



# AUTOMATED TRANSLATION OF VDM-SL TO JML-ANNOTATED JAVA

TECHNICAL REPORT

PETER W. V. TRAN-JØRGENSEN

Peter Gorm Larsen

GaryT. Leavens

Aarhus University - Department of Engineering



AARHUS  
UNIVERSITY

DEPARTMENT OF ENGINEERING

# Table of Contents

<b>Table of Contents</b>	<b>i</b>
<b>Chapter 1 Introduction</b>	<b>1</b>
1.1 The tool implementation . . . . .	1
1.2 About this technical report . . . . .	2
<b>Chapter 2 The Translation</b>	<b>3</b>
2.1 Introduction . . . . .	3
2.2 Design-by-Contract (DbC) with the Vienna Development Method Specification Language (VDM-SL) and the Java Modeling Language (JML) . . . . .	4
2.3 The implementation of the JML translator . . . . .	9
2.4 Case study example . . . . .	10
2.5 Translating VDM-SL contracts to JML . . . . .	13
2.6 Checking the Vienna Development Method (VDM) types using JML . . . . .	24
2.7 Other aspects of VDM-SL affecting the JML-generation . . . . .	32
2.8 Translation assessment . . . . .	37
2.9 Related work . . . . .	38
2.10 Conclusion and future plans . . . . .	39
<b>A The Automated Teller Machine (ATM) model</b>	<b>41</b>
<b>B The code-generated ATM model</b>	<b>47</b>
<b>C Validation of the translation rules</b>	<b>77</b>
C.1 Map.vdmsl . . . . .	77
C.2 Seq.vdmsl . . . . .	80
C.3 Set.vdmsl . . . . .	83
C.4 AtomicStateInvViolation.vdmsl . . . . .	86
C.5 AtomicStateInvNoViolation.vdmsl . . . . .	89
C.6 InvChecksOnFlagInOtherModule.vdmsl . . . . .	92
C.7 AtomicRecUnion.vdmsl . . . . .	98
C.8 NamedTypeInvValues.vdmsl . . . . .	104
C.9 NamedTypeInvMapUpdate.vdmsl . . . . .	106
C.10 NamedTypeInvSeqUpdate.vdmsl . . . . .	108
C.11 RecursionConservativeChecking.vdmsl . . . . .	109
C.12 NamedTypeInvLocalDecls.vdmsl . . . . .	113
C.13 NamedTypeInvReturn.vdmsl . . . . .	115
C.14 NamedTypeInvMethodParam.vdmsl . . . . .	119
C.15 NamedTypeInvNullAllowed.vdmsl . . . . .	121
C.16 NamedTypeMadeOptional.vdmsl . . . . .	122

## Table of Contents

C.17	NamedTypeInvAsssignments.vdmsl	124
C.18	CaseExp.vdmsl	129
C.19	TernaryIf.vdmsl	131
C.20	LetBeStStm.vdmsl	135
C.21	LetBeStExp.vdmsl	136
C.22	RealParamNil.vdmsl	139
C.23	QuoteAssignNil.vdmsl	140
C.24	NatParamNil.vdmsl	142
C.25	CharReturnNil.vdmsl	143
C.26	Nat1InitWithZero.vdmsl	145
C.27	IntAssignNonInt.vdmsl	146
C.28	BoolReturnNil.vdmsl	148
C.29	RatAssignBool.vdmsl	149
C.30	TokenAssignNil.vdmsl	151
C.31	RecLet.vdmsl	152
C.32	TupLet.vdmsl	156
C.33	RecParam.vdmsl	157
C.34	TupParam.vdmsl	161
C.35	SeqNat1BoolMaskedAsNamedTypeInv.vdmsl	162
C.36	SeqOfNatNilElem.vdmsl	164
C.37	Seq1EvenNatsMaskedAsNamedTypeInv.vdmsl	166
C.38	Seq1AssignEmptySet.vdmsl	168
C.39	SeqEven.vdmsl	170
C.40	RecUnion.vdmsl	172
C.41	Simple.vdmsl	176
C.42	AtomicRecUnion.vdmsl	180
C.43	SetEvenNamedTypeInv.vdmsl	185
C.44	SetOfNat.vdmsl	187
C.45	SetPassNil.vdmsl	188
C.46	RecTypesUnion.vdmsl	190
C.47	OptionalBasicUnion.vdmsl	195
C.48	RecWithRecFieldUpdate.vdmsl	197
C.49	RecWithRecFieldAtomicViolation.vdmsl	207
C.50	CharUnionEven.vdmsl	218
C.51	RecWithRecFieldAtomicNoViolation.vdmsl	220
C.52	RecInRecInAtomic.vdmsl	228
C.53	NamedTypeInvUnionTypeRec.vdmsl	236
C.54	RecWithMapOfRec.vdmsl	256
C.55	RecInRecInvViolation.vdmsl	261
C.56	MaskedRecNamedTypeInv.vdmsl	274
C.57	MaskedRecInvViolated.vdmsl	285
C.58	ModifyRecInMap.vdmsl	301
C.59	Bool.vdmsl	307
C.60	Real.vdmsl	309
C.61	String.vdmsl	310
C.62	Quote.vdmsl	311
C.63	Int.vdmsl	313
C.64	Nil.vdmsl	314
C.65	Char.vdmsl	316

## Table of Contents

C.66 StateInitViolatesInv.vdmsl . . . . .	318
C.67 RecTypeDefInv.vdmsl . . . . .	320
C.68 StateInv.vdmsl . . . . .	324
C.69 PostCond.vdmsl . . . . .	328
C.70 PreCond.vdmsl . . . . .	332
C.71 TupleSizeMismatch.vdmsl . . . . .	337
C.72 NatBoolTupNil.vdmsl . . . . .	339
C.73 NatBooolBasedNamedTypeInv.vdmsl . . . . .	341
C.74 NatBoolNegField.vdmsl . . . . .	343
C.75 ReturnNonInjMapWhereInjMapRequired.vdmsl . . . . .	344
C.76 AssignNonInjMapToInjMap.vdmsl . . . . .	348
C.77 MapBoolToNatAssignNil.vdmsl . . . . .	350
C.78 MapBoolToNatDetectNegInt.vdmsl . . . . .	351
C.79 AssignBoolTypeViolation.vdmsl . . . . .	353
C.80 VarDeclTypeViolation.vdmsl . . . . .	355
C.81 FuncReturnTokenViolation.vdmsl . . . . .	357
C.82 OpParamQuoteTypeViolation.vdmsl . . . . .	359
C.83 Exists.vdmsl . . . . .	360
C.84 ForAll.vdmsl . . . . .	362
C.85 Exists1.vdmsl . . . . .	363
<b>Bibliography</b>	<b>365</b>

# Introduction

A model specified using the VDM can be validated against its contract-based elements (e.g. pre- and postconditions and invariants) in order to ensure that the system behaves as intended. This can, for example, be done through model animation using Overture's VDM interpreter.

When sufficient insight into the system under development has been obtained during the formal analysis, development proceeds to the implementation phase, where the system is realised. One way to realise a VDM model (which forms the focus of this technical report) is by implementing it in a programming language using code generation. However, since no guarantees are currently made about the correctness of the generated code, other measures must be taken to increase the confidence in the correctness of the derived model implementation.

To support this approach, Overture enables fully automated translation of VDM-SL's contract-based elements (pre- and postconditions, and invariants) and type constraints into JML annotations. This translation is achieved using Overture's *JML translator*, which translates VDM-SL models into JML-annotated Java programs. In this way JML tools can be used to validate the generated Java code against the *intended* system behaviour, described using JML. This work-flow is illustrated in fig. 1.1.

## 1.1 The tool implementation

---

The translation is defined as a set of rules that are implemented as an extension of Overture's VDM-to-Java code generator [16] to make the approach fully automated. The JML translator is available in Overture 2.3.8 onwards and can be downloaded via the Overture tool's website [30]. For instructions on how to use the JML translator we refer the reader to Overture's user guide [22], specifically the chapter on the VDM-to-Java code generator.

The generated Java programs can be checked for correctness using JML tools that support Java 7 or later. In particular, the generated Java programs, including this translation, have been tested using the OpenJML [8] runtime assertion checker, which at the current time of writing, supports Java 8. In particular, OpenJML, is the only JML tool that we are aware of that currently supports all the JML constructs generated by the JML translator. The most recent version of OpenJML is available via the OpenJML website [29].

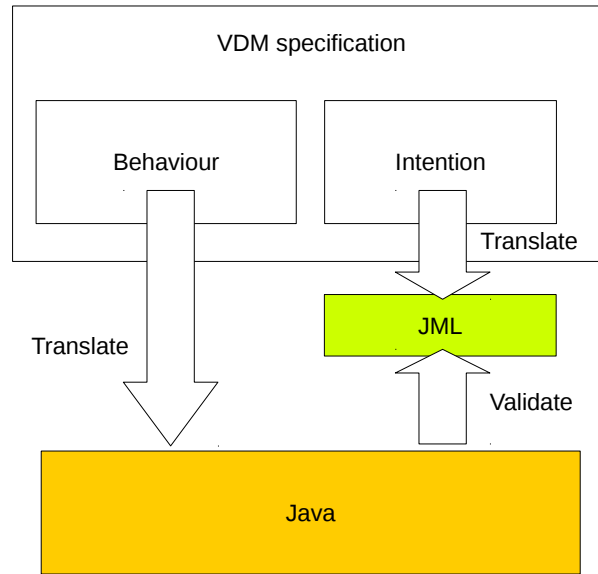


Figure 1.1: Overview of the VDM-to-JML translation.

## 1.2 About this technical report

---

The purpose of this report is to assist VDM users with getting started using the JML translator. Moreover, this report is complementary to [36] – a journal paper that describes the JML translation. In that paper, as well as in this report, the translation is exemplified using a VDM-SL model of an ATM. Due to space limitations only a limited number of examples are provided in [36]. To improve this, this report presents a more complete definition of the translation, including more examples that demonstrate how the translation works.

This report is structured as follows: Chapter 2 presents the translation and demonstrates how the JML translator supports the implementation of VDM-SL models in Java. Appendix A contains the complete version of the ATM model, and the corresponding Java/JML implementation is available in appendix B. Finally, all the regression tests that are used to validate the translation rules are presented in appendix C.

# The Translation

## 2.1 Introduction

---

Design-by-Contract (DbC) is an approach for designing software based on concepts such as pre-conditions, postconditions and invariants [27]. These concepts are referred to as “*contracts*”, according to a conceptual metaphor for the conditions and obligations of a business contract. An example of a formal method that uses DbC elements is the Vienna Development Method (VDM), which was originally developed at IBM in Vienna for the development of a compiler for PL/1 [5, 10, 11]. One way to realise a VDM specification in a programming language is through refinement [39]. This is a stepwise process by which one can transform a formal model into a program that can be verified to semantically satisfy its contracts [15].

Another way to realise a VDM specification is using code-generation. The idea is for the generated code to be a refinement of the specification, but which is not achieved through step-wise refinement, but rather in one step through code-generation translation rules. Code-generation aims to reduce the resources needed to realise the model as well as to avoid introducing problems in the implementation due to manual translation of model into code. However, current VDM code-generators do not make any guarantees about the correctness of the generated code, nor do they provide the necessary means to help check that the code meets the specification. Naturally, this casts doubt on the value of code-generation as a way to realise a VDM model, since the goal is to develop software that meets the specification.

In this report we improve code-generation of VDM models by allowing the generated code to be checked against the system properties described by the VDM contracts. This helps ensure that the generated code meets the VDM specification, and is achieved as described in this report.

Some DbC technologies are tailored to specify detailed designs of programming interfaces for a particular programming language [38]. An example of one such technology is the Java Modeling Language (JML) [6] – a formal specification language that uses DbC elements, written as specialized comments, to specify the behaviour of Java classes and interfaces. JML annotations can be analysed statically or checked dynamically using JML tools. Therefore, JML can be seen as a technology that serves to bridge the gap between an abstract system specification and its Java implementation.

In this report we attempt to bridge this gap even further by proposing a way to automatically translate a specification written in the Vienna Development Method Specification Language (VDM-SL) to a JML-annotated Java implementation. Current VDM code-generators either ignore or provide limited code-generation support for the contract-based elements and type con-

straints of VDM. Ideally we should be able to preserve the contracts and type constraints when the system specification is implemented, since (1) they serve to document the intention and properties of the system and (2) they can be used to check the system realisation for correctness. Ensuring that the contracts and type constraints, as originally specified in VDM, hold for the system implementation potentially requires many extra checks to be added to the code. Adding these checks to the code manually is tedious and prone to errors. Instead, these checks could be generated automatically. Representing contracts and type constraints in JML also has the advantage that these checks may be ignored by the Java compiler. This allows the system realisation to be executed without the overhead of checking the contracts and type constraints, if desired.

The two main contributions of our work are (1) a collection of semantics-preserving rules for translating a VDM-SL specification to a JML-annotated Java program and (2) an implementation of these rules as an extension to Overture’s [19, 30] VDM-to-Java code-generator [16].

The rules propose ways to translate the DbC elements of VDM-SL to JML annotations; these annotations are added to the Java code produced by Overture’s Java code-generator. The rules cover checking of preconditions, postconditions and invariants, but the translator also produces JML checks to ensure that no type constraints are violated across the translation. We present the rules one by one and demonstrate, using a case study model of an Automated Teller Machine (ATM), how the code-generator extension translates a VDM-SL specification to JML-annotated Java code.

Since the translation is not formally defined we have used the OpenJML [8] runtime assertion checker to validate our work — in particular by generating JML constructs supported by this tool. More specifically, the JML translator has been tested by running examples through the tool in order to validate each of the translation rules (see section 2.8 for more details).

Following this section, we describe DbC with VDM-SL and JML in section 2.2. We continue by presenting the implementation of the JML translator in section 2.3. Then we describe the rules used to translate a VDM-SL specification to a JML-annotated Java program in sections 2.5 to 2.7. Next, we assess the correctness of the translation in section 2.8. Finally we describe related work in section 2.9 and present future plans and conclude in section 2.10.

## 2.2 DbC with VDM-SL and JML

---

In this section we describe VDM-SL and JML. We cover different types and all the contract-based elements of VDM-SL, focusing specifically on the VDM-10 release, which we are targeting in our work. The JML constructs described in this section cover those that are used to implement the translation rules.

### 2.2.1 VDM-SL

VDM-SL is an ISO standardised sequential modelling language that supports description of data and functionality. The ISO standard has later been informally extended with modules to allow type definitions, values (constants) and functionality to be imported and exported between modules. A module may define a single state component, which can be constrained by a state invariant. State is modified by assigning a new value to a state designator, which can be either a name, a field reference or a map or sequence reference, as described in the VDM language reference manual [21].

Module state, if specified, implicitly defines a record type, which is tagged with the state name and also defines the type of the state component. The state type can be used like any other record



type explicitly defined by the modeller – the difference being that the state invariant [3] constrains the state type and thus every instance of this record type.

Data are defined by means of built-in basic types covering, for instance, numbers, booleans, quote types and characters. A quote type corresponds to an enumerated type in a language such as Pascal. The basic types can be used to form new structured data types using built-in type constructors that support creation of union types, tuple types and record types. A type may also be declared optional, which allows **nil** to be used to represent the absence of a value. For collections of values, VDM-SL supports sets, sequences and maps. The built-in data types, type constructors and collections can be used to form named user defined types, which can be constrained by invariants. We refer to these types as *named invariant types*. As an example, Listing 2.1 shows the definition of the named invariant type `Amount`, which is used to represent an amount of money deposited or withdrawn by an account holder. This type is defined based on natural numbers (excluding zero), i.e. the built-in basic type **nat1** in VDM-SL. For this particular example, we say that **nat1** is the *domain type* of `Amount`. We further constrain `Amount` using an invariant, by requiring a value of this type to be less than 2000. Specifically, for the invariant shown in Listing 2.1, the `a` on the left-hand side of the equality is a pattern that matches values of type `Amount`. This pattern is used to express the invariant predicate for this named invariant type.

```

1 types
2 Amount = nat1
3 inv a == a < 2000;
```

Listing 2.1: Example of a VDM-SL named invariant type.

### 2.2.1.1 Functional descriptions

In VDM, functionality can be defined in terms of functions and operations over data types with a traditional call-by-value semantics. Functions are referentially transparent and therefore they are not allowed to access or manipulate state directly, whereas operations are. Therefore, a function cannot call an operation.<sup>1</sup> In addition to accessing module state, operations may also use the **dcl** statement to declare local state designators which can be assigned to. Subsequently the term *functional description* will be used to refer to both functions and operations. As an example, a function that uses the `MATH`sqrt` library function to calculate the square root of a real number is shown in Listing 2.2.

```

1 sqrt : real -> real
2 sqrt (x) == MATH`sqrt (x)
3 pre x >= 0
4 post RESULT * RESULT = x;
```

Listing 2.2: VDM-SL function for calculating the square root of a number.

Functional descriptions can be implicitly defined in terms of pre- and postconditions, which specify conditions that must hold before and after invoking the functional description. Alternatively, a functional description can be *explicitly* defined by means of an algorithm, as shown in

<sup>1</sup>With the recent introduction of **pure** operations into VDM-10 (not to be confused with **pure** methods in JML) it has become possible to invoke operations, albeit **pure** ones, from a function. This feature was introduced to address issues with the object-oriented dialect of VDM, called VDM++, but was made available in every VDM-10 dialect (including VDM-SL).

Listing 2.2. The JML translator supports both implicitly and explicitly defined functional descriptions. However, only methods that originate from explicitly defined functional descriptions can be executed.

The precondition of a function can refer to all the arguments of the function it guards. The same applies to the postcondition of a function, which can also refer to the result of the execution using the reserved word **RESULT**. For the square root function in Listing 2.2 we require that the input is a positive number (the precondition), and that the square of the function result equals the input value (the postcondition).

Function definitions are derived for the pre- and postconditions of `sqrt` from `sqrt`'s **pre** and **post** clauses. These function definitions do not appear in the model, but they are used internally by the Overture interpreter to check for contract violations. However, to clarify, the pre- and postcondition functions of `sqrt` are shown in Listing 2.3. In this listing, `+>` specifies that `pre_sqrt` and `post_sqrt` are total functions, and not partial functions, which use the `->` type constructor.

```

1 pre_sqrt:real +> bool
2 pre_sqrt(x) == x >= 0;
3
4 post_sqrt:real*real +> bool
5 post_sqrt(x,RESULT) == RESULT * RESULT = x;
```

Listing 2.3: Pre- and postcondition functions for the `sqrt` function shown in Listing 2.2.

Similarly, the pre- and postcondition functions of an operation are also derived. To demonstrate this, consider the `inc` operation in Listing 2.4. This operation takes a real number as input, adds it to a counter (defined using a state designator), and returns the new counter value. In this listing `counter~` and `counter` refer to the counter values before and after the operation has been invoked, respectively.

```

1 inc : real ==> real
2 inc (i) == (
3   counter := counter + i;
4   return counter;
5 )
6 pre i > 0
7 post counter = counter~ + i and
8   RESULT = counter;
```

Listing 2.4: VDM-SL operation for incrementing a counter.

A precondition of an operation can refer to the state, `s`, before executing the operation, whereas the postcondition of an operation can read both the before and after states. State access is achieved by passing copies of the state to the pre- and postcondition functions. The corresponding pre- and postcondition functions for `inc` are shown in Listing 2.5 where the parameters `s~` and `s` of `post_inc` refer to the state (that contains the counter value) before and after execution of `inc`. We further use `S` to denote the record type that represents the module's state.

```

1 pre_inc:real*S +> bool
2 pre_inc(i,s) == i > 0;
3
4 post_inc:real*real*S*S +> bool
5 post_inc(i,RESULT,s~,s) ==
```

```

6 | s.counter = s~.counter + i and
7 | RESULT = s.counter;

```

Listing 2.5: Pre- and postcondition functions for the `inc` operation shown in Listing 2.4.

The function descriptions in Listing 2.5 assume that the pre- and postconditions are defined (using the **pre** and **post** clauses) and that the state of the module enclosing the functional description exists. For the cases where pre- and postconditions are not defined they can be thought of as functions that yield **true** for every input. Furthermore, when no state component is defined, the pre- and postcondition functions simply omit the state parameters. Similarly, when an operation does not return a result (it specifies `void` as the return type) the postcondition function omits the **RESULT** parameter.

For each type definition constrained by an invariant, such as `Amount` shown in Listing 2.1, a function is implicitly created to represent the invariant – see Listing 2.6. The Overture tool uses this function internally to check whether a value is consistent with respect to a given type (e.g. `Amount`) [23]. Note that since all invariants are functions they are not allowed to depend on state of other modules. Specifically, invariants can only invoke functions and access global constants (possibly defined in other modules).

```

1 | inv_Amount : Amount -> bool
2 | inv_Amount (a) == a < 2000;

```

Listing 2.6: Invariant function for type definition `Amount`.

