



ELSEVIER

Available online at www.sciencedirect.com



ScienceDirect

Electronic Notes in
Theoretical Computer
Science

Electronic Notes in Theoretical Computer Science 240 (2009) 61–78

www.elsevier.com/locate/entcs

Specification and Runtime Verification of Java Card Programs

Umberto Souza da Costa¹ Anamaria Martins Moreira¹
Martin A. Musicante¹

*DIMAp - Universidade Federal do Rio Grande do Norte
Campus Universitário - Lagoa Nova - Natal - RN - Brazil*

Plácido A. Souza Neto²

*Centro Federal de Educação Tecnológica do Rio Grande do Norte
Caixa Postal 1559 - 59.015-000 - Natal - RN - Brazil*

Abstract

Java Card is a version of Java developed to run on devices with severe storage and processing restrictions. The applets that run on these devices are frequently intended for use in critical, highly distributed, mobile conditions. They are required to be portable and safe. Often, the requirements of the application impose the use of dynamic, on-card verifications, but most of the research developed to improve safety of Java Card applets concentrates on static verification methods. This work presents a runtime verification approach based on Design by Contract to improve the safety of Java Card applications. To this end, we propose JCML (Java Card Modeling Language) a specification language derived from JML (Java Modeling Language) and its implementation: a compiler that generates runtime verification code. We also present some experiments and quality indicators.

Keywords: JML, Java Card, JCML, Compiler, Runtime Verification.

1 Introduction

The Java Card programming language [17] is a version of Java. Its programs are intended to run on very restricted architectures such as Smart Cards, SIM cards or security tokens. Many features and constructors of Java are not present in Java Card. These include some primitive types (such as `integer` or `float`) and most library classes. A specific version of the Java Virtual Machine (JVM) has been

¹ Email: umberto@dimap.ufrn.br, anamaria@dimap.ufrn.br, mam@dimap.ufrn.br

² Email: placidoneto@cefetrn.br

devised to run Java Card applets [5]. The Java Card virtual machine includes support for atomic transactions, transient and persistent memory, as well as a firewall mechanism.

Java Card applets [5] are usually deployed in highly distributed and mobile situations and tend to be developed for critical applications. The verification of such applets is often required to guarantee the intended behavior of the system to which these applets belong, in order to reduce financial and/or human risks.

The relevance of formal specification and verification methods for Java Card applications is reflected in the large number of works on this area. A typical example may be found in the Mondex case study [8], developed in the context of the Grand Challenge on Verified Software, where the banks want to be sure that no money may be created in a system of electronic wallets.

The Java Modeling Language (JML) [9] [11] is a language designed to specify Java programs in detail. Software developers can use JML to add specifications in accordance with the Design by Contract [15] principles by means of assertions, such as method preconditions and postconditions and class invariants. JML annotations can be automatically translated into runtime assertion checking code by JMLc [6] [4], the JML compiler. JMLc produces Java executable bytecode supposed to run on any Java virtual machine where the JML runtime classes are available.

The usefulness of Design by Contract in general and JML for Java is already well established, as presented in [11]. Due to the critical nature of smart card applications, runtime verifications associated to Design by Contract could contribute to the development of more robust code, e.g., by dealing with exceptional behaviour. However, JML and JMLc are *not* supported by the Java Card virtual machine. The input programming language accepted by the Java Card virtual machine has been restricted to cope with the restrictions imposed by the target devices where most of Java Card applets run. A consequence of this restriction is that Java Card cannot benefit from JML specification and verification tools in order to improve safety of its applets at runtime.

The motivation for our work is that, although the Java Card virtual machine is not able to deal with the code produced from a full JML specification, the safety of Java Card applets can be improved at least by a subset of JML. Such a subset can be defined in order to avoid all those features that are not supported by the Java Card virtual machine. It is necessary to ensure that both data and control structures involved in the specifications as well as the code generated for the verification of these specifications are compliant with the Java Card virtual machine.

In this context the main contributions of this paper are:

- The proposal of JCML, a restricted version of JML as a Java Card specification language.
- The design and implementation of a compiler for this language. Unlike the original JML compiler, our implementation focuses on the generation of concise and efficient code. To achieve this goal: (1) some optimization techniques are used for the generation of the Java Card code that will be run on-card, and (2) some ver-

ifications cannot be dealt with completely, and, if needed, have to be performed statically or in an off-card testing environment.

- A case study where the size of the JCML-generated programs is compared to those programs generated by the standard JML compiler. The size of the generated code is the main restriction when considering constrained devices after compatibility with the Virtual Machine.

