Runtime Constraint Checking Approaches for OCL, A Critical Comparison

Carmen Avila  
*The University of Texas at El Paso, ceavila3@miners.utep.edu*

Amritam Sarcar

Yoonsik Cheon  
*The University of Texas at El Paso, ycheon@utep.edu*

Cesar Yeep  
*The University of Texas at El Paso, cyeep@miners.utep*

Follow this and additional works at: https://scholarworks.utep.edu/cs_techrep

Part of the Computer Engineering Commons

Comments:
Technical Report: UTEP-CS-10-04

**Recommended Citation**
Avila, Carmen; Sarcar, Amritam; Cheon, Yoonsik; and Yeep, Cesar, "Runtime Constraint Checking Approaches for OCL, A Critical Comparison" (2010). *Departmental Technical Reports (CS)*. 4.  
[https://scholarworks.utep.edu/cs_techrep/4](https://scholarworks.utep.edu/cs_techrep/4)

This Article is brought to you for free and open access by the Computer Science at ScholarWorks@UTEP. It has been accepted for inclusion in Departmental Technical Reports (CS) by an authorized administrator of ScholarWorks@UTEP. For more information, please contact lweber@utep.edu.
Runtime Constraint Checking Approaches for OCL, A Critical Comparison

Carmen Avila, Amritam Sarcar, Yoonsik Cheon, and Cesar Yeep

TR #10-04
February 2010; revised May 2010

Keywords: design constraints, runtime checking, class invariants, pre and postconditions, aspect-oriented programming, Object Constraints Language (OCL), AspectJ language, JML language.


Department of Computer Science
The University of Texas at El Paso
500 West University Avenue
El Paso, Texas 79968-0518, U.S.A.
Abstract—There are many benefits of checking design constraints at runtime—for example, automatic detection of design drift or corrosion. However, there is no comparative analysis of different approaches although such an analysis could provide a sound basis for determining the appropriateness of one approach over the others. In this paper we conduct a comparative analysis and evaluation of different constraint checking approaches possible for the Object Constraint Language (OCL). We compare several approaches including (1) direct translation to implementation languages, (2) use of executable assertion languages, and (3) use of aspect-oriented programming languages. Our comparison includes both quantitative metrics such as runtime performance and qualitative metrics such as maintainability of constraint checking code. We found that the implementation language-based approaches perform better in terms of memory footprint and runtime overheads but the other approaches are more appealing in terms of maintainability.

Keywords—pre and postconditions; runtime constraint checking; AspectJ; JML; OCL

I. INTRODUCTION

A recent trend in software development is a shift of focus from writing code to building models [1]. The idea is to systematically generate an implementation from a model through a series of transformations. A key requirement of this model-driven development is the availability of a precise model to generate working code from it. A formal notation such as the Object Constraint Language (OCL) [2] can play an important role to build such a precise model because the most popular modeling language, UML [3], lacks sufficient precision to enable complete code generation; OCL is a textual, declarative notation to specify constraints or rules that apply to UML models. Modeling and specifying design constraints explicitly is also said to improve reasoning of software architectures and thus their qualities [4].

Besides static reasoning, formally specified design constraints such as OCL constraints can be checked at runtime, and there are many benefits of checking design constraints at runtime. For example, it can detect when an implementation deviates from its design, often called design corrosion or drift [5] [6]. Design corrosion is said to be proportional to the development and maintenance time and occurs when the initial design of software gets modified to accommodate new or changed requirements or to correct defects. It also occurs as the result of code hacks and workarounds, a common practice of software maintenance. Runtime constraint checking can also facilitate automating program or conformance testing by allowing constraints to be used as test oracles [7].

Several different approaches are possible for checking design constraints such as OCL constraints against implementations at runtime. The most common approach is to translate constraints directly to an implementation language by coding a constraint checker in that language and making it part of the implementation [8]. Constraints can also be translated to executable assertions if the implementation language provides an assertion facility such as an assert statement or if it has a separate assertion languages [9] [10]. Yet another possibility is to apply aspect-oriented programming to modularize constraint checking code by implementing constraint checking as a crosscutting concern (see Section III-C for details) [11] [12].