### 2.2.1.2 Atomic execution

Multiple consecutive statements are sometimes needed to update the state designators to make them consistent with the system’s invariants. For example, assume that we have a system that uses two state designators called `evenID1` and `evenID2` to store even and different numbers. For this example, we will assume that these state designators are of type `Even` – a type that constrains these state designators to store even numbers. To help ensure that the uniqueness constraint (a state invariant) is not violated during an update, multiple assignments can be grouped in an **atomic** statement block as shown in Listing 2.7. Given the type `Even` of the state designators `evenID1` and `evenID2` it is as if the atomic statement is evaluated as shown in Listing 2.8.

```

1 | atomic (
2 |   evenID1 := exp1;
3 |   evenID2 := exp2;
4 | )

```

Listing 2.7: Atomic update in VDM.

```

1 | let t1 : Even = exp1,
2 |     t2 : Even = exp2
3 | in (
4 |   -- Turn off invariants
5 |   evenID1 := t1;
6 |   evenID2 := t2;
7 |   -- Turn on invariants
8 |   -- Check invariants hold

```

9 `);`Listing 2.8: The execution semantics of the **atomic** statement.

Executing the **atomic** statement block is semantically equivalent to first evaluating the right-hand sides of all the assignments before turning off invariant checks, and then binding the results to the corresponding state designators. After all the assignments have been executed, it must be ensured that all invariants hold.

There are three properties that follow from the evaluation semantics of the **atomic** statement block that are worth mentioning:

1. When evaluating the right-hand sides of the assignment statements, potential contract violations will be reported.
2. Temporary identifiers, used to store the right-hand side results, are explicitly typed and therefore violations of named invariant types for these variables will be reported. The explicit type annotations thus ensure that the right-hand side of a state designator assignment is checked to be consistent with the type of said state designator.
3. Assignment statements cannot see intermediate values of state designators.

## 2.2.2 JML

Although JML [24] is designed to specify arbitrary sequential Java programs, in this subsection we only describe the features needed for the translation from VDM-SL.

A method specified with the **pure** modifier in JML is not permitted to have write effects; such methods are allowed to be used in specifications. Pure methods are used to translate VDM-SL functions.

A class invariant in JML should hold whenever the non-helper methods of that class are not being executed; thus invariants must hold in each method's before and after states. However, a method declared with the **helper** annotation in a type *T* does not have its pre- and postconditions augmented with *T*'s invariants. Helper methods (and constructors) must either be pure or private [24], so that the invariant will hold at the beginning and end of all client-visible methods [28]. The before and after states of non-helper methods and constructors are said to be *visible states*; thus invariants must hold in all visible states. JML distinguishes between instance and static invariants. An *instance* invariant can refer to the non-static (i.e. instance) fields of an object. A *static* invariant cannot refer to an object's non-static fields; thus static invariants are used to specify properties of static fields.

An assertion can reference the invariant for an object explicitly using a predicate of the form `\invariant_for (e)`, which is equivalent to the invariant for *e*'s static type [24, section 12.4.22].

In JML pre- and postconditions are written using the keywords **requires** and **ensures**, respectively. In the specification of a postcondition, one writes `\old (e)` to refer to the before state value of an expression *e*. For example, an `increment` method that writes a field `count` could be specified as shown in Listing 2.9.

```

1 //@ requires count < Integer.MAX_VALUE;
2 //@ modifies count;
3 //@ ensures count == \old(count)+1;
4 void increment() {
5     count++;
6 }
```

Listing 2.9: Example of a JML specification for a Java method.

Method postconditions may also use the keyword `\result` to refer to the value returned by the method.

Specification expressions in JML can use Java expressions that are pure (have no write effects), and also some logical operators, such as implication `==>`, and quantifiers such as `\forall` and `\exists`.

In addition to method pre- and postconditions, one can also write assertions anywhere a Java statement can appear, using JML's `assert` keyword. Such assertions must hold whenever they are executed.

One way to specify the abstract state of a class is to use JML's `ghost` variables. Ghost variables are specification-only variables and fields of objects that can only be used in JML specifications and in JML `set` statements. A set statement is an assignment statement whose target is a ghost variable.

By default, JML variables and fields may not hold the `null` value. However, should one wish to specify that all fields of a class may hold `null`, then one can annotate the class's declaration with `nullable_by_default`.

## 2.3 The implementation of the JML translator

The JML translator is implemented as an extension to Overture's VDM-SL-to-Java code-generator, which provides code-generation support for a large executable subset of VDM. This section describes how the JML translator has been implemented, and explains the details of the Java code-generator that are needed in order to understand how the JML translator works.

### 2.3.1 The implementation

The Java code-generator is developed using Overture's code-generation platform – a framework for constructing code-generators for VDM [16]. This platform is used by the Java code-generator to parse the VDM-SL model sources and to construct an Intermediate Representation (IR) of the model – an Abstract Syntax Tree (AST) that constitutes an internal representation of the generated code. The Java code-generator uses the code-generation platform to *transform* the IR into a tree structure that eventually is translated directly into Java code. The translation of the IR into Java is handled by the code-generation platform's code emission framework, which uses the Apache Velocity template engine [4].

The Java code-generator exposes the IR during the code-generation process, which allows the JML translator to intercept the code-generation process and further transform the IR. These additional transformations are used to decorate the IR with nodes that contain the JML annotations. Using the code emission framework, the final version of the IR is translated into a JML-annotated Java program.

The JML translator is publicly available in Overture version 2.3.8 (as of July 2016) onwards [30]. Furthermore, the JML translator's source code is available via the Overture tool's open-source code repository [31].

### 2.3.2 Overview of the translation

In the generated code, a module is represented using a **final** Java class with a **private** constructor, since VDM-SL does not support inheritance and a module cannot be instantiated. Due to the latter, both operations and functions are code-generated as **static** Java methods.

Module state is represented using a **static** class field in the module class to ensure that only a single state component exists at any given time. The state component is represented using a record value, and as a consequence, an additional record type is generated to represent it.

Each variable in VDM-SL is passed by value, i.e. as a *deep copy*, when it is passed as an argument, appears on the right-hand side of an assignment or is returned as a result. As a consequence, aliasing can never occur in a VDM-SL model. Types are different in Java, where objects are modified via object references or pointers. Therefore different object references can be used to modify the same object. To avoid such aliasing in the generated code, data types are code-generated with functionality to support value type behaviour.

Every record definition code-generates to a class definition with accessor methods for reading and manipulating the fields. This class implements `equals` and `copy` methods to support comparison based on structural equivalence and deep copying, respectively. In this way the call-by-value semantics of VDM-SL can be preserved in the generated code by invoking the `copy` method, which helps to prevent aliasing. Similarly the `equals` method can be invoked to compare code-generated records based on structural equivalence rather than comparing addresses of object references. A record object can then be obtained by invoking the constructor of the record class or by invoking the `copy` method of an existing record object.

Java does not support the definition of aliases of existing types, such as the `Amount` named invariant type in Listing 2.1. Therefore, the Java code-generator chooses not to code-generate class definitions for these types. Instead, a use of a named invariant type is replaced with its domain type (described in subsection 2.2.1). Since the named invariant type is an alias of an existing type this is fine, as long as we make sure to check that the type invariant holds.

To assist the translation of VDM to Java, the existing Java code-generator uses a runtime library, which among other things, includes Java implementations for some of the different VDM types and operators. The `Tuple` class, for example, is used to represent tuple types and enables construction of tuple values. Sets, sequences and maps are represented using the `VDMSet`, `VDMSeq` and `VDMMap` classes, which themselves are based on Java collections, and so on. The runtime library's collection classes are used as raw types (e.g. `VDMSet`) in the generated code, and therefore they are never passed a generic type argument. Raw types provide a convenient way to represent VDM collections that store elements of some union type – a kind of type that Java does not support.

In addition to using the existing runtime library, the JML translator also contributes a small runtime library to aid the generation of JML checks. This runtime library, which we subsequently refer to as `V2J`, is an extension of the existing Java code-generator runtime library. As we shall see in subsection 2.6.6, the `V2J` runtime is mostly used in the generated JML checks to ensure that instances of collections respect the VDM types that produce them.

## 2.4 Case study example

---

Throughout the report we will demonstrate the translation rules using a case study model of an ATM. The model consists of a single module, `ATM` (shown in Listing 2.10), which uses a state definition to record information about

- The debit cards considered valid by the system (named `validCards`).
- The debit card currently inserted into the ATM, if any (`currentCard`).
- If a valid PIN code has been entered (`pinOk`) for the debit card currently inserted into the ATM and,
- all the bank accounts known to the system (`accounts`).

```

1 module ATM
2 definitions
3 state St of
4   validCards : set of Card
5   currentCard : [Card]
6   pinOk : bool
7   accounts : map AccountId to Account
8   init St == St = mk_St({},nil,false,{|->})
9   inv mk_St(v,c,p,a) ==
10     (p or c <> nil => c in set v)
11   and
12   forall id1, id2 in set dom a &
13     id1 <> id2 =>
14       a(id1).cards inter a(id2).cards = {}
15 end
16 ...
17 operations
18 GetStatus : () ==> bool * seq of char
19 GetStatus () == ...
20
21 OpenAccount : set of Card * AccountId ==> ()
22 OpenAccount (cards,id) == ...
23
24 AddCard : Card ==> ()
25 AddCard (c) == ...
26
27 RemoveCard : Card ==> ()
28 RemoveCard (c) == ...
29
30 InsertCard : Card ==>
31   <Accept>|<Busy>|<Reject>
32 InsertCard (c) == ...
33
34 EnterPin : Pin ==> ()
35 EnterPin (pin) == ...
36
37 ReturnCard : () ==> ()
38 ReturnCard () == ...
39
40 Withdraw : AccountId * Amount ==> real
41 Withdraw (id, amount) == ...
42
43 Deposit : AccountId * Amount ==> real
44 Deposit (id, amount) == ...
45 end

```

Listing 2.10: VDM-SL module representing an ATM.

For simplicity, Listing 2.10 omits type definitions and only shows the state definition (including the state invariant) and the signatures for some of the operations. The state invariant, shown in Listing 2.10, requires that at all times the following two conditions must be met: a debit card must at most be associated with a single account and secondly, for a PIN code to be considered valid, the debit card currently inserted into the ATM must itself be a valid debit card.

When the ATM model is translated to a JML-annotated Java program it can be checked for correctness using JML tools. To demonstrate this, consider the example in Listing 2.11, which creates a debit card, inserts it into the ATM, and performs a transaction scenario.

```

1 Card c = new Card(5,1234);
2 // atm.ATM.AddCard(c); (missing statement)
3 atm.ATM.InsertCard(c);
4 atm.ATM.EnterPin(1234);
5 System.out.println(atm.ATM.GetStatus());
6 /* Transaction related code omitted */
7 atm.ATM.ReturnCard();

```

Listing 2.11: Java code demonstrating use of the implementation of the ATM model.

If this program is executed using the OpenJML runtime assertion checker the output in Listing 2.12 is reported.

```

Exception in thread "main" java.lang.AssertionError: Main.java:12: JML
    precondition is false
        atm.ATM.EnterPin(1234);
            ^
atm/ATM.java:276: Associated declaration: Main.java:12:
    //@ requires pre_EnterPin(pin,St);
        ^
    at Main.main(Main.java:17)

```

Listing 2.12: Inconsistent use of the system detected using the OpenJML runtime assertion checker.

For this particular example, this error is reported because the debit card `c` is not recognised as a valid debit card by the system. Specifically, the scenario did not invoke `atm.ATM.AddCard(c)` immediately after creating the debit card. The return value of the `Insert` method did indicate that the debit card was rejected, but this value was mistakenly discarded in Listing 2.11. The error is reported by the runtime assertion checker because entering a PIN code when no debit card is inserted into the ATM is considered an error. After changing the example in Listing 2.11 to add `c` as a valid debit card, no problems are detected by the runtime assertion checker, as expected. Therefore, the code executes as if it was compiled using a standard Java compiler and executed on a regular Java virtual machine. More, specifically, the system will report the status as shown in Listing 2.13 to indicate that the ATM is not awaiting a debit card, and that a transaction is in progress.

```
mk_(false, "transaction in progress.")
```

Listing 2.13: System output after fixing the problem in Listing 2.11.

As we proceed, in section 2.5 and section 2.6 we elaborate on the specifics of each VDM definition in the case study model and demonstrate the translation to JML-annotated Java.

## 2.5 Translating VDM-SL contracts to JML



In this section we present the rules used to translate the DbC elements of VDM-SL to JML annotations that are added to the generated Java code. For each of the elements, we describe the approach used to translate the element to JML. This is afterwards generalised as a rule, which appears in a grey box.

### 2.5.1 Allowing null values by default

Overture's Java code-generator may sometimes introduce auxiliary variables that are initialised to **null** when it code-generates some of the constructs of VDM. To avoid having errors reported when checking the generated code with a JML tool, we allow **null** as a legal value by default for all references in the generated code.

#### 1. Allowing null values by default

Annotate every class output by the Java code-generator with the **nullable\_by\_default** modifier to allow all references to use **null** as a legal value.

As a consequence we also have to guard against **null** values for variables that originate from VDM variables or patterns<sup>2</sup> that do not allow **nil**.

### 2.5.2 Translating functional descriptions to JML

Recall that a VDM-SL function code-generates to a **static** Java method. In addition, a VDM-SL function does not have side-effects and therefore the code-generated version of the method can be annotated as JML **pure**.

#### 2. Translation of functions

Any function – whether it is defined by the user or derived, e.g. from a **pre** or **post** condition clause – code-generates to a **static** Java method that is annotated with the **pure** modifier.

Operations, on the other hand, can read and manipulate the state of the enclosing module, or invoke other operations that may have side-effects. Therefore, the method that the operation code-generates to cannot be annotated as JML **pure**.

When a VDM-SL definition (e.g. a functional description) is code-generated to Java, the visibility of the corresponding Java definition can, in principle, be set according to whether the VDM-SL definition is exported (**public**) or not (**private**). In the presentation of the translation rules following this section, we omit explicit use of access specifiers in the rule formulation as we do not consider it crucial to our work.

### 2.5.3 Translating preconditions to JML

In terms of semantics there is no difference between a precondition in VDM-SL and JML. There are, however, interesting issues worth mentioning regarding how the JML translator implements the translation. We start by covering preconditions of operations, and we end this subsection by describing how they differ from those of functions. As an example of how a VDM-SL precondition is translated, consider the operation in Listing 2.14. This operation models withdrawal from a bank account identified by the parameter **id**.

<sup>2</sup>The generated code uses variables to represent the patterns (record pattern, tuple pattern, identifier pattern etc.) introduced by use of pattern matching in VDM.

```

1 Withdraw : AccountId * Amount ==> real
2 Withdraw (id, amount) ==
3 let newBalance =
4   accounts(id).balance - amount
5 in (
6   accounts(id).balance := newBalance;
7   return newBalance;
8 )
9 pre
10 currentCard in set validCards and pinOk and
11 currentCard in set accounts(id).cards and
12 id in set dom accounts

```

Listing 2.14: VDM-SL operation for bank account withdrawal guarded by a precondition.

In order to withdraw money from the account, we require that a valid card has been inserted, the PIN code is accepted, and that the bank account exists. Note that since `currentCard` is of the optional type `[Card]` it can be `nil`, which is not a valid member of `validCards`. Therefore, the precondition is **false** when no debit card has been inserted into the ATM. The `pre_Withdraw` function, which is not a visible part of the model, is derived from the **pre** clause of the `Withdraw` operation. In the generated code this function is represented using a **pure** method according to rule 2 – see Listing 2.15. Note that for the method in Listing 2.15, the Java code-generator uses extra variables to perform the equivalent VDM computation. These extra variables are also type checked using JML (although they are only used to store intermediate results).

The `Withdraw` operation is translated to the method shown in Listing 2.16. This method introduces several JML assertions that will be described in section 2.6. Note that the method `pre_Withdraw` is invoked from the **requires** clause of the `Withdraw` method to check whether the precondition is met. In addition to the input parameters of the `Withdraw` method, the `pre_Withdraw` method is also passed the state `St`.

### 3. Translating the precondition of an operation

Let `op` be a method code-generated from a VDM-SL user-defined operation and let the signature of `op` be:

```
static R op(I1 i1, ..., In in)
```

Then `op` has a code-generated precondition method `pre_op` that is **pure** and which in addition to the parameters of `op` also takes the state component `s` as an argument, i.e.

```
/*@ pure @*/ static boolean
```

```
pre_op(I1 i1, ..., In in, S s)
```

To ensure that the precondition is evaluated, we annotate `op` with the following **requires** annotation:

```
/*@ requires pre_op(i1, ..., in, s);
```

Rule 3 assumes the existence of a state component `s`. However, when the state of the module enclosing `op` is not defined, rule 3 changes to not include the state parameter in the definition of `pre_op`.

The example above considers the case where the precondition is guarding an operation (i.e. `Withdraw`). As described in section 2.2, a precondition is defined differently for a function than it is for an operation. In particular, the precondition of a function is not passed the state, so neither is the code-generated version of it. We also note that the visibility of the precondition function

```

1  /*@ pure @*/
2  public static Boolean pre_Withdraw(
3      final Number id, final Number amount, final atm.ATMtypes.St St) {
4      /*@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
5       /*@ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
6       /*@ assert Utils.is_(St, atm.ATMtypes.St.class);
7      Boolean andResult_3 = false;
8      /*@ assert Utils.is_bool(andResult_3);
9      if (SetUtil.inSet(St.get_currentCard(), St.get_validCards())) {
10         Boolean andResult_4 = false;
11         /*@ assert Utils.is_bool(andResult_4);
12         if (St.get_pinOk()) {
13             Boolean andResult_5 = false;
14             /*@ assert Utils.is_bool(andResult_5);
15             if (SetUtil.inSet(St.get_currentCard(),
16                 ((atm.ATMtypes.Account) Utils.get(St.accounts, id)).get_cards()))
17                 {
18                 if (SetUtil.inSet(id, MapUtil.dom(St.get_accounts()))) {
19                     andResult_5 = true;
20                     /*@ assert Utils.is_bool(andResult_5);
21                 }
22             }
23             if (andResult_5) {
24                 andResult_4 = true;
25                 /*@ assert Utils.is_bool(andResult_4);
26             }
27         }
28         if (andResult_4) {
29             andResult_3 = true;
30             /*@ assert Utils.is_bool(andResult_3);
31         }
32     }
33     Boolean ret_29 = andResult_3;
34     /*@ assert Utils.is_bool(ret_29);
35     return ret_29;
36 }

```

Listing 2.15: Code-generated version of the `pre_Withdraw` operation.

must be the same as that of the functional description it guards. Otherwise it cannot be invoked from the corresponding **requires** clause.

#### 4. Translating the precondition of a function

Let  $f$  be a method code-generated from a VDM-SL user-defined function and let the signature of  $f$  be:

**static**  $R$   $f(I_1\ i_1, \dots, I_n\ i_n)$

Then  $f$  has a code-generated precondition method `pre_f` that is **pure** and which accepts the same parameters as  $f$ , i.e.

**/\*@ pure @\*/ static boolean**

`pre_f(I_1 i_1, ..., I_n i_n)`

To ensure that the precondition is evaluated, we annotate  $f$  with the following **requires** annotation:

**/\*@ requires** `pre_f(i_1, ..., i_n);`

```

1  //@ requires pre-Withdraw(id,amount,St);
2  public static Number Withdraw(final Number id, final Number amount) {
3  //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
4  //@ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
5  final Number newBalance =
6      ((atm.ATMtypes.Account) Utils.get(St.accounts, id)).get_balance().
        doubleValue()
7      - amount.longValue();
8  //@ assert Utils.is_real(newBalance);
9  {
10     VDMMap stateDes_1 = St.get_accounts();
11     atm.ATMtypes.Account stateDes_2 = ((atm.ATMtypes.Account) Utils.get(
        stateDes_1, id));
12     //@ assert stateDes_2 != null;
13     stateDes_2.set_balance(newBalance);
14     //@ assert (V2J.isMap(stateDes_1) && (\forall int i; 0 <= i && i < V2J.
        size(stateDes_1); (Utils.is_nat(V2J.getDom(stateDes_1,i)) &&
        inv_ATM_AccountId(V2J.getDom(stateDes_1,i)) && Utils.is_(V2J.getRng(
        stateDes_1,i),atm.ATMtypes.Account.class)));
15     //@ assert Utils.is_(St,atm.ATMtypes.St.class);
16     //@ assert \invariant_for(St);
17     Number ret_7 = newBalance;
18     //@ assert Utils.is_real(ret_7);
19     return ret_7;
20 }
21 }

```

Listing 2.16: Code-generated version of the `Withdraw` operation.

