Constraint-Based Test Input Generation for Java Bytecode
Florence Charreteur, Arnaud Gotlieb

To cite this version:
Florence Charreteur, Arnaud Gotlieb. Constraint-Based Test Input Generation for Java Bytecode. Proc. of the 21st IEEE Int. Symp. on Softw. Reliability Engineering (ISSRE’10), Nov 2010, San Jose, CA, USA, United States. hal-00699236

HAL Id: hal-00699236
https://inria.hal.science/hal-00699236
Submitted on 21 May 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Constraint-based test input generation for Java bytecode

Florence Charreteur
Universite de Rennes 1
Rennes, France
Florence.Charreteur@irisa.fr

Arnaud Gotlieb
INRIA Rennes Bretagne Atlantique
Rennes, France
Arnaud.Gotlieb@irisa.fr

Abstract—In this paper, we introduce a constraint-based reasoning approach to automatically generate test input for Java bytecode programs. Our goal-oriented method aims at building an input state of the Java Virtual Machine (JVM) that can drive program execution towards a given location within the bytecode. An innovative aspect of the method is the definition of a constraint model for each bytecode that allows backward exploration of the bytecode program, and permits to solve complex constraints over the memory shape (e.g., p == p.next enforces the creation of a cyclic data structure referenced by p).

We implemented this constraint-based approach in a prototype tool called JAUT, that can generate input states for programs written in a subset of JVM including integers and references, dynamic-allocated structures, objects inheritance and polymorphism by virtual method call, conditional and backward jumps. Experimental results show that JAUT generate test input for executing locations not reached by other state-of-the-art code-based test input generators such as jCUTE, JTEST and Pex.

I. INTRODUCTION

As integrated within current development environments, automatic test input generation is a promising approach for reducing the cost of software unit testing. In particular, having an approach able to generate and check 100% code coverage of a unit under test is highly desirable for increasing our confidence in the program correctness. However, current realistic solutions for this problem do not achieve complete coverage of usual structural criteria such as all statements or all branches. In fact, modern automatic test input generators adequately sacrifice completeness for efficiency. They are able to generate test inputs for programs containing hundreds of thousands lines of code in a couple of minutes but they fail to generate complete statement coverage on simple Java methods that contain cyclic data structures, multi-level dereference aliasing problems, inter-dependent loop statements or non-linear decisions.

Although the underlying reachability problem is undecidable in the general case, it seems that there is room for code-based test input generators applying more costly methods and having the goal of completeness. Constraint-based testing, as introduced by Offutt in 1991 [1], combined symbolic execution and dynamic constraint solving [2] to generate test inputs able to execute specific paths in the code. It was then adapted for C programs and refined with standard constraint programming techniques to target specific locations in the code regardless of the particular path executed [3], [4]. Constraint-based testing was extended to the exhaustive generation of structured inputs for Java programs [5], [6] and the constraint solving of structurally complex constraints [7]. An important work in the area is also the symbolic execution approach of Java PathFinder [8] where “lazy initialization” was proposed [9].

Recent code-based test input generators such as DART [10], PathCrawler [11], CUTE and jCUTE [12], [13] or Pex [14] are based on dynamic symbolic execution. They dynamically select a feasible path by picking up a test input and by observing which instructions are executed; then, they report path conditions by symbolically evaluating the instructions along the path. Finally, by negating the last decision of path conditions and submitting the corresponding system to a constraint or an SMT\(^4\) solver, they try to infer another test input covering a distinct path. When such a test input is found, path coverage of the program is necessarily increased. Whenever path conditions are unsatisfiable, the process backtracks and selects another path to execute. Dynamic symbolic execution performs forward exploration as it visits the paths from the entry to the exit and this works fine for quickly exploring a few paths. However, when the goal is to complement an existing test set in order to increase code or branch coverage, this approach is less adapted as forward exploration can be trapped in large subspaces of the path search space. In this paper, we introduce a new constraint-based approach to generate automatically test inputs for Java bytecode programs. Our approach generates a test input under the form of a concrete state of a JVM memory, that can drive the program execution towards a selected bytecode instruction. In the context of unit testing, our approach is made to improve the statements coverage of each method under test thanks to a context-free test case generation. This paper contains two contributions:

1) unlike other approaches [10], [12], [11], [15], [14], our framework explores program paths from the target location towards the program entry point. Backward exploration at the bytecode level is not trivial as it requires the development of a kind of inverse reasoning on each bytecode instruction, that is neither available in the SUN’s JVM specifications nor in the literature. For that, we developed constraint reasoning on partial abstract memory states. For backward exploration, we also developed a depth-first strategy which takes advantage of early detection of infeasible parts of paths to prune the search space of feasible paths;

2) a new constraint-based model of the JVM is defined with the notion of constrained memory variable. This notion captures abstract memory states and permits to implement deductive rules for a meaningful subset of Java bytecode, including those dealing with objects, inheritance, polymorphism and dynamic memory management. In this model, each bytecode expresses a relation between two constrained memory variables, which contain unknown or only partially known variables associated to registers, operands stack or heap. Using constraint propagation and an existing finite domain constraint solver, this model allows decisions that involve

\(^4\)Satisfiability Modulo Theories.
cyclic data structures and reference aliasing problems such as if( p == p.next ) to be effectively solved.

We implemented our approach in a tool called JAUT (Java Automatic Unit Testing) that can generate input memory states for reaching specific locations within Java bytecode programs. Experimental results on small-sized benchmark programs, including the TreeMap Java library of red-black trees, show that JAUT can complement an existing test set with test inputs for locations not covered by other code-based test input generators such as JCUTE[12], JTEST[16] and Pex[14].

The rest of the paper is organized as follows: section 2 introduces our method on a simple example, section 3 presents the memory model we defined to generate test inputs for the JVM, section 4 explains constraint generation and constraint solving for a few bytecodes, section 5 presents the test input generation process which performs backward search across Java bytecode programs, section 6 is dedicated to our experimental validation and discussion of related work, while section 7 concludes and draws perspectives to this work.

