Bytecode Verification and its Applications

August 8, 2006

Contents

Chapter 1

Introduction

Chapter 2

Java bytecode language and its operational semantics

The purpose of this chaprter is to introduce the fundamental concepts of the present thesis. In particular, we present a bytecode language and its operational semantics. Those concepts will be used later in Chapter 5 for the definition of the verification procedure as well as for establishing its correctnes w.r.t. the operational semantics given in this section. As our verification procedure is tailored to Java bytecode the bytecode language introduced hereafter is close to the Java Virtual Machine language [25](JVM for short). However, it abstracts from some of the JVM language features while supporting others. Thus, we concentrate on the the most important features of the JVM. In the following, we look closer at what are the characteristic of our bytecode language.

The features supported by our bytecode language are

- arithmetic operations like multiplication, division, addition and substruction.
- stack manipulation. Similarly to the JVM our abstract machine is stack based, i.e. instructions get their arguments from the operand stack and push their result on the operand stack.
- method invokation. In the following, we consider only non void methods. We restrict our modelization for the sake of simplicity without losing any specific feature of the Java language.
- object manipulation and creation. We support field access and update as well as object creation.
- exception throwing and handling. Our bytecode language supports runtime and programmatic exceptions as the JVM does. An example for a situation where a runtime exception is thrown is a null object dereference.

- classes and class inheritance. Like in the JVM language, our bytecode language supports a tree class hierarchy in which every class has a super class except the class `Object` which is the root of the class hiearchy.
- the unique basic type which is supported is the integer type. This is not so unrealistic as the JVM supports only few instructions for dealing with the other integral types, like byte and short. However, it is true that the formalization of the long type and manipulation of long values can be more complicated because of the fact that long values are stored in two adjacent registers. For our purposes, we do not consider that long values represent an interesting case and we discard them.

Our bytecode language omits some of the features of Java, in order to concentrate on the features listed above.

The features not supported by our bytecode language are

- void methods. Note that the current formalization can be extended to void methods without major difficulties.
- static fields and methods. Static data is shared between all the instances of the class where it is declared. We can extend our formalization to deal with static fields and methods, however it would have made the presentation heavier without gaining new feature from the JVM bytecode language
- static initialization. This part of the JVM is discarded as its formal understanding is difficult and complex. Static initialization is a good candidate for a future work

J. Kiniry

- subroutines. The basic reason that our bytecode language does not support subroutines is that in the implementation of our bytecode verification condition generator we inline them and thus, there is no need of supporting them on bytecode level.
- interface types. These are reference types whose methods are not implemented and whose variables are constants. Such interface types are then implemented by classes and allow that a class get more than one behavior. A class may implement several interfaces. The class must give an implementation for every method declared in any interface that it implements. If a class implements an interface then every object which has as type the class is also of the interface type. Interfaces are the cause of problems in the bytecode verifier as the type hierarchy is no more a lattice in the presence of interface types and thus, the least common super type of two types is not unique. However, in the current thesis we do not deal with bytecode verification but we will be interested in the program functional behaviour. For instance, if a method overrides a method from the super class or implements a method from an interface, our objective will be to establish that the method respects the specification of the method it overrides or implements. In this sense, super classes or interfaces are treated similarly in our verification tool.

Moreover, considering interfaces would have complicated the current formalization without gaining more new features of Java. For instance, in the presence of interfaces, we should have extended the subtyping relation.

- floating point arithmetic. We omit this data in our bytecode language for the following reasons. There is no support for floating point data by automated tools. For instance, the automatic theorem prover Simplify which interfaces our verification tool lacks support for floating point data, see [22]. Although larger and more complicated than integral data, formalization of floating point arithmetic is possible. For example, the specification of IEEE for floating point arithmetic as well as a proof for its consistency is done in the interactive theorem prover Coq. However, including floating point data would not bring any interesting part of Java but would rather turn more complicated and less understandable the formalizations in this thesis.

reference

In what follows, we give a big step operational semantics of the bytecode language whose major difference with most of the formalizations of the JVM is that it abstracts from the method frame stack. This is different from most of the existing formalization of the JVM (or JVM like languages), which use usually a small step semantics. However, this semantics is sufficient for our purposes which are to prove the correctness of our verification calculus.

The rest of this chapter is organized as follows: subsection 2.1 is a discussion about our choice for operational semantics, subsection 2.2 is an overview of existing formalisations of the JVM semantics, subsection 2.3 gives some particular notations that will be used from now on along the thesis, subsection 2.4 introduces the structures classes, fields and methods used in the virtual machine, subsection 2.5 gives the type system which is supported by the bytecode language, subsection 2.6 introduces the notion of state configuration, subsection 2.6.1 gives the modelisation of the memory heap, subsection 2.8 gives the operational semantics of our language.

2.1 Design choices for the operational semantics

Before proceeding with the motivations for the choice of the operational semantics, we shall first look at a brief description of the semantics of the Java Virtual Machine (JVM).

JVM is stack based and when a new method is called a new method frame is pushed on the frame stack and the execution continues on this new frame. A method frame contains the method operand stack, the array of registers and the constant pool of the class the method belongs to. When a method terminates its execution normally, the result, if any, is popped from the method operand stack, the method frame is popped from the frame stack and the method result (if any) is pushed on the operand stack of its caller. If the method terminates with an exception, it does not return any result and the exception object is propagated back to its callers.

Most of the existing formalizations of the JVM semantics model the method frame stack and use a small step operational semantics. This approach is necessary when reasoning about the properties of the JVM or the bytecode verifier.

However the purpose of the operational semantics presented in this chapter is to give a model w.r.t.which a proof of correctness of our verification calculus will be done. Because the latter is modular and assumes termination, i.e. the verification calculus assumes the correctness and the termination of the invoked methods, we do not need a model for reasoning about the termination or the correctness of invoked methods. A big step semantics provides a suitable level of abstraction as it does not express those details. In the following, we give a short review of the formalizations of the JVM.

2.2 Related Work

A considerable effort has been done on the formalization of the semantics of the JVM. Most of the existing formalizations cover a representative subset of the language. Among them is the work [16] by N.Freund and J.Mitchell and [28] by Qian, which give a formalization in terms of a small step operational semantics of a large subset of the Java bytecode language including method calls, object creation and manipulation, exception throwing and handling as well subroutines, which is used for the formal specification of the language and the bytecode verifier.

Based on the work of Qian, in [27] C.Pusch gives a formalization of the JVM and the Java Bytecode Verifier in Isabelle/HOL and proves in it the soundness of the specification of the verifier. In [20], Klein and Nipkow give a formal small step and big step operational semantics of a Java-like language called Jinja, an operational semantics of a Jinja VM and its type system and a bytecode verifier as well as a compiler from Jinja to the language of the JVM. They prove the equivalence between the small and big step semantics of Jinja, the type safety for the Jinja VM, the correctness of the bytecode verifier w.r.t. the type system and finally that the compiler preseves semantics and well-typedness.

The small size and complexity of the JavaCard platform simplifies the formalization of the system and thus, has attracted particularly the scientific interest. CertiCartes [6, 5] is an in-depth formalization of JavaCard. It has a formal executable specification written in Coq of a defensive and an offensive JCVM and an abstract JCVM together with the specification of the Java Bytecode Verifier. Siveroni proposes a formalization of the JCVM in [32] in terms of a small step operational semantics.

2.3 Notation

Here we introduce several notations used in the rest of this chapter. If we have a function f with domain type A and range type B we note it with $f : A \to B$. If the function receives n arguments of type $A_1 \ \ldots \ A_n$ respectively and maps them

to elements of type B we note the function signature with $f : A_1 * ... * A_n \rightarrow B$. The set of elements which represent the domain of the function f is given by the function $\mathsf{Dom}(f)$ and the elements in its range are given by $\mathsf{Range}(f)$.

Function updates of function f with n arguments is denoted with $f[\oplus x_1 \dots x_n \rightarrow y]$ and the definition of such function is :

$$f[\oplus x_1 \dots x_n \rightarrow y](z_1 \dots z_n) = \begin{cases} y & if\ x_1 = z_1 \wedge ... \wedge x_n = z_n \\ f(z_1 \dots z_n) & else \end{cases}$$

The type $list$ is used to represent a sequence of elements. The empty list is denoted with [ ]. If it is true that the element e is in the list l, we use the notation $e \in l$. The function :: receives two arguments an element e and a list l and returns a new list $e::l$ whose head and tail are respectively e and l. The number of elements in a list l is denoted with $l.length$. The i-th element in a list l is denoted with $l[i]$. Note that the indexing in a list l starts at 0, thus the last index in l being $l.length - 1$.

2.4 Classes, Fields and Methods

Java programs are a set of classes. As the JVM says *A class declaration specifies a new reference type and provides its implementation. ... The body of a class declares members (fields and methods), static initializers, and constructors.* In our formalisation, the set of classes is denoted with **Class**, the set of fields with **Field**, the set of methods **Method**. We define a domain for class names **ClassName**, for field names **FieldName** and for method names **MethodName** respectively.

An object of type **Class** is a tuple with the following components: list of field objects (fields), which are declared in this class, list of the methods declared in the class (methods), the name of the class (className) and the super class of the class (superClass). All classes, except the special class `Object` , have a unique direct super class. Formally, a class of our bytecode language has the following structure:

$$\mathbf{Class} = \left\{ \begin{array}{ll} \mathsf{fields} & : list\ \mathbf{Field} \\ \mathsf{methods} & : list\ \mathbf{Method} \\ \mathsf{className} & : \mathbf{ClassName} \\ \mathsf{superClass} & : \mathbf{Class} \cup \{\bot\} \end{array} \right\}$$

A field object is a tuple that contains the unique field id (Name) and a field type (Type) and the class where it is declared (declaredIn):

$$\mathbf{Field} = \left\{ \begin{array}{ll} \mathsf{Name} & : \mathbf{FieldName}; \\ \mathsf{Type} & : JType; \\ \mathsf{declaredIn} & : \mathbf{Class} \cup \{\bot\} \end{array} \right\}$$

From the above definition, we can notice that the field declaredIn may have a value $\bot$. This is because we model the length of a reference pointing to an array

object as an element from the set **Field** . Because the length of an array is not declared in any class, we assign to its attribute declaredIn the value $\perp$. The special field which stands for the array length (the name of the object and its field Name have the same name) is the following:

$$\text{arrLength} = \left\{ \begin{array}{ll} \mathsf{Name} & = \text{arrLength}; \\ \mathsf{Type} & = int; \\ \mathsf{declaredIn} & = \perp \end{array} \right\}$$

Note that there are other possible approaches for modeling the array length. For instance, the array length can be part of the array reference. We consider that both of the choices are equivalent. However, the current formalization follows closely our implementation of the verification condition generator which is necessary if we want to do a proof of correctness of the implementation.

A method has a unique method id (Name), a return type (retType), a list containing the formal parameter names and their types(args), the number of its formal parameters (nArgs), list of bytecode instructions representing its body (body), the exception handler table (excHndlS) and the list of exceptions (exceptions) that the method may throw

$$\mathbf{Method} = \left\{ \begin{array}{ll} \mathsf{Name} & : \mathbf{MethodName} \\ \mathsf{retType} & : JType \\ \mathsf{args} & : list\ (name * JType) \\ \mathsf{nArgs} & : nat \\ \mathsf{body} & : list\ \ \mathrm{I} \\ \mathsf{excHndlS} & : list\ \mathbf{ExcHandler} \\ \mathsf{exceptions} & : list\ \mathbf{Class}_{exc} \end{array} \right\}$$

We assume that for every method `m` the entrypoint is the first instruction in the list of instructions of which the method body consists, i.e. `m`.entryPnt = `m`.body[0].

An object of type **ExcHandler** contains information about the region in the method body that it protects, i.e. the start position (startPc) of the region and the end position (endPc), about the exception it protects from (exc), as well as what position in the method body the exception handler starts (handlerPc) at.

$$\mathbf{ExcHandler} = \left\{ \begin{array}{ll} \mathsf{startPc} & : nat \\ \mathsf{endPc} & : nat \\ \mathsf{handlerPc} & : nat \\ \mathsf{exc} & : \mathbf{Class}_{exc} \end{array} \right\}$$

We require that startPc, endPc and handlerPc fields in any exception handler attribute `m`.excHndlS for any method `m` are valid indexes in the list of instructions of the method body `m`.body:

$$\begin{array}{l}\forall \mathtt{m} : \textbf{Method},\\ \forall i : nat, 0 \leq i < \mathtt{m}.\mathsf{excHndlS}.length,\\ \quad 0 \leq \mathtt{m}.\mathsf{excHndlS}[i].\mathsf{endPc} < \mathtt{m}.\mathsf{body}.length \wedge\\ \quad 0 \leq \mathtt{m}.\mathsf{excHndlS}[i].\mathsf{startPc} < \mathtt{m}.\mathsf{body}.length \wedge\\ \quad 0 \leq \mathtt{m}.\mathsf{excHndlS}[i].\mathsf{handlerPc} < \mathtt{m}.\mathsf{body}.length\end{array}$$

2.5 Program types and values

The types supported by our language are a simplified version of the types supported by the JVM. Thus, we have a unique simple type : the integer data type **int**. The reference type (*RefType*) stands for the simple reference types (*RefTypeCl*) and array reference types (*RefTypeArr*). As we said in the beginning of this chapter, the language does not support interface types.

$$\begin{array}{ll}JType & ::= \textbf{int} \mid RefType\\ RefType & ::= RefTypeCl \mid RefTypeArr\\ RefTypeCl & ::= \textbf{Class}\\ RefTypeArr & ::= JType[]\end{array}$$

Our language supports two kinds of values : values of the basic type **int** and reference values *RefVal*. *RefVal* may be either references to class objects or references to array objects. The set of references of class objects is denoted with ref and the set of references to array objects is represented with $refArr$. The following definition gives the formal grammar of values:

$$\begin{array}{ll}Values & ::= i \mid RefVal\\ RefVal & ::= RefValCl \mid RefValArr \mid \textbf{null}\\ RefValArr & ::= refArr\end{array}$$

Every type has an associated default value which can be accessed via the function *defVal*. The function is defined as follows:

$$\mathsf{defVal} : RefType \rightarrow Values$$

$$\mathsf{defVal}(\mathtt{T}) = \begin{cases} \textbf{null} & \mathtt{T} \in RefType\\ 0 & \mathtt{T} = \textbf{int}\end{cases}$$

We define also a subtyping relation as follows:

$$\frac{}{\mathsf{subtype}\ (C,C)} \qquad \frac{C2{=}C1.\mathsf{superClass}}{\mathsf{subtype}\ (C1,C2)}$$

$$\frac{C3{=}C1.\mathsf{superClass}\ \ \mathsf{subtype}\ (C3,C2)}{\mathsf{subtype}\ (C1,C2)} \qquad \frac{}{\mathsf{subtype}\ (C1,\mathtt{Object})}$$

$$\frac{}{\mathsf{subtype}\ (C[],\mathtt{Object})} \qquad \frac{\mathsf{subtype}\ (C1,C2)}{\mathsf{subtype}\ (C1[],C2[])}$$

2.6 State configuration

In this section, we introduce the notion of program state. A state configuration Smodels the program state in particular execution program point by specifying what is the memory heap in the state, the stack and the stack counter, the values of the local variables of the currently executed method and what is the instruction which is executed next. Note that, as we stated before our semantics ignores the method call stack and so, state configurations also omit the call frames stack.

We define two kinds of state configurations:

$$S = S^{interm} \cup S^{final}$$

The set S^{interm} consists of method intermediate state configurations, which stand for an *intermediate state* in which the execution of the current method is not finished i.e. there is still another instruction of the method body to be executed. The configuration $< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \in S^{interm}$ has the following elements:

- the function H: HeapType which stands for the heap in the state configuration
- Cntr is a variable that contains a natural number which stands for the number of elements in the operand stack.
- Stis a partial function from natural numbers to values which stands for the operand stack.
- Reg is a partial function from natural numbers to values which stands for the array of local variables of a method. Thus, for an index `i` it returns the value $\mathbf{reg}(i)$ which is stored at that index of the array of local variables
- Pc stands for the program counter and contains the index of the instruction to be executed in the current state

The elements of the set S^{final} are the final states, states in which the current method execution is terminated and consists of normal termination states (S^{norm}) and exceptional termination states (S^{exc}):

$$S^{final} = S^{norm} \cup S^{exc}$$

A method may terminate either normally (by reaching a return instruction) or exceptionally (by throwing an exception).

- $< \mathrm{H}, \mathrm{Res} >^{norm} \in S^{norm}$ which describes a *normal final state*, i.e. the method execution terminates normally. The normal termination configuration has the following components :
  - the function H: HeapType which reflects what is the heap state after the method terminated

  - Res stands for the return value of the method

- $< \mathrm{H}, \mathrm{Exc} >^{exc} \in S^{exc}$ which stands for an *exceptional final state* of a method, i.e. the method terminates by throwing an exception. The exceptional configuration has the following components:
  - the heap H
  - Exc is a reference to the uncaught exception that caused the method termination

When an element of a state configuration $< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ is updated we use the notation:

$$S[E \leftarrow V],\ E \in \{\mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc}\}$$

We will denote with $< \mathrm{H}, \mathit{Final} >^{final}$ for any configuration which belongs to the set S^{final}. Later on in this chapter, we define in terms of state configuration transition relation the operational semantics of our bytecode programming language. In the following, we focus in more detail on the heap modelization and the operand stack.

2.6.1 Modeling the Object Heap

An important issue for the modelization of an object oriented programming language and its operational semantics is the memory heap. The heap is the runtime data area from which memory for all class instances and arrays is allocated. Whenever a new instance is allocated, the JVM returns a reference value that points to the newly created object. We introduce a record type HeapType which models the memory heap. We do not take into account garbage collection and thus, we assume that heap objects has an infinite memory space.

In our modelization, a heap consists of the following components:

- a component named Fld which is a partial function that maps field structures (of type **Field** introduced in subsection 2.4) into partial functions from references (*RefType*) into values (*Values*).
- a component Arr which maps the components of arrays into their values
- a component Loc which stands for the list of references that the heap has allocated
- a component TypeOf is a partial function which maps references to their dynamic type

Formally, the data type HeapType has the following structure:

$$\forall \mathrm{H} : \mathsf{HeapType},$$
$$\mathrm{H} = \left\{ \begin{array}{ll} \mathsf{Fld} & : \mathbf{Field} \rightharpoonup (\mathit{RefVal} \rightharpoonup \mathit{Values}) \\ \mathsf{Arr} & : \mathit{RefValArr} * \mathit{nat} \rightharpoonup \mathit{Values} \\ \mathsf{Loc} & : \mathit{list}\ \mathit{RefVal} \\ \mathsf{TypeOf} & : \mathit{RefVal} \rightharpoonup \mathit{RefType} \end{array} \right\}$$

Another possibility is to model the heap as partial function from locations to objects where objects contain a function from fields to values. Both formalizations are equivalent, still we have chosen this model as it follows closely the verification condition generator implementation.

In the following, we are interested only in heap objects H which guarantee that the value of the components H.Fld and H.Arr are functions which are defined only for references from the proper type and which are in the list of references of the heap H.Loc:

$$\begin{array}{ll} \forall f : \textbf{Field}, \forall \texttt{ref} \in \mathit{RefVal}, & \texttt{ref} \in \mathsf{Dom}(\mathrm{H.Fld}(f)) \Rightarrow \\ & \texttt{ref} \in \mathrm{H.Loc} \wedge \\ & \mathsf{subtype}\ (\mathrm{H.TypeOf}\ (\texttt{ref}), f.\mathsf{declaredIn}) \\ \wedge & \\ \forall \texttt{ref} \in \mathit{RefValArr}, & (\texttt{ref}, i) \in \mathsf{Dom}(\mathrm{H.Arr}) \Rightarrow \\ & \texttt{ref} \in \mathrm{H.Loc} \wedge \\ & 0 \leq i < \mathrm{H.Fld}(\mathrm{arrLength})(\texttt{ref}) \end{array}$$

Also, we assume that the heap must contain well formed values. By this, we mean that the heap maps any field object f : **Field** which has a reference type (i.e. the component f .Type contains a reference type) into a function which may only return references which are already defined in the heap. The same condition is required for array references whose elements are references, i.e. the value of an array elements is either a reference defined in the heap or **null**. The next formalization expresses the restriction for field functions :

$$\begin{array}{ll} \forall f : \textbf{Field}, & \forall \texttt{ref} \in \mathit{RefVal}, \\ & f.\mathsf{Type} \in \mathit{RefType} \wedge \\ & \texttt{ref} \in \mathsf{Range}(\mathrm{H.Fld}(f)) \Rightarrow \\ & \quad \texttt{ref} \in \mathrm{H.Loc} \vee \texttt{ref} = \textbf{null} \end{array}$$

We define an operation allocator which adds a new reference to the list of references in a heap. The only change that the operation will cause to the heap H is to add a new reference ref to the list of references of the heap H.Loc:

$$\mathrm{allocator}\ : \mathsf{HeapType} * \mathit{RefType} \rightarrow \mathsf{HeapType}$$

Formally, the operation is defined as follows:

$$\begin{array}{l} \mathrm{allocator}(\mathrm{H}, \texttt{ref})\ = \mathrm{H}' \iff^{def} \\ \\ \texttt{ref} \notin \mathrm{H.Loc} \\ \mathrm{H}'.\mathsf{Loc} = \texttt{ref}::\mathrm{H.Loc} \wedge \\ \mathrm{H.Fld} = \mathrm{H}'.\mathsf{Fld} \wedge \\ \mathrm{H.Arr} = \mathrm{H}'.\mathsf{Arr} \wedge \end{array}$$

In the above definition, we use the function *instFlds*, which for a given field f and C returns true if f is an instance field of C:

$$\mathit{instFlds} : \mathbf{Field} \rightarrow \mathbf{Class} \rightarrow \mathit{bool}$$

$$\mathit{instFlds}(f, C) = \begin{cases} \mathit{true} & f.\mathsf{declaredIn} = C \\ \mathit{false} & C = \mathtt{Object} \wedge f.\mathsf{declaredIn} \neq \mathtt{Object} \\ \mathit{instFlds}(f, C.\mathsf{superClass}) & \mathit{else} \end{cases}$$

If a new object of class C is created in the memory, a fresh reference `ref` which points to the newly created object is added in the heap H and all the values of the field functions that correspond to the fields in class C are updated for the new reference with the default values for their corresponding types. The function which for a heap H and a class type C returns the same heap but with a fresh reference of type C has the following name and signature:

$$\text{newRef} : \text{H} \rightarrow \mathit{RefTypeCl} \ \rightarrow \text{H} * \mathit{RefValCl}$$

The formalization of the resulting heap and the new reference is the following:

$$\begin{array}{l} \text{newRef}(\text{H}, C) = (\text{H}', \mathtt{ref}) \iff^{def} \\ \\ \text{allocator}(\text{H}, \mathtt{ref}) \ = \text{H}' \wedge \\ \mathtt{ref} \neq \mathbf{null} \wedge \\ \text{H}'.\mathsf{TypeOf} \ := \text{H}.\mathsf{TypeOf}\ [\oplus \mathtt{ref} \rightarrow C] \wedge \\ \ \forall f : \mathbf{Field}, \quad \mathit{instFlds}(f, C) \Rightarrow \\ \qquad\qquad \text{H}'.\mathsf{Fld} := \text{H}'.\mathsf{Fld}[\oplus f \rightarrow f[\oplus \mathtt{ref} \rightarrow \mathsf{defVal}(f.\mathsf{Type})]] \wedge \end{array}$$

Identically, when allocating a new object of array type whose elements are of type `T` and length l, we obtain a new heap object $\text{newArrRef}(\text{H}, \mathtt{T}[\,], l)$ which is defined similarly to the previous case:

$$\text{newArrRef} : \text{H} \rightarrow \mathit{RefTypeArr} \rightarrow \text{H} * \mathit{refArr}$$

$$\begin{array}{l} \text{newArrRef}(\text{H}, \mathtt{T}[\,], l) \ = (\text{H}', \mathtt{ref}) \iff^{def} \\ \\ \text{allocator}(\text{H}, \mathtt{ref}) \ = \text{H}' \wedge \\ \mathtt{ref} \neq \mathbf{null} \wedge \\ \text{H}'.\mathsf{TypeOf} \ := \text{H}.\mathsf{TypeOf}\ [\oplus \mathtt{ref} \rightarrow \mathtt{T}[\,]] \wedge \\ \text{H}'.\mathsf{Fld} := \text{H}'.\mathsf{Fld}[\oplus \text{arrLength} \rightarrow \text{arrLength}[\oplus \mathtt{ref} \rightarrow l]] \wedge \\ \forall i, 0 \leq i < l \Rightarrow \text{H}'.\mathsf{Arr} := \text{H}'.\mathsf{Arr}[\oplus(\mathtt{ref}, i) \rightarrow \mathsf{defVal}(\mathtt{T})] \end{array}$$

In the following, we adopt few more naming conventions which do not create any ambiguity. Getting the function corresponding to a field f in a heap H : $\text{H}.\mathsf{Fld}(f)$ is replaced with $\text{H}(f)$ for the sake of simplicity.

The same abreviation is done for access of an element in an array object referenced by the reference `ref`at index i in the heap H. Thus, the usual denotation: $\mathrm{H.Arr}(\mathtt{ref}, i)$ becomes $\mathrm{H}(\mathtt{ref}, i)$.

Whenever the field f for the object pointed by reference `ref` is updated with the value *val*, the component H.Fld is updated:

$$\mathrm{H.Fld} := \mathrm{H.Fld}[\oplus f \rightarrow \mathrm{H.Fld}(f)[\oplus \mathtt{ref} \rightarrow val]]$$

In the following, for the sake of clarity, we will use another lighter notation for a field update which do not imply any ambiguities:

$$\mathrm{H}[\oplus f \rightarrow f[\oplus \mathtt{ref} \rightarrow val]]$$

If in the heap H the i^{th} component in the array referenced by `ref` is updated with the new value *val*, this results in assigning a new value of the component H.Arr:

$$\mathrm{H.Arr} := \mathrm{H.Arr}[\oplus(\mathtt{ref}, i) \rightarrow val]$$

In the following, for the sake of clarity, we will use another lighter notation for an update of an array component which do not imply any ambiguities:

$$\mathrm{H}[\oplus(\mathtt{ref}, i) \rightarrow val]$$

2.6.2 Registers

State configurations have an array of registers which is denoted with Reg. Registers are addressed by indexing and the index of the first local variable is zero. Thus, Reg(0) stands for the first register in the state configuration. An integer is be considered to be an index into the local variable array if and only if that integer is between zero and one less than the size of the local variable array. Registers are used to pass parameters on method invocation. On class method invocation any parameters are passed in consecutive local variables starting from register Reg(0). Reg(0) is always used to pass a reference to the object on which the instance method is being invoked (`this` in the Java programming language). Any parameters are subsequently passed in consecutive local variables starting from local variable 1.

2.6.3 The operand stack

Like the JVM language, our bytecode language is stack based. This means that every method is supplied with a Last In First Out stack which is used for the method execution to store intermediate results. The method stack is modeled by the partial function St and the variable Cntr keeps track of the number of the elements in the operand stack. St is defined for any integer `ind` smaller than the operand stack counter Cntr and returns the value St(`ind`) stored in the operand stack at `ind` positions of the bottom of the stack. When a method starts execution its operand stack is empty and we denote the empty stack with [ ]. Like in the JVM our language supports instructions to load values stored

in registers or object fields and viceversa. There are also instructions that take their arguments from the operand stack St, operate on them and push the result on the operand stack. The operand stack is also used to prepare parameters to be passed to methods and to receive method results.

2.6.4 Program counter

The last component of an intermediate state configuration is the program counter Pc. It contains the number of the instruction in the array of instructions of the current method which must be executed in the state.

2.7 Throwing and handling exceptions

As the JVM specification states *exception are thrown if a program violates the semantic constraints of the Java programming language, the Java virtual machine signals this error to the program as an exception. An example of such a violation is an attempt to index outside the bounds of an array. The Java programming language specifies that an exception will be thrown when semantic constraints are violated and will cause a nonlocal transfer of control from the point where the exception occurred to a point that can be specified by the programmer. An exception is said to be thrown from the point where it occurred and is said to be caught at the point to which control is transferred. A method invocation that completes because an exception causes transfer of control to a point outside the method is said to complete abruptly. Programs can also throw exceptions explicitly, using throw statements ...*

Our language supports an exception handling mechanism similar to the JVM one. More particularly, it supports Runtime exceptions:

- `NullPntrExc` thrown if a null pointer is dereferenced
- `NegArrSizeExc` thrown if an array is accessed out of its bounds
- `ArrIndBndExc` thrown if an array is accessed out of its bounds
- `ArithExc` thrown if a division by zero is done
- `CastExc` thrown if an object reference is cast to to an incompatible type
- `ArrStoreExc` thrown if an object is tried to be stored in an array and the object is of incompatible type with type of the array elements

The language also supports programming exceptions. Those exceptions are forced by the programmer, by a special bytecode intruction as we shall see later in the coming section. The modelization of the exception handling mechanism involves several functions. The function *getStateOnExc* deals with bytecode instructions that may throw exceptions. The function returns the state configuration after the current instruction during the execution of `m` throws an exception of type `E`. If the method `m` has an exception handler which can handle

exceptions of type E thrown at the index of the current instruction, the execution will proceed and thus, the state is an intermediate state configuration. If the method m does not have an exception handler for dealing with exceptions of type E at the current index, the execution of m terminates exceptionally and the current instruction causes the method exceptional termination:

$$getStateOnExc : S^{interm} * ExcType * \mathbf{ExcHandler}[] \rightarrow S^{interm} \cup S^{exc}$$

$$getStateOnExc(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, \mathtt{E}, \mathsf{excH}[]) =$$
$$\begin{cases} < \mathrm{H}', 0, \mathrm{St}[\oplus 0 \rightarrow \mathtt{ref}], \mathrm{Reg}, \mathsf{handlerPc} > & \text{if } findExcHandler(\mathtt{E},\mathrm{Pc},\mathsf{excH}[]) = \mathsf{handlerPc} \\ < \mathrm{H}', \mathtt{ref} >^{exc} & \text{if } findExcHandler(\mathtt{E},\mathrm{Pc},\mathsf{excH}[]) = \bot \end{cases}$$

where
$(\mathrm{H}', \mathtt{ref}) = \mathrm{newRef}(\mathrm{H}, \mathtt{E})$

If an exception E is thrown by instruction at position i while executing the method m, the exception handler table m.excHndlS will be searched for the first exception handler that can handle the exception. The search is done by the function *findExcHandler*. If there is found such a handler the function returns the index of the instruction at which the exception handler starts, otherwise it returns $\bot$:

$$findExcHandler : ExcType * nat * \mathbf{ExcHandler}[] \rightarrow nat$$

$$findExcHandler(\ \mathtt{E}, \mathrm{Pc}, \mathsf{excH}[]) =$$
$$\begin{cases} \mathsf{excH}[m].\mathsf{handlerPc} & if\ hExc \neq emptySet \\ & where\ m = min(hExc) \\ \bot & else \end{cases}$$

where

$$hExc = \{k \mid \begin{array}{l} \mathsf{excH}[k] = (\mathsf{startPc}, \mathsf{endPc}, \mathsf{handlerPc}, \mathtt{E}') \wedge \\ \mathsf{startPc} \leq \mathrm{Pc} < \mathsf{endPc} \wedge \\ \mathsf{subtype}\ (\mathtt{E}, \mathtt{E}') \end{array} \}$$

2.8 Bytecode Language and its Operational Semantics

The bytecode language that we introduce here corresponds to a representative subset of the Java bytecode language. In particular, it supports object manipulation and creation, method invokation, as well as exception throwing and

handling. In fig. 2.1, we give the list of instructions that constitute our bytecode language.

$$
\begin{array}{rl}
\mathrm{I} ::= & \mathrm{if\_cond} \\
| & \mathrm{goto} \\
| & \mathrm{return} \\
| & \mathrm{arith\_op} \\
| & \mathrm{load} \\
| & \mathrm{store} \\
| & \mathrm{push} \\
| & \mathrm{pop} \\
| & \mathrm{dup} \\
| & \mathrm{iinc} \\
| & \mathrm{new} \\
| & \mathrm{newarray} \\
| & \mathrm{putfield} \\
| & \mathrm{getfield} \\
| & \mathrm{type\_astore} \\
| & \mathrm{type\_aload} \\
| & \mathrm{arraylength} \\
| & \mathrm{instanceof} \\
| & \mathrm{checkcast} \\
| & \mathrm{athrow} \\
| & \mathrm{invoke}
\end{array}
$$

Figure 2.1: Bytecode Language instructions

Note that the instruction arith_op stands for any arithmetic instruction in the list add , sub , mult , and , or , xor , ishr , ishl , div , rem).

We define the operational semantics of a single Java instruction in terms of relation between the instruction and the state configurations before and after its execution.

Definition 2.8.1 (State Transition) *If an instruction* I *in the body of method* m *starts execution in a state with configuration* $< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and terminates execution in state with configuration* $< \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}', \mathrm{Pc}' >$ *we denote this by*

$$\mathtt{m} \vdash \mathrm{I} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}', \mathrm{Pc}' >$$

We also define how the execution of a list of instructions change the state configuration in which their execution starts.

Definition 2.8.2 (Transitive closure of a method state transition relation) *If the method* m *starts execution in a state* $< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *with* m.body*[0]*

and there exists a transitive state transition to the state $< \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}', \mathrm{Pc}' >$ *we denote this with:*

$$< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow^* < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}', \mathrm{Pc}' >$$

Definition 2.8.3 (Termination of method execution) *If the method* `m` *starts execution in a state* $< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *with* `m.body`*[0] and there is a transitive state transition to* $< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, k >$ *such that the instruction* `m.body`*[k] is either a* return *instruction or an instruction which terminates execution with an uncaught exception and the configuration after its execution is* $< \mathrm{H}', \mathrm{Reg}' >^{final}$ *Final then we denote this with:*

$$\mathtt{m} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \Rightarrow < \mathrm{H}', \mathrm{Reg}' >^{final} \mathit{Final}$$

We first give the operational semantics of a method execution. The execution of method `m`is the execution of its body upto reaching a final state configuration:

$$\frac{\mathtt{m} \vdash \mathtt{m.body}[0] :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow^* < \mathrm{H}', \mathrm{Reg}' >^{final} \mathit{Final}}{\mathtt{m} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \Rightarrow < \mathrm{H}', \mathrm{Reg}' >^{final} \mathit{Final}}$$

Next, we define the operational semantics of every instruction. The operational semantics of an instruction states how the execution of an instruction affects the program state configuration in terms of state configuration transitions defined in the previous subsection 2.6. Note that we do not model the method frame stack of the JVM which is not needed for our purposes.

- Control transfer instructions

1. Conditional jumps : if_cond

$$\frac{\mathtt{cond}(\mathrm{St}(\mathrm{Cntr}), \mathrm{St}(\mathrm{Cntr}-1))}{\mathtt{m} \vdash \text{if\_cond } n :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}-2, \mathrm{St}, \mathrm{Reg}, n >}$$

$$\frac{\mathit{not}(\ \mathtt{cond}(\mathrm{St}(\mathrm{Cntr}), \mathrm{St}(\mathrm{Cntr}-1)))}{\mathtt{m} \vdash \text{if\_cond } n :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}-2, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc}+1 >}$$

The condition `cond` $= \{=, \neq, \leq, <, >, \geq\}$ is applied to the stack top St(Cntr) and the element below the stack top St(Cntr -1)which must be of type **int**. If the condition is true then the control is transfered to the instruction at index `n`, otherwise the control continues at the instruction following the current instruction. The top two elements St(Cntr) and St(Cntr - 1) of the stack top are popped from the operand stack.

2. Unconditional jumps: goto

$$\frac{}{\mathtt{m} \vdash \text{ goto } n :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, n >}$$

Transfers control to the instruction at position n.

3. return

$$\frac{}{\mathtt{m} \vdash \text{ return } :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Reg} >^{norm} \mathrm{St}(\mathrm{Cntr})}$$

The instruction causes the normal termination of the execution of the current method m. The instruction does not affect changes on the heap Hand the return result is contained in the stack top element St(Cntr)

- Arithmetic operations

$$\frac{\begin{array}{l}\mathrm{Cntr}' = \mathrm{Cntr} - 1 \\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} - 1 \rightarrow \mathrm{St}(\mathrm{Cntr}) \text{ op } \mathrm{St}(\mathrm{Cntr} - 1)] \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathrm{m} \vdash op :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

Pops the values which are on the stack top St(Cntr) and St(Cntr - 1) at the position below and applies the arithmetic operation op on them. The stack counter is decremented and the resulting value on the stack top St(Cntr - 1) op St(Cntr) is pushed on the stack top St(Cntr - 1).

case for arithmetic instructions that throw exception

- Load Store instructions

1. load

$$\frac{\begin{array}{l}\mathrm{Cntr}' = \mathrm{Cntr} + 1 \\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} + 1 \rightarrow \mathrm{Reg}(i)] \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathrm{m} \vdash \text{ load } \mathrm{i} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

The instruction increments the stack counter Cntr and pushes the content of the local variable **reg**(i) on the stack top St(Cntr + 1)

2. store

$$\frac{\begin{array}{l}\mathrm{Cntr}' = \mathrm{Cntr} - 1 \\ \mathrm{Reg}' = \mathrm{Reg}[\oplus \mathrm{i} \rightarrow \mathrm{St}(\mathrm{Cntr})] \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathrm{m} \vdash \text{ store } \mathrm{i} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}', \mathrm{St}, \mathrm{Reg}', \mathrm{Pc}' >}$$

Pops the stack top element St(Cntr) and stores it into local variable **reg**(i) and decrements the stack counter Cntr

3. iinc

$$\frac{\begin{array}{l}\mathrm{Reg}' = \mathrm{Reg}[\oplus \mathrm{i} \rightarrow \mathbf{reg}(\mathrm{i}) + 1] \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathrm{m} \vdash \text{ iinc } \mathrm{i} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}', \mathrm{Pc}' >}$$

Increments the value of the local variable **reg**(i)

4. push

$$\frac{\begin{array}{l}\mathrm{Cntr}' = \mathrm{Cntr} + 1\\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} + 1 \rightarrow \mathrm{i}]\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathrm{m} \vdash \text{ push } \mathrm{i} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr} + 1, \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

5. pop

$$\frac{}{\mathrm{m} \vdash \text{ pop} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr} + 1, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} + 1 >}$$

- Object creation and manipulation

1. new `Cl`

$$\frac{\begin{array}{l}(\mathrm{H}', \texttt{ref}) = \mathrm{newRef}(\mathrm{H}, C)\\ \mathrm{Cntr}' = \mathrm{Cntr} + 1\\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} + 1 \rightarrow \texttt{ref}]\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathrm{m} \vdash \text{ new } C :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

A new fresh location `ref` is added in the memory heap H of type C, the stack counter Cntr is incremented. The reference `ref` is put on the stack top St(Cntr + 1).