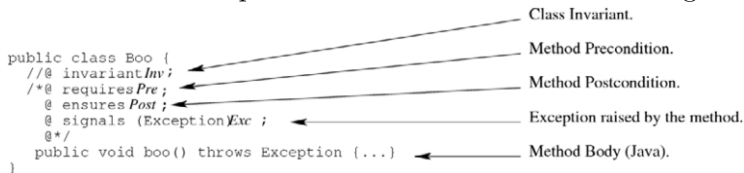
This paper is organized as follows: Section 2 presents Design by Contract and JML. Section 3 introduces the Java Card platform and discusses related limitations and advantages. After that, Section 4 shows how Java Card restrictions affect the choice of the JML subset compliant with the Java Card virtual machine, called JCML. Section 5 introduces the implementation of the JCML compiler, including the translation rules from JCML assertions to Java Card code. Experimental results are shown in section 6, where we compare the code produced by the JCML compiler and that produced by the JML compiler in terms of size. Finally, sections 7 and 8 present some related work and the next steps to be taken to improve JCML and its compiler, as well as our final remarks.

2 Design by contract and JML

Design by Contract [14] [15] is a software development method based on the definition of contracts between software units. The method proposes the run-time verification of these contracts. Design by Contract uses logical assertions (preconditions, postconditions and class invariants) to specify contracts. These assertions can be added to the source code of a program and can be dynamically verified.

JML implements these ideas by using model-based specifications with mathematical concepts such as sets and first order logic to specify the contents of each contract condition. However, differently from other model-based specification languages such as Z [22] and B [1], JML uses Java syntax as much as possible in its specifications, adding extra constructs to cope with specification concepts that are not directly expressed in Java, such as first order logic quantifiers.

In JML, assertions are expressed within the Java program by using a special kind of comments which express the conditions as first-order logic formulae, as follows:



```

public class Boo {
  //@ invariant Inv;
  /*@ requires Pre;
   @ ensures Post;
   @ signals (Exception) Exc;
  */
  public void boo() throws Exception { ... }
}

```

Class Invariant.
 Method Precondition.
 Method Postcondition.
 Exception raised by the method.
 Method Body (Java).

JML supports Design by Contract by means of two styles of specifications: *lightweight* specifications and *heavyweight* specifications. In this work, due to the restricted platform for which it is being developed, we are only concerned with *lightweight* specifications, where only preconditions are required for all methods, but postconditions can be omitted. Omitted postconditions are interpreted as **true** (trivially satisfied) in *lightweight* specifications.

JML annotated Java programs may be compiled with the JML compiler into instrumented Java programs. These resulting programs perform the original computation together with the verification steps. For instance, if a precondition p is specified for a method m and, at runtime, m is called in a context where p evaluates to false, the execution of m can be blocked and a warning message be sent to the user. Also, if in spite of all care, a specified class invariant is broken by some method execution, this situation can be immediately detected and made visible to the user. Together with static verification, this kind of verification provides confidence in applications, and so, it should be particularly useful in the smart card domain. However, because of this domain's severe restrictions, it is not yet available for it. More precisely, what is currently done is that most of this instrumentation code is manually programmed and inserted in the card programs without the required rigor.

3 Java Card

Java Card is a Java platform designed for resource-constrained devices. Due to the nature of those devices, the platform is quite limited. Memory restrictions are crucial for the design of Java Card applications: typical smart cards have as low as 12KB RAM, 374KB ROM and 144KB EEPROM. The read-only memory is used to store the Java Card Virtual Machine (JCVM), a severely downsized version of the JVM. The main differences between JVM and JCVM standards are the exclusion of some important JVM features such as many primitive types, dynamic classes and threads.

Java Card applications are called applets. In order to run one of these applets in a Java Card device, one must: (1) write the Java Card applet; (2) compile the applet; (3) convert the binary classes into a converted applet CAP file; (4) install the CAP file on the card; (5) run the applet. Compliance problems are detected by an off-card component of the JCVM [5], the converter, before the applet is installed on the card.

Because of these restrictions, a typical Java Card application will be very limited, and only some basic functionalities will be provided on-card. Most of the more heavy processing is executed on the so-called *host side*, the program that runs on the terminal to which the card is temporarily connected. However, for safety reasons, some card data may not be seen by the host application. Such sensible data must be manipulated on the card, safely and correctly. That is one of the advantages of smart cards with respect to magnetic strip cards: their on-card code may be used to ensure the safety and correctness of data apart from the host application. And this is where tools for a rigorous specification and verification of on-card data and functionalities becomes necessary.

4 Java Card Modeling Language (JCML)

JML has been designed for standard Java. This means that all Java constructs can be used in the generated verification code. To specify and verify Java Card applications, only those commands that can be run on the device may be used. So, the verification code generated by our specification must be Java Card compliant. Besides, time and memory consumption have to be taken into account on the definition of the modeling language and for the generation of code. The design of such a specification language has to consider the trade-off between expressiveness and feasibility.

We propose JCML: the Java Card Modeling Language [19]. JCML inherits as many JML constructs as possible. In particular, the specification part of the language is preserved. Only the Java part of JML has been pruned to cope with the restrictions of the Java Card language. The removed features include:

- Types: The primitive Java types `long`, `float`, `double` and `char`, as well as multidimensional arrays.
- Language Features: Dynamic class loading, threads, object cloning, and some aspects of package access control.
- Exceptions: Some exception and error subclasses.
- Library classes: Most of the Java core API classes and interfaces such as `Java.io`, `Java.lang` and `Java.util`. Classes such as `Boolean`, `Integer` and `String` are not supported either. The `Object` class exists, but without most of its methods.