II. DETAILED EXAMPLE

```java
class Coord {
  int x, y;
  Coord(int cx, int cy) { x = cx; y = cy; }

  public Coord moveY(Chrono chrono, int speed) {
    if(chrono.time <= 0 || speed <= 0)
      return this;
    int ytemp = y + chrono.time * speed;
    if( ytemp > 65536 )
      return new Coord(x,ytemp);
    else return new Coord(x,ytemp);
  }

  class Chrono {
    int time;
  }
}
```

Figure 1. Example in Java source code

Consider the Java program of Fig.1 that implements the class Coord standing for the Cartesian coordinates in a 2D-space. We selected this simple example just to illustrate the memory model of our constraint-based test input generation approach. Let our test objective be the generation of an input JVM state for method moveY that reaches the bytecode corresponding to the instruction i in the source code. Note that we do not pay attention to how the methods of class Coord can build such an input state that may be “invalid” if it cannot be reached from other method calls. Object-oriented languages offer ways to directly manipulate the object receiver state without using constructors and accessors (e.g., using Java reflection with setAccessible or bytecode translation) and nothing can guarantee, without additional information, that a given method will not be called from an “invalid input state”. Hence testing a program with states that may be invalid is equally important.

The bytecode program shown in Fig.2 corresponds to method moveY where bytecode 51 corresponds to the selected test objective.

2JAUT and all our experiments are freely accessible at http://www.irisa.fr/lande/gottlieb/resources/jaut.html.
Java bytecode program, currently have type `intFD`, with domain $[-268435456..268435455]$.

The constraint generation and solving process of our test input generation method aims at refining this input CMV for method `moveY` by finding values for each variable. We illustrate this process below by showing how this input CMV is successively refined to satisfy the test objective.

Our constraint solving examines each bytecode one by one in a backward fashion. On this program, there is no choice point on the backward exploration as there is only a single path going towards the program entry point. Constraint solving operates with two interleaved processes: `constraint propagation` which uses each constraint to prune the domain of CMV of its inconsistent values and `labeling`, which enumerates the possible values of CMV and launches constraint propagation until no more deduction is possible.

Those processes are not new and form the basis of finite domain constraint solving [17]. Let us just recall that all the constraints are added to a constraint propagation queue that iteratively manages each constraint one by one, and each constraint is used to prune the variation domain of its variables. At a given step of the constraint solving process, the following input CMV is produced:

```java
lin: this -<[Coord], dom=[0] ndom=[], speed -< intFD, [1..268435455]>,
    hin: 0:([Coord], [x=<intFD, [-268435456..268435455]>,
            y=<intFD, [-268435456..268435455]>)
```

The `ndom` set of reference `chrono` has increased to `[null, 0]`, meaning that `chrono` can neither be null nor points to the object pointed by `this`. These deductions come from the fact that 1) reaching location 51 in the bytecode program requires a non-null value for `chrono` as it is dereferenced several times and 2) `chrono` has to point to a `Chrono` object and not a `Coord` object. The domain of `speed` has been pruned during initial constraint propagation as constraint `speed > 0` was considered.

Next steps include the creation of object `Chrono` and the start of the `labeling` process for producing a completely instantiated CMV, suitable for test script generation. Suppose that the labeling process has instantiated `speed` to 363 and `this.y` to 5206 using a random labeling heuristic, then we get the following refined input CMV:

```java
lin: this -<[Coord], dom=[0] ndom=[]>,
    chrono -<[Chrono], dom=all ndom=[null,0]>,
    speed -< intFD, [363]>,
    hin: 0:([Coord], [x=<intFD, [-268435456..268435455]>,
            y=<intFD, [-268435456..268435455]>)
```

An object of class `Chrono` has been created and is referenced by `chrono` which has now value 1. Accordingly, the domain of `chrono.time` has been pruned to `[167..739477]` as the arithmetic constraints `ytemp = this.y + chrono.time * speed, ytemp > 65536` were considered by the underlying finite domain constraint solver.

However, the input CMV has still uninstantiated variables such as `this.x` and `chrono.time`. Therefore, the labeling process enumerates values for these variables.

So, we get:

```java
lin: this -<[Coord], dom=[0] ndom=[]>,
    chrono -<[Chrono], dom=[1] ndom=[]>,
    speed -< intFD, [363]>,
    hin: 0:([Coord], [x=<intFD, [254]>, y=<intFD, [5206]>,
            time=<intFD, [167]>])
```

This CMV characterizes an input JVM state that satisfies the test objective of reaching bytecode numbered 51 in method `moveY`. Submitting a test script derived from this state shows that the fault on the converted parameters of `new Coord(ytemp, x)` can be detected.

## III. Memory model

Java virtual machine states represent runtime data storage locations such as registers, operand stacks and heap data. This section details the representation of data types and data storage locations in our memory model. Note that our framework handles a meaningful subset of Java bytecodes, including integers and references, dynamic allocation and heap-allocated structures, objects inheritance and polymorphism, static and dynamic method invocations, conditional jumps and backward jumps. Arrays accesses and updates are only partially supported and floating-point computations, exceptions, native methods and multithreading are currently left apart.

### A. Constraint memory variable

In our memory model, constrained memory variables (CMV) are used to represent JVM states. A CMV contains data storage locations where data can be represented by variables along with a domain. Formally, a CMV $M$ is a tuple $(F, S, H)$ where $F$ denotes the set of registers, $S$ denotes the operand stack and $H$ denotes the heap. Note that several distinct CMV $M$ can be created at the same instruction number when loops are present in the bytecode. Each Java bytecode will then be seen as a relation among two CMVs: the CMV $M_j$ before activation of bytecode and the CMV $M_k$ after its activation and before the activation of the following bytecode in the considered sequence of instructions. The tuple $(F, S, H)$ contains variables and domains that are described in the rest of the section.