2. putfield

$$\frac{\begin{array}{l}\mathrm{St}(\mathrm{Cntr} - 1) \neq \textbf{null}\\ \mathrm{H}' = \mathrm{H}[\oplus f \rightarrow f[\oplus \mathrm{St}(\mathrm{Cntr} - 1) \rightarrow \mathrm{St}(\mathrm{Cntr})]]\\ \mathrm{Cntr}' = \mathrm{Cntr} - 2\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \text{ putfield } f :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}, \mathrm{Reg}, \mathrm{Pc}' >}$$

$$\frac{\begin{array}{l}\mathrm{St}(\mathrm{Cntr} - 1) = \textbf{null}\\ \mathit{getStateOnExc}(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, \texttt{NullPntrExc}, \mathtt{m}.\mathsf{excHndlS}) = S\end{array}}{\mathtt{m} \vdash \text{ putfield } f :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow S}$$

The top value contained on the stack top St(Cntr) and the reference contained in St(Cntr - 1) are popped from the operand stack. If St(Cntr - 1) is not **null**[1] , the value of its field `f` for the object is updated with the valueSt(Cntr) and the counter Cntr is decremented. If the reference in St(Cntr - 1) is **null**then a `NullPntrExc` is thrown

3. getfield

$$\frac{\begin{array}{l}\mathrm{St}(\mathrm{Cntr}) \neq \textbf{null}\\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} \rightarrow \mathrm{H}(f)(\mathrm{St}(\mathrm{Cntr}))]\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \text{ getfield } f :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

[1]here we assume that the code has passed successfully the bytecode verification procedure and thus, for instance, St(Cntr - 1) contains certainly a reference of type `C`

$$\frac{\begin{array}{l}\mathrm{St(Cntr)} = \mathbf{null} \\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >,\ \mathtt{NullPntrExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \text{getfield } f :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

The top stack element St(Cntr) is popped from the stack. If St(Cntr) is not **null**the value of the field `f` in the object referenced by the reference contained in St(Cntr), is fetched and pushed onto the operand stack St(Cntr). If St(Cntr) is **null**then a `NullPointerExc` is thrown, i.e. the stack counter is set to 0, a new object of type `NullPointerExc` is created in the memory heap store Hand a reference to it *RefValClNullPointerExc* is pushed onto the operand stack

4. newarray `T`

$$\frac{\begin{array}{l}\mathrm{St(Cntr)} \geq 0 \\ (\mathrm{H}', \mathtt{ref}) = \mathrm{newArrRef(H}, \mathit{type}, \mathrm{St(Cntr)}) \\ \mathrm{Cntr}' = \mathrm{Cntr} + 1 \\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} + 1 \rightarrow \mathtt{ref}] \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \ \text{newarray } \mathtt{T} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr)} < 0 \\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >,\ \mathtt{NegArrSizeExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \text{newarray } \mathtt{T} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

A new array whose components are of type `T` and whose length is the stack top value is allocated on the heap. The array elements are initialised to the default value of `T` and a reference to it is put on the stack top. In case the stack top is less than 0, then `NegArrSizeExc` is thrown

5. type_astore

$$\frac{\begin{array}{l}\mathrm{St(Cntr} - 2) \neq \mathbf{null} \\ 0 \leq \mathrm{St(Cntr} - 1) < \mathrm{arrLength(St(Cntr} - 2)) \\ \mathrm{H}' = \mathrm{H}[\oplus(\mathrm{St(Cntr} - 2), \mathrm{St(Cntr} - 1)) \rightarrow \mathrm{St(Cntr)}] \\ \mathrm{Cntr}' = \mathrm{Cntr} - 3 \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \ \text{type\_astore } :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}, \mathrm{Reg}, \mathrm{Pc}' >}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr} - 2) = \mathbf{null} \\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >,\ \mathtt{NullPntrExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \text{type\_astore } :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr} - 2) \neq \mathbf{null} \\ (\mathrm{St(Cntr} - 1) < 0 \vee \\ \mathrm{St(Cntr} - 1) \geq \mathrm{arrLength(St(Cntr} - 2))) \Rightarrow \\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >,\ \mathtt{ArrIndBndExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \text{type\_astore } :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

The three top stack elements St(Cntr), St(Cntr - 1) and St(Cntr - 2) are popped from the operand stack. The type value contained

in St(Cntr) must be assignment compatible with the type of the elements of the array reference contained in St(Cntr - 2), St(Cntr - 1) must be of type int.

say what assignment compatible is

The value St(Cntr) is stored in the component at index St(Cntr - 1) of the array in St(Cntr - 2). If St(Cntr - 2) is **null**a `NullPntrExc`is thrown. If St(Cntr - 1) is not in the bounds of the array in St(Cntr - 2) an `ArrIndBndExc` exception is thrown. If St(Cntr) is not assignment compatible with the type of the components of the array, then `ArrStoreExc` is thrown

one more case of exceptional termination if it terminates on an exception

6. type_aload

$$\frac{\begin{array}{l}\mathrm{St(Cntr}-1)\neq \textbf{null}\\ \mathrm{St(Cntr)}\geq 0\\ \mathrm{St(Cntr)} < \mathrm{arrLength(St(Cntr}-1))\\ \mathrm{Cntr}' = \mathrm{Cntr}-1\\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr}-1 \rightarrow \mathrm{H(St(Cntr}-1)\mathrm{St(Cntr))}]\\ \mathrm{Pc}' = \mathrm{Pc}+1\end{array}}{\mathtt{m} \vdash \ \mathrm{type\_aload} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow < \mathrm{H, Cntr}', \mathrm{St}', \mathrm{Reg, Pc}' >}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr}-1) = \textbf{null}\\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >, \ \mathtt{NullPntrExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \mathrm{type\_aload} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr}-1)\neq \textbf{null}\\ (\mathrm{St(Cntr)} < 0 \vee\\ \mathrm{St(Cntr)}\geq \mathrm{arrLength(St(Cntr}-1)))\\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >, \ \mathtt{ArrIndBndExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \mathrm{type\_aload} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

Loads a value from an array. The top stack element St(Cntr) and the element below it St(Cntr -1) are popped from the operand stack. St(Cntr) must be of type **int**. The value in St(Cntr -1) must be of type *RefTypeCl* whose components are of type type. The value in the component of the array `arrRef` at index `ind` is retrieved and pushed onto the operand stack. If St(Cntr -1) contains the value **null**a `NullPntrExc`is thrown. If St(Cntr) is not in the bounds of the array object referenced by St(Cntr -1) a `ArrIndBndExc` is thrown

7. arraylength

$$\frac{\begin{array}{l}\mathrm{St(Cntr)}\neq \textbf{null}\\ \mathrm{H}' = \mathrm{H}\\ \mathrm{Cntr}' = \mathrm{Cntr}\\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr} \rightarrow \mathrm{H(arrLength)(St(Cntr))}]\\ \mathrm{Pc}' = \mathrm{Pc}+1\end{array}}{\mathtt{m} \vdash \ \mathrm{arraylength} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow < \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg, Pc}' >}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr)} = \textbf{null}\\ \mathit{getStateOnExc}(< \mathrm{H, Cntr, St, Reg, Pc} >, \ \mathtt{NullPntrExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \ \mathrm{arraylength} :< \mathrm{H, Cntr, St, Reg, Pc} > \hookrightarrow S}$$

The stack top element is popped from the stack. It must be a reference that points to an array. If the stack top element St(Cntr) is not **null**the length of the array arrLengthSt(Cntr) is fetched and pushed on the stack. If the stack top element St(Cntr) is **null**then a `NullPntrExc`is thrown.

8. instanceof

$$\frac{\begin{array}{l}\mathsf{subtype}\ (\mathrm{H.TypeOf}\ (\mathrm{St(Cntr)}), C)\\ \mathrm{St}' = \mathrm{St}[\oplus\mathrm{Cntr} \rightarrow 1]\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\text{instanceof } C :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

$$\frac{\begin{array}{l}\mathit{not}(\mathsf{subtype}\ (\mathrm{H.TypeOf}\ (\mathrm{St(Cntr)}), C)) \vee \mathrm{St(Cntr)} = \mathbf{null}\\ \mathrm{St}' = \mathrm{St}[\oplus\mathrm{Cntr} \rightarrow 0]\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \text{instanceof } \mathsf{C} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

The stack top is popped from the stack. If it is of subtype Cor is **null**, then the `1` is pushed on the stack, otherwise `0`.

9. checkcast

$$\frac{\begin{array}{l}\mathsf{subtype}\ (\mathrm{H.TypeOf}\ (\mathrm{St(Cntr)}), C) \vee \mathrm{St(Cntr)} = \mathbf{null}\\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \text{checkcast } C :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc}' >}$$

$$\frac{\begin{array}{l}\mathit{not}(\mathsf{subtype}\ (\mathrm{H.TypeOf}\ (\mathrm{St(Cntr)}), C))\\ \mathit{getStateOnExc}(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, \mathtt{CastExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \text{checkcast } C :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow S}$$

The stack top is popped from the stack. If it is not of subtype C an exception of type `CastExc`is thrown.

- Throw exception instruction. athrow

$$\frac{\begin{array}{l}\mathrm{St(Cntr)} \neq \mathbf{null}\\ \mathit{getStateOnExc}(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, \mathit{typeof}(\mathrm{St(Cntr)}), \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \text{athrow} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow S}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr)} = \mathbf{null}\\ \mathit{getStateOnExc}(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, \mathtt{NullPntrExc}, \mathtt{m.excHndlS}) = S\end{array}}{\mathtt{m} \vdash \text{athrow} :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} > \hookrightarrow S}$$

The stack top element must be a reference of an object of type `Throwable`. If there is a handler that protects this bytecode instruction from the exception thrown, the control is transfered to the instruction at which the exception handler starts. If the object on the stack top is **null**, a `NullPntrExc` is thrown.

- Method Invokation. invoke [2]

$$\frac{\begin{array}{l}\mathrm{St(Cntr} - meth.\mathsf{nArgs}) \neq \mathbf{null} \\ meth :< \mathrm{H}, 0, [\,], [\mathrm{St(Cntr} - meth.\mathsf{nArgs}), \ldots, \mathrm{St(Cntr)}], 0 >\Rightarrow< \mathrm{H}', \mathrm{Reg}' >^{norm} \mathrm{Res} \\ \\ \mathrm{Cntr}' = \mathrm{Cntr} - \mathtt{m}.\mathsf{nArgs} + 1 \\ \mathrm{St}' = \mathrm{St}[\oplus \mathrm{Cntr}' \rightarrow \mathrm{Res}] \\ \mathrm{Pc}' = \mathrm{Pc} + 1\end{array}}{\mathtt{m} \vdash \text{ invoke } meth :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >\hookrightarrow< \mathrm{H}', \mathrm{Cntr}', \mathrm{St}', \mathrm{Reg}, \mathrm{Pc}' >}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr} - meth.\mathsf{nArgs}) \neq \mathbf{null} \\ meth :< \mathrm{H}, 0, [\,], [\mathrm{St(Cntr} - meth.\mathsf{nArgs}), \ldots, \mathrm{St(Cntr)}], 0 >\Rightarrow< \mathrm{H}', \mathrm{Reg}' >^{exc} \mathrm{Exc} \\ \Rightarrow \\ getStateOnExc(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, typeof(\mathrm{Exc}), \mathtt{m}.\mathsf{excHndlS}) = S\end{array}}{\mathtt{m} \vdash \text{ invoke } meth :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >\hookrightarrow S}$$

$$\frac{\begin{array}{l}\mathrm{St(Cntr} - meth.\mathsf{nArgs}) = \mathbf{null} \\ getStateOnExc(< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, \ \mathtt{NullPntrExc}, \mathtt{m}.\mathsf{excHndlS}) = S\end{array}}{\mathtt{m} \vdash \text{ invoke } meth :< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >\hookrightarrow S}$$

The first top $meth.\mathsf{nArgs}$ elements in the operand stack St are popped from the operand stack. If St(Cntr - meth.nArgs) is not **null**, the invoked method is executed on the object St(Cntr - meth.nArgs) and where the first nArgs+ 1 elements of the list of its of local variables is initialised with St(Cntr - meth.nArgs) ... St(Cntr). In case that the execution of method $meth$ terminates normally, the return value Res of its execution is stored on the operand stack of the invoker. If the execution of of method $meth$ terminates because of an exception Exc, then the exception handler of the invoker is searched for a handler that can handle the exception. In case the object St(Cntr - meth.nArgs) on which the method $meth$ must be called is **null**, a `NullPntrExc`is thrown.

2.9 Representing bytecode programs as control flow graphs

This section will introduce a formalization of an unstructured program in terms of a control flow graph. The notion of a loop in a bytecode program will be also defined. Note that in the following, the control flow graph corresponds to a method body.

Recall from Section 2.4 that every method `m` has an array of bytecode instructions `m.body`. The $k-th$ instruction in the bytecode array `m.body` is denoted with `m.body`$[k]$. A method entry point instruction is an instruction at which an execution of a method starts. We assume that a method body has exactly one entry point and this is the first element in the method body `m.body`[0].

[2] only the case when the invoked method returns a value

The array of bytecode instructions of a method m determine the control flow graph $G(V, \rightarrow)$ of method m in which the vertices are the instructions of the method body, i.e.

$$V = \{ins \mid \exists k, 0 \leq k < \mathtt{m.body}.length \wedge ins = \mathtt{m.body}[k]\}$$

The following definition defines the set of edges in the control flow graph.

Definition 2.9.1 (Edge in control flow graph) *The set of edges $\rightarrow$ is a relation between the vertices elements*

$$\rightarrow : V * V$$

and is defined as follows:

$$\begin{array}{l}
(\mathtt{m.body}[j], \mathtt{m.body}[k]) \in \rightarrow \\
\Longleftrightarrow \\
\mathtt{m.body}[j] \neq \text{ return } \wedge (\\
\mathtt{m.body}[j] = \text{ if_cond } k \vee \\
\mathtt{m.body}[j] = \text{ goto } k \vee \\
\mathtt{m.body}[j] \neq \text{ goto } \wedge k = j + 1 \vee \\
\mathtt{m.body}[j] = \text{ putfield} \wedge \mathit{findExcHandler}(\ \mathtt{NullPntrExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ getfield} \wedge \mathit{findExcHandler}(\ \mathtt{NullPntrExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ type_astore} \wedge \mathit{findExcHandler}(\ \mathtt{NullPntrExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ type_astore} \wedge \mathit{findExcHandler}(\ \mathtt{ArrIndBndExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ type_aload} \wedge \mathit{findExcHandler}(\ \mathtt{NullPntrExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ type_aload} \wedge \mathit{findExcHandler}(\ \mathtt{ArrIndBndExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ invoke n} \wedge \mathit{findExcHandler}(\ \mathtt{NullPntrExc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ invoke n} \wedge \forall \mathtt{Exc}, \exists s, \mathtt{n.exceptions}[s] = \mathtt{Exc} \wedge \\
\qquad\qquad \mathit{findExcHandler}(\mathtt{Exc}, j, \mathtt{m.excHndlS}) = k \vee \\
\mathtt{m.body}[j] = \text{ athrow} \wedge \forall \mathtt{Exc}, \mathit{findExcHandler}(\mathtt{Exc}, j, \mathtt{m.excHndlS}) = k \vee \\
)
\end{array}$$

From the Def. 2.9.1 follows that there is an edge between two vertices $\mathtt{m.body}[j]$ and $\mathtt{m.body}[k]$ if they may execute immediately one after another. We say that $\mathtt{m.body}[j]$ is a predecessor of $\mathtt{m.body}[k]$ and that $\mathtt{m.body}[k]$ is a successor of $\mathtt{m.body}[j]$. The definition states the return instruction does not have successors. If $\mathtt{m.body}[j]$ is the jump instruction if_cond k then its successors are the instruction at index k in the method body $\mathtt{m.body}[k]$ and the instruction and the instruction $\mathtt{m.body}[j+1]$. From the definition, we also get that every instruction which potentially may throw an exception of type Exc has as successor the first instruction of the exception handler that may handle the exception type Exc. For instance, a successor of the instruction putfield is the exception handler entry point which can handle the NullPntrExc exception. The possible successors of the instruction athrow are the entry point of any exception handler in the method m. In the following, we will rather use the infix notation $\mathtt{m.body}[j] \rightarrow \mathtt{m.body}[k]$.

We assume that the control flow graph of every method is reducible, i.e. every loop has exactly one entry point. This actually is admissible as it is rarely the case that a compiler produce a bytecode with a non reducible control flow graph and the practice shows that even hand written code is usually reducible. However, there exist algorithms to transform a non reducible control flow graph into a reducible one. For more information on program control flow graphs, the curious reader may refer to [1]. The next definition identifies backedges in the reducible control flow graph (intuitively, the edge that goes from an instruction in a given loop in the control flow graph to the loop entry) with the special execution relation $\rightarrow^l$ as follows:

Definition 2.9.2 (Backedge Definition) *Assume we have the method* `m` *with body* `m.body` *which determine the control flow graph* $G(V, \rightarrow)$*. We assume also that the entry point of* G *is the vertice* `m.body`$[0]$*. In such a graph* G*, we say that* $loopEntry$: `instr` *is a loop entry instruction and* f : `instr` *is a loop end instruction of the same loop if the following conditions hold:*

- *for every execution path* P *from* `m.body`$[0]$ *to* f : `instr`*:* P = `m.body`$[0] \rightarrow^+ f$: `instr` *there exists a subpath which is a prefix of* P $subP$ = `m.body`$[0] \rightarrow^*$ $loopEntry$: `instr` *such that* f : `instr` $\notin$ $subP$
- *there is a path in which* $loopEntry$: `instr` *is executed immediately after the execution of* f : `instr` *(* f : `instr` $\rightarrow$ $loopEntry$: `instr`*)*

We denote the execution relation between f : `instr` *and* $loopEntry$: `instr` *with* f : `instr` $\rightarrow^l$ $loopEntry$: `instr` *and we say that* $\rightarrow^l$ *is a backedge.*

Note that in [1] reducibility is defined in terms of the dominator relation. Although not said exlicitely, the first condition in the upper definition corresponds to the dominator relation[3].

We illustrate the above definition with the control flow graph of the example from Fig. 3.1 in Fig. 2.2. In the figure, we rather show the execution relation between basic blocks which is a standard notion denoting a sequence of instructions which execute sequentially and where only the last one may be a jump and the first may be a target of a jump. The black edges represent a sequential execution relation, while dashed edges represent a backedge, i.e. the edge which stands for the execution relation between a final instruction (instruction at index `18`) in the bytecode cycle and the entry instruction of the cycle (instruction at index `19`).

[3] we decided to not introduce the standard definitions as it has several technical details for the exposition of which we would need more space and which are of not particular interest for the current thesis

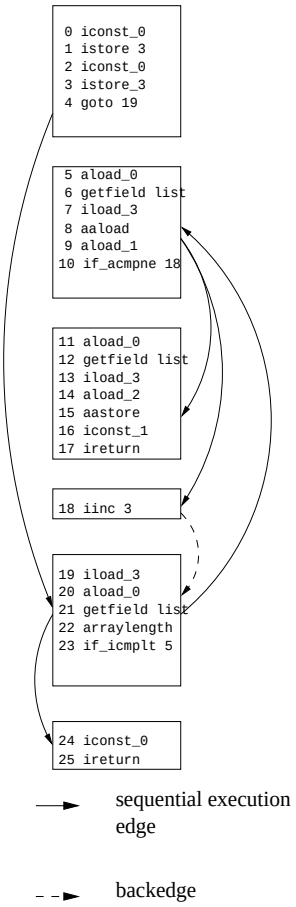

Figure 2.2: THE CONTROL FLOW GRAPH OF THE SOURCE PROGRAM FROM FIG.3.1

Chapter 3

Bytecode modeling language

3.1 Introduction

This section presents a bytecode level specification language, called for short BML and a compiler from a subset of the high level Java specification language JML to BML which from now we shall call JML2BML.

Before going further, we discuss what advocates the need of a low level specification language. Traditionally, specification languages were tailored for high level languages. Source specification allows to express complex functional or security properties about programs. Thus, they are successfully be used for software audit and validation. Still, source specification in the context of mobile code does not help a lot for several reasons.

First, the executable or interpreted code may not be accompanied by its specified source. Second, it is more reasonable for the code receiver to check the executable code than its source code, especially if he is not willing to trust the compiler. Third, if the client has complex requirements and even if the code respects them, in order to establish them, the code should be specified. Of course, for properties like well typedness this specification can be inferred automatically, but in the general case this problem is not decidable. Thus, for more sophisticated policies, an automatic inference will not work.

It is in this perspective, that we propose to make the Java bytecode benefit from the source specification by defining the BML language and a compiler from JML towards BML.

BML supports the most important features of JML. Thus, we can express functional properties of Java bytecode programs in the form of method pre and postconditions, class and object invariants, assertions for particular program points like loop invariants. To our knowledge BML does not have predecessors that are tailored to Java bytecode.

In section 3.2, we give an overview of the main features of JML. A de-

tailed overview of BML is given in section 3.4. As we stated before, we support also a compiler from the high level specification language JML into BML. The compilation process from JML to BML is discussed in section 3.6. The full specification of the new user defined Java attributes in which the JML specification is compiled is given in the appendix.

3.2 Overview of JML

JML [17] (short for Java Modeling Language) is a behavioral interface specification language tailored to Java applications which follows the design-by-contract approach (see [8]).

Over the last few years, JML has become the de facto specification language for Java source code programs. Several case studies have demonstrated that JML can be used to specify realistic industrial examples, and that the different tools allow to find errors in the implementations (see e.g. [9]). One of the reasons for its success is that JML uses a Java-like syntax. Other important factors for the success of JML are its expressiveness and flexibility.

JML is supported by several verification tools. Originally, it has been designed as a language of the runtime assertion checker [12] created by G.T. Leavens and . The JML runtime assertion checker compiles both the Java code and the JML specification into executable bytecode and thus, in this case, the verification consists in executing the resulting bytecode. Several static checkers based on formal logic exist which use JML as a specification language. Esc/java [23] whose first version used a subset of JML [1] is among the first tools supporting JML. Among the static checkers with JML are the Loop tool developed by the Formal group at the University of Nijmegen, the Jack tool developed at Gemplus, the Krakatoa tool created by the Coq group at Inria, France. The tool Daikon [15] tool uses a subset of JML for detecting loop invariants by run of programs. A detailed overview of the tools which support JML can be found in [10].

who are the others

Specifications in JML are written using different predicates which are side-effect free Java expressions, extended with specification-specific keywords. JML specifications are written as comments so they are not visible by Java compilers. The JML syntax is close to the Java syntax: JML extends the Java syntax with few keywords and operators. For introducing method precondition and postcondition the keywords **requires** and **ensures** are used respectively, **modifies** keyword introduces the locations that can be modified by the method, **loop_invariant** stands for a loop invariant, the **loop_modifies** keyword gives the locations modified by a loop etc. The latter is not standard in JML and is an extension introduced in [11]. Special JML operators are, for instance, **result** which stands for the value that a method returns if it is not void, the **old(expression)** operator designates the value of **expression** in the prestate of a method and is usually used in the method's postcondition.

[1] the current version of the tool esc/java 2 supports almost all JML constructs

Figure 3.1 gives an example of a Java class that models a list stored in a private array field. The method `replace` will search in the array for the first occurence of the object `obj1` passed as first argument and if found, it will be replaced with the object passed as second argument `obj2` and the method will return true; otherwise it returns false. Thus the method specification between lines 5 and 9 which exposes the method contract states the following. First the precondition (line 5) requires from any caller to assure that the instance variable `list` is not `null`. The frame condition (line 6) states that the method may only modify any of the elements in the instance field `list`. The method postcondition (lines 7—9) states the method will return `true` only if the replacement has been done. The method body contains a loop (lines 17—22) which is specified with a loop fame condition and a loop invariant (lines 13—16). The loop invariant (lines 14—16) says that all the elements of the list that are inspected up to now are different from the parameter object `obj1` as well as the local variable `i` is a valid index in the array `list`. The loop frame condition (line 13) states that only the local variable `i` and any element of the array field `list` may be modified in the loop.

```
1  public class ListArray {
2
3    private Object[] list;
4
5    //@ requires list != null;
6    //@ modifies list[*];
7    //@ ensures \result ==(\exists int i;
8    //@          0 <= i && i < list.length &&
9    //@          \old(list[i]) == obj1 && list[i] == obj2);
10   public boolean replace(Object obj1,Object obj2){
11     int i = 0;
12
13     //@ loop_modifies i, list[*];
14     //@ loop_invariant i <= list.length && i >=0
15     //@ && (\forall int k;0 <= k && k < i ==>
16     //@      list[k] != obj1);
17     for (i = 0; i < list.length; i++){
18       if ( list[i] == obj1){
19         list[i] = obj2;
20         return true;
21       }
22     }
23     return false;
24   }
25 }
```

Figure 3.1: CLASS ListArray WITH JML ANNOTATIONS

JML also allows the declaration of special JML variables, that are used only for specification purposes. These variables are declared in comments with the **ghost** modificator and may be used only in specification clauses. Those variables can also be assigned. Ghost variables are usually used for expressing properties which can not be expressed with the program variables.

Fig. 3.2 is an example for how ghost variables are used. The example shows the class `Transaction` which manages transactions in the program. The class is provided with a method for opening transactions `beginTransaction` and a method for closing transactions (`commitTransaction`). The specification declares a ghost variable `TRANS` (line 3) which keeps track if there is a running transaction or not, i.e. if the value of `TRANS` is 0 then there is no running transaction and if it has value 1 then there is a running transaction. The specification of the methods `beginTransaction` and `commitTransaction` models the property for no nested transactions. Thus, when the method `beginTransaction` is invoked the precondition (line 5) requires that there should be no running transaction and when the method is terminated the postcondition guarantees (line 6) that there is already a transaction running. We can also remark that the variable `TRANS` is set to its new value (line 8) in the body `beginTransaction`. Note that this high level property is difficult to express without the presence of the ghost variable `TRANS`.

```
1  public class Transaction {
2
3    //@ ghost static private int TRANS = 0;
4
5    //@ requires TRANS == 0;
6    //@ ensures TRANS == 1;
7    public void beginTransaction() {
8      //@ set TRANS = 1;
9        ...
10   }
11
12   //@ requires TRANS == 1;
13   //@ ensures TRANS == 0;
14   public void commitTransaction() {
15     //@ set TRANS = 0;
16       ...
17   }
18
19 }
```

Figure 3.2: SPECIFYING NO NESTED TRANSACTION PROPERTY WITH GHOST VARIABLE

A useful feature of JML is that it allows two kinds of method specification,

a *light* and *heavy* weight specification. An example for a *light* specification is the annotation of method `replace` (lines 5—9) in Fig. 3.1. The specification in the example states what is the expected behavior of the method and under what conditions it might be called. The user, however in JML, has also the possibility to write very detailed method specifications. This style of specification is called a *heavy* weight specification. It is introduced by the JML keywords **normal_behavior** and **exceptional_behavior**. As the keywords suggest every of them specifies a specific normal or exceptional behavior of a method. (see [21]).

The keyword **normal_behavior** introduces a precondition, frame condition and postcondition such that if the precondition holds in the prestate of the method then the method will terminate normally and the postcondition will hold in the poststate. Note that this clause guarantees that the method will not terminate on an exception and thus the exceptional postcondition for any kind of exception (i.e. for the exception class `Exception`) is **false**. An example for a *heavy* weight specification is given in Fig. 3.3. In the figure, method `divide` has two behaviors, one in case the method terminates normally (lines 11—14) and the other (lines 17—20) in case the method terminates by throwing an object reference of `ArithmeticException`. In the normal behavior case, the exceptional postcondition is ommitted specification as by default if the precondition (line 12) holds this assures that no exceptional termination is possible. Another observation over the example is that the exceptional behavior is introduced with the JML keyword **also**. The keyword **also** serves for introducing every new behavior of a method except the first one. Note that the keyword **also** is used in case a method overrides a method from the super class. In this case, the method specification (*heavy* or *light* weight) is preceded by the keyword **also** to indicate that the method should respect also the specification of the super method.

JML can be used to specify not only methods but also properties of a class or interfaces. A Java class may be specified with an invariant or history constraints. An invariant of a class is a predicate which holds at all visible states of every object of this class (see for the definition of visible state in the JML reference manual [13]). An invariant may be either static (i.e. talks only about static fields) or instance (talks about instance fields). A Class history constraints is a property which relates the initial and terminal state of every method in the corresponding class. The class `C` in Fig.3.3 has also an instance invariant which states that the instance variable `a` is always greater than `0`.

3.3 Design features of BML

Before proceeding with the syntax and semantics of BML, we would like to discuss the design choices made in the language. Particularly, we will see what are the benefits of our approach as well as the restrictions that we have to adopt. Now, we focus on the desired features of BML, how they compare to JML and what are the motivations that led us to these decisions:

- **Java compiler independance**

```
1  public class C {
2      int a;
3
4      //@ public instance invariant a > 0 ;
5
6      //@ requires val > 0 ;
7      public C(int val){
8         a = val ;
9      }
10
11     //@ public normal_behavior
12     //@ requires b > 0;
13     //@ modifies a;
14     //@ ensures  a == \old(a) / b;
15     //@
16     //@ also
17     //@ public exceptional_behavior
18     //@ requires b == 0;
19     //@ modifies \nothing;
20     //@ exsures (ArithmeticException) a == \old(a);
21     public void divide(int b) {
22         a = a / b;
23     }
24 }
```

Figure 3.3: An example for a method with a heavy weight specification in JML

Class files containing BML specification must not depend on any non optimizing compiler.

To do this, the process of the Java source compilation is separate from the JML compilation. More particularly, the JML2BML(short for the compiler from JML to BML) compiler takes as input a Java source file annotated with JML specification and its Java class produced by a non optimizing compiler containing a debug information.

- **JVM compatibility**
  The class files augmented with the BML specification must be executable by any implementation of the JVM specification. Because the JVM specification does not allow inlining of any user specific data in the bytecode instructions BML annotations must be stored separately from the method body (the list of bytecode instructions which represents its body).

  In particular, the BML specification is written in the so called user defined attributes in the class file. The JVM specification defines the format of

those attributes and mandates that any user specific information should be stored in such attributes. Note, that attribute which encodes the specification referring to a particular bytecode instruction contains information about the index of this instruction. For instance, BML loop invariants are stored in a user defined attribute in the class file format which contains the invariant as well as the index of the entry point instruction of the loop.

Thus, BML encoding is different from the encoding of JML specification where annotations are written directly in the source text as comments at a particular point in the program text or accompany a particular program structure. For instance, in Fig. 3.1 the reader may notice that the loop specification refers to the control structure which follows after the specification and which corresponds to the loop. This is possible first because the Java source language is structured, and second because writing comments in the source text does not violate the Java or the JVM specifications.

- **Compactness** and **Efficiency**
  Although opposite, we consider those two features together because they are mutually dependent. By the first, we mean that the class files augmented with BML should be as compact as possible. The second feature refers to that tools supporting BML should not be slowed down by the processing of the BML specification and more precisely we refer verification condition generator tools. This is an important condition if verification is done on devices with limited resources.

  For fulfilling these conditions, BML is designed to correspond to a subset of the desugared version of JML. In particular, it brings a relative compactness of the class file as well as makes the verification procedure more efficient.

  We first see in what sense this allows the class file compactness. Because every kind of BML specification clause is stored in a different user defined attribute, supporting all constructs of JML would mean that class files may contain a large number of attributes which would increase considerably the class file size. Of course, the size of a BML specification depends also on how much detailed is the specification, the more detailed it is, the larger size it would have.

  Because BML corresponds to a desugared version of JML, this means that on verification time the BML specification does not need much processing and thus, it can be easily translated to the data structures used in the verification scheme. This makes BML suitable for verification on devices with limitted resources.

As the attentive reader has noticed, we impose some restrictions on the structure of the class file format and the bytecode programs. These restrictions are the following:

- **Debug Information**
  A requirement to the class file format is that it must contain a debug

information, more particularly the **Line_Number_Table** and **Local_Variable_Table** attributes. The presence in the Java class file format of these attribute is optional [25], yet almost all standard non optimizing compilers can generate these data. The **Line_Number_Table** is part of the compilation of a method and describes the link between the Java source lines and the Java bytecode. The **Local_Variable_Table** describes the local variables that appear in a method. This debug information is necessary for the compiler from JML to BML, as we shall see later in Section 3.6.

- **Reducible control flow graph**
  The control flow graph corresponding to the list of bytecode instructions resulting from the compilation of a method body must be a reducible control flow graph. An intuition to the notion of reducibility is that every cycle in the graph must have exactly one entry point, or in other words a cycle can not be jumped from outside inside (see [1] for the definition of reducibility). This condition is necessary for the compilation phase of the loop invariants as well as for the verification procedure (Section 5). Note, that this restriction is realistic as nonoptomizing Java compilers produce reducible control flow graphs and in practice even hand written code is in most cases reducible.

3.4 The subset of JML supported in BML

BML corresponds to a representative subset of JML and is expressive enough for most purposes including the description of non trivial functional and security properties. The following Section 3.4.1 gives the notation conventions adopted here and Section 3.4.2 gives the formal grammar of BML as well as an informal description of its semantics.

3.4.1 Notation convention

- Nonterminals are written with a *italics* font
- Terminals are written with a **boldface** font
- brackets [ ] surround optional text.

3.4.2 BML Grammar

$constants_{bml}$ ::= *intLiteral* | *signedIntLiteral* | **null** | *ident*

signedIntLiteral ::= $+$*nonZerodigit*[*digits*] | $-$*nonZerodigit*[*digits*]

intLiteral ::= *digit* | *nonZerodigit*[*digits*]

digits ::= *digit*[*digits*]

digit ::= **0** | *nonZerodigit*

nonZerodigit ::= **1** | ... | **9**

ident ::= # *intLiteral*

boundVar ::= **bv_***intLiteral*

E_{bml} ::= $constants_{bml}$
| **reg**(*digits*)
| E_{bml}**.***ident*
| *ident*
| **arrayAccess**(E_{bml}, E_{bml})
| E_{bml} *op* E_{bml}
| **cntr**
| **st**(E_{bml})
| **\old(**E_{bml}**)**
| **\EXC**
| **\result**
| *boundVar*
| **\typeof(**E_{bml}**)**
| **\type(***ident***)**
| **\elemtype(**E_{bml}**)**
| **\TYPE**

op ::= **+** | **-** | **mult** | **div** | **rem**

$\mathcal{R}$ ::= $=|\neq|\leq|\leq|\geq|>|<:$

P_{bml} ::= E_{bml} $\mathcal{R}$ E_{bml}
| **true**
| **false**
| *not* P_{bml}
| $P_{bml} \wedge P_{bml}$
| $P_{bml} \vee P_{bml}$
| $P_{bml} \Rightarrow P_{bml}$
| $P_{bml} \iff P_{bml}$
| $\forall$ *boundVar*, P_{bml}
| $\exists$ *boundVar*, P_{bml}

classSpec ::= **invariant** *modifier* P_{bml}
| **classConstraint** P_{bml}
| **declare ghost** *ident ident*

modifier ::= **instance** | **static**

intraMethodSpec ::= **atIndex** *nat*;
assertion;

assertion ::= *loopSpec*

methodSpec ::= *specCase*
| *specCase* **also** *methodSpec*

specCase ::= {|
requires P_{bml};
modifies *list locations*;
ensures P_{bml};
exsuresList
|}

exsuresList ::= [] | **exsures** (*ident*) P_{bml}; *exsuresList*

locations ::= E_{bml}.*ident*
| **reg**(i)
| *arrayModAt*(E_{bml}, *specIndex*)
| **everything**
| **nothing**

specIndex ::= all | $i_1..i_2$ | i

bmlKeyWords ::= **requires**
| **ensures**
| **modifies**
| **assert**
| **set**
| **exsures**
| **also**
| **invariant**
| **classConstraint**
| **atIndex**
| **loop_invariant**
| **loop_decreases**
| **loop_modifies**
| \ **typeof**
| \ **elemtype**
| **TYPE**
| **result**

3.4.3 Syntax and semantics of BML

In the following, we will discuss informally the semantics of the syntax structures of BML. Note that most of them have an identical counterpart in JML and their semantics in both languages is the same. In the following, we will concentrate more on the specific syntactic features of BML and will just briefly comment the BML features which it inherits from JML like for instance, preconditions

and which we have mentioned already[2].

BML expressions

Among the common features of BML and JML are the following expressions: field access expressions E_{bml}.*ident*, array access (**arrayAccess**(E^1_{bml}, E^2_{bml})), arithmetic expressions (E_{bml} *op* E_{bml}). Like JML, BML may talk about expression types. As the BML grammar shows, **typeof(**E_{bml}**)** denotes the dynamic type of the expression E_{bml}, **type(***ident***)** is the class described at index *ident* in the constant pool of the corresponding class file. The construction **elemtype(**E_{bml}**)** denotes the type of the elements of the array E_{bml}, and **TYPE** , like in JML, stands for the Java type `java.lang.Class`.

However, expressions in JML and BML differ in the syntax more particularly this is true for identifiers of local variables, method parameters, field and class identifiers. In JML, all these constructs are represented syntactically by their names in the Java source file. This is not the case in BML.

We first look at the syntax of method local variables and parameters. The class file format stores information for them in the array of local variables. That is why, both method parameters and local variables are represented in BML with the construct **reg**(i) which refers to the element at index i in the array of local variables of a method. Note that the `this` expression in BML is encoded as **reg**(0). This is because the reference to the current object is stored at index 0 in the array of local variables.

Field and class identifiers in BML are encoded by the respective number in the constant pool table of the class file. For instance, the syntax of field access expressions in BML is E_{bml}.*ident* which stands for the value in the field at index *ident* in the class constant pool for the reference denoted by the expression E_{bml}.

The BML grammar defines the syntax of identifiers differently from their usual syntax. Particularly, in BML those are positive numbers preceded by the symbol # while usually the syntax of identifiers is a chain of characters which always starts with a letter. The reason for this choice in BML is that identifiers in BML are indexes in the constant pool table of the corresponding class.

Fig.3.4 gives the bytecode as well as the BML specification of the code presented in Fig.3.3. As we can see, the names of the local variables, field and class names are compiled as described above. For instance, at line 3 in the specification we can see the precondition of the first specification case. It talks about **reg**(1) which is the element in the array of local variables of the method and which is the compilation of the method parameter `b` (see Fig. 3.3).

About the syntax of class names, after the **exsures** clause at line 5 follows a BML identifier (#25) enclosed in parenthesis. This is the constant pool index at which the Java exception type `java.lang.Exception` is declared.

A particular feature of BML is that it supports stack expressions which do not have a counterpart in JML. These expressions are related to the way

[2]because we have already discussed in Section 3.2 the JML constructs for pre and post-conditions, loop invariants, operators like **old**, **result**, etc. we would not return to them anymore as their semantics is exactly the same as the one of JML

```
1
2  Class instance invariant:
3     lv(0).#19 > 0;
4
5
6  Method specification:
7     {|
8      requires lv(1) > 0;
9      modifies lv(0).#19;
10     ensures  lv(0).#19 == \old( lv(0).#19 ) / lv(1);
11     exsures  ( #25 ) false;
12    |}
13    also
14    {|
15     requires lv(1) == 0;
16     modifies \nothing;
17     ensures false;
18     exsures ( #26 ) lv(0).#19  == \old(lv(0).#19);
19    |}
20
21  public void divide(int lv(1))
22        0 aload 0
23        1 dup
24        2 getfield #19 // instance field a
25        3 iload 1
26        4 idiv
27        5 putfield #19 // instance field a
28        6 return
```

Figure 3.4: An example for a heavy weight specification in BML

in which the virtual machine works, i.e. we refer to the stack and the stack counter. Because intermediate calculations are done by using the stack, often we will need stack expressions in order to characterise the states before and after an instruction execution. Stack expressions are represented in BML as follows:

- **cntr** represents the stack counter.

- **st**(E_{bml}) stands for the element in the operand stack at position E_{bml}. For instance, the element below the stack top is represented with **st**(**cntr** − 1) Note that those expressions may appear in predicates that refer to intermediate instructions in the bytecode.

BML predicates

The properties that our bytecode language can express are from first order predicate logic. The formal grammar of the predicates is given by the nonterminal P_{bml}. From the formal syntax, we can notice that BML supports the standard logical connectors $\wedge, \vee, \Rightarrow$, existential $\exists$ and universal quantification $\forall$ as well as standard relation between the expressions of our language like $\neq, =, \leq, \leq \ldots$

Class Specification

The nonterminal *classSpec* in the BML grammar defines syntax constructs for the support of class specification. Note that these specification features exist in JML and have exactly the same semantics. However, we give a brief description of the syntax. Class invariants are introduced by the terminal **invariant**, history constraints are introduced by the terminal **classConstraint**. For instance, in Fig. 3.4 we can see the BML invariant resulting from the compilation of the JML specification in Fig. 3.3.

Like JML, BML supports ghost variables. As we can notice in the BML grammar, their syntax in the grammar is **declare ghost** *ident ident*. The first *ident* is the index in the constant pool which contains a description of the type of the ghost field. The second *ident* is the index in the constant pool which corresponds to the name of the ghost field.

Frame conditions

BML supports frame conditions for methods and loops. These have exactly the same semantics as in JML. The nonterminal that defines the syntax for frameconditions is *locations*. We look now what are the syntax constructs that may appear in the frame condition:

- E_{bml}**.***ident* states that the method or loop modifies the value of the field at index *ident* in the constant pool for the reference denoted by E_{bml}
- **reg**(i) states that the local variable may modified by a loop. Note that this kind of modified expression makes sense only for expressions modified in a loop. Indeed, a modification of a local variable does not make sense for a method frame condition, as methods in Java are called by value, and thus, a method can not cause a modification of a local variable that is observable from the outside of the method.
- *arrayModAt*$(E_{bml}, specIndex)$ states that the components at the indexes specified by *specIndex* in the array denoted by E_{bml} may be modified. The indexes of the array components that may be modified *specIndex* have the following syntax:
  - i is the index of the component at index i. For instance, *arrayModAt*(E_{bml}, i) means that the array component at index i might be modified.

  - all specifies that all the components of the array may be modified, i.e. the expression $arrayModAt(E_{bml}, \text{all})$ means that any element in the array may potentially be modified.
  - $i_1..i_2$ specifies the interval of array components between the index i_1 and i_2.

- **everything** states that every location might be modified by the method or loop
- **nothing** states that no location might be modified by a method or loop

Inter — method specification

In this subsection, we will focus on the method specification which is visible by the other methods in the program or in other words the method pre, post and frame conditions. The syntax of those constructs is given by the nonterminal *methodSpec*. As their meaning is exactly the same as in JML and we have already discussed the latter in Section 3.2, we shall not spend more lines here on those.

The part of the method specification which deserves more attention is the syntax of heavy weight method specification in BML. In Section 3.2, we saw that JML supports syntactic sugar for the definition of the normal and exceptional behavior of a method. The syntax BML does not support these syntactic constructs but rather supports their desugared version (see [30] for a detailed specification of the JML desugaring process). A specification in BML may declare several method specification cases like in JML. The syntactic structure of a specification case is defined by the nonterminal *specCase*.