The following list shows some of the JCML constructs:

- class and interface specifications: class invariants;
- method preconditions, normal and exceptional postconditions;
- method assignable conditions (variables that may be modified by a method);
- JML's extensions to Java's expression syntax such as quantifier keywords (`\forall` and `\exists`) and forward and reverse implication operators (`==>` and `<==`).

The complete JCML grammar is available at [19]³, and has been produced from the JML grammar [10] by selecting the set of rules concerned with *lightweight* specifications and removing all constructs not supported by Java Card. JCML specifications support Java Card expressions, in the same way that JML supports Java expressions. The (Java) code generated by our JCML compiler (section 5) obeys these constraints.

³ Available at <http://www.cefetrn.br/~placido/PlacidoAntonioDeSouzaNeto.pdf>

5 The JCML Compiler

The current version of the JCML compiler generates Java Card-compliant verification code for lightweight specifications. It implements invariant and condition verifications. The organization of the generated code preserves the structure of the original Java Card program, adding the verification code to it. The focus of the implementation is the generation of code suitable to be run on very restrictive devices. Because of this, our compiler had to be developed from scratch.

For each condition in the JCML annotations, a checking method is generated. The compiler uses the *wrapper* approach proposed in [6]. In this approach, the code of each (annotated) method of the program is embedded in a new method, whose task is to verify the assertions and call the original method. The embedded methods are renamed and made private. The wrapper method has the same name and signature as the original method it wraps. The wrapper method checks the preconditions and invariants and then executes the original method. After that, the wrapper checks the invariant and any specified postconditions.

In JCML one can specify static and instance invariants. Static invariants are properties over static attributes. Instance invariants deal with instance fields. Instance methods can contain both static and instance invariants. The JCML compiler generates a separate invariant method for each kind of invariant found in the source code.

According to the proposal in [6], some auxiliary methods are generated for the wrapper. Such methods are defined for the verification of preconditions, postconditions and invariants. The auxiliary methods rise exceptions when the assertions are violated.

In Figure 1 we present the structure of the auxiliary methods that check invariants and preconditions. Each assertion is defined by a predicate P_i . The condition verified by the auxiliary method `checkInv$ClassName$` (lines 1–11) corresponds to the conjunction of all the predicates for the invariants for the class `ClassName`. This method does not take parameters, since invariants are defined over global variables. If any of the predicates P_i evaluates to *false*, an `InvariantException` is signaled.

Notice that lines 8–10 and 20–22 of Figure 1 define the treatment of exceptions (of any kind) raised during the evaluation of conditions. These lines implement a *closed-world condition* of our implementation: Any specification predicate that cannot be checked, e.g., an undefined expression, is assumed false.

The `checkPre$MethodName$(T1 a1, ..., Tn an)` method (Figure 1, lines 13–23) performs the verification of precondition. This method has the same parameters as the method being verified. Once again, if the precondition cannot be verified (*i.e.*, if an error condition is raised during the verification), then the condition is assumed to be false. The case of postconditions is analogous.

5.1 An Example

We present a simple Java Card application named *UserAccess* (Figure 2), which runs as a card-controlled printing quota for students and staff. The application also

```

1 private void checkInv$ClassName$() {
2   try{
3     if (!(P1)) {
4       ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);}
5     ...
6     if (!(Pn)) {
7       ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);}
8   }catch(Exception e){
9     ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);}
10  }
11}
12
13 private void checkPre$MethodName$(T1 a1,..., Tk ak) {
14   try{
15     if (!(P1)) {
16       ISOException.throwIt(RequiresException.SW_REQUIRES_ERROR);}
17     ...
18     if (!(Pm)) {
19       ISOException.throwIt(RequiresException.SW_REQUIRES_ERROR);}
20   }catch(Exception e){
21     ISOException.throwIt(RequiresException.SW_REQUIRES_ERROR);}
22   }
23}

```

Fig. 1. Java Card methods to check invariants and preconditions.

grants access to certain parts of the building to the user. We propose a JCML specification for this application. It will be used to demonstrate how runtime verification code is generated.

The *UserAccess* class includes the following methods:

setID(byte[] m): Defines the user ID.

getID(): Returns the user ID.

addArea(byte local_cod): Includes a new local to the array of places accessible by the user.

hasAccess(byte local_cod): Return true if the user has access granted to the place identified by the parameter.

addCredits(short value): Adds some printing credits to the user.

removeCredits(short value): Removes a number of printing credits from the user.

short getCredits(): Returns the balance of printing credits.

setType(byte[] m): Defines the user type (student or professor).

getType(): Returns the user type.