### B. Integer and reference variables

Finite domain variables model integer and reference variables of the program. Their default variation domain depends on the size of their precise type. For instance, the domain $-2^{31}..2^{31} - 1$ is associated to an `int` variable. Other integer types are treated accordingly. The default domain of a reference is the *all* symbolic value. This means that the reference can point to every object of the heap. When the solving process prunes the domain of the reference variable, then the domain is composed of a set of integer values, which represent all the heap addresses the reference can point to. Note that the *null* value can also be part of the domain.

\[a.k.a. local variables in the SUN JVM specifications.\]
C. Objects

Each object of the heap is modeled by a pair of elements. The first one, called type variable, represents the class of the object, the domain of which is a set of possible classes. This allows to properly handle inheritance and polymorphism. The second element is a mapping associating an integer or a reference variable to each attribute, which corresponds to the value of the attribute. Note that when the domain of the type variable contains more than one class, all the possible attributes have to be in the mapping.

For example, if a program defines two classes A and B where B inherits from A, and A defines attribute t1 and B defines attribute t2, then

\( ([A,B], [t1<-\text{intFD}, [2..5]>, t2<-\text{intFD}, [15..17]>]) \)

represents an object of class either A or B, with attribute t1 necessarily in 2..5. If the object happens to be of class B during the solving process, then its t2 attribute will belong to 15..17.

D. Registers and operand stack

In a JVM state, registers are used to store the parameters and the local variables of a method. When the method is dynamic (as opposed to static methods), the first register contains the reference to the object (this) that calls the method. The operand stack is used to perform the calculations of the method. In a CMV, we use two sequences of variables to represent registers and operand stack. As registers are numbered, the first sequence is a convenient way of implementing an indexed array. On the contrary, the sequence used for representing operand stack is accessed with a convenient way of implementing an indexed array. On the contrary, the sequence used for representing operand stack is accessed with

E. Heap

In a CMV, the JVM’s heap corresponds to a mapping from a set of addresses to a set of objects, possibly stored at these addresses. We associated a unique integer to each address without taking into consideration the actual physical addresses in the JVM. The domain of a variable \( H \) that models the heap is composed of a set of pairs, representing the mapping, and a status. 1) The set of pairs (address,object), denoted by \( C_H \), contains the objects necessarily present in the heap. During the solving process, new pairs can be added to \( C_H \) when a dynamic memory allocation bytecode is encountered (i.e., new). As our model does not model garbage collection, \( C_H \) can only be enriched, reducing the possible states of the heap. 2) The status is either closed or unclosed. A closed status of the heap denotes a set of addresses entirely known, even if some objects can still be unknown or only partially known through their domain. On the contrary, an unclosed status denotes states where memory allocation can still enrich the CMV. During the constraint solving process, status can only move from unclosed to closed. This notion is introduced to tackle cases where the input memory shape is unknown and we will have to explore the input space during labelling to find it.

IV. CONSTRAINT GENERATION AND SOLVING

In our framework, constraint generation and solving are performed altogether. This has similarities with the on-the-fly generation of paths of [11] and [14] where path conditions are incrementally tested for satisfiability. We first detail the specification of test objective (Sec. IV-A), and then we present the constraint generation and solving process (Sec. IV-B). We illustrate the constraint generation on an example (Sec. IV-C) and we explain the deduction capabilities of the constraints we have defined to model dynamic memory management (Sec. IV-D).

A. Test objective

Test input generation aims at finding an input CMV that satisfies a given test objective in a Java bytecode method. In our framework, test objectives are specified with the bytecode instruction number that corresponds to a bytecode program location. In general, for a given test objective, there are many feasible or infeasible paths that can reach the target locations. Our goal is just to find one input CMV that will drive the computation towards the selected location, whatever is the feasible path executed. Note that such a test objective potentially specifies an infinite set of dynamic locations when the bytecode instruction number is located within loops.

B. Constraint generation from the bytecode

Initially, the input CMV of the method is an unconstrained variable and the constraint generation process will accumulate and solve the constraints, for the current selected path, from the test objective to the program entry point. These constraints capture the path condition that must be satisfied to follow the current selected path and are used to prune the possible values of the input CMV. Each bytecode can potentially constrain the input CMV variable or intermediate CMV variables, throughout its behavior on the registers, operand stack or heap variables. Based on the semantics of each bytecode as defined in the SUN’s specification, we build constraints that implement deductive rules on the CMVs.

Arithmetic bytecodes such as iadd, ladd, isub, imul, idiv, irem, ineg, ... and comparison bytecodes if_icmp, if_acmp, lcmp, ..., act directly on logical variables associated with integers or references, and the elements of the operand stack. They generate arithmetical constraints on the finite domain constraint solver, depending on the type of the operands and the operator. For example, iadd generates a relation \( V_{temp} = V_a + V_b \) over two CMVs \( M_1 \) and \( M_2 \), where \( V_{temp} \) is a fresh finite domain variable associated to the top of the operand stack of \( M_2 \), while \( V_a \) and \( V_b \) are the two finite domain variable associated with the integers on the top of the stack of \( M_1 \). Other arithmetic bytecodes generate similar constraints according to the considered integer type (int or long) and operator. Comparison bytecodes are handled in a similar way by considering the arithmetic constraint extracted from the condition or from the negation of the condition. This will be made clearer in section V.

Bytecodes for simple constant pool accesses (ldc, bipush, ...) or register accesses iload, aaload, astore, astore_<n>, ... or register updates istore, astore, istore_<n>, astore_<n>, ..., generate equality constraints between the top of the operand stack and registers, depending on the type of the register variable. Equality on reference variables (when iload or astore is considered) generates a finite domain equality, as well.

To deal with bytecodes for dynamic memory management new, newarray, ... and accesses and updates of object fields getfield, putfield, ..., special constraints
have to be built. Indeed, these operations maintain complex relations between the CMVs. They can constrain the shapes of heap-allocated data structures and the contents of registers and operand stack. We detail the relations we built for only three of them, as the other can easily be deduced from these ones: 

- \text{new}(\text{class}, H0, H1, A) maintains the relation between H0 the heap of the CMV before execution and H1 the CMV after execution, and A a fresh address for the newly created object of type class.

The relation says that H1 is the updated heap H0 where reference A points to a newly allocated object.

- \text{getfield}(A, \text{Id}, H, Val) maintains the relation between the heap H, from which an access to an attribute Id of the object designated by reference A is performed and Val a finite domain variable. When reference A has for domain a set of possible references, special deductions can be performed on the possible values for Val. Conversely, using the possible values of Val, special deductions on reference A can be performed. In addition, information on the domains of variables in H allows for deductions on the domains of A and Val. This permits the implementation of powerful forward and backward constraint reasoning.