We expect that each of the aforementioned approaches have its strengths and weaknesses. In this paper we conduct a comparative analysis of these approaches in order to determine appropriateness of one approach over the others. In our study we use OCL as the constraint specification language and Java as the implementation language. Our analysis will involve applying different approaches to a common set of OCL constraints and recording a set of metrics from each application. For the comparison we will use both quantitative metrics such as runtime speed and memory usage and qualitative metrics such as maintainability of constraint checking code. We will consider various types of OCL constraints such as class invariants, operation pre and postconditions.

The remainder of this paper is structured as follows. In Section II we briefly explain OCL by introducing example constraints to be used throughout this paper. In Section III we describe in detail four different constraint checking approaches by applying them to the example constraints. In Section IV we first describe the case study that we performed...
to compare the approaches and then analyze the results from the case study. In Section V we conclude this paper with a summary of our findings.

II. BACKGROUND ON OCL

The Object Constraint Language (OCL) [2] is a textual, declarative notation to specify constraints or rules that apply to UML models. OCL can play an important role in model-driven software development because UML lacks sufficient precision to enable the transformation of a UML model to complete code. In fact, it is a key component of OMG’s standard for model transformation for the model-driven architecture [13].

A UML diagram alone cannot express a rich semantics of and all relevant information about an application. The diagram shown in Figure 1, for example, is a UML class diagram for bank accounts. A customer can own several accounts, and an account can be linked to another account for overdraft protection. However, the class diagram doesn’t express the fact that an account cannot be linked to itself for overdraft protection. It is very likely that a system built based only on diagrams alone will be incorrect. OCL allows to precisely describe this kind of additional constraints on the objects and entities present in a UML model. It is based on mathematical set theory and predicate logic and supplements UML by providing expressions that have neither the ambiguities of natural language nor the inherent difficulty of using complex mathematics. The above-mentioned fact, for example, can be expressed in OCL as follows.

```ocl
class Account {
  context Account
  inv: self <> overdraft
}
```

This constraint, called an invariant, states a fact that should be always true in the model. The keyword self denotes the object being constrained by an OCL expression, called a contextual instance; in this case it is an instance of the Account class. The invariant says that an account cannot be equal to its overdraft protection account. It is also possible to specify the behavior of an operation in OCL. For example, the following OCL constraints specifies the behavior of an operation Customer::addAccount by writing a pair of predicates called pre and postconditions.

```ocl
class Customer
  def addAccount(acc: Account): void
  inv: not accounts->includes(acc)
  post: accounts = accounts@pre->including{acc}
```

The pre and postconditions states that, given an account not already owned by a customer, the operation should insert the account to the set of accounts owned by the customer. The postfix operator @pre denotes the value of a property (accounts) in the pre-state, i.e., just before an operation invocation. The constraints are written using OCL collection operations such as includes and including; the includes operation tests whether an object is contained in a collection, and the including operation adds an element to a collection.

OCL provides a few other constructs. The def construct specifies the initial value of an attribute or association end. The derive construct introduces a new attribute or query operation to a UML model such as a class diagram. It also specifies the value of the new attribute or the return value of the new operation. The def construct specifies the value of a derived attribute or association end, and the body construct defines the result of a query operation.

III. RUNTIME CONSTRAINT CHECKING

Several different approaches are possible for checking design constraints against implementations at runtime. For example, Froihofer et al. reviewed and evaluated different constraint validation approaches for Java [14]. They discussed handcrafted approaches, code instrumentation using OCL and JML [15], aspect-oriented programming, proxy implementations, CORBA, and EJBs. Each approach has its own advantages and disadvantages such as runtime overhead that ranges from a factor of two to more than one hundred. In this paper we focus on approaches available for OCL by considering OCL-specific features and consider only those approaches that do not require external or separate constraint checking monitors. We study the following three approaches classified by the target language to which OCL constraints are translated or in which the checking code is written.