The file (*UserAccessJCML.Java*) is generated from the JCML source containing

```

1 import Javacard.framework.*;
2 public class UserAccess {
3
4     public static final byte    MAX_USER_ID_LENGTH = 15;
5
6     //types of users
7     public static final byte    STUDENT = 0;
8     public static final byte    PROFESSOR = 1;
9
10    //different requirements for different types of users
11    public static final byte    MAX_AREAS = 20;
12    public static final short   MAX_CREDITS = 3000;
13    public static final byte    STUDENT_MAX_AREAS = 10;
14    public static final short   STUDENT_MAX_CREDITS = 1000;
15
16    //class attributes
17    private /*@ spec_public @*/ byte[]   userId;
18    private /*@ spec_public @*/ byte     userType;
19    private /*@ spec_public @*/ byte[]   authorizedAreas;
20    private /*@ spec_public @*/ byte     nextArea;
21    private /*@ spec_public @*/ short    printerCredits;
22
23    // no userId may have more than MAX_USER_ID_LENGTH
24    /*@ invariant userId.length <= MAX_USER_ID_LENGTH; @*/
25
26    //every user is either a student or a professor
27    /*@ invariant userType == STUDENT || userType == PROFESSOR; @*/
28
29    // global limits and values
30    /*@ invariant authorizedAreas.length <= MAX_AREAS; @*/
31    /*@ invariant \forall byte a; 0 <= a &&
32        a < authorizedAreas.length; authorizedAreas[a] >= 0; @*/
33    /*@ invariant printerCredits >= 0 &&
34        printerCredits <= MAX_CREDITS; @*/
35
36    //restricted limits for students
37    /*@ invariant userType == STUDENT ==>
38        authorizedAreas.length <= STUDENT_MAX_AREAS; @*/
39
40    /*@ invariant userType == STUDENT ==> printerCredits <=
41        STUDENT_MAX_CREDITS; @*/
42    ...

```

Fig. 2. UserAccess Class (with invariants).

the *UserAccess* class. The generated file contains the assertion-checking methods. The *UserAccessJCML.java* program can be compiled with a standard Java compiler in order to generate the executable class, and finally converted into the CAP file which runs on the card.

Specification of Invariants:

In JCML, invariants for a class are properties that must hold throughout every instance of the class. JCML invariants are checked before and after each method is called. The only variables allowed to appear in JCML invariants are the class attributes.

The *UserAccess* invariant (Figure 2, lines 23–39) defines: (i) that no *userId* may have more than *MAX_USER_ID_LENGTH* (line 24); (ii) that every user is either a student or a professor (line 27); (iii) global limits and values for the number of authorized areas and printer credits per user (lines 30 and 33); (iv) restricted limits for students (lines 36 to 39); (v) that area codes are natural numbers (lines 31 and 32).

The JCML compiler translates the invariant expressions into a private invariant checking method that raises an *InvariantException* when one of the conditions is broken. The generated code is shown on Figure 3, where manual comments have been included to associate each verification to the items above. The verification code for the forall quantifier, item (iv) includes a for loop that will be explained in section 5.2.

UserAccess Methods Specification:

Let us now see how a JCML-annotated method is dealt with. The *addCredits* method is used to add credits to the user. This method, shown in figure 4, has one parameter, called *value*, corresponding to the amount to be credited. The specification requires that the resulting credit balance is not greater than the allowed limit for the user, where *getCredits()* provides the current balance on the card.

The *addCredits* wrapper method (Figure 5), generated by JCML, wraps the original method call in a try-catch block that (i) checks the invariant and precondition; (ii) calls the original method and (iii) checks the invariant and postcondition. Figure 6 shows the generated code for *checkPre\$addCredits\$*.

5.2 Supporting Non-Java Operators

JCML includes, in its assertions, some operators that are not primitive in Java (nor in Java Card). These operators are logical implication (\Rightarrow) and universal and existential quantifiers. The JCML compiler generates the implementation of these operators in Java Card, as follows:

Modeling Implications:

Formulas of the type $A \Rightarrow B$ found in a specification generate verification conditions corresponding to their equivalent: $\neg A \vee B$.

```

1 private void checkInv$UserAccessJCML$() throws InvariantException{
2   try{
3     if (!(userId.length <=MAX_USER_ID_LENGTH ))           //(i)
4       ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
5     if (!(userType == STUDENT || userType == PROFESSOR )) //(ii)
6       ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
7     if (!(authorizedAreas.length <=MAX_AREAS ))           //(iii)
8       ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
9     for (byte a = 0; a < authorizedAreas.length ;a++){
10      if (!(authorizedAreas [a ]>=0 ))                     //(v)
11        ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
12    }
13    if (!(printerCredits >=0 &&
14          printerCredits <=MAX_CREDITS ))                 //(iii)
15      ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
16    if (!(!(userType == STUDENT ) ||
17          ( authorizedAreas.length <=STUDENT_MAX_AREAS ))) //(iv)
18      ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
19    if (!(!(userType == STUDENT ) ||
20          ( printerCredits <=STUDENT_MAX_CREDITS )))      //(iv)
21      ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);
22  }catch(Exception e){
23    ISOException.throwIt(InvariantException.SW_INVARIANT_ERROR);}
24  }
25}