We illustrate this with an example in Fig. 3.4. In the figure, we remark that BML does not have the syntactic sugar for normal and exceptional behavior. On the contrary, the specification cases now explicitely declare their behavior. The first specification case (the first bunch of specification enclosed in {| |}) corresponds to the **normal_behavior** specification case in the code from Fig. 3.3. Note that it does not have an analog for the JML keyword **normal_behavior** and that it declares explicitely what is the behavior of the method in this case, i.e. the exceptional postcondition is declared **false** for any exceptional termination.

The second specification case in Fig.3.4 corresponds to the **exceptional_behavior** case of the source code specification in Fig.3.3. It also specifies explicitely all details of the expected behavior of the method, i.e. the method postcondition is declared to be **false**.

Intra — method specification

As we can see from the formal grammar in subsection 3.4.2, BML allows to specify a property that must hold at particular program point inside a method body. The nonterminal which describes the grammar of assertions is *intraMethodSpec*.

Note that a particularity of BML specification, i.e. loop specifications or assertion at particular program point contains information about the point in the method body at which it refers. For instance, the loop specification in BML given by the nonterminal *loopSpec* may contain apart from the loop invariant predicate (**loop_invariant**), the list of modified variables (**loop_modifies**) and the decreasing expression (**loop_decreases**) but also the index of the loop entry point instruction (**atIndex**).

We illustrate this with the example in Fig. 3.5 which represents the bytecode and the BML specification from the example in Fig. 3.1. The first line of the BML specification specifies that the loop entry is the instruction at index 19 in the array of bytecode instructions. The predicate representing the loop invariant introduced by the keword **loop_invariant** respects the syntax for BML expressions and predicates that we described above.

3.5 Well formed BML specification

In the previous Section 3.4, we gave the formal grammar of BML. However, we are interested in a strict subset of the specifications that can be generated from this grammar. In particular, we want that a BML specification is well typed and respects structural constraints. The constraints that we impose here are similar to the type and structural constraints that the bytecode verifier imposes over the class file format.

Examples for type constraints that a valid BML specification must respect :

- the array expression **arrayAccess**(E^1_{bml}, E^2_{bml}) must be such that E^1_{bml} is of array type and E^2_{bml} is of integer type.
- the field access expression E_{bml}.*ident* is such that E_{bml} is of subtype of the class where the field described by the constant pool element at index *ident* is declared
- For any expression $E^1_{bml} op E^2_{bml}$, E^1_{bml} and E^2_{bml} must be of a numeric type.
- in the predicate $E^1_{bml} r E^2_{bml}$ where $r = \leq, <, \geq, >$ the expressions E^1_{bml} and E^2_{bml} must be of numerical type.
- in the predicate $E^1_{bml} <: E^2_{bml}$, the expressions E^1_{bml} and E^2_{bml} must be of type **TYPE** (which is the same as `java.lang.Class`).
- the expression **elemtype**(E_{bml}) must be such that E_{bml} has an array type.
- etc.

Example for structural constraint are :

```
1
2
3  Loop specification :
4
5      atIndex 19;
6      loop_modifies lv(0).#19[*], lv(3);
7      loop_invariant
8        lv(3) >= 0 &&
9        lv(3) < lv(0).#19.arrLength &&
10       \forall  bv_1 ;
11                ( bv_1 >= 0 &&
12                bv_1 < lv(0).#19.arrLength ==>
13                     lv(0).#19[bv_1] != lv(1) )
14
15  public int replace(Object  lv(1),Object lv(2) )
16   0 const 0
17   1 store 3
18   2 const 0
19   3 store 3
20   4 goto 19
21   5 load 0
22   6 getfield #19 // instance field list
23   7 load 3
24   8 aaload
25   9 load 1
26  10 if_acmpne 18
27  11 load 0
28  12 getfield #19 // instance field list
29  13 load 3
30  14 load 2
31  15 aastore
32  16 const 1
33  17 return
34  18 iinc 3
35  19 load 3    // loop entry
36  20 load 0
37  21 getfield #19 // instance field list
38  22 arraylength
39  23 if_icmplt 5
40  24 const 0
41  25 return
```

Figure 3.5: An example for a loop specification in BML

- All references to the constant pool must be to an entry of the appropriate type. For example: the field access expression E_{bml}.*ident* is such that the *ident* must reference a field in the constant pool; or for the expression **type**(*ident*)**, *ident*must be a reference to a constant class in the constant pool

- every *ident* in a BML specification must be a correct index in the constant pool table.

- if the expression **reg**(i) appears in a method BML specification, then i must be a valid index in the array of local variables of the method

An extension of the bytecode verifier may perform the checks if a BML specification respects this kind of structural and type constraints. However, we have not worked on this problem and is a good candidate for a future work. For the curious reader, it will be certainly of interest to turn to the Java Virtual Machine specification [25] which contains the official specification of the Java bytecode verifier or to the existing literature on bytecode verification (see the overview article [24])

3.6 Compiling JML into BML

In this section, we turn to the JML2BML compiler. As we shall see, the compilation consists of several phases, namely compiling the Java source file, preprocessing of the JML specification, resolution and linking of names, locating the position of intra — method specification, processing of boolean expressions and finally encoding the BML specification in user defined class file attributes. (their structure is predefined by JVMS). In the following, we look in details at the phases of the compilation process:

1. Compilation of the Java source file
   This can be done by any Java compiler that supplies for every method in the generated class file the **Line_Number_Table**
   and **Local_Variable_Table** attributes. Those attributes are important for the next phases of the JML compilation.

2. Compilation of Ghost field declarations
   JML specification is invisible by the Java compilers. Thus Java compilers omit the compilation of ghost variables declaration. That is why it is the responsibility of the JML2BML compiler to do this work. For instance, the compilation of the declaration of the ghost variable from Fig. 3.2 is given in Fig.3.6 which shows the data structure **Ghost_field_Attribute** in which the information about the field `TRANS` is encoded in the class file format. Note that, the constant pool indexes **#18** and **#19** which contain its description were not in the constant pool table of the class file `Transaction.class` before running the JML2BML compiler on it.

```
Ghost_field_Attribute {
    ...
    {  access_flag 10;
       name_ index = #18;
       descriptor_index = #19
    } ghost[1];
}
```

- **access_flag**: The kind of access that is allowed to the field
- **name_index**: The index in the constant pool which contains information about the source name of the field
- **descriptor_index**: The index in the constant pool which contains information about the name of the field type

Figure 3.6: Compilation of ghost variable declaration

3. Desugaring of the JML specification
   The phase consists in converting the JML method heavy-weight behaviours and the light - weight non complete specification into BML specification cases. It corresponds to part of the standard JML desugaring as described in [30]. For instance, the BML compiler will produce from the specification in Fig.3.3 the BML specification given in Fig.3.4

4. Linking with source data structures
   When the JML specification is desugared, we are ready for the linking and resolving phases. In this stage, the JML specification gets into an intermediate format in which the identifiers are resolved to their corresponding data structures in the class file. The Java and JML source identifiers are linked with their identifiers on bytecode level, namely with the corresponding indexes either from the constant pool or the array of local variables described in the **Local_Variable_Table** attribute.

   For instance, consider once again the example in Fig. 3.3 and more particularly the first specification case of method `divide` whose precondition `b > 0` contains the method parameter identifier `b`. In the linking phase, the identifier `b` is resolved to the local variable **reg**(1) in the array of local variables for the method `divide`. We have a similar situation with the postcondition `a == \old(a) / b` which mentions also the field `a` of the current object. The field name `a` is compiled to the index in the class constant pool which describes the constant field reference. The result of the linking process is in Fig.3.4.

   If, in the JML specification a field identifier appears for which no constant pool index exists, it is added in the constant pool and the identifier in question is compiled to the new constant pool index. This happens when

declarations of JML ghost fields are compiled.

5. Locating the points for the intra —method specification

   In this phase the specification parts like the loop invariants and the assertions which should hold at a certain point in the source program must be associated to the respective program point in the bytecode. For this, the **Line_Number_Table** attribute is used. The **Line_Number_Table** attribute describes the correspondence between the Java source line and the instructions of its respective bytecode. In particular, for every line in the Java source code the **Line_Number_Table** specifies the index of the beginning of the basic block[3] in the bytecode which corresponds to the source line. Note however, that a source line may correspond to more than one instruction in the **Line_Number_Table**.

   This poses problems for identifying loop entry instruction of a loop in the bytecode which corresponds to a particular loop in the source code. For instance, for method `replace` in the Java source example in Fig. 3.1 the java compiler will produce two lines in the **Line_Number_Table** which correspond to the source line **17** as shown in Fig. 3.7. The problem is that none of the basic bloks determined by instructions **2** and **18** contain the loop entry instruction of the compilation of the loop at line **17** in Fig. 3.1. Actually, the loop entry instruction in the bytecode in Fig. 3.5 (remember that this is the compilation in bytecode of the Java source in Fig. 3.1) which corresponds to the in the bytecode is at index **19**.

   Thus for identifying loop entry instruction corresponding to a particular loop in the source code, we use an heuristics. It consists in looking for the first bytecode loop entry instruction starting from one of the **start_pc** indexes (if there is more than one) corresponding to the start line of the source loop in the **Line_Number_Table**. The algorithm works under the assumption that the control flow graph of the method bytecode is reducible. This assumption guarantees that the first loop entry instruction found starting the search from an index in the **Line_Number_Table** corresponding to the first line of a source loop will be the loop entry corresponding to this source loop. However, we do not have a formal argumentation for this algorithm because it depends on the particular implementation of the compiler. From our experiments, the heuristic works successfully for the Java Sun non optimizing compiler.

une presentation tres laide

6. Compilation of the JML boolean expressions into BML

   Another important issue in this stage of the JML compilation is how the type differences on source and bytecode level are treated. By type

[3] a basic block is a sequence of instructions which does not contain jumps except may be for the last instruction and neither contains target of jumps except for the first instruction. This notion comes from the compiler community and more information on this one can find at [1]

Line_Number_Table

start_pc	**line**
...	
2	**17**
18	**17**

Figure 3.7: **Line_Number_Table** FOR THE METHOD `replace` IN FIG. 3.1

differences we refer to the fact that the JVM (Java Virtual Machine) does not provide direct support for integral types like byte, short, char, neither for boolean. Those types are rather encoded as integers in the bytecode. Concretely, this means that if a Java source variable has a boolean type it will be compiled to a variable with an integer type.

For instance, in the example for the method `replace` and its specification in Fig.3.1 the postcondition states the equality between the JML expression **result** and a predicate. This is correct as the method `replace` in the Java source is declared with return type boolean and thus, the expression **result** has type boolean. Still, the bytecode resulting from the compilation of the method `replace` returns a value of type integer. This means that the JML compiler has to "make more effort" than simply compiling the left and right side of the equality in the postcondition, otherwise its compilation will not make sense as it will not be well typed. Actually, if the JML specification contains program boolean expressions that the Java compiler will compile to bytecode expression with an integer type, the JML compiler will also compile them in integer expressions and will transform the specification condition in equivalent one[4].

Finally, the compilation of the postcondition of method `replace` is given in Fig. 3.8. From the postcondition compilation, one can see that the expression **result** has integer type and the equality between the boolean expressions in the postcondition in Fig.3.1 is compiled into logical equivalence.

7. Encoding BML specification into user defined class attributes
   The specification expression and predicates are compiled in binary form using tags in the standard way. The compilation of an expression is a tag followed by the compilation of its subexpressions.

   Method specifications, class invariants, loop invariants are newly defined attributes in the class file. For example, the specifications of all the loops in a method are compiled to a unique method attribute whose syntax

[4] when generating proof obligations we add for every source boolean expression an assumption that it must be equal to 0 or 1. A reasonable compiler would encode boolean values in a similar way

$$\backslash\mathbf{result} = 1$$

$$\Longleftrightarrow$$

$$\exists \mathbf{bv\_0}, \left(\begin{array}{l} 0 \leq \mathbf{bv\_0} \wedge \\ \mathbf{bv\_0} < len(\#19(\mathbf{reg}(0))) \wedge \\ \mathbf{arrayAccess}(\#19(\mathbf{reg}(0)), \mathbf{bv\_0}) = \mathbf{reg}(1) \end{array} \right)$$

Figure 3.8: The compilation of the postcondition in Fig. 3.1

```
JMLLoop_specification_attribute {
    ...
    {  u2 index;
       u2 modifies_count;
       formula modifies[modifies_count];
       formula invariant;
       expression decreases;
    } loop[loop_count];
}
```

- **index**: The index in the `LineNumberTable` where the beginning of the corresponding loop is described
- **modifies**[]: The array of locations that may be modified
- **invariant** : The predicate that is the loop invariant. It is a compilation of the JML formula in the low level specification language
- **decreases**: The expression which decreases at every loop iteration

Figure 3.9: Structure of the Loop Attribute

is given in Fig. 3.9. This attribute is an array of data structures each describing a single loop from the method source code. From the figure, we notice that every element describing the specification for a particular loop contains the index of the corresponding loop entry instruction **index**, the loop modifies clause (**modifies**), the loop invariant (**invariant**), an expression which guarantees termination (**decreases**).

Chapter 4

Assertion language for the verification condition generator

In this chapter we shall focus on a particular fragment of BML which will be extended with few new constructs. The part of BML in question is the assertion language that our verification condition generator manipulates as we shall see in the next Chapter **??**.

The assertion language presented here will abstract from most of the BML specification clauses described in Section 3.4. Our interest will be focused only on method and loop specification. Some parts of BML will be completely ignored either for keeping things simple or because those parts are desugared and result into the BML fragment of interest. For instance, we do not consider here multiple method specification cases, neither assertions in particular program point for the first reason. The assertion language presented here discards also class invariants and history constraints because they boil down to method pre and postconditions.

The rest of this chapter is organized as follows. Section 4.1 presents what is exactly the BML fragment of interest and its extensions. Section 4.4 shows how we encode method and loop specification as well as presents a discussion how some of the ignored BML specification constructs are transformed into method pre and postconditions. The last two sections are concentrated on the formal meaning of the assertion language, i.e. Section 4.2 defines the substitution for the assertion language and Section 4.3 gives formal semantics of the assertion language.

4.1 The assertion language

The assertion language in which we are interested corresponds to the BML expressions (nonterminal E_{bml}) and predicates (nonterminal P_{bml}) extended with several new constructs. The extensions that we add are the following:

- Extensions to expressions. The assertion language that we present here must be suitable for the verification condition calculus. Because the verification calculus talks about updated field and array access we should be able to express them in the assertion language. Thus we extend the grammar of BML expression with the following constructs concerning update of fields and arrays :
  - update field access expression $f[\oplus E_{bml} \rightarrow E_{bml}](E_{bml})$.
  - update array access expression
    $\text{arrAccess}[\oplus(E_{bml}, E_{bml}) \rightarrow E_{bml}](E_{bml}, E_{bml})$

  The verification calculus will need to talk about reference values. Thus we extend the BML expression grammar to support reference values *RefVal*. Note that in the following integers **int** and *RefVal* will be referred to with *Values*.

- Extensions to predicates. Our bytecode language is object oriented and thus supports new object creation. Thus we will need a means for expressing that a new object has been created during the method execution.

  We extend the language of BML formulas with a new user defined predicate **instances**(*RefVal*). Informally, the semantics of the predicate **instances**(`ref`) where `ref` $\in$ *RefVal* means that the reference `ref` has been allocated when the current method started execution.

The assertion language will use the names of fields and classes for the sake of readability instead of their corresponding indexes in the constant pool as is in BML.

We would like to discuss in the following how and why BML constructs like class invariants and history constraints can be expressed as method pre and postconditions:

- Class invariants. A class invariant (**invariant**) is a property that must hold at every visible state of the class. This means that a class invariant must hold when a method is called and also must be established at the end of a method execution. A class invariant must be established in the poststate of the constructor of this class. Thus the semantics of a class invariant is part of the pre and postcondition of every method and is a part of the postcondition of the constructor of the class.

- History constraints. A class history constraint (**classConstraint**) gives a relation between the pre and poststate of every method in the class. A class history constraint thus can be expressed as a postcondition of every method in the class.

4.2 Substitution

In this section we focus on how substitution is defined in our assertion language. Basically, it is is defined inductively in a standard way over the expression structure. Still, we extend substitution to deal with field and array update as follows:

$$E_{bml}[f \leftarrow f[\oplus E_{bml} \rightarrow E_{bml}]]$$

This substitution does not affect any of the ground expressions,, i.e. it does not affect local variables (**reg**(i)), the constants of our language (*constants*), the stack counter (**cntr**), the result expression (**result**), the thrown exception instance variable (**EXC**). For instance, the following substitution does not change **reg**(1):

$$\mathbf{reg}(1)[f \leftarrow f[\oplus E_{bml} \rightarrow E_{bml}]] = \mathbf{reg}(1)$$

Field substitution affects only field objects as we see in the following:

$$E_{bml}.f^1[f^2 \leftarrow f^2[\oplus E^1_{bml} \longrightarrow E^2_{bml}]] =$$

$$\begin{cases} E_{bml}.f^1 & if\ f^1 \neq f^2 \\ E_{bml}.f^2[\oplus E^1_{bml} \longrightarrow E^2_{bml}] & else \end{cases}$$

$$E_{bml}.f^1[\oplus E^1_{bml} \rightarrow E^2_{bml}][f^2 \leftarrow f^2[\oplus E^3_{bml} \rightarrow E^4_{bml}]] =$$

$$\begin{cases} f^1[\oplus E^1_{bml}[f^2 \leftarrow f^2[\oplus E^3_{bml} \rightarrow E^4_{bml}]] \rightarrow E^2_{bml}[f^2 \leftarrow f^2[\oplus E^3_{bml} \rightarrow E^4_{bml}]]] & if\ f^1 \neq f^2 \\ f^1\ \begin{array}{l}[\oplus E^1_{bml}[f^2 \leftarrow f^2[\oplus E^3_{bml} \rightarrow E^4_{bml}]] \longrightarrow E^2_{bml}[f^2 \leftarrow f^2[\oplus E^3_{bml} \rightarrow E^4_{bml}]]] \\ [\oplus E^3_{bml} \longrightarrow E^4_{bml}]\end{array} & else \end{cases}$$

For example, consider the following substitution expression:

$$\mathbf{reg}(1).f[f \leftarrow f[\oplus \mathbf{reg}(2) \rightarrow 3]]$$

This results in the new expression :

$$\mathbf{reg}(1).f[\oplus \mathbf{reg}(2) \rightarrow 3]$$

The same kind of substitution is allowed for array access expressions, where the array object arrAccess can be updated.

4.3 Interpretation

We discuss the evaluation of expressions and interpretation of predicates in a particular program state configuration. Thus, we first define a function for

expression evaluation, as well as a function which for a given state and predicate returns the interpretation of the given predicate in the given state. The function *eval* which evaluates expressions in a state has the following signature:

$$eval : E_{bml} \rightarrow S \rightarrow S \rightharpoonup Values \cup JType$$

Note that the evaluation function is partial and takes as arguments an expression of the assertion language presented in the previuos Section 4.1 and two states (see Section 2.6) and returns a value as defined in Section 2.5.

what is the impact of the evaluation partiallity

Definition 4.3.0.1 (Evaluation of expressions) *The evaluation in a state* $s =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *or* $s =< \mathrm{H}, \mathrm{Reg} >^{final}$ *Final of an expression* E_{bml} *w.r.t. an initial state* $s_0 =< \mathrm{H}_0, 0, [\,], \mathrm{Reg}, 0 >$ *is denoted with* $\|E_{bml}\|_{s_0,s}$ *and is defined inductively over the grammar of expressions* E_{bml} *as follows:*

$$\|v\|_{s_0,s} = v$$
$$where\ v \in\ \mathbf{int}\ \vee\ v \in RefVal$$

$$\|f(E)\|_{s_0,s} =$$
$$= \mathrm{H}(f)(\|E\|_{s_0,s})$$

$$\|f[\oplus E^1_{bml} \rightarrow E^2_{bml}](E^3_{bml})\|_{s_0,s} =$$
$$= \mathrm{H}[\oplus f \rightarrow f[\oplus \|E^1_{bml}\|_{s_0,s} \rightarrow \|E^2_{bml}\|_{s_0,s}]](f)(\|E^3_{bml}\|_{s_0,s})$$

$$\|\mathbf{arrayAccess}(E^1_{bml}, E^2_{bml})\|_{s_0,s} =$$
$$= \mathrm{H}(\|E^1_{bml}\|_{s_0,s}, \|E^2_{bml}\|_{s_0,s})$$

$$\|\mathrm{arrAccess}[\oplus(E^1_{bml}, E^2_{bml}) \rightarrow E^3_{bml}](E^4_{bml}, E^5_{bml})\|_{s_0,s} =$$
$$= \mathrm{H}[\oplus(\|E^1_{bml}\|_{s_0,s}, \|E^2_{bml}\|_{s_0,s}) \rightarrow \|E^3_{bml}\|_{s_0,s}]$$
$$(\|E^4_{bml}\|_{s_0,s}, \|E^5_{bml}\|_{s_0,s})$$

$$\|\mathbf{reg}(i)\|_{s_0,s} = \mathrm{Reg}(i)$$

$$\|\backslash\mathbf{old}(E)\|_{s_0,s} = \|E\|_{s_0,s_0}$$

$$\|E^1_{bml}\ op\ E^2_{bml}\|_{s_0,s} = \|E^1_{bml}\|_{s_0,s} op \|E^2_{bml}\|_{s_0,s}$$

$$\|\backslash\mathbf{typeof}(E)\|_{s_0,s} =$$
$$\begin{cases} \mathbf{int} & \|E\|_{s_0,s} \in \mathbf{int} \\ \mathrm{H.TypeOf}\ (\|E\|_{s_0,s}) & else \end{cases}$$

$$\|\backslash\mathbf{elemtype}(E)\|_{s_0,s} =$$
$$\begin{cases} \texttt{T} & if\ \mathrm{H.TypeOf}\ (\|E\|_{s_0,s}) = \texttt{T[ ]} \end{cases}$$

$$\|\backslash\mathbf{TYPE}\|_{s_0,s} = \texttt{java.lang.Class}$$

The evaluation of stack expressions can be done only in intermediate state configurations $s =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *:*

$$\|\mathbf{cntr}\|_{s_0,s} = \mathrm{Cntr}$$

$$\|\mathbf{st}(E)\|_{s_0,s} = \mathrm{St}(\|E\|_{s_0,s})$$

The evaluation of the following expressions can be done only in a final state $s =< \mathrm{H}, \mathrm{Reg} >^{final}$ *Final:*

$$\begin{array}{ll} \|\backslash\mathbf{result}\|_{s_0,s} = \mathrm{Res} & \textit{where } s =< \mathrm{H}, \mathrm{Reg} >^{norm} \mathrm{Res} \\ \|\backslash\mathbf{EXC}\|_{s_0,s} = \mathrm{Exc} & \textit{where } s =< \mathrm{H}, \mathrm{Reg} >^{exc} \mathrm{Exc} \end{array}$$

The relation $\vDash$ that we define next, gives a meaning to the formulas from our assertion language P.

Definition 4.3.0.2 (Interpretation of predicates) *The interpretation* $s \vDash P$ *of a predicate* P *in a state configuration* $s =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *w.r.t. an initial state* $s_0 =< \mathrm{H}_0, 0, [\,], \mathrm{Reg}, 0 >$ *is defined inductively as follows:*

$s, s_0 \vDash$ **true** *is true in any state* s

$s, s_0 \vDash$ **false** *is false in any state* s

$s, s_0 \vDash \neg\ P$ *if and only if not* $s, s_0 \vDash P$

$s, s_0 \vDash P_1 \wedge P_2$ *if and only if* $s, s_0 \vDash P_1$ *and* $s, s_0 \vDash P_2$

$s, s_0 \vDash P_1 \vee P_2$ *if and only if* $s, s_0 \vDash P_1$ *or* $s, s_0 \vDash P_2$

$s, s_0 \vDash P_1 \Rightarrow P_2$ *if and only if if* $s, s_0 \vDash P_1$ *then* $s, s_0 \vDash P_2$

$s, s_0 \vDash P_1$ *if and only if*P_2 *if and only if* $s, s_0 \vDash P_1$ *if and only if* $s, s_0 \vDash P_2$

$s, s_0 \vDash \forall x : T.P(x)$ *if and only if forall value* $\mathbf{v}$ *of type* T $s, s_0 \vDash P(\ \mathbf{v})$

$s, s_0 \vDash \exists x : T.P(x)$ *if and only if a value* $\mathbf{v}$ *of type* T *exists such that* $s, s_0 \vDash P(\ \mathbf{v})$

$$s, s_0 \vDash E^1_{bml}\ \mathcal{R}\ E^2_{bml} \textit{ if and only if } \begin{array}{l} \|E^1_{bml}\|_{s_0,s} \neq \perp \wedge \\ \|E^2_{bml}\|_{s_0,s} \neq \perp \wedge \\ \|E^1_{bml}\|_{s_0,s}\ \textit{rel}(\mathcal{R})\|E^2_{bml}\|_{s_0,s}\ \textit{is true} \end{array}$$

$s, s_0 \vDash$ **instances**(`ref`), *where* `ref` $\in$ *RefVal if and only if inList*(`ref`, getLoc(H_0))

4.4 Extending method declarations with specification

In the following, we propose an extension of the method formalization given in Section 2.4. The extension takes into account the method specification. The extended method structure is given below:

$$\textbf{Method} = \left\{ \begin{array}{ll} \mathsf{Name} & : \textbf{MethodName} \\ \mathsf{retType} & : \mathit{JType} \\ \mathsf{args} & : (\mathit{name} * \mathit{JType})[] \\ \mathsf{nArgs} & : \mathit{nat} \\ \mathsf{body} & : \ \mathrm{I}[] \\ \mathsf{excHndlS} & : \textbf{ExcHandler}[] \\ \mathsf{exceptions} & : \textbf{Class}_{exc}[] \\ \mathsf{pre} & : P \\ \mathsf{modif} & : \mathit{Expr}[\,] \\ \mathsf{excPostSpec} & : \mathit{ExcType} \rightharpoonup P \\ \mathsf{normalPost} & : P \\ \mathsf{loopSpecS} & : \textbf{LoopSpec}[\,] \end{array} \right\}$$

Let's see the meaning of the new elements in the method data structure.

- `m`.pre gives the precondition of the method, i.e. the predicate that must hold whenever `m` is called
- `m`.normalPost is the postcondition of the method in case `m`terminates normally
- `m`.modif is also called the method frame condition. It is a list of expressions that the method may modify during its execution
- `m`.excPostSpec is a total function from exception types to formulas which returns the predicate `m`.excPostSpec(`Exc`) that must hold in the method's poststate if the method `m` terminates on an exception of type `Exc`. Note that this function is constructed from the **exsures** clause of a method introduced in Chapter 3.1, section 3.4. For instance, if method `m` has an exsures clause:

  $$\textbf{exsures}\ (\ \texttt{Exc})\ \textbf{reg}(1) = \textbf{null}$$

  then for every exception type `SExc` such that subtype (`SExc` ,`Exc`) the function the result of the function `m`.excPostSpec for `SExc` is `m`.excPostSpec(`SExc`) = $\textbf{reg}(1) = \textbf{null}$. If for an exception `Exc` there is not specified exsures clause then the function excPostSpec returns the default exceptional postcondition predicate *false* , i.e. `m`.excPostSpec(`Exc`) = *false*
- `m`.loopSpecS is an array of **LoopSpec** data structures which give the specifcication information for a particular loop in the bytecode

The contents of a **LoopSpec** data structure is given hereafter:

$$\mathbf{LoopSpec} = \left\{ \begin{array}{ll} \mathsf{pos} & : nat \\ \mathsf{invariant} & : P \\ \mathsf{modif} & : Expr[\,] \end{array} \right\}$$

define modifies locations in the grammar

For any method `m` for any k such that $0 \leq k < \texttt{m.loopSpecS}.length$

- the field `m.loopSpecS`$[k]$.pos is a valid index in the body of `m`: $0 \leq \texttt{m.loopSpecS}[k].\mathsf{pos} < \texttt{m.body}.length$ and is a loop entry instruction in the sense of Def.2.9.2
- `m.loopSpecS`$[k]$.invariant is the predicate that must hold whenever the instruction `m.body`[`m.loopSpecS`$[k]$.pos] is reached in the execution of the method `m`
- `m.loopSpecS`$[k]$.modif are the locations such that for any two states $state_1$, $state_2$ in which the instruction `m.body`[`m.loopSpecS`$[k]$.pos] executes agree on local variables and the heap modulo the locations that are in the list modif. We denote the equality between $state_1$, $state_2$ modulo the modifies locations like this $state_1 =^{\mathsf{modif}} state_2$

Chapter 5

Verification condition generator for Java bytecode

This section describes a Hoare style verification condition generator for bytecode based on a weakest precondition predicate transformer function.

A natural question is to ask what are the motivations behind building a bytecode verification condition generator (vcGen for short) while a considerable list of tools for source code verification exists. We consider that today's software industry requires more and more guarantees about software security especially when mobile computing becomes a reality. Thus in mobile code scenarios, performing verification on source code of untrusted executable unit requires a trust in the compiler but which is not always reasonable. On the other hand, type based verification used for example, in the Java bytecode verifier could not deal with complex functional or security properties which is the case for a verification condition generator. The vcGen is tailored to the bytecode language introduced in Section 2.8 and thus, it deals with stack manipulation, object creation and manipulation, field access and update, as well as exception throwing and handling.

Different ways of generating verification conditions exist. The verification condition generator presented propagates the weakest precondition and exploits the information about the modified locations by methods and loops. In Section 5.1, we discuss the existing approaches and motivate the choice done here.

Bytecode verification has become lately quite fashionable, thus several works exist on bytecode verification. Section 5.2 is an overview of the existing work in the domain.

Performing Hoare style logic verification over an unstructured program like bytecode programs has few particularities which verification of structured programs lacks. For example, loops on source level correspond to a syntactic structure in the source language and thus, identifying a loop in a source program is not difficult. However, this is not the case for unstructured programs. As we saw in the previous section 3.1, our approach consists in compiling source

specification into bytecode specification. When compiling a loop invariant, we need to know where exactly in the bytecode the invariant must hold. Section 2.9 introduces the notion of a loop in an unstructured program.

As we stated earlier, our verification condition generator is based on a weakest precondition (wp) calculus. As we shall see in Section 5.3 a wp function for bytecode is similar to a wp function for source code. However, a logic tailored to stack based bytecode should take into account particular bytecode features as for example the operand stack.

5.1 Discussion

In this section, we make an overview of the different ways for generating verification conditions. Next, we shall see how we argument our design decisions of the verification condition generator presented here.

Our verification condition generator has the following features :

- it is based on a weakest precondition predicate transformer
  The weakest precondition generates a precondition predicate starting from the end of the program with a specified postcondition and "goes " in a backward direction to the entry point of the program. There is an alternative for generating verification condition which works in a forward direction called a strongest postcondition predicate transformer. However, strongest postcondition tends to generate large formulas which is less practical than the more concise formulae generated by the weakest precondition calculus. Next, it generates existential quantification for every assignment expression in a program which are not easily treated by automatic theorem provers. For more detailed information on strongest postcondition calculus the reader may refer to [14].

???

- it works directly on the bytecode
  Another possible approach is to generate verification conditions over a guarded command language program. This in particular would mean that the verification procedure would have one more stage where the bytecode programs is transformed in a program in a guarder command language. A guarded command language is useful for an interactive verification and is the case for the extended static checker ESC/java ([23]) and Spec# ([4]). The reason for this is that its representation is close to the semantics of the original program and thus is understandable by programmers.

  However, we consider that a guarded command language is impractical for our purposes for several reasons. First, the transformation is usually a complex procedure which needs computational resources. This could be a problem, if the verification procedure is done on a small device with limitted resources. Second, proving the transformation correct is not trivial. We consider that performing the verification procedure directly over the original bytecode program avoids the aformentioned problems.

- it propagates the verification conditions up to the program entry instruction
  For this feature we also have an alternative solution. An alternative is that verification conditions are discharged immediately when a loop entry is reached by the verifiction condition generator (see). These verification conditions (in the case of a weakest precondition predicate calculus) state that the loop invariant implies the postcondition of the loop if the loop condition is not true and that the invariant implies the weakest precondition of the loop body if the loop condition holds. Although, this verification condition generator is simpler than our approach it needs much stronger invariants than the verification condition generator proposed here. In particular, the specification required for this alternative approach may increase the size of the program considerably which will be not desirable if for instance the program and its specification must be sent via the network.

Benjamin, Tamara

5.2 Related work

In the following, we review briefly the existing work related to program verification and more particularly program verification tailored to Java and Java bytecode programs.

gilles: what do you mean by giving a title to every section

Floyd is among the first to work on program verification using logic methods for unstructured program languages (see [31]). Following the Floyd's approach, T.Hoare gives a formal logic for program verification in [18] known today under the name Hoare logic. Dijkstra [14] proposes then an efficient way for applying Hoare logic in program verification, i.e. he comes up with a weakest precondition (wp) and strongest postcondition (sp) calculi.

As Java has been gaining popularity in industry since the nineties of the twentieth century, it also attracted the research interest. Thus the nineties upto nowadays give rise to several verification tools tailored to Java based on Hoare logic. Among the ones that gained most popularity are esc/java developed at Compaq [23], the Loop tool [19], Krakatoa, Jack [11] etc.

Few works have been dedicated to the definition of a bytecode logic. Among the earliest work in the field of bytecode verification is the thesis of C.Quigley [29] in which Hoare logic rules are given for a bytecode like language. This work is limited to a subset of the Java virtual machine instructions and does not treat for example method calls, neither exceptional termination. The logic is defined by searching a structure in the bytecode control flow graph, which gives an issue to complex and weak rules.

The work by Nick Benton [7] gives a typed logic for a bytecode language with stacks and jumps. The technique that he proposes checks at the same time types and specifications. The language is simple and supports basically stack and arithmetic operations. Finally, a proof of correctness w.r.t. an operational semantics is given.

Following the work of Nick Benton, Bannwart and Muller [3] give a Hoare

logic rules for a bytecode language with objects and exceptions. A compiler from source proofs into bytecode proofs is also defined. As in our work, they assume that the bytecode has passed the bytecode verification certification. The bytecode logic aims to express functional properties. Invariants are inferred by fixpoint calculation. However, inferring invariants is not a decidable problem.

The Spec# ([4]) programming system developed at Microsoft proposes a static verification framework where the method and class contracts (pre, post conditions, exceptional postconditions, class invariants) are inserted in the intermediate code . Spec# is a superset of the C# programming language, with a built-in specification language, which proposes a verification framework (there is a choice to perform the checks either at runtime or statically). The static verification procedure involves translation of the contract specification into metadata which is attached to the intermediate code. The verification procedure [26] that is performed includes several stages of processing the bytecode program: elimination of irreducible loops, transformation into an acyclic control flow graph, translation of the bytecode into a guarded passive command language program. Despite that here in our implementation we also do a transformation in the graph into an acyclic program, we consider that in a mobile code scenario one should limit the number of program transformations for several reasons. First, we need a verification procedure as simple as possible, and second every transformation must be proven correct which is not always trivial.

5.3 Weakest precondition calculus

In what follows, we assume that the bytecode has passed the bytecode verifier, thus it is well typed and well structured. Actually, our calculus is concerned only with functional properties of programs leaving the problem of code well structuredness and welltypedness to the bytecode verification techniques

The weakest precondition predicate transformer function which for any instruction of the Java sequential fragment determines the predicate that must hold in the prestate of the instruction has the following signature:

$$wp : (nat,\ \mathrm{I}) \longrightarrow \mathbf{Method} \longrightarrow P$$

The function *wp* takes two arguments : the second argument is the method `m` to which the instruction belongs and the first argument is the instruction (for instance putfield) along with its position in `m`.

The function *wp* returns a predicate $wp(pos\ ins, \mathtt{m})$ such that if it holds in the prestate of the method `m` and if the `m` terminates normally then the normal postcondition `m.normalPost` holds when `m` terminates execution, otherwise if `m` terminates on an exception `Exc` the exceptional postcondition `m.excPost( Exc)` holds. Thus, the *wp* function takes into account both normal and exceptional program termination. Note however, that *wp* deals only with partial correctness, i.e. it does not guarantee program termination.

In order to define the *wp* function, we will need two other notions. The first one is a function which will determine the predicate between two instructions

that are in execution relation as defined in Def. 2.9.1. Note that this is not necessary for structured programs. However, for unstructured programs with loops annotated with invariants and frame conditions, this is a necessary step. The definition of the intermediate predicate is given in the next subsection 5.3.1. We will also see how the weakest precondition is defined in presence of exceptions. This is done in subsection **??**.

5.3.1 Intermediate predicates

In this subsection, we define a function *inter* which for two instructions that may execute one after another in a control graph of a method `m` determines the predicate $inter(j, k, \mathtt{m})$ which must hold in between them. The function has the signature:

$$inter : nat \longrightarrow nat \longrightarrow \mathbf{Method} \longrightarrow P$$

The predicate $inter(j, k, \mathtt{m})$ will be used for determining the weakest predicate that must hold in the prestate of the instruction j : `instr` if the execution path after passes through the instruction k : `instr`.

This predicate depends on the execution relation between the two instructions j : `instr` and k : `instr` as the next definition shows.

Definition 5.3.1 (Intermediate predicate between two instructions) *Assume that* j : `instr` $\rightarrow k$: `instr`. *The predicate* $inter(j, k, \mathtt{m})$ *must hold after the execution of* j : `instr` *and before the execution of* k : `instr` *and is defined as follows:*

- *if* k : `instr` *is a loop entry instruction,* j : `instr` $\rightarrow^l$ k : `instr` *and* $\mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{pos} = k$ *then the corresponding loop invariant must hold:*

$$inter(j, k, \mathtt{m}) \equiv \mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{invariant}$$

- *else if* k : `instr` *is a loop entry and* $\mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{pos} = k$ *then the corresponding loop invariant* $\mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{invariant}$ *must hold before* k : `instr` *is executed, i.e. after the execution of* j : `instr`. *We also require that* $\mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{invariant}$ *implies the weakest precondition of the loop entry instruction. The implication is quantified over the locations* $\mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{modif}$ *that may be modified in the loop body:*

$$\begin{array}{l} inter(j, k, \mathtt{m}) \equiv \\ \mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{invariant} \wedge \\ \forall i, i = 1..\mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{modif}.length, \\ \forall \mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{modif}[i], (\\ \qquad \mathtt{m}.\mathsf{loopSpecS}[s].\mathsf{invariant} \Rightarrow \\ \qquad\qquad wp(k\ , \mathtt{m})) \end{array}$$

- *else*

$$inter(j, k, \mathtt{m}) \equiv wp(k\ , \mathtt{m})$$

5.3.2 Weakest precondition in the presence of exceptions

Our weakest precondition calculus deals with exceptional termination and thus, we need some mechanism for providing the exceptional postcondition predicate of an instruction when it throws an exception. For this, we define the function getExcPostIns with signature :

$$\mathsf{getExcPostIns} : int \longrightarrow ExcType \longrightarrow P$$

The function m.getExcPostIns takes as arguments an index i in the array of instructions of method m and an exception type Exc and returns the predicate m.getExcPostIns(i, Exc) that must hold after the instruction at index i throws an exception. We give a formal definition hereafter.

Definition 5.3.2.1 (Postcondition in case of a thrown exception)

$$\mathtt{m}.\mathsf{getExcPostIns}(i,\ \mathtt{Exc}) = \begin{cases} inter(i, \mathsf{handlerPc}, \mathtt{m}) & if\ findExcHandler(\ \mathtt{Exc}, i, \mathtt{m}.\mathsf{excHndlS}) = \mathsf{handlerPc} \\ \mathtt{m}.\mathsf{excPostSpec}(\ \mathtt{Exc}) & findExcHandler(\ \mathtt{Exc}, i, \mathtt{m}.\mathsf{excHndlS}) = \bot \end{cases}$$

Next, we introduce an auxiliary function which will be used in the definition of the *wp* function for instructions that may throw runtime exceptions. Thus, for every method m we define the auxiliary function m.excPost with signature:

$$\mathtt{m}.\mathsf{excPost} : int \longrightarrow ExcType \longrightarrow P$$

m.excPost(i, Exc) returns the predicate that must hold in the preststate of the instruction at index i which may throw a runtime exception of type Exc. Note that the function m.excPost does not deal with programmatic exceptions thrown by the instruction athrow , neither exception caused by a method invokation (execution of instruction invoke) as the exceptions thrown by those instructions are handled in a different way as we shall see later in the definition of the *wp* function in Section 5.3.