- **Implementation languages.** This is the most widely-used approach and maps OCL constraints to an implementation language in that a constraint checker is written in that language and becomes part of the implementation (see for example [8]). If the implementation language supports an assertion facility such as the assert macro or statement, constraints can also be translated to executable assertions.

- **Assertion languages.** Some programming languages such as Eiffel support class invariants and operation pre and postconditions as built-in language constructs called design-by-contract [16]. Design-by-contract is not a formal part of Java, but there are several extensions or tools to support it for Java [15] [17]. OCL constraints can be translated to design-by-contract assertions [9] [10].

- **Aspect-oriented languages.** If an implementation language has an aspect-oriented extension, e.g., AspectJ for Java, it can be used to implement constraint checking code [11] [12] [18]. Constraint checking is viewed as a crosscutting concern and implemented as a so-called
aspect that resides in a separate module and advises the implementation code (see Section III-C below).

In the following subsections we explain each of the aforementioned approaches in detail using the OCL examples introduced in Section II.

A. Translating to Implementation Languages

1) Using Programming Language Statements: In this approach one injects hand-crafted checking code to an implementation. For each OCL constraint, one has to decide appropriate checking points and then translate the constraint to programming language statements. For example, a class invariant should be checked at the end of a constructor execution and before and after the execution of every method because a constructor has to establish the class invariant and every method has to preserve it. As an example, let us consider the addAccount operation of the Customer class introduced in Section II. Here is a possible implementation of the operation in Java.

```java
public void addAccount(Account acc) {
    accounts.add(acc);
    acc.setOwner(this);
    // check invariant at pre-state if any
    if (accounts.contains(acc))
        throw new OclError("Precondition violation");
    // calculate accounts@pre
    Set<Account> accsPre = new HashSet<Account>(accounts);
    accounts.add(acc);
    acc.setOwner(this);
    // check postcondition
    accsPre.add(acc);
    if (!accounts.equals(accsPre))
        throw new OclError("Postcondition violation");
    // check invariant at post-state if any
}
```

As shown, the method body is wrapped with constraint checking code that checks the pre and postconditions and the class invariant as well in the pre and post-states.

In practice one would prefer to have a separate constraint checking method for each OCL constraint rather than embedding the checking code to the method body. This will modularize constraint checking code by eliminating duplicate code such as the invariant checking code. It will also facilitate reuse of constraint checking code and support for constraint inheritance; for example, to support the inheritance of an invariant, one only needs to make the invariant checking method of the subclass to call that of the superclass.

The main shortcoming of this approach is that there are a lot of manual work involved, such as translating OCL constraints to programming language statements and implementing the supporting infrastructure (e.g., one for constraint inheritance). Additionally, the resulting code may not be maintainable (refer to Section IV for an analysis).

2) Using Assertion Facilities: This approach is similar to the previous one except that OCL constraints are now translated to executable assertions of the implementation language. For example, the following is the addAccount method with OCL constraints translated to Java assert statements.

```java
public void addAccount(Account acc) {
    // check precondition
    if (accounts.contains(acc))
        throw new OclError("Precondition");
    Set<Account> accsPre = new HashSet<Account>(accounts);
    accounts.add(acc);
    acc.setOwner(this);
    accsPre.add(acc);
    assert accounts.equals(accsPre) : "Postcondition";
}
```

As in the previous approach, one has to determine appropriate constraint checking points and manually translate the constraints. However, one advantage of this approach is its ability to selectively enable or disable assertions; in Java, for example, one can control assertions at various granularities by using command-line switches.