```

Fig. 3. UserAccessJCML Check Invariant Method.

```

1 /*@ requires value >= 0 &&
2     (value + getCredits()) <= MAX_CREDITS &&
3     (userType == STUDENT ==>
4     (value + getCredits()) <= STUDENT_MAX_CREDITS);
5   ensures printerCredits >= value;
6 @*/
7 public void addCredits(short value) {
8     printerCredits += value;
9 }
10
11 public short getCredits(){
12     return printerCredits;
13 }

```

Fig. 4. addCredits and getCredits Methods.

```

1 public void addCredits(short value) {
2     try{
3         checkInv$UserAccessJCML$();
4         checkPre$addCredits$(value);

5         addCredits$original(value); // Call the original method

6         checkPost$addCredits$(value);
7         checkInv$UserAccessJCML$();
8     }catch (InvariantException invEx) {
9         ISOException.throwIt(ISO7816.SW_CONDITIONS_NOT_SATISFIED);
10    }catch (RequiresException reqEx) {
11        ISOException.throwIt(ISO7816.SW_CONDITIONS_NOT_SATISFIED);
12    }catch (EnsuresException ensEx) {
13        ISOException.throwIt(ISO7816.SW_CONDITIONS_NOT_SATISFIED);
14    }
15 }

```

Fig. 5. Generated addCredits Methods (wrapper).

```

1 private void checkPre$addCredits$( short value)
2     throws RequiresException{
3     try{
4         if(!(value >=0 && (value + getCredits ())<=MAX_CREDITS &&
5             (!(userType == STUDENT ) ||
6             ( (value + getCredits ())<=STUDENT_MAX_CREDITS ))))
7             ISOException.throwIt(RequiresException.SW_REQUIRES_ERROR);
8     }catch(Exception e){
9         ISOException.throwIt(RequiresException.SW_REQUIRES_ERROR);}
10 }
11 }

```

Fig. 6. Generated method for precondition verification.

Modeling Quantifiers:

Consider the JCML quantified expression:

$\forall \text{forall short } i, j; 0 \leq i \ \&\& \ i < j \ \&\& \ j < 10; a[i] < a[j];$

which follows the JCML grammar rule:

spec-quantified-expr : (*quantifier* *quantified-var-decls* ; [[*predicate*] ;]
spec-expression)

This expression uses the universal quantifier to specify that the vector *a* is sorted at indexes between 0 and 9. According to the JML Reference Manual [10], in the absence of a range predicate, the quantified expression must be evaluated over every value of the type of the quantified variable. For instance, in the previous example, the verifier would check all the possible values of *i* and *j*, from *MinShort* to *MaxShort*.

Evaluating this kind of expression can be very problematic in the context of Java Card: even for short-based types, the time required for on-card verification can be unacceptable.

Our implementation tackles this problem by using static analysis to reduce the state space. The algorithm processes the conditions in a quantifier, in order to restrict the range of values assumed by each variable. Initially, our algorithm assumes the lower and upper bounds defined by [10]. The algorithm proceeds in two steps: (1) the definition of tighter bounds for each variable and (2) the code generation.

The first step is a traversal of the quantifier's predicate. In the example predicate given above, we have the following sequence of upper and lower bounds for its variables:

- (i) We begin with $\text{MinShort} \leq i \leq \text{MaxShort}$ and $\text{MinShort} \leq j \leq \text{MaxShort}$.
- (ii) From the equation $0 \leq i$ we can define a new lower bound for i . Now we have $0 \leq i \leq \text{MaxShort}$ and $\text{MinShort} \leq j \leq \text{MaxShort}$.
- (iii) From the equation $i < j$ we can define new bounds for both i and j . Now we have $0 \leq i \leq j - 1$ and $i + 1 \leq j \leq \text{MaxShort}$.
- (iv) Finally, from the condition $j < 10$ we can define a new upper bound for j . Now we have $0 \leq i \leq j - 1$ and $i + 1 \leq j \leq 9$.

The second step generates code to verify the specification in accordance with the bounds defined in the first step. For each variable, a (nested) for-loop is generated using the upper and lower bounds. The order in which the variables are defined is relevant. For instance, in the given example, the bounds for i must be absolute. This means that the expression $j - 1$ must be replaced by its maximum possible value 8. The bounds for j can refer to i . Our algorithm produces the following code:

```

1 private void checkMethod() {
2   for (i = 0; i <= 8; i = i + 1) {
3     for (j = i+1; j <= 9; j = j + 1) {
4       if (!(a[i] < a[j])) throws Exception; }}}

```

The range predicate presented above is a conjunction of conditions (that can be part of a larger, disjunctive expression). Our algorithm will suppose that predicates in the quantifier expressions are given in disjunctive normal form. For each one of the (conjunctive) components of a disjunctive clause, the algorithm will produce a nested for-loop. The loops generated for each conjunctive clause will be placed in a sequence. For instance, if the code generated for a conjunctive clause P is $\mathcal{C}(P)$, the code generated for the quantified expression $\forall i, j; P \text{ and } Q \text{ and } S; E$ will have the following structure:

```

try {
  C(P)
} catch { try {
  C(Q)
} catch {

```

```
C(S)
}}
```

Even using our algorithm, this number of operations can be too high to be run on-card. Our JCML compiler issues a warning when such a situation arises. The user can enable the code generation for quantifiers, for instance to be used during the application test phase. This code will not be generated for the production, on-card version of the applet.