## 2.5.4 Translating postconditions to JML

Postconditions in VDM-SL and JML are semantically similar, although VDM-SL represents the postcondition function as a derived function definition (as was done for preconditions). Furthermore, in VDM and JML postconditions of operations and methods, respectively, can access both the before and after states. Returning to the `Withdraw` operation, one could specify a postcondition requiring that exactly the value specified by the `amount` parameter is withdrawn from the account – see Listing 2.17.

```

1  Withdraw : AccountId * Amount ==> real
2  Withdraw (id, amount) == ...
3  post
4  let accountPre = accounts~(id),
5      accountPost = accounts(id)
6  in
7      accountPre.balance =
8      accountPost.balance + amount and
9      accountPost.balance = RESULT;

```

Listing 2.17: The `Withdraw` operation guarded by a postcondition.

The JML translator produces a **pure** Java method to represent the postcondition function. This Java method is invoked from the **ensures** clause to check that the postcondition holds. The invocation of the postcondition method of the `Withdraw` operation is shown in Listing 2.18.

```

1  //@ requires pre-Withdraw(id,amount,St);
2  //@ ensures post-Withdraw(id,amount,\result,\old(St.copy()),St);

```

```
3 public static Number Withdraw(final Number id, final Number amount) {...}
```

Listing 2.18: Code-generated version of the `Withdraw` operation.

Note in particular how the before and after states are passed to the `post_Withdraw` method. Reasoning about before state is achieved using JML's `\old` expression. For the `Withdraw` operation the before state is constructed as `\old(St.copy())`. Since `St.copy()` is a deep copy of the state (as explained in section 2.3) the evaluation inside the `\old` expression ensures that the result indeed is a representation of the before state.

The JML translator deep copies the state because Java represents every composite data type using a class. So without deep copying the state, only the address of the before state object reference is copied. In effect, only a single object would exist to represent the pre- and post states. This would never work, since state changes made by the operation would affect what was intended to be a representation of the before state. Therefore, the state is deep copied to get a separate object to represent the before state.

### 5. Translating the postcondition of an operation

Let `op` be a method code-generated from a VDM-SL user-defined operation and let the signature of `op` be:

```
static R op(I1 i1, ..., In in)
```

Then `op` has a code-generated postcondition method `post_op` that is **pure** and which in addition to the parameters of `op`, also takes the result and the before and after states of `op` as arguments, i.e.

```
/*@ pure @*/ static boolean
```

```
post_op(I1 i1, ..., In in,  
        R RESULT, S _s, S s)
```

To ensure that the postcondition is evaluated we annotate `op` with the following **ensures** annotation:

```
//@ ensures post_op(i1, ..., in, \result,  
                    \old(s.copy()), s);
```

While the primary concern is to preserve the behaviour of the specification across the translation, deep copying values may significantly affect system performance in a negative way. In particular, because it is difficult (in general) to avoid deep copying values unnecessarily when they are passed around in the generated code. To address this issue, the Java code-generator (and hence the JML translator) offers an option that, when selected by the user, omits deep copying of values (other than the old state). While the purpose of this is to generate performance-efficient code, this option is, however, only safe to use if Java objects that originate from VDM-SL values are not modified via aliases.

Yi et al. identify and address a number of problems with the `\old` expression [40]. In particular, the authors of that work conduct experiments showing that passing deep copies of the old state may drastically increase a system's memory usage. To address this, Yi et al. propose the `\past` expression as a more memory-efficient alternative to the `\old` expression. Yi et al. further show that the `\past` expression can be implemented as an extension of the OpenJML runtime assertion checker by means of aspect-oriented programming principles. However, OpenJML does not officially support the `\past` expression yet, which is why the translation rules do not currently rely on this expression. As we see it, the ideas proposed by Yi et al. could potentially support the development of a more performance-efficient way to handle old states in the JML translator.

Similar to rule 3, rule 5 also assumes that the state of the module enclosing `op` exists. If the state component does not exist, rule 5 changes to not include the state parameters in the definition

of `post_op`. Furthermore, if `op` does not return a result (the return type is `void`), then the definition of `post_op` does not include the `RESULT` parameter.

The example above considers the postcondition of an operation (i.e. `Withdraw`). As described in section 2.2, the postcondition of a function is not allowed to access state. Therefore, the code-generated version of the postcondition function is not passed the state.

### 6. Translating the postcondition of a function

Let `f` be a method code-generated from a VDM-SL user-defined function and let the signature of `f` be:

```
static R f(I1 i1, ..., In in)
```

Then `f` has a code-generated postcondition method `post_f` that is **pure** and which in addition to the parameters of `f` also takes the result of `f` as an argument, i.e.

```
/*@ pure @*/ static boolean
```

```
post_f(I1 i1, ..., In in, R RESULT)
```

To ensure that the postcondition is evaluated we annotate `f` with the following **ensures** annotation:

```
/*@ ensures post_f(i1, ..., in, \result);
```

## 2.5.5 Translating record invariants to JML

A record can, like any other type definition in VDM-SL, be constrained by an invariant. As an example, Listing 2.19 shows a record definition modelling a bank account.

```
1 Account ::
2   cards : set of Card
3   balance : real
4   inv a == a.balance >= -1000;
```

Listing 2.19: A VDM-SL record definition modelling a bank account.

An `Account` comprises the available balance as well as the debit cards associated with the account. We further constrain an `Account` to not have a balance of less than -1000, which is expressed using an invariant.

As described in section 2.3, a record definition is translated to a class that emulates the behaviour of a value type using `copy` and `equals` methods.

Since a record invariant is required to hold for every record value, or object instance in the generated code, we represent it using an **instance invariant** in JML as shown in Listing 2.20. Note that the **instance invariant** is formulated as an implication such that invariant violations are not reported when invariant checks are disabled. As we shall see in subsection 2.5.6 this has to do with the way VDM-SL handles atomic execution.

The code-generated record `Account` defines an *invariant method* `inv_Account` that takes all the record fields of `Account` as input and evaluates the invariant predicate. This method is invoked directly from the JML invariant, as shown in Listing 2.20. Note that `inv_Account` is a **static** method according to rule 2. In addition, this method is annotated as a **helper** to avoid the invariant check triggering another invariant check, which eventually would cause a stack-overflow.

```

1  //@ nullable_by_default
2  final public class Account implements Record
3  {
4      public VDMSet cards;
5      public Number balance;
6      //@ public instance invariant atm.ATM.invChecksOn ==> inv_Account(cards,
          balance);
7      ...
8      /*@ pure @*/
9      public boolean equals(final Object obj)
10     {...}
11     /*@ pure @*/
12     public atm.ATMtypes.Account copy(){...}
13     /*@ pure @*/
14     public VDMSet get_cards() {...}
15     public void set_cards(final VDMSet _cards)
16     {...}
17     /*@ pure @*/
18     public Number get_balance() {...}
19     public void set_balance(final Number _balance) {...}
20     /*@ pure @*/
21     /*@ helper @*/
22     public static Boolean inv_Account(final VDMSet _cards, final Number
          _balance){
23         return _balance.doubleValue() >= -1000L;
24     }
25 }

```

Listing 2.20: Code-generated version of the Account record.

## 7. Translating a record invariant

Let  $D$  be a code-generated record definition with fields  $f_1, \dots, f_n$  of types  $F_1, \dots, F_n$ , respectively, and let  $D$  be constrained by an invariant. Then  $D$  has an invariant method  $\text{inv\_D}$  that is annotated as a **helper** to allow it to be invoked from the invariant clause of  $D$ . The invariant method can also be annotated as **pure** since it originates from a function definition. The annotated signature of  $\text{inv\_D}$  thus becomes:

```

/*@ pure @*/
/*@ helper @*/
boolean inv_D( $F_1$   $f_1, \dots, F_n$   $f_n$ )

```

Let further  $\text{invChecksOn}$  be a variable that is true if invariant checking is enabled and false otherwise. To represent the record invariant of  $D$  we annotate  $D$  with the **invariant** annotation:

```

/*@ public instance invariant
invChecksOn ==> inv_D( $f_1, \dots, f_n$ ); @*/

```

As we shall later see in subsection 2.5.6, atomic execution sometimes requires extra assertions to be inserted into the generated code in order to guarantee that the record invariant semantics of VDM-SL are preserved.

All the methods inside a record class – except for the constructor and the “setter” methods – do not modify the state of the record class and therefore they are marked as **pure**. Updates to a record object in the generated code are made using the “setter” methods of the generated record class, or by using the record modification expression [21]. Use of “setter” methods instead of

direct field access to manipulate the state of a record (which is how field access is achieved in VDM-SL) forces the record object into a *visible state* (as described in subsection 2.2.2) after it has been updated, thus triggering the invariant check according to the VDM-SL semantics. For example, in VDM-SL we could set the balance of an account as shown in Listing 2.21.

```
acc.balance := newBalance;
```

Listing 2.21: Updating the `Account` balance in VDM-SL.

This assignment produces the Java code shown in Listing 2.22. Note that for this particular case there is no need to generate any additional JML assertions since the state of `acc` becomes visible after the call to `set_balance`. This causes the invariant check of `Account` to trigger.

```
acc.set_balance(newBalance);
```

Listing 2.22: Updating the `Account` balance in the generated code.

## 2.5.6 Atomic execution

There are situations where multiple assignment statements in VDM-SL need to be evaluated atomically in order to avoid unintentional violation of a state invariant. In our example, this is the case when the ATM returns the card to the owner, which is done as the last step of a transaction. Returning the debit card also requires us to invalidate the PIN code currently entered. These two things have to be done atomically to avoid violating the state invariant of the ATM module, which is checked using the `inv_St` function, derived from the state invariant shown in Listing 2.10 in section 2.4. Therefore the body of the `ReturnCard` operation is executed inside an **atomic** statement block as shown in Listing 2.23. Note that the invariant is evaluated internally by the interpreter, and therefore the example in Listing 2.23 makes no explicit mention of the invariant.

```
1 ReturnCard : () ==> ()
2 ReturnCard () ==
3 atomic (
4   currentCard := nil;
5   pinOk := false;
6 )
7 pre currentCard <> nil
8 post currentCard = nil and not pinOk;
```

Listing 2.23: Removal of the debit card from the ATM in VDM-SL.

JML does not include a syntactic construct similar to that of the **atomic** statement. Instead atomic execution must be achieved using different means – for example by manipulating state directly using field access or **helper** methods.

To be consistent with the way record state is updated, and to reflect the way that VDM-SL handles atomic execution, we believe a better approach is to use a flag that indicates if invariant checks are enabled or not. Since this flag should not affect the generated code, we make it a **ghost** field such that it is only visible at the specification level. Since this **ghost** field must be accessible everywhere in the translation, we make it a static field of the class, as shown in Listing 2.24. The **ghost** field must be added to one of the generated Java classes since Java does not really have global variables. Note that this flag does not affect pre- and postconditions since these checks must always be evaluated.



```
1 /*@ public ghost static boolean invChecksOn = true; @*/
```

Listing 2.24: Ghost field used to control invariant checking.

The declaration of `invChecksOn` allows us to formulate invariants such that violations are reported only if invariant checking is enabled. An example of this is shown in Listing 2.25 for the record state class of the ATM module.

```
1 /*@ public instance invariant atm.ATM.invChecksOn ==> inv_St(validCards,
   currentCard, pinOk, accounts);
```

Listing 2.25: The invariant of the record state class.

The `invChecksOn` flag provides the means to emulate the behaviour of atomic execution in a Java environment as shown in Listing 2.26. Specifically, the JML **set** statement is used to disable/enable invariant checking before/after executing the body of the `ReturnCard` method.

```
1 /*@ requires pre_ReturnCard(St);
2    //@ ensures post_ReturnCard(\old(St.copy()), St);
3 public static void ReturnCard() {
4   atm.ATMtypes.Card atomicTmp_1 = null;
5   //@ assert ((atomicTmp_1 == null) || Utils.is_(atomicTmp_1, atm.ATMtypes.
6     Card.class));
7   Boolean atomicTmp_2 = false;
8   //@ assert Utils.is_bool(atomicTmp_2);
9   { /* Start of atomic statement */
10    //@ set invChecksOn = false;
11    //@ assert St != null;
12    St.set_currentCard(Utils.copy(atomicTmp_1));
13    //@ assert St != null;
14    St.set_pinOk(atomicTmp_2);
15    //@ set invChecksOn = true;
16    //@ assert \invariant_for(St);
17  } /* End of atomic statement */
18 }
```

Listing 2.26: Code-generated version of the `ReturnCard` operation.

## 8. Enabling and disabling invariant checking

Declare in a code-generated module `M` a globally accessible JML **ghost** field `invChecksOn` to control invariant checking:

```
/*@ public ghost static
boolean invChecksOn = true; @*/
```

Before executing a code-generated atomic statement (in any of the code-generated modules) invariant checking is disabled using the following JML **set** statement:

```
/*@ set M.invChecksOn = false;
```

After the code-generated atomic block has finished executing invariant checking is re-enabled using:

```
/*@ set M.invChecksOn = true;
```

When all the statements have been executed it must be ensured that no invariants have been violated. For the example in Listing 2.26, the only thing that needs to be checked is that the state component of the ATM class, i.e. `St` does not violate its invariant. This is checked by asserting that `\invariant_for(St)` holds.

### 9. Resuming invariant checking

Let  $d_1, \dots, d_n$  be state designators of records that have been updated, or affected by an update, during execution of a code-generated atomic statement block. Further assume that  $d_1, \dots, d_n$  have been updated in the given order, i.e.  $d_i$  was updated (for the first time) before  $d_{i+1}$  and that  $d_i$  may be of one of  $m_i$  record types  $D_{i1}, \dots, D_{im_i}$ . Immediately after executing the code-generated atomic statement block, it is checked that the state designators  $d_1, \dots, d_n$  do not violate any invariants using the following sequence of **assert** statements:

```
//@ assert  $d_1$  instance of  $D_{11}$  ==>
  \invariant_for( ( $D_{11}$ )  $d_1$  );
...
//@ assert  $d_1$  instance of  $D_{1m_1}$  ==>
  \invariant_for( ( $D_{1m_1}$ )  $d_1$  );
...
//@ assert  $d_n$  instance of  $D_{n1}$  ==>
  \invariant_for( ( $D_{n1}$ )  $d_n$  );
...
//@ assert  $d_n$  instance of  $D_{nm_n}$  ==>
  \invariant_for( ( $D_{nm_n}$ )  $d_n$  );
```

The **\invariant\_for** construct is not currently implemented in OpenJML. Instead this check can be inlined as a method call (rather than explicitly using **\invariant\_for**). However, throughout this report we use **\invariant\_for** to check record invariants as we believe it makes the examples easier to understand.

The JML translator keeps track of state designators of records that potentially have been updated as part of executing the code-generated atomic statement block. This is done by analysing the left-hand sides of the assignment statements. Immediately after invariant checking is re-enabled, i.e. the code-generated atomic statement block has finished execution, it is checked that no record violates its invariant.

There are a few things related to rule 9 that are worth clarifying. First, for assignments to composite state designators such as  $a.b.c := 42$ , the invariants of the individual state designators  $a$ ,  $b$  and  $c$ , have to be checked, if these are defined. For this particular example we say that  $c$  was updated, and that  $a$  and  $b$  were affected by the update. Second, the order in which the invariants are checked follows that used by the Overture VDM interpreter. Third, regardless of how many times a state designator is updated, the corresponding invariant is only checked once (for each state designator) since this is how atomic execution works in VDM, i.e. the update(s) are performed atomically, and afterwards the constraints that the state designators are subjected to are checked. Fourth, rule 9 includes all the state designators that have been updated or affected by an update. No particularly complex situations can arise that makes it difficult to identify these state designators since all VDM-SL's data types use call-by-value semantics, and therefore no aliasing can occur. Essentially this means that for the assignment statement  $a.b.c := 42$ , the only invariants (if defined) that have to be checked are those of the state designators  $a$ ,  $b$  and  $c$  since aliases do not exist. Therefore, the JML translator can determine (using static analysis) that assertions only have to be generated for these state designators. Naturally this simplifies the translation process, since the JML translator does not have to identify additional state designators (other than those that appear on the left-hand side of the assignment) that are affected by the assignment.

A state designator can be “masked” as a union type and in such situations it cannot always be statically determined what the runtime type of a state designator will be. To demonstrate this,

consider the record types  $R1$  and  $R2$  and a state designator declared as **decl**  $r : R1 \mid R2 := \dots$ . Further assume that  $R1$  and  $R2$  code-generate to classes  $R1_c$  and  $R2_c$ . After updating  $r$  atomically in the generated code, it is ensured that `\invariant_for(( $R1_c$ )  $r$ )` holds if  $r$  is of type  $R1_c$ , and similarly that the equivalent condition is true if  $r$  is of type  $R2_c$ . Since rule 9 has to take all possible types into account, the invariant checks are formulated as implications.

Although the VDM type system allows state designators to be “masked” as union types, most of the time it is possible to statically determine the runtime type of a state designator. For example, in Listing 2.26 no **instanceof** check is needed since the static type of the state component is  $St$ . This is an example where the JML translator simplifies the checks proposed by rule 9.

There are more aspects to rule 9 worth discussing – especially when state designators are based on arbitrarily complex data structures such as nested records. These will be addressed in subsection 2.7.1.

### 2.5.7 Translating module state to JML

As described in subsection 2.2.1, a module state invariant constrains the record type used to represent the state component of the enclosing module. Therefore, a module state invariant can essentially be seen as a record invariant that can be translated into JML-annotated Java without introducing additional translation rules. This subsection instead explains how a VDM-SL state definition is translated into a form that allows the rules related to record invariants to be applied (see subsection 2.5.5).

In our example each account can be accessed from an ATM using one of the debit cards associated with it. In addition to the bank accounts, the state of the ATM also keeps track of the debit cards that the system considers valid, the debit card that is currently inserted into the ATM, and whether the PIN code entered by the user is valid. The state (including the state invariant) as specified in VDM-SL is shown in Listing 2.10 and described in section 2.4. Based on the state definition, a record class is generated that represents the state type as shown in Listing 2.27. Recall that the fields in this class are nullable according to rule 1.

```

1 final public class St implements Record {
2   public VDMSet validCards;
3   public atm.ATMtypes.Card currentCard;
4   public Boolean pinOk;
5   public VDMMap accounts;
6
7   //@ public instance invariant atm.ATM.invChecksOn ==> inv_St(validCards,
8     currentCard, pinOk, accounts);
9   /* Record methods omitted */
}
```

Listing 2.27: The record class used to represent the state type.

In addition, an instance of the record class is created to represent the state component as shown in Listing 2.28. The state component is annotated with the **spec\_public** modifier so that it can be referred to from the **requires** and **ensures** clauses of **public** methods. Also note that the module is not constrained by an invariant. This is handled entirely by the record invariant shown in Listing 2.27.

```

1 final public class ATM {
2   /* Fields omitted */
3
4   /*@ spec_public @*/
5   private static atm.ATMtypes.St St = new atm.ATMtypes.St(SetUtil.set(),
6     null, false, MapUtil.map());
}
```

```

7  /* Module methods omitted */
8  }

```

Listing 2.28: The state component in the ATM module.

### 10. Translating the state component

Annotate state components of module classes with the **spec\_public** modifier to ensure that the state components can be referred to from the **requires** and **ensures** clauses of **public** methods.

## 2.6 Checking VDM types using JML

In this section we describe how the translator uses JML to check the consistency of VDM types when they are code-generated.

Throughout this section we construct a function called  $\text{Is}(v, T)$  that takes as input a Java value  $v$  and a VDM type  $T$  and produces a JML expression that can be used to check whether  $v$  represents a value of type  $T$ . We use  $\text{Is}(v, T)$  to check whether a Java value remains consistent with the VDM type that produces it. The check produced by  $\text{Is}(v, T)$  can be added to the generated Java code to ensure that no type violations occur.

This section covers some of the different classes of VDM types that the JML translator supports, and explains using our case study example, how JML is used to check a Java value against the VDM type that produces it. Finally, we summarise and provide the complete definition of  $\text{Is}(v, T)$  in Figure 2.1.

### 2.6.1 Where to generate dynamic type checks

Most of the types available in VDM are also present in Java in some form or other. The VDM and Java type systems do, however, have some differences that require us to generate extra checks to ensure that a Java value remains consistent with the VDM type that produces it.

