούρης Δημήτριος

Επιβλέπων: **Σμαραγδάκης Γιάννης**, Καθηγητής ΕΚΠΑ

ΑΘΗΝΑ

ΣΕΠΤΕΜΒΡΗΣ 2016

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Doop-Soot: Parallel Fact Generation

Μούρης Δημήτριος
1115201200114: 1115201200114

ΕΠΙΒΛΕΠΩΝ: **Σμαραγδάκης Γιάννης,** Καθηγητής ΕΚΠΑ

ΠΕΡΙΛΗΨΗ

Παραλληλοποίηση του Fact Generation του Doop. Το Doop χρησιμοποιείται για μπλαμα-πλπαλαμπλ

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Τεκμηρίωση

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

Πανεπιστήμιο Αθηνών

ABSTRACT

In this paper, we provide documentation for the LaTeX document class dithesis, which can be used for preparing undergraduate theses at the Department of Informatics and Telecommunications, University of Athens. The class conforms to all requirements imposed by the Library, as of September 2011. My thesis, which was based on the dithesis class, was accepted by the Library sometime during the summer semester of 2011.

SUBJECT AREA: Documentation

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

University of Athens

Αφιέρωση σε κάποιους.

ΕΥΧΑΡΙΣΤΙΕΣ

Ακολουθεί δείγμα ευχαριστιών.

Θα ήθελα να ευχαριστήσω τον επιβλέποντα κ. Αλέξη Δελή για τη συνεργασία και τη βοήθεια κατά την εκπόνηση αυτής της πτυχιακής.

Θα ήθελα επίσης να ευχαριστήσω το φίλο μου Μένιο για τις πολύτιμες παρατηρήσεις του σε προκαταρκτικές εκδόσεις του κειμένου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Το παρόν έγγραφο δημιουργήθηκε στην Αθήνα, το 2016, στα πλαίσια της τεκμηρίωσης της κλάσσης LaTeX dithesis. Η κλάσση αυτή διανέμεται με την ελπίδα ότι θα αποδειχθεί χρήσιμη, παρόλα αυτά *χωρίς καμιά εγγύηση*: χωρίς ούτε και την σιωπηρή εγγύηση εμπορευσιμότητας ή καταλληλότητας για συγκεκριμένη χρήση. Για περισσότερες λεπτομέρειες, ανατρέξτε στην άδεια LaTeX Project Public License.

1. ΕΙΣΑΓΩΓΗ

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.

2.1 Fact Generation

Doop before running a pointer or points-to analysis, intergrates 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

Πίνακας 1: Soot 2.5.0 times

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.

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.

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 convinient 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. The local variables which start with a $ sign represent stack positions.

The code of the program to analyze is called Application Code. Soot loads Basic Java classes and then specific Application classes. Then, an interface is created between Java bytecode and Soot (ClassSource) and starts resolving class source and produce sootClasses. These objects is used later to get the Jimple representation of a Class. So, if during an analysis with soot the Jimple code was not already generated, soot will call getActiveBody() to compute Jimple.

4. FOUR APPROACHES

Abstract: Linear Fact Generation

```
public class FactGenerator {
    /* ... */

    public void generate(sootClass) {
        if (c.hasSuperclass() && !c.isInterface () )
            _writer .writeDirectSuperclass(c, c.getSuperclass());
        for (SootField f : c.getFields () )
            generate(f);
        for (SootMethod m : c.getMethods()) {
            Session session = new Session();
            generate(m, session);
        }
    }

    public void generate(SootMethod m, Session session) {
        /* ... */

        /* This instruction spends more than 80% of FG time */
        m.retrieveActiveBody()

        /* ... */
    }

    /* ... */
}
```

4.1 One Thread Per Method

```
public class FactGenerator {
    private ExecutorService MgExecutor = new ThreadPoolExecutor(8, 16, 0L,
        TimeUnit.MILLISECONDS, new LinkedBlockingQueue<Runnable>());
    /* ... */

    public void generate(sootClass) {
        if (c.hasSuperclass() && !c.isInterface () )
            _writer .writeDirectSuperclass(c, c.getSuperclass());
        for (SootField f : c.getFields () )
            generate(f);
        for (SootMethod m : c.getMethods()) {
            Session session = new Session();
```

```
                Runnable mg = new MethodGenerator();
                MgExecutor.execute(mg);
            }
        }
    }

    public class MethodGenerator {
        public void run() {
            generate(this.m, this.s)
        }

        /* ... */
    }
```

4.2 One Thread Per Class

```
    public class FactGenerator {
        private ExecutorService CgExecutor = new ThreadPoolExecutor(8, 16, 0L,
            TimeUnit.MILLISECONDS, new LinkedBlockingQueue<Runnable>());
        /* ... */

        public void generate(sootClass) {
            Runnable cg = new ClassGenerator();
            CgExecutor.execute(cg);
        }
    }

    public class ClassGenerator {
        public void run() {
            if (c.hasSuperclass() && !c.isInterface())
                _writer.writeDirectSuperclass(c, c.getSuperclass());
            for (SootField f : c.getFields())
                generate(f);
            for (SootMethod m : c.getMethods()) {
                Session session = new Session();
                Runnable mg = new MethodGenerator();
                MgExecutor.execute(mg);
                generate(m, session);
            }
        }

        /* ... */
    }
```