The treatment of existential quantifiers uses the equivalence $\exists x.P(x) \equiv \neg\forall x.\neg(P(x))$.

6 Experiments, Optimization and Results

In this section, the *UserAccess* example is used as a case study for our JCML compiler. Several experiments have been performed in order to evaluate the resulting code.

In order to ensure the optimal use of the resources, the JCML compiler complies with the following requirements:

- *No checking methods or calls are generated for empty specifications.* For instance, if a class does not contain an invariant specification, the method to check invariant is not generated.
- *No checking methods or calls are generated for the trivial specification (true).*
- *If there is no verification to be done for a method call, then, this method is not renamed and a wrapper for it is not defined.*
- *If the specification to be checked is a Java Card expression, then this expression is used as it is, without generating extra evaluation code for it.* This does not happens, for instance, with quantifiers.
- *Compilation flags are used to set the level of verification required.* For instance, no methods are generated for invariant or postcondition when only preconditions are required.
- *If a specification does not hold, an exception is signaled.*
- *If a specification cannot be checked, it is supposed to be false.* (Closed-world assumption.)

The source and object code generated by our implementation is compared to the original JML implementation [6]. Our experiments consist on compiling the *UserAccess* example using our JCML and the original JML compilers. Our compiler generates Java Card code. The code generated by the JML compiler is not Java Card compliant. We analyze both compilers in terms of the sizes of the generated code, the size of the executable class file and the execution time for each method.

Figure 7 shows the compilation process of both compilers. Both workflows are similar: the source code is translated into a Java/Java Card program, which is then compiled to obtain a CAP file. Notice that the CAP file generated from the JML

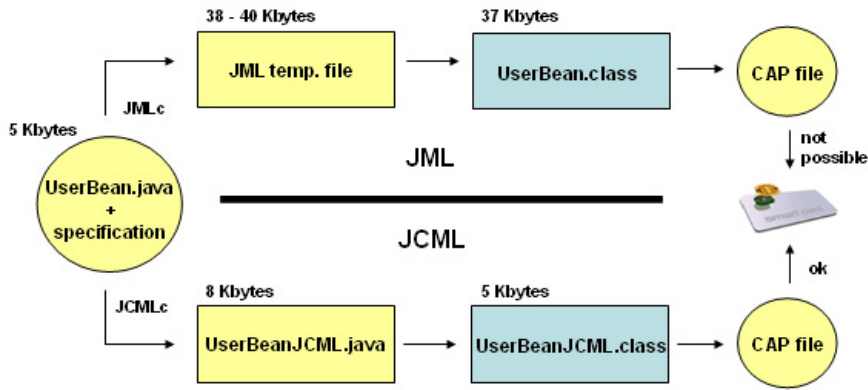


Fig. 7. JCMLc x JMLc.

specification cannot be run on-card, even if the original annotated code is Java Card compliant. This happens because the verification code generated by JMLc uses libraries and types which are not in the Java Card platform.

The wrapper approach proposed in section 5 generates methods for preconditions, postconditions, invariants and renames the original method, which becomes internal, private. This situation generates a large number of method calls.

In the following, we explore the inlining optimization technique for the JCML compiler. Method inlining can have the advantage of reducing the processing time, at the cost of possibly increasing the size of the generated code. Due to the restrictive nature of our applications, the use of this technique on the compiler should be carefully studied. We devised several versions of the compiler, using inlining to different extents:

- JCMLc1:** No inlining. This is the wrapper approach, as presented in section 5.
- JCMLc2:** Inlining is used only for the original methods. Instead of creating new, private methods, the body of each original method is inlined into its wrapper.
- JCMLc3:** Inlining of original methods, pre and postconditions. Pre and postconditions are also inlined in the wrapper methods. Invariant-checking methods are still generated.
- JCMLc4:** All the methods are inlined into the wrapper.

Table 1 presents the number of lines of code generated for for each method of the example. The last three lines of Table 1 show the total size of the generated code, expressed in lines of Java code (**Source (LOC)**), Kbytes of Java code (**.Java (KB)**) and Kbytes of the executable file (**.class (KB)**). The column **Original** shows the number of lines of the original annotated program. The columns **JCMLc1** to **JCMLc4** show the number of lines of Java code for each version of the program, as they are generated by our JCML compiler, using the optimization levels described above. The column **JMLc** contains the number of lines generated by JMLc for our example.