In addition to producing the JML expression needed to check the consistency of a type, i.e.  $\text{Is}(v, T)$ , we also need to consider where to add the check to the generated code. The description below summarises the VDM-SL constructs that must be considered when adding these checks to the generated Java code. We use the term *parameter* to refer to an identifier whose value does not change. A parameter can be defined using a **let** construct, which is different from a state designator or variable that can be locally defined using a **dcl** statement or globally using a state definition (see section 2.2). The constructs to be considered are:

- **return** statement: If a functional description has a specified result type in its signature, then the returned value must be checked against the specified type.
- Parameters of functions and operations: The arguments passed to a functional description must be checked against the specified types of the corresponding formal parameters upon entry to the functional description.
- State designators: After updating a local or global state designator, the new value assigned must respect the type of the state designator.
- Variable or parameter declaration: After initialising a variable or parameter it must be checked against its declared type.

$\text{Is}(v, T) =$	<pre> Utils.is_bool(v) Utils.is_nat(v) Utils.is_nat1(v) Utils.is_int(v) Utils.is_rat(v) Utils.is_real(v) Utils.is_char(v) Utils.is_token(v) Utils.is_(v, String.class)  Utils.is_(v, S<sub>CG</sub>.class)  (v == null    Is(v, S)) V2J.isTup(v, n) &amp;&amp; Is(v, T<sub>1</sub>) &amp;&amp; ... &amp;&amp; Is(v, T<sub>n</sub>) Is(v, T<sub>1</sub>)    ...    Is(v, T<sub>n</sub>) V2J.isSet(v) &amp;&amp; (\forall int i;   0 &lt;= i &amp;&amp; i &lt; V2J.size(v); Is(V2J.get(v, i), S)) V2J.isSeq(v) &amp;&amp; (\forall int i;   0 &lt;= i &amp;&amp; i &lt; V2J.size(v); Is(V2J.get(v, i), S)) V2J.isSeq1(v) &amp;&amp; (\forall int i;   0 &lt;= i &amp;&amp; i &lt; V2J.size(v); Is(V2J.get(v, i), S)) V2J.isMap(v) &amp;&amp; (\forall int i;   0 &lt;= i &amp;&amp; i &lt; V2J.size(v);   Is(V2J.getDom(v, i), D) &amp;&amp; Is(V2J.getRng(v, i), R)) V2J.isInjMap(v) &amp;&amp; (\forall int i;   0 &lt;= i &amp;&amp; i &lt; V2J.size(v);   Is(V2J.getDom(v, i), D) &amp;&amp; Is(V2J.getRng(v, i), R))  Is(v, D) &amp;&amp; inv_T(v) </pre>	<pre> if T = bool if T = nat if T = nat1 if T = int if T = rat if T = real if T = char if T = token if T = seq of char  if T is a record or quote type S that generates to a Java class with the fully qualified name S<sub>CG</sub>  if T = [S] if T = T<sub>1</sub>*...*T<sub>n</sub> if T = T<sub>1</sub> ... T<sub>n</sub>  if T = set of S  if T = seq of S  if T = seq1 of S  if T = map D to R  if T = inmap D to R  if T is a named invariant type with domain type D and invariant method inv_T </pre>
---------------------	--	---

Figure 2.1: Complete definition of  $\text{Is}(v, T)$ .

- Value definition: An explicitly typed value definition must specify a value consistent with its type.

All of the constructs in the list above – with the exception of the value definition – can be checked using a JML **assert** statement. The reason for this is that the code-generated versions of these constructs appear inside methods in the generated code. Since a VDM value definition code-generates to a **public static final** field (a constant) it is checked using a **static invariant**.

## 2.6.2 Translating basic types

In our example we may wish to check that the amount being withdrawn from an account is valid – for example by requiring that it is a natural number larger than zero, as shown in Listing 2.29.

```

1 | let amount : nat1 = expense - profit
2 | in
3 |   Withdraw(accId, amount);

```

Listing 2.29: Use of explicit type annotation to ensure that a valid amount is being withdrawn.

In the generated Java code, shown in Listing 2.30, this is checked by analysing the value of the `amount` variable using the `Utils.is_nat1` method available from the Java code-generator's runtime library. This method is invoked from a JML annotation in order to check that `amount` is different from `null` and that it represents an integer larger than zero.

```

1 | Number amount = expense.longValue() - profit.longValue();
2 | //@ assert Utils.is_nat1(amount);
3 | return Withdraw(accId, amount);

```

Listing 2.30: Use of JML to check that a valid amount is being withdrawn.

### 11. Checking of the `nat1` type

Let  $v$  be a value or object reference in the generated code that originates from a variable or pattern of type `nat1` and further define  $Is(v, \text{nat1}) = \text{Utils.is\_nat1}(v)$ . To ensure that  $v$  represents a value of type `nat1`, generate a JML check to ensure that  $Is(v, \text{nat1})$  holds.

The approach used to check other basic types follows the principles demonstrated using Listing 2.29 and Listing 2.30 – the main difference being that each basic type uses a dedicated method from the Java code-generator's runtime library. Therefore, we omit the details of how other basic types of VDM are checked using JML, and instead provide the complete set of rules in Figure 2.1.

We note that a record type or a quote type can be checked in a way similar to that of a basic type. The reason for this is that the Java code-generator produces a Java class for each of the record definitions and quote types in the VDM model. Therefore, all there is to checking whether an object reference represents a given record or quote class is to check whether the object reference is an instance of said class. The rules for checking record and quote types are included in Figure 2.1.

### 2.6.3 Translating optional types

To demonstrate how the JML translator handles optional types consider the `GetCurrentCardId` operation in Listing 2.31. This operation returns the identification of the debit card currently inserted into the machine, if any. Otherwise the operation returns `nil` to indicate the absence of a debit card. To allow `null` as a return value, the optional type operator is used to specify the return type of the operation as `[nat]`.

```

1 | GetCurrentCardId : () ==> [nat]
2 | GetCurrentCardId () ==
3 |   if currentCard <> nil then
4 |     return currentCard.id
5 |   else
6 |     return nil;

```

Listing 2.31: Operation for getting the id of the debit card currently inserted into the ATM.

Considering solely the signature of the code-generated version of this operation, shown in Listing 2.32, there is no way to tell that the return type represents a `[nat]`.

```
1 public static Number GetCurrentCardId(){...}
```

Listing 2.32: Signature of the code-generated version of the `GetCurrentCardId` operation.

The reason for this is that the Java code-generator uses the `Number` class (which is part of the Java standard library) to represent all numeric VDM types. That the return type of the operation is `[nat]` only becomes apparent when we start using the corresponding method.

To demonstrate this, Listing 2.33 uses the result of invoking the `GetCurrentCardId` method to initialise a variable named `id`. The initialisation of `id` is immediately followed by a check that ensures that it represents either `null` or a natural number. The approach of allowing `null` values like this is the same for all optional types.

```
1 Number id = GetCurrentCardId();
2 //@ assert id == null || Utils.is_nat(id);
```

Listing 2.33: Use of the `GetCurrentCardId` method in the generated code.

## 12. Checking of optional types

Let  $v$  be a value or object reference in the generated code that originates from a variable or pattern of the VDM type  $[T]$  and further define

$\text{Is}(v, [T]) = (v == \text{null} \mid \mid \text{Is}(v, T))$

To ensure that  $v$  represents a value of type  $[T]$ , generate a JML check to ensure that  $\text{Is}(v, [T])$  holds.

### 2.6.4 Translating tuple types

In our case study example we use a tuple type to represent the status of the ATM: the first field is a `boolean` flag that indicates if the ATM is currently awaiting a debit card to be inserted, and the second field is a human-readable description of the current state of the ATM, e.g. “transaction in progress”. The signature of the operation that retrieves the status of the ATM is shown in Listing 2.34. Note in particular that the status returned is represented using the tuple type `bool * seq of char`.

```
1 GetStatus : () ==> bool * seq of char
2 GetStatus () == ...
```

Listing 2.34: The signature of the `GetStatus` operation.

In the generated Java code, every tuple value is represented as an instance of the `Tuple` class available from the Java code-generator runtime library. Since the `Tuple` class represents tuple values in general, each instance of this class must be checked against the specific tuple type that it originates from.

After the status of the ATM has been retrieved using the `GetStatus` method in the generated code, the status is checked as shown in Listing 2.35. First it is checked that `status` is a tuple of size two. Afterwards it is checked that the first field is a `boolean` and that the second field is a Java `String` (which represents the `seq of char` type).

```
1 Tuple status = GetStatus();
2 //@ assert (V2J.isTup(status,2) && Utils.is_bool(V2J.field(status,0)) &&
   Utils.is_(V2J.field(status,1),String.class));
```

Listing 2.35: Checking the ATM status in the generated code.

**13. Checking of tuple types**

Let  $v$  be a value or object reference in the generated code that originates from a variable or pattern of the VDM tuple type  $T_1 * \dots * T_n$  and further define

$$\text{Is}(v, T_1 * \dots * T_n) = \text{V2J.isTup}(v, n) \ \&\& \ \text{Is}(v, T_1) \ \&\& \dots \&\& \ \text{Is}(v, T_n)$$

To ensure that  $v$  represents a value of type  $T_1 * \dots * T_n$ , generate a JML check to ensure that  $\text{Is}(v, T_1 * \dots * T_n)$  holds.

**2.6.5 Translating union types**

Attempting to insert a debit card into the ATM results in the debit card being accepted, if no card is currently inserted and it is considered a valid card by the system. Otherwise the card is rejected. Based on the outcome of this the `NotifyUser` operation, shown in Listing 2.36, displays a message to inform the card holder about the current status of the session. This operation uses a union type, formed by the three quote types `<Accept>`, `<Busy>` and `<Reject>`, to represent one of three outcomes of the card holder attempting to insert a debit card into the ATM.

```

1 NotifyUser : <Accept>|<Busy>|<Reject> ==> ()
2 NotifyUser (outcome) ==
3 if outcome = <Accept> then
4   Display("Card accepted")
5 elseif outcome = <Busy> then
6   ...

```

Listing 2.36: Operation used to notify a ATM user.

The code-generated version of the `NotifyUser` operation is shown in Listing 2.37. Since the `outcome` parameter originates from the union type formed by the three quote types, it must be checked that `outcome` equals one of the three possible values. This check is performed immediately after entering the `NotifyUser` method, as shown in Listing 2.37.

```

1 public static void NotifyUser(final Object outcome) {
2   //@ assert (Utils.is_(outcome, atm.quotes.AcceptQuote.class) ||
3     Utils.is_(outcome, atm.quotes.BusyQuote.class) ||
4     Utils.is_(outcome, atm.quotes.RejectQuote.class));
5   if (Utils.equals(outcome, atm.quotes.AcceptQuote.getInstance())) {
6     Display("Card_accepted");
7   } else if (Utils.equals(outcome, atm.quotes.BusyQuote.getInstance())) {
8     ...
9   }

```

Listing 2.37: Code-generated version of the `NotifyUser` operation.



#### 14. Checking of union types

Let  $v$  be a value or object reference in the generated code that originates from a variable or pattern of the VDM union type  $T_1 \mid \dots \mid T_n$  and further define

$\text{Is}(v, T_1 \mid \dots \mid T_n) = \text{Is}(v, T_1) \mid \dots \mid \text{Is}(v, T_n)$

To ensure that  $v$  represents a value of type  $T_1 \mid \dots \mid T_n$ , generate a JML check to ensure that  $\text{Is}(v, T_1 \mid \dots \mid T_n)$  holds.

### 2.6.6 Translating collections

In the generated code the `VDMSet`, `VDMSeq` and `VDMMap` collection classes are used as raw types. Therefore the code-generator does not take advantage of Java generics to make compile-time guarantees about the types of the objects a collection stores. This approach has the advantage of making it easier to store Java objects and values of different types in the same collection without having to introduce additional types. Although this allows the type system of VDM to be represented in Java it has the disadvantage that no compile-time guarantees can be made about the types of the objects that a collection stores.

In the ATM example we use the `TotalBalance` function, shown Listing 2.38, to calculate the total balance available from a set of accounts.

```

1 TotalBalance : set of Account -> real
2 TotalBalance (acs) ==
3   if acs = {} then
4     0
5   else
6     let a in set acs
7     in
8       a.balance + TotalBalance(acs \ {a});

```

Listing 2.38: Function that calculates the total balance available from a set of accounts.

When the `TotalBalance` function is code-generated to JML-annotated Java, the code-generator adds JML assertions to ensure that the set of accounts is consistent with the collection type used in VDM. Since an `Account` record is represented using a Java class with the same name, we have to check that every element in the set is an instance of said Java class. As shown in Listing 2.39, this is checked using a quantified expression. This expression uses a bound variable  $i$  to iterate over all the accounts and check that each element is an instance of the `Account` record class. Although sets are unordered collections, the quantified expression takes advantage of `VDMSet` being implemented as an ordered collection. The formulation of the range expression in the quantified expression further ensures that the assertion can be checked using a tool such as the OpenJML runtime assertion checker, i.e. the assertion is executable.

```

1 /*@ pure @*/
2 public static Number TotalBalance(final VDMSet acs) {
3   /*@ assert (V2J.isSet(acs) && (\forallall int i; 0 <= i && i < V2J.size(acs);
4     Utils.is_(V2J.get(ac, i), atm.ATMtypes.Account.class))) ;
5   if (Utils.empty(ac)) {
6     Number ret_1 = 0L;
7     /*@ assert Utils.is_real(ret_1);
8     return ret_1;
9   } else { ... /*Compute sum recursively */

```

Listing 2.39: Code-generated version of the `TotalBalance` operation.

The JML translator only uses Java 7 features since OpenJML did not support Java 8 at the time the JML translator was developed. Iterating over collections (as shown in Listing 2.39) may also be achieved using Java 8 features such as lambda expressions. For example, one could imagine a method used to check collection types that would take as input two arguments (1) the collection itself and (2) a predicate method (e.g. lambda expression) that would be evaluated for each of the elements in the collection. In that way the generated JML annotations would not have to rely on sets implemented as ordered collections. Since lambda expressions in Java are mostly syntactic sugar for anonymous inner classes, lambda expressions could in principle be represented solely using Java 7 features. However, using this approach, the generated JML annotations would not be concise, although this is only a concern if a human will read them.

### 15. Checking of sets

Let  $v$  be a value or object reference in the generated code that originates from a variable or pattern of the VDM set type **set of**  $T$  and further define

```
Is( $v$ , set of  $T$ ) = V2J.isSet( $v$ ) &&
(\forall forall  $i$ ; 0 <=  $i$  &&
 $i$  < V2J.size( $v$ ); Is(V2J.get( $v$ ,  $i$ ),  $T$ ))
```

To ensure that  $v$  represents a value of type **set of**  $T$ , generate a JML check to ensure that `Is( $v$ , set of  $T$ )` holds.

The VDM sequence types **seq** and **seq1** are checked in a way similar to sets. The difference between checking the **seq** and **seq1** collection types is that the **seq1** type requires at least one element to be present in the sequence. Checking a map, which like a set is an unordered collection, takes advantage of `VDMMap` imposing an order on the domain and range values. The main difference between checking a map and a set is that both the domain and range values of a map have to be checked. Checking the injective map type **inmap** is similar to checking a standard map, except that the injectivity property must hold. We refrain from providing examples of how to check each of the collection types in VDM since they are similar to what has already been shown. Instead we summarise the rules for checking all of the collection types in Figure 2.1.

### 2.6.7 Translating named invariant types to JML

Since the Java code-generator does not generate additional class definitions for named invariant types, the invariant imposed on such a type cannot be expressed as a JML invariant. This is only possible for a record since it translates to a class definition.

Instead, we identify places in the generated code where a named invariant type may be violated, as described in subsection 2.6.1, and check that the invariant holds. Also, it is worth noting that a named invariant type, unlike a record type, does not have an explicit type constructor. Therefore, an expression can only violate a named invariant type if the expression is explicitly declared to be of that type.

The ATM in our example is not capable of dispensing cents and also imposes a limit on the amount of money that can be withdrawn. Therefore, the amount of money can be represented as a named invariant type. An attempt to withdraw an amount of money that exceeds 2000 will yield a runtime error. The named invariant type used to represent the amount withdrawn from an account is shown together with the `Withdraw` operation in Listing 2.40.

```

1 types
2 Amount = nat1
3 inv a == a < 2000;
4
5 operations
6 Withdraw : AccountId * Amount ==> real
7 Withdraw (id, amount) == ...

```

Listing 2.40: The amount to withdraw modelled using a named invariant type.

On entering the code-generated version of `Withdraw`, shown in Listing 2.41, we assert that `amount` meets the named invariant type `Amount`. The assertion does two things: First it performs a dynamic type check to ensure that `amount` is a valid domain type of `Amount` and secondly, it checks that the invariant predicate holds. For the example in Listing 2.41 this means checking that `amount` is of type `nat1` and smaller than 2000. Note that meeting the invariant condition does not imply compatibility with the domain type of the named invariant type and vice versa. For example, `-1` is smaller than 2000 but it is not of type `nat1`. Likewise, `2001` is of type `nat1` but it exceeds 2000 so neither `-1` nor `2001` are of type `Amount`.

```

1 public static Number Withdraw(final Number id, final Number amount){
2   ...
3   //@ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
4   ...
5 }

```

Listing 2.41: Checking a named invariant type of an operation parameter in JML.

The code-generated invariant method for type `Amount` is shown in Listing 2.42. Since the named invariant type check, shown in Listing 2.41, is evaluated from left to right using short-circuit evaluation semantics [26], the invariant method is only invoked if the value subject to checking is compatible with the domain type of the named invariant type. Therefore, it is safe to narrow (or cast) the type of the argument passed to the invariant method before performing the invariant check.

```

1 /*@ pure @*/
2 /*@ helper @*/
3 public static Boolean inv_ATM_Amount(final Object check_a) {
4   Number a = ((Number) check_a);
5   return a.longValue() < 2000L;
6 }

```

Listing 2.42: The named invariant type method for `Amount`.

**16. Checking of named invariant types**

Let  $v$  be a value or object reference in the generated code that originates from a variable or pattern of the VDM named invariant type  $T$  based on the domain type  $D$  and constrained by invariant predicate  $e(p)$ , i.e.  $T$  is defined as

**types**

$T = D$

**inv**  $p == e(p)$

Then  $T$  has an invariant method, responsible for running the code-generated version of the  $e(p)$  check, with a signature defined as:

**public static boolean**  $inv\_T(Object\ o)$

Further define  $Is(v, T) = Is(v, D) \ \&\& \ inv\_T(v)$

To ensure that  $v$  represents a value of type  $T$ , generate a JML check to ensure that  $Is(v, T)$  holds.

Note that the invariant method  $inv\_T$  in rule 16 defines the input parameter  $o$  to be of type `Object`, thus allowing  $inv\_T$  to accept inputs of any type. Therefore,  $inv\_T$  must narrow the type of the input parameter  $o$  before performing the invariant check (see the example in Listing 2.42). This approach has the advantage that it allows simpler JML checks since the argument type does not need to be narrowed before the invariant method is invoked. Had the input parameter of the invariant method been defined using the smallest possible type, then the argument type would need to be narrowed for situations where the argument is masked as a union type. Although this would complicate the JML checks, it would have the advantage of allowing type narrowing to be removed from the invariant methods.

## 2.7 Other aspects of VDM-SL affecting the JML-generation

There are other aspects of VDM-SL that further complicate the generation of VDM-SL models to JML-annotated Java. In this section we use examples to demonstrate these issues and explain how they may be overcome.

### 2.7.1 Complex state designators

State designators may be composite data structures such as records with fields that themselves are records. Such a data type forms *complex state designators* that when modified require careful handling during the translation process. To demonstrate this, consider the three VDM-SL record definitions  $R1$ ,  $R2$  and  $R3$  in Listing 2.43. Note in particular how the invariants of  $R1$  and  $R2$  depend on the field of  $R3$ . This transitive dependency complicates checking of invariants in the generated code. To demonstrate this, the operation in Listing 2.43 instantiates  $R1$  as  $r1$  and modifies it to violate the  $R1$  invariant, which causes a runtime-error to be reported.

```

1  types
2   $R1 :: r2 : R2$ 
3  inv  $r1 == r1.r2.r3.x <> -1;$ 
4   $R2 :: r3 : R3$ 
5  inv  $r2 == r2.r3.x <> -2;$ 
6   $R3 :: x : \text{int}$ 
7  inv  $r3 == r3.x <> -3;$ 
8
9  operations
```

```

10 op: () ==> nat
11 op () ==
12 (
13   dcl r1 : R1 := mk_R1(mk_R2(mk_R3(5)));
14   r1.r2.r3.x := -1;
15   return 0;
16 )

```

Listing 2.43: Record nesting in VDM-SL.

