



b
**UNIVERSITÄT
BERN**

Where does this null come from ?

Bachelor Thesis

Lina Tran

from

Biel/Bienne BE, Switzerland

Faculty of Science
University of Bern

31. July 2016

Prof. Dr. Oscar Nierstrasz

Research assistant Nevena Milojković

Research assistant Boris Spasojević

Software Composition Group

Institute for Computer Science
University of Bern, Switzerland

Abstract

A previous study found out that `NullPointerException`s are very serious in Java projects. When a `NullPointerException` occurs the developer is provided only with a stack trace to where the exception happened. This only gives insight into the effect of the fault but not into its cause. So we have to ask the question when and why this reference was set to null.

The aim of the project is to be able to provide the user with an additional stack trace of where the value was actually set to null, next to the normal stack trace of an exception. We attempt to achieve this goal by instrumenting java source code ideally with a minimal overhead.

By tracking the null assignments the debugging after a `NullPointerException` will be simplified.

Contents

1	Introduction	1
2	Technical Background	3
2.1	Javassist	3
2.2	JAD	6
3	NullSpy	7
3.1	High level overview/Rough Scheme	7
3.2	Low level overview	8
3.2.1	Method Receiver Data Collection	9
3.2.2	Variable Data Collection	10
3.3	Challenges	12
3.3.1	Obtaining Method Receiver Data Difficulties	12
3.3.2	Obtaining Variable Data Difficulties	12
3.4	Limitations	13
4	Validation	14
4.1	JHotDraw	14
5	Conclusion and Future Work	15
6	Anleitung zu wissenschaftlichen Arbeiten	16

1

Introduction

Nowadays, certainly every programmer is confronted with `NullPointerExceptions` in big Java Projects, whether it is for an enterprise or for private purposes. Not to mention even in small Java Projects they are also heavily present.

So what are those `NullPointerExceptions`? This thesis is going to attach importance to Java that is a concurrent, class-based, object-oriented programming language. We chose Java because `NullPointerExceptions` are more serious in this language than in others, e.g. Smalltalk. `NullPointerException` is a `RuntimeException`. In Java, an object reference can be assigned with a special null value. The exception is thrown when an application attempts to use an object reference that has the null value. (There are multiple ways this exception can be thrown, like: Calling an instance method on the object referred by a null reference; Accessing or modifying an instance field of the object referred by a null reference and so on.) In Java Projects developers always have to deal with a huge amount of references which means avoiding these `NullPointerExceptions` is as good as impossible.

On regular meetings among programmers they report what they have been doing and what they are planning to do for the next few weeks. But all too often it is stated that they are trying to fix bugs or have spent a lot of time fixing them. If there would be a way to minimize the time fixing exceptions and allow to work more efficiently, projects would progress much faster.

The main goal of the NullSpy application takes a step to that ideal vision. Anytime

developers are facing a `NullPointerException` they don't have to spend time on debugging finding where and why a reference was set to null. With `NullSpy` the exact location of the null assignment is shown next to the ordinary stack trace the Java virtual machine produces.

In this thesis it is explained how the goal mentioned above is achieved step by step, by using a class library `Javassist` (Java Programming Assistant) which allows us to deal with Java bytecode.

2

Technical Background

This chapter provides a short overview of works/technologies used in this project.

2.1 Javassist

Javassist or Java Programming Assistant¹, a subproject of Jboss, is a class library which allows you to deal with Java bytecode. Since 1999 it is used as an engineering toolkit in a broad domain, and is still being extended by Shigeru Chiba. It enables developers to manipulate Java bytecode in a simplified way like defining a new class at runtime or modifying a class file when it is loaded by the JVM. All manipulations are performed at load-time through a provided class loader.

¹<http://jboss-javassist.github.io/javassist/>

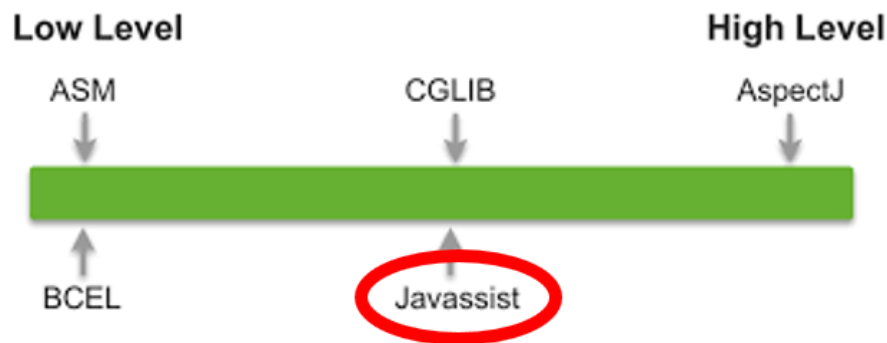


Figure 2.1: Bytecode modification levels

Unlike many other libraries Javassist offers two levels of API: source level and bytecode level (See figure 2.1). Using the source-level API, the user can edit a class file without any familiarity with the specifications of the Java bytecode. Only knowing the Java language is enough because the API is designed only with the vocabulary of Java. On this level the programmer just has to write normal source code and Javassist compiles it automatically. The bytecode level allows the user to modify classes directly in binary form like other editors, e.g. ASM.