The function application m.excPost(i, Exc) is defined as follows:

Definition 5.3.2.2 (Auxuliary function for instructions throwing runtime exceptions)

$$\begin{array}{l} i : \mathtt{instr} \neq \text{ athrow} \wedge i : \mathtt{instr} \neq \text{ invoke} \Rightarrow \\ \mathtt{m}.\mathsf{excPost}(\ i,\ \mathtt{Exc}) = \\ \forall \mathtt{ref}, \\ \quad \neg\ \mathbf{instances}(\mathtt{ref}) \wedge \\ \quad \mathtt{ref} \neq \mathbf{null} \Rightarrow \\ \qquad \mathtt{m}.\mathsf{getExcPostIns}(\ i,\ \mathtt{Exc}) \\ \qquad\ [\mathbf{cntr} \leftarrow 0] \\ \qquad\ [\mathbf{st}(0) \leftarrow \mathtt{ref}] \\ \qquad\ [f \leftarrow f[\oplus \mathtt{ref} \rightarrow defVal(f.\mathsf{Type})]]_{\forall f:\mathbf{Field},\ \mathsf{subtype}\ (f.\mathsf{declaredIn},\ \mathtt{Exc})} \\ \qquad\ [\backslash \mathbf{typeof}(\mathtt{ref}) \leftarrow\ \mathtt{Exc}] \end{array}$$

The function m.excPost will return a predicate which states that for every newly created exception reference the predicate returned by the function getExcPostIns must hold.

5.3.3 Rules for single instruction

In the following, we give the definition of the weakest precondition function for every instruction.

- Control transfer instructions
  1. unconditional jumps

$$wp(i \;\; \text{goto} \;\; n, \mathtt{m}) = \;\; inter(i, n, \mathtt{m})$$

     The rule says that an unconditional jump does not modify the program state and thus, the postcondition and the precondition of this instruction are the same

  2. conditional jumps

$$\begin{array}{l} wp(i \;\; \text{if\_cond} \;\; n, \mathtt{m}) = \\ \quad \mathtt{cond}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr} - 1)) \Rightarrow \\ \qquad inter(i, n, \mathtt{m})[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2] \\ \wedge \\ not(\;\; \mathtt{cond})(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr} - 1))) \Rightarrow \\ \qquad inter(i, i+1, \mathtt{m})[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2] \end{array}$$

     In case of a conditional jump, the weakest precondition depends on if the condition of the jump is satisfied by the two stack top elements. If the condition of the instruction evaluates to true then the predicate between the current instruction and the instruction at index n must hold where the stack counter is decremented with 2 $inter(i, n, \mathtt{m})[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2]$ If the condition evaluates to false then the predicate between the current instruction and its next instruction holds where once again the stack counter is decremented with two $inter(i, i+1, \mathtt{m})[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2]$.

  3. return

$$wp(\mathtt{m} \;\; \text{return} \;, i) = \mathtt{m}.\mathsf{normalPost}[\backslash\mathbf{result} \leftarrow \mathbf{st}(\mathbf{cntr})]$$

     As the instruction return marks the end of the execution path, we require that its postcondition is the normal method postcondition normalPost. Thus, the weakest precondition of the instruction is normalPost where the specification variable $\backslash\mathbf{result}$ is substituted with the stack top element.

- load and store instructions
  1. load a local variable on the operand stack

$$\begin{array}{l} wp(i \;\; \text{load} \;\; \mathtt{j}, \mathtt{m}) = \\ inter(i, i+1, \mathtt{m}) \;\; \begin{array}{l} [\mathbf{cntr} \leftarrow \mathbf{cntr} + 1] \\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathbf{reg}(j)] \end{array} \end{array}$$

The weakest precondition of the instruction then is the predicate that must hold between the current instruction and its successor, but where the stack counter is incremented and the stack top is substituted with $\mathbf{reg}(j)$. For instance, if we have that the predicate $inter(i, i+1, \mathtt{m})$ is equal to $\mathbf{st}(counter) == 3$ then we get that the precondition of instruction is $\mathbf{reg}(j) == 3$:

$$\begin{array}{l}\{\mathbf{reg}(j) == 3\}\\ i: \text{ load } \mathtt{j}\\ \{\mathbf{st}(\mathbf{cntr}) == 3\}\\ i+1: \ldots\end{array}$$

2. store the stack top element in a local variable

$$\begin{array}{l} wp(i \text{ store } \mathtt{j}, \mathtt{m}) = \\ inter(i, i+1, \mathtt{m}) \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} - 1]\\ [\mathbf{reg}(j) \leftarrow \mathbf{st}(\mathbf{cntr})]\end{array}\end{array}$$

Contrary to the previous instruction, the instruction store j will take the stack top element and will store its contents in the local variable $\mathbf{reg}(j)$.

3. push an integer constant on the operand stack

$$\begin{array}{l} wp(i \text{ push } \mathtt{j}, \mathtt{m}) = \\ inter(i, i+1, \mathtt{m}) \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1]\\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \text{ j }]\end{array}\end{array}$$

The predicate that holds after the instruction holds in the prestate of the instruction but where the stack counter **cntr** is incremented and the constant j is stored in the stack top element

4. incrementing a local variable

$$\begin{array}{l} wp(\mathtt{m} \text{ iinc } \mathtt{j}, i) = \\ inter(i, i+1, \mathtt{m})[\mathbf{reg}(j) \leftarrow \mathbf{reg}(j) + 1]\end{array}$$

- arithmetic instructions

1. instructions that cannot cause exception throwing (`arithOp` = add , sub , mult , and , or , xor , ishr , ishl ,)

$$\begin{array}{l} wp(i \text{ arith\_op}, \mathtt{m}) = \\ inter(i, i+1, \mathtt{m}) \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} - 1]\\ [\mathbf{st}(\mathbf{cntr} - 1) \leftarrow \mathbf{st}(\mathbf{cntr}) \mathtt{op}\ \mathbf{st}(\mathbf{cntr} - 1)]\end{array}\end{array}$$

We illustrate this rule with an example. Let us have the arithmetic instruction add at index i such that the predicate $inter(i, i+1, \mathtt{m}) \equiv$

$\mathbf{st}(\mathbf{cntr}) \geq 0$. In this case, applying the rule we get that the weakest precondition is $\mathbf{st}(\mathbf{cntr}-1)+\mathbf{st}(\mathbf{cntr}) \geq 0$:

$$\{\mathbf{st}(\mathbf{cntr}-1)+\mathbf{st}(\mathbf{cntr}) \geq 0\}$$
$$i: \text{ add}$$
$$\{\mathbf{st}(\mathbf{cntr}) \geq 0\}$$

2. instructions that may throw exceptions (`arithOp` = rem , div)

$$wp(i \text{ arithOp }, \mathtt{m}) =$$
$$\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow$$
$$inter(i, i+1, \mathtt{m}) \; [\mathbf{cntr} \leftarrow \mathbf{cntr}-1] \; [\mathbf{st}(\mathbf{cntr}-1) \leftarrow \mathbf{st}(\mathbf{cntr}) \text{ op } \mathbf{st}(\mathbf{cntr}-1)]$$
$$\wedge$$
$$\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathtt{m}.\mathsf{excPost}(i, \texttt{NullPntrExc})$$

- object creation and manipulation

1. create a new object

$$wp(i \text{ new } C, \mathtt{m}) =$$
$$\forall \mathtt{ref},$$
$$not \; \mathbf{instances}(\mathtt{ref}) \wedge$$
$$\mathtt{ref} \neq \mathbf{null} \Rightarrow$$
$$inter(i, i+1, \mathtt{m})$$
$$[\mathbf{cntr} \leftarrow \mathbf{cntr}+1]$$
$$[\mathbf{st}(\mathbf{cntr}+1) \leftarrow \mathtt{ref}]$$
$$[f \leftarrow f[\oplus \mathtt{ref} \rightarrow \mathsf{defVal}(f.\mathsf{Type})]]_{\forall f:\mathbf{Field}.\mathsf{subtype}\ (f.\mathsf{declaredIn}, C)}$$
$$[\backslash \mathbf{typeof}(\mathtt{ref}) \leftarrow C]$$

The postcondition of the instruction new is the intermediate predicate $inter(i, i+1, \mathtt{m})$. The weakest precondition of the instruction says that for any reference `ref` if `ref` was not instantiated in the initial state of the execution of `m` then the precondition is the same predicate but in which the stack counter is incremented and `ref` is pushed on the stack top where the fields for the `ref` are initialized with their default values

2. array creation

$$
\begin{array}{l}
wp(i \ \ \text{newarray } \mathtt{T}, \mathtt{m}) = \\
\forall \mathtt{ref}, \\
\quad \mathit{not}\ \mathbf{instances}(\mathtt{ref}) \wedge \\
\quad \mathtt{ref} \neq \mathbf{null} \wedge \\
\quad \mathbf{st}(\mathbf{cntr}) \geq 0 \Rightarrow \\
\qquad \mathit{inter}(i, i+1, \mathtt{m}) \\
\qquad [\mathbf{st}(\mathbf{cntr}) \leftarrow \mathtt{ref}] \\
\qquad [\text{arrAccess} \leftarrow \text{arrAccess}[\oplus(\mathtt{ref}, j) \rightarrow \mathsf{defVal}(\mathtt{T})]]_{\forall j, 0 \leq j < \mathbf{st}(\mathbf{cntr})} \\
\qquad [\text{arrLength} \leftarrow \text{arrLength}[\oplus \mathtt{ref} \rightarrow \mathbf{st}(\mathbf{cntr})]] \\
\wedge \\
\mathbf{st}(\mathbf{cntr}) < 0 \Rightarrow \mathtt{m}.\mathsf{excPost}(i, \ \mathtt{NegArrSizeExc})
\end{array}
$$

Here, the rule for array creation is similar to the rule for object creation. However, creation of an array might terminate exceptionally in case the length of the array stored in the stack top element **st**(**cntr**) is smaller than 0. In this case, function m.excPost will search for the corresponding postcondition of the instruction at position i and the exception NegArrSizeExc

3. field access

$$
\begin{array}{l}
wp(i \ \ \text{getfield } f, \mathtt{m}) = \\
\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\
\qquad \mathit{inter}(i, i+1, \mathtt{m})[\mathbf{st}(\mathbf{cntr}) \leftarrow f(\mathbf{st}(\mathbf{cntr}))] \\
\wedge \\
\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathtt{m}.\mathsf{excPost}(i, \ \mathtt{NullPntrExc})
\end{array}
$$

The instruction for accessing a field value takes as postcondition the predicate that must hold between it and its next instruction $\mathit{inter}(i, i+1, \mathtt{m})$. This instruction may terminate normally or on an exception. In case the stack top element is not **null**, the precondition of getfield is its postcondition where the stack top element is substituted by the field access expression $f(\mathbf{st}(\mathbf{cntr}))$. If the stack top element is **null**, then the instruction will terminate on a NullPntrExc exception. In this case the precondition of the instruction is the predicate returned by the function m.excPost for position i in the bytecode and exception NullPntrExc

4. field update

$$
\begin{array}{l}
wp(i \ \ \text{putfield } f, \mathtt{m}) = \\
\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\
\qquad \mathit{inter}(i, i+1, \mathtt{m}) \ \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2] \\ [f \leftarrow f[\oplus \mathbf{st}(\mathbf{cntr} - 1) \rightarrow \mathbf{st}(\mathbf{cntr})]]\end{array} \\
\wedge \\
\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathtt{m}.\mathsf{excPost}(i, \ \mathtt{NullPntrExc})
\end{array}
$$

This instruction also may terminate normally or exceptionally. The termination depends on the value of the stack top element in the prestate of the instruction. If the top stack element is not **null** then in the precondition of the instruction $inter(i, i+1, \mathtt{m})$ must hold where the stack counter is decremented with two elements and the f object is substituted with an updated version $f[\oplus \mathbf{st}(\mathbf{cntr}-2) \rightarrow \mathbf{st}(\mathbf{cntr}-1)]$
For example, let us have the instruction putfield f in method `m`. Its normal postcondition is $inter(i, i+1, \mathtt{m}) \equiv f(\mathbf{reg}(1)) \neq \mathbf{null}$. Assume that `m` does not have exception handler for `NullPntrExc` exception for the region in which the putfield instruction. Let the exceptional postcondition of `m` for `NullPntrExc` be *false* , i.e. `m.excPostSpec( NullPntrExc)` = *false* If all these conditions hold, the function *wp* will return for the putfield instruction the following formula :

$$\begin{array}{l}\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\ \quad (f(\mathbf{reg}(1)) \neq \mathbf{null})\ \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr}-2] \\ [f \leftarrow f[\oplus \mathbf{st}(\mathbf{cntr}-1) \rightarrow \mathbf{st}(\mathbf{cntr})]]\end{array} \\ \wedge \\ \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathit{false}\end{array}$$

After applying the substitution following the rules described in Section 4.2, we obtain that the precondition is

$$\begin{array}{l}\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\ \quad f[\oplus \mathbf{st}(\mathbf{cntr}-1) \rightarrow \mathbf{st}(\mathbf{cntr})](\mathbf{reg}(1)) \neq \mathbf{null} \\ \wedge \\ \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathit{false}\end{array}$$

Finally, we give the instruction putfield its postcondition and the respective weakest precondition:

$$\begin{array}{l}\left\{\begin{array}{l}\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\ f[\oplus \mathbf{st}(\mathbf{cntr}-1) \rightarrow \mathbf{st}(\mathbf{cntr})](\mathbf{reg}(1)) \neq \mathbf{null}\} \\ \wedge \\ \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathit{false}\end{array}\right\} \\ i:\ \text{putfield } f \\ \{f(\mathbf{reg}(1)) \neq \mathbf{null}\} \\ i+1: \ldots\end{array}$$

5. access the length of an array

$$\begin{array}{l}wp(i\ \ \text{arraylength}, \mathtt{m}) = \\ \mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\ \quad inter(i, i+1, \mathtt{m})[\mathbf{st}(\mathbf{cntr}) \leftarrow \text{arrLength}(\mathbf{st}(\mathbf{cntr}))] \\ \wedge \\ \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathtt{m.excPost}(i,\ \mathtt{NullPntrExc})\end{array}$$

The semantics of arraylength is that it takes the stack top element which must be an array reference and puts on the operand stack the length of the array referenced by this reference. This instruction may terminate either normally or exceptionally. The termination depends on if the stack top element is **null** or not. In case $\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null}$ the predicate $inter(i, i+1, \mathtt{m})$ must hold where the stack top element is substituted with its length. The case when a `NullPntrExc`is thrown is similar to the previous cases with exceptional termination

6. checkcast

$$
\begin{array}{l}
wp(i \ \text{ checkcast } C, \mathtt{m}) = \\
\backslash\mathbf{typeof(st(cntr))} <: C \vee \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \\
\quad inter(i, i+1, \mathtt{m}) \\
\wedge \\
not(\backslash\mathbf{typeof(st(cntr))} <: C) \Rightarrow \mathtt{m.excPost}(i, \mathtt{CastExc})
\end{array}
$$

The instruction checks if the stack top element can be cast to the class C. Two termination of the instruction are possible. If the stack top element $\mathbf{st}(\mathbf{cntr}\ )$ is of type which is a subtype of class C or is **null** then the predicate $inter(i, i+1, \mathtt{m})$ holds in the prestate. Otherwise, if $\mathbf{st}(\mathbf{cntr}\ )$ is not of type which is a subtype of class C, the instruction terminates on `CastExc` and the predicate returned by `m.excPost` for the position i and exception `CastExc` must hold

7. instanceof

$$
\begin{array}{l}
wp(i \ \text{ instanceof } C, \mathtt{m}) = \\
\backslash\mathbf{typeof(st(cntr))} <: C \Rightarrow \\
\quad inter(i, i+1, \mathtt{m})[\mathbf{st}(\mathbf{cntr}) \leftarrow 1] \\
\wedge \\
not(\backslash\mathbf{typeof(st(cntr))} <: C) \vee \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \\
\quad inter(i, i+1, \mathtt{m})[\mathbf{st}(\mathbf{cntr}) \leftarrow 0]
\end{array}
$$

This instruction, depending on if the stack top element can be cast to the class type C pushes on the stack top either 0 or 1. Thus, the rule is almost the same as the previous instruction checkcast .

- method invocation (only the case for non void instance method is given).

$$
\begin{array}{l}
wp(i \;\; \text{invoke } \mathtt{n}\ , \mathtt{m}) = \\
\mathtt{n}\ .\mathsf{pre}[\mathbf{reg}(s) \leftarrow \mathbf{st}(\mathbf{cntr} + s - \mathtt{m}.\mathsf{nArgs})]_{s=0}^{\mathtt{n}\ .\mathsf{nArgs}} \\
\\
\wedge \\
\\
\forall mod, (mod \in \mathtt{n}\ .\mathsf{modif}), \forall freshVar(\\
\quad \mathtt{n}\ .\mathsf{normalPost} \begin{array}{l}[\backslash\mathbf{result} \leftarrow freshVar] \\ [\mathbf{reg}(s) \leftarrow \mathbf{st}(\mathbf{cntr} + s - \mathtt{n}\ ).\mathsf{nArgs}]_{s=0}^{\mathtt{n}\ .\mathsf{nArgs}}\end{array} \Rightarrow \\
\\
\qquad inter(i, i+1, \mathtt{m}) \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} - \mathtt{n}\ .\mathsf{nArgs}] \\ [\mathbf{st}(\mathbf{cntr} - \mathtt{n}\ .\mathsf{nArgs}) \leftarrow freshVar]\end{array}) \\
\\
\wedge_{j=0}^{\mathtt{n}\ .\mathsf{exceptions}.length-1} \\
\\
\forall mod, (mod \in \mathtt{n}\ .\mathsf{modif}), \\
\quad (findExcHandler(\mathtt{n}\ .\mathsf{exceptions}[j], i, \mathtt{m}.\mathsf{excHndlS}) = \bot \Rightarrow \\
\quad \forall \mathbf{bv}_i(\\
\quad\quad \mathtt{n}\ .\mathsf{excPostSpec}(\mathtt{n}\ .\mathsf{exceptions}[j])[\backslash\mathbf{EXC} \leftarrow \mathbf{bv}_i] \Rightarrow \\
\quad\quad\quad \mathtt{m}.\mathsf{getExcPostIns}(i, \mathtt{m}.\mathsf{exceptions}[j])[\backslash\mathbf{EXC} \leftarrow \mathbf{bv}_i])) \\
\quad \wedge \\
\quad (findExcHandler(\mathtt{m}\ .\mathsf{excPostSpec}(\mathtt{n}\ .\mathsf{exceptions}[j]), i, \mathtt{m}.\mathsf{excHndlS}) = k \Rightarrow \\
\quad \forall \mathbf{bv}_i(\\
\quad\quad \mathtt{n}\ .\mathsf{excPostSpec}(\mathtt{n}\ .\mathsf{exceptions}[j])[\backslash\mathbf{EXC} \leftarrow \mathbf{bv}_i] \Rightarrow \\
\quad\quad\quad \mathtt{m}.\mathsf{getExcPostIns} \begin{array}{l}[\mathbf{cntr} \leftarrow 0] \\ [\mathbf{st}(0) \leftarrow \mathbf{bv}_i]\end{array}))
\end{array}
$$

Let us look in detail what is the meaning of the weakest precondition for method invokation. Because we are following a contract based approach the caller, i.e. the current method `m` must establish several facts. First, we require that the precondition `n`.pre of the invoked method `n` holds where the formal parameters are correctly initialized with the first `n`.nArgs elements from the operand stack.

Second, we get a logical statement which guarantees the correctness of the method invokation in case of normal termination. On the other hand, its postcondition `n`.normalPost is assumed to hold and thus, we want to establish that under the assumption that `m`.normalPost holds with $\backslash\mathbf{result}$ substituted with a fresh bound variable $\mathbf{bv}_i$ and correctly initialized formal parameters is true we want to establish that the predicate *inter*(i, i+1 , `m`) holds . This implication is quantified over the locations `n`.modif that a method may modify and the variable $\mathbf{bv}_i$ which stands for the result that the invoked method `n` returns.

The third part of the rule deals with the exceptional termination of the method invokation. In this case, if the invoked method `n` terminates on

any exception which belongs to the array of exceptions n.exceptions that n may throw. Two cases are considered - either the thrown exception can be handled by m or not. If the thrown exception Exc can not be handled by the method m (i.e. $\mathit{findExcHandler}(\mathtt{n}.\mathsf{excPostSpec}(\mathtt{n}.\mathsf{exceptions}[j]), i, \mathtt{m}.\mathsf{excHndlS}) = \bot$) then if the exceptional postcondition predicate n .excPostSpec(Exc) of n holds then m.excPostSpec(Exc) for any value of the thrown exception object. In case the thrown exceptionExc is handled by m, i.e. $\mathit{findExcHandler}(\mathtt{n}.\mathsf{excPostSpec}(\mathtt{n}.\mathsf{exceptions}[j]), i, \mathtt{m}.\mathsf{excHndlS}) = k$ then if the exceptional postcondition n .excPostSpec(Exc) of n holds then the intermediate predicate $\mathit{inter}(i, k, \mathtt{m})$ that must hold after i : instr and before k : instr must hold once again for any value of thrown exception.

- throw exception instruction

$$
\begin{array}{l}
\mathit{wp}(i \ \ \mathrm{athrow}, \mathtt{m}) = \\
\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathtt{m}.\mathsf{getExcPostIns}(i, \ \mathtt{NullPntrExc}) \\
\wedge \\
\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\
\ \forall \mathtt{Exc}, \\
\ \backslash \mathbf{typeof(st(cntr))} <: \mathtt{Exc} \Rightarrow \\
\quad \mathtt{m}.\mathsf{getExcPostIns}(i, \mathtt{Exc})[\backslash \mathbf{EXC} \leftarrow \mathbf{st}(\mathbf{cntr})]
\end{array}
$$

The thrown object is on the top of the stack **st**(**cntr**). If the stack top object **st**(**cntr**) is **null**, then the instruction athrow will terminate on an exception NullPntrExc where the predicate returned by the function m.excPost must hold. The case when the thrown object is not **null** should consider all the possible exceptions that might be thrown by the current instruction. This is because we do not know the type of the thrown object which is on the stack top. The part of the *wp* when the thrown object on the stack top **st**(**cntr**) is not **null** considers all the possible types of the exception thrown. In any of

Supposing the execution of a method always terminates, the verification condition for a method m with a precondition m.pre is defined in the following way:

$$\mathtt{m}.\mathsf{pre} \Rightarrow \mathit{wp}(0 \ \ \mathrm{m}.\mathsf{body}[0], \mathtt{m})$$

5.4 Example

In the following, we will consider an example of the application of the verification procedure with *wp*. Consider Fig. 5.1, which gives an example of a Java method which calculates the square of its input which is stated in its postcondition. The calculation of the square of the parameter i is done with an iteration which sums all the impair numbers 2∗s + 1, 0<=s <=i in the local variable sqr. The invariant states that whenever the loop entry is reached the variable sqr will

```
1  //@ ensures \result == i*i;
2  public int square( int i ) {
3    int sqr  = 0;
4    if ( i < 0) {
5      i = -i;
6    }
7    //@ loop_modifies s, sqr;
8    //@ loop_invariant (0 <= s) && (s <= i) && sqr == s*s ;
9    for (int s = 0 ; s < i; s++ ) {
10     sqr = sqr + 2*s + 1;
11   }
12   return sqr;
13 }
```

Figure 5.1: JAVA METHOD WHICH CALCULATES THE SQUARE OF ITS INPUT

contain the square of the local variable s and that 0 <=s <=i. In Fig.5.2, we show the bytecode of method square. The weakest precondition for a fragment of the instructions are shown in Fig. 5.3.

Fig.5.3 shows the resulting preconditions for some of the instructions in the bytecode of the method square. In the figure, the line before every instruction gives the calculated weakest precondition of the instruction in the execution path which reaches the end of the method. Thus, the weakest precondition of the instruction return at line 28 states that before the instruction is executed the stack top element **st**(**cntr**) must contain the square of the local variable **reg**(1) . Note that this precondition is calculated from the method postcondition which is given in curly brackets at line 38. The instruction before the return instruction has as precondition that the local variable **reg**(2) must be equal to the square of **reg**(1) . The instruction if_cond at line 24 has as weakest precondition that if the stack element below the stack top element **st**(**cntr** - 1) is not smaller than **st**(**cntr**) then **reg**(2) == **reg**(1) ***reg**(1) . Note that we give only a part of the precondition of this instruction for the sake of clarity. In particular, we give the precondition which must hold if the condition is not true, or in other words the precondition of the if_cond instruction for the execution path which goes to the end of the method. The case which deserves more attention is the instruction goto at line 14 which jumps to the loop entry instruction at line 21. As discussed in Section 5.3.1, the weakest precondition of this goto consists in the specified loop invariant and the a formula which states that the invariant implies the precondition of the loop entry.

Another point to notice is that the instruction at line 19 which is a loop end instruction w.r.t. Def 2.9.2 has as precondition the loop invariant where the **reg**(3) is incremented.

```
1  0  const 0
2  1  store 2
3  2  load 1
4  3  if\_ge 7
5  4  load 1
6  5  neg
7  6  store 1
8  7  const 0
9  8  store 3
10 9  goto 19
11 10 load 2
12 11 const 2
13 12 load 3
14 13 mul
15 14 add
16 15 const 1
17 16 add
18 17 store 2
19 18 iinc 3
20 //loop start
21 19 load 3
22 20 load 1
23 21 if\_icmplt 10
24 22 load 2
25 23 return
```

$$\text{square.normalPost} = \backslash\mathbf{result} == \mathbf{reg}(1) * \mathbf{reg}(1)$$

$$\text{square.loopSpecS} = \begin{cases} \mathsf{pos} = 19 \\ \\ \mathsf{invariant} = \begin{array}{l} 0 <= \mathbf{reg}(3) \wedge \\ \mathbf{reg}(3) <= \mathbf{reg}(1) \wedge \\ \mathbf{reg}(2) = \mathbf{reg}(3) * \mathbf{reg}(3) \end{array} \\ \\ \mathsf{modif} = \mathbf{reg}(3), \mathbf{reg}(2) \end{cases}$$

Figure 5.2: BYTECODE OF METHOD SQUARE AND ITS SPECIFICATION

```
1  ...
2  // invariant initialization
3  {   0 <= lv(3) &&
4      lv(3) <= lv(1) &&
5      lv(2) = lv(3) * lv(3) }
6  // invariant implies the loop postcondition
7  { forall lv(3), forall lv(2),
8      0 <= lv(3) &&
9      lv(3) <= lv(1) &&
10     lv(2) = lv(3) * lv(3) &&
11     not(lv(3) < lv(1))==>
12        lv(2) = old(lv(1)) * old(lv(1)) }
13 9  goto 19
14
15 ...
16
17 {  0 <= lv(3) + 1 &&
18     lv(3) + 1 <= lv(1) &&
19     lv(2) = (lv(3) + 1) * ( lv(3) + 1) }
20 18 iinc 3
21
22 { not (lv(3) < lv(1)) ==>lv(2) == lv(1)*lv(1) }
23 19 load 3 //loop start
24
25 { not (st(cntr) < lv(1))==>lv(2)==lv(1)*lv(1) }
26 20 load 1
27
28 {not ( st(cntr - 1)<st(cntr))==>lv(2) == lv(1)*lv(1)}
29 21 if icmplt 10
30
31 {lv(2) == lv(1)*lv(1)    }
32 22 load 2
33
34 {st(cntr) == lv(1)*lv(1) }
35 23 return
36
37 { \result == lv(1)*lv(1) }
```

Figure 5.3: BYTECODE OF METHOD SQUARE AND WEAKEST PRECONDITIONS FOR A FRAGMENT OF THE EXECUTION PATH WHICH REACHES THE METHOD END

Chapter 6

Correctness of the verification condition generator

In the previous chapter 5, we defined a verification condition generator for a Java bytecode like language. We used a weakest precondition to build the verification conditions. In this section, we will argue formally that the proposed verification condition generator is correct, or in other words that it is sufficient to prove the verification conditions generated over a bytecode program and its specification for establishing that the program respects the specification.

In particular, we will prove the correctness of our methodology w.r.t. the operational semantics of our bytecode language given in chapter 2.8. The way in which the proof is done is standard. Note that the formalization of the operational semantics in terms of relation on states serves us to give a model for our assertion language.

We now proceed with the proof of the partial correctness of the weakest precondition calculus, i.e. we assume that programs always terminate. Note also that in the following we do not consider recursive methods. The first section 6.1 introduces several properties concerning expression evaluation and interpretation of predicates in a particular state. Those properties will play role in the correctness proof of the verification condition generator in section 6.2. Section 6.2 starts with a formal definition for method correctness. Then, we establish the correctness of a single instruction (lemma 6.2.1). The next step of the proof is to establish that if all the steps in an execution path establish the intermediate predicates then the execution can either proceed by establishing the next weakest precondition predicate or will terminate in a state which respects the adequate postcondition.

6.1 Substitution properties

The following lemmas estasblish that substitution over state configurations or expressions / formulas result in the same evaluation

Lemma 6.1.1 (Update a local variable) *For any expressions* $Expr_1, Expr_2$ *if we have that the states* s_1 *and* s_2 *are such that* $s_1 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and* $s_2 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}[\oplus i \rightarrow \|Expr_2\|_{s_0,s_1}], \mathrm{Pc} >$ *then the following holds:*

1. $\|Expr_1[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr_1\|_{s_0,s_2}$
2. $s_1, s_0 \vDash \psi[\mathbf{reg}(i) \leftarrow Expr_2] \iff s_2, s_0 \vDash \psi$

Proof : by structural induction on the structure of $Expr_1$

1. we look at the first part of the lemma concerning expression evaluation

   - $Expr_1 = \mathbf{reg}(i)$

     $(left)$ $\mathbf{reg}(i)[\mathbf{reg}(i) \leftarrow Expr_2] = Expr_2$
     $\Rightarrow$
     (1) $\|\mathbf{reg}(i)[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr_2\|_{s_0,s_1}$

     $(right)$ $\|\mathbf{reg}(i)\|_{s_0,s_2} =$
     { *by Def.4.3.0.1 of the evaluation for local variables* }
     (2) $= \|Expr_2\|_{s_0,s_1}$
     { *from (1) and (2) we get that the lemma holds in this case* }

   - $Expr_1 = Expr_3.f$

     $Expr_3.f[\mathbf{reg}(i) \leftarrow Expr_2] =$
     { *by definition of the substitution* }
     $= Expr_3[\mathbf{reg}(i) \leftarrow Expr_2].f$
     { *by induction hypothesis* }
     (1)$\|Expr_3[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr_3\|_{s_0,s_2}$

     { *by Def.4.3.0.1 of the evaluation for field access expressions* }
     $(left)$ $\|Expr_3.f[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} =$
     $= \mathrm{H}(f)(\|Expr_3[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1})$

     $(right)$ $\|Expr_3.f\|_{s_0,s_2} =$
     $= \mathrm{H}(f)(\|Expr_3\|_{s_0,s_2})$

     { *from (1),(left) and (right)*
     we get that the lemma holds in this case }

   - the rest of the cases proceed in a similar way by appluing the induction hypothesis

2. second case of the lemma

   - $\psi = E' \ \mathcal{R} \ E'$

     $\{$ *from the first part of the lemma we get* $\}$
     (1) $\|Expr'[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr'\|_{s_0,s_2}$
     (2) $\|Expr''[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr''\|_{s_0,s_2}$

     $s_1, s_0 \vDash \psi[\mathbf{reg}(i) \leftarrow Expr_2]$
     $\{$ *definition of substitution* $\}$
     (3) $\equiv$
     $s_1, s_0 \vDash Expr'[\mathbf{reg}(i) \leftarrow Expr_2] \ \mathcal{R} \ Expr''[\mathbf{reg}(i) \leftarrow Expr_2]$
     $\{$ *by Def.4.3.0.2 we get* $\}$
     $\Longleftrightarrow$
     $\|Expr'[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1} \ rel(\mathcal{R}) \|Expr''[\mathbf{reg}(i) \leftarrow Expr_2]\|_{s_0,s_1}$ *is true*
     $\{$ *from (1) , (2) and (3)* $\}$
     $\Longleftrightarrow$
     $\|Expr'\|_{s_0,s_2} \ rel(\mathcal{R}) \|Expr''\|_{s_0,s_2}$
     $\equiv$
     $s_2, s_0 \vDash \psi$

   - the rest of the cases are by structural induction

Lemma 6.1.2 (Update of the heap) *For any expressions* $Expr_1, Expr_2, Expr_3$ *and any field* f *if we have that the states* s_1 *and* s_2 *are such that* $s_1 =<$ $\mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and* $s_2 =< \mathrm{H}[\oplus f \rightarrow f[\oplus \|Expr_2\|_{s_0,s_1} \rightarrow \|Expr_3\|_{s_0,s_1}]], \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *the following holds*

1. $\|Expr_1[f \leftarrow f[\oplus Expr_2 \rightarrow Expr_3]]\|_{s_0,s_1} = \|Expr_1\|_{s_0,s_2}$
2. $s_1, s_0 \vDash \psi[f \leftarrow f[\oplus Expr_2 \rightarrow Expr_3]] \iff s_2, s_0 \vDash \psi$

Lemma 6.1.3 (Update of the heap with a newly allocated object) *For any expressions* $Expr_1$ *if we have that the states* s_1 *and* s_2 *are such that* $s_1 =<$ $\mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and* $s_2 =< \mathrm{H}', \mathrm{Cntr}, \mathrm{St}[\oplus \mathrm{Cntr} \rightarrow \|\mathtt{ref}\|_{s_0,s_1}], \mathrm{Reg}, \mathrm{Pc} >$ *where* $\mathrm{newRef}(\mathrm{H}, C) = (\mathrm{H}', \mathtt{ref})$ *the following holds*

1. $$\|Expr_1 \begin{array}{l}[\mathbf{st}(\mathbf{cntr}) \leftarrow \mathtt{ref}] \\ [f \leftarrow f[\oplus \mathtt{ref} \rightarrow defVal(f.\mathsf{Type})]]_{\forall f:\mathbf{Field},\mathsf{subtype}\ (f.\mathsf{declaredIn}, C)}\end{array} \|_{s_0,s_1} = \|Expr_1\|_{s_0,s_2}$$
2. $$s_1, s_0 \vDash \psi \begin{array}{l}[\mathbf{st}(\mathbf{cntr}) \leftarrow \mathtt{ref}] \\ [f \leftarrow f[\oplus \mathtt{ref} \rightarrow defVal(f.\mathsf{Type})]]_{\forall f:\mathbf{Field},\mathsf{subtype}\ (f.\mathsf{declaredIn}, C)}\end{array} \Longleftrightarrow s_2, s_0 \vDash \psi$$

Lemma 6.1.4 (Update the stack) *For any expressions* $Expr_1, Expr_2, Expr_3$ *if we have that the states* s_1 *and* s_2 *are such that* $s_1 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and* $s_2 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}[\oplus \|Expr_2\|_{s_0,s_1} \rightarrow \|Expr_3\|_{s_0,s_1}], \mathrm{Reg}, \mathrm{Pc} >$ *then the following holds:*

1. $\|Expr_1[\mathbf{st}(Expr_2) \leftarrow Expr_3]\|_{s_0,s_1} = \|Expr_1\|_{s_0,s_2}$
2. $s_1, s_0 \vDash \psi[\mathbf{st}(Expr_2) \leftarrow Expr_3] \iff s_2, s_0 \vDash \psi$

Lemma 6.1.5 (Update the stack counter) *For any expressions* $Expr_1, Expr_2$ *if we have that the states* s_1 *and* s_2 *are such that* $s_1 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and* $s_2 =< \mathrm{H}, \|Expr_2\|_{s_0,s_1}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *then the following holds:*

1. $\|Expr_1[\mathbf{cntr} \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr_1\|_{s_0,s_2}$
2. $s_1, s_0 \vDash \psi[\mathbf{cntr} \leftarrow Expr_2] \iff s_2, s_0 \vDash \psi$

Lemma 6.1.6 (Return value property) *For any expression* $Expr_1$ *and* $Expr_2$*, for any two states* s_1 *and* s_2 *such that* $s_1 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >$ *and* $s_2 =< \mathrm{H}, \|Expr_2\|_{s_0,s_1} >^{norm}$ *then the following holds:*

1. $\|Expr_1[\backslash\mathbf{result} \leftarrow Expr_2]\|_{s_0,s_1} = \|Expr_1\|_{s_0,s_2}$
2. $s_1, s_0 \vDash \psi[\backslash\mathbf{result} \leftarrow Expr_2] \iff s_2, s_0 \vDash \psi$

The next definition defines a particular set of assertion formulas which we call valid formulas.

Definition 6.1.1 (Valid formulas) *If an assertion formula* $f \in P$ *holds in any current state and any initial state, i.e.* $\forall state, state_{init}, state, s_0 \vDash f$ *we say that this is a valid formula and we note it with :* $\vDash f$

6.2 Proof of Correctness

The correctness of our verification condition generator is established w.r.t. to the operational semantics described in Section 2.8. We look only at partial correctness, i.e. we assume that programs always terminate and we assume that there are no recursive methods.

We first give a definition that a "method is correct w.r.t its specification"

Definition 6.2.1 (A method is correct w.r.t. its specification) *For every method* `m` *with precondition* `m.pre`*, normal postcondition* `m.normalPost`*and exceptional postcondition function* `m.excPostSpec`*, we say that* `m` *respects its specification if for every two states* s_0 *and* s_1 *such that :*

- $\mathtt{m} : s_0 \Rightarrow s_1$
- $s_0, s_0 \vDash \mathtt{m.pre}$

Then if `m` *terminates normally then the normal postcondition holds in the final state* s_1*:* $s_1, s_0 \vDash$ `m.normalPost`*. Otherwise, if* `m` *terminates on an exception* `Exc` *the exceptional postcondition holds in the poststate* s_1 $s_1, s_0 \vDash$ `m.excPostSpec( Exc)`

The next issue that is important for understanding our approach is that we follow the design by contract paradigm [8]. This means that when verifying a method body, we assume that the rest of the methods respect their specification in the sense of the previuos definition 6.2.1.

First, we establish the correctness of the weakest precondition function for a single instruction: if the *wp* (short for weakest precondition) of an instruction holds in the prestate then in the poststate of the instruction the postcondition upon which the wp is caclulated holds.