The operation `op` in Listing 2.43 produces the method in Listing 2.44. For this example, `r1` is the same in both listings, `r2` is the same as `stateDes_1` in Listing 2.44, and `r3` is the same as `stateDes_2`. Note that in Listing 2.44 we have removed fully qualified names of record classes and other JML checks that are not relevant.

```

1 public static Number op() {
2   R1 r1 = new R1(new R2(new R3(5L)));
3   R2 stateDes_1 = r1.get_r2();
4   R3 stateDes_2 = stateDes_1.get_r3();
5   stateDes_2.set_x(-1L);
6   //@ assert \invariant_for(stateDes_1);
7   //@ assert \invariant_for(r1);
8   Number ret_1 = 0L;
9   return ret_1;
10 }

```

Listing 2.44: Code-generated version of the operation from Listing 2.43.

Immediately after completing the state update, i.e. invoking `stateDes_2.set_x(-1L)`, the following things happen:

1. The state of `stateDes_2` becomes *visible* thus triggering the `stateDes_2` invariant check.
2. The invariant check of `stateDes_1` is run as `\invariant_for(stateDes_1)` and finally,
3. the invariant check of `r1` is run by asserting `\invariant_for(r1)`, which causes a runtime-error to be reported.

Strictly speaking the objects pointed to by `stateDes_1` and `r` are also in visible states after executing the update to `stateDes_2` and therefore the invariants of those objects should also hold. In particular a state is *visible* for an object `o` “when no constructor, destructor, non-static method invocation with `o` as receiver, or static method invocation for a method in `o`’s class or some superclass of `o`’s class is in progress [24]”. So in theory the invariant checks should not have to be run explicitly (step 2 and step 3). The reason that the JML translator generates these checks anyway has to do with the strategies JML tools use to check invariants.

Tools such as JML runtime checkers may assume no problems with ownership aliasing to avoid having to keep track of what objects and types are in visible states. Although this reduces the overhead of checking invariants, it also means that some invariant violations might go unnoticed. Alternatively, tools can check every applicable invariant for classes and objects in visible states but this adds a significant overhead to the program execution.

Since aliasing can never occur in VDM-SL, it becomes simpler to keep track of what objects are in a visible state in the generated code and thus generate JML checks that explicitly trigger

the invariants checks. This has the advantage that invariant violations do not go unnoticed even though a JML tool adopts a more practical approach to checking invariants.

For the example in Listing 2.44, the important thing is to ensure that the violation of the invariant of  $R1$  is reported after executing the state update. This is done by asserting the entire chain of state designators. The JML translator is able to generate these checks since it keeps track of state designators of records that may have been affected by updates to other state designators.

17. Checking transitive dependencies
<p>Let <math>d_n</math> be a state designator of a record in the generated code that has been updated non-atomically, and let <math>d_k, \dots, d_1</math>, for <math>k = n-1</math>, be state designators that were affected by the update to <math>d_n</math>. Further assume that <math>d_i</math> may be of one of <math>m_i</math> record types <math>D_{i1}, \dots, D_{im_i}</math>. Immediately after executing the update to <math>d_n</math> the state of <math>d_n</math> becomes visible. To ensure that the invariant is evaluated for all affected state designators, execute the following sequence of assertions:</p> <pre>//@ assert d_k instance of D_{k1} ==&gt;   \invariant_for( (D_{k1}) d_k ); ... //@ assert d_k instance of D_{km_k} ==&gt;   \invariant_for( (D_{km_k}) d_k ); .... //@ assert d_1 instance of D_{11} ==&gt;   \invariant_for( (D_{11}) d_1 ); ... //@ assert d_1 instance of D_{1m_1} ==&gt;   \invariant_for( (D_{1m_1}) d_1 );</pre>

Note that the code in Listing 2.44 omits the **instance of** checks, proposed by rule 17, since the types of the affected state designators can be determined statically.

Regarding rule 9, similar issues with transitive dependencies may occur in the generated code when dealing with atomic execution. Recall that invariant checking is disabled before a code-generated atomic statement block is executed. Once the atomic execution has completed, invariant checking is re-enabled, and therefore rule 9 must also take into account all the state designators that were affected by the atomic execution.

## 2.7.2 Recursive types

It is possible to formulate recursive types for which the generated JML checks can only perform limited type checking. To demonstrate this, consider the recursive VDM type definition in Listing 2.45. For this example,  $S$  represents an infinite number of types including **nat1** as well as all possible dimensions of sequences that store elements of type **nat1**, i.e. **seq of nat1**, **seq of seq of nat1** and so on.

```
1 types
2 S = nat1 | seq of S;
```

Listing 2.45: Example of recursive type definition in VDM.

The issue with this kind of type definition is that  $Is(v, S)$  in theory becomes an expression of infinite length. The JML translator stops generating type checks whenever it encounters type

cycles. For the particular example in Listing 2.45 this means that a Java value or object reference  $v$  is only considered to respect  $S$  if `Utils.is_nat1(v)` holds. For the rest of this section, we discuss the current limitations of type checking recursive types, and describe how these limitations may be addressed.

The approach used to check types could be changed to also take the depth of the recursion  $n$  into account, i.e. use `Is(v, T, n)` to generate the type checks. The current approach used by the JML translator thus corresponds to generating checks using `Is(v, T, 1)`. `Is(v, S, 2)` then generates checks for types **nat1** and **seq of nat**, whereas `Is(v, S, 3)` additionally generates a check for the type **seq of seq of nat1**.

Alternatively, checking a recursive type  $T$  (such as  $S$  shown in Listing 2.45) can be done using a code-generated recursive method that is constructed in a way that allows a value  $v$  to be validated against  $T$ . Although static provers may not be able to perform checking of such types it should be possible using runtime assertion checking. However, in order to enable this style of type checking, the JML translator would have to be extended with functionality that enables these methods to be generated such that they can be invoked from the generated JML assertions.

The limitation of the JML translator for the example shown in Listing 2.45 is a consequence of  $S$  being defined using the union type constructor “ $|$ ”. However, it is possible to check more practical examples of recursively defined types such as the linked list  $LL$  shown in Listing 2.46.

To demonstrate this, consider the construction of a linked list value in VDM that contains the numbers 1, 2 and 3 as shown in Listing 2.47. In the generated code this value is represented using the code shown in Listing 2.48.

```

1 types
2 LL ::
3   element : nat
4   tail : [LL]

```

Listing 2.46: Example of a linked list defined using a record type.

```
mk_LL(1, mk_LL(2, mk_LL(3, nil)))
```

Listing 2.47: Example of a linked list value in VDM.

```
new LL(1L, new LL(2L, new LL(3L, null)));
```

Listing 2.48: Example of a linked list value in Java.

Each time an object of type  $LL$  is instantiated in Java the constructor checks the types of the current `element` and the `tail` – see Listing 2.49. For this linked list example, it is therefore possible to type check  $LL$  since the VDM type is represented using a recursively defined class in the generated code.

```

1 public LL(final Number _element, final LL _tail) {
2   //@ assert Utils.is_nat(_element);
3   //@ assert (_tail == null || Utils.is_(_tail, LL.class));
4   ...
5 }

```

Listing 2.49: Type checking a linked list using JML.

### 2.7.3 Detecting problems with the generated code

As explained in subsection 2.5.4 deep copying objects may significantly affect the performance of the generated code. Therefore, the user may not always want to have these copy calls generated. However, from a general perspective this may result in code that does not preserve the semantics across the translation. JML specifications can help detect such problems. To demonstrate this consider the VDM-SL operation in Listing 2.50. This operation assumes the existence of a two-dimensional vector `Vector2D`, defined as a record (a value type). In Listing 2.50 `v2` is created as a deep copy of `v1`, and therefore the assignment to `v1` has no affect on `v2`, and `op` therefore returns 1 (see the postcondition).

If this example is translated to Java with deep copying *disabled* the code shown in Listing 2.51 is produced. Note that this listing omits the generated JML assertions to focus on the postcondition.

```

1 op : () ==> nat
2 op () == (
3   dcl v1 : Vector2D := mk_Vector2D(1,2);
4   dcl v2 : Vector2D := v1; -- Copy value
5   v1.x := 2;
6   return v2.x;
7 post RESULT = 1

```

Listing 2.50: Use of value types in VDM.

```

1 //@ ensures post_op(\result);
2 public static Number op() {
3   Vector2D v1 = new Vector2D(1L,2L);
4   Vector2D v2 = v1;
5   v1.set_x(2L);
6   Number ret_1 = v2.get_x();
7   return ret_1;
8 }

```

Listing 2.51: Generated Java code without copy calls.

If this code is executed using the OpenJML runtime assertion checker an error is reported because the method returns 2, which is different from the result obtained by executing the corresponding VDM-SL operation. Since deep copying is disabled only the `v1` reference is copied, and therefore the update to `v1`, i.e. `v1.set_x(2L)`, also affects `v2`.

The detection of the postcondition violation as reported by the OpenJML runtime assertion checker is shown in Listing 2.52. However, if the code is generated with deep copying enabled (at the cost of performance) then `v2` will be constructed as `Utils.copy(v1)` and the method will change to return 1, as expected.

```

Ex/DEFAULT.java:17: JML postcondition is false
    public static Number op() {
Ex/DEFAULT.java:16: Associated declaration: Ex/DEFAULT.java:17:
    //@ ensures post_op(\result);

```

Listing 2.52: Detection of a postcondition violation.

## 2.8 Translation assessment



In this section we provide an assessment of the translation. We first describe how the correctness of the translation was assessed, and afterwards we discuss the scope and treated feature set in relation to existing JML tools.

### 2.8.1 Translation correctness

The translation rules have been validated by running examples through the JML translator and analysing the generated Java/JML using the OpenJML runtime assertion checker. Some of the examples used to test the tool constitute *integration tests* that have been developed by the authors. In addition, we have used the tool to analyse an *external specification* (originally used as part of an industrial case study) that the authors have not been involved in the development of. A summary of the different examples used to test the translation is given below. Additional details about the examples can be found via the references provided.

The *integration tests* currently consist of 85 examples that cover testing of all the translation rules. Each test (typically) forms a minimal example that exercises a small part of the entire translation (such as a single rule). The workflow for running these tests is as follows: First, the test model is translated to JML-annotated Java using the JML translator. Next, the generated Java/JML is compiled and executed using the OpenJML runtime assertion checker. Finally, the (actual) output reported by the OpenJML runtime assertion checker is compared to the expected output in order to confirm that the behaviour of the test model is preserved across the translation. For example, if the execution of a test model produces a precondition violation then the equivalent error is expected to be produced when the generated Java/JML is executed using the OpenJML runtime assertion checker. All the examples used to test the JML translator are available via Overture’s GitHub page [31] or can be found in appendix C.

Compared to the *integration tests*, the *external specification* is a large example that is rich in terms of DbC elements. The model was originally developed to study the properties of an algorithm used to obfuscate Financial Accounting District (FAD) codes, which are six digit numbers used to identify branches of a retailer. The customer required that obfuscated FAD codes were still six digit numbers, remained unique (per branch), and that the entire range of FAD codes (0-999999) was still available. In addition, the obfuscation had to be a light-weight calculation (rather than a look-up in a table). The properties of the algorithm were described using VDM contracts to allow the algorithm to be validated using VDM’s test automation features [20].

Investigating whether the algorithm met the requirements necessitated the generation and execution of one million tests that initially could not be handled by any of the VDM tools (either due to intractable execution times, or because the VDM interpreter ran out of memory). Motivated by this, the specification was translated into a JML-annotated Java program [35], and all one million tests were executed using a code-generated version of the VDM specification. In that way, the properties of the obfuscation algorithm could be validated by executing a code-generated version of the VDM specification using the OpenJML runtime assertion checker.

### 2.8.2 Translation scope and treated feature set

As explained in subsection 2.7.2 it is possible to formulate recursive types that currently are not supported by the JML translator. Aside from that, all VDM-SL’s types and contract-based elements are supported. However, the JML translator does not currently support the object-oriented and real-time dialects of VDM, called VDM++ [12] and VDM-RT [23].

The Java code-generator that we extend currently only uses Java 7 features in the generated code. OpenJML is the only JML tool that we are aware of that supports this version of Java.

Specifically, as of December 2016, OpenJML version 0.8.5 was released with support for Java 8, i.e. the latest official Java version (at the current time of writing). Other JML tools, on the other hand, lack support for recent Java versions (in particular Java 7 and 8). Therefore, these tools cannot currently be used to analyse the generated Java/JML.

The JML translation is only valuable if the JML features that it relies on are supported by JML tools. Specifically, we have aimed to develop a translation that generates Java/JML that can be analysed using OpenJML. However, the translation would benefit from the `\invariant_for` construct, which OpenJML does not currently support. Instead we offer an alternative way to represent this construct in order to achieve compatibility with OpenJML (see subsection 2.5.6 for details).

## 2.9 Related work

---

In [37] Vilhena considers the possibilities for automatically converting between VDM++ and JML and the approach is demonstrated using a proof-of-concept implementation. That work considers a bi-directional mapping, whereas we only consider a one-way translation from VDM-SL to Java/JML. The bi-directional mapping proposed by Vilhena only produces the JML specification files (where non-model methods do not define bodies). Therefore, Vilhena’s mapping does not generate annotations at the statement level, which is an essential part of our work. The implementation of the bi-directional mapping was originally targeting the Overture tool, but it never reached maturity to be included in the release of the tool.

Rules for translating from a subset of VDM-SL to JML are proposed by Jin et al. in [14]. Their approach also considers implicit functional descriptions but it provides limited support for translation of record definitions and named invariant types. In the early phases of the software development process the authors propose to formulate requirements in natural language or using the Unified Modeling Language (UML) [34] and then formalise them in VDM-SL to eliminate ambiguity. Subsequently the authors manually apply their rules to the VDM-SL specification to produce an initial version of the software implementation. Their work does, however, not take generation of the bodies of functions and operations into account. Therefore, the authors only produce the method signatures for the Java methods when translating the functional descriptions of the VDM-SL model.

The translation rules proposed by Jin et al. have been implemented as an Eclipse plugin by Zhou et al. in [42]. The plugin takes a VDM-SL specification as input, which is type-checked using VDMTools [18], and outputs JML-annotated Java classes that must be completed manually by the developer.

Translations from other formal notations or modelling languages to JML-annotated Java have also been developed. As an example, Rivera et al. present the EventB2Java tool [33] – a code-generator, which is capable of translating both abstract and refinement Event-B [1] models into JML-annotated Java. EventB2Java has the advantage over other Event-B code-generators that it does not require user intervention as part of the code-generation process, which is similar to our approach.

In [25] Lensink et al. present a prototype code-generator that translates a subset of the Prototype Verification System (PVS) [32] to an intermediate representation in Why [9] suitable for program verification. Subsequently the Why representation is translated to JML-annotated Java. In their work the authors focus on translating executable PVS constructs, which is similar to what we do for VDM-SL. A key feature of their code-generator is that it, in addition to specification code, also translates proven properties, which is outside the scope of our work.

Hubbers et. al propose AutoJML [13] – a tool for translating UML state diagrams into JML-annotated Java Card code [41]. A state diagram describes a Java Card applet from which AutoJML produces Java skeleton code annotated with JML. In the generated code the different states are represented as constant values, and an additional Java field is used to represent the current state of the applet. A JML **invariant** is used to specify the valid state values for this field, and a JML **constraint** is used to describe the valid state transitions. This is comparable to the way we enable and disable invariant checking, which we do by toggling the `invChecksOn` **ghost** field using **set** statements.

In [17] Klebanov proposes an approach similar to that of Hubbers et al. Instead of using UML state diagrams, Klebanov uses automata-based programming to describe the behaviour of a smart card application, which is generated to JML-annotated Java Card code. Klebanov argues that use of automata-based programming over UML state diagrams is a better way to describe application-specific behaviour. A similar argument can be made for VDM-SL, which is suitable for capturing the dynamic aspects of a system.

## 2.10 Conclusion and future plans

---

In this report we have demonstrated how VDM-SL models can be translated to JML-annotated Java programs that can be checked for correctness using JML tools. The JML translator uses JML to represent the DbC elements of VDM-SL, and generates checks that help ensure the consistency of VDM-SL types across the translation.

The principles for pre- and postconditions in VDM-SL and JML are similar although there are subtle semantic differences between the two notations. These differences are mostly caused by the fact that JML is built on top of Java, where object types use reference semantics. VDM-SL, on the other hand, solely uses value types. Therefore, it is necessary to employ deep cloning principles when representing value types in JML-annotated Java code.

Checking state and record invariants in the generated code is complicated due to two reasons: First, atomic execution in VDM requires a way to control when invariant checking must be done. We achieve this by using a **ghost** field to indicate when invariant checking is enabled, and update it before entering and leaving the **atomic** statement. Secondly, we have demonstrated that transitive dependencies between records sometimes require extra JML checks to be generated to ensure that the invariant checks are evaluated when they should.

The differences between the type systems of VDM-SL and Java further necessitate extra checks to be produced. These checks are needed to ensure that the generated code does not violate any of the constraints imposed by the types in the VDM-SL model. Overture performs these dynamic type checks internally, whereas they must be made explicit in Java.

Although DbC languages often support many of the same DbC concepts, it is the semantic differences between the languages that make developing a translation challenging. In this report we have shown several examples of such differences and how they can be addressed. Naturally, translating between other specification language pairs may reveal other differences and design details that are of interest to researchers and practitioners working on comparable tasks. However, based on the experiences gained by developing the VDM-SL-to-JML translation, we list some of the design details that we believe are likely to challenge the development of translations between other specification language pairs:

**Invariants:** The times when invariants are evaluated varies across specification languages. For example, in VDM they have to hold at all times (except inside **atomic** statements), whereas

in JML they must hold in visible states. When invariants have different semantics the translation must find a way to either produce or reduce the number of invariant checks at the appropriate places in the code.

**Type systems:** The differences between type systems require careful attention when developing a translation. Especially, when the destination language (e.g. JML) uses a more “coarse-grained” type system than the source language (e.g. VDM-SL). For such situations extra checks must be produced to ensure that types are used consistently across the translation. In our work we use the function  $\text{Is}(v, T)$  to produce these extra checks.

**Atomic execution:** Languages may use dedicated constructs to represent atomic execution (e.g. VDM) or by allowing invariants not to hold at certain times (e.g. JML). In this report an example was given of how a dedicated construct can be emulated in a language that does not support one natively.

**Old state:** Despite pre- and postconditions being similar concepts in different specification languages it is likely that the notion of old state may require careful handling when developing a translation between two specification languages. In our work, a deep cloning principle was employed to ensure the correct construction of the old state.

In the future we plan to use this work in the context of test automation. In VDM it is possible to specify a trace definition in a way similar to that of a regular expression. This trace can then be expanded into a large collection of tests that can be executed against the model. This is a useful way to detect deficiencies in the model, such as missing preconditions, postconditions and invariants [20].

We plan to code-generate the trace expansion such that the tests can be executed against the code-generated version of the model. The work presented in this report can then be used to detect contract or type violations and give verdicts to the code-generated trace tests. We believe that this will be particularly advantageous for execution of large collections of tests. We expect this approach to significantly increase execution speed for test cases and also allow more tests to be executed. In addition, we plan to look into JML-generation for other VDM dialects such as VDM++. However, since VDM++ is object-oriented and supports concurrency, we envisage that this will give rise to a completely new set of challenges not addressed by the work in this report.

So far the analysis of the generated Java/JML has primarily been limited to runtime assertion checking. Another item of future work is to formally verify the generated code against the JML specification. In particular, by investigating to what extent this is possible, and whether the JML translation can be optimised in a way that better supports formal verification through static analysis. For example, currently the translation produces auxiliary methods for invariants and pre- and postconditions that are used as part of the JML specification. However, use of method calls in specifications complicates static analysis due to, for example, the possibility of exceptions or non-terminating behaviour [7].

We hope that our work will serve as inspiration for other researchers who seek to bridge the gap between other specification notations and implementation technologies that support the DbC approach. We believe that the rules proposed in this report can be useful for others who want to translate between specification languages such as ASM, B and Z and implementation technologies such as Spec#, Sparc-Ada and Eiffel.