B. Using Assertion Languages

In this approach, OCL constraints are translated to executable assertions such as design-by-contract. There are several extensions to Java that support design-by-contract [14]. For example, the Java Modeling Language (JML) [15] [17] is a formal interface specification language for Java to document the behavior of Java classes and interfaces, and a significant subset of JML is executable. The following code shows the addAccount method annotated with JML specifications.

```java
/**
 * @public model JMLObjectSet accSet;
 * @private represents accSet
 * @old = JMLObjectSet.convertFrom(accounts);
 * @*/

public void addAccount(Account acc) { /*...*/
    /*
    * @requires !accSet.has(acc);
    * @ ensures accSet.equals(\old(accSet.insert(acc)));
    */
}
```

As shown, JML annotations are enclosed in special comments such as /*@ */ and precede the Java declarations such as method declarations that are being annotated. Method pre and postconditions follow the keywords requires and ensures, respectively. The JML-specific \old expression denotes the pre-state value of its argument. An interesting feature of JML is that it provides a built-in support for writing abstract specifications [19]. For example, the above pre and postconditions are written in terms of a specification-only variable accSet of which value is given as a mapping from a program variable accounts. This way of writing assertions has several advantages; for example, such assertions are less affected by implementation changes and do not expose implementation details such as a private field accounts. Another strength of using assertion languages is that OCL constraints are often directly mapped to assertions. This is particularly noticeable when translating OCL constraints consisting of iterator operations such as forAll and

1JML specifications can also reside in separate specification files.
exists because similar sorts of quantifiers are supported in JML.

C. Using Aspect-Oriented Programming Languages

Aspect-oriented programming is a new programming paradigm to address in a modular way so-called crosscutting concerns such as logging that have to be implemented in multiple program modules. The key idea is to denote a set of execution points, called join points, and introduce additional behavior, called an advice, at the join points. AspectJ [20] is an aspect-oriented extension for Java and provides built-in language constructs for join points and advices. OCL constraints can be systematically translated to AspectJ code to check at runtime the conformance of a Java implementation [11] [12] [18]. For example, the following AspectJ code checks the pre and postconditions of the addAccount operation.

```java
public privileged aspect CustomerChecker {
    pointcut addAccountExe(Customer c, Account a):
        execution(void Customer.addAccount(Account)) && this(c) && args(a);

    void around(Customer c, Account a): addAccountExe(c, a) {
        Set<Account> accsPre = new HashSet<Account>(c.accounts);
        proceed(c, a);
        accsPre.add(a);
        assert c.accounts.equals(accsPre) : "Postcondition";
    }
}
```

The pointcut declaration designates a set of execution points and optionally exposes certain values at these execution points. For example, the pointcut addAccountExe denotes execution of the addAccount method and exposes the receiver (c) and the argument (a). The around keyword introduces an advice that wraps around a join point and can potentially replace it; there are also before and after advices. The above advice first checks the precondition by referring to the values exposed by the pointcut, proceeds to continue with the normal flow of execution at the join point (as indicated by the proceed keyword), and finally checks the postcondition. If the Customer class is compiled with the above aspect, every execution of the addAccount method will be checked against the pre and postconditions. The aspect-oriented approach has several advantages over the previous approaches. For example, the constraint checking logic is completely separated from the implementation, and the implementation modules are oblivious of the constraint checking code, even its existence. Thus, constraint checking code can be easily added or removed from the implementation. It will also enable runtime checks to be applied to different implementations of the same design and be selectively enabled or disabled, for example, for production code.

IV. Comparison

To find out the strengths and weaknesses of the approaches explained in the previous section, we compare them both quantitatively and qualitatively. For the comparison we use the following quantitative metrics.

- Source code size. We measure and compare this because it indicates the amount of work needed to implement constraint checking code. We also measure the number of source code lines needed to translate one line of a constraint.
- Bytecode size. This is one factor that determines the memory footprint of a program and thus may be important for certain systems like consumer electronics and embedded systems where low-memory-footprint programs are required.
- Dynamic memory usage. This is another factor that determines the memory footprint of a program.
- Execution time. This may be one of the most important criteria for selecting a constraint checking approach, especially for use in production code.

We also compare the approaches qualitatively using such criteria as easiness of translation, support for automation, and maintainability of checking code. In the following subsections we first describe the case study that we performed for the comparison and then analyze the comparison results.