At this point, let us look at a small example to give you an idea how the bytecode manipulation works.

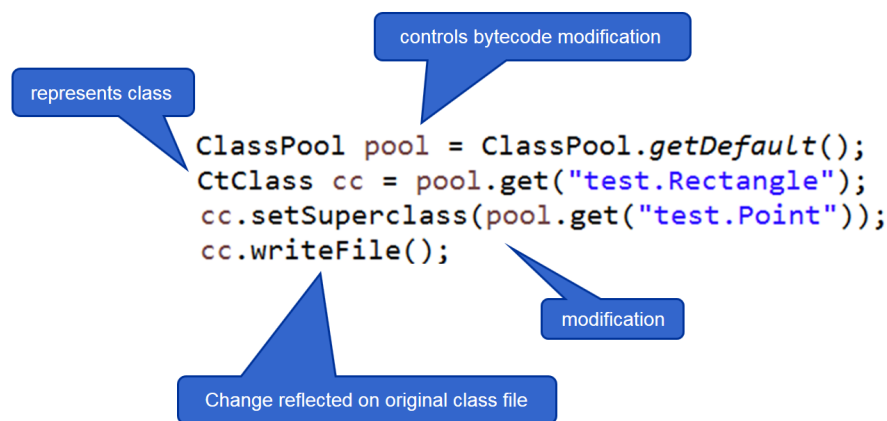


Figure 2.2: Javassist example

First a `ClassPool` object is obtained that controls bytecode modification with Javassist. With the `ClassPool` a class file can be read on demand for constructing a `CtClass` object.

The class `CtClass` (compile-time class) is just an abstract representation of a class file which means all manipulations are performed on the `CtClass`. With the method invocation `get()` on `ClassPool` a reference to the class file `test.Rectangle` is obtained. In this example the superclass of `test.Rectangle` is just changed to `test.Point`. If the changes are done, the method call `writeFile()` on `CtClass` is necessary to make sure that the changes are reflected on the original class file.²

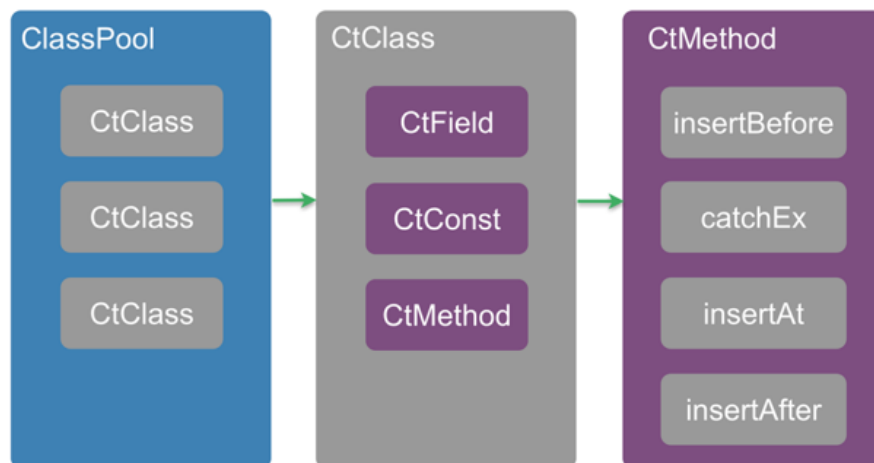



Figure 2.3: Javassist Modules

Figure 2.3 gives you an understanding/overview how the main part of bytecode manipulation with Javassist is built up. The `ClassPool` is nothing else than a container of multiple `CtClasses`. As described before `CtClass` is just the abstract representation of a class file on which modifications are done. Like typical classes, it can hold several compile-time fields, constants or methods. While speaking about bytecode manipulation all the time, nothing but editing methods is mainly meant. It is possible to insert additional source code at the beginning of the method body, at the end or at a specific line. Next to these options even a *catchBlock* can be added.