Lemma 6.2.1 (Single execution step correctness) *For every instruction* s : `instr`*, for every state* $s_0 =< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, s >$ *and initial state* $s_0 =< \mathrm{H}_0, 0, [\,], \mathrm{Reg}, 0 >$ *of the execution of method* `m` *if the following conditions hold:*

- $\mathtt{m.body}[0] : s_0 \hookrightarrow^* s_n$
- $\mathtt{m.body}[s] : s_n \hookrightarrow s_{n+1}$
- $s_n, s_0 \vDash wp(\ \mathrm{Pc}_n : \mathtt{instr}, \mathtt{m})$
- $\forall\ \mathtt{n} : \mathbf{Method}.\ \mathtt{n} \neq \mathtt{m}$ *n is correct w.r.t. its specification*

then :

- *if* Pc_n : `instr` $\neq$ return *and the instruction does not terminate on exception,* $s_{n+1} =< \mathrm{H}_{n+1}, \mathrm{Cntr}_{n+1}, \mathrm{St}_{n+1}, \mathrm{Reg}_{n+1}, \mathrm{Pc}_{n+1} >$ *then* $s_{n+1}, s_0 \vDash$ *inter*$(\mathrm{Pc}_n, \mathrm{Pc}_{n+1}, \mathtt{m})$ *holds*
- *if* Pc_n : `instr` $=$ return *then* $s_{n+1}, s_0 \vDash$ `m.normalPost` *holds*
- *else if* Pc_n : `instr` $\neq$ return *and the instruction terminates on a not handled exception* `Exc` *, then* $s_{n+1}, s_0 \vDash$ `m.excPostSpec( Exc )`

Proof : The proof is by case analysis on the type of instruction that will be next executed. We are going to see only the proofs for the instructions return , load and invoke , the other cases being the same

1. Pc_n : `instr` $=$ return

   { *by initial hypothesis* }
   $< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash wp(\mathtt{m}$ return $, \mathrm{Pc}_n)$
   { *by definition the weakest precondition for* return }
   $< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash \mathtt{m.normalPost}[\backslash\mathbf{result} \leftarrow \mathbf{st}(\mathrm{cntr})]$
   { *by the substitution property 6.1.6* }
   $\Longleftrightarrow$
   $< \mathrm{H}_n, \|\mathbf{st}(\mathrm{cntr})\|_{s_0, <\mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n>} >^{norm}, s_0 \vDash \mathsf{normalPost}$
   { *by definition of the evaluation function eval* }
   $\Longleftrightarrow$
   $< \mathrm{H}_n, \mathrm{St}_n(\mathrm{Cntr}_n) >^{norm}, s_0 \vDash \mathsf{normalPost}$

2. Pc_n : **instr** = load i

$\{$ *by initial hypothesis* $\}$
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash wp(\mathrm{Pc}_n \ \text{load}\ i, \mathtt{m})$
$\{$ *definition of the wp function* $\}$
$\equiv$
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash \mathit{inter}(\mathrm{Pc}_n, \mathrm{Pc}_n + 1, \mathtt{m})\ [\mathrm{cntr} \leftarrow \mathrm{cntr} + 1]\ [\mathbf{st}(\mathrm{cntr} + 1) \leftarrow \mathbf{reg}(i)]$
$\{$ *applying the substitution properties 6.1.5 and 6.1.4* $\}$
$\Longleftrightarrow$
$< \mathrm{H}_n, \mathrm{Cntr}_n + 1, \mathrm{St}_n[\oplus \mathrm{Cntr}_n + 1 \rightarrow \mathrm{Reg}_n(i)], \mathrm{Reg}_n, \mathrm{Pc}_{n+1} >, s_0 \vDash$
$\mathit{inter}(\mathrm{Pc}_n, \mathrm{Pc}_n + 1, \mathtt{m})$
$\{$ *from the operational semantics of the* load *instruction in section 2.8*$\}$
$s_{n+1}, s_0 \vDash \mathit{inter}(\mathrm{Pc}_n, \mathrm{Pc}_n + 1, \mathtt{m})$
$\{$ *and the lemma holds in this case* $\}$

3. new C

$\{$ *by initial hypothesis* $\}$
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash wp(\mathrm{Pc}\ \text{new}\ C, \mathtt{m})$
$\{$ *definition of the wp function* $\}$
$\equiv$
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash$
$\forall \mathtt{ref}, \mathit{not}\ \mathbf{instances}(\mathtt{ref}) \wedge$
$\mathtt{ref} \neq \mathbf{null} \Rightarrow$
(1) $\mathit{inter}(i, i+1, \mathtt{m})\ [\mathbf{cntr} \leftarrow \mathbf{cntr} + 1]\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathtt{ref}]\ [f \leftarrow f[\oplus \mathtt{ref} \rightarrow \mathsf{defVal}(f.\mathsf{Type})]]_{\forall f : \mathbf{Field}.\mathsf{subtype}\ (f.\mathsf{declaredIn}, C)}\ [\backslash \mathbf{typeof}(\mathtt{ref}) \leftarrow C]$

$\{$ *from the operational semantics of* new *in section 2.8* $\}$

(2) $s_{n+1} =< \mathrm{H}_{n+1}, \mathrm{Cntr}_n + 1, \mathrm{St}_n[\oplus \mathrm{Cntr}_n + 1 \rightarrow \mathtt{ref}], \mathrm{Reg}_n, \mathrm{Pc}_n + 1 >$

(3) $\mathrm{newRef}(\mathrm{H}, C) = (\mathrm{H}_{n+1}, \mathtt{ref}')$

{ *following Def. 4.3.0.2 instantiate (1) with* $\mathtt{ref}'$ }
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash$
not **instances**$(\mathtt{ref}') \wedge$
$\mathtt{ref}' \neq \mathbf{null} \Rightarrow$

(4) $inter(i, i+1, \mathtt{m})$ $[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1]$ $[\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathtt{ref}']$ $[f \leftarrow f[\oplus \mathtt{ref}' \rightarrow \mathsf{defVal}(f.\mathsf{Type})]]_{\forall f:\mathbf{Field}.\mathsf{subtype}\ (f.\mathsf{declaredIn}, C)}$ $[\backslash \mathbf{typeof}(\mathtt{ref}) \leftarrow C]$

{ *from (3)* }

(5) $< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash$ *not* **instances**$(\mathtt{ref}') \wedge$ $\mathtt{ref}' \neq \mathbf{null}$

{ *from (4) and (5) and Def. 4.3.0.2* }
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash$

$inter(i, i+1, \mathtt{m})$ $[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1]$ $[\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathtt{ref}']$ $[f \leftarrow f[\oplus \mathtt{ref}' \rightarrow \mathsf{defVal}(f.\mathsf{Type})]]_{\forall f:\mathbf{Field}.\mathsf{subtype}\ (f.\mathsf{declaredIn}, C)}$ $[\backslash \mathbf{typeof}(\mathtt{ref}) \leftarrow C]$

{*from lemmas 6.1.5, 6.1.4 and 6.1.2, 6.1.3*
and the operational semantics of the instruction new }
$s_{n+1}, s_0 \vDash inter(i, i+1, \mathtt{m})$

4. $\mathrm{Pc} : \mathtt{instr} =$ putfield f

{ *by initial hypothesis* }
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash wp(\ \mathrm{Pc}_n\ \ \text{putfield}\ f, \mathtt{m})$
{ *definition of the wp function* }
$\equiv$
$< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash$
$\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow$

(1) $inter(i, i+1, \mathtt{m})$ $[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2]$ $[f \leftarrow f[\oplus \mathbf{st}(\mathbf{cntr} - 1) \rightarrow \mathbf{st}(\mathbf{cntr})]]$

$\wedge$
$\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathtt{m}.\mathsf{excPost}(i,\ \mathtt{NullPntrExc})$
{ *we get three cases* }

(a) the dereferenced reference on the stack top is **null** and an exception handler starting at instruction k exists for `NullPntrExc` and Pc_n :

`instr` is in its scope

$$
\begin{array}{l}
\{\ \textit{thus, we get the hypothesis}\ \} \\
< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \\
\{\ \textit{from the above conclusion and (1) we get}\ \} \\
< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash \mathtt{m.excPost}(\mathrm{Pc}_n,\ \mathtt{NullPntrExc}) \\
\{\ \textit{from Def. 5.3.2.2 of the function}\ \mathtt{m.excPost} \\
???\ \textit{and the assumption that the exception is handled we get}\ \} \\
\quad < \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash \\
\quad \forall \mathtt{ref}, \\
\qquad \neg\ \mathbf{instances}(\mathtt{ref}) \wedge \\
\qquad \mathtt{ref} \neq \mathbf{null} \Rightarrow \\
\qquad\quad \mathit{inter}(\mathrm{Pc}_n, \mathrm{Pc}_{n+1}, \mathtt{m}) \\
\qquad\quad [\mathbf{cntr} \leftarrow 0] \\
\qquad\quad [\mathbf{st}(0) \leftarrow \mathtt{ref}] \\
\qquad\quad [f \leftarrow f[\oplus \mathtt{ref} \rightarrow \mathit{defVal}(f.\mathsf{Type})]]_{\forall f:\mathbf{Field},\ \mathsf{subtype}\ (f.\mathsf{declaredIn},\ \mathtt{Exc})} \\
\{\ \textit{from lemmas 6.1.5, 6.1.2, 6.1.4 and 6.1.3} \\
\quad \textit{and the operational semantics of}\ \ \mathrm{putfield}\ \} \\
s_{n+1}, s_0 \vDash\ \ \mathit{inter}(\mathrm{Pc}_n, \mathrm{Pc}_{n+1}, \mathtt{m})
\end{array}
$$

(b) the reference on the stack top is **null** and and the exception thrown is not handled. In this case, we obtain following the same way of reasoning as the previous case :

$$
\begin{array}{l}
< \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >, s_0 \vDash \\
\quad \forall \mathtt{ref}, \\
\qquad \neg\ \mathbf{instances}(\mathtt{ref}) \wedge \\
\qquad \mathtt{ref} \neq \mathbf{null} \Rightarrow \\
\quad \mathtt{m.excPostSpec(\ NullPntrExc)} \\
\qquad [\backslash \mathbf{EXC} \leftarrow \mathtt{ref}] \\
\qquad [f \leftarrow f[\oplus \mathtt{ref} \rightarrow \mathit{defVal}(f.\mathsf{Type})]]_{\forall f:\mathbf{Field},\mathsf{subtype}\ (f.\mathsf{declaredIn},\ \mathtt{Exc})} \\
\{\ \textit{from lemmas 6.1.4, 6.1.2, 6.1.3 and} \\
\quad \textit{the operational semantics of}\ \ \mathrm{putfield}\ \} \\
s_{n+1}, s_0 \vDash \mathtt{m.excPostSpec(\ NullPntrExc)}
\end{array}
$$

(c) the reference on the stack top is not **null**

$$
\begin{array}{l}
\{\ \textit{thus, we get the hypothesis}\ \} \\
< \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, s_0 \vDash \mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \\
\{\ \textit{from the above conclusion and (1) we get}\ \} \\
\quad < \mathrm{H}, \mathrm{Cntr}, \mathrm{St}, \mathrm{Reg}, \mathrm{Pc} >, s_0 \vDash \\
\quad \mathit{inter}(i, i+1, \mathtt{m})\ \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} - 2] \\ [f \leftarrow f[\oplus \mathbf{st}(\mathbf{cntr} - 1) \rightarrow \mathbf{st}(\mathbf{cntr})]]\end{array} \\
\{\ \textit{applying lemmas 6.1.5 and 6.1.2 and} \\
\quad \textit{of the operational semantics of}\ \ \mathrm{putfield}\ \} \\
s_{n+1}, s_0 \vDash\ \ \mathit{inter}(i, i+1, \mathtt{m})
\end{array}
$$

We now establish a property of the correctness of the wp function for an execution path. The following lemma states that if the calculated preconditions of all the instructions in an execution path holds then either the execution terminates normally (executing a return) or exceptionally, or another step can be made and the *wp* of the next instruction holds.

Lemma 6.2.2 (Progress) *Assume we have a method* `m` *with normal postcondition* `m.normalPost` *and exception function* `m.excPostSpec`. *Assume that the execution starts in state*
$< \mathrm{H}_0, \mathrm{Cntr}_0, \mathrm{St}_0, \mathrm{Reg}_0, \mathrm{Pc}_0 >$ *and the there are made n execution steps causing the transitive state transition*
$< \mathrm{H}_0, \mathrm{Cntr}_0, \mathrm{St}_0, \mathrm{Reg}_0, \mathrm{Pc}_0 > \hookrightarrow^n < \mathrm{H}_n, \mathrm{Cntr}_n, \mathrm{St}_n, \mathrm{Reg}_n, \mathrm{Pc}_n >$. *Assume that* $\forall i, (\ 0 \leq i \leq n),\ s_i, s_0 \vDash wp(\ \mathrm{Pc}_i : \mathtt{instr}, \mathtt{m})$ *holds then*

1. *if* $\mathrm{Pc}_n : \mathtt{instr} =$ return *then* $< \mathrm{H}_n, \mathrm{St}_n(\mathrm{Cntr}_n) >^{norm}, s_0 \vDash \mathtt{m.normalPost}$ *holds.*

2. *if* $\mathrm{Pc}_n : \mathtt{instr} \neq$ athrow *throws a not handled exception of type* Exc $< \mathrm{H}_{n+1}, \mathtt{ref} >^{exc}, s_0 \vDash \mathtt{m.excPostSpec}(\mathrm{Exc})$ *holds where* $\mathrm{newRef}(\mathrm{H}_n, \mathrm{Exc}) = (\mathrm{H}_{n+1}, \mathtt{ref})$.

3. *if* $\mathrm{Pc}_n : \mathtt{instr} =$ athrow *throws a not handled exception of type* Exc $< \mathrm{H}_n, \mathrm{St}(\mathrm{Cntr}) >^{exc}, s_0 \vDash \mathtt{m.excPostSpec}(\mathrm{Exc})$ *holds*

4. *else exists a state* s_{n+1} *such that another execution step can be done* $s_n \hookrightarrow s_{n+1}$ *and* $s_{n+1}, s_0 \vDash wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m})$ *holds*

Proof : The proof is by case analysis on the type of instruction that will be next executed.

We consider three cases: the case when the next execution step doesnot enter a cycle (the next instruction is not a loop entry in the sense of Def.2.9.2) the case when the current instruction is a loop end and the next instruction to be executed is a loop entry instruction (the execution step is $\rightarrow_l$) and the case when the current instruction is not a loop end and the next instruction is a loop entry instruction (corresponds to the first iteration of a loop)

1. the next instruction to be executed is not a loop entry instruction.

{ *following Def. 5.3.1 of the function inter in this case* }
(1) $inter(\mathrm{Pc}_n, \mathrm{Pc}_{n+1}, \mathtt{m}) = wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m})$
{ *by initial hypothesis* }
(2) $s_n, s_0 \vDash wp(\ \mathrm{Pc}_n : \mathtt{instr}, \mathtt{m})$
{ *from the previous lemma 6.2.1 and (2) , we know that* }
(3) $s_{n+1}, s_0 \vDash inter(\mathrm{Pc}_n, \mathrm{Pc}_{n+1}, \mathtt{m})$
{ *from (1) and (3)* }
$s_{n+1}, s_0 \vDash wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m})$

2. Pc_n : `instr` is not a loop end and the next instruction to be executed is a loop entry instruction at index *loopEntry* in the array of bytecode instructions of the method `m`(i.e. the execution step is of kind $\rightarrow^l$, see Def.2.9.2). Thus, there exists a natural number $i, 0 \leq i < \mathtt{m.loopSpecS}.length$ such that $\mathtt{m.loopSpecS}[i].\mathsf{pos} = loopEntry$, $\mathtt{m.loopSpecS}[i].\mathsf{invariant} = I$ and $\mathtt{m.loopSpecS}[i].\mathsf{modif} = \{mod_i, i = 1..s\}$. We look only at the case when the current instruction is a load instruction

$\{$ *by initial hypothesis* $\}$
$s_n, s_0 \vDash wp(\ \mathrm{Pc}_n\ \ \mathrm{load}\ i, \mathtt{m})$
$\{$ *by defintion of the wp function in section 5.3 of the previous chapter* $\}$
$s_n, s_0 \vDash \ inter(\mathrm{Pc}_n, \mathrm{Pc}_n + 1, \mathtt{m})\ \begin{matrix}[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1] \\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathbf{reg}(j)]\end{matrix}$
$\{$*by the definition 5.3.1 for the case when*
the execution step is not a backedge but the target instruction is a loop entry $\}$
$s_n, s_0 \vDash$
$I\ \begin{matrix}[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1] \\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathbf{reg}(i)]\end{matrix}$
$\wedge$
$\forall mod_i, i = 1..s(I \Rightarrow wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m}))\ \begin{matrix}[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1] \\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow \mathbf{reg}(i)]\end{matrix}$
$\{$ *from lemmas 6.1.5 and 6.1.4* $\}$
$\Longleftrightarrow$
$s_n\ \begin{matrix}[\mathrm{Cntr} \leftarrow \|\mathbf{cntr} + 1\|_{s_0,s_n}] \\ [\mathrm{St} \leftarrow \mathrm{St}[\oplus(\|\mathbf{cntr} + 1\|_{s_0,s_n}) \rightarrow \|\mathbf{reg}(i)\|_{s_0,s_n}]]\end{matrix}\ , s_0 \vDash$
$I \wedge$
$\forall mod_i, i = 1..s(I \Rightarrow wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m}))$
$\{$ *from the Def. 4.3 of the evaluation function* $\}$
$\equiv$
$s_n\ \begin{matrix}[\mathrm{Cntr} \leftarrow \mathrm{Cntr} + 1] \\ [\mathrm{St} \leftarrow \mathrm{St}[\oplus \mathrm{Cntr} + 1 \rightarrow \mathrm{Reg}(i)]]\end{matrix}\ , s_0 \vDash$
$I \wedge$
$\forall mod_i, i = 1..s(I \Rightarrow wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m}))$
$\{$ *from the operational semantics of* load $\}$
$s_{n+1}, s_0 \vDash \begin{matrix}I \wedge \\ \forall mod_i, i = 1..s(I \Rightarrow wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m}))\end{matrix}$
$\{$ *we can get from the last formulation* $\}$
(1) $s_{n+1}, s_0 \vDash I$

(2)$s_{n+1}, s_0 \vDash I \Rightarrow wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m})$
$\{$ *from (1) and (2)* $\}$
$s_{n+1}, s_0 \vDash wp(\ \mathrm{Pc}_{n+1} : \mathtt{instr}, \mathtt{m})$

3. Pc_n : `instr` is an end of a cycle and the next instruction to be executed is a loop entry instruction at index *loopEntry* in the array of bytecode instructions of the method `m`(i.e. the execution step is of kind $\rightarrow^l$

). Thus, there exists a natural number $i, 0 \leq i < \texttt{m.loopSpecS}.length$ such that $\texttt{m.loopSpecS}[i].\mathsf{pos} = loopEntry$, $\texttt{m.loopSpecS}[i].\mathsf{invariant} = I$ and $\texttt{m.loopSpecS}[i].\mathsf{modif} = \{mod_i, i = 1..s\}$. We consider the case when the current instruction is a sequential instruction. The cases when the current instruction is a jump instruction are similar.

{ *by hypothesis we get* }

$$s_n, s_0 \vDash wp(\ \mathrm{Pc}_n : \texttt{instr}, \texttt{m})$$

{ *from Def. 5.3.1 and transformation over the above statement* }

$$(1) \quad s_{n+1}, s_0 \vDash I$$

{ *by hypothesis, loopEntry* $= \mathrm{Pc}_{n+1}$. *From def. 2.9.2, we conclude that there is a prefix subP* $= \texttt{m.body}[0] \rightarrow^* loopEntry : \texttt{instr}$ *of the current execution path which does not pass through* $\mathrm{Pc}_n : \texttt{instr}$. *We can conclude that the transition between loopEntry* : `instr` *and its predecessor* k : `instr` *(which is at index* k *in* `m.body`*) in the path subP is not a backedge. By hypothesis we know that* $\forall i, 0 \leq i \leq n, s_i, s_0 \vDash wp(\ \mathrm{Pc}_i : \texttt{instr}, \texttt{m})$. *From def.5.3.1 and lemma 6.2.1 we conclude* }

$$\exists k, 0 \leq k \leq n \Rightarrow$$

$$(2) \quad \begin{array}{l} s_k, s_0 \vDash \\ I \\ \wedge \forall mod_i, i = 1..s(\ \begin{array}{l} I \Rightarrow \\ wp(\ loopEntry : \texttt{instr}, \texttt{m}) \end{array}\ ) \end{array}$$

$$(3) \quad s_k =_{\mathsf{modif}} s_{n+1}$$

{ *because* $\texttt{m.loopSpecS}[i].\mathsf{modif} = \{mod_i, i = 1..s\}$ *and from (2) and (3)* }

$$(4)\ s_{n+1}, s_0 \vDash I \Rightarrow wp(\ loopEntry : \texttt{instr}, \texttt{m})$$

{ *from (1) and (4)* }

$$\begin{array}{l} s_{n+1}, s_0 \vDash wp(\ loopEntry : \texttt{instr}, \texttt{m}) \\ \Longleftrightarrow \\ s_{n+1}, s_0 \vDash wp(\ \mathrm{Pc}_{n+1} : \texttt{instr}, \texttt{m}) \end{array}$$

Qed.

Lemma 6.2.3 (*wp* of method entry point instruction) *Assume we have a method* `m`. *Assume that execution of method* `m` *starts execution in state* s_0 *and* $s_0, s_0 \vDash wp(\ \texttt{m.body}[0], \texttt{m})$ *where and makes* n *steps to reach state* s_n*:* $s_0 \hookrightarrow^n s_n$, *then*

$$\forall i, 0 < i \leq n,\ s_i, s_0 \vDash wp(\ \texttt{m.body}[\mathrm{Pc}_i], \texttt{m})$$

Proof : Induction over the number of execution steps n

1. $s_0 \hookrightarrow s_1$. From the initial hypothesis we can apply lemma 6.2.2, we get that $s_1, s_0 \vDash wp(\ \mathrm{Pc}_1 : \texttt{instr}, \texttt{m})$ and thus, the case when one step is made from the initial state s_0 holds

2. Induction hypothesis: $s_0 \hookrightarrow^{n-1} s_{n-1}$ and
   $\forall i, 0 < i \leq n-1,\ s_i, s_0 \vDash wp(\ \texttt{m.body}[\mathrm{Pc}_i], \texttt{m})$ and there can be made one step $s_{n-1} \hookrightarrow s_n$. Lemma 6.2.2 can be applied and we get that

   (1) $s_n, s_0 \vDash wp(\ \texttt{m.body}[\mathrm{Pc}_n], \texttt{m})$. From the induction hypothesis and *(1)* follows that

   $$\forall i, 0 < i \leq n,\ s_i, s_0 \vDash wp(\ \texttt{m.body}[\mathrm{Pc}_i], \texttt{m})$$

Lemma 6.2.4 (Validity of *wp* for a method implies that postcondition holds) *Assume we have a method* m *with normal postcondition* m.normalPost *and exception function* m.excPostSpec.

Assume that execution of methodd m *starts in state* $_0$ *and* $s_0, s_0 \vDash wp(0\ \texttt{m.body}[0], \texttt{m})$ *Then if the method* m *terminates, i.e. there exists a state* s_n, $s_0 \hookrightarrow^* s_n$ *such that* Pc_n : `instr` = return *or* Pc_n : `instr` *throws an unhandled exception of type* Exc *the following holds:*

- *if* Pc_n : `instr` = return *then* $s_{n+1}, s_0 \vDash$ m.normalPost
- *if* Pc_n : `instr` *throws a not handled exception of type* `Exc` *then* $s_{n+1}, s_0 \vDash$ m.excPostSpec(Exc)

Proof: Let $s_0 \hookrightarrow^* s_n$ and $\texttt{m.body}[\mathrm{Pc}_n]$ is a return or an instruction that throws a not handled exception. Applying lemma 6.2.3, we can get that $s_n, s_0 \vDash wp(\ \texttt{m.body}[\mathrm{Pc}_n], \texttt{m})$. We apply lemma 6.2.1 for the case for a return or instruction that throws an unhandled exception which allows to conclude that the current statement holds.

Now, we are ready to state the theorem which expresses the correctness of our verification condition generator w.r.t. the operational semantics of our language

Theorem 6.2.5 *For any method* m *if the verification condition is valid:*

$$\vDash \texttt{m.pre} \Rightarrow wp(\ \ \texttt{m}\ .\texttt{body}[0], \texttt{m})$$

then m *is correct in the sense of the definition 6.2.1.*

Proof: From lemma 6.2.4 and the initial hypothesis that the weakest precondition of the entry point holds we conclude that the method m is correct

Chapter 7

Equivalence between Java source and bytecode proof Obligations

In this chapter, we will look at the relationship between the verification conditions generated for a Java like source programming language and the verification conditions generated for the bytecode language as defined in Chapter 5. More particularly, we argue that they are syntactically equivalent if the compiler is nonoptmizing and satisfies certain conditions.

First, we would like to give the context and motivations for studying the relationship between source and bytecode verification.

Security becomes an important issue for the overall software quality. This is especially the case for mobile code or what so ever untrusted code. A solution proposed by G.Necula (see his thesis **??**) is the PCC framework which brings the possibility to a code receiver to verify if an unknown code or untrusted code respects certain safety conditions before being executed by the code receiver. In this framework the code client annotates the code automatically, generates verification conditons automatically and proves them automatically. The program accompanied by the proof is sent to the code receiver who will typecheck the proof against the verification conditions that he will generate. Because of its full automation this architecture fails to deal with complex functional or security properties.

The relation of the verification conditions over bytecode and source code can be used for building an alternative PCC architecture which can deal with complex security policy. More particularly, such an equivalence can be exploited by the code producer to generate the certificate interactively over the source code. Because of the equivalence between the proof obligations over source and bytecode programs (modulo names and types), their proof certificates are also the same and thus the certificate generated interactively over the source code can be sent along with the code.

In the following, Section 7.1 presents an overview of existing work on this subject. In Section 7.2, we introduce the source programming language. As we shall see, this programming language has the basic features of Java as it supports object creation and manipulation, like instance field access and update, exception throwing and handling, method calls as well as subroutines.

Section 7.3 presents a simple non optimizing compiler from the source language to the bytecode language presented already in Chapter 2.9. In this section, we will discuss certain properties of the compiler which are necessary conditions for establishing this equivalence.

Next, Section 7.4 presents the weakest precondition predicate transformer which we define over the source language.

Section 7.5 introduces a new formulation of the weakest precondition for bytecode, which is defined over the compilation of source expressions and statements. This formulation of the weakest precondition is helpful for establishing the desired relation between bytecode and source proof obligations. In this section, we also discuss upon what conditions the weakest precondition given before in Chapter 5 and this new version are equivalent.

In Section 7.6, we proceed with the proof of equivalence between the proof obligations generated by the weakest precondition defined in Chapter 5. To do this, we first establish the equivalence between the source weakest precondition and the bytecode weakest precondition defined over the compilation of statements and expressions. We exploit also the equivalence between the two bytecode weakest preconditions to conclude that the source verification condition generator and the bytecode verification condition generator presented in Chapter 5

7.1 Related Work

Several works dealing with the relation between source and its compilation verification condition generated.

Barthe, Rezk and Saabas in **??** also argue that proof obligations produced over source code and bytecode produced by a nonoptimizing compiler are equivalent. The source language supports method invokation, exception throwing and handling.They do not consider instructions that may throw runtime exceptions. Note that because of this However, in their work they do not discuss what are the compiler assumptions and properties which will guarantee this equivalence. We claim that their proof for the verification condition preserving compilation holds only if their non optimizing compiler has the properties discussed here in Section 7.3.

In [2], F.Bannwart and P.Muller show how to transform a Hoare style logic derivation on source Java like program into a Hoare style logic derivation of a Java bytecode like program. This solution however has the shortcoming that the certificate (in this case it is the Hoare style logic derivation) can be potentially large. In particular, this means that applying this technique in scenarios like PCC could be hard because of the large size of the certificate.

7.2 Source language

We present a source Java-like programming language which supports the following features: object manipulation and creation, method invokation, throwing and handling exceptions, subroutines etc. The next definition presents the expressions of the source language, i.e. the language constructs that evaluate.

Definition 7.2.1 (Expression) *The grammar for source expressions is defined as follows*

$$
\begin{aligned}
\mathcal{E}^{src} ::= \quad & \textbf{constInt} \\
& \mid \mathit{true} \\
& \mid \mathit{false} \\
& \mid \mathcal{E}^{src}\ \mathit{op}\ \mathcal{E}^{src} \\
& \mid \mathcal{E}^{src}.f \\
& \mid \textbf{var} \\
& \mid (\mathit{Class})\ \mathcal{E}^{src} \\
& \mid \textbf{null} \\
& \mid \textbf{this} \\
& \mid \mathcal{E}^{\mathcal{R}} \\
& \mid \mathcal{E}^{src}.m() \\
& \mid \textbf{new}\ \mathit{Class}(\mathcal{E}^{src})
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{E}^{\mathcal{R}} ::= \quad & \mathcal{E}^{src}\ \mathcal{R}\ \mathcal{E}^{src} \\
& \mid \mathcal{E}^{src}\ \textbf{instanceof}\ \mathit{Class} \\
& \\
& \mathcal{R} \in \{\leq, <, \geq, >, =, \neq\}
\end{aligned}
$$

We now a give an informal description of the meaning of the expressions of the above grammar:

- **constInt** is any integer literal
- *true* and *false* are the unique boolean constants
- **constRef** is a reference to an object in the memory heap
- $\mathcal{E}^{src}$ *op* $\mathcal{E}^{src}$ which stands for an arithmetic expression with any of the arithmetic operators $+, -, div, rem, *$
- $\mathcal{E}^{src}.f$ is a field access expression where the field with name f is accessed
- the cast expression $(Class)\mathcal{E}^{src}$ which is applied only to expressions from a reference type
- the expression **null** stands for the null reference which does not point to any location in the heap
- **this** refers to the current object

- $\mathcal{E}^{src}.m()$ stands for a method invokation expression. Note that here we consider only methods without arguments which return a value
- **new** $Class(\mathcal{E}^{src})$ stands for an object creation expression of class $Class$. We consider only constructors which take only one argument for the sake of readability

The language is also provided with relational expressions, which evaluate to the boolean values:

- $\mathcal{E}^{src}\ \mathcal{R}\ \mathcal{E}^{src}$ where $\mathcal{R} \in \{\leq, <, \geq, >, =, \neq\}$ stands for the relation between two expressions
- $\mathcal{E}^{src}$ **instanceof** $Class$ states that $\mathcal{E}^{src}$ has as type the class $Class$ or one of its subclasses

The expressions can be of object types or basic types. Formally the types are

$$JType ::= Class,\ Class \in \ \texttt{ClassTypes} \mid \textbf{int} \mid \texttt{boolean}$$

est-ce que je dois dire qu'on considere un sousensemble de Class qui represente les exceptions ?

The next definition gives the control flow constructs of our language as well as the expressions that have a side effect

Definition 7.2.2 (Statement) *The grammar for expressions is defined as follows :*

$$\begin{array}{rl} \mathcal{STMT} ::= & \mathcal{STMT};\mathcal{STMT} \\ & \mid \texttt{if}\ (\mathcal{E}^{\mathcal{R}})\ \texttt{then}\ \{\mathcal{STMT}\}\ \texttt{else}\ \{\mathcal{STMT}\} \\ & \mid \texttt{try}\ \{\mathcal{STMT}\}\ \texttt{catch}\ (\texttt{Exc}\ )\ \{\mathcal{STMT}\} \\ & \mid \texttt{try}\ \{\mathcal{STMT}\}\ \texttt{finally}\ \{\mathcal{STMT}\} \\ & \mid \texttt{throw}\ \mathcal{E}^{src} \\ & \mid \texttt{while}\ (\mathcal{E}^{\mathcal{R}})[\texttt{INV},\texttt{modif}]\ \ \{\mathcal{STMT}\} \\ & \mid \texttt{return}\ \mathcal{E}^{src} \\ & \mid \mathcal{E}^{src} = \mathcal{E}^{src} \end{array}$$

From the definition we can see that the language supports also the following constructs :

- $\mathcal{STMT};\mathcal{STMT}$, i.e. statements that execute sequentially
- $\texttt{if}\ (\mathcal{E}^{\mathcal{R}})\ \texttt{then}\ \{\mathcal{STMT}\}\ \texttt{else}\ \{\mathcal{STMT}\}$ which stands for an if statement. The semantics of the construct is the standard one, i.e. if the relation expression $\mathcal{E}^{\mathcal{R}}$ evaluates to true then the statement in the `then` branch is executed, otherwise the statement in the `else` branch is executed
- $\texttt{try}\ \{\mathcal{STMT}\}\ \texttt{catch}\ (Class)\ \{\mathcal{STMT}\}$ which states that if the statement following the `try` keyword throws an exception of type `Exc` then the exception will be caught by the statement following the `catch` keyword
- $\texttt{try}\ \{\mathcal{STMT}\}\ \texttt{finally}\ \{\mathcal{STMT}\}$

- `while` $(\mathcal{E}^{\mathcal{R}})$[`INV`, `modif`] $\{\mathcal{STMT}\}$ states for a loop statement where the body statement $\mathcal{STMT}$ will be executed until the relational expression $\mathcal{E}^{\mathcal{R}}$ evaluates to true.
- `return` $\mathcal{E}^{src}$ is the statement by which the execution will be finished
- $\mathcal{E}^{src} = \mathcal{E}^{src}$ stands for an assignment expression, where the value of the left expression is updated with the value of the right expression

7.3 Compiler

We now turn to specify a simple compiler from the source language presented in Section 7.2 into the bytecode language. The compiler does not perform any optimizations.

The compiler is the triple

$$< \ulcorner * \urcorner, *, *, \mathsf{addExcHandler}, \mathsf{addLoopSpec} >$$

The first element in the triple is a function $\ulcorner \urcorner$ which transforms statements and expressions into a sequence of bytecode instructions, the second element is the procedure addExcHandler which keeps track of the exception handlers. The third element of the compiler is the procedure addLoopSpec which manages the compilation of loop specification, namely loop invariants and the modified expressions.

In the following, in the next Section 7.3.1 we define the procedure for exception handlers, in Section 7.3.2, we will present the procedure for compiling loops and in Sections **??** and 7.3.4 we will proceed with the definition of the function $\ulcorner \urcorner$ for exressions and statements.

the exception handler function

7.3.1 Exception handler table

Our source language contains exception handler constructions, and thus, when compiling a method body the compiler should keep track of the exception handlers by adding information in the exception handler table array excHndlS (presented in Section 2.4) every time it sees one. To do this, the compiler is provided with a procedure with the following name and signature:

$$\mathsf{addExcHandler} : nat \rightarrow nat \rightarrow nat \rightarrow \mathbf{Class}_{exc} \rightarrow \mathbf{Method}$$

The definition of the procedure is the following:

$$\begin{array}{l} \mathsf{addExcHandler}(start,\ end,\ h,\ \mathtt{Exc}, \mathtt{m})) = \\ \quad \mathtt{m}.\mathsf{excHndlS} := \{(start, end, h, \mathtt{Exc}), \mathtt{m}.\mathsf{excHndlS}\} \end{array}$$

The function adds a new element in the exception handler table of a method `m`. The meaning of the new element is that every exception of type `Exc` thrown in between the instructions $start \ldots end$ can be handled by the code starting at index h.

We can remark that when the function addExcHandler adds a new element in the exception handler table array of a method m, the new element is added at the beginning of the exception handler table m.excHndlS.

7.3.2 Compiling loop invariants

When compiling a method m, the compiler will also take care of the loop specification in the source loops by adding it in the loop specification table m.loopSpecS(defined in Section 4.4) of the method m.

This is done by the procedure addLoopSpec which has the following signature

$$\mathsf{addLoopSpec} : nat \rightarrow P_{bml} \rightarrow list\ E_{bml} \rightarrow \mathbf{Method}$$

The definition of the procedure is hereafter:

$$\begin{array}{l}\mathsf{addLoopSpec}(i,\ \mathtt{INV},\ \mathtt{modif}, \mathtt{m}) = \\ \ \mathtt{m.loopSpecS} := \{(i, \mathtt{INV}, \mathtt{modif}), \mathtt{m.loopSpecS}\}\end{array}$$

7.3.3 Compiling expressions in bytecode instructions

As we stated in the beginning the function for compiling statements in bytecode instruction is named $\ulcorner\urcorner$

$$\ulcorner\urcorner : nat * (\mathcal{STMT} \cup \mathcal{E}^{src}) * nat \longrightarrow \text{I}[\ ]$$

The compiler function takes three arguments: a natural number s from which the labeling of the compilation of $\mathcal{STMT}$ starts, the statement $\mathcal{STMT}$ to be compiled and a natural number which is the greatest label in the compilation of $\mathcal{STMT}$ and returns an array of bytecode instructions. In the next we look at the definition of the compiler over expressions.

- integer or boolean constant access
  - integer constant access

$$\ulcorner s, \mathbf{constInt}, s\urcorner = s :\ \text{push } \mathbf{constInt}$$

  - boolean constant access

$$\ulcorner s, \mathit{true}, s\urcorner = s :\ \text{push } 1$$

$$\ulcorner s, \mathit{false}, s\urcorner = s :\ \text{push } 0$$

  Note: the source boolean expressions are compiled down to integers

- method invokation

$$\ulcorner s, \mathcal{E}_1^{src}.m(\mathcal{E}_2^{src}), e\urcorner = \begin{array}{l}\ulcorner s, \mathcal{E}_1^{src}, e'\urcorner; \\ \ulcorner e'+1, \mathcal{E}_2^{src}, e-1\urcorner; \\ e :\ \text{invoke } m\end{array}$$

- field access

$$\ulcorner s, \mathcal{E}^{src}.f, e \urcorner = \begin{array}{l} \ulcorner s, \mathcal{E}^{src}, e-1 \urcorner; \\ e: \text{ getfield } f \end{array}$$

- local variable access

$$\ulcorner s, \mathbf{var}, s \urcorner = s: \text{ load } \mathbf{reg}(i)$$

  where $\mathbf{reg}(i)$ is the local variable at index i

- arithmetic expressions

$$\ulcorner s, \mathcal{E}_1^{src} \; op \; \mathcal{E}_2^{src}, e \urcorner = \begin{array}{l} \ulcorner s, \mathcal{E}_1^{src}, e' \urcorner; \\ \ulcorner e'+1, \mathcal{E}_2^{src}, e-1 \urcorner; \\ e: \text{ arith\_op} \end{array}$$

- cast expression

$$\ulcorner s, (\texttt{ Class}) \; \mathcal{E}^{src}, e \urcorner = \begin{array}{l} \ulcorner s, \mathcal{E}^{src}, e-1 \urcorner; \\ e: \text{ checkcast } \texttt{Class} \; ; \end{array}$$

- instanceof expression

$$\ulcorner s, \mathcal{E}^{src} \textbf{ instanceof } Class, e \urcorner = \begin{array}{l} \ulcorner s, \mathcal{E}^{src}, e-1 \urcorner; \\ e: \text{ instanceof } Class; \end{array}$$

- null expression

$$\ulcorner s, \mathbf{null}, s \urcorner = s: \text{ push } \mathbf{null}$$

- object creation

$$\ulcorner s, \mathbf{new} \; Class(\mathcal{E}^{src}), e \urcorner = \begin{array}{l} s: \text{ new } Class; \\ s+1: \text{ dup}; \\ \ulcorner s+2, \mathcal{E}^{src}, e-1 \urcorner; \\ e: \text{ invoke } \mathsf{constr}(Class); \end{array}$$

- this instance

$$\ulcorner s, \mathbf{this}, s \urcorner = s: \text{ load } \mathbf{reg}(0)$$

7.3.4 Compiling control statements in bytecode instructions

- compositional statement

$$\begin{array}{l} \ulcorner s, \mathcal{STMT}_1; \mathcal{STMT}_2, e \urcorner = \\ \ulcorner s, \mathcal{STMT}_1, e' \urcorner; \\ \ulcorner e'+1, \mathcal{STMT}_2, e \urcorner \end{array}$$

about the compilation of exception handlers

a redundant jump added in the compilation in order to see explicitely the relation between stmt1 and stmt2

- if statement

$$
\begin{array}{l}
\ulcorner s, \texttt{if}\ (\mathcal{E}^{\mathcal{R}})\ \texttt{then}\ \{\mathcal{STMT}_1\}\ \texttt{else}\ \{\mathcal{STMT}_2\}, e\urcorner = \\
\ulcorner s, \mathcal{E}^{\mathcal{R}}, e'\urcorner; \\
e'+1:\ \text{if\_cond}\ \ e''+2; \\
\ulcorner e'+2, \mathcal{STMT}_2), e''\urcorner \\
e''+1:\ \text{goto}\ \ e+1; \\
\ulcorner e''+2, \mathcal{STMT}_1, e\urcorner;
\end{array}
$$

- assignment statement. We consider the case for instance field assignment as well as assignemnts to method local variables and parameters.

  - field assignement.

$$
\begin{array}{l}
\ulcorner s, \mathcal{E}_1^{src}.f = \mathcal{E}_2^{src}, e\urcorner = \\
\ulcorner s, \mathcal{E}_1^{src}, e'\urcorner; \\
\ulcorner e'+1, \mathcal{E}_2^{src}, e-1\urcorner; \\
e:\ \text{putfield}\ f;
\end{array}
$$

  - method local variable or parameter update

$$
\begin{array}{l}
\ulcorner s, \mathbf{var} = \mathcal{E}^{src}, e\urcorner = \\
\ulcorner s, \mathcal{E}^{src}, e-1\urcorner \\
e:\ \text{store}\ \mathbf{reg}(i);
\end{array}
$$

- try catch statement

$$
\begin{array}{l}
\ulcorner s, \texttt{try}\ \{\mathcal{STMT}_1\}\ \texttt{catch}\ (\mathit{ExcType}\ \mathbf{var})\{\mathcal{STMT}_2\}, e\urcorner = \\
\ulcorner s, \mathcal{STMT}_1, e'\urcorner; \\
e'+1:\ \text{goto}\ \ e+1; \\
\ulcorner e'+2, \mathcal{STMT}_2, e\urcorner;
\end{array}
$$

$$\mathsf{addExcHandler}(s,\ e',\ e'+2,\ \mathit{ExcType}, \texttt{m}))$$

  The compiler compiles the normal statement $\mathcal{STMT}_1$ and the exception handler $\mathcal{STMT}_2$.

- try finally statement

$\ulcorner s, \texttt{try}\ \{\mathcal{STMT}_1\}\ \texttt{finally}\ \{\mathcal{STMT}_2\}, e \urcorner =$
$\ulcorner s, \mathcal{STMT}_1, e' \urcorner;$
$\ulcorner e'+1, \mathcal{STMT}_2, e'' \urcorner;$
$e''+1:$ goto $e+1;$

{ default exception handler}
$e''+2:$ store $l;$
$\ulcorner e''+3, \mathcal{STMT}_2, e-2 \urcorner;$
$e-1:$ load $l;$
$e:$ athrow;

$\mathsf{addExcHandler}(s,\ e',\ e''+2,\ \texttt{Exception}, \texttt{m})$

As you can notice, we compile the finally statement $\mathcal{STMT}_2$ by inlining, it is first compiled as a code executed after $\mathcal{STMT}_1$ and then it is compiled as part of the default exception handler. The default exception handler which starts at index $e''+2$ and which will handle any exception thrown by $\ulcorner s, \mathcal{STMT}_1, e' \urcorner$. The exception handler first stores the thrown exception in the local variable at index l, then executed the subroutine code and after the execution rethrows the exception stored in the local variable l.

This compilation differs from the compilation scheme in the JVM specification for finally statements, which requires that the subroutines must be compiled using jsr and ret instructions. However, the semantics of the programs produced by the compiler presented here and a compiler which follows closely the JVM specification is equivalent. In the following, we discuss informally why this is true. The semantics of a jsr k insruction is to jump to the first instruction of the compiled subroutine which starts at index k and pushes on the operand stack the index of the next instruction of the jsr that caused the execution of the subroutine. The first instruction of the compilation of the subroutine stores the stack top element in the local variable at index k (i.e. stores in the local variable at index k the index of the instruction following the jsr instruction). Thus, after the code of the subroutine is executed, the ret k instruction jumps to the instruction following the corresponding jsr . This behaviour can be actually simulated by programs without jsr and ret but which inline the subroutine code at the places where a jsr to the subroutine is done.