- \text{putfield}(A, \text{Id}, Val, H0, H1) is more complex as it maintains a relation between H0 and H1 the heaps of both CMVs, reference A and Val. H1 is similar to H0 except for object referenced by A where the field Id has been modified to value Val. Possible deductions with this relation are illustrated below.

Bytecodes for arrays manipulation \text{baload}, \text{iaload}, \text{lastore}, ... and method invocations \text{invokespecial}, \text{invokevirtual}, \text{invokespecial} are taken into account but they are not described here as we considered they were outside the scope of the paper.

C. Example

From the \text{moveY} method of Fig.2 and the test objective which consists to reach bytecode numbered 51, we get the following constraint system (omitting some details about the calls to constructors). For this example, \( M_i \) denotes the memory state before the bytecode instruction number \( i \).

\[
\begin{align*}
F1 &= \text{This.Chrono.Speed.Ytemp, This} \neq \text{null} \\
M_{S1} &= (F1, S1, H1), \\
M_{A1} &= (F1, X.Y.A1.S1, H2), \\
\text{invokespecial} &= (\text{Coord, init, [A1, Y, X], H2, H1}), \\
M_{A3} &= (F1, A2.Y.A1.S1, H2), A2 \neq \text{null, getfield(A2, x, H2, X)}, \\
M_{A4} &= (F1, Y.A1.S1, H2), A2 = \text{this}, \\
M_{A3} &= (F1, A1.S1, H2), Y = \text{Ytemp}, \\
M_{A2} &= (F1, A2.S1, H2), S1 = \text{A1.S2}, \\
M_{A0} &= (F1, S2, H3), A \neq \text{null, new(Coord, H3, H2, A1)}, \\
M_{A8} &= (F2, Ytemp, S2, H3), F2 = \text{This.Chrono.Speed.Ytemp2}, \\
M_{A9} &= (F2, S2, H3), \text{Ytemp} = 65536, \\
M_{A3} &= (F2, Val1.Val2.S2, H3), Val2 > Val1, \\
M_{A1} &= (F2, Val2.S2, H3), Val1 = 65636, \\
M_{A6} &= (F2, S2, H3), \text{Val2} = \text{Ytemp2}, \\
M_{A7} &= (F2, Val3.A3.S2, H4), A3 \neq \text{null, putfield(A3, time, Val3, H4, H3)}, \\
M_{A5} &= (F2, A3.S2, H4), \text{Val3} = 0, \\
M_{A5} &= (F2, A3.S2, H4), A3 = \text{Chrono}, \\
M_{A4} &= (F3, Ytemp2.S2, H4), F3 = \text{This.Chrono.Speed.Ytemp3}, \\
M_{A3} &= (F3, Val4.Val5.S2, H4), \text{Ytemp2} = \text{Val4 + Val5}, \\
M_{A2} &= (F3, Val6.Val7.Val5.S2, H4), \text{Val4 = Val6 + Val7}, \\
M_{A1} &= (F3, Val7.Val5.S2, H4), \text{Val6} = \text{Speed}, \\
M_{A8} &= (F3, A4.Val5.S2, H4), A4 \neq \text{null, getfield(A4, time, H4, Val17)}, \\
M_{A7} &= (F3, Val5.S2, H4), A4 = \text{Chrono}, \\
M_{A6} &= (F3, A5.S2, H4), A5 \neq \text{null, getfield(A5, y, H4, Val5)}, \\
M_{A5} &= (F3, S2, H4), A5 = \text{This}, \\
M_{A8} &= (F3, Val8.S2, H4), \text{Val8} > 0, \\
M_{A7} &= (F3, S2, H4), \text{Val8} = \text{Speed}, \\
M_4 &= (F3, \text{Val9.S2, H4}), \text{Val9} > 0, \\
M_3 &= (F3, A6.S2, H4), A6 \neq \text{null, putfield(A6, time, H4, Val9)}, \\
M_3 &= (F3, S2, H4), A6 = \text{Chrono, S2} = \epsilon
\end{align*}
\]

\( \epsilon \) is the empty sequence, while \( v.s \) denotes the stack \( s \) where \( v \) is pushed. The elements of the sequence \( F2 \) represent the parameters and the local variables at the bytecode instruction 51. Instruction 48 calls a constructor and links both CMVs \( M_{A8} \) and \( M_{S1} \). The elements on the top of the stack before instruction are the parameters \( Y \) and \( X \) as well as the reference \( A1 \) to the object that calls the method. The heaps \( H2 \) and \( H1 \) are linked by the constructor call effect, represented here by a relation \( \text{invokespecial} \).

The top of the stack before the instruction \( \text{getfield} \) 45 is a reference \( A2 \), while the top of stack \( X \) after the instruction is the value of the attribute \( x \) of the object referenced by \( A3 \) in the heap \( H1 \).

The relation is maintained by a constraint \( \text{getfield}(A3, x, H2, X) \). The instruction 39 allocates memory to store a new object of type \( \text{Coord} \). The relation \( \text{new} \text{(Coord, H3, H2, A1)} \) states that the heap \( H2 \) contains one added object of type \( \text{Coord} \). A1 is pushed on top of the stack after the instruction. As the only instruction that permits to reach 51 after the conditional instruction 33 is 36, then the top of the stack \( A.B \) before the instruction 33 constrains \( B \) to be greater than \( A \).

The top of the stack before the instruction 27 contains the value \( \text{Val3} \) and the reference \( A4 \). The instruction \( \text{putfield} \) updates the value of the attribute \( \text{time} \) with the value \( \text{Val3} \), for the object referenced by \( A3 \). \( H4 \) is the heap before the instruction while \( H3 \) is the heap after instruction and the constraint \( \text{putfield}(A3, \text{time}, \text{Val3}, H4, H3) \) maintains this relation. Finally, the values of the registers \( F3 \), and the heap \( H4 \), of the memory \( M_8 \), describe a possible test input to reach our test objective 51.