4.3 Fork-Join Framework

```
public class FactGenerator {
    private ForkJoinPool classGeneratorPool = new ForkJoinPool();
    /* ... */

    public void generate(sootClass) {
        if (c.hasSuperclass() && !c.isInterface ())
            _writer.writeDirectSuperclass(c, c.getSuperclass());
        for (SootClass i : c.getInterfaces ())
            _writer.writeDirectSuperinterface(c, i);
        for (SootField f : c.getFields ())
            generate(f);
        if (c.getMethods().size() > 0) {
            ClassGenerator classGenerator = new ClassGenerator(_writer, _ssa, c,
                0, c.getMethods().size());
            classGeneratorPool.invoke(classGenerator);
        }
    }
}

public class ClassGenerator {
    /* ... */

    public void compute() {
        List<SootMethod> sootMethods = _sootClass.getMethods();
        /* if (my portion of the work is small enough) */
        if (_to - _from < threshold) {
            for (int i = _from ; i < _to ; i++) {
                SootMethod m = sootMethods.get(i);
                Session session = new Session();
                generate(m, session);
            }
        } else { /* split work*/
            int half = (_to - _from)/2;
            ClassGenerator c1 = new ClassGenerator(_writer, _ssa, _sootClass,
                _from, _from + half);
            ClassGenerator c2 = new ClassGenerator(_writer, _ssa, _sootClass,
                _from + half, _to);
            invokeAll(c1, c2);
        }
```

```
            }

            /*   ...   */
        }
```

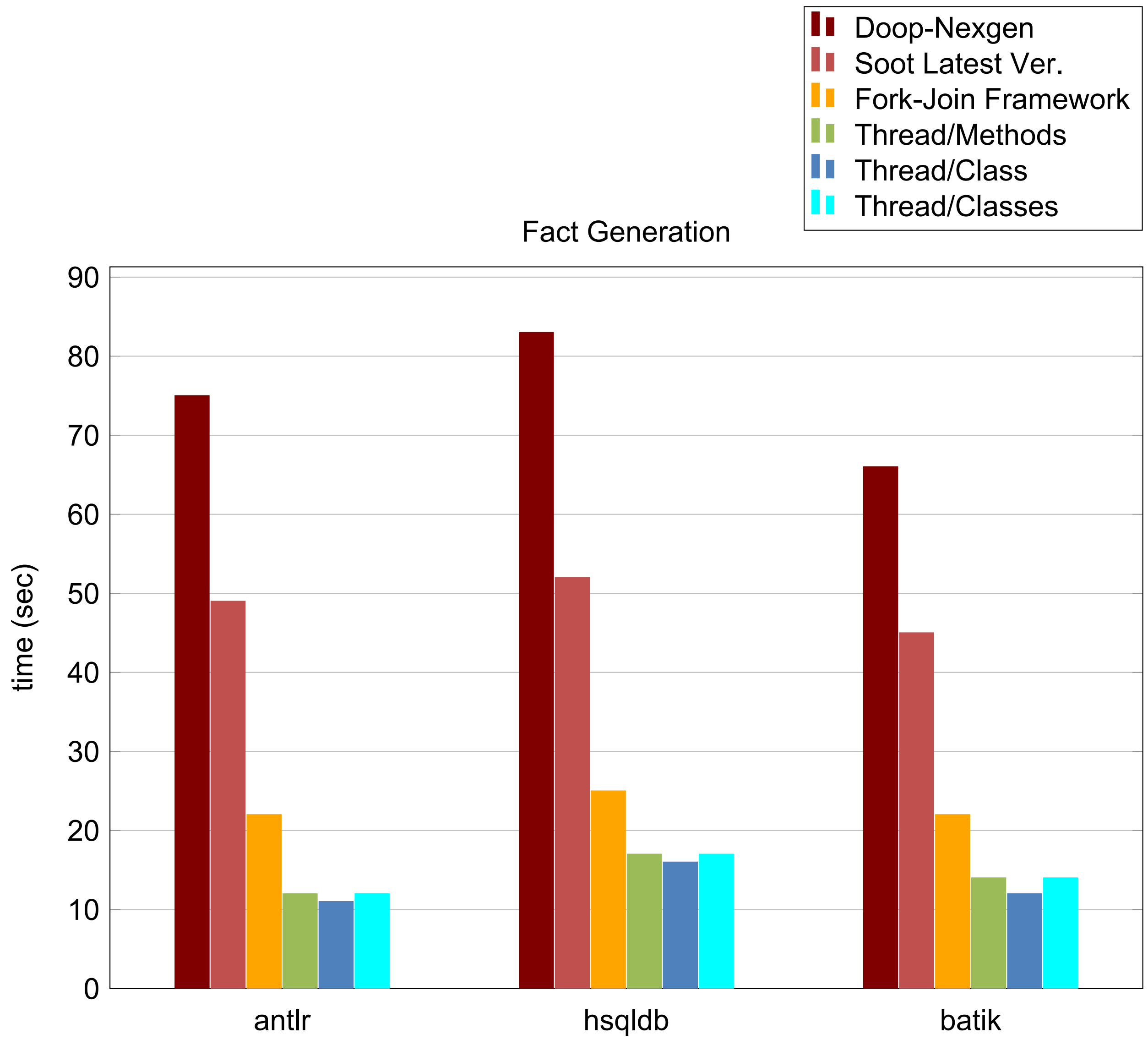
4.4 One Thread Per Classes

Similar as the second approach, but insted of having one thread per class, now we have one thread per multiple classes.

5. LOCKING

Threads and locks blah blah blah

6. TIME RESULTS


Doop-Nexgen
Soot Latest Ver.
Fork-Join Framework
Thread/Methods
Thread/Class
Thread/Classes
Fact Generation
time (sec)
antlr
hsqldb
batik