Note:

1. we assume that the local variable l is not used in the compilation of the statement $\mathcal{STMT}_2$, which guarantees that after any execution which terminates normally of $\ulcorner e''+3, \mathcal{STMT}_2, e-2 \urcorner$ the local variable l will still hold the thrown object
2. here we also assume that the statement $\mathcal{STMT}_1$ does not contain a return instruction

verify this

The last remark that we would like to make is that subroutines and their compilation via ret and jsr has always presented a problem for Java. First, they slow down the performance of the JVM because of the special way ret and jsr work . Second, the analysis performed by the bytecode verifier in the JVM becomes rather complex because (and its first version was erroneus) of the Java subroutines. In the last version of Java Sun compiler, subroutines has become obsolete where they are compiled by inlining. Thus, the compiler presented here represents a realistic approximation of the Java Sun compiler.

- throw exception statement

$$\ulcorner s,\ \text{athrow}\ \mathcal{E}^{src}, e\urcorner = \begin{array}{l}\ulcorner s, \mathcal{E}^{src}, e-1\urcorner;\\ e:\ \text{athrow};\end{array}$$

- loop statement

$$\begin{array}{l}\ulcorner s, \texttt{while}\ (\mathcal{E}^{\mathcal{R}})[\texttt{INV},\texttt{modif}]\ \ \{\mathcal{STMT}\}, e\urcorner =\\ \quad s:\ \text{goto}\ \ e'+1;\\ \quad \ulcorner s+1, \mathcal{STMT}, e'\urcorner;\\ \quad \ulcorner e'+1, \mathcal{E}^{\mathcal{R}}, e-1\urcorner;\\ \quad e:\ \text{if\_cond}\ \ s+1;\end{array}$$

$$\mathsf{addLoopSpec}(e'+1,\ \texttt{INV},\ \texttt{modif},\texttt{m})$$

- return statement

$$\ulcorner s, \texttt{return}\ \mathcal{E}^{src}, e\urcorner = \begin{array}{l}\ulcorner s, \mathcal{E}^{src}, e-1\urcorner;\\ e:\ \text{return}\end{array}$$

7.3.5 Properties of the compiler function

In this subsection, we will focus on the properties of the bytecode produced by the compiler. These properties although a straightforward consequence of the compiler definition are actually important for establishing formally the equivalence between source and bytecode proof obligations. Note also that those properties are respected by any non optimizing compiler.

In the following, we use the notation $\mathcal{S}$ when we refer both to statements $\mathcal{STMT}$ and $\mathcal{E}^{src}$.

The first property that we observe is that the last instruction e : `instr` in the compilation $\ulcorner s, \mathcal{STMT}, e\urcorner$ of a statement $\mathcal{STMT}$ is always in execution relation with the instruction $e+1$: `instr`.

Property 7.3.5.1 (Compilation of statements and expressions) *For any statement or expression $\mathcal{S}$ which does not terminate on* return *, start label s and end label e, the compiler will produce a list of bytecode instruction*

$\ulcorner s, \mathcal{STMT}, e \urcorner$ *such that*

$$e : \texttt{instr} \rightarrow e + 1 : \texttt{instr}$$

The proof is trivial by case analysis of the compiled statements.

Informally, the following property states that if there are instructions inside a compiled statetement or expression $\ulcorner s, \mathcal{S}, e \urcorner$ which are in execution relation[1] with an instruction $k : \texttt{instr}$ which is not the start of an exception handler and which is outside $\ulcorner s, \mathcal{S}, e \urcorner$ then $k = e+1$. The conditions $\neg(k : \texttt{instr} \in \ulcorner s, \mathcal{S}, e \urcorner)$ and
$\neg isExcHandlerStart(k : \texttt{instr})$ eliminate the case when the execution relation is between an instruction inside $\ulcorner s, \mathcal{S}, e \urcorner$ which may throw an exception and the start instruction of the proper handler exception handler.

Property 7.3.5.2 (Compilation of statements and expressions) *For any statement or expression $\mathcal{S}$, start label s and end label e, the compiler will produce a list of bytecode instruction $\ulcorner s, \mathcal{S}, e \urcorner$ such that:*

$$\begin{array}{l} \forall i, (i : \texttt{instr} \in \ulcorner s, \mathcal{S}, e \urcorner) \wedge \\ \quad (i : \texttt{instr} \rightarrow k : \texttt{instr}) \wedge \\ \quad \neg(k : \texttt{instr} \in \ulcorner s, \mathcal{S}, e \urcorner) \\ \quad \neg isExcHandlerStart(k : \texttt{instr}) \Rightarrow \\ \qquad k = e + 1 \end{array}$$

The proof is done by induction on the structure of the compiled statement. We scatch the proof for the compilation of the if statement, the rest of the cases being similar

[1] see Def. 2.9.1

Proof:

{ *Assume that* $\exists i, i \in [s \dots e], \exists k, k \notin [s \dots e+1] \wedge i : \texttt{instr} \rightarrow k : \texttt{instr}$ }

{ *by definition of the compiler function for if statements in section 7.3.4* }
$\ulcorner s, \texttt{if } (\mathcal{E}^{\mathcal{R}}) \texttt{ then } \{\mathcal{STMT}_1\} \texttt{ else } \{\mathcal{STMT}_2\}, e \urcorner =$
$\ulcorner s, \mathcal{E}^{\mathcal{R}}, e' \urcorner;$
$e'+1$ if_cond $e''+2;$
$\ulcorner e'+2, \mathcal{STMT}_2, e'' \urcorner$
$e''+1$ goto $e+1;$
$\ulcorner e''+2, \mathcal{STMT}_1, e \urcorner;$

(1) { *Assume that* $s \leq i \leq e'$ }
{ *by induction hypothesis for* $\mathcal{E}^{\mathcal{R}}$ *we get* }
(2)$\forall i, s \leq i \leq e',\ i : \texttt{instr} \rightarrow k : \texttt{instr}) \wedge$
$\neg(k : \texttt{instr} \in \ulcorner s, \mathcal{STMT}, e \urcorner)$
$\neg isExcHandlerStart(k : \texttt{instr}) \Rightarrow$
$k = e' + 1$
{ *From (1) and (2) we get a contradiction in this case*}

(3) { *Assume that* $e'+2 \leq i \leq e''$ }
(4) $\forall i, e'+2 \geq i \leq e'',\ i : \texttt{instr} \rightarrow k : \texttt{instr}) \wedge$
$\neg(k : \texttt{instr} \in \ulcorner s, \mathcal{STMT}, e \urcorner)$
$\neg isExcHandlerStart(k : \texttt{instr}) \Rightarrow$
$k = e'' + 1$
{ *From (3) and (4) we get a contradiction in this case*}

(5) { *Assume that* $e''+2 \leq i \leq e$ }
(6) $\forall i, e''+2 \geq i \leq e,\ i : \texttt{instr} \rightarrow k : \texttt{instr}) \wedge$
$\neg(k : \texttt{instr} \in \ulcorner s, \mathcal{STMT}, e \urcorner)$
$\neg isExcHandlerStart(k : \texttt{instr}) \Rightarrow$
$k = e + 1$

{ *From (5) and (6) we get a contradiction in this case*}

(7){ *Assume that* $s = e' + 1$ }
{ *as* $e'+1$ if_cond $e''+2$ *and* $e''+2$ *and* $e'+2$ *are labels in the compilation of the statement, we get a contradiction in this case* }

(8){ *Assume that* $s = e'' + 1$ }
{ *as* $e''+1$ goto $e+1$ *we get a contradiction once again*

Qed.

Another property of the compiler is that any statement or expression is compiled in a list of bytecode instructions such that there could not be jumps from outside inside the list, i.e. the control flow can reach the instructions

representing the compilation $\ulcorner s, \mathcal{S}, e \urcorner$ of statement $\mathcal{S}$ only by passing through the beginning of the compilation i_s.

Property 7.3.5.3 (Compilation of statements and expressions) *For all statements $\mathcal{S}'$ and $\mathcal{S}$, such that*

- *$\mathcal{S}$ is such that it has as substatement $\mathcal{S}'$, which we denote with $\mathcal{S}[\mathcal{S}']$*
- *their compilations are $\ulcorner s, \mathcal{S}, e \urcorner$ and $\ulcorner s', \mathcal{S}', e' \urcorner$*

then :

$$\begin{array}{l}\neg(\exists i_j, \exists i_k, \\ \quad i_j \in \ulcorner s, \mathcal{S}[\mathcal{S}'], e \urcorner \wedge \\ \quad \neg(i_j \in \ulcorner s', \mathcal{S}', e' \urcorner) \wedge \\ \quad i_k \in \ulcorner s', \mathcal{S}', e' \urcorner \wedge \\ \quad s' \neq k \wedge \qquad i_j \rightarrow i_k)\end{array}$$

The proof is done by induction over the structure of statements and expressions and uses the previous lemma 7.3.5.2

The following property establishes that the compiler preserves the substatement relation between statements and expressions.

Property 7.3.5.4 (Substatement and subexpression relation preserved) *For all statements $\mathcal{S}_1$ and $\mathcal{S}_2$ such that their compilations are $\ulcorner s_1, \mathcal{S}_1, e_1 \urcorner$ and that $\ulcorner s_2, \mathcal{S}_2, e_2 \urcorner$, if we have that $\exists k, s_1 \leq k \leq e_1 \wedge s_2 \leq k \leq e_2$ then the following holds:*

$$\begin{array}{l}\ulcorner s_2, \mathcal{S}_2, e_2 \urcorner \in \ulcorner s_1, \mathcal{S}_1, e_1 \urcorner \\ \vee \\ \ulcorner s_1, \mathcal{S}_1, e_1 \urcorner \in \ulcorner s_2, \mathcal{S}_2, e_2 \urcorner\end{array}$$

Now, we give a definition for a set of instructions such that they execute sequentially

Definition 7.3.5.1 (Block of instructions) *If the list of instructions $l = [i_1 : \texttt{instr} \ldots i_n : \texttt{instr}]$ in the compilation of method $\texttt{m}$is such that*

- *none of the instructions is a target of an instruction $i_j : \texttt{instr}$ which does not belong to l except for $i_1 : \texttt{instr}$*
- *none of the instructions in the set is a jump instruction, i.e. $\forall m, m = 1..k \Rightarrow \neg(i_m : \texttt{instr} \in \{$ goto , if_cond $\})$*
- *$\forall j, i_1 < j \leq i_n, \neg\exists k \in \texttt{m.body}, k : \texttt{instr} \rightarrow^l j : \texttt{instr}$*

We denote such a list of instructions with $i_1 : \texttt{instr}; ...; i_k : \texttt{instr}$

The next lemma states that the compilation of an expression $\mathcal{E}^{src}$ results in a block of bytecode instructions.

Property 7.3.5.5 (Compilation of expressions) *For any expression $\mathcal{E}^{src}$, starting label s and end label e, the compilation $\ulcorner s, \mathcal{E}^{src}, e \urcorner$ is a block of bytecode instruction in the sense of Def. 7.3.5.1*

Following the definition 7.3.5.1 of block of bytecode instructions, the property states that the compilation of an expression results in a list of instructions that cannot be jumped from outside its compilation except for the first instruction of the compilation. This follows from lemma 7.3.5.3.

Definition 7.3.5.1 also requires that there are no jump instructions in the list of instructions representing the compilation of an expression. This is established by induction over the structure of the expression.

The third condition in Def. 7.3.5.1 states that the compilation $\ulcorner s, \mathcal{E}^{src}, e \urcorner$ is such that no instruction except s : `instr` may be a loop entry in the sense of Def. 2.9.2 in Chapter 5, Section 2.9. This is the case, as there are no jump instructions inside the compiled expression and all the instructions inside an expression are sequential .

this is not well explained

Our source language supports also exception handling. As we saw in the previous section, the compiler will keep track of the exception handlers by adding them in the exception handler table. We now establish that the elements in the exception handler table correspond to a statement in the source language.

Property 7.3.5.6 (Exception handler element corresponds to a statement) *Every element $(s, e, eH, \texttt{Exc})$ in the exception handler table* m.excHndlS *is such that exists a statement $\mathcal{STMT}$ such that $\ulcorner s, \mathcal{STMT}, e \urcorner$*

Proof: The proof is done by contradiction. From the compiler definition, we get that elements are added in m.excHndlS only in the cases of try catch and try finally statement compilation and that the guarded regions in the added elements correspond to statements.

In the rest of this subsection we will look at properties of the compiler which are a consequence of the upper properties. We can establish also that the compilation of a statement $\mathcal{STMT}$ may contain cycles only if $\mathcal{STMT}$ is a cycle or contains a substatement which is a cycle.

alternative formulation: say that the only loop entries are the first instructions of a loop body

Property 7.3.5.7 (Cycles in the control flow graph) *The compilation $\ulcorner s, \mathcal{STMT}, e \urcorner$ of a $\mathcal{STMT}$ may contain an instruction k : `instr` which is a loop entry in the sense of definition* **??** *(i.e. there exists j : `instr` such that j : `instr` $\rightarrow^l$ k : `instr`) only if $\mathcal{STMT}$ is a loop or contains a substatement*

$\mathcal{STMT}'$ which is a loop statement and the following holds:

$$\mathcal{STMT} = \texttt{while } (\mathcal{E}^{\mathcal{R}})[\texttt{INV}, \texttt{modif}] \ \ \{\mathcal{STMT}\}$$

$$\vee$$

$$\mathcal{STMT}[\mathcal{STMT}'] \wedge \mathcal{STMT}' = \texttt{while } (\mathcal{E}^{\mathcal{R}})[\texttt{INV}, \texttt{modif}] \ \ \{\mathcal{STMT}\}$$

$$\ulcorner s, \texttt{while } (\mathcal{E}^{\mathcal{R}})[\texttt{INV}, \texttt{modif}] \ \ \{\mathcal{STMT}\}, e \urcorner = s: \text{ goto } e' + 1; \ulcorner s+1, \mathcal{STMT}, e' \urcorner; \ulcorner e'+1, \mathcal{E}^{\mathcal{R}}, e-1 \urcorner; e: \text{ if\_cond } s+1;$$

$$\Rightarrow k = e' + 1 \wedge j = e'$$

Another property concerning cycles in the control flow graph is that all the instructions in a compilation$\ulcorner s, \mathcal{STMT}, e \urcorner$ of a statement $\mathcal{STMT}$which target the instruction $e+1$: `instr` are in the same execution relation with $e+1$: `instr`,i.e. if $e+1$: `instr` is a loop entry either all are loop ends or none of them is:

Property 7.3.5.8 (Cycles in the control flow graph) *For every statement $\mathcal{STMT}$ its compilation $\ulcorner s, \mathcal{STMT}, e \urcorner$ is such that* $(\exists k, s \leq k \leq e, k : \texttt{instr} \rightarrow^{l} e+1 : \texttt{instr}) \iff (\forall k, s \leq k \leq e, k : \texttt{instr} \rightarrow e+1 : \texttt{instr} \Rightarrow k : \texttt{instr} \rightarrow^{l} e+1 : \texttt{instr})$

Property 7.3.5.9 (Exception handler property for statements) *For every statement $\mathcal{STMT}$ which is not a try catch in method* `m` *and its substatement $\mathcal{STMT}'$, which we denote with $\mathcal{STMT}[\mathcal{STMT}']$ such that $\neg\,(\exists \mathcal{STMT}'', \mathcal{STMT}[\mathcal{STMT}''] \wedge \mathcal{STMT}''[\mathcal{STMT}'])$ we have that if their respective compilations are $\ulcorner s, \mathcal{STMT}, e \urcorner$ and $\ulcorner s', \mathcal{STMT}', e' \urcorner$ then the following holds:*

$$\forall \texttt{Exc}, \mathit{findExcHandler}(\texttt{Exc}, e, \texttt{m.excHndlS}) = \mathit{findExcHandler}(\texttt{Exc}, e', \texttt{m.excHndlS})$$

give the definition of the function *isExcHandlerStart*(`k` : `instr`)

Proof: The proof is by contradiction. Assume this is not true, i.e.

$$\begin{array}{ll} \exists \mathcal{STMT}, \mathcal{STMT}', & \\ (1) & \mathcal{STMT} \neq \texttt{try}\{\ldots\}\texttt{catch}\{\ldots\} \wedge \\ (2) & \mathcal{STMT}[\mathcal{STMT}'] \wedge \neg\,(\exists \mathcal{STMT}'', \mathcal{STMT}[\mathcal{STMT}''] \wedge \mathcal{STMT}''[\mathcal{STMT}']) \wedge \\ (3) & \ulcorner s, \mathcal{STMT}, e \urcorner \wedge \\ (4) & \ulcorner s', \mathcal{STMT}', e' \urcorner \wedge \\ (5) & \exists \texttt{Exc}, \mathit{findExcHandler}(\texttt{Exc}, e, \texttt{m.excHndlS}) \neq \\ & \mathit{findExcHandler}(\texttt{Exc}, e', \texttt{m.excHndlS}) \end{array}$$

This means that there exists two elements $(s_1, e_1, eH_1, \texttt{Exc})$ and $(s_2, e_2, eH_2, \texttt{Exc})$ in the exception handler table of method $\texttt{m}$ $\texttt{m.excHndlS}$ such that :

$$(6) \quad eH_1 \neq eH_2$$

From lemma 7.3.5.6 we get that :

$$(7) \quad \begin{array}{l} \exists \mathcal{STMT}_1, s_1, e_1, \ulcorner s_1, \mathcal{STMT}_1, e_1 \urcorner \\ \wedge \\ \exists \mathcal{STMT}_2, s_2, e_2, \ulcorner s_2, \mathcal{STMT}_2, e_2 \urcorner \end{array}$$

From the initial condition *(2)* we conclude that

$$(8) \quad \ulcorner s_1, \mathcal{STMT}_1, e_1 \urcorner \notin \ulcorner s, \mathcal{STMT}, e \urcorner$$

Because $e \in [s_2 \dots e_2] \wedge e' \in [s_1 \dots e_1] \wedge e, e' \in [s \dots e]$, *(8)* by applying Lemma 7.3.5.4 we can conclude that

$$\begin{array}{l} \ulcorner s, \mathcal{STMT}, e \urcorner \in \ulcorner s_1, \mathcal{STMT}_1, e_1 \urcorner \in \ulcorner s_2, \mathcal{STMT}_2, e_2 \urcorner \\ \vee \\ \ulcorner s, \mathcal{STMT}, e \urcorner \in \ulcorner s_2, \mathcal{STMT}_2, e_2 \urcorner \in \ulcorner s_1, \mathcal{STMT}_1, e_1 \urcorner \end{array}$$

In both of the cases and of the definition of *findExcHandler* in Chapter 2.8, Section 2.7 this means that

$$\mathit{findExcHandler}(\texttt{Exc}, e, \texttt{m.excHndlS}) = \mathit{findExcHandler}(\texttt{Exc}, e', \texttt{m.excHndlS})$$

which is in contradiction with *(6)*.

A similar property can be established about expressions

Property 7.3.5.10 (Exception handler property for expressions) *For every statement $\mathcal{STMT}$ which is not a try catch in method $\texttt{m}$ and its subexpression $\mathcal{E}^{src}$, which we denote with $\mathcal{STMT}[\mathcal{E}^{src}]$ such that $\neg\ (\exists \mathcal{STMT}'', \mathcal{STMT}''[\mathcal{E}^{src}] \wedge \mathcal{STMT}[\mathcal{STMT}''])$ we have that if their respective compilations are $\ulcorner s, \mathcal{STMT}, e \urcorner$ and $\ulcorner s', \mathcal{E}^{src}, e' \urcorner$ and (2) then the following holds:*

$$\begin{array}{l} \forall \texttt{Exc}, \forall i, s' \leq i \leq e', \mathit{findExcHandler}(\texttt{Exc}, e, \texttt{m.excHndlS}) = \\ \quad \mathit{findExcHandler}(\texttt{Exc}, i, \texttt{m.excHndlS}) \end{array}$$

The last property concerns try catch statements

Property 7.3.5.11 (Exception handlers and try catch statements) *For ever try catch statement* $\texttt{try}\ \{\mathcal{STMT}_1\}\ \texttt{catch}\ (\mathit{ExcType}\ \textbf{var})\{\mathcal{STMT}_2\}$ *its compilation*

$$\begin{array}{l} \ulcorner s, \mathcal{STMT}_1, e' \urcorner; \\ e' + 1 :\ \text{goto}\ \ e + 1; \\ \ulcorner e' + 2, \mathcal{STMT}_2, e \urcorner; \end{array}$$

is such that the following holds

$$\begin{array}{l} \forall \neg(\texttt{Exc} <: \mathit{ExcType}) \Rightarrow \quad \mathit{findExcHandler}(\texttt{Exc}, e', \texttt{m.excHndlS}) = \\ \quad \mathit{findExcHandler}(\texttt{Exc}, e, \texttt{m.excHndlS}) \\ \wedge \mathit{findExcHandler}(\mathit{ExcType}, e', \texttt{m.excHndlS}) = e' + 2 \end{array}$$

7.4 Weakest precondition calculus for source programs

7.4.1 Source assertion language

The properties that our predicate calculus treats are from first order predicate logic. In the following, we give the formal definition of the assertion language into which the properties are encoded. Note that the language is the same to the bytecode assertion language presented earlier modulo the stack expressions **st**(**cntr** $+ - \ldots$) and **cntr** .

Formulas 1 (Definition) *The set of formulas is defined inductively as follows*

$$
\begin{array}{ll}
\mathcal{F} ::= & \psi(\mathcal{E}^{spec}, \mathcal{E}^{spec}) \\
& |\textbf{instances}(\mathcal{E}^{spec}) \\
& |\textbf{true} \\
& |\textbf{false} \\
& |\mathcal{F} \wedge \mathcal{F} \\
& |\mathcal{F} \vee \mathcal{F} \\
& |\mathcal{F} \Rightarrow \mathcal{F} \\
& |\forall x(\mathcal{F}(x)) \\
& |\exists x(\mathcal{F}(x))
\end{array}
$$

$$
\mathcal{R} ::= \quad ==|\neq|\leq|\leq|\geq|>|<:
$$

$$
\begin{array}{ll}
\mathcal{E}^{spec} ::= & \textbf{constInt} \\
& | \ \textit{true} \\
& | \ \textit{false} \\
& | \ \textbf{boundVar} \\
& | \ \mathcal{E}^{spec} \ \textit{op} \ \mathcal{E}^{spec} \\
& | \ \mathcal{E}^{spec}.f \\
& | \ \textbf{var} \\
& | \ \textbf{null} \\
& | \ \textbf{this} \\
& | \ \backslash\textbf{typeof}(\mathcal{E}^{spec}) \\
& | \ \backslash\textbf{result}
\end{array}
$$

7.4.2 Weakest Predicate Transformer for the Source Language

The weakest precondition calculates for every statement $\mathcal{STMT}$ in method `m` from our source language, for any normal postcondition *Post* and exceptional postcondition function $\mathsf{excPost}^{src}$ ($\mathtt{Exc} \rightarrow \mathcal{STMT} \rightarrow \mathcal{F}$), the predicate *Pre* such that if it holds in the pre state of $\mathcal{STMT}$ and if $\mathcal{STMT}$ terminates normally then *Post* holds in the poststate and if $\mathcal{STMT}$ terminates on exception

Exc then $\mathsf{excPost}^{src}(Exc, \mathcal{STMT})$ holds. In the following, in subsection 7.4.2 we discuss how the exceptional postcondition function is defined. Subsections 7.4.2 and 7.4.2 present respectively the definition of *wp* function for expressions and for statements.

Exceptional Postcondition Function

As we stated earlier the weakest predicate transformer manages both the normal and exceptional termination of an expression(statement). In both cases the expression(statement) has to satisfy some condition : the normal postcondition in case of normal termination and the exceptional postcondition for exception `Exc` if it terminates on exception `Exc`

We introduce a function $\mathsf{excPost}^{src}$ which maps exception types to predicates

$$\mathsf{excPost}^{src} : \ \texttt{ETypes} \ \longrightarrow Predicate$$

The function $\mathsf{excPost}^{src}$ returns the predicate $\mathsf{excPost}^{src}(\texttt{Exc})$ that must hold in a particular program point if at this point an exception of type `Exc` is thrown.

We also use function updates for $\mathsf{excPost}^{src}$ which are defined in the usual way

$$\mathsf{excPost}^{src}[\oplus\texttt{Exc'} \rightarrow P](\texttt{Exc}, exp) = \begin{cases} P & if \texttt{Exc} <: \texttt{Exc'} \\ \mathsf{excPost}^{src}(\texttt{Exc}, exp) & else \end{cases}$$

Expressions

The weakest precondition function for expressions has the following signature:

$$wp^{src} : \mathcal{E}^{src} \rightarrow \mathcal{F} \rightarrow (\ \texttt{Exc} \rightarrow \mathcal{F}) \rightarrow \textbf{Method} \rightarrow \mathcal{E}^{spec} \rightarrow \mathcal{F}$$

For calculating the wp^{src} predicate of an expression $\mathcal{E}^{src}$ declared in method `m`, the function wp^{src} takes as arguments $\mathcal{E}^{src}$, a postcondition nPost^{src}, an exceptional postcondition function $\mathsf{excPost}^{src}$ and an $\mathcal{E}^{spec}$ and returns the formula $\mathrm{wp}^{src}(\mathcal{E}^{src}, \psi, \mathsf{excPost}^{src}, \texttt{m})_{\mathcal{E}^{spec}}$ which is the *wp* precondition of $\mathcal{E}^{src}$ if the its value is represented by $\mathcal{E}^{spec}$.

In the following, we give the rules of wp^{src}.

- integer and boolean constant access
  ($const \in \{\textbf{constInt}, true, false, \textbf{constRef}\}$)

$$\mathrm{wp}^{src}(const, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \texttt{m})_{const} = \mathsf{nPost}^{src}$$

- field access expression

$$\begin{array}{l}\mathrm{wp}^{src}(\mathcal{E}_1^{src}.f, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{v.f} = \\ \mathrm{wp}^{src}(\mathcal{E}_1^{src}, \\ \qquad v \neq \mathbf{null} \Rightarrow \mathsf{nPost}^{src} \\ \qquad \wedge \\ \qquad v = \mathbf{null} \Rightarrow \mathsf{excPost}^{src}(\ \mathtt{NullPointerExc}, \mathcal{E}_1^{src}) \\ \qquad \mathsf{excPost}^{src}, \mathtt{m})_v\end{array} ,$$

- arithmetic expressions

$$\begin{array}{l}\mathrm{wp}^{src}(\mathcal{E}_1^{src}\ op\ \mathcal{E}_2^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{v_1+v_2} = \\ \mathrm{wp}^{src}(\mathcal{E}_1^{src}, \mathrm{wp}^{src}(\mathcal{E}_2^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{v_2}, \mathsf{excPost}^{src}, \mathtt{m})_{v_1}\end{array}$$

- method invokation

$$\begin{array}{l}\mathrm{wp}^{src}(\mathcal{E}^{src}.m(), \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_v = \\ \mathrm{wp}^{src}(\mathcal{E}^{src}, \\ \left\{\begin{array}{l} v' \neq\ \mathbf{null} \Rightarrow \\ \qquad m.\mathsf{Pre}^{src}[\mathbf{this} \leftarrow v'] \\ \qquad \wedge \\ \qquad \forall \mathbf{boundVar},\ \forall\ m \in m.\mathsf{modif}^{src} \\ \qquad \left\{\begin{array}{l} \backslash\mathbf{typeof(boundVar)} <: m.\mathsf{retType} \wedge \\ m.\mathsf{nPost}^{src}\ [\backslash\mathbf{result} \leftarrow \mathbf{boundVar}] \\ \qquad\qquad [\mathbf{this} \leftarrow v'] \\ \qquad\quad \Rightarrow \mathsf{nPost}^{src}[v \leftarrow \mathbf{boundVar}] \end{array}\right. \\ \qquad \wedge \\ \qquad \forall \mathtt{E} \in m.\mathsf{exceptions}^{src}, \\ \qquad \forall\ m \in m.\mathsf{modif}^{src} \\ \qquad\ m.\mathsf{excPostSpec}^{src}(\mathtt{E}) \Rightarrow \mathsf{excPost}^{src}(\mathtt{E}) \\ \mathcal{E}_1^{src} =\ \mathbf{null} \Rightarrow \mathsf{excPost}^{src}(\ \mathtt{NullPntrExc}) \end{array}\right. \\ \mathsf{excPost}^{src}, \mathtt{m})_{v'}\end{array} ,$$

- Cast expression

may be give an example

$$\begin{array}{l}\mathrm{wp}^{src}((\ \mathrm{Cl}\ )\ \mathcal{E}^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_v = \\ \mathrm{wp}^{src}(\mathcal{E}^{src}, \\ \qquad \backslash\mathbf{typeof}(v) <:\ \mathrm{Cl}\ \Rightarrow \\ \qquad\qquad \mathsf{nPost}^{src} \\ \qquad \wedge \\ \qquad \neg\ \backslash\mathbf{typeof}(v) <:\ \mathrm{Cl}\ \Rightarrow \\ \qquad\qquad \mathsf{excPost}^{src}(\ \mathtt{CastExc}) \\ \qquad \mathsf{excPost}^{src}, \mathtt{m})_v\end{array} ,$$

- Null expression

$$\mathrm{wp}^{src}(\mathbf{null}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{\mathbf{null}} = \mathsf{nPost}^{src}$$

- this

$$\mathrm{wp}^{src}(\mathbf{this}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{\mathbf{this}} = \mathsf{nPost}^{src}$$

- instance creation

$$\begin{array}{l}\mathrm{wp}^{src}(\mathbf{new}\ \ \mathrm{Cl}\ (\mathcal{E}^{src}), \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_v = \\ \mathrm{wp}^{src}(\mathcal{E}^{src},\end{array}$$

$$\left\{\begin{array}{l}\forall \mathbf{boundVar},\\ \quad \mathit{not}\ \mathbf{instances}(\mathbf{boundVar}) \wedge\\ \quad \mathbf{boundVar} \neq \mathbf{null} \Rightarrow\\ \qquad \mathsf{constr}(\ \mathrm{Cl}\ ).\mathsf{Pre}^{src}\ \begin{array}{l}[\mathbf{this} \leftarrow \mathit{RefValClClass}]\\ [\mathit{arg} \leftarrow v']\end{array}\\ \qquad \wedge\\ \qquad \forall\ m \in \mathsf{constr}(\mathit{Class}).\mathsf{modif}^{src},\\ \qquad\quad \mathsf{constr}(\mathit{Class}).\mathsf{nPost}^{src}\ \begin{array}{l}[\mathbf{this} \leftarrow \mathbf{boundVar}]\\ [\mathit{arg} \leftarrow v']\\ [\backslash\mathbf{typeof(boundVar)} \leftarrow \mathit{Class}]\end{array}\\ \qquad\quad \Rightarrow \mathsf{nPost}^{src}[v \leftarrow \mathbf{boundVar}]\\ \qquad \wedge\\ \qquad \forall \mathtt{Exc} \in \mathsf{constr}(\mathit{Class}).\mathsf{exceptions}^{src},\\ \qquad \forall\ m \in \mathsf{constr}(\mathit{Class}).\mathsf{modif}^{src},\\ \qquad\quad \mathsf{constr}(\mathit{Class}).\mathsf{excPostSpec}^{src}(\mathtt{Exc}) \Rightarrow \mathsf{excPost}^{src}(\mathtt{Exc})\end{array}\right. ,$$

$$\mathsf{excPost}^{src}, \mathtt{m})_{v'}$$

Let us see the relational expressions supported in the source programming language

- Instanceof expression

$$\begin{array}{l}\mathrm{wp}^{src}(\mathcal{E}^{src}\ \mathit{instanceof}\ \ \mathrm{Cl}\ , \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{\backslash\mathbf{typeof}(v)<:\ \mathrm{Cl}\ \wedge v \neq \mathbf{null}} = \\ \mathrm{wp}^{src}(\mathcal{E}^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_v\end{array}$$

- Binary relation over expressions

$$\begin{array}{l}\mathrm{wp}^{src}(\mathcal{E}_1^{src}\ \mathcal{R}\ \mathcal{E}_2^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{v_1 \mathcal{R} v_2} = \\ \mathrm{wp}^{src}(\mathcal{E}_1^{src}, \mathrm{wp}^{src}(\mathcal{E}_2^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})_{v_2}, \mathsf{excPost}^{src}, \mathtt{m})_{v_1}\end{array}$$

Statements

In the following, we present the rules of the predicate transformer for control statements.

- integer and boolean constant access

$$\mathrm{wp}^{src}(\mathcal{STMT}_1;\mathcal{STMT}_2, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{STMT}_1, \mathrm{wp}^{src}(\mathcal{STMT}_2, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}), \mathsf{excPost}^{src}, \mathtt{m})$$

- assignment

  - local variable assignemnt

$$\mathrm{wp}^{src}(\mathcal{E}_1^{src} = \mathcal{E}_2^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{E}_2^{src}, \mathsf{nPost}^{src}[\mathcal{E}_1^{src} \leftarrow v_2], \mathsf{excPost}^{src}, \mathtt{m})_{v_2}$$

  - instance field assignemnt

$$\mathrm{wp}^{src}(\mathcal{E}_1^{src}.f = \mathcal{E}_2^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{E}_1^{src}, \mathrm{wp}^{src}(\mathcal{E}_2^{src}, v_1 \neq \mathbf{null} \Rightarrow \mathsf{nPost}^{src}[f \leftarrow f[\oplus v_1 \rightarrow v_2]] \wedge v_1 = \mathbf{null} \Rightarrow \mathsf{excPost}^{src}(\mathtt{NullPointerExc}), \mathsf{excPost}^{src}, \mathtt{m})_{v_2}, \mathsf{excPost}^{src}, \mathtt{m})v_1$$

- if statement

$$\mathrm{wp}^{src}(\ \begin{array}{l}\mathtt{if}\ (\mathcal{E}^{\mathcal{R}})\\ \mathtt{then}\{\mathcal{STMT}_1\}\\ \mathtt{else}\ \{\mathcal{STMT}_2\}\end{array}\ , \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{E}^{\mathcal{R}}, v = \mathit{true} \Rightarrow \mathrm{wp}^{src}(\mathcal{STMT}_1, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) \wedge v = \mathit{false} \Rightarrow \mathrm{wp}^{src}(\mathcal{STMT}_2, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}), \mathsf{excPost}^{src}, \mathtt{m})_v$$

- throw exceptions

$$\mathrm{wp}^{src}(\texttt{throw}\ \mathcal{E}^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{E}^{src},\ v = \textbf{null} \Rightarrow \mathsf{excPost}^{src}(\texttt{NullPointerExc}) \wedge v \neq \textbf{null} \Rightarrow \forall \texttt{Exc}\ , \backslash\textbf{typeof}(\mathcal{E}^{src}) <: \texttt{Exc}\ \Rightarrow \mathtt{m}.\mathsf{excPost}^{src}(\texttt{Exc}\ ),\ \mathsf{excPost}^{src}, \mathtt{m})_v$$

- try catch statement

$$\mathrm{wp}^{src}(\texttt{try}\ \{\mathcal{STMT}_1\}\ \texttt{catch(Exc}\ c)\ \{\mathcal{STMT}_2\}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{STMT}_1,\ \mathsf{nPost}^{src},\ \mathsf{excPost}^{src} \oplus [\texttt{Exc} \longrightarrow \mathrm{wp}^{src}(\mathcal{STMT}_2, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m})], \mathtt{m})$$

- try finally

$$\mathrm{wp}^{src}(\texttt{try}\ \{\mathcal{STMT}_1\}\ \texttt{finally}\ \{\mathcal{STMT}_2\}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\mathrm{wp}^{src}(\mathcal{STMT}_1,\ \mathrm{wp}^{src}(\mathcal{STMT}_2, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}),\ \mathsf{excPost}^{src} \oplus [\texttt{Exception} \longrightarrow \mathrm{wp}^{src}(\mathcal{STMT}_2, \mathsf{excPost}^{src}(\texttt{Exception}), \mathsf{excPost}^{src}, \mathtt{m})], \mathtt{m})$$

where *exc* is the exception object thrown by $\mathcal{STMT}_1$.

- loop statement

$$\mathrm{wp}^{src}(\texttt{while}\ (\mathcal{E}^{\mathcal{R}})\ [\texttt{INV}, \texttt{modif}]\ \ \{\mathcal{STMT}\}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) =$$

$$\texttt{INV} \wedge \forall\ m, m \in \texttt{modif},\ \texttt{INV} \Rightarrow \mathrm{wp}^{src}(\mathcal{E}^{\mathcal{R}},\ v = \mathit{true} \Rightarrow\ \mathrm{wp}^{src}(\mathcal{STMT}, \texttt{INV}, \mathsf{excPost}^{src}, \mathtt{m}) \quad v = \mathit{false} \Rightarrow \mathsf{nPost}^{src},\ \mathsf{excPost}^{src}, \mathtt{m})_v$$

- return statement

$$\mathrm{wp}^{src}(\texttt{return}\ \mathcal{E}^{src}, \mathsf{nPost}^{src}, \mathsf{excPost}^{src}, \mathtt{m}) = \mathrm{wp}^{src}(\mathcal{E}^{src}, \mathsf{nPost}^{src}[\backslash\textbf{result} \leftarrow v], \mathsf{excPost}^{src}, \mathtt{m})_v$$

where **result**is a specification variable that can be met in the postcondition and denotes to the value returned of a non void method

7.5 Weakest precondition calculus for bytecode programs

7.5.1 Weakest predicate transformer over compiled statements and expressions

In the following, we introduce a new formulation of the *wp* function which will be based on the compiler from source to bytecode language. The motivation for this new definition is that it will allow to reason about the relation between source and bytecode proof obligations. Of course, it is also important to see what is the relation between the new definition of the *wp* introduced here and the definition given earlier in Chapter 5, section 5.3. We will argue under what conditions both formulations of the *wp* function produce the same formulas.

We give now a definition of the *wp* function for a single sequential instruction (instructions different from goto , if_cond , jsr , ret) which takes explicitely the postcondition and the exceptional postcondition function upon which the precondition will be calculated. Its signature is the following:

$$\text{wp}^{bc} : \text{ I}\backslash\{ \text{ goto , if\_cond } \} \rightarrow P_{bml} \rightarrow (\ \texttt{ExcType} \rightarrow P_{bml}) \rightarrow P_{bml}$$

For instance, the *wp* definition for getfield is :

$$\begin{array}{l} wp^{bc}(\text{ getfield } f, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = \\ \mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \psi[\mathbf{st}(\mathbf{cntr}) \leftarrow f(\mathbf{st}(\mathbf{cntr}))] \wedge \\ \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathsf{excPost}^{src2bc}(\ \mathtt{NullPntrExc}) \end{array}$$

Note that this differs from the definition of the *wp* given in Chapter 5, section 5.3 where the postcondition is a function of the successor of the current instruction. We do not give the rest of the rules because they the same as the rules presented in 5.3 except for the fact that the local postconditions are given explicitely.

We also define the weakest predicate transformer function for a block of instruction that always execute sequentially as follows:

Definition 7.5.1.1 (*wp* for a block of instructions)

$$\begin{array}{l} wp^{bc}_{seq}(1 : \mathtt{instr}; ...; k : \mathtt{instr}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = \\ wp^{bc}_{seq}(1 : \mathtt{instr}; ...; k-1 : \mathtt{instr}, wp^{bc}(k : \mathtt{instr}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}), \mathsf{excPost}^{src2bc}, \mathtt{m}) \end{array}$$

We turn now to the rules for compiled expressions. Note that from Property 7.3.5.3 it follows that the compilation of any expression is a sequence of instructions of instructions that execute sequentially and there is no jump from outside inside the sequence. Thus, we use the predicate transformer for a sequence of bytecode instructions defined above in order to define the predicate transformer for expressions.