Method/LOC	Original	JCMLc1	JCMLc2	JCMLc3	JCMLc4	JMLc
<i>setID</i>	7	58	55	37	43	294
<i>getID</i>	3	36	32	32	39	221
<i>setType</i>	8	58	55	37	43	299
<i>getType</i>	3	36	32	32	39	196
<i>addArea</i>	10	49	46	41	44	277
<i>hasAccess</i>	11	54	50	42	46	270
<i>addCredits</i>	7	46	43	37	43	262
<i>removeCredits</i>	6	46	43	35	41	268
<i>getCredits</i>	3	36	32	32	39	196
Source (LOC)	103	315	281	197	460	2394
.Java (KB)	4.78	10.00	9.12	6.76	22.60	82.2
.class (KB)	2.0	5.46	4.68	3.24	7.04	30.1

Table 1
UserAccess - Lines of code.

Notice that the number of lines of Java code generated by our implementation is much smaller than those of the equivalent JML code. For instance, for those methods without specification, such as `getCredits`, there is no additional code to be generated. In this case, our compiler copies the original code for the method, while, the JML compiler generates a large amount of code.

The code generated by JCMLc (*i*) is, in all cases, much smaller than the one generated by JMLc and (*ii*) depending on the complexity of The column **Original** shows the number of lines of the original annotated program. The columns **JCMLc1** to **JCMLc4** show the number of lines for each method, as they are generated by our JCML compiler, using the optimization levels described above. The column **JMLc** contains the number of lines generated by JMLc for our example. the specification, may have a size which is similar to the original annotated program, specially when we consider the executable code, which is the one effectively loaded to the card (last line of table 1).

Execution times for each method of our example are shown in Table 2. The numbers in this table are CPU times, in milliseconds. The experiment was run on a Celeron 1.3 GHz laptop with 1.2GB RAM. These data were collected using the *Profiler* plugin for Eclipse.

Notice that the inlining for all the generated methods resulted in execution times that are comparable to the ones without verification code, even with one quantifier in the invariant that is repeatedly checked. These execution times, together with the sizes shown in Table 1, show that the use of JCML is both possible for Java Card and not too expensive. The code generated by our compiler is consistently faster and smaller than the code generated by JMLc. The facts stated above allow us to conclude that one can afford the use of a behavioral specification language on Java Card.

7 Related Work

Formal method systems that take Java Card features into account include Krakatoa [13] and the KeY System [3,2]. Krakatoa proves Java/Java Card programs

Method	Original	JCMLc 1	JCMLc 2	JCMLc 3	JCMLc4	JMLc
setID	0.008	0.184	0.136	0.037	0.011	1.420
getID	0.008	0.111	0.077	0.076	0.014	1.179
setType	0.008	0.178	0.131	0.037	0.010	1.436
getType	0.007	0.070	0.037	0.037	0.010	1.069
addArea	0.058	0.218	0.251	0.155	0.069	2.809
hasAccess	0.008	0.171	0.124	0.075	0.014	1.429
addCredits	0.008	0.245	0.201	0.124	0.046	1.591
removeCredits	0.021	0.244	0.160	0.113	0.062	1.306
getCredits	0.007	0.070	0.037	0.036	0.010	1.123

Table 2
UserAccess - Execution times (milliseconds).

annotated with JML specifications by using the *Why* [7] and *Coq* [20] tools. *Why* is a proof obligation generator and *Coq* is a proof assistant. Krakatoa translates Java/Java Card code into the *Why* input language (an ML-like language), which generates proof obligations to be interactively proved by means of the *Coq* proof assistant. The KeY system is intended to integrate the design, implementation and formal specification and verification of object-oriented languages. The KeY system is based on a theorem prover for the first-order Dynamic Logic for Java and can verify Java Card programs thoroughly. Both Krakatoa and KeY perform static verification only, as it is the case of other related works [12][16] [21].

Efforts towards runtime verification of Java (and Java ME) can be found in [18]. That work proposes the use of AspectJ to implement a JML compiler that takes specifications and generates bytecode compliant with both Java and Java ME virtual machines. Regarding their language constructs, Java ME is a richer language than Java Card and the architectures for which Java ME is targeted are less constrained than those in which Java Card applets run.

8 Conclusions and Future Work

This paper presented JCML – a language for specification of Java Card programs – and its associated compiler. JCML annotates Java Card programs to produce run-time verification code which can be performed on devices with severe memory and processing restrictions. JCML includes all JML constructs which can be translated into Java Card compliant code. A case study was used, and the obtained results show that the proposed approach is effective. For instance, in our example, JCML generated an executable code which is approximately 75% smaller than the one generated by JMLc, even when execution speed is the primary concern (all verification methods inlined).

The code generated by our compiler is smaller and faster than equivalent code generated by the original JML compiler. This is due to the following facts:

- JCMLc is devised to be optimized: For instance, no tests or calls are generated for empty conditions. The original JML compiler generates code for all conditions, independently of the original JML specification.
- We use static analysis to define the upper and lower bound of variables in quan-

tifiers.