D. Possible deductions with operator putfield

In order to illustrate the behavior of a complex constraint, we show the possible deductions by \( \text{putfield} \) on a simple example. Consider the heap \( H0 = \{ (1, a, [t1 \rightarrow V1, t2 \rightarrow V2]), (2, a, [t1 \rightarrow V3, t2 \rightarrow V4]), (3, b, [t3 \rightarrow V5]) \} \) and the heap \( H1 = \{ (1, a, [t1 \rightarrow V6, t2 \rightarrow V7]), \}
\text{(2, a, [t1 \rightarrow V8, t2 \rightarrow V9]), (3, b, [t3 \rightarrow V10])} \), which both contain two objects of class \( a \) and one object of class \( b \), and the relation \( \text{putfield}(A, t1, \text{Val}, H0, H1) \) where \( t1 \) is the first of the two attributes of the class \( a \). Class \( b \), which does not inherit from \( a \), has only a single attribute. Suppose that \( \text{dom}(V1) = [0..10], \text{dom}(V3) = [1..3], \text{dom}(V8) = 15.23^{11} - 1 \) while other domains are unconstrained, let \( \text{dom}(A) = \{a\} \) and \( \text{dom}(\text{Val}) = [10..40] \), and suppose that status of \( H0 \) is unsealed and status of \( H1 \) is closed. Using the relation \( \text{putfield}(A, t1, \text{Val}, H0, H1) \), several deductions can be performed. 1) As the relation operates on attribute \( t1 \), one deduces that \( \text{dom}(A) = \{a\} \times \{0\} \) as object 3 has only attribute \( t3 \) and its class \( b \) does not inherit from \( a \). Consequently, the following equalities can be added \( V2 = V7, V4 = V9 \) and \( V5 = V10 \) as the relation does not modify variables associated with the attributes \( t2 \) and \( t3 \). 2) Considering variables \( V3 \) and \( V8 \), we see that \( \text{dom}(V3) \mathbin{\cap} \text{dom}(V8) = \emptyset \) then one deduces that \( A \) refers necessarily to object 2 in the heaps \( H0 \) and \( H1 \): \( A = 2 \). Consequently, \( V1 = V6 \) is added as the object at the address 1 is not modified and \( V8 = Val \) leading to
objective is to reach constraint block \( \text{e\_target} \).

Backward search relies on constraint block accumulation and solving. A constraint block in a bytecode program is a set of instructions that is submitted to constraint propagation. The test objective specifies a bytecode to reach, which corresponds to a specific constraint block. So, starting from this block, backward search incrementally accumulates other constraint blocks by trying to find a path towards the program entry point. It is worth noticing that constraint consistency is tested on the fly, each time a new constraint block is added to the constraint system. This permits to quickly detect infeasible parts of program paths. These subpaths should not be confounded with path prefix as they do not begin by the method entry point. When a constraint block has several parent blocks in the control-flow graph, then a choice point is created. Each choice is then explored in a depth-first search until one of them gets to the program entry point. If a choice is shown as being incoherent with the rest of the constraint system, then the process backtracks to the first ancestor choice point and takes an alternative. The strategy gives priorities to shortest intraprocedural subpaths towards the program entry points (i.e., in presence of loops, targeting exit loop constraint blocks). Note however that a parameter has to be set to prevent the process from iterating without terminating in presence of loops.

Let us illustrate why backward search can be interesting w.r.t. forward exploration on the simple example of Fig. 3, where the test objective is to reach constraint block \( \text{g\_target} \). Suppose also that block \( \text{e} \) and block \( \text{g} \) contain contradictory conditions. For example, \( \text{e} \) contains assignment \( \text{i} = \text{i} \) while condition to go from block \( \text{e} \) to block \( \text{g} \) is \( \text{i} > 2 \). Starting from block \( \text{g} \), backward search will first explore subpath \( \text{g} \rightarrow \text{e} \) by positioning a choice point. As constraint consistency is tested on the fly, the process fails and backtracks to the choice point without exploring the other backward paths starting by \( \text{g} \rightarrow \text{e} \). Subpath \( \text{g} \rightarrow \text{f} \rightarrow \text{a} \rightarrow ... \) is then considered without failing. Constraint inconsistency detection is possible as our framework can reason both in a forward and backward manner, thanks to the use of constraint programming to express relations between CMV. Moreover, our framework implements a precise memory model able to deal with partially known memory states. On this example, forward exploration such as implemented in several dynamic symbolic execution tools would have first considered \( \text{a} \rightarrow \text{b} \rightarrow \text{c} \rightarrow \text{e} \rightarrow \text{g} \) and failed. Then, backtracking at point \( \text{b} \), depth-first forward exploration would have considered \( \text{a} \rightarrow \text{b} \rightarrow \text{d} \rightarrow \text{e} \rightarrow \text{g} \) and failed again before finding \( \text{a} \rightarrow \text{f} \rightarrow \text{g} \). To be fair, similar poor behavior can be found for backward exploration as well just by considering incoherent subpaths near the program entry point. We are not saying that backward exploration is better than forward, we just say that both approaches complement each other. Our backward search approach is useful to complement an existing test set by looking at not-covered locations.

B. Test input labeling

When a set of consistent constraint blocks has been found to flow backward from the test objective to the program entry point, every variable of the input CMV has not necessarily been instantiated. A labeling step on the input CMV has then to be launched in order to complement the CMV. The process is recursive and tries to select the best option at each step. It starts by labeling the input formal parameters of the method under test. For references, it first tries \text{null}, then it tries the addresses of objects in the heap that have compatible type and finally, upon failure, it creates a new object that has a compatible type. Each time a value is assigned to a variable from its domain, the constraints that operate on this variable are awaked and constraint propagation is relaunched. This process can efficiently prune the domain of other variables. When all the input parameter values are fixed, the values of the object attributes have to be labeled in order to build a complete CMV. The process labels first the object attributes that are reachable from the parameters with a single dereferencing level. If the corresponding input state satisfies the test objective, then we get a solution of the problem. On the contrary, upon failure, the process backtracks and the dereferencing level is increased until a given bound, defined by the user. The status is also labeled to the “closed” value in order to indicate that no more object can be added to the input memory state. When the labeling process is finished, then either a complete input CMV is found that reaches the test objective or a failure is reported. Failure may be provoked by several causes, including unreachable test objective, bounds on backward search or dereferencing level, or timeout. Hence, the method is incomplete but note that it can find input cyclic data structures when necessary.