# The ATM model

This appendix contains the complete version of the ATM model that is used in this report to demonstrate the JML translation.

```
1 module ATM
2
3 imports from IO all
4 exports all
5
6 definitions
7
8 state St of
9   validCards : set of Card
10  currentCard : [Card]
11  pinOk : bool
12  accounts : map AccountId to Account
13  init St == St = mk_St({},nil,false,{|->})
14  inv mk_St(v,c,p,a) ==
15    (p or c <> nil => c in set v)
16    and
17    forall id1, id2 in set dom a &
18      id1 <> id2 =>
19        a(id1).cards inter a(id2).cards = {}
20 end
21
22 types
23
24 Card ::
25   id : nat
26   pin : Pin;
27
28 Pin = nat
29 inv p == 0 <= p and p <= 9999;
30
31 AccountId = nat
32 inv id == id > 0;
33
34 Account ::
35   cards : set of Card
36   balance : real
37   inv a == a.balance >= -1000;
38
39 Amount = nat1
```

## Appendix A. The ATM model

```

40 inv a == a < 2000;
41
42 functions
43
44 TotalBalance : set of Account -> real
45 TotalBalance (acs) ==
46   if acs = {} then
47     0
48   else
49     let a in set acs
50     in
51       a.balance + TotalBalance(acs \ {a})
52 measure TotalBalanceMes;
53
54 TotalBalanceMes: set of Account +> nat
55 TotalBalanceMes(acs) == card acs;
56
57 operations
58
59 GetStatus : () ==> bool * seq of char
60 GetStatus () ==
61   if currentCard <> nil then
62     if pinOk then
63       return mk_(false, "transaction_in_progress.")
64     else
65       return mk_(false, "debit_card_inserted._Awaiting_pin_code.")
66   else
67     return mk_(true, "no_debit_card_is_currently_inserted_into_the_machine.");
68
69 OpenAccount : set of Card * AccountId ==> ()
70 OpenAccount (cards, id) ==
71   accounts := accounts munion {id |-> mk_Account(cards, 0.0)}
72 pre id not in set dom accounts
73 post id in set dom accounts and
74   accounts(id).balance = 0;
75
76 AddCard : Card ==> ()
77 AddCard (c) ==
78   validCards := validCards union {c}
79 pre c not in set validCards
80 post c in set validCards;
81
82 RemoveCard : Card ==> ()
83 RemoveCard (c) ==
84   validCards := validCards \ {c}
85 pre c in set validCards
86 post c not in set validCards;
87
88 InsertCard : Card ==> <Accept>|<Busy>|<Reject>
89 InsertCard (c) ==
90   if c in set validCards then
91     (
92       currentCard := c;
93       return <Accept>;
94     )
95   elseif currentCard <> nil then
96     return <Busy>
97   else
98     return <Reject>
99   pre currentCard = nil

```

```

100 post
101   if RESULT = <Accept> then
102     currentCard = c
103   else if RESULT = <Busy> then
104     currentCard = currentCard~
105   else currentCard = nil;
106
107 Display : seq of char ==> ()
108 Display (msg) ==
109   IO`println(msg);
110
111 NotifyUser : <Accept>|<Busy>|<Reject> ==> ()
112 NotifyUser (outcome) ==
113   if outcome = <Accept> then
114     Display("Card_accepted")
115   elseif outcome = <Busy> then
116     Display("Another_card_has_already_been_inserted")
117   else if outcome = <Reject> then
118     Display("Unknown_card")
119   else
120     error;
121
122 EnterPin : Pin ==> ()
123 EnterPin (pin) ==
124   pinOk := (currentCard.pin = pin)
125 pre currentCard <> nil;
126
127 ReturnCard : () ==> ()
128 ReturnCard () ==
129   atomic
130   (
131     currentCard := nil;
132     pinOk := false;
133   )
134 pre currentCard <> nil
135 post currentCard = nil and not pinOk;
136
137 Withdraw : AccountId * Amount ==> real
138 Withdraw (id, amount) ==
139   let newBalance = accounts(id).balance - amount
140   in
141   (
142     accounts(id).balance := newBalance;
143     return newBalance;
144   )
145 pre currentCard in set validCards and pinOk and
146   currentCard in set accounts(id).cards and
147   id in set dom accounts
148 post
149   let accountPre = accounts~(id),
150   accountPost = accounts(id)
151   in
152     accountPre.balance = accountPost.balance + amount and
153     accountPost.balance = RESULT;
154
155 Deposit : AccountId * Amount ==> real
156 Deposit (id, amount) ==
157   let newBalance = accounts(id).balance + amount
158   in
159   (

```

## Appendix A. The ATM model

```

160 | accounts(id).balance := newBalance;
161 | return newBalance;
162 | )
163 | pre pre-Withdraw(id, amount, St)
164 | post
165 | let accountPre = accounts~(id),
166 |     accountPost = accounts(id)
167 | in
168 |     accountPre.balance + amount = accountPost.balance and
169 |     accountPost.balance = RESULT;
170 |
171 | PrintAccount: AccountId ==> ()
172 | PrintAccount(id) ==
173 | let balance = accounts(id).balance
174 | in
175 |     IO`printf("Balance_is_for_account_%s_is_%s\n", [id, balance]);
176 |
177 | GetCurrentCardId : () ==> [nat]
178 | GetCurrentCardId () ==
179 |     if currentCard <> nil then
180 |         return currentCard.id
181 |     else
182 |         return nil;
183 |
184 | --
185 | -- Test operations
186 | --
187 |
188 | TestCurrentCardId : () ==> [nat]
189 | TestCurrentCardId () ==
190 | let id = GetCurrentCardId()
191 | in
192 |     return id;
193 |
194 | TestStatus : () ==> real
195 | TestStatus () ==
196 | let accId = 1,
197 |     c1 = mk_Card(1, 1234)
198 | in
199 | (
200 |
201 |     AddCard(c1);
202 |     OpenAccount({mk_Card(1, 1234)}, accId);
203 |
204 |     let status = GetStatus(),
205 |         awaitingCard = status.#1,
206 |         msg = status.#2
207 |     in
208 |     (
209 |         IO`println("Message:_ " ^ msg);
210 |         if awaitingCard and <Accept> = InsertCard(c1) then
211 |         (
212 |             NotifyUser(<Accept>);
213 |             EnterPin(1234);
214 |             Deposit(accId, 100);
215 |         );
216 |     );
217 |
218 |     return 0;
219 | );

```



```

220
221 TestWithdraw : () ==> real
222 TestWithdraw () ==
223 let accId = 1,
224     cardId = 1,
225     pin = 1234,
226     c1 = mk_Card(cardId, pin)
227 in
228 (
229
230   AddCard(c1);
231   OpenAccount({mk_Card(1, 1234)}, accId);
232
233   if InsertCard(c1) = <Accept> then
234   (
235     EnterPin(pin);
236     let expense = 600,
237         profit = 100
238     in
239       let amount : nat1 = expense - profit
240       in
241         Withdraw(accId, amount);
242   );
243
244   error;
245 );
246
247 TestTotalBalance : () ==> real
248 TestTotalBalance () ==
249 let card1 = mk_Card(1, 1234),
250     card2 = mk_Card(2, 5678),
251     ac1 = mk_Account({card1}, 1000),
252     ac2 = mk_Account({card2}, 500)
253 in
254   TotalBalance({ac1, ac2});
255
256 TestScenario : () ==> ()
257 TestScenario() ==
258 let accId1 : AccountId = 1,
259     pin1 = 1234,
260     card1 = mk_Card(1, pin1),
261     pin2 = 2345,
262     card2 = mk_Card(2, pin2)
263 in
264 (
265   AddCard(card1);
266   AddCard(card2);
267   OpenAccount({card1, card2}, accId1);
268   let - = InsertCard(card2) in skip;
269   PrintAccount(accId1);
270   EnterPin(2345);
271   let - = Deposit(accId1, 200) in skip;
272
273   PrintAccount(accId1);
274
275   ReturnCard();
276   RemoveCard(card1);
277   RemoveCard(card2);
278 );
279

```

280 | **end** ATM

---



# The code-generated ATM model

This appendix contains the code-generated version of the ATM model in appendix A.

```
1 package atm;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class ATM implements java.io.Serializable {
11     /* @ spec_public @ */
12
13     private static atm.ATMTypes.St St =
14         new atm.ATMTypes.St(SetUtil.set(), null, false, MapUtil.map());
15     /* @ public ghost static boolean invChecksOn = true; @ */
16
17     private ATM() {}
18
19     public static Tuple GetStatus() {
20
21         if (!(Utils.equals(Utils.copy(St.get_currentCard()), null))) {
22             if (St.get_pinOk()) {
23                 Tuple ret_1 = Tuple.mk_(false, "transaction_in_progress.");
24                 /* @ assert (V2J.isTup(ret_1, 2) && Utils.is_bool(V2J.field(ret_1, 0))
25                     && Utils.is_(V2J.field(ret_1, 1), String.class)); @ */
26
27                 return Utils.copy(ret_1);
28             } else {
29                 Tuple ret_2 = Tuple.mk_(false, "debit_card_inserted._Awaiting_pin_
30                     code.");
31                 /* @ assert (V2J.isTup(ret_2, 2) && Utils.is_bool(V2J.field(ret_2, 0))
32                     && Utils.is_(V2J.field(ret_2, 1), String.class)); @ */
33
34                 return Utils.copy(ret_2);
35             }
36         } else {
37             Tuple ret_3 = Tuple.mk_(true, "no_debit_card_is_currently_inserted_
38                 into_the_machine.");
39         }
40     }
41 }
```

## Appendix B. The code-generated ATM model

```

37      //@ assert (V2J.isTup(ret_3,2) && Utils.is_bool(V2J.field(ret_3,0)) &&
        Utils.is_(V2J.field(ret_3,1),String.class));
38
39      return Utils.copy(ret_3);
40  }
41  }
42  //@ requires pre_OpenAccount(cards,id,St);
43  //@ ensures post_OpenAccount(cards,id,\old(St.copy()),St);
44
45  public static void OpenAccount(final VDMSet cards, final Number id) {
46
47      //@ assert (V2J.isSet(cards) && (\forallall int i; 0 <= i && i < V2J.size(
        cards); Utils.is_(V2J.get(cards,i),atm.ATMtypes.Card.class));
48
49      //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
50
51      //@ assert St != null;
52
53      St.set_accounts(
54          MapUtil.munion(
55              Utils.copy(St.get_accounts()),
56              MapUtil.map(new Maplet(id, new atm.ATMtypes.Account(cards, 0.0))
57                  ));
58  }
59  //@ requires pre_AddCard(c,St);
60  //@ ensures post_AddCard(c,\old(St.copy()),St);
61
62  public static void AddCard(final atm.ATMtypes.Card c) {
63
64      //@ assert Utils.is_(c,atm.ATMtypes.Card.class);
65
66      //@ assert St != null;
67
68      St.set_validCards(SetUtil.union(Utils.copy(St.get_validCards()), SetUtil
69          .set(Utils.copy(c))));
70  }
71  //@ requires pre_RemoveCard(c,St);
72  //@ ensures post_RemoveCard(c,\old(St.copy()),St);
73
74  public static void RemoveCard(final atm.ATMtypes.Card c) {
75
76      //@ assert Utils.is_(c,atm.ATMtypes.Card.class);
77
78      //@ assert St != null;
79
80      St.set_validCards(SetUtil.diff(Utils.copy(St.get_validCards()), SetUtil
81          .set(Utils.copy(c))));
82  }
83  //@ requires pre_InsertCard(c,St);
84  //@ ensures post_InsertCard(c,\result,\old(St.copy()),St);
85
86  public static Object InsertCard(final atm.ATMtypes.Card c) {
87
88      //@ assert Utils.is_(c,atm.ATMtypes.Card.class);
89
90      if (SetUtil.inSet(c, Utils.copy(St.get_validCards()))) {
91          //@ assert St != null;
92
93          St.set_currentCard(Utils.copy(c));

```

## Appendix B. The code-generated ATM model

```

92     Object ret_4 = atm.quotes.AcceptQuote.getInstance();
93     //@ assert (Utils.is_(ret_4, atm.quotes.AcceptQuote.class) || Utils.is_
        (ret_4, atm.quotes.BusyQuote.class) || Utils.is_(ret_4, atm.quotes.
        RejectQuote.class));
94
95     return ret_4;
96
97 } else if (!(Utils.equals(Utils.copy(St.get_currentCard()), null))) {
98     Object ret_5 = atm.quotes.BusyQuote.getInstance();
99     //@ assert (Utils.is_(ret_5, atm.quotes.AcceptQuote.class) || Utils.is_
        (ret_5, atm.quotes.BusyQuote.class) || Utils.is_(ret_5, atm.quotes.
        RejectQuote.class));
100
101     return ret_5;
102
103 } else {
104     Object ret_6 = atm.quotes.RejectQuote.getInstance();
105     //@ assert (Utils.is_(ret_6, atm.quotes.AcceptQuote.class) || Utils.is_
        (ret_6, atm.quotes.BusyQuote.class) || Utils.is_(ret_6, atm.quotes.
        RejectQuote.class));
106
107     return ret_6;
108 }
109 }
110
111 public static void Display(final String msg) {
112
113     //@ assert Utils.is_(msg, String.class);
114
115     IO.println(msg);
116 }
117
118 public static void NotifyUser(final Object outcome) {
119
120     //@ assert (Utils.is_(outcome, atm.quotes.AcceptQuote.class) || Utils.is_
        (outcome, atm.quotes.BusyQuote.class) || Utils.is_(outcome, atm.quotes.
        .RejectQuote.class));
121
122     if (Utils.equals(outcome, atm.quotes.AcceptQuote.getInstance())) {
123         Display("Card_accepted");
124     } else if (Utils.equals(outcome, atm.quotes.BusyQuote.getInstance())) {
125         Display("Another_card_has_already_been_inserted");
126     } else {
127         if (Utils.equals(outcome, atm.quotes.RejectQuote.getInstance())) {
128             Display("Unknown_card");
129         } else {
130             throw new RuntimeException("ERROR_statement_reached");
131         }
132     }
133 }
134 //@ requires pre_EnterPin(pin, St);
135
136 public static void EnterPin(final Number pin) {
137
138     //@ assert (Utils.is_nat(pin) && inv_ATM_Pin(pin));
139
140     //@ assert St != null;
141
142     St.set_pinOk(Utils.equals(St.get_currentCard().get_pin(), pin));
143 }

```

## Appendix B. The code-generated ATM model

```

144  // @ requires pre_ReturnCard(St);
145  // @ ensures post_ReturnCard(\old(St.copy()), St);
146
147  public static void ReturnCard() {
148
149      atm.ATMtypes.Card atomicTmp_1 = null;
150      // @ assert ((atomicTmp_1 == null) || Utils.is_(atomicTmp_1, atm.ATMtypes.
          Card.class));
151
152      Boolean atomicTmp_2 = false;
153      // @ assert Utils.is_bool(atomicTmp_2);
154
155      {
156          /* Start of atomic statement */
157          // @ set invChecksOn = false;
158
159          // @ assert St != null;
160
161          St.set_currentCard(Utils.copy(atomicTmp_1));
162
163          // @ assert St != null;
164
165          St.set_pinOk(atomicTmp_2);
166
167          // @ set invChecksOn = true;
168
169          // @ assert St.valid();
170
171      } /* End of atomic statement */
172  }
173  // @ requires pre_Withdraw(id, amount, St);
174  // @ ensures post_Withdraw(id, amount, \result, \old(St.copy()), St);
175
176  public static Number Withdraw(final Number id, final Number amount) {
177
178      // @ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
179
180      // @ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
181
182      final Number newBalance =
183          ((atm.ATMtypes.Account) Utils.get(St.accounts, id)).get_balance().
              doubleValue()
184          - amount.longValue();
185      // @ assert Utils.is_real(newBalance);
186
187      {
188          VDMMap stateDes_1 = St.get_accounts();
189
190          atm.ATMtypes.Account stateDes_2 = ((atm.ATMtypes.Account) Utils.get(
              stateDes_1, id));
191
192          // @ assert stateDes_2 != null;
193
194          stateDes_2.set_balance(newBalance);
195          // @ assert (V2J.isMap(stateDes_1) && (\forall int i; 0 <= i && i < V2J
              .size(stateDes_1); (Utils.is_nat(V2J.getDom(stateDes_1, i)) &&
              inv_ATM_AccountId(V2J.getDom(stateDes_1, i))) && Utils.is_(V2J.
              getRng(stateDes_1, i), atm.ATMtypes.Account.class)));
196
197          // @ assert Utils.is_(St, atm.ATMtypes.St.class);

```

## Appendix B. The code-generated ATM model

```

198
199     //@ assert St.valid();
200
201     Number ret_7 = newBalance;
202     //@ assert Utils.is_real(ret_7);
203
204     return ret_7;
205 }
206 }
207 //@ requires pre_Deposit(id,amount,St);
208 //@ ensures post_Deposit(id,amount,\result,\old(St.copy()),St);
209
210 public static Number Deposit(final Number id, final Number amount) {
211
212     //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
213
214     //@ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
215
216     final Number newBalance =
217         ((atm.ATMtypes.Account) Utils.get(St.accounts, id)).get_balance().
218         doubleValue()
219         + amount.longValue();
220     //@ assert Utils.is_real(newBalance);
221
222     {
223         VDMMMap stateDes_3 = St.get_accounts();
224
225         atm.ATMtypes.Account stateDes_4 = ((atm.ATMtypes.Account) Utils.get(
226             stateDes_3, id));
227
228         //@ assert stateDes_4 != null;
229
230         stateDes_4.set_balance(newBalance);
231         //@ assert (V2J.isMap(stateDes_3) && (\forall int i; 0 <= i && i < V2J
232             .size(stateDes_3); (Utils.is_nat(V2J.getDom(stateDes_3,i)) &&
233             inv_ATM_AccountId(V2J.getDom(stateDes_3,i)) && Utils.is_(V2J.
234             getRng(stateDes_3,i),atm.ATMtypes.Account.class))););
235
236         //@ assert Utils.is_(St,atm.ATMtypes.St.class);
237
238         //@ assert St.valid();
239
240         Number ret_8 = newBalance;
241         //@ assert Utils.is_real(ret_8);
242
243         return ret_8;
244     }
245 }
246
247 public static void PrintAccount(final Number id) {
248
249     //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
250
251     final Number balance = ((atm.ATMtypes.Account) Utils.get(St.accounts, id
252     )).get_balance();
253     //@ assert Utils.is_real(balance);
254
255     IO.printf("Balance_is_for_account_%s_is_%s\n", SeqUtil.seq(id, balance))
256         ;
257 }

```

## Appendix B. The code-generated ATM model

```
251
252 public static Number GetCurrentCardId() {
253
254     if (!(Utils.equals(Utils.copy(St.get_currentCard()), null))) {
255         Number ret_9 = St.get_currentCard().get_id();
256         //@ assert ((ret_9 == null) || Utils.is_nat(ret_9));
257
258         return ret_9;
259
260     } else {
261         Number ret_10 = null;
262         //@ assert ((ret_10 == null) || Utils.is_nat(ret_10));
263
264         return ret_10;
265     }
266 }
267
268 public static Number TestCurrentCardId() {
269
270     final Number id = GetCurrentCardId();
271     //@ assert ((id == null) || Utils.is_nat(id));
272
273     Number ret_11 = id;
274     //@ assert ((ret_11 == null) || Utils.is_nat(ret_11));
275
276     return ret_11;
277 }
278
279 public static Number TestStatus() {
280
281     final Number accId = 1L;
282     //@ assert Utils.is_nat1(accId);
283
284     final atm.ATMtypes.Card c1 = new atm.ATMtypes.Card(1L, 1234L);
285     //@ assert Utils.is_(c1, atm.ATMtypes.Card.class);
286
287     {
288         AddCard(Utils.copy(c1));
289         OpenAccount(SetUtil.set(new atm.ATMtypes.Card(1L, 1234L)), accId);
290         {
291             final Tuple status = GetStatus();
292             //@ assert (V2J.isTup(status,2) && Utils.is_bool(V2J.field(status,0)
293                 ) && Utils.is_(V2J.field(status,1), String.class));
294
295             final Boolean awaitingCard = ((Boolean) status.get(0));
296             //@ assert Utils.is_bool(awaitingCard);
297
298             final String msg = SeqUtil.toStr(status.get(1));
299             //@ assert Utils.is_(msg, String.class);
300
301             {
302                 IO.println("Message:_" + msg);
303                 Boolean andResult_8 = false;
304                 //@ assert Utils.is_bool(andResult_8);
305
306                 if (awaitingCard) {
307                     if (Utils.equals(atm.quotes.AcceptQuote.getInstance(),
308                         InsertCard(Utils.copy(c1)))) {
309                         andResult_8 = true;
310                         //@ assert Utils.is_bool(andResult_8);
```



## Appendix B. The code-generated ATM model

```

309     }
310     }
311 }
312
313     if (andResult_8) {
314         NotifyUser(atm.quotes.AcceptQuote.getInstance());
315         EnterPin(1234L);
316         return Deposit(accId, 100L);
317     }
318 }
319 }
320
321     Number ret_12 = 0L;
322     //@ assert Utils.is_real(ret_12);
323
324     return ret_12;
325 }
326 }
327
328 public static Number TestWithdraw() {
329
330     final Number accId = 1L;
331     //@ assert Utils.is_nat1(accId);
332
333     final Number cardId = 1L;
334     //@ assert Utils.is_nat1(cardId);
335
336     final Number pin = 1234L;
337     //@ assert Utils.is_nat1(pin);
338
339     final atm.ATMtypes.Card c1 = new atm.ATMtypes.Card(cardId, pin);
340     //@ assert Utils.is_(c1, atm.ATMtypes.Card.class);
341
342     {
343         AddCard(Utils.copy(c1));
344         OpenAccount(SetUtil.set(new atm.ATMtypes.Card(1L, 1234L)), accId);
345         if (Utils.equals(InsertCard(Utils.copy(c1)), atm.quotes.AcceptQuote.
346             getInstance())) {
347             EnterPin(pin);
348             {
349                 final Number expense = 600L;
350                 //@ assert Utils.is_nat1(expense);
351
352                 final Number profit = 100L;
353                 //@ assert Utils.is_nat1(profit);
354
355                 {
356                     final Number amount = expense.longValue() - profit.longValue();
357                     //@ assert Utils.is_nat1(amount);
358
359                     return Withdraw(accId, amount);
360                 }
361             }
362
363             throw new RuntimeException("ERROR_statement_reached");
364         }
365     }
366
367     public static Number TestTotalBalance() {