²Getting started with Javassist: <http://jboss-javassist.github.io/javassist/tutorial/tutorial.html>

```
method.insertAt(8,
    "runtimeSupporter.NullDisplayer.test( \""
        + method.getDeclaringClass().getName() + "\", "
        + variableName + ");");
```



```
ch.unibe.scg.nullSpy.runtimeSupporter.NullDisplayer.test(
    "className", variable);
```

Figure 2.4: Inserting code example

2.2 JAD

Java Decompiler³ is a decompiler and a Eclipse plugin for the programming language Java. A short explanation what a decompiler is: a computer program that takes an executable file as input, and attempts to create a high level, compatible source file that does the same thing. So it is used in software reverse engineering.

```
// Method descriptor #28 ([Ljava/lang/String;)V
// Stack: 2, Locals: 13
public static void main(java.lang.String[] args) {
    0  getstatic java.lang.System.out : java.io.PrintStream
    3  ldc <String "\nMethod main starts."> [35]
    5  invokevirtual java.io.PrintStream.println(java.lang.
    8  aconst_null
    9  putstatic isFieldOrLocalVariableNullException.Main:11
    12 aconst_null
    13 astore_1 [d]
    14 aconst_null
    15 astore_1 [d]
    16 getstatic isFieldOrLocalVariableNullException.Main:19
    19 putstatic isFieldOrLocalVariableNullException.Main:20
    22 aload_1 [d]
    23 putstatic isFieldOrLocalVariableNullException.Main:21
    26 getstatic isFieldOrLocalVariableNullException.Main:24
    29 astore_1 [d]
    30 aconst_null
    31 astore_2 [d2]
    32 aload_2 [d2]
    33 astore_1 [d]
    34 new isFieldOrLocalVariableNullException.Person [45]
    37 dup
    38 invokespecial isFieldOrLocalVariableNullException.Person() [47]
    41 astore_3 [p]
    42 new isFieldOrLocalVariableNullException.Person [45]
    45 dup
    46 invokespecial isFieldOrLocalVariableNullException.Person() [47]
    49 putstatic isFieldOrLocalVariableNullException.MainAssignToNull.o : isFieldOrLocalVariableNullException.Person [48]
    52 invokestatic isFieldOrLocalVariableNullException.Person.say() : java.lang.Object [50]
    55 checkcast isFieldOrLocalVariableNullException.Person [45]
    58 astore_4 [p2]
```

```
3 public class MainAssignToNull {
4     public static Object o = null;
5     public static Object b;
6     public static Object c;
7     public static Integer i;
8     public static NullObject nul(Object);
9     public static Person o;
10
11     public static void main(String[] args) {
12         // long startLine = System.nanoTime();
13
14         System.out.println("\nMethod main starts.");
15
16         o = null;
17         Object d = null;
18         d = null;
19
20         b = o;
21         o = o;
22         d = o;
23         Object d2 = null;
24         d = d2;
25
26         Person p = new Person();
27         o = new Person();
28         Person p2 = (Person) Person.say();
29         p.o = null; // aload, aconst, putfield Person.o
```

Figure 2.5: Decompile example

JAD is used in NullSpy since after running NullSpy on a project only the modified bytecodes are available. To simplify the check whether the modification by Javassist, e.g. inserting source code, has succeeded, a decompiler is needed.

³<https://sourceforge.net/projects/jadclipse/>

3

NullSpy

As earlier explained in the introduction (1), this project is about providing the user with additional stack trace where the origin of a `NullPointerException` is actually rooted. Briefly worded, it shows the developer the exact location of where a method receiver, which causes the NPE, was assigned to null.

This is the main chapter of the thesis. Here we would like to give you a short insight of how we managed to successfully implement the core of the project NullSpy. Next to how it is built up, we will also let you know what challenges we were encountering during the implementation and about the limitations we planned for future work (5).

3.1 High level overview/Rough Scheme

The general approach of NullSpy is to statically analyze and add additional bytecode to a project. After reading the section Javassist (2.1) you should be more familiar with how bytecode manipulation with Javassist works.

What NullSpy first does is loading the project you want it to be able to track the null assignment if a `NullPointerException` is thrown. By loading the project to NullSpy, the compiled class files of the project are addressed only, which means the project itself does not have to be imported to the programming environment, e.g. Eclipse. Simultaneously at

load time each class file is modified with help of Javassist; In what way will be discussed in the following section Low level overview.

Once the project modification is done it is stored in a destination folder that the user has chosen before. This means after the changes there will be another version of the project which can do additional stuff like tracking the null assignment. Because only the class files are accessed previously, the result which is stored in the destination folder is as expected only the modified bytecode.