A. Case Study

We performed a case study by using an open-source Java program that has a formal UML model including OCL constraints. The use of an open-source program eliminates subjectiveness during the experiment and makes the case study more realistic. The OCL standard specification defines several collection types such as Collection, Set, OrderedSet, Bag, and Sequence, and the behavior of each type is formally specified in OCL [21]. There are Java implementations of the OCL collection types [9] [22], and for our case study we used the one included in the Dresden OCL Toolkit [22]. This implementation supports all the collection operations specified in the standard except for iterator operations such as forAll that take OCL expressions as parameters and work on each element of a collection. The standard specifies 336 lines of OCL constraints, most of which are postconditions, and the implementation has 87 methods and 1781 lines of source code including comments.

We manually translated OCL constraints to runtime checks using each of the approaches. For the two Java-based approaches we directly modified the source code to insert assertion checking code. For the JML-based approach we also changed the source code to add JML annotations. For the AOP-based approach, however, instead of modifying the Java source code we introduced one AspectJ aspect for each Java class, responsible for checking all the constraints specified for that class. We next devised a suite of test data for each collection type and measured the runtime performance of each approach. The test suite also showed that all approaches are equally effective in detecting constraint
violations at runtime; it revealed several errors both in the implementation and in the constraints themselves [12].

B. Results

1) Source Code Size: The source code size is an important metric because it indicates the amount of work needed. Table I shows the measurement of source code size for each approach, given in the number of source code lines. It also shows the average number of source code lines needed to translate one line of OCL constraints (see the CC/OCL column). As expected, JML is superior in this metric because it supports similar language constructs as OCL including invariants, pre and postconditions, and quantifiers, and thus most OCL constraints can be directly translated to JML specifications. The AOP approach requires the most work because one has to not only translate OCL constraints to Java statements but also introduce AOP-specific declarations such as pointcuts, advices, and aspects.

2) Bytecode Size: Table II shows the bytecode size of constraint checking code. The Java assert statement-based approach produces the most compact bytecode. It produces about 24 times more compact bytecode than the JML approach and requires on average about 21 times less bytecode per line of OCL constraints. It is interesting to learn that the bytecode size is not always proportional to the source code size. This is perhaps because both AspectJ and JML compilers have to produce code for a runtime support framework—for example, for dynamic pointcut resolution and for specification inheritance. Furthermore, the particular JML compiler (jml4c) that we used for this case translates quantifiers to inner classes, which brings an additional overhead on bytecode size [23]; more than half of the translated JML assertions were quantified expressions.

3) Dynamic Memory Usage: Table III shows the dynamic memory requirement for each approach, obtained using the Eclipse profiling tools. It shows the number of live instances, active size in bytes, the total number of instances, and the total size in bytes; a live instance is an instance that is alive, i.e., not garbage collected. The table also shows the memory overhead for each approach. The JML-based approach requires eight times more heap storages than the base code, and for other approaches the memory overhead is negligible. We suspect that this is because the JML compiler translates quantified assertions to inner classes.

4) Execution Time: Table IV shows the number of method calls and the CPU time required to run the test suite by each approach, along with the overhead due to constraint checking. As shown, the Java-based approaches outperform both the JML and the AOP-based approaches; for example, the JML-based approach is about 27 to 38 times slower than the Java-based approaches and requires 80 times more CPU time than the base code. This may be explained in part by the huge number of additional method calls introduced by the constraint checking code; JML translates each assertion to a separate assertion checking method and uses Java’s reflection facility to support inheritance of specifications, e.g., to inherit specifications from the abstract superclass Collection. We also learned that application characteristics influence the execution times differently for different approaches; for example, both the AOP and the Java statement-based approaches require the longest execution time for the Collection class, the Java assert-based approach for the Set class, and the JML approach for the Sequence class.