VI. EXPERIMENTAL VALIDATION

A. Implementation

Our prototype tool JAUT (Java Automatic Unit Tesing) takes as inputs a bytecode program given under textual form, obtained with SUN’s command javap which decomplies the binary bytecode, and a test objective composed of the method name and bytecode instruction number. It reports as output an input CMV, excerpts of which have been presented in Sec. 2 of the paper. JAUT includes 1) a bytecode analysis module that generates a prolog-based internal
structure that can be efficiently explored with backtracks and unification; 2) a backward search module which is parameterized by: a bound on the number of times certain branches are executed, a bound on the length of paths to be explored, a bound on the dereferencing level and a timeout; 3) a constraint solver which implements constraint generation and deduction rules for the constraints associated with bytecodes. The constraint solver implements its own constraint propagation queue and its own memory labeling strategy, but it calls the SICStus Prolog clpfd library for solving arithmetic constraints.

JAUT handles a meaningful subset of bytecodes, as discussed earlier, but as a research prototype tool, it handles only about a third of the one hundred or so bytecodes of the SUN’s JVM specification. Bytecodes that were left apart include bytecodes for integer conversions and low-level shifting, bytecodes for floating-point computations. Note that, for each bytecode, a specific constraint model was developed and deduction rules that captures the operational semantics of the JVM were implemented.

B. Experiments

All the results were computed on a standard single-core machine: an Intel Pentium, 2.16GHZ machine running Windows XP with 2.0GB of RAM. Our experiments aimed at evaluating the capabilities of JAUT to complement an existing test set, obtained by another forward path-exploration test data generator. We selected three such white-box test data generation tools: jCUTE, JTEST version 8.0 and Pex version 0.15.40714.1. Pex is dedicated to .NET but the constraint solver and backtracking is hard-coded in Prolog.

Simple programs are used in our experiments: versions of the classical trityp and josephus programs in bytecodes, methods of the DoublyLinkedList and TreeMap Java classes. Trityp has many infeasible paths while josephus manages a cyclic dynamic data structure. We also considered a modified version of this program, called josephus/m, where the hard-to-reach decision ndeEnd.key=31 & nde.key=31 is inserted at the end of the program. The DoublyLinkedList class also implements dynamic data structures management and contains input object references and method calls in its code. The TreeMap class implements red-black trees which are cyclic structures. The source code of these programs, the source code of JAUT, as well as all the test drivers used for Pex and jCUTE can be found online at www.irisa.fr/lande/gotlieb/resources/jaut.html.

In all the programs, private fields have been turned into public ones in order, for the three tools, to equally generate valid and invalid input states. For the depth-first backward exploration of JAUT, a bound of 150 bytecodes on the length of path and a bound of 10 for the maximum dereferencing level have been set.

In addition, we considered the following program (in bytecodes) that illustrates a problem related to forward exploration:

```
static int a=1;
```

5In our results, difference of the .NET runtime cost vs. JVM runtime have been considered negligible.

public static int foo(int i){
    int j = 10 ;
    while (i > 1){ j++; i--; }
    if (j > 50*a)
        return 1; // test objective I
    return 0; }

Reaching the test objective I implicitly constrains the number of iterations within the loop. On this example, forward exploration will unroll the loop without taking into account the test objective. The parameter a can be increased to study the scaling effect of the underlying problem.

C. Results and analysis

On the foo program, both JTEST and Pex fail to reach the test objective I. Unlike these tools, jCUTE covers every instructions of the foo method, including instruction I, but it takes 10.9sec of CPU time. JAUT also generated an input CMV (corresponding to i = 42) that reaches I in 0.15sec of CPU time. Its backward exploration strategy is useful on this example.

We studied the behavior of both jCUTE and JAUT on the foo example by increasing the value of a. Fig. 4 shows the results of this experiment. The time required by jCUTE increases dramatically on this example as the tool requires an increasing number of trials to satisfy this hard-to-reach test objective. As jCUTE compiles and executes programs to perform dynamic symbolic execution, the CPU time increases accordingly. The JAUT approach is better on this example as constraints are directly handled in the constraint solver and backtracking is hard-coded in Prolog. For other experiments, results are shown in Fig.5 where #Bc is the number of bytecode instructions, #To is the number of test objectives. We report the results of jCUTE, Pex, and JAUT to get complete bytecode instructions coverage and the results of JAUT to complement the test sets produced by Pex. The fourth tool JTEST reveals itself too poor on this task. In fact, its test input generation strategy is based on the analysis of constants in the program, which prevents many symbolic decisions to be covered. jCUTE and Pex have the primary goal of covering all the feasible paths of the program while JAUT is designed to reach a single instruction in the program. Hence, none of these three tools is optimized to efficiently get complete bytecode instruction coverage. However, in all the cases, there are claims on their ability
to reach instruction coverage. For JAUT, instruction coverage can be automatically reached by launching incrementally requests on not-covered instructions in a script. For the three tools, we report coverage percentage, which we have computed ourselves on a common basis. Indeed, Pex reports dynamic bytecode coverage which does not necessarily correspond to bytecode instruction coverage. So, we computed the coverage by looking at the covered portions of code, rather than taking into account the numbers provided by the tools. We selected two search modes for jCUTE: the former corresponds to depth-first search on the execution tree (both columns noted jCUTE) while the second corresponds to random path exploration (both columns noted jCUTEr). We measured the CPU time required by JAUT to complement the test set generated by Pex (column compl. JAUT) when it was incomplete. When this measure was unnecessary, n/a was reported.