Definition 7.5.1.2 (*wp* for compiled expressions) *For any expression $\mathcal{E}^{src}$, postcondition ψ and exceptional postcondition function* $\mathsf{excPost}^{src2bc}$ *the wp function for the compilation $\ulcorner E_{bml} \urcorner$ is $wp^{bc}_{seq}(\ulcorner E_{bml} \urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})$*

For instance, the rule of the *wp* for the compilation of access field expression $\mathcal{E}^{src}.f$ where its compilation is

$$\begin{array}{l} \ulcorner s, \mathcal{E}^{src}_1;, e-1 \urcorner \\ e \ \text{ getfield } f \end{array}$$

produce the following formula

$$wp^{bc}_{seq}(\ \begin{array}{l} \ulcorner s, \mathcal{E}^{src}, e-1 \urcorner; \\ e \ \text{ getfield } f \end{array}\ , \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})$$

This is equivalent to :

$$wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{src}, e-1 \urcorner, wp^{bc}(\ \text{getfield } f, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}), \mathsf{excPost}^{src2bc}, \mathtt{m})$$

The function which calculates the *wp* predicate of a compiled statement is called wp^{bc}_{stmt} and has the following signature :

$$wp^{bc}_{stmt} : Set(\ \mathrm{I}) \rightarrow P_{bml} \rightarrow (\ \mathtt{Exc} \rightarrow P_{bml}) \rightarrow P_{bml}$$

The definition of wp^{bc}_{stmt} uses the compiler function defined in Section **??**

- sequential statement compilation $\ulcorner s, \mathcal{STMT}_1; \mathcal{STMT}_2, e \urcorner$ which by definition is

$$\begin{array}{l} wp^{bc}_{stmt}(\ulcorner s, \mathcal{STMT}_1; \mathcal{STMT}_2, e \urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def} \\ wp^{bc}_{stmt}(\ulcorner s, \mathcal{STMT}_1, e' \urcorner;, \\ \qquad wp^{bc}_{stmt}(\ulcorner e'+1, \mathcal{STMT}_2, s \urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}), \\ \qquad \mathsf{excPost}^{src2bc}, \mathtt{m}) \end{array}$$

- if statement compilation $\ulcorner s, \mathtt{if}\ (\mathcal{E}^{\mathcal{R}})\ \mathtt{then}\ \{\mathcal{STMT}_1\}\ \mathtt{else}\ \{\mathcal{STMT}_2\}, e \urcorner$

$$wp^{bc}_{stmt}(\ulcorner s, \begin{array}{l} \mathtt{if}\ (\mathcal{E}^{\mathcal{R}}) \\ \mathtt{then}\ \{\mathcal{STMT}_1\} \\ \mathtt{else}\ \{\mathcal{STMT}_2\} \end{array}\ , e \urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}$$

$$\begin{array}{l} wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{\mathcal{R}}, e' \urcorner; \\ , \\ \qquad \mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow \\ \qquad\quad wp^{bc}_{stmt}(\ulcorner e''+2, \mathcal{STMT}_1, e \urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})[t \leftarrow t-2] \\ \qquad \wedge \\ \qquad \neg\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow \\ \qquad\quad wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e'' \urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})[t \leftarrow t-2] \\ \quad \mathsf{excPost}^{src2bc}, \mathtt{m}) \end{array} ,$$

- assignment expression. We will look only at the case for compiled field assignment expressions $\ulcorner s, \mathcal{E}_1^{src}.f = \mathcal{E}_2^{src}, e \urcorner$.

$$wp_{stmt}^{bc}(\ulcorner s, \mathcal{E}_1^{src}.f = \mathcal{E}_2^{src}, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}$$

- try catch statement compilation

$$wp_{stmt}^{bc}(\ulcorner s, \begin{array}{l}\texttt{try } \{\mathcal{STMT}_1\} \\ \texttt{catch } (ExcType\ \textbf{var})\{\mathcal{STMT}_2\}\end{array}, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}$$

$$wp_{stmt}^{bc}(\begin{array}{l}\ulcorner s, \mathcal{STMT}_1, e'\urcorner; \\ e'+1: \text{ goto } e+1;\end{array},$$

$$\psi,$$

$$\mathsf{excPost}^{src2bc}[\oplus ExcType \rightarrow wp_{stmt}^{bc}(\ulcorner e'+2, \mathcal{STMT}_2, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})], \mathtt{m})$$

- try finally statement compilation $\ulcorner s, \texttt{try } \{\mathcal{STMT}_1\} \texttt{ finally } \{\mathcal{STMT}_2\}, e\urcorner$

$$wp_{stmt}^{bc}(\ulcorner s, \begin{array}{l}\texttt{try } \{\mathcal{STMT}_1\} \\ \texttt{finally } \{\mathcal{STMT}_2\}\end{array}, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}$$

$$wp_{stmt}^{bc}(\ulcorner s, \mathcal{STMT}_1, e'\urcorner$$
$$,$$

$$wp_{stmt}^{bc}(\ulcorner e'+1, \mathcal{STMT}_2, e''\urcorner;, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}),$$

$$\mathsf{excPost}^{src2bc}[\oplus ExcType \rightarrow wp_{stmt}^{bc}(\begin{array}{l}e''+2: \text{ store } l; \\ \ulcorner e''+3, \mathcal{STMT}_2, e-2\urcorner; \\ e-1: \text{ load } l; \\ e: \text{ athrow}\end{array}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})], \mathtt{m})$$

- throw exception compilation $\ulcorner s, \texttt{throw } \mathcal{E}^{src}, e\urcorner$

$$wp_{stmt}^{bc}(\ulcorner s, \texttt{throw } \mathcal{E}^{src}, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}$$
$$wp_{seq}^{bc}(\ulcorner s, \mathcal{E}^{src}, e-1\urcorner, wp^{bc}(e/\text{ athrow}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}), \mathsf{excPost}^{src2bc}, \mathtt{m})$$

- loop statement

$$
\begin{array}{l}
wp^{bc}_{stmt}(\ulcorner s, \begin{array}{l}\texttt{while}\ (\mathcal{E}^{\mathcal{R}})\\ [\texttt{INV}, \texttt{modif}]\\ \{\mathcal{STMT}\}\end{array}, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}\\
\texttt{INV}\\
\wedge\\
\forall mod \in \texttt{modif},\\
\texttt{INV} \Rightarrow\\
wp^{bc}_{seq}(\ulcorner e'+1, \mathcal{E}^{\mathcal{R}}, e-1\urcorner,\\
\quad \mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow\\
\quad\quad wp^{bc}_{stmt}(\ulcorner s+1, \mathcal{STMT}, e'\urcorner, \texttt{INV}, \mathsf{excPost}^{src2bc}, \mathtt{m})\\
\quad \wedge\\
\quad \neg\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow \psi\\
\quad \mathsf{excPost}^{src2bc}, \mathtt{m})
\end{array}
,
$$

7.5.2 Properties of the *wp* functions

The previous subsection introduced a new formulation of the *wp* function for bytecode which is defined over the source statement from which it is compiled. However, it is important to establish a relation between this new definition and the *wp* formulation given in Chapter 5. The following statements establish the relation between the two versions of the *wp* calculus.

The first lemma states that the wp^{bc} function defined in the previous subsection 7.5.1 for a single bytecode instruction will return the same result as the *wp* function defined in Chapter 5. In particular, the explicite weakest precondition function for a single bytecode instruction $wp^{bc}(i_j, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})$ is equivalent to $wp(i_j\ , \mathtt{m})$ only if ψ is the intermediate predicate between j : `instr` and the next instruction k : `instr` to be executed. A similar condition we get for the function $\mathsf{excPost}^{src2bc}$.

Lemma 7.5.2.1 (Equivalence of the formulations for single instructions) *For all instructions* $i_j \in$ I\{ goto , if_cond , jsr, ret} *and* i_k *which belong to method* m*, formula* ψ*,and function* $\mathsf{excPost}^{src2bc}$: $\mathtt{ExcType} \rightarrow P_{bml}$ *such that*

- $i_j \rightarrow i_k$
- $\psi = \ inter(i_j, i_k, \mathtt{m})$
- $\forall \mathtt{Exc}, \mathsf{excPost}^{src2bc}(\mathtt{Exc}) = \mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, j)$

the following holds
$wp^{bc}(i_j, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = wp(i_j\ , \mathtt{m})$

The proof is done by case analysis on the instruction i_j

Proof: We scatch the case for a getfield instruction.

{ *by hypothesis* }
$i_j =$ getfield f
{ *by definition of the wp function* }
(1) $wp^{bc}($ getfield $f, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =$
$\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \psi[\mathbf{st}(\mathbf{cntr}) \leftarrow f(\mathbf{st}(\mathbf{cntr}))]$
$\wedge$
$\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathsf{excPost}^{src2bc}(\ \mathtt{NullPntrExc})$

{ *by definition of the wp function* }
(2) $wp($ getfield f $,\mathtt{m}) =$
$\mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow$ $inter(i_j, i_k, \mathtt{m})$ $[\mathbf{st}(\mathbf{cntr}) \leftarrow f(\mathbf{st}(\mathbf{cntr}))]$
$\wedge$
$\mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathsf{excPost}(\ \mathtt{NullPntrExc}, j)$

{ *from the initial hypothesis, (1) and (2) the lemma holds in that case* }

Qed.

The following lemma establishes that calculating the *wp* predicate of the first instruction of a block of bytecode instructions and calculating it by using a wp^{bc}_{seq} is the same under several conditions about the postcondition predicates.

Lemma 7.5.2.2 (*wp* for a block of instructions) *For every block of instructions* $1 : \mathtt{instr}; \ldots; j : \mathtt{instr}$ *and instruction* $k : \mathtt{instr}$ *in method* $\mathtt{m}$*, formula* ψ *and function* $\mathsf{excPost}^{src2bc} : \ \mathtt{ExcType} \rightarrow P_{bml}$ *such that*

- $j : \mathtt{instr} \rightarrow k : \mathtt{instr}$
- $\psi =$ $inter(j : \mathtt{instr}, j+1 : \mathtt{instr}, \mathtt{m})$
- $\forall \mathtt{Exc}, \forall i, 1 \leq i \leq j, \mathsf{excPost}^{src2bc}(\mathtt{Exc}) = \mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, i)$

then the following holds

$$wp^{bc}_{seq}(1 : \mathtt{instr}; \ldots; j : \mathtt{instr}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = wp(1 : \mathtt{instr}\ , \mathtt{m})$$

The proof is done by induction on the length of the sequence of instructions.
Proof:

(1) $wp^{bc}_{seq}(1 : \texttt{instr}; \ldots; j : \texttt{instr}, \psi, \mathsf{excPost}^{src2bc}, \texttt{m}) =$
{ *by Def. 7.5.1.1 for wp of block of instructions* }
$wp^{bc}_{seq}(1 : \texttt{instr}; \ldots; j-1 : \texttt{instr}, wp^{bc}(j : \texttt{instr}, \psi, \mathsf{excPost}^{src2bc}, \texttt{m}), \mathsf{excPost}^{src2bc}, \texttt{m})$
{ *by initial hypothesis we can apply lemma 7.5.2.1 from which it follows* }
$wp^{bc}(j : \texttt{instr}, \psi, \mathsf{excPost}^{src2bc}, \texttt{m}) = wp(\ j : \texttt{instr}, \texttt{m})$
{*by definition 7.3.5.1 ,* $j : \texttt{instr}$ *is not a loop entry*
and from Def. 5.3.1 }
(2) $inter(j, j+1, \texttt{m}) = wp(\ j : \texttt{instr}, \texttt{m})$
{*apply the induction hypothesis over* $1 : \texttt{instr}; \ldots; j-1 : \texttt{instr}$,
(2) and the initial hypothesis for exception handlers }
(3) $wp^{bc}_{seq}(1 : \texttt{instr}; \ldots; j-1 : \texttt{instr}, wp^{bc}(j : \texttt{instr}, \psi, \mathsf{excPost}^{src2bc}, \texttt{m}), \mathsf{excPost}^{src2bc}, \texttt{m}) =$
$wp(\ 1 : \texttt{instr}, \texttt{m})$
{ *from (1) and (3) the proposition holds*}

Qed.

The same property is established for compilation of expressions.

Lemma 7.5.2.3 (*wp* for compiled expressions) *For every compiled expression* $\ulcorner s, \mathcal{E}^{src}, e \urcorner$ *in method* $\texttt{m}$ *formula* ψ *and function* $\mathsf{excPost}^{src2bc} : \texttt{ExcType} \rightarrow P_{bml}$ *such that*

- $\psi = \ inter(e, e+1, \texttt{m})$
- $\forall \texttt{Exc}, \forall 1 \leq i, k \leq j, \mathsf{excPost}^{src2bc}(\texttt{Exc}) = \texttt{m}.\mathsf{excPost}(\texttt{Exc}, i)$

then the following holds:

$$wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{src}, e \urcorner, \psi, \mathsf{excPost}^{src2bc}, \texttt{m}) = wp(s : \texttt{instr}\ , \texttt{m})$$

Proof: From Property 7.3.5.5 of the compiler it follows that for every expression $\mathcal{E}^{src}$, start label s and end label e, the resulting compilation $\ulcorner s, \mathcal{E}^{src}, e \urcorner$ is a block of instructions. We can apply the previous lemma 7.5.2.2 and we get the result. *Qed.*

The next lemma states the same property but this time for the compilation of statements.

Lemma 7.5.2.4 *For every compiled statement* $\ulcorner s, \mathcal{STMT}, e \urcorner$ *in method* $\texttt{m}$*, formula* ψ *and function* $\mathsf{excPost}^{src2bc} : \texttt{ExcType} \rightarrow P_{bml}$ *such that*

- $\psi = \ inter(e, e+1, \texttt{m})$
- $\forall \texttt{Exc}, \mathsf{excPost}^{src2bc}(\texttt{Exc}) = \texttt{m}.\mathsf{excPost}(\texttt{Exc}, e)$

then the following holds:

$$wp^{bc}_{stmt}(\ulcorner s, \mathcal{STMT}, e \urcorner, \psi, \mathsf{excPost}^{src2bc}, \texttt{m}) = wp(s : \texttt{instr}\ , \texttt{m})$$

Proof : the proof is by induction on the compilation of a statement. We scatch here the proof of few cases

- if statement

$$wp^{bc}_{stmt}(\ulcorner s,\ \begin{array}{l}\texttt{if } (\mathcal{E}^{\mathcal{R}})\\ \texttt{then } \{\mathcal{ST}\mathcal{MT}_1\}\\ \texttt{else } \{\mathcal{ST}\mathcal{MT}_2\}\end{array}\ , e^{\urcorner}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) =^{def}$$

$$wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{\mathcal{R}}, e'^{\urcorner};$$
,
$$\begin{array}{l}\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow\\ \qquad wp^{bc}_{stmt}(\ulcorner e''+2, \mathcal{ST}\mathcal{MT}_1, e^{\urcorner}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})[t \leftarrow t-2]\\ \wedge\\ \neg\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow\\ \qquad wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{ST}\mathcal{MT}_2, e''^{\urcorner}, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})[t \leftarrow t-2]\\ \mathsf{excPost}^{src2bc}, \mathtt{m})\end{array}\ ,$$

{ by initial hypothesis, we have }
(1.1) $\psi =$ *inter*$(e, e+1, \mathtt{m})$
{ by the compiler definition $e''+1 : \mathtt{instr} =$ goto $e+1$; }
(1.2) $e''+1 : \mathtt{instr} \rightarrow e+1 : \mathtt{instr}$
{ *from Property 7.3.5.8 which states that every instruction inside the compilation of* $\ulcorner s, \mathcal{ST}\mathcal{MT}, e^{\urcorner}$,
is in the same execution relation with $e+1 : \mathtt{instr}$,
Def. 5.3.1 for inter, (1.1) and (1.2) we conclude that }
(1.3) *inter*$(e''+1, e+1, \mathtt{m}) =$ *inter*$(e, e+1, \mathtt{m}) = \psi$
{*From property 7.3.5.7 the edge between* e'' *and* $e''+1$ *is not a loop edge and from Def. 5.3.1* }
(1.4) *inter*$(e'', e''+1, \mathtt{m}) = wp(\ e''+1, m)$
{ *From the definition of the wp for* goto *instructions and (1.4)* }
(1.5) $wp(\ e''+1, m) =$ *inter*$(e''+1, e+1, \mathtt{m})$

{ *From (1.4), (1.3) and (1.5)* }
(1.6) $inter(e'', e''+1, \mathtt{m}) = inter(e, e+1, \mathtt{m}) = \psi$
{ *From 7.3.5.9* }
(1.7) $\mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, e) = \mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, e'')$
{ *apply the induction hypothesis over (1.6) and (1.7)* }
(1.8) $wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e''\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = wp(\ e'+2, m)$
{ *apply the induction hypothesis over the initial hypothesis* }
(1.9) $wp^{bc}_{stmt}(\ulcorner e''+2, \mathcal{STMT}_1, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = wp(\ e''+2, m)$
{ *by definition of* if_cond *function* }
(1.10) $wp(\ e'+1 :$ if_cond $\ e''+2;, m) =$
$\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow wp(\ e''+2, m)$
$\wedge$
$\neg\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow wp(\ e'+2, m)$
{ *from (1.8), (1.9) and (1.10)*}
(1.11) $wp(\ e'+1 :$ if_cond $\ e''+2;, m) =$
$\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow$
$\quad wp^{bc}_{stmt}(\ulcorner e''+2, \mathcal{STMT}_1, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})$
$\wedge$
$\neg\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow$
$\quad wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e''\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})$
{ *From Property 7.3.5.8* }
(1.12) $inter(e', e'+1, \mathtt{m}) = wp(\ e'+1 :$ if_cond $\ e''+2;, m)$
{ *From the initial hypothesis* }
(1.13) $\mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, e) = \mathsf{excPost}^{src2bc}(\mathtt{Exc})$
{ *From Property 7.3.5.10 and (1.13)*}
(1.14) $\forall \mathtt{Exc}, \forall s \leq i \leq e', \mathsf{excPost}^{src2bc}(\mathtt{Exc}) =$
$\mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, i)$
{ *apply Lemma 7.5.2.3 over hypothesis (1.11), (1.12), (1.14)* }
$wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{\mathcal{R}}, e'\urcorner;$
,
$\quad \mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow$
$\quad\quad wp^{bc}_{stmt}(\ulcorner e''+2, \mathcal{STMT}_1, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})[t \leftarrow t-2]$
$\quad \wedge$,
$\quad \neg\mathcal{R}(\mathbf{st}(\mathbf{cntr}), \mathbf{st}(\mathbf{cntr}-1)) \Rightarrow$
$\quad\quad wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e''\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})[t \leftarrow t-2]$
$\mathsf{excPost}^{src2bc}, \mathtt{m}) = wp(\ s, m)$

{ *and this case holds*}

- try catch statement

$$
\begin{array}{l}
\textit{(1) } wp^{bc}_{stmt}(\ulcorner s,\ \begin{array}{l}\texttt{try}\ \{\mathcal{STMT}_1\}\\ \texttt{catch}\ (\mathit{ExcType}\ \textbf{var})\{\mathcal{STMT}_2\}\end{array}\ , e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = \mathit{def} \\
\{\ \textit{Def. of } wp^{bc}_{stmt}\ \textit{in the previous Section 7.5.1}\ \} \\
wp^{bc}_{stmt}(\ulcorner s, \mathcal{STMT}_1, e'\urcorner;, \\
\qquad \psi, \\
\qquad \mathsf{excPost}^{src2bc}[\oplus \mathit{ExcType} \rightarrow wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})], \mathtt{m}) \\
\{\ \textit{apply the induction hypothesis over } \mathcal{STMT}_2 \textit{ and the initial hypothesis}\} \\
\textit{(2) } wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m}) = wp(\ e'+2, \mathtt{m}) \\
\{\ \textit{from the definition of } \mathsf{excPost} \textit{ and property 7.3.5.11}\} \\
\textit{(3) } \forall \mathtt{Exc}, \mathsf{excPost}^{src2bc}[\oplus \mathit{ExcType} \rightarrow wp(\ e'+2, \mathtt{m})] = \\
\qquad \mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, e') \\
\{\ \textit{we can also conclude from Prop. 7.3.5.8 and 7.3.5.7}\ \} \\
\textit{(4) } \mathit{inter}(e', e'+1, \mathtt{m}) = \mathit{inter}(e'+1, e+1, \mathtt{m}) = \mathit{inter}(e, e+1, \mathtt{m}) \\
\{\ \textit{apply induction hypothesis over (1), (3) and (4)}\ \} \\
wp^{bc}_{stmt}(\ulcorner s, \mathcal{STMT}_1, e'\urcorner;, \\
\qquad \psi, \\
\qquad \mathsf{excPost}^{src2bc}[\oplus \mathit{ExcType} \rightarrow wp^{bc}_{stmt}(\ulcorner e'+2, \mathcal{STMT}_2, e\urcorner, \psi, \mathsf{excPost}^{src2bc}, \mathtt{m})], \mathtt{m}) = \\
wp(\ s, \mathtt{m})
\end{array}
$$

Qed.

7.6 Proof obligation equivalence on source and bytecode level

In the following, we will argue that the proof obligations generated by the weakest precondition over programs of our source language are equivalent to the proof obligations generated over bytecode.

First, we remark that a wp^{src} defined over source expressions generates formulas which may have two possible normal forms.

Lemma 7.6.1 (Normal form of wp^{src}) *for any source expression $\mathcal{E}^{src}$ normal form of wp^{src} is such that*

$$
\begin{array}{l}
\textit{either there exists } Q, R : \mathcal{F} \\
wp^{src}(\mathcal{E}^{src}, \psi, \mathsf{excPost}, \mathtt{m})_v \ \equiv \\
Q \Rightarrow \psi \\
\wedge \\
R \\
\\
\textit{or exists } Q, R : \mathcal{F}, v_1 \ldots v_k : \mathcal{E}^{src} \\
\\
wp^{src}(\mathcal{E}^{src}, \psi, \mathsf{excPost}, \mathtt{m})_v \ \equiv \\
\forall \mathbf{boundVar}_1, \ldots \mathbf{boundVar}_k, Q \Rightarrow \psi \ \begin{array}{l} [v_1 \leftarrow \mathbf{boundVar}_1] \\ \ldots \\ [v_k \leftarrow \mathbf{boundVar}_k] \end{array} \wedge \\
R
\end{array}
$$

This follows from the definition of wp^{src} in Section 7.4.2. The second form in which the part of the calculated weakest precondition predicate is quantified appears in the cases for instance creation and method invokation expressions.

We now turn to see what is the relation between the weakest precondition formulas for an expression $\mathcal{E}^{src}$ and its compilation $\ulcorner s, \mathcal{E}^{src}, e \urcorner$. Depending on the form of the weakest precondition (as we saw with the previous lemma there are two possible forms of the weakest precondition for source expressions) of a soure expression $\mathcal{E}^{src}$ obtained from wp^{src} we will state the relation between wp^{src} and wp^{bc}_{seq} in the following two lemmas. Informally, both lemmas express the fact that

- the hypothesis of the part of the weakest preconditions on source and bytecode level concerning the normal termination of the expression are the same

- the part of the weakest preconditions on source and bytecode level concerning the exceptional termination of the expression are the same

Lemma 7.6.2 (Wp of a compiled expression) *For any expression $\mathcal{E}^{src}$ from our source language, for any formula $\psi : \mathcal{F}$ of the source assertion language and any formula $\phi : P_{bml}$ such that ϕ may only contain stack expressions of the form $\mathbf{st}(\mathbf{cntr} - k), k \geq 0$, the following holds*

There exist $Q, R : \mathcal{F}$ *such that*

$$
\begin{array}{l}
wp^{src}(\mathcal{E}^{src}, \psi, \mathsf{excPost}, \mathtt{m})_v \ \equiv \\
Q \Rightarrow \psi \\
\wedge \\
R \\
\\
\Rightarrow \\
\\
wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{src}, e \urcorner, \phi, \mathsf{excPost}, \mathtt{m}) \ \equiv \\
Q \Rightarrow \phi \ \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1] \\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow v]\end{array} \\
\\
\wedge \\
R
\end{array}
$$

We proceed with several cases of the proof, which is done by induction over the structure of the formula

Proof :

1. $\mathcal{E}^{src} = const, const \in$ **constInt**, *true*, *false*

{ *source case* }
(1)$\mathrm{wp}^{src}(const, \psi, \mathsf{excPost}, \mathtt{m})_{const}$
{ *following the definition of the wp function for source expressions in subsection 7.4.2* }
$\equiv \psi$

{ *bytecode case* }
(2)$wp^{bc}_{seq}(\ulcorner s, const, s \urcorner, \phi, \mathsf{excPost}, \mathtt{m})$

{ *following the definition of the compiler function in subsection 7.3.3* }
$\equiv wp^{bc}(s \ \ \mathrm{push}const, \phi, \ulcorner \mathsf{excPost} \urcorner, \mathtt{m})$
{ *following the definition of the wp function for bytecode in subsection 7.4.2* }
$\equiv \phi \ \begin{array}{l}[\mathbf{cntr} \leftarrow \mathbf{cntr} + 1] \\ [\mathbf{st}(\mathbf{cntr} + 1) \leftarrow const]\end{array}$

{ *from (1) and (2) and* $Q, R =$ **true** *this case holds* }

2. $\mathcal{E}^{src} = \mathcal{E}^{src}.f$

$\{$ *source case* $\}$
(1) $\mathrm{wp}^{src}(\mathcal{E}^{src}.f, \psi, \mathsf{excPost}, \mathtt{m})_{v.f}$
{*following the definition of the wp function for source expressions in subsection 7.4.2* }

$$\equiv \mathrm{wp}^{src}(\mathcal{E}^{src}, \begin{array}{l} v \neq \mathbf{null} \Rightarrow \psi \\ \wedge \\ v = \mathbf{null} \Rightarrow \mathsf{excPost}(\ \mathtt{NullPntrExc}) \end{array}, \mathsf{excPost}, \mathtt{m})_v$$

$\{$ *bytecode case* $\}$
(2) $wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{src}.f, e\urcorner, \phi, \ulcorner \mathsf{excPost}\urcorner, \mathtt{m})$
$\{$ *following the definition of the compiler function in subsection 7.3.3* $\}$

$$\equiv wp^{bc}_{seq}(\begin{array}{l} \ulcorner s, \mathcal{E}^{src}, e-1\urcorner \\ e \ \ \mathrm{getfield}\ f \end{array}, \phi, \mathsf{excPost}, \mathtt{m})$$

{*following the definition of the wp function for bytecode in subsection 7.5.1* }

$$\begin{array}{l} \equiv wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{src}, e-1\urcorner, \\ \quad \mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\ \quad \phi[\mathbf{st}(\mathbf{cntr}) \leftarrow \mathbf{st}(\mathbf{cntr}).f] \\ \quad \wedge \\ \quad \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathsf{excPost}(\ \mathtt{NullPntrExc}) \\ \quad \ulcorner \mathsf{excPost}\urcorner, \mathtt{m}) \end{array} ,$$

$\{$ *From (1) and (2) we apply the induction hypothesis* $\}$
$\exists Q', R' : \mathcal{F},$

$$\textit{(3)}\ \mathrm{wp}^{src}(\mathcal{E}^{src}, \begin{array}{l} v \neq \mathbf{null} \Rightarrow \psi \\ \wedge \\ v = \mathbf{null} \Rightarrow \mathsf{excPost}(\ \mathtt{NullPntrExc}) \end{array}, \mathsf{excPost}, \mathtt{m})_v$$

$$\equiv$$

$$Q' \Rightarrow \begin{array}{l} v \neq \mathbf{null} \Rightarrow \psi \\ \wedge \\ v \neq \mathbf{null} \Rightarrow \mathsf{excPost}(\ \mathtt{NullPntrExc}) \end{array}$$

$$\wedge$$

$$R'$$

$$\Rightarrow$$

$$\begin{array}{l} wp^{bc}_{seq}(\ulcorner \mathcal{E}^{src}\urcorner, \\ \quad \mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \\ \quad \phi[\mathbf{st}(\mathbf{cntr}) \leftarrow \mathbf{st}(\mathbf{cntr}).f] \\ \quad \wedge \\ \quad \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathsf{excPost}(\ \mathtt{NullPntrExc}) \\ \quad \ulcorner \mathsf{excPost}\urcorner, \mathtt{m}) \end{array} ,$$

$$\equiv$$

$$
\begin{array}{ll}
 & \mathbf{st}(\mathbf{cntr}) \neq \mathbf{null} \Rightarrow \phi[\mathbf{st}(\mathbf{cntr}) \leftarrow \mathbf{st}(\mathbf{cntr}).f] \quad [\mathbf{cntr} \leftarrow \mathbf{cntr}+1] \\
Q' \Rightarrow & \wedge \quad [\mathbf{st}(\mathbf{cntr}+1) \leftarrow v] \\
 & \mathbf{st}(\mathbf{cntr}) = \mathbf{null} \Rightarrow \mathsf{excPost}(\texttt{NullPntrExc}) \\
\wedge & \\
R' & \\
\equiv & \\
\{ & \phi \textit{ contains only stack expressions } \mathbf{st}(\mathbf{cntr}-k), k \geq 0 \textit{ and properties of substitution } \}
\end{array}
$$

$$
\begin{array}{ll}
 & v \neq \mathbf{null} \Rightarrow \phi \; [\mathbf{cntr} \leftarrow \mathbf{cntr}+1] \\
 & \qquad\qquad\qquad\quad [\mathbf{st}(\mathbf{cntr}+1) \leftarrow v.f] \\
Q' \Rightarrow & \wedge \\
 & v = \mathbf{null} \Rightarrow \mathsf{excPost}(\texttt{NullPntrExc}) \\
\wedge & \\
R' &
\end{array}
$$

$$
\{ \quad \textit{from (3) this case holds} \quad \}
$$

Lemma 7.6.3 (Wp of a compiled expression) *For any expression $\mathcal{E}^{src}$ from our source language, for any formula $\psi : \mathcal{F}$ of the source assertion language and any formula $\phi : P_{bml}$ such that ϕ may only contain stack expressions of the form $\mathbf{st}(\mathbf{cntr}-k), k \geq 0$, the following holds there exist $Q, R : \mathcal{F}, v_1 \ldots v_k : \mathcal{E}^{src}$*

$$
\begin{array}{l}
wp^{src}(\mathcal{E}^{src}, \psi, \mathsf{excPost}, \mathtt{m})_v \equiv \\
\forall \mathbf{boundVar}_1, \ldots \mathbf{boundVar}_k, Q \Rightarrow \\
\qquad [v_1 \leftarrow \mathbf{boundVar}_1] \\
\quad \psi \; \ldots \qquad\qquad \wedge \\
\qquad [v_k \leftarrow \mathbf{boundVar}_k] \\
R \\
\Rightarrow
\end{array}
$$

$$
\begin{array}{l}
wp^{bc}_{seq}(\ulcorner s, \mathcal{E}^{src}, e \urcorner, \psi, \mathsf{excPost}, \mathtt{m}) \equiv \\
\forall \mathbf{boundVar}_1, \ldots \mathbf{boundVar}_k, Q \Rightarrow \\
\qquad [\mathbf{cntr} \leftarrow \mathbf{cntr}+1] \\
\qquad [\mathbf{st}(\mathbf{cntr}+1) \leftarrow v] \\
\quad \phi \; [v_1 \leftarrow \mathbf{boundVar}_1] \\
\qquad \ldots \\
\qquad [v_k \leftarrow \mathbf{boundVar}_k] \\
\\
\wedge \\
R
\end{array}
$$

The next lemma establishes a relation between the source and bytecodewpw.r.t. to the same weakest precondition.

excPost

Lemma 7.6.4 (Proof obligation equivalence on statements)

$$
\begin{array}{l}
\forall \mathcal{STMT}, \psi, \mathsf{excPost}^{src}, \\
\quad wp^{bc}_{stmt}(\ulcorner s, \mathcal{STMT}, e \urcorner, \psi, \mathsf{excPost}^{src}, \mathtt{m}) = \\
\quad wp^{src}(\mathcal{STMT}, \psi, \mathsf{excPost}^{src}, \mathtt{m})
\end{array}
$$

This follows from the previous lemma (which establishes the relation between the *wp*over source and the *wp* over bytecode that takes into account the compilation structure) and lemma 7.5.2.4 (which establishes the relation between the *wp* over bytecode that takes into account the compilation structure and the original *wp*which does not consider the properties of the compiler)

The next statement establishes under what conditions the *wp* over source and the *wp*defined in the previous Chapter are equivalent.

for the next lemma we have to say also : if $\ulcorner s, \mathcal{STMT}, e \urcorner$ and $inter(e, e+1, \mathtt{m})$ does not contain stack expr. then $wp(\ s, \mathtt{m})$ does not contain stack expr

Lemma 7.6.5 (Proof obligation equivalence on statements) *For every $\mathcal{STMT}$, compilation $\ulcorner s, \mathcal{STMT}, e \urcorner$, formula ψ and exceptional postcondition function* $\mathsf{excPost}^{src2bc}$ *such that :*

- $\psi = \ inter(e, e+1, \mathtt{m})$
- $\forall \mathtt{Exc}, \mathsf{excPost}^{src2bc}(\mathtt{Exc}) = \mathtt{m}.\mathsf{excPost}(\mathtt{Exc}, e)$

then it holds

$$wp^{src}(\mathcal{STMT}, \psi, \mathsf{excPost}^{src}, \mathtt{m}) = wp(s : \mathtt{instr}\ , \mathtt{m})$$

From the last lemma follows that if the body of the method m is $\mathcal{STMT}$, and its compilation is $\ulcorner s, \mathcal{STMT}, e \urcorner$, then the proof obligations generated over $\mathcal{STMT}$ upon postcondition m .normalPost and exceptional postcondition function m .excPostSpec and its compilation $\ulcorner s, \mathcal{STMT}, e \urcorner$ are the same

$$\mathrm{wp}^{src}(\mathcal{STMT}, \mathsf{normalPost}, \mathsf{excPost}^{src}, \mathtt{m}) = wp(s : \mathtt{instr}\ , \mathtt{m})$$

Chapter 8

A compact verification condition generator

Chapter 9

Applications

9.1 Introduction

Trusted personal devices (TPDs for short) such as smart cards, mobile phones, and PDAs commonly rely on execution platforms such as the Java Virtual Machine and the Common Language Runtime. Such platforms are considered appropriate for such TPDs since they allow applications to be developed in a high-level language without committing to any specific hardware and since they feature security mechanisms that guarantee the innocuousness of downloaded applications. For example, the Java security architecture ensures that applications will not perform illegal memory accesses through stack inspection, which performs access control during execution, and bytecode verification, which performs static type-checking prior to execution. On the other hand, current security architectures for TPDs do not provide any mechanism to control resource usage by downloaded applications, despite TPDs being subject to stringent resource constraints. Therefore, TPDs are particularly vulnerable to denial-of-service attacks, since executing a downloaded application may potentially lead to resource exhaustion.

Several approaches have been suggested to date to enforce memory consumption policies for programs; all approaches are automatic, but none of them is ideally suited for TPDs, either for their lack of precision, or for the runtime penalty they impose on programs:

- *Static analyses and abstract interpretations:* in such an approach, one performs an abstract execution of an approximation of the program. The approximation is chosen to be coarse enough to be computable, as a result of which it yields automatically bounds on memory consumption, but at the cost of precision. Such methods are not very accurate for recursive methods and loops, and often fail to provide bounds for programs that contain dynamic object creation within a loop or a recursive method;
- *Proof-carrying code:* here the program comes equipped with a specification of its memory consumption, in the form of statements expressed in an

appropriate program logic, and a certificate that establishes that the program verifies the memory consumption specification attached to it. The approach potentially allows for precise specifications. However, existing works on proof carrying code for resource usage sacrifice the possibility of enforcing accurate policies in favor of the possibility of generating automatically the specification and the certificate, in line with earlier work on certifying compilation;

- *Run-time monitoring:* here the program also comes equipped with a specification of its memory consumption, but the verification is performed at run-time, and interrupted if the memory consumption policy is violated. Such an approach is both precise and automatic, but incurs a runtime overhead which makes it unsuitable for TPDs.

The objective of this work is to explore an alternative approach that favors precision of the analysis at the cost of automation. The approach is based on program logics, which originate from the seminal work on program verification by C.A.R. Hoare and E.W. Dijkstra and have been used traditionally to verify functional properties of programs. In earlier work, we have shown how general purpose logics can be used to enforce security properties of Java programs, including confidentiality [**?**] and high-level security rules [**?**]. In this paper, we demonstrate that program logics are also appropriate for performing a precise analysis of resource consumption for Java programs. Although our method is applicable both at source code level and bytecode level, our work has focused on bytecode level, since in many application domains verification has to be performed without access to the source code of the applet. (However, for the clarity of the explanations all examples in the introduction deal with source code level.)

In order to illustrate the principles of our approach, let us consider the following program:

```
public void m(A a){
  if (a  == null) {
    a = new A();
  }
   a.b = new B();
}
```

In order to model the memory consumption of this program, we introduce a *ghost* (or, *model*) variable `Mem` that accounts for memory consumption; more precisely, the value of `Mem` at any given program point is meant to provide an upper bound to the amount of memory consumed so far. To keep track of the memory consumption, we perform immediately after every bytecode that allocates memory an increment of `Mem` by the amount of memory consumed by the allocation. Thus, if the programmer specifies that `ka` and `kb` is the memory consumed by the allocation of an instance of class `A` and `B` respectively, the program must be annotated as:

```
public void m(A a) {
  if (a  == null) {
    a = new A();
    // set Mem = ka;
  }
   a.b = new B();
   // set Mem = kb;
}
```

Such annotations allow to compute at run-time the memory consumption of the program. However, we are interested in static prediction of memory consumption, and resort to preconditions and postconditions to this end. Even for a simple example as above, one can express the specification at different levels of granularity. For example, fixing the amount of memory that the the program may use `Max` one can specify that the method will use at most `ka + kb` memory units and will not overpass the authorized limit to use `Max` with the following specification:

```
//@  requires Mem + ka +  kb <= Max
//@ ensures  Mem <= \old(Mem) + ka +  kb
public void m(A a) {
  if (a  == null) {
    a = new A();
    // set Mem = ka;
  }
   a.b = new B();
   // set Mem = kb;
}
```

Or try to be more precise and relate memory consumption to inputs with the following specification:

```
//@ requires a == null ==> Mem + ka +  kb <= Max &&
   !(a  == null) ==> Mem + kb <= Max
//@ ensures \old(a) == null ==> Mem <= \old(Mem) + ka +  kb &&
    !(\old(a)  == null) ==> Mem <= \old(Mem) + kb
public void m(A a) {
  if (a  == null) {
    a = new A();
  }
   a.b = new B();
}
```

More complex specifications are also possible. For example, one can take into account whether the program will throw an exception or not. using (possibly several) exceptional postconditions stating that $\mathtt{k_E}$ memory units are allocated in case the method exits on exception `E`.

The main characteristics of our approach are:

- *Precision:* our analysis allows to specify and enforce very precise memory consumption policies, including policies that take into account the results of branching statements or the values of parameters in method calls. Being based on program logics, which are very versatile, the precision of our analysis can be further improved by using it in combination with other analyses, such as control flow analysis and exception analysis;

- *Correctness:* our analysis exploits existing program logics which are (usually) already known to be sound. In fact, it is immediate to derive the soundness of our analysis from the soundness of the program logic, provided ghost annotations that update memory consumption variables are consistent with an instrumented semantics that extends the language operational semantics with a suitable cost model that reflects resource usage;

- *Language coverage:* our analysis relies on the existence of a verification condition generator for the programming language at hand, and is therefore scalable to complex programming features. In the course of the paper, we shall illustrate applications of our approach to programs featuring recursive methods, method overriding and exceptions;

- *Usability:* our approach can be put to practice immediately using existing verification tools for program logics. We have applied our approach to annotated Java bytecode programs using a verification environment developed in [**?**], but it is also possible to use our approach on JML annotated Java source code [**?**], and more generally on programs that are written in a language for which appropriate support for contract-based reasoning exists;

- *Annotation generation:* in contrast to other techniques discussed above, our approach requires user interaction, both for specifying the program and for proving that it meets its specification. In order to reduce the burden of the user, we have developed heuristics that infer automatically part of the annotations;

- *Feasibility:* thanks to annotation generation mechanisms and powerful provers that help discharge many proof obligations automatically, our approach can be applied to realistic Java bytecode programs with a reasonable overhead.

In the course of the article, we illustrate the principles and characteristics of our approach in the context of Java bytecode programs. More specifically, the paper is organized as follows: Section 9.2 provides a brief introduction to Java bytecode programs and to the modeling language and weakest precondition calculus used to specify and verify such programs. Section 9.3 describes in some detail how the infrastructure described in Section 9.2 can be used to specify and verify precise memory consumption policies. Section 9.4 is devoted to a presentation of our algorithms for inferring automatically annotations. We conclude in Section 9.5 with related work and in Section 9.6 with directions for future work.

9.2 Preliminaries

9.2.1 Java class files

The standard format for Java bytecode programs is the so-called class file format which is specified in the Java Virtual Machine Specification [**?**]. For the purpose of this paper, it is sufficient to know that class files contain the definition of a single class or interface, and are structured into a hierarchy of different attributes that contain information such as the class name, the name of its superclass or the interfaces it implements, a table of the methods declared in the class. Moreover an attribute may contain other attributes. For example the attribute that describes a single method contains an `Local_Variable_Table` attribute that describes the method parameters and its local variables; further in this section we will denote the table of local variables by l and the i^{th} variable by $l[i]$. In addition to these attributes which provide all the information required by a standard implementation of the Java Virtual Machine, class files can accommodate user-defined attributes, which are not used by standard implementations of the Java Virtual Machine but can be used for other purposes. We take advantage of this possibility and introduce additional attributes that contain annotations such as method preconditions and postconditions, variants and invariants. Annotations are given in the Bytecode Modeling Language, which we describe below.

9.2.2 The Bytecode Modeling Language

The bytecode modeling language BML is a variant of the Java Modeling Language (JML) [17] tailored to Java bytecode; the BML specification language is described in [**?**]. For our purposes, we only need to consider a restricted fragment of BML, which is given in Fig. 9.1; we let E_{bml} and $\mathcal{P}$ denote respectively the set of BML expressions and BML predicates. As for JML, BML specifications contain different forms of statements, in the form of BML predicates tagged with appropriate keywords. BML predicates are built from BML expressions using standard predicate logic; furthermore BML expressions are bytecode programs that correspond to effect-free Java expressions, or BML specific expressions. The latter include expressions of the form `\old(exp)` which refers to the value of the expression `exp` at the beginning of the method, or $\texttt{exp}^{\texttt{pc}}$ which refers to the value of the expression `expr` at program point `pc`. Note that the latter is not a standard expression in JML but can be emulated introducing a ghost variable $\texttt{exp}^{\texttt{pc}}$ and performing the ghost assignment `set` $\texttt{exp}^{\texttt{pc}}$`= exp` at program point `pc`.