How do we check whether the instrumentation worked and the project really tracks the null assignment? The answer is wrapping the modified project into a jar file with which the modified project can be executed in the terminal or in Eclipse.

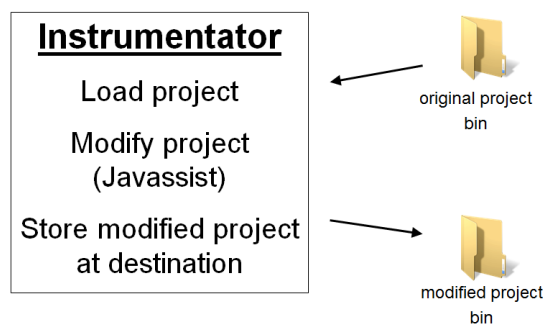


Figure 3.1: Modification overview

3.2 Low level overview

So we first load the project which should be modified and then go through all class files of it. A `NullPointerException` can only be thrown if a method call was performed on a method receiver which is null. That means we have to gather information about the method receiver. To know the exact location of the null assignment of course we also have to collect information about the variable assignments.

The main idea behind NullSpy actually is to get information about method receivers and information about the variables on one side and comparing those together if a `NullPointerException` occurs on the other side. If there is a hit on the matching the null assignment location can be obtained easily.

3.2.1 Method Receiver Data Collection

Unfortunately, Javassist does not provide the function to directly get the method receiver. We got a suggestion to use AST (Abstract Syntax Tree footnote wiki) to get it but we decided to not go deeper into this and implement our own algorithm.

The algorithm contains following steps (abstract):

1. Getting pc-interval of method invocation
2. Storing all possible method receiver interval within the interval of step 1 into an ArrayList
3. Getting the number of parameters, the method invocation takes
4. Traversing back the ArrayList the amount of parameters obtained in step 3
5. Result: method receiver interval
6. Store variable name, type etc. into an external csv file

In step 1 we had big troubles getting the right interval of the method receiver because only by statically analyzing the bytecode it is unapparent where the method receiver is situated exactly. But more about the challenges you will learn more in chapter 3.3.1.

Statically analyzing bytecode for method receiver means looking for certain opcodes which matches all opcodes that matches with the regex `"invoke.*"`. There are exactly five kinds of bytecode instruction: *invokedynamic*, *invokeinterface*, *invokespecial*, *invokestatic*, *invokevirtual*. The invocation opcode *invokedynamic* facilitates the dynamic-typed languages¹ through dynamic method invocation. In our case it can be ignored because NullSpy only supports the static-typed language² Java.

In case of the *invokestatic* instruction we do not have a method receiver. That is why NullSpy treats it extraordinary like ignoring it completely or wrap it as a possible method receiver when it is actually a parameter of a method invocation. In all other cases we normally use the algorithm to get the method receiver.

¹Language whose type checking is usually performed at runtime.

²Language whose type checking is performed at compile time.

3.2.2 Variable Data Collection

While going through the bytecode attention is paid to some opcodes³. Right after each keyword that indicates a variable assignment we insert some bytecode. The inserted code represents a test method which tests whether the value of the assigned variable is null or not and store some information about it. Unlike in getting information about the method receiver in subsection 3.2.1 the data about the variables are stored in a HashMap.

What kind of opcodes were NullSpy looking for? For instance or class/static variables the bytecode instruction *getfield* and *getstatic* were essential, for local variables the important opcodes were those which matches the regex *"aload.*"*. Due to different types of variables and the limitation of Javassist gathering information about them was performed differently. Again getting the necessary data about the variables we encountered many difficulties which will be discussed in the subsection 3.3.

Unfortunately, Javassist does not provide any support for gaining information about local variables that is why getting the needed data we had to understand how bytecode is constructed. At this point we would like to give you a small bytecode introduction.

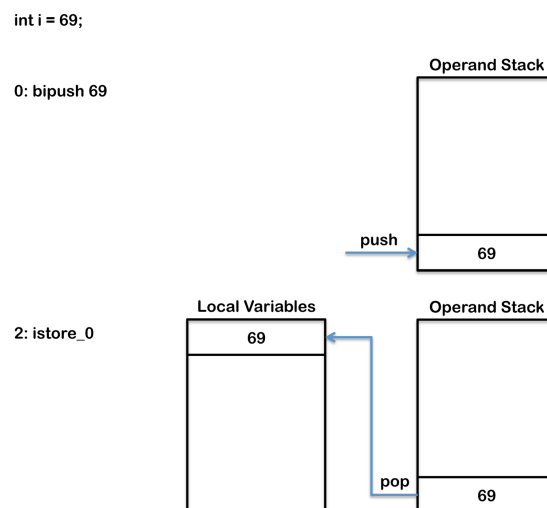


Figure 3.2: Local variable creation bytecode⁴

If a local variable is created, the value assigned to it is pushed onto the operand stack. With the bytecode instruction *".*store.*"* the local variable is popped from the operand stack and stored into a local variable array slot. In which slot it is stored can be extracted from the instruction. Opcodes for storing local variables is composed of one, or in some