For the trit-yp method, experiments show that, unlike jCUTE in both versions, Pex and JAUT succeed to get complete coverage. However, the CPU time required to get this result for JAUT is very long (almost one hour). Indeed, SicStus Prolog needs a long time to demonstrate the insatisfiability of some path condition, as \( i + j > k, j + k > i, i + j > k, j \neq k, i \neq k, i \neq j, k \neq 0, j \neq 0, i \neq 0 \) where \( i, j, k \) denote three 32-bit integers, because it requires long-term labeling. Note that another approach would be to use dedicated SMT solver such as Z3 [19] in JAUT to avoid these problems.

Program josephus in both versions is hard to cover. The program computes first a dynamic cyclic chain in function of input parameters and then it eliminates one by one the elements by cycling around the chain. Satisfying all the test objectives require parameters and then it eliminates one by one the elements by program computes first a dynamic cyclic chain in function of input parameters. The results obtained for method fixAfterInsertion are the most interesting. Both modes of jCUTE cover only about 20% of the method while Pex covers about 45%. The CPU times required to get these results is rather long for jCUTEr and Pex (resp. 28.30 and 120.00 sec). On the contrary, JAUT covers 100% of the method in 22.18 sec. When used to complement the Pex test set, it takes 15.49 sec, showing that not-covered bytecode instructions are indeed hard to reach. So, JAUT performs well on the methods of the TreeMap class as it contains many hard test input generation problems. We interpret this result as a confirmation that using a precise memory model, which in particular deals with reference aliasing, is advantageous for completing an existing test set.

D. Related work

Test input generation at the Bytecode level. JAUT performs constraint-based test input generation from Java bytecode. Therefore, it is mainly related to JPF [8], jCUTE [12], [13], and Pex [14]. Unlike these three tools, JAUT implements backward exploration, meaning that it starts from a target bytecode location and incrementally discovers a feasible path towards the entry. Indeed, JPF, jCUTE and Pex are based on forward symbolic execution which consists to evaluate symbolically the instructions along a path in the same order as execution. Improvements on the search strategy of Pex have been proposed [20] to leverage some of the problems of forward exploration. Note that backward symbolic execution exists for a long time [21], but our approach extends and generalizes this idea to programs containing references on the stack and the heap, as well possibly cyclic dynamic data structures. Reasonning backward at the bytecode level requires a precise memory model to be defined. Our memory model has similarities with those of JPF [8], [9] in that it also implements a form of “lazy initialization”. In our approach, decisions such \( \text{if}(\ p.\text{next} == p) \) constrains two variables to be equal and non null without instantiating them. Unlike lazy initialization which makes choices during constraint solving, JAUT reports the choice to the labeling phase. Our memory model also has similarities with the constraint-based models of CUTE [12] and Pex [14] that can deal with symbolic pointer equalities and inequalities, dynamic memory allocation and input data structures. We argued below that JAUT can complement an existing test set produced by one of these tools by applying more costly analysis for specific unreached locations within the bytecode. In fact, the constraint-based reasoning step of JAUT defines precise relations between two CMVs (constraint memory variables) for each bytecode. Of course, the scope of JAUT is currently too restricted (a meaningful subset of JVM bytecodes) to compete with the industrial development of Pex, but we believe that both approaches could complement each other in the long term.

Test input generation for binary programs. OSMOSE [22] and SAGE [23] both implement forward dynamic symbolic execution for binary programs. They handle dynamic jumps and use an untyped memory model able to deal with pointer arithmetic, type casting and multiple dereferencing levels. SAGE builds path conditions that are submitted to the SMT solver Z3 [19]. Unlike SAGE [23], JAUT is based on a constraint propagation and labeling solver. Such solvers are used with success in the context of combinatorial optimization problems as they can solve linear as well as non-linear
problems over the reals or the integers. Variable multiplication or
divisions are typical examples of non-linear constraints that are
efficiently handled by these solvers. Another advantage of
constraint propagation relies on its flexibility to add new user-
defined constraints. For JAUT, we built several constraint operators
that apply deduction rules to reason over the memory shapes. These
operators captures both forward and backward exploration at the
same time and propagates domain reductions without instantiating
any variable or equality. However, using a SMT-solver such as
Z3 [19] to solve arithmetical constraints over fixed-length integer
variables would be very interesting to replace $\text{clpfd}$ in JAUT.
Note also that test input generation for binary programs is harder
than at the bytecode level as the control flow cannot easily be
recovered and variable types are unknown which makes the
building of constrained input memory states more complex.

**Test input generation from C and Java source code.** There are
many approaches of automatic test input generation from source
code. In our previous works [4], [18], we built memory models for
constraint-based test data generator of C programs. Our previous
model handled pointers toward named locations of the memory and
dynamically allocated structures but they were limited in their
scope. Unlike JAUT, the model of [4] did not contain representa-
tion of the heap and then it was unable to deal with dynamic
memory allocation. The model of [18] was very complex and the
generation took too much time. Furthermore, in these preliminary
memory models, backward exploration has not been implemented.
PathCrawler [11], DART [10], CUTE [12] implement dynamic
symbolic execution for C source code. On the contrary, JAUT
implements static backward exploration. These two approaches
complement each other as dynamic symbolic execution rapidly
covers many feasible paths while static backward exploration focusses
on hard-to-reach instructions. One advantage of dynamic symbolic
execution is that it can deal with third-party libraries or
calls to native methods while static backward exploration cannot as
there is no available constraint model. Another difference concerns
the capabilities of dynamic symbolic exploration to use concrete
value instead of symbolic ones for simplifying constraint solving.
Note that the constraint reasoning model of JAUT handles com-
plex constraints and just reports value choices to the labeling phase.
EXE [15] implements global symbolic evaluation by launching
an eager path exploration of the C program under test. Although
this approach is appealing if implemented on a grid platform, it
can reveal disastrous for programs that contain a huge number
of paths. As soon as a program contains a loop, its number of
paths is unbounded and even when it contains only conditionals, its
number of path grows exponentially with the number of decisions
in the worst case. Unlike JAUT, EXE does not use incremental
constraint solving, so inconsistencies due to infeasible paths may
be lately discovered and this could penalize the test input generation
if implemented on a single machine. Note that EXE uses the STP
SMT-solver which won several competitions and that it implements
nice optimizations such as constraint caching and symbolic mem-
ory accesses tracking. However, as pointed out by the authors,
its memory model does not handle double pointer dereferencing
levels. The memory model of JAUT handles multiple dereferencing
levels, up to a user-defined bound. Exhaustive bounded testing of
Java programs as implemented in TestEra [5] and KORAT [6]
is a test input generation method that exhaustively explores the
input search space. The approach can generate a large number of
dynamically allocated structures but, unlike JAUT, it does not target
specific locations or paths in the code. In fact, these constraint-
based approaches have developed complex strategies to efficiently
generate test inputs [7] but they cannot solve path constraints
extracted from programs.