- In the original JML compiler, assertion undefinedness is treated in such a way that assertion runtime checking considers the context and the kind of event that led to the exception to conservatively preserve JML semantics avoiding false positives as much as possible. This complex treatment given by JMLc is however too heavy for a smart card environment. Our choice was then to assume that any uncheckable specification is false.

The version of the compiler presented here is able to check some simple (yet meaningful) properties. Current work includes the extension of the class of specifications dealt with by the compiler. To be able to generate verification code for a greater class of specifications, additional optimizations need to be employed. Our next step is to deal with exceptional behaviour so that the application that runs on-card is able to gracefully recover from faults.

In another line of work, studies concerning the use of aspects in the implementation of the compiler, as done in [18], will also be carried out. We plan to compare results with our current approach and to identify possible common features and improvements.

Finally, new case studies will be carried out, in order to complete the validation of the approach and to define the range of applications that can benefit from it.

Acknowledgement

The authors would like to thank SBMF reviewers and attendants which provided interesting feedback on this work and, particularly, Prof. Jim Woodcock, for his important observation on undefined expressions.

References

- [1] J.-R. Abrial. *The B Book: Assigning Programs to Meanings*. Cambridge University Press, August 1996.
- [2] Bernhard Beckert, Martin Giese, Reiner Hähnle, Vladimir Klebanov, Philipp Rümmer, Steffen Schlager, and Peter H. Schmitt. The KeY System 1.0 (Deduction Component). In *CADE*, pages 379–384, 2007.
- [3] Bernhard Beckert, Reiner Hähnle, and Peter H. Schmitt, editors. *Verification of Object-Oriented Software: The KeY Approach*. LNCS 4334. Springer-Verlag, 2007.
- [4] A. Bhorkar. A Run-time Assertion Checker for Java using JML. Technical Report 00-08, Department of Computer Science, Iowa State University, May 2000.
- [5] Zhiqun Chen. *Java Card Technology for Smart Cards: Architecture and Programmer's Guide*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2000.
- [6] Y. Cheon. *A Runtime Assertion Checker for the Java Modeling Language*. PhD thesis, Department of Computer Science, Iowa State University, April 2003.
- [7] J.-C. Filliâtre. Why: a Multi-language Multi-prover Verification Condition Generation. Technical report, Université Paris-Sud, France, LRI - CNRS UMR 8623, March 2003.
- [8] Cliff B. Jones and Jim Woodcock. Special Edition on the Mondex Case Study. *Formal Aspects of Computing*, 20(1), 2008.
- [9] G. T. Leavens and Y. Cheon. Design by Contract with JML. Draft, Available from <http://www.jmlspecs.org>, 2006.

- [10] G. T. Leavens, E. Poll, C. Clifton, Y. Cheon, C. Ruby, D. Cok, P. Müller, J. Kiniry, and P. Chalin. *JML Reference Manual*, May 2006. Draft revision 1.193.
- [11] Gary T. Leavens. Tutorial on JML, the Java Modeling Language. In *ASE*, page 573, 2007.
- [12] K. R. M. Leino, G. Nelson, and J. B. Saxe. ESC/Java User’s Manual. Technical note, Compaq Systems Research Center, October 2000.
- [13] C. Marche, C. Paulin Mohring, and X. Urbain. The KRAKATOA Tool for Certification of JAVA/JAVACARD Programs Annotated in JML. *Journal of Logic and Algebraic Programming*, 58(1–2):89–106, 2004.
- [14] Bertrand Meyer. Applying “Design by Contract”. *IEEE Computer*, 25(10):40–51, 1992.
- [15] Bertrand Meyer. *Object-Oriented Software Construction*. Prentice Hall PTR, March 2000.
- [16] Jeremy W. Nimmer and Michael D. Ernst. Static Verification of Dynamically Detected Program Invariants: Integrating Daikon and Esc/java, 2001.
- [17] E. Ortiz. An Introduction to Java Card Technology. Technical report, Sun Microsystems, 2005.
- [18] H. Rebêlo, S. Soares, M. Cornélio, R. Lima, and L. Ferreira. Implementing Java Modeling Language Contracts with AspectJ. In *Proceedings of the 23rd Annual ACM Symposium on Applied Computing*, pages pp. 228–233, Fortaleza-Brazil, 2008.
- [19] Plácido A. Souza Neto. JCML - Java Card Modeling Language: Definição e Implementação. Master’s thesis, Programa de Pós-Graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, 2007.
- [20] The Coq Development Team. *The Coq Proof Assistant : Reference Manual : Version 8.1*. INRIA, 2007. available at <http://coq.inria.fr/doc-eng.html>.
- [21] J. Van den Berg and B. Jacobs. The LOOP Compiler for Java and JML. In Tiziana Margaria and Wang Yi, editors, *TACAS*, volume 2031 of *Lecture Notes in Computer Science*, pages 299–312. Springer, 2001.
- [22] Jim Woodcock and Jim Davies. *Using Z: Specification, Refinement, and Proof*. Series in Computer Science. Prentice Hall International, Upper Saddle River, NJ, USA, 1996.