³Operation code: Machine language instruction.

cases two bytes. There are reserved machine commands for the first four local variables, index-linked from 0 to 3 and each of them contains one byte (astore_0, astore_1, astore_2, astore_3). If there is no slot number visible in the instruction, it indicates that the slot number is stored in the second byte from where it can be extracted. Next to storing the local variable loading it from the local variable array is possible to, but only with the local variable slot number.

With this short introduction understanding the local variable table should be easier. Each method of a class file contains a local variable table (see figure 3.3) with which many information can be read out of it, e.g. the lifespan of the local variable, what it is called, in which slot it is stored and what type it has.

Local variable table:

```
[pc: 0, pc: 31] local: this index: 0 type: org.jhotdraw.samples.javadraw.JavaDrawApp
[pc: 0, pc: 31] local: newDrawing index: 1 type: org.jhotdraw.framework.Drawing
[pc: 5, pc: 31] local: d index: 2 type: java.awt.Dimension
[pc: 22, pc: 31] local: newDrawingView index: 3 type: org.jhotdraw.framework.DrawingView
```

Figure 3.3: Local variable table

We had to pay attention to be sure to get the right local variable. Every time when we bumped into the opcode `".*store.*"` we could only get its slot and the `pc`⁵ where it is situated in the bytecode sequence. In the earlier paragraph the lifespan of the local variable was mentioned, the importance behind this is as soon as the lifespan of one ends, the slot can be reused by the next instantiated local variable. This way, the local variable table could contain multiple entries with the same local variable slot.

Local variable table:

```
[pc: 0, pc: 456] local: args index: 0 type: java.lang.String[]
[pc: 16, pc: 456] local: m index: 1 type: isFieldOrLocalVaria
[pc: 18, pc: 456] local: i index: 2 type: int
[pc: 31, pc: 38] local: k index: 3 type: java.lang.Object
[pc: 44, pc: 456] local: d index: 3 type: java.lang.Object
[pc: 63, pc: 456] local: d2 index: 4 type: java.lang.Object
```

Figure 3.4: Local variable table entries with same slot

After extracting the slot of the local variable we will get the first local variable table entry which contains that slot. If the `pc` of the local variable assignment is not included

⁵Program counter/instruction pointer: A processor register that indicates where a computer is in its program sequence.

in the lifespan-pc-interval of the entry, the next entry with the same slot will be checked until both criteria (slot and pc) fits. Once those criteria are met we can be positive about having got the right local variable table entry to extract the information needed.

Next to the local variable table each methods of a class file also holds another attribute called line number attribute. This is just the mapping table from pc to source code line number. Since encountering the storing keyword the pc is available , with help of it the line number can be easily obtained.

```
Line numbers:
[pc: 0, line: 27]
[pc: 8, line: 28]
[pc: 16, line: 29]
[pc: 18, line: 30]
```

Figure 3.5: Line number table

There was a big problem about inserting additional source code after assignments in certain situations. It is mainly caused by the limitation of the class library Javassist (see 3.3.2).

3.3 Challenges

..

3.3.1 Obtaining Method Receiver Data Difficulties

bla bla

...

3.3.2 Obtaining Variable Data Difficulties

bla bla

...

3.4 Limitations

...

4

Validation

In which you show how well the solution works.

4.1 JHotDraw

JHotDraw To check whether the logic of the bytecode manipulation in this project NullSpy is working as desired, we had to perform them on a large working project. Thanks to Nevena Milojković and her experience with the combination Javassist and JHotDraw we as well decided to test NullSpy on the project JHotDraw. It is an open-source Java GUI framework for technical and structured Graphics. Its original authors have been Erich Gamma and Thomas Eggenchwiler.

5

Conclusion and Future Work

In which we step back, have a critical look at the entire work, then conclude, and learn what lays beyond this thesis.

6

Anleitung zu wissenschaftlichen Arbeiten

This consists of additional documentation, e.g. a tutorial, user guide etc. Required by the Informatik regulation.

Bibliography

”Ich erkläre hiermit, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls der Senat gemäss Artikel 36 Absatz 1 Buchstabe r des Gesetzes vom 5. September 1996 über die Universität zum Entzug des auf Grund dieser Arbeit verliehenen Titels berechtigt ist.