**Counter-example generation.** Software model-checkers such as
Save [24], Blast [25], Magic [26] or Cbmc [27] explore the
paths of a bounded model of C programs in order to find a
counter-example path to a temporal property. Some of them also
address statement reachability by generating test inputs to reach
specific locations within the source code [8]. Some of them exploit
predicate abstraction to boost the exploration in the context of
CEGAR that stands for (Counter-Example Generation through Ab-
straction Refinement). JAUT contrasts with these model-checkers
and CEGAR as it does not abstract the program and does not
generate spurious counter-example paths. In particular JAUT builds
a constraint model of bytecode program by capturing an error-free
concrete semantics without considering a boolean abstraction of the
program structure. On the one hand, this allows for precise input
memory state to be built but, on the other hand, requires costly
analysis to be implemented.

**VII. CONCLUSIONS AND FURTHER WORK**

In this paper, we proposed a new constraint-based test input
generation approach for testing Java programs at the bytecode

<table>
<thead>
<tr>
<th>Methods</th>
<th>#Bc</th>
<th>#Io</th>
<th>jCUTE (cov)</th>
<th>jCUTE (sec)</th>
<th>jCUTEr (cov)</th>
<th>jCUTEr (sec)</th>
<th>Pex (cov)</th>
<th>Pex (sec)</th>
<th>JAUT (cov)</th>
<th>JAUT (sec)</th>
<th>JAUT+ (sec)</th>
<th>Compl.JAUT+ (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>trityp</td>
<td>89</td>
<td>24</td>
<td>83.3%</td>
<td>2.20</td>
<td>87.5%</td>
<td>30.88</td>
<td>100%</td>
<td>4.17</td>
<td>100%</td>
<td>313.00</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>foo</td>
<td>15</td>
<td>3</td>
<td>100%</td>
<td>10.90</td>
<td>75%</td>
<td>18.80</td>
<td>66%</td>
<td>4.51</td>
<td>100%</td>
<td>0.17</td>
<td>0.15</td>
<td>n/a</td>
</tr>
<tr>
<td>josephus</td>
<td>51</td>
<td>3</td>
<td>100%</td>
<td>1.06</td>
<td>100%</td>
<td>1.06</td>
<td>100%</td>
<td>8.07</td>
<td>100%</td>
<td>0.36</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>josephus/m</td>
<td>60</td>
<td>5</td>
<td>70%</td>
<td>192.00</td>
<td>70%</td>
<td>**</td>
<td>100%</td>
<td>8.41</td>
<td>60%</td>
<td>**</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Node class</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>insertBefore</td>
<td>36</td>
<td>4</td>
<td>100%</td>
<td>3.02</td>
<td>100%</td>
<td>35.80</td>
<td>100%</td>
<td>4.03</td>
<td>100%</td>
<td>0.20</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>DoublyLinkedList</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pop</td>
<td>13</td>
<td>2</td>
<td>100%</td>
<td>2.16</td>
<td>100%</td>
<td>23.00</td>
<td>100%</td>
<td>0.59</td>
<td>100%</td>
<td>0.13</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>add</td>
<td>42</td>
<td>4</td>
<td>100%</td>
<td>9.19</td>
<td>88%</td>
<td>45.00</td>
<td>100%</td>
<td>6.09</td>
<td>100%</td>
<td>0.14</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>remove</td>
<td>31</td>
<td>4</td>
<td>100%</td>
<td>2.94</td>
<td>100%</td>
<td>1.89</td>
<td>100%</td>
<td>0.69</td>
<td>100%</td>
<td>0.16</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>RedBlackTree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rotateLeft</td>
<td>48</td>
<td>5</td>
<td>20%</td>
<td>26.56</td>
<td>20%</td>
<td>25.10</td>
<td>88.9%</td>
<td>0.65</td>
<td>100%</td>
<td>0.23</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td>deleteEntry</td>
<td>124</td>
<td>14</td>
<td>50%</td>
<td>2.12</td>
<td>91.6%</td>
<td>5.64</td>
<td>78.6%</td>
<td>56.00</td>
<td>100%</td>
<td>1.44</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>fixAfterDeletion</td>
<td>175</td>
<td>11</td>
<td>36.3%</td>
<td>1.11</td>
<td>54.5%</td>
<td>**</td>
<td>81.9%</td>
<td>92.00</td>
<td>100%</td>
<td>7.78</td>
<td>0.88</td>
<td></td>
</tr>
<tr>
<td>fixAfterInsert</td>
<td>127</td>
<td>9</td>
<td>19%</td>
<td>1.30</td>
<td>18.7%</td>
<td>28.30</td>
<td>44.4%</td>
<td>120.00</td>
<td>100%</td>
<td>22.18</td>
<td>15.49</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5. Time and coverage with jCUTE, Pex and JAUT (**: timeout of 3600sec)
level. We developed a logical memory model for a meaningful subset of bytecodes and proposed deductive rules to solve complex constraints such as $p == p_.next$. Unlike other approaches, our prototype tool JAUT implements depth-first backward search and our experimental results indicate that this strategy complements forward search test data generation. Several short term improvements include the use of more dedicated constraint solvers to solve arithmetical constraints of the path conditions (e.g., $Z3$). Backward search could also be refined with an iterated bounded depth-first strategy to improve our handling of nested and sequential loop computations. Finally, our memory model could be improved by considering more fine-tuned awakening conditions. In the long term, our memory model could be completed to deal with exceptions as they just represent new control flow structures. Multi-threading also appears as an essential topic in Java programming and implementing a backward search strategy for test input generation of multi-threaded bytecode programs would certainly be beneficial to the community.

REFERENCES