5) Summary of Overheads: Table V and Figure 2 summarize the overheads of runtime constraint checking. The use of languages such as JML and AspectJ introduces significant runtime overheads on CPU time and dynamic memory storage. For example, programs with JML annotations require 84 times more CPU time and 13 times more heap storage than those without JML annotations. However, the increases of source and bytecode sizes are relatively negligible compared to runtime overheads. In summary, the Java-based approaches outperform the other approaches when considering only runtime overheads.

6) Qualitative Comparison: The case study also allowed us to compare the four approaches qualitatively using such criteria as translation easiness and maintainability of check-
Table III

<table>
<thead>
<tr>
<th>Activity</th>
<th>Live instances</th>
<th>Active size</th>
<th>Total instance</th>
<th>Total size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number</td>
<td>Overhead</td>
<td>Byte</td>
<td>Overhead</td>
</tr>
<tr>
<td>Base</td>
<td>248</td>
<td>0</td>
<td>5552</td>
<td>0</td>
</tr>
<tr>
<td>Stmt</td>
<td>337</td>
<td>0.26</td>
<td>6976</td>
<td>0.20</td>
</tr>
<tr>
<td>Asrt</td>
<td>316</td>
<td>0.22</td>
<td>6640</td>
<td>0.16</td>
</tr>
<tr>
<td>JML</td>
<td>447</td>
<td>0.45</td>
<td>47256</td>
<td>0.88</td>
</tr>
<tr>
<td>AOP</td>
<td>461</td>
<td>0.46</td>
<td>8936</td>
<td>0.38</td>
</tr>
</tbody>
</table>

Table V

<table>
<thead>
<tr>
<th>Source</th>
<th>Bytecode</th>
<th>Memory</th>
<th>CPU Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stmt</td>
<td>0.58</td>
<td>0.91</td>
<td>0.01</td>
</tr>
<tr>
<td>Asrt</td>
<td>0.22</td>
<td>0.55</td>
<td>0.01</td>
</tr>
<tr>
<td>JML</td>
<td>0.19</td>
<td>12.96</td>
<td>0.84</td>
</tr>
<tr>
<td>AOP</td>
<td>0.71</td>
<td>2.22</td>
<td>0.02</td>
</tr>
</tbody>
</table>

Table VI

<table>
<thead>
<tr>
<th>Source</th>
<th>Bytecode</th>
<th>Memory</th>
<th>CPU Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stmt</td>
<td>×</td>
<td>δ</td>
<td>○</td>
</tr>
<tr>
<td>Asrt</td>
<td>×</td>
<td>δ</td>
<td>○</td>
</tr>
<tr>
<td>JML</td>
<td>×</td>
<td>δ</td>
<td>○</td>
</tr>
<tr>
<td>AOP</td>
<td>×</td>
<td>δ</td>
<td>○</td>
</tr>
</tbody>
</table>

3 However, there are a few rarely-used OCL operators such as message sending that are hard to express in JML because JML doesn’t have built-in support for them.

V. Conclusion

We explained four different approaches for translating OCL constraints to runtime checks: (1) using implementation languages such as Java, (2) using built-in assertion facilities such as the `assert` statement, (3) using assertion or design-by-contract languages such as JML, (4) using aspect-oriented programming language such as AspectJ. We then compared these approaches critically through a case study. We learned that the first two approaches based on implementation languages are most efficient in terms of runtime performance such as CPU time and heap storage. However, our qualitative comparison favored the other two approaches. For example, OCL constraints, in most cases, can be directly translated to JML annotations, and the resulting JML specifications are easy to read and understand. There are translation rules from OCL to JML and AspectJ.
JML specifications and AspectJ code are better modularized and thus reusable, plug-and-playable, controllable, and maintainable. In summary, the first two approaches may be a better choice for the use of constraint checking in production code if memory footprint or runtime speed is an important concern. On the other hand, the other two approaches may be more appealing for the development use (e.g., testing and debugging) of constraint checking where concerns such as accommodation for changes are more important.

ACKNOWLEDGMENT
The work of the authors was supported in part by NSF grants CNS-0707874 and DUE-0837567.

REFERENCES