Statements can be used for the following purposes:

- Specifying method preconditions, which following the design by contract principles, must be satisfied upon method invocation. Such preconditions are formulated using statements of the form **requires** $\mathcal{P}$;

- Specifying method postconditions, which following the design by con-

$$
\begin{array}{rcl}
\text{BML} - \mathsf{stmt} & = & \textbf{requires } \mathcal{P} \\
& | & \textbf{ensures } \mathcal{P} \\
& | & \textbf{exsures} Exception\ \mathcal{P} \\
& | & \textbf{assert } \mathcal{P} \\
& | & \texttt{INV } \mathcal{P} \\
& | & \texttt{variant } E_{bml} \\
& | & \textbf{declare ghost } Type\ name \\
& | & \textbf{modifies } var \\
& | & \textbf{set } E_{\text{bml}} = E_{\text{bml}}
\end{array}
$$

Figure 9.1: Specification language

tract principles, must be guaranteed upon returning normally from the method. Such postconditions are formulated using statements of the form **ensures** $\mathcal{P}$;

- Specifying method exceptional postconditions, which must be guaranteed upon returning exceptionally from the method. Such postconditions are formulated using statements of the form **exsures***Exception* $\mathcal{P}$, that record the reason for exceptional termination;

- Stating loop invariants, which are predicates that must hold every time the program enters the loop;

- Guaranteeing termination of loops and recursive methods, using statements of the form `variant` E_{bml} which provide a measure (in the case of BML a positive number) that strictly decreases at each iteration of the loop/recursive call;

- Local assertions, using **assert** $\mathcal{P}$, which asserts that $\mathcal{P}$ holds at the program point immediately after the assertion;

- Declaring and updating ghost variables, using statements of the form **declare ghost** *Type name* and **set** $E_{\text{bml}} = E_{\text{bml}}$;

- Keeping track of variables that are modified by a method or in a loop, using declarations of the form **modifies** *var*. During the generation of verification conditions, one checks that variables that are not declared as modifiable by the clause above will not be modified during the execution of the method/loop, and one also uses the information about modified variables to generate the verification conditions.

Note that, as alluded in the previous paragraph, annotations are not inserted directly into bytecode; instead they are gathered into appropriate user defined attributes of an extended class file. Such extended class files can be obtained either through direct manipulation of standard class files, or using an extended compiler that outputs extended class files from JML annotated programs, see [**?**].

9.2.3 Verification of annotated bytecode

In order to validate annotated Java bytecode programs, we resort to a verification environment for Java bytecode (described in [**?**]), which is an adaptation of JACK [**?**]. It consists of two main components:

- A verification condition generator, which takes as input an annotated applet and generates a set of verification conditions which are sufficient to guarantee that the applet meets its specification;
- A proof engine that attempts to discharge the verification conditions automatically using automatic tools such as B and Simplify, and then sends the remaining verification conditions to proof assistants where they can be discharged interactively by the user. We are currently generating verification conditions for the proof assistants Coq [**?**] and PVS [**?**].

Generating the Verification Conditions

The verification condition generator, or VCGen for short, takes as input an extended class file and returns as outputs a set of proof obligations, whose validity guarantees that the program satisfies its annotations. The VCGen proceeds in a modular fashion in the sense that it addresses each method separately, and is based on computing weakest preconditions. More precisely, for every method m , postcondition ψ that must hold after normal termination of m , and exceptional postcondition ψ' that must hold after exceptional termination of m (for simplicity we consider only one exception in our informal discussion), the VCGen computes a predicate ϕ whose validity at the onset of method execution guarantees that ψ will hold upon normal termination, and ψ' will hold upon exceptional termination. The VCGen will then return several proof obligations that correspond, among other things, to the fact that the precondition of m given by the specification entails the predicate ϕ that has been computed, and to the fact that variants and invariants are correct.

The procedure for computing weakest preconditions is described in detail in [**?**]. In a nutshell, one first defines for each bytecode a predicate transformer that takes as input the postconditions of the bytecode, i.e. the predicates to be satisfied upon execution of the bytecode (different predicates can be provided in case the bytecode is a branching instruction), and returns a predicate whose validity prior to the execution of bytecode guarantees the postconditions of the bytecode. The definition of such functions is completely generic and independent of any program, so the next step is to use these functions to compute weakest preconditions for programs. This is done by building the control flow graph of the program, and then by computing the weakest preconditions of the program using its control flow graph.

Note that the verification condition generator operates on BML statements which are built from extended BML expressions. Indeed, predicate transformers for instructions need to refer to the operand stack and must therefore consider expressions of the form `st(top -+ i)` which represent the `st(top -+ i)`-th

element from the stack top:

$$wp(\text{ store } l(i), \psi, \psi') = \psi[\texttt{top} \leftarrow \texttt{top-1}][l[i] \leftarrow \texttt{st(top)}].$$

Discharging verification conditions

Verification conditions are expressed in an intermediate language for which translations to automatic theorem provers and proof assistants exist.

9.2.4 Correctness of the method

The verification method is correct in the sense that one can prove that for all methods m of the program the postcondition (resp. exceptional postcondition) of the method holds upon termination (resp. exceptional termination) of the method provided the method is called in a state satisfying the method precondition and provided all verification conditions can be shown to be valid.

The correctness of the verification method is established relative to an operational semantics that describes the transitions to be taken by the virtual machine depending upon the state in which the machine is executed. There are many formalizations of the operational semantics of the Java Virtual Machine, see e.g. [**?**, **?**, **?**, **?**]. Such semantics manipulate states of the form $\langle\langle h, \langle m, \mathrm{Pc}, l, s\rangle, sf\rangle\rangle$, where h is the heap of objects, $\langle m, \mathrm{Pc}, l, s\rangle$ is the current *frame* and sf is the current call stack (a list of frames). A frame $\langle m, \mathrm{Pc}, l, s\rangle$ contains a method name m and a program point Pc within m, a set of local variables l, and a local operand stack s. The operational semantics for each instruction is formalized as rules specifying transition between states, or between a state and some tag that indicates abnormal termination. For example, the semantics of the instruction store is given by the transition rule below, where $\texttt{InstAt}(m, \mathrm{Pc})$ is the function that extracts the Pc-th instruction from the body of method m .

$$\frac{\texttt{InstAt}(m, \mathrm{Pc}) = \text{ store } i}{\langle\langle h, \langle m, \mathrm{Pc}, l, v :: s\rangle, sf\rangle\rangle \rightarrow_{\text{ store } i} \langle\langle h, \langle m, \mathrm{Pc}+1, l[i \mapsto v], s\rangle, sf\rangle\rangle.}$$

In order to establish the correctness of our method, one first needs to establish the correctness of the predicate transformer for each bytecode. For example for the instruction store we show that:

$$wp(\text{ store } i, \psi)(\langle\langle h, \langle m, \mathrm{Pc}, l, v :: s\rangle, sf\rangle\rangle) \Rightarrow \psi(\langle\langle h, \langle m, \mathrm{Pc}+1, l[i \mapsto v], s\rangle, sf\rangle\rangle)$$

In the above $\psi(\langle\langle h, \langle m, \mathrm{Pc}, l, v :: s\rangle, sf\rangle\rangle)$ is to be understood as the instance of the formula ψ in which all local variables l and field references are substituted with their corresponding values in state $\langle\langle h, \langle m, \mathrm{Pc}, l, v :: s\rangle, sf\rangle\rangle$.

The proof proceeds by a case analysis on the instruction to be executed, and makes an intensive use of auxiliary substitution lemmas that relate e.g. the

stack of the pre-state with the stack of the post-state of executing an instruction. Then one proves the correctness of the method by induction on the length of the execution sequence. We have proved the correctness of our method for a fragment of the JVM that includes the following constructs:

- Stack manipulation: push , pop , dup , dup 2, swap etc;
- Arithmetic instructions: arith_op ;
- Local variables manipulation: type_ load , type_ store , etc;
- Jump instructions: if_cond , goto , etc;
- Object creation and object manipulation: new , putfield , getfield , newarray , etc;
- Array instructions: type_astore , type_aload , etc;
- Method calls and return: invoke , return , etc;
- subroutines: jsr and ret .

Note however that our method imposes some mild restrictions on the structure of programs: for example, we require that jsr and `throw` instructions are not entry for loops in the control flow graph in order to prevent pathological recursion. Lifting such restrictions is left for future work.

9.3 Modeling memory consumption

The objective of this section is to demonstrate how the user can annotate and verify programs in order to obtain an upper bound on memory consumption. We begin by describing the principles of our approach, then turn to establish its soundness, and finally show how it can be applied to non-trivial examples involving recursive methods and exceptions.

9.3.1 Principles

Let us begin with a very simple memory consumption policy which aims at enforcing that programs do not consume more than some fixed amount of memory `Max`. To enforce this policy, we first introduce a ghost variable `MemUsed` that represents at any given point of the program the memory used so far. Then, we annotate the program both with the policy and with additional statements that will be used to check that the application respects the policy.

The precondition of the method m should ensure that there must be enough free memory for the method execution. Suppose that we know an upper bound of the allocations done by method m in any execution. We will denote this upper bound by `methodConsumption( m )`. Thus there must be at least `methodConsumption( m )` free memory units from the allowed `Max` when method m starts execution. Thus the precondition for the method m is:

$$\textbf{requires } \texttt{MemUsed} + \texttt{methodConsumption(m)} \leq \texttt{Max}.$$

The precondition of the program entry point (i.e., the method from which an application may start its execution) should state that the program has not allocated any memory, i.e. require that variable `MemUsed` is 0:

$$\textbf{requires } \texttt{MemUsed} == 0.$$

The normal postcondition of the method m must guarantee that the memory allocated during a normal execution of m is not more than some fixed number `methodConsumption( m )` of memory units. Thus for the method m the postcondition is:

$$\textbf{ensures } \texttt{MemUsed} \leq \textbf{\textbackslash old(}()\texttt{MemUsed}) + \texttt{methodConsumption(m)}.$$

The exceptional postcondition of the method m must say that the memory allocated during an execution of m that terminates by throwing an exception `Exception` is not more than `methodConsumption( m )` units. Thus for the method m the exceptional postcondition is:

$$\textbf{exsures}\mathit{Exception}\ \texttt{MemUsed} \leq \textbf{\textbackslash old(}()\texttt{MemUsed}) + \texttt{methodConsumption(m)}.$$

Loops must also be annotated with appropriate invariants. Let us assume that loop l iterates no more than $iter^l$ and let $loopConsumption(l)$ be an upper bound of the memory allocated per iteration in l. Below we give a general form of loop specification w.r.t. the property for constraint memory consumption. The loop invariant of a loop l states that at every iteration the loop body is not going to allocate more than $loopConsumption(l)$ memory units and that the iterations are no more than $iter^l$. We also declare an expression which guarantees loop termination, i.e. a variant (here an integer expression whose values decrease at every iteration and is always bigger or equal to 0).

$$\begin{array}{ll}
\textbf{modifies} & i, \texttt{MemUsed} \\
\texttt{INV}: & \texttt{MemUsed} \leq \texttt{MemUsed}^{Before_l} + i * loopConsumption(l) \\
 & \wedge \\
 & i \leq iter^l \\
\texttt{variant}: & iter^l - i
\end{array}$$

A special variable appears in the invariant, $\texttt{MemUsed}^{Before_l}$. It denotes the value of the consumed memory just before entering for the first time the loop l. At

every iteration the consumed memory must not go beyond the upper bound given for the body of loop.

For every instruction that allocates memory the ghost variable `MemUsed` must also be updated accordingly. For the purpose of this paper, we only consider dynamic object creation with the bytecode new ; arrays are left for future work and briefly discussed in the conclusion.

The function $allocInstance : Class \rightarrow int$ gives an estimation of the memory used by an instance of a class. At every program point where a bytecode new `A` is found, the ghost variable `MemUsed` must be incremented by `allocInstance(A)`. This is achieved by inserting a ghost assignment immediately after any new instruction, as shown below:

```
new A
//set MemUsed = MemUsed+allocInstance(A).
```

9.3.2 Correctness

We want to guarantee that the memory allocated by a given program is bounded by a constant `Max`. We can prove that our annotation is correct w.r.t. to the policy for constraint memory use, by instrumenting the operational semantics of the bytecode language given in Section 9.2.4. The instrumented operational semantics manipulates states as before, but it is extended with the special variable `MemUsed`. Thus, states in the new semantics have the form:

$$\langle\langle h, \langle m, \mathrm{Pc}, l, s\rangle, sf, \texttt{MemUsed}\rangle\rangle$$

The other instructions do not affect `MemUsed`, so the corresponding rules of the operational semantics are as before. As we saw in the previous section to every instruction of the form new A we attach the annotation **set** `MemUsed` = `MemUsed` + `allocInstance(()`A). The proof obligation generator converts this annotation into new value for the variable `MemUsed`:

$$wp(\textbf{set } \texttt{MemUsed} = \texttt{MemUsed} + \texttt{allocInstance(A)}, \psi) = \\ \psi[\texttt{MemUsed} \leftarrow \texttt{MemUsed} + \texttt{allocInstance(A)}]$$

We can prove that whenever the allocated space in the heap increments, the ghost variable `MemUsed` also increments, which is a sufficient condition to guarantee the correctness of the annotations. So far we do not deal with garbage collection (see discussion in Section 9.6).

9.3.3 Examples

We illustrate hereafter our approach by several examples.

Inheritance and overridden methods

Overriding methods are treated as follows: whenever a call is performed to a method m , we require that there is enough free memory space for the maximal consumption by all the methods that override or are overridden by m . In Fig. 9.2 we show a class `A` and its extending class `B`, where `B` overrides the method m from class `A`. Method m is invoked by n. Given that the dynamic type of the parameter passed to n is not known, we cannot know which of the two methods will be invoked. This is the reason for requiring enough memory space for the execution of any of these methods.

Specification of method m in class A:

requires $\texttt{MemUsed} + k \leq \texttt{Max}$
modifies `MemUsed`
ensures $\texttt{MemUsed} \leq \backslash\textbf{old(}()\texttt{MemUsed}) + k$

Specification for method m in class B:

requires $\texttt{MemUsed} + l \leq \texttt{Max}$
modifies `MemUsed`
ensures $\texttt{MemUsed} \leq \backslash\textbf{old(}()\texttt{MemUsed}) + l$

```
method n(A a)
...
//{ prove Mem <= Mem +max(l,k) }
invokevirtual m <A>
//{ assume Mem <= \old(Mem) + max(l,k)}
...
```

Figure 9.2: Example of overridden methods

Recursive Methods

In Fig. 9.3 the bytecode of the recursive method m and its specification is shown. For sake of space we show only a simplified version of the bytecode; we assume that the constructors for the class `A` and `C` do not allocate memory. Besides the precondition and the postcondition, the specification also includes information about the termination of the method: `variant locVar1`, meaning that the local variable `locVar1` decreases on every recursive call down to and no more than 0, guaranteeing that the execution of the method will terminate.

We explain first the precondition. If the condition of line `1` is not true, the execution continues at line `2`.

In the sequential execution up to line `7`, the program allocates at most `allocInstance(A)` memory units and decrements by 1 the value of `locVar1`. The instruction at line `8` is a recursive call to m, which either will take the

```
public class D {
  public void m( int i) {
    if (i > 0) {
      new A();
      m(i - 1);
      new A();
    } else {
      new C();
      new A();
   }
  }
}
```

requires $(\texttt{MemUsed} + \texttt{locVar1} * 2 * \texttt{allocInstance(A)} +$
$\texttt{allocInstance(A)} + \texttt{allocInstance(C)}) \leq \texttt{Max}$
variant locVar1
ensures $\texttt{locVar1} \geq 0$
$\wedge$
$\texttt{MemUsed} <= \backslash\textbf{old}(()\texttt{MemUsed}) + \backslash\textbf{old}(()\texttt{locVar1}) * 2 * \texttt{allocInstance(A)} + \texttt{allocInstance(A)}$
$+\texttt{allocInstance(C)})$

```
public void m()
//local variable loaded on
//the operand stack of method m
0   load _1
//  if locVar1 <= 0 jump
1 ifle 12
2 new <A> //  here locVar1 > 0
//set MemUsed = MemUsed +  allocInstance(A)
3 invokespecial <A.<init>>
4 aload_0
5 iload_1
6 iconst_1
//locVar1 decremented with 1
7 isub
//  recursive call with the new value of locVar1
8 invokevirtual <D.m>//
9 new <A>
//set MemUsed = MemUsed +  allocInstance(A)
10 invokespecial <A.<init>>
11 goto 16
//target of the jump at 1
12 new <A>
//set MemUsed = MemUsed +  allocInstance(A)
13 invokespecial <A.<init>>
14 new  <C>
//set MemUsed = MemUsed +  allocInstance(C)
15 invokespecial <C.<init>>
16 return
```

Figure 9.3: Example of a recursive method

same branch if `locVar1` > 0 or will jump to line `12` otherwise, where it allocates at most `allocInstance(A)` + `allocInstance(C)` memory units. On returning from the recursive call one more allocation will be performed at line `9`. Thus m will execute, `locVar1` times, the instructions from lines `4` to `35`, and it finally will execute all the instructions from lines `12` to `16`. The postcondition states that the method will perform no more than **old**(()`locVar1`) recursive calls (i.e., the value of the register variable in the pre-state of the method) and that on every recursive call it allocates no more than two instances of class `A` and that it will finally allocate one instance of class `A` and another of class `C`.

More precise specification

We can be more precise in specifying the precondition of a method by considering what are the field values of an instance, for example. Suppose that we have the method m as shown in Fig. 9.4. We assume that in the constructor of the class `A` no allocations are done. The first line of the method m initializes one of the fields of field `b`. Since nothing guarantees that field `b` is not **null**, the execution may terminate with `NullPointerException`. Depending on the values of the parameters passed to m , the memory allocated will be different. The precondition establishes what is the expected space of free resources depending on if the field `b` is **null**or not. In particular we do not require anything for the free memory space in the case when `b` is **null**. In the normal postcondition we state that the method has allocated an object of class `A`. The exceptional postcondition states that no allocation is performed if `NullpointerException` causes the execution termination.

requires	`locVar1` $!=$ **null** $\Rightarrow$ `MemUsed` + `allocInstance(A)` $\leq$ `Max`
modifies	`MemUsed`
ensures	`MemUsed` $\leq$ **old**(()`MemUsed`) + `allocInstance(A)`
exsures$NullPointerException$	`MemUsed` $==$ **old**(()`MemUsed`)

```
0 aload_0
1 getfield<C.b>
2 iload_2
3 putfield <B.i>
4 new <A>
//set MemUsed = MemUsed +
      allocInstance(A)
5 dup
6 invokespecial <A.<init>>
7 astore_1
8 return
```

```
public class C {
  B b;
  public void m(A a, int i) {
    b.i = i ;
    a = new A();
  }
}
```

Figure 9.4: Example of a method with possible exceptional termination

9.4 Inferring memory allocation for methods

In the previous section, we have described how the memory consumption of a program can be modeled in BML and verified using an appropriate verification environment. While our examples illustrate the benefits of our approach, especially regarding the precision of the analysis, the applicability of our method is hampered by the cost of providing the annotations manually. In order to reduce the burden of manually annotating the program, one can rely on annotation assistants that infer automatically some of the program annotations (indeed such assistants already exist for loop invariants, loop variants, or class invariants). In this section, we describe an implementation of an annotation assistant dedicated to the analysis of memory consumption, and illustrate its working on an example.

9.4.1 Annotation assistant

The user must provide annotations about the memory required to create objects of the given classes. The variants for each loop and recursive method may be given by the user or be synthesized through appropriate mechanisms.

Based on this information, the annotation assistant inserts the ghost assignments on appropriate places, and then computes recursively the memory allocated on each loop and method. A pseudo-code of the algorithm for inferring an upper bound for method allocations is given in Fig. 9.5. Essentially, it finds the maximal memory that can be allocated in a method by exploring all its possible execution path. The algorithm computes the set of blocks contained in a loop, the loop entry block and the set of end blocks of a loop; see Section 10 of [**?**] for a description of the algorithms used.

function `methodConsumption(.)`
Input: Bytecode of a method m.
Output: Upper bound of the memory allocated by m.
Body:

1. Detect all the loops in m;
2. For every loop l determine $loopSet(l)$, $entry(l)$ and $loopEndSet()$;
3. Apply the function *alloc* to each instruction i_k, such that $i_k =$ return ;
4. Take the maximum of the results given in the previous step: $max_{i_k=\text{ return }} allocPath(i_k)$.

Figure 9.5: Inference algorithm

The auxiliary function *allocPath*, which infers the maximal allocations done by the set of execution paths ending with the same return instruction, is given in Fig. 9.6. Inferring the memory allocated inside loops is done by

the function $alloc\_loop\_path(\cdot,\cdot)$, which is invoked by $allocPath$ whenever the current instruction belong to a loop. The specification of the function is shown in Fig. 9.7.

$allocPath(\texttt{InstAt}s) =$

$$\begin{cases} alloc\_instr(\texttt{InstAt}s) & if\ \texttt{InstAt}s\ has\ no\ predecessors \\ \\ loopConsumption(entry(l)) & \\ + & if\ \texttt{InstAt}s \in loopSet(l) \\ max_{\texttt{InstAt}k \in preds(\texttt{InstAt}s) - loopEndSet(l)}(allocPath(\texttt{InstAt}k)) & \\ \\ alloc\_instr(\texttt{InstAt}s) & \\ + & else \\ max_{\texttt{InstAt}k \in preds(\texttt{InstAt}s)}(allocPath(\texttt{InstAt}k)) & \end{cases}$$

Figure 9.6: Definition of the function $allocPath(\texttt{InstAt}s)$

$alloc\_loop\_path(entry(l), \texttt{InstAt}s) =$

$$\begin{cases} alloc\_instr(entry(l)) & if\ \texttt{InstAt}s = entr \\ \\ loopConsumption(entry(l')) & \\ + & if\ \texttt{InstAt}s \in loo \\ max_{\texttt{InstAt}k \in preds(entry(l')) - loopEndSet(l')}(alloc\_loop\_path(entry(l), \texttt{InstAt}k)) & l'\ is\ nested\ in\ l \\ \\ alloc\_instr(\texttt{InstAt}s) & \\ + & else \\ max_{\texttt{InstAt}k \in preds(\texttt{InstAt}s)}(alloc\_loop\_path(entry(l), \texttt{InstAt}k)) & \end{cases}$$

Figure 9.7: Definition of the function $alloc\_loop\_path(entry(l), \texttt{InstAt}s)$

The annotation assistant currently synthesize only simple memory policies (i.e., whenever the memory consumption policy does not depend on the values of inputs). Furthermore, it does not deal with arrays, subroutines, nor exceptions. Our approach may be extended to treat such cases (see the discussion in Section 9.6 about how to include arrays in our analysis). For sake of simplicity, we have also restricted the loop analysis only to those with a unique entry point, which is the case for code produced by non-optimizing compilers. A pre-analysis could give us all the entry points of more general loops, for instance by the algorithms given in [**?**]; our approach may be thus applied straightforwardly.

9.4.2 Example

Let us consider the bytecode given in Fig. 9.8, which is a simplified version of the bytecode corresponding to the source code given in the right of the figure. For simplicity of presentation, we do not show all the instructions (the result of the inference procedure is not affected). Method m has two branching instructions, where two objects are created: one instance of class A and another of class B. Our inference algorithm gives that `methodConsumption(m)` = `allocInstance(A)`+`methodConsumption(A.init)`+`allocInstance(B)`+`methodConsumption(B.init)`. Due to limitation on space, we do not explain the details of such inference, which are given in Fig. 9.9 (`InstAt`k refers to the bytecode instruction at position k).

```
0 aload_1                              public void m(A a , B b ) {
1 ifnonnull 6                            if ( a == null ) {
2 new <A>                                  a = new A();
...                                      }
4 invokespecial <A.<init>>               if (b == null) {
6 aload_2                                  b = new B();
7 ifnonnull 12                           }
8 new <B>                              }
...
10 invokespecial <B.<init>>
...
12 return
```

Figure 9.8: Example

9.5 Related work

The use of type systems has been a useful tool for guaranteeing that well typed programs run within stated space-bounds. Previous work along these lines defined typed assembly languages, inspired on [**?**] while others emphasised the use of type systems for functional languages [**?**, **?**, **?**].

For instance in [**?**] the authors present a first-order linearly typed assembly language which allows the safe reuse of heap space for elements of different types. The idea is to design a family of assembly languages which have high-level typing features (e.g. the use of a special *diamond* resource type) which are used to express resource bound constraints. Closely related to the previous-mentioned paper, [**?**] describes a type theory for certified code, in which type safety guarantees cooperation with a mechanism to limit the CPU usage of untrusted code. Another recent work is [**?**] where the resource bounds problem is studied in a simple stack machine. The authors show how to perform type, size and termination verifications at the level of the byte-code.

An automatic heap space usage static analysis for first-order functional pro-

$$
\begin{aligned}
&\texttt{methodConsumption(m)}\\
&=\\
&allocPath(\texttt{InstAt12})\\
&= max_{\texttt{InstAt}k \in preds(1_{12})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt12})\\
&\{alloc\_instr(\texttt{InstAt12}) = 0, preds(\texttt{InstAt}i_{12}) = \{i_{10}, i_7\}\}\\
&= max(allocPath(\texttt{InstAt10}), allocPath(\texttt{InstAt7}))\\
&= max(max_{\texttt{InstAt}k \in preds(\texttt{InstAt10})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt10}),\\
&\qquad max_{\texttt{InstAt}k \in preds(\texttt{InstAt7})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt7})\\
&\quad)\\
&\{preds(\texttt{InstAt10}) = \{i_8\}, preds(\texttt{InstAt7}) = \{i_6\}\}\\
&= max(allocPath(\texttt{InstAt8}) + alloc\_instr(\texttt{InstAt10}), allocPath(\texttt{InstAt6}) + alloc\_instr(\texttt{InstAt7}))\\
&\{alloc\_instr(\texttt{InstAt10}) = \texttt{methodConsumption(B.init)}, alloc\_instr(\texttt{InstAt7}) = 0\}\\
&= max(max_{\texttt{InstAt}k \in preds(\texttt{InstAt8})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt8}) + \texttt{methodConsumpti}\\
&\qquad max_{\texttt{InstAt}k \in preds(\texttt{InstAt6})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt6})\\
&\quad)\\
&\{preds(\texttt{InstAt8}) = \{i_7\}, preds(\texttt{InstAt6}) = \{i_4\}\}\\
&= max(allocPath(\texttt{InstAt7}) + +alloc\_instr(\texttt{InstAt8}) + \texttt{methodConsumption(B.init)},\\
&\qquad allocPath(\texttt{InstAt4}) + alloc\_instr(\texttt{InstAt6})\\
&\quad)\\
&\{alloc\_instr(\texttt{InstAt8}) = \texttt{allocInstance(B)}, alloc\_instr(\texttt{InstAt6}) = 0\}\\
&= max(max_{\texttt{InstAt}k \in preds(\texttt{InstAt7})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt7}) + \texttt{allocInstance(B}\\
&\qquad max_{\texttt{InstAt}k \in preds(\texttt{InstAt4})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt4})\\
&\quad)\\
&\{preds(\texttt{InstAt7}) = \{i_6\}, preds(\texttt{InstAt4}) = \{i_2\}\}\\
&= max(allocPath(i_6) + alloc\_instr(\texttt{InstAt7}) + \texttt{allocInstance(B)} + \texttt{methodConsumption(B.init)},\\
&\qquad allocPath(i_2) + alloc\_instr(i_4)\\
&\quad)\\
&\{alloc\_instr(\texttt{InstAt7}) = 0, alloc\_instr(\texttt{InstAt4}) = \texttt{methodConsumption(A.init)}\}\\
&= max(max_{\texttt{InstAt}k \in preds(\texttt{InstAt6})}(allocPath(\texttt{InstAt}k)) + alloc\_instr(\texttt{InstAt6}) + \texttt{allocInstance(B}\\
&\qquad max_{\texttt{InstAt}k \in preds(\texttt{InstAt2})}(allocPath(\texttt{InstAt}k) + alloc\_instr(\texttt{InstAt2}) + \texttt{methodConsumptio}\\
&\quad)\\
&= \{preds(\texttt{InstAt6}) = \{i_4, i_1\}, preds(\texttt{InstAt2}) = \{i_1\}\}\\
&= max(max(allocPath(i_4), allocPath(i_1)) + alloc\_instr(\texttt{InstAt6}) + \texttt{allocInstance(B)} + \texttt{methodCons}\\
&\qquad allocPath(i_1) + alloc\_instr(\texttt{InstAt2}) + \texttt{methodConsumption(A.init)}\\
&\quad)\\
&\{alloc\_instr(\texttt{InstAt6}) = 0, alloc\_instr(\texttt{InstAt2}) = \texttt{allocInstance(A)}\}\\
&= max(max(max_{i_k \in preds(i_4)}(allocPath(i_k)) + alloc\_instr(i_4),\\
&\qquad\qquad max_{i_k \in preds(i_1)}(allocPath(i_k)) + alloc\_instr(i_1)\\
&\qquad) + \texttt{allocInstance(B)} + \texttt{methodConsumption(B.init)},\\
&\qquad allocPath(i_0) + \texttt{allocInstance(A)} + \texttt{methodConsumption(A.init)},\\
&\quad)\\
&\{preds(i_4) = \{i_2\}, preds(i_1) = \{i_0\}\}\\
&\{allocPath(i_0) = alloc\_instr(i_0) = 0, alloc\_instr(i_1) = 0, alloc\_instr(i_4) = \texttt{methodConsumption(A.init}\\
&= max(max(allocPath(i_2) + \texttt{methodConsumption(A.init)},\\
&\qquad\qquad allocPath(i_0)\\
&\qquad) + \texttt{allocInstance(B)} + \texttt{methodConsumption(B.init)},\\
&\qquad \texttt{allocInstance(A)} + \texttt{methodConsumption(A.init)},\\
&\quad)\\
&\{allocPath(i_0) = alloc\_instr(i_0) = 0\}\\
&= max(allocPath(i_2) + \texttt{methodConsumption(A.init)} + \texttt{allocInstance(B)} + \texttt{methodConsumption(B.}\\
&\qquad \texttt{allocInstance(A)} + \texttt{methodConsumption(A.init)},\\
&\quad)\\
&\ldots\\
&= max(\texttt{allocInstance(A)} + \texttt{methodConsumption(A.init)} + \texttt{allocInstance(B)} + \texttt{methodConsumpti}\\
&\qquad \texttt{allocInstance(A)} + \texttt{methodConsumption(A.init)},\\
&\quad)\\
&= \texttt{allocInstance(A)} + \texttt{methodConsumption(A.init)} + \texttt{allocInstance(B)} + \texttt{methodConsumption(B}
\end{aligned}
$$

grams is given in [**?**]. The analysis both determines the amount of free cells necessary before execution as well as a safe (under)-estimate of the size of a *free-list* after successful execution of a function. These numbers are obtained as solutions to a set of linear programming (LP) constraints derived from the program text. Automatic inference is obtained by using standard polynomial-time algorithms for solving LP constraints. The correctness of the analysis is proved with respect to an operational semantics that explicitly keeps track of the memory structure and the number of free cells.

A logic for reasoning about resource consumption certificates of higher-order functions is defined in [**?**]. The certificate of a function provides an over-approximation of the execution time of a call to the function. The logic only defines what is a correct deduction of a certificate and has no inference algorithm associated with it. Although the logic is about computation time the authors claim it could be extended to measure memory consumption.

Another mechanical verification of a byte code language is [**?**], where a constraint-based algorithm is presented to check the existence of new instructions inside intra- and inter-procedural loops. It is completely formalised in Coq and a certified analyser is obtained using Coq's extraction mechanism. The time complexity of such analysis performs quite good but the auxiliary memory used does not allow it to be on-card. Their analysis is less precise than ours, since they work on an abstraction of the execution traces not considering the number of times a cycle is iterated (there are no annotations). Along these lines, a similar approach has been followed by [**?**]; no mechanical proof nor implementation is provided in such work.

Other related research direction concerns runtime memory analysis. The work [**?**] presents a method for analysing, monitoring and controlling dynamic memory allocation, using pointer and scope analysis. By instrumenting the source code they control memory allocation at run-time. In order to guarantee the desired memory allocation property, in [**?**] is implemented a runtime monitor to control the execution of a Java Card applet. The applet code is instrumented: a call to a monitor method is added before a new instruction. Such monitor method has as parameter the size of the allocation request and it halts the execution of the applet if a predefined allocation bound is exceeded.

There exists research on the definition of bytecode logics. In [**?**] a Hoare logics for bytecode is defined. Yet the approach there is based on searching structure in the bytecode programs which is not very natural for untsructured bytecode programs. In [**?**] a Hoare bytecode logics is defined in terms of weakest precondition calculus over the Jinja language (subset of Java). They use the logics for verifying bytecode against arithmetic overflow.

Upon completion of this work we became aware of a recent, and still unpublished, result along the same lines of ours. Indeed, a hybrid (i.e., static and dynamic) resource bound checker for an imperative language designed to admit decidable verification is presented in [**?**]. The verifier is based on a variant of Dijkstra's weakest precondition calculus using "generalized predicates", which keeps track of the resource units available. Besides adding loop invariants, pre- and post-conditions, the programmer must insert "acquires" annotations to re-

serve the resource units to be consumed. Our approach has the advantage of treating recursive methods and exceptions, not taken into account in [**?**]. Another difference with our work is that we operate on the bytecode instead of on the source code.

9.6 Conclusion

Program logics have traditionally been used to verify functional properties of applications, but we have shown that such logics are also appropriate to enforce security properties including memory consumption policies. We have shown that program logics complement nicely existing methods to verify memory consumption, over which they are superior in terms of the precision of the analysis (and inferior in terms of automation).

We intend to pursue our work in three directions. Firstly, we would like to extend our approach to arrays. In principle, it should be reasonably easy to extend the verification method to arrays; however, it seems more complicated to extend our inference algorithm to arrays. The main difficulty here is to provide an estimate of the size of an array, as it is given by the top value on the operand stack at the time of its creation. Our intuition is that this can be done using an abstract interpretation or a symbolic evaluation of the program. If we look at the example code below (in source code):

```
void m(int s){
 int len = s;
 int[] i = new int[len]
}
```

where `len` is a local variable to the method, one can infer by symbolic computation that its value is the value of the method parameter. Thus the method can be given the precondition `Mem + s <= Max`. In a similar line of work, we would like to extend our results to concurrency using recent advances in program logics for multi-threaded Java programs [**?**]. Providing an appropriate treatment of arrays and multi-threading is an important step towards applying our results to mobile phone applications.

Secondly, we would like to adapt our approach to account for explicit memory management. More precisely, we would like to consider an extended language with a special instruction `free(o)` that deallocates the object `o`, and establish the correctness of our method under the assumption that deallocation is correct, i.e. that the object `o` is not reachable from the program point where `free(o)` is inserted. By combining our approach with existing compile-time analysis that infers for each program point which objects are not reachable, we should be able to provide more precise estimates of memory consumption.

Thirdly, we intend to apply our technique to other resources such as communication channels, bandwidth, and power consumption, as well as to more refined analyses that distinguish between different kinds of memory, such as RAM or non-volatile EEPROM. As suggested by the MRG project [**?**], it seems

also interesting to consider policies that enforce limits on the interaction between the program and its environment, for example w.r.t. the number of system calls or the bounds on parameters passed to them.

Chapter 10

Conclusion

Bibliography

[1] AV, Sethi R, and Ullman JD. *Compilers-Principles, Techniques and Tools*. Addison-Wesley: Reading, 1986.

[2] Fabian Bannwart. A logic for bytecode and the translation of proofs from sequential java. Technical report, ETHZ, 2004.

[3] Fabian Bannwart and Peter Muller. A program logic for bytecode. In *Bytecode 2005*, ENTCS, 2005.

[4] Mike Barnett, K. Rustan M. Leino, and Wolfram Schulte. The Spec# programming system: An overview. In "G.Barthe, L.Burdy, M.Huisman, J.Lanet, and T.Muntean", editors, *CASSIS workshop proceedings*, LNCS, pages 49–69. Springer, 2004.

[5] Gilles Barthe, Guillaume Dufay, Line Jakubiec, and Simao Melo de Sousa. A formal correspondence between offensive and defensive javacard virtual machines. In *VMCAI*, pages 32–45, 2002.

[6] Gilles Barthe, Guillaume Dufay, Line Jakubiec, Bernard Serpette, and Simão Melo de Sousa. A formal executable semantics of the JavaCard platform. *Lecture Notes in Computer Science*, 2028:302+, 2001.

[7] Nick Benton. A typed logic for stack and jumps. DRAFT, 2004.

[8] B.Meyer. *Object-Oriented Software Construction*. Prentice Hall, second revised edition edition, 1997.

[9] C. Breunesse, N. Cataño, M. Huisman, and B. Jacobs. Formal methods for smart cards: an experience report. *Science of Computer Programming*, 2004. To appear.

[10] L. Burdy, Y. Cheon, D. Cok, M. Ernst, J. Kiniry, G.T. Leavens, K.R.M. Leino, and E. Poll. An overview of JML tools and applications. In T. Arts and W. Fokkink, editors, *Formal Methods for Industrial Critical Systems (FMICS 2003)*, volume 80 of *ENTCS*. Elsevier, 2003.

[11] L. Burdy, A. Requet, and J.-L. Lanet. Java applet correctness: A developer-oriented approach. In K. Araki, S. Gnesi, and D. Mandrioli, editors, *FME*

2003: Formal Methods: International Symposium of Formal Methods Europe, volume 2805 of *LNCS*, pages 422–439, 2003.

[12] Yoonsik Cheon and Gary T. Leavens. A runtime assertion checker for the Java modeling language. In *Software Engineering Research and Practice (SERP'02)*, CSREA Press, pages 322–328, June 2002.

[13] Draft Revision December. Jml reference manual.

[14] Edsger W. Dijkstra and Carel S. Scholten. *Predicate Calculus and Program Semantics*. Springer, 1990.

[15] Michael D. Ernst, Jake Cockrell, William G. Griswold, and David Notkin. Dynamically discovering likely program invariants to support program evolution. *IEEE Trans. Softw. Eng.*, 27(2):99–123, 2001.

[16] Stephen N. Freund and John C. Mitchell. A formal framework for the java bytecode language and verifier. In *OOPSLA '99: Proceedings of the 14th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications*, pages 147–166, New York, NY, USA, 1999. ACM Press.

[17] G.T.Leavens, Erik Poll, Curtis Clifton, Yoonsik Cheon, Clyde Ruby, David Cok, and Joseph Kiniry. *JML Reference Manual*. technical report.

[18] C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, 1969.

[19] B. Jacobs and E. Poll. Java program verification at nijmegen: Developments and perspective, 2003.

[20] Gerwin Klein and Tobias Nipkow. A machine-checked model for a Java-like language, virtual machine and compiler. Technical Report 0400001T.1, National ICT Australia, Sydney, March 2004.

[21] Gary T. Leavens, Albert L. Baker, and Clyde Ruby. Preliminary design of jml: a behavioral interface specification language for java. *SIGSOFT Softw. Eng. Notes*, 31(3):1–38, 2006.

[22] "K. Rustan M. Leino, Greg Nelson, , and James B. Saxe ". Esc/java user's manual.

[23] R.K. Leino. escjava. `http://secure.ucd.ie/products/opensource/ESCJava2/docs.html`.

[24] Xavier Leroy. Java bytecode verification: Algorithms and formalizations. In *Journal of Automated Reasoning 2003*, 2003.

[25] Tim Lindholm and Frank Yellin. Java virtual machine specification. Technical report, Java Software, Sun Microsystems, Inc., 2004.

[26] M.Barnett and K. Rustan M. Leino. Weakest-precondition of unstructured programs. Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA.

[27] Cornelia Pusch. Proving the soundness of a java bytecode verifier in isabelle/hol, 1998.

[28] Zhenyu Qian. A formal specification of java virtual machine instructions for objects, methods and subrountines. In *Formal Syntax and Semantics of Java*, pages 271–312, 1999.

[29] C.L. Quigley. A programming logic for Java bytecode programs. In *Proceedings of the 16th International Conference on Theorem Proving in Higher Order Logics*, volume 2758 of *Lecture Notes in Computer Science*. Springer-Verlag, 2003.

[30] A.D. Raghavan and G.T. Leavens. Desugaring JML method specification. Report 00-03d, Iowa State University, Department of Computer Science, 2003.

[31] R.W.Floyd. Assigning meaning to programs. In J. T. Schwartz, editor, *volume 19 of Proceedings of Symposia in Applied Mathematics*, pages 19–32, 1967.

[32] I. Siveroni. Operational semantics of the java card virtual machine, 2004.