```

## Appendix B. The code-generated ATM model

```
368
369     final atm.ATMtypes.Card card1 = new atm.ATMtypes.Card(1L, 1234L);
370     //@ assert Utils.is_(card1,atm.ATMtypes.Card.class);
371
372     final atm.ATMtypes.Card card2 = new atm.ATMtypes.Card(2L, 5678L);
373     //@ assert Utils.is_(card2,atm.ATMtypes.Card.class);
374
375     final atm.ATMtypes.Account ac1 =
376         new atm.ATMtypes.Account(SetUtil.set(Utils.copy(card1)), 1000L);
377     //@ assert Utils.is_(ac1,atm.ATMtypes.Account.class);
378
379     final atm.ATMtypes.Account ac2 = new atm.ATMtypes.Account(SetUtil.set(
380         Utils.copy(card2)), 500L);
381     //@ assert Utils.is_(ac2,atm.ATMtypes.Account.class);
382
383     return TotalBalance(SetUtil.set(Utils.copy(ac1), Utils.copy(ac2)));
384 }
385
386 public static void TestScenario() {
387
388     final Number accId1 = 1L;
389     //@ assert (Utils.is_nat(accId1) && inv_ATM_AccountId(accId1));
390
391     final Number pin1 = 1234L;
392     //@ assert Utils.is_nat1(pin1);
393
394     final atm.ATMtypes.Card card1 = new atm.ATMtypes.Card(1L, pin1);
395     //@ assert Utils.is_(card1,atm.ATMtypes.Card.class);
396
397     final Number pin2 = 2345L;
398     //@ assert Utils.is_nat1(pin2);
399
400     final atm.ATMtypes.Card card2 = new atm.ATMtypes.Card(2L, pin2);
401     //@ assert Utils.is_(card2,atm.ATMtypes.Card.class);
402
403     {
404         AddCard(Utils.copy(card1));
405         AddCard(Utils.copy(card2));
406         OpenAccount(SetUtil.set(Utils.copy(card1), Utils.copy(card2)), accId1)
407         ;
408         {
409             final Object ignorePattern_1 = InsertCard(Utils.copy(card2));
410             //@ assert (Utils.is_(ignorePattern_1,atm.quotes.AcceptQuote.class)
411                 || Utils.is_(ignorePattern_1,atm.quotes.BusyQuote.class) ||
412                 Utils.is_(ignorePattern_1,atm.quotes.RejectQuote.class));
413
414             /* skip */
415         }
416
417         PrintAccount(accId1);
418         EnterPin(2345L);
419         {
420             final Number ignorePattern_2 = Deposit(accId1, 200L);
421             //@ assert Utils.is_real(ignorePattern_2);
422
423             /* skip */
424         }
425
426         PrintAccount(accId1);
427         ReturnCard();
428     }
429 }
```

## Appendix B. The code-generated ATM model

```

424         RemoveCard(Utils.copy(card1));
425         RemoveCard(Utils.copy(card2));
426     }
427 }
428 /*@ pure @*/
429
430 public static Number TotalBalance(final VDMSet acs) {
431
432     //@ assert (V2J.isSet(acs) && (\forallall int i; 0 <= i && i < V2J.size(acs)
433         ); Utils.is_(V2J.get(acs,i), atm.ATMtypes.Account.class));
434
435     if (Utils.empty(acs)) {
436         Number ret_13 = 0L;
437         //@ assert Utils.is_real(ret_13);
438
439         return ret_13;
440     } else {
441         Number letBeStExp_1 = null;
442         atm.ATMtypes.Account a = null;
443
444         Boolean success_1 = false;
445         //@ assert Utils.is_bool(success_1);
446
447         VDMSet set_1 = Utils.copy(acs);
448         //@ assert (V2J.isSet(set_1) && (\forallall int i; 0 <= i && i < V2J.size
449             (set_1); Utils.is_(V2J.get(set_1,i), atm.ATMtypes.Account.class));
450
451         for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() &&
452             !(success_1); ) {
453             a = ((atm.ATMtypes.Account) iterator_1.next());
454             success_1 = true;
455             //@ assert Utils.is_bool(success_1);
456
457         }
458         if (!(success_1)) {
459             throw new RuntimeException("Let_Be_St_found_no_applicable_bindings")
460                 ;
461         }
462
463         letBeStExp_1 =
464             a.get_balance().doubleValue()
465             + TotalBalance(SetUtil.diff(Utils.copy(acs), SetUtil.set(Utils
466                 .copy(a))))
467             .doubleValue();
468         //@ assert Utils.is_real(letBeStExp_1);
469
470         Number ret_14 = letBeStExp_1;
471         //@ assert Utils.is_real(ret_14);
472
473         return ret_14;
474     }
475 }
476 /*@ pure @*/
477
478 public static Number TotalBalanceMes(final VDMSet acs) {
479
480     //@ assert (V2J.isSet(acs) && (\forallall int i; 0 <= i && i < V2J.size(acs)
481         ); Utils.is_(V2J.get(acs,i), atm.ATMtypes.Account.class));
482

```

## Appendix B. The code-generated ATM model

```

478     Number ret_15 = acs.size();
479     //@ assert Utils.is_nat(ret_15);
480
481     return ret_15;
482 }
483 /*@ pure @*/
484
485 public static Boolean pre_OpenAccount(
486     final VDMSet cards, final Number id, final atm.ATMtypes.St St) {
487
488     //@ assert (V2J.isSet(cards) && (\forallall int i; 0 <= i && i < V2J.size(
489         cards); Utils.is_(V2J.get(cards,i),atm.ATMtypes.Card.class)));
490
491     //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
492
493     //@ assert Utils.is_(St,atm.ATMtypes.St.class);
494
495     Boolean ret_16 = !(SetUtil.inSet(id, MapUtil.dom(Utils.copy(St.
496         get_accounts()))));
497     //@ assert Utils.is_bool(ret_16);
498
499     return ret_16;
500 }
501 /*@ pure @*/
502
503 public static Boolean post_OpenAccount(
504     final VDMSet cards, final Number id, final atm.ATMtypes.St _St, final
505     atm.ATMtypes.St St) {
506
507     //@ assert (V2J.isSet(cards) && (\forallall int i; 0 <= i && i < V2J.size(
508         cards); Utils.is_(V2J.get(cards,i),atm.ATMtypes.Card.class)));
509
510     //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
511
512     //@ assert Utils.is_(_St,atm.ATMtypes.St.class);
513
514     //@ assert Utils.is_(St,atm.ATMtypes.St.class);
515
516     Boolean andResult_1 = false;
517     //@ assert Utils.is_bool(andResult_1);
518
519     if (SetUtil.inSet(id, MapUtil.dom(Utils.copy(St.get_accounts())))) {
520         if (Utils.equals((atm.ATMtypes.Account) Utils.get(St.accounts, id)).
521             get_balance(), 0L)) {
522             andResult_1 = true;
523             //@ assert Utils.is_bool(andResult_1);
524         }
525     }
526
527     Boolean ret_17 = andResult_1;
528     //@ assert Utils.is_bool(ret_17);
529
530     return ret_17;
531 }
532 /*@ pure @*/
533
534 public static Boolean pre_AddCard(final atm.ATMtypes.Card c, final atm.
535     ATMtypes.St St) {

```

## Appendix B. The code-generated ATM model

```
532     //@ assert Utils.is_(c, atm.ATMtypes.Card.class);
533
534     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
535
536     Boolean ret_18 = !(SetUtil.inSet(c, Utils.copy(St.get_validCards())));
537     //@ assert Utils.is_bool(ret_18);
538
539     return ret_18;
540 }
541 /*@ pure */
542
543 public static Boolean post_AddCard(
544     final atm.ATMtypes.Card c, final atm.ATMtypes.St _St, final atm.
545     ATMtypes.St St) {
546
547     //@ assert Utils.is_(c, atm.ATMtypes.Card.class);
548
549     //@ assert Utils.is_(_St, atm.ATMtypes.St.class);
550
551     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
552
553     Boolean ret_19 = SetUtil.inSet(c, Utils.copy(St.get_validCards()));
554     //@ assert Utils.is_bool(ret_19);
555
556     return ret_19;
557 }
558 /*@ pure */
559
560 public static Boolean pre_RemoveCard(final atm.ATMtypes.Card c, final atm.
561     ATMtypes.St St) {
562
563     //@ assert Utils.is_(c, atm.ATMtypes.Card.class);
564
565     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
566
567     Boolean ret_20 = SetUtil.inSet(c, Utils.copy(St.get_validCards()));
568     //@ assert Utils.is_bool(ret_20);
569
570     return ret_20;
571 }
572 /*@ pure */
573
574 public static Boolean post_RemoveCard(
575     final atm.ATMtypes.Card c, final atm.ATMtypes.St _St, final atm.
576     ATMtypes.St St) {
577
578     //@ assert Utils.is_(c, atm.ATMtypes.Card.class);
579
580     //@ assert Utils.is_(_St, atm.ATMtypes.St.class);
581
582     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
583
584     Boolean ret_21 = !(SetUtil.inSet(c, Utils.copy(St.get_validCards())));
585     //@ assert Utils.is_bool(ret_21);
586
587     return ret_21;
588 }
589 /*@ pure */
590
591 public static Boolean pre_InsertCard(final atm.ATMtypes.Card c, final atm.
```

## Appendix B. The code-generated ATM model

```

589     ATMtypes.St St) {
590     //@ assert Utils.is_(c, atm.ATMtypes.Card.class);
591
592     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
593
594     Boolean ret_22 = Utils.equals(Utils.copy(St.get_currentCard()), null);
595     //@ assert Utils.is_bool(ret_22);
596
597     return ret_22;
598 }
599 /*@ pure @*/
600
601 public static Boolean post_InsertCard(
602     final atm.ATMtypes.Card c,
603     final Object RESULT,
604     final atm.ATMtypes.St _St,
605     final atm.ATMtypes.St St) {
606
607     //@ assert Utils.is_(c, atm.ATMtypes.Card.class);
608
609     //@ assert (Utils.is_(RESULT, atm.quotes.AcceptQuote.class) || Utils.is_(
610         RESULT, atm.quotes.BusyQuote.class) || Utils.is_(RESULT, atm.quotes.
611         RejectQuote.class));
612
613     //@ assert Utils.is_(_St, atm.ATMtypes.St.class);
614
615     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
616
617     if (Utils.equals(RESULT, atm.quotes.AcceptQuote.getInstance())) {
618         Boolean ret_23 = Utils.equals(Utils.copy(St.get_currentCard()), c);
619         //@ assert Utils.is_bool(ret_23);
620
621         return ret_23;
622     } else {
623         if (Utils.equals(RESULT, atm.quotes.BusyQuote.getInstance())) {
624             Boolean ret_24 =
625                 Utils.equals(Utils.copy(St.get_currentCard()), Utils.copy(_St.
626                     get_currentCard()));
627             //@ assert Utils.is_bool(ret_24);
628
629             return ret_24;
630         } else {
631             Boolean ret_25 = Utils.equals(Utils.copy(St.get_currentCard()), null
632             );
633             //@ assert Utils.is_bool(ret_25);
634
635             return ret_25;
636         }
637     }
638 }
639 /*@ pure @*/
640
641 public static Boolean pre_EnterPin(final Number pin, final atm.ATMtypes.St
642     St) {
643
644     //@ assert (Utils.is_nat(pin) && inv_ATM_Pin(pin));

```

## Appendix B. The code-generated ATM model

```

643     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
644
645     Boolean ret_26 = !(Utils.equals(Utils.copy(St.get_currentCard()), null))
        ;
646     //@ assert Utils.is_bool(ret_26);
647
648     return ret_26;
649 }
650 /*@ pure @*/
651
652 public static Boolean pre_ReturnCard(final atm.ATMtypes.St St) {
653
654     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
655
656     Boolean ret_27 = !(Utils.equals(Utils.copy(St.get_currentCard()), null))
        ;
657     //@ assert Utils.is_bool(ret_27);
658
659     return ret_27;
660 }
661 /*@ pure @*/
662
663 public static Boolean post_ReturnCard(final atm.ATMtypes.St _St, final atm
        .ATMtypes.St St) {
664
665     //@ assert Utils.is_(_St, atm.ATMtypes.St.class);
666
667     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
668
669     Boolean andResult_2 = false;
670     //@ assert Utils.is_bool(andResult_2);
671
672     if (Utils.equals(Utils.copy(St.get_currentCard()), null)) {
673         if (!(St.get_pinOk())) {
674             andResult_2 = true;
675             //@ assert Utils.is_bool(andResult_2);
676
677         }
678     }
679
680     Boolean ret_28 = andResult_2;
681     //@ assert Utils.is_bool(ret_28);
682
683     return ret_28;
684 }
685 /*@ pure @*/
686
687 public static Boolean pre_Withdraw(
688     final Number id, final Number amount, final atm.ATMtypes.St St) {
689
690     //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
691
692     //@ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
693
694     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
695
696     Boolean andResult_3 = false;
697     //@ assert Utils.is_bool(andResult_3);
698
699     if (SetUtil.inSet(Utils.copy(St.get_currentCard()), Utils.copy(St.

```

## Appendix B. The code-generated ATM model

```

700         get_validCards())) {
701     Boolean andResult_4 = false;
702     //@ assert Utils.is_bool(andResult_4);
703     if (St.get_pinOk()) {
704         Boolean andResult_5 = false;
705         //@ assert Utils.is_bool(andResult_5);
706
707         if (SetUtil.inSet(
708             Utils.copy(St.get_currentCard()),
709             Utils.copy((atm.ATMtypes.Account) Utils.get(St.accounts, id)).
710                 get_cards())) {
711             if (SetUtil.inSet(id, MapUtil.dom(Utils.copy(St.get_accounts()))))
712                 {
713                 andResult_5 = true;
714                 //@ assert Utils.is_bool(andResult_5);
715             }
716         }
717         if (andResult_5) {
718             andResult_4 = true;
719             //@ assert Utils.is_bool(andResult_4);
720         }
721     }
722 }
723
724 if (andResult_4) {
725     andResult_3 = true;
726     //@ assert Utils.is_bool(andResult_3);
727 }
728 }
729
730 Boolean ret_29 = andResult_3;
731 //@ assert Utils.is_bool(ret_29);
732
733 return ret_29;
734 }
735
736 /*@ pure @*/
737
738 public static Boolean post_Withdraw(
739     final Number id,
740     final Number amount,
741     final Number RESULT,
742     final atm.ATMtypes.St _St,
743     final atm.ATMtypes.St St) {
744
745     //@ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
746
747     //@ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
748
749     //@ assert Utils.is_real(RESULT);
750
751     //@ assert Utils.is_(_St, atm.ATMtypes.St.class);
752
753     //@ assert Utils.is_(St, atm.ATMtypes.St.class);
754
755     final atm.ATMtypes.Account accountPre =
756         Utils.copy((atm.ATMtypes.Account) Utils.get(_St.accounts, id));

```



## Appendix B. The code-generated ATM model

```

757 // @ assert Utils.is_(accountPre, atm.ATMtypes.Account.class);
758
759 final atm.ATMtypes.Account accountPost =
760     Utils.copy((atm.ATMtypes.Account) Utils.get(St.accounts, id));
761 // @ assert Utils.is_(accountPost, atm.ATMtypes.Account.class);
762
763 Boolean andResult_6 = false;
764 // @ assert Utils.is_bool(andResult_6);
765
766 if (Utils.equals(
767     accountPre.get_balance(), accountPost.get_balance().doubleValue() +
768     amount.longValue())) {
769     if (Utils.equals(accountPost.get_balance(), RESULT)) {
770         andResult_6 = true;
771         // @ assert Utils.is_bool(andResult_6);
772     }
773 }
774
775 Boolean ret_30 = andResult_6;
776 // @ assert Utils.is_bool(ret_30);
777
778 return ret_30;
779 }
780 /* @ pure @ */
781
782 public static Boolean pre_Deposit(
783     final Number id, final Number amount, final atm.ATMtypes.St St) {
784
785     // @ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
786
787     // @ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
788
789     // @ assert Utils.is_(St, atm.ATMtypes.St.class);
790
791     Boolean ret_31 = pre-Withdraw(id, amount, Utils.copy(St));
792     // @ assert Utils.is_bool(ret_31);
793
794     return ret_31;
795 }
796 /* @ pure @ */
797
798 public static Boolean post_Deposit(
799     final Number id,
800     final Number amount,
801     final Number RESULT,
802     final atm.ATMtypes.St _St,
803     final atm.ATMtypes.St St) {
804
805     // @ assert (Utils.is_nat(id) && inv_ATM_AccountId(id));
806
807     // @ assert (Utils.is_nat1(amount) && inv_ATM_Amount(amount));
808
809     // @ assert Utils.is_real(RESULT);
810
811     // @ assert Utils.is_(_St, atm.ATMtypes.St.class);
812
813     // @ assert Utils.is_(St, atm.ATMtypes.St.class);
814
815     final atm.ATMtypes.Account accountPre =

```

## Appendix B. The code-generated ATM model

```
816         Utils.copy((atm.ATMtypes.Account) Utils.get(_St.accounts, id));
817     //@ assert Utils.is_(accountPre,atm.ATMtypes.Account.class);
818
819     final atm.ATMtypes.Account accountPost =
820         Utils.copy((atm.ATMtypes.Account) Utils.get(St.accounts, id));
821     //@ assert Utils.is_(accountPost,atm.ATMtypes.Account.class);
822
823     Boolean andResult_7 = false;
824     //@ assert Utils.is_bool(andResult_7);
825
826     if (Utils.equals(
827         accountPre.get_balance().doubleValue() + amount.longValue(),
828         accountPost.get_balance())) {
829         if (Utils.equals(accountPost.get_balance(), RESULT)) {
830             andResult_7 = true;
831             //@ assert Utils.is_bool(andResult_7);
832         }
833     }
834
835     Boolean ret_32 = andResult_7;
836     //@ assert Utils.is_bool(ret_32);
837
838     return ret_32;
839 }
840
841 public String toString() {
842
843     return "ATM{" + "St_:=_" + Utils.toString(St) + "}";
844 }
845
846 /*@ pure @*/
847 /*@ helper @*/
848
849 public static Boolean inv_ATM_Pin(final Object check_p) {
850
851     Number p = ((Number) check_p);
852
853     Boolean andResult_9 = false;
854
855     if (0L <= p.longValue()) {
856         if (p.longValue() <= 9999L) {
857             andResult_9 = true;
858         }
859     }
860
861     return andResult_9;
862 }
863
864 /*@ pure @*/
865 /*@ helper @*/
866
867 public static Boolean inv_ATM_AccountId(final Object check_id) {
868
869     Number id = ((Number) check_id);
870
871     return id.longValue() > 0L;
872 }
873
874 /*@ pure @*/
```

## Appendix B. The code-generated ATM model

```

875  /*@ helper @*/
876
877  public static Boolean inv_ATM_Amount(final Object check_a) {
878
879      Number a = ((Number) check_a);
880
881      return a.longValue() < 2000L;
882  }
883  }

```

---

```

1  package atm.ATMtypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class St implements Record, java.io.Serializable {
11     public VDMSet validCards;
12     public atm.ATMtypes.Card currentCard;
13     public Boolean pinOk;
14     public VDMMap accounts;
15     //@ public instance invariant atm.ATM.invChecksOn ==> inv_St(validCards,
16         currentCard, pinOk, accounts);
17
18     public St(
19         final VDMSet _validCards,
20         final atm.ATMtypes.Card _currentCard,
21         final Boolean _pinOk,
22         final VDMMap _accounts) {
23
24         //@ assert (V2J.isSet(_validCards) && (\forallall int i; 0 <= i && i < V2J.
25             size(_validCards); Utils.is_(V2J.get(_validCards,i), atm.ATMtypes.
26                 Card.class)));
27
28         //@ assert ((_currentCard == null) || Utils.is_(_currentCard, atm.
29             ATMtypes.Card.class));
30
31         //@ assert Utils.is_bool(_pinOk);
32
33         //@ assert (V2J.isMap(_accounts) && (\forallall int i; 0 <= i && i < V2J.
34             size(_accounts); (Utils.is_nat(V2J.getDom(_accounts,i)) &&
35                 inv_ATM_AccountId(V2J.getDom(_accounts,i)) && Utils.is_(V2J.getRng(
36                     _accounts,i), atm.ATMtypes.Account.class)));
37
38         validCards = _validCards != null ? Utils.copy(_validCards) : null;
39         //@ assert (V2J.isSet(validCards) && (\forallall int i; 0 <= i && i < V2J.
40             size(validCards); Utils.is_(V2J.get(validCards,i), atm.ATMtypes.Card.
41                 class)));
42
43         currentCard = _currentCard != null ? Utils.copy(_currentCard) : null;
44         //@ assert ((currentCard == null) || Utils.is_(currentCard, atm.ATMtypes.
45             Card.class));
46
47         pinOk = _pinOk;
48         //@ assert Utils.is_bool(pinOk);
49
50         accounts = _accounts != null ? Utils.copy(_accounts) : null;

```

## Appendix B. The code-generated ATM model

```

41      //@ assert (V2J.isMap(accounts) && (\forall int i; 0 <= i && i < V2J.
        size(accounts); (Utils.is_nat(V2J.getDom(accounts,i)) &&
        inv_ATM_AccountId(V2J.getDom(accounts,i))) && Utils.is_(V2J.getRng(
        accounts,i),atm.ATMtypes.Account.class)));
42
43    }
44    /*@ pure @*/
45
46    public boolean equals(final Object obj) {
47
48      if (!(obj instanceof atm.ATMtypes.St)) {
49        return false;
50      }
51
52      atm.ATMtypes.St other = ((atm.ATMtypes.St) obj);
53
54      return (Utils.equals(validCards, other.validCards))
55        && (Utils.equals(currentCard, other.currentCard))
56        && (Utils.equals(pinOk, other.pinOk))
57        && (Utils.equals(accounts, other.accounts));
58    }
59    /*@ pure @*/
60
61    public int hashCode() {
62
63      return Utils.hashCode(validCards, currentCard, pinOk, accounts);
64    }
65    /*@ pure @*/
66
67    public atm.ATMtypes.St copy() {
68
69      return new atm.ATMtypes.St(validCards, currentCard, pinOk, accounts);
70    }
71    /*@ pure @*/
72
73    public String toString() {
74
75      return "mk_ATM'St" + Utils.formatFields(validCards, currentCard, pinOk,
        accounts);
76    }
77    /*@ pure @*/
78
79    public VDMSet get_validCards() {
80
81      VDMSet ret_37 = validCards;
82      //@ assert atm.ATM.invChecksOn ==> ((V2J.isSet(ret_37) && (\forall int i
        ; 0 <= i && i < V2J.size(ret_37); Utils.is_(V2J.get(ret_37,i),atm.
        ATMtypes.Card.class))););
83
84      return ret_37;
85    }
86
87    public void set_validCards(final VDMSet _validCards) {
88
89      //@ assert atm.ATM.invChecksOn ==> ((V2J.isSet(_validCards) && (\forall
        int i; 0 <= i && i < V2J.size(_validCards); Utils.is_(V2J.get(
        _validCards,i),atm.ATMtypes.Card.class))););
90
91      validCards = _validCards;
92      //@ assert atm.ATM.invChecksOn ==> ((V2J.isSet(validCards) && (\forall

```

## Appendix B. The code-generated ATM model

```

    int i; 0 <= i && i < V2J.size(validCards); Utils.is_(V2J.get(
    validCards,i), atm.ATMtypes.Card.class)))));
93
94 }
95 /*@ pure @*/
96
97 public atm.ATMtypes.Card get_currentCard() {
98
99     atm.ATMtypes.Card ret_38 = currentCard;
100     /*@ assert atm.ATM.invChecksOn ==> (((ret_38 == null) || Utils.is_(
        ret_38, atm.ATMtypes.Card.class)))));
101
102     return ret_38;
103 }
104
105 public void set_currentCard(final atm.ATMtypes.Card _currentCard) {
106
107     /*@ assert atm.ATM.invChecksOn ==> ((_currentCard == null) || Utils.is_(
        _currentCard, atm.ATMtypes.Card.class)))));
108
109     currentCard = _currentCard;
110     /*@ assert atm.ATM.invChecksOn ==> ((currentCard == null) || Utils.is_(
        currentCard, atm.ATMtypes.Card.class)))));
111
112 }
113 /*@ pure @*/
114
115 public Boolean get_pinOk() {
116
117     Boolean ret_39 = pinOk;
118     /*@ assert atm.ATM.invChecksOn ==> (Utils.is_bool(ret_39));
119
120     return ret_39;
121 }
122
123 public void set_pinOk(final Boolean _pinOk) {
124
125     /*@ assert atm.ATM.invChecksOn ==> (Utils.is_bool(_pinOk));
126
127     pinOk = _pinOk;
128     /*@ assert atm.ATM.invChecksOn ==> (Utils.is_bool(pinOk));
129
130 }
131 /*@ pure @*/
132
133 public VDMMap get_accounts() {
134
135     VDMMap ret_40 = accounts;
136     /*@ assert atm.ATM.invChecksOn ==> ((V2J.isMap(ret_40) && (\forallall int i
        ; 0 <= i && i < V2J.size(ret_40); (Utils.is_nat(V2J.getDom(ret_40,i)
        ) && inv_ATM_AccountId(V2J.getDom(ret_40,i))) && Utils.is_(V2J.
        getRng(ret_40,i), atm.ATMtypes.Account.class)))));
137
138     return ret_40;
139 }
140
141 public void set_accounts(final VDMMap _accounts) {
142
143     /*@ assert atm.ATM.invChecksOn ==> ((V2J.isMap(_accounts) && (\forallall
        int i; 0 <= i && i < V2J.size(_accounts); (Utils.is_nat(V2J.getDom(

```

## Appendix B. The code-generated ATM model

```

    _accounts,i)) && inv_ATM_AccountId(V2J.getDom(_accounts,i))) &&
    Utils.is_(V2J.getRng(_accounts,i), atm.ATMtypes.Account.class)));
144
145    accounts = _accounts;
146    //@ assert atm.ATM.invChecksOn ==> ((V2J.isMap(accounts) && (\forall int
        i; 0 <= i && i < V2J.size(accounts); (Utils.is_nat(V2J.getDom(
        accounts,i)) && inv_ATM_AccountId(V2J.getDom(accounts,i))) && Utils.
        is_(V2J.getRng(accounts,i), atm.ATMtypes.Account.class)))));
147
148    }
149    /*@ pure @*/
150
151    public Boolean valid() {
152
153        return true;
154    }
155    /*@ pure @*/
156    /*@ helper @*/
157
158    public static Boolean inv_St(
159        final VDMSet _validCards,
160        final atm.ATMtypes.Card _currentCard,
161        final Boolean _pinOk,
162        final VDMMap _accounts) {
163
164        Boolean success_2 = true;
165        VDMSet v = null;
166        atm.ATMtypes.Card c = null;
167        Boolean p = null;
168        VDMMap a = null;
169        v = _validCards;
170        c = _currentCard;
171        p = _pinOk;
172        a = _accounts;
173
174        if (!(success_2)) {
175            throw new RuntimeException("Record_pattern_match_failed");
176        }
177
178        Boolean andResult_10 = false;
179
180        Boolean orResult_1 = false;
181
182        Boolean orResult_2 = false;
183
184        if (p) {
185            orResult_2 = true;
186        } else {
187            orResult_2 = !(Utils.equals(c, null));
188        }
189
190        if (!(orResult_2)) {
191            orResult_1 = true;
192        } else {
193            orResult_1 = SetUtil.inSet(c, v);
194        }
195
196        if (orResult_1) {
197            Boolean forAllExpResult_1 = true;
198            VDMSet set_2 = MapUtil.dom(a);

```

## Appendix B. The code-generated ATM model

```
199     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext() &&
200         forAllExpResult_1; ) {
201         Number id1 = ((Number) iterator_2.next());
202         for (Iterator iterator_3 = set_2.iterator(); iterator_3.hasNext() &&
203             forAllExpResult_1; ) {
204             Number id2 = ((Number) iterator_3.next());
205             Boolean orResult_3 = false;
206
207             if (!(Utils.equals(id1, id2))) {
208                 orResult_3 = true;
209             } else {
210                 orResult_3 =
211                     Utils.empty(
212                         SetUtil.intersect(
213                             Utils.copy(((atm.ATMtypes.Account) Utils.get(a, id1)
214                                 ).cards),
215                             Utils.copy(((atm.ATMtypes.Account) Utils.get(a, id2)
216                                 ).cards)));
217             }
218             forAllExpResult_1 = orResult_3;
219         }
220     }
221     if (forAllExpResult_1) {
222         andResult_10 = true;
223     }
224     return andResult_10;
225 }
226
227 /*@ pure @*/
228 /*@ helper @*/
229
230 public static Boolean inv_ATM_Pin(final Object check_p) {
231     Number p = ((Number) check_p);
232
233     Boolean andResult_9 = false;
234
235     if (0L <= p.longValue()) {
236         if (p.longValue() <= 9999L) {
237             andResult_9 = true;
238         }
239     }
240
241     return andResult_9;
242 }
243
244 /*@ pure @*/
245 /*@ helper @*/
246
247 public static Boolean inv_ATM_AccountId(final Object check_id) {
248     Number id = ((Number) check_id);
249
250     return id.longValue() > 0L;
251 }
252
253 /*@ pure @*/
```

## Appendix B. The code-generated ATM model

```
255  /*@ helper @*/
256
257  public static Boolean inv_ATM_Amount(final Object check_a) {
258
259      Number a = ((Number) check_a);
260
261      return a.longValue() < 2000L;
262  }
263  }
```

```
1  package atm.ATMtypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Account implements Record, java.io.Serializable {
11     public VDMSet cards;
12     public Number balance;
13     //@ public instance invariant atm.ATM.invChecksOn ==> inv_Account(cards,
14         balance);
15
16     public Account(final VDMSet _cards, final Number _balance) {
17
18         //@ assert (V2J.isSet(_cards) && (\forallall int i; 0 <= i && i < V2J.size(
19             _cards); Utils.is_(V2J.get(_cards,i),atm.ATMtypes.Card.class)));
20
21         //@ assert Utils.is_real(_balance);
22
23         cards = _cards != null ? Utils.copy(_cards) : null;
24         //@ assert (V2J.isSet(cards) && (\forallall int i; 0 <= i && i < V2J.size(
25             cards); Utils.is_(V2J.get(cards,i),atm.ATMtypes.Card.class)));
26
27         balance = _balance;
28         //@ assert Utils.is_real(balance);
29     }
30     /*@ pure @*/
31
32     public boolean equals(final Object obj) {
33
34         if (!(obj instanceof atm.ATMtypes.Account)) {
35             return false;
36         }
37
38         atm.ATMtypes.Account other = ((atm.ATMtypes.Account) obj);
39
40         return (Utils.equals(cards, other.cards) && (Utils.equals(balance,
41             other.balance)));
42     }
43     /*@ pure @*/
44
45     public int hashCode() {
46
47         return Utils.hashCode(cards, balance);
48     }
49     /*@ pure @*/
```



## Appendix B. The code-generated ATM model

```

47
48 public atm.ATMtypes.Account copy() {
49
50     return new atm.ATMtypes.Account(cards, balance);
51 }
52 /*@ pure @*/
53
54 public String toString() {
55
56     return "mk_ATM'Account" + Utils.formatFields(cards, balance);
57 }
58 /*@ pure @*/
59
60 public VDMSet get_cards() {
61
62     VDMSet ret_35 = cards;
63     //@ assert atm.ATM.invChecksOn ==> ((V2J.isSet(ret_35) && (\forallall int i
        ; 0 <= i && i < V2J.size(ret_35); Utils.is_(V2J.get(ret_35,i), atm.
        ATMtypes.Card.class)))));
64
65     return ret_35;
66 }
67
68 public void set_cards(final VDMSet _cards) {
69
70     //@ assert atm.ATM.invChecksOn ==> ((V2J.isSet(_cards) && (\forallall int i
        ; 0 <= i && i < V2J.size(_cards); Utils.is_(V2J.get(_cards,i), atm.
        ATMtypes.Card.class)))));
71
72     cards = _cards;
73     //@ assert atm.ATM.invChecksOn ==> ((V2J.isSet(cards) && (\forallall int i;
        0 <= i && i < V2J.size(cards); Utils.is_(V2J.get(cards,i), atm.
        ATMtypes.Card.class)))));
74
75 }
76 /*@ pure @*/
77
78 public Number get_balance() {
79
80     Number ret_36 = balance;
81     //@ assert atm.ATM.invChecksOn ==> (Utils.is_real(ret_36));
82
83     return ret_36;
84 }
85
86 public void set_balance(final Number _balance) {
87
88     //@ assert atm.ATM.invChecksOn ==> (Utils.is_real(_balance));
89
90     balance = _balance;
91     //@ assert atm.ATM.invChecksOn ==> (Utils.is_real(balance));
92
93 }
94 /*@ pure @*/
95
96 public Boolean valid() {
97
98     return true;
99 }
100 /*@ pure @*/

```

## Appendix B. The code-generated ATM model

```

101  /*@ helper @*/
102
103  public static Boolean inv_Account(final VDMSet _cards, final Number
    _balance) {
104
105      return _balance.doubleValue() >= -1000L;
106  }
107
108  /*@ pure @*/
109  /*@ helper @*/
110
111  public static Boolean inv_ATM_Pin(final Object check_p) {
112
113      Number p = ((Number) check_p);
114
115      Boolean andResult_9 = false;
116
117      if (0L <= p.longValue()) {
118          if (p.longValue() <= 9999L) {
119              andResult_9 = true;
120          }
121      }
122
123      return andResult_9;
124  }
125
126  /*@ pure @*/
127  /*@ helper @*/
128
129  public static Boolean inv_ATM_AccountId(final Object check_id) {
130
131      Number id = ((Number) check_id);
132
133      return id.longValue() > 0L;
134  }
135
136  /*@ pure @*/
137  /*@ helper @*/
138
139  public static Boolean inv_ATM_Amount(final Object check_a) {
140
141      Number a = ((Number) check_a);
142
143      return a.longValue() < 2000L;
144  }
145  }

```

```

1  package atm.ATMtypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Card implements Record, java.io.Serializable {
11     public Number id;
12     public Number pin;
13

```

## Appendix B. The code-generated ATM model

```
14 public Card(final Number _id, final Number _pin) {
15
16     //@ assert Utils.is_nat(_id);
17
18     //@ assert (Utils.is_nat(_pin) && inv_ATM_Pin(_pin));
19
20     id = _id;
21     //@ assert Utils.is_nat(id);
22
23     pin = _pin;
24     //@ assert (Utils.is_nat(pin) && inv_ATM_Pin(pin));
25
26 }
27 /*@ pure @*/
28
29 public boolean equals(final Object obj) {
30
31     if (!(obj instanceof atm.ATMtypes.Card)) {
32         return false;
33     }
34
35     atm.ATMtypes.Card other = ((atm.ATMtypes.Card) obj);
36
37     return (Utils.equals(id, other.id)) && (Utils.equals(pin, other.pin));
38 }
39 /*@ pure @*/
40
41 public int hashCode() {
42
43     return Utils.hashCode(id, pin);
44 }
45 /*@ pure @*/
46
47 public atm.ATMtypes.Card copy() {
48
49     return new atm.ATMtypes.Card(id, pin);
50 }
51 /*@ pure @*/
52
53 public String toString() {
54
55     return "mk_ATM`Card" + Utils.formatFields(id, pin);
56 }
57 /*@ pure @*/
58
59 public Number get_id() {
60
61     Number ret_33 = id;
62     //@ assert atm.ATM.invChecksOn ==> (Utils.is_nat(ret_33));
63
64     return ret_33;
65 }
66
67 public void set_id(final Number _id) {
68
69     //@ assert atm.ATM.invChecksOn ==> (Utils.is_nat(_id));
70
71     id = _id;
72     //@ assert atm.ATM.invChecksOn ==> (Utils.is_nat(id));
73 }
```

## Appendix B. The code-generated ATM model

```
74     }
75     /*@ pure @*/
76
77     public Number get_pin() {
78
79         Number ret_34 = pin;
80         /*@ assert atm.ATM.invChecksOn ==> ((Utils.is_nat(ret_34) && inv_ATM_Pin
            (ret_34))) */;
81
82         return ret_34;
83     }
84
85     public void set_pin(final Number _pin) {
86
87         /*@ assert atm.ATM.invChecksOn ==> ((Utils.is_nat(_pin) && inv_ATM_Pin(
            _pin))) */;
88
89         pin = _pin;
90         /*@ assert atm.ATM.invChecksOn ==> ((Utils.is_nat(pin) && inv_ATM_Pin(
            pin))) */;
91
92     }
93     /*@ pure @*/
94
95     public Boolean valid() {
96
97         return true;
98     }
99
100    /*@ pure @*/
101    /*@ helper @*/
102
103    public static Boolean inv_ATM_Pin(final Object check_p) {
104
105        Number p = ((Number) check_p);
106
107        Boolean andResult_9 = false;
108
109        if (0L <= p.longValue()) {
110            if (p.longValue() <= 9999L) {
111                andResult_9 = true;
112            }
113        }
114
115        return andResult_9;
116    }
117
118    /*@ pure @*/
119    /*@ helper @*/
120
121    public static Boolean inv_ATM_AccountId(final Object check_id) {
122
123        Number id = ((Number) check_id);
124
125        return id.longValue() > 0L;
126    }
127
128    /*@ pure @*/
129    /*@ helper @*/
130
```

## Appendix B. The code-generated ATM model

```
131 public static Boolean inv_ATM_Amount (final Object check_a) {
132
133     Number a = ((Number) check_a);
134
135     return a.longValue() < 2000L;
136 }
137 }
```

```
1 package atm.quotes;
2
3 import org.overture.codegen.runtime.*;
4 import org.overture.codegen.vdm2jml.runtime.*;
5
6 @SuppressWarnings("all")
7 //@ nullable_by_default
8
9 final public class startQuote implements java.io.Serializable {
10     private static int hc = 0;
11     private static startQuote instance = null;
12
13     public startQuote() {
14
15         if (Utils.equals(hc, 0)) {
16             hc = super.hashCode();
17         }
18     }
19
20     public static startQuote getInstance() {
21
22         if (Utils.equals(instance, null)) {
23             instance = new startQuote();
24         }
25
26         return instance;
27     }
28
29     public int hashCode() {
30
31         return hc;
32     }
33
34     public boolean equals(final Object obj) {
35
36         return obj instanceof startQuote;
37     }
38
39     public String toString() {
40
41         return "<start>";
42     }
43 }
```

```
1 package atm.quotes;
2
3 import org.overture.codegen.runtime.*;
4 import org.overture.codegen.vdm2jml.runtime.*;
5
6 @SuppressWarnings("all")
7 //@ nullable_by_default
```

## Appendix B. The code-generated ATM model

```
8
9 final public class RejectQuote implements java.io.Serializable {
10     private static int hc = 0;
11     private static RejectQuote instance = null;
12
13     public RejectQuote() {
14
15         if (Utils.equals(hc, 0)) {
16             hc = super.hashCode();
17         }
18     }
19
20     public static RejectQuote getInstance() {
21
22         if (Utils.equals(instance, null)) {
23             instance = new RejectQuote();
24         }
25
26         return instance;
27     }
28
29     public int hashCode() {
30
31         return hc;
32     }
33
34     public boolean equals(final Object obj) {
35
36         return obj instanceof RejectQuote;
37     }
38
39     public String toString() {
40
41         return "<Reject>";
42     }
43 }
```

```
1 package atm.quotes;
2
3 import org.overture.codegen.runtime.*;
4 import org.overture.codegen.vdm2jml.runtime.*;
5
6 @SuppressWarnings("all")
7 //@ nullable_by_default
8
9 final public class AcceptQuote implements java.io.Serializable {
10     private static int hc = 0;
11     private static AcceptQuote instance = null;
12
13     public AcceptQuote() {
14
15         if (Utils.equals(hc, 0)) {
16             hc = super.hashCode();
17         }
18     }
19
20     public static AcceptQuote getInstance() {
21
22         if (Utils.equals(instance, null)) {
23             instance = new AcceptQuote();
```

## Appendix B. The code-generated ATM model

```
24     }
25
26     return instance;
27 }
28
29 public int hashCode() {
30
31     return hc;
32 }
33
34 public boolean equals(final Object obj) {
35
36     return obj instanceof AcceptQuote;
37 }
38
39 public String toString() {
40
41     return "<Accept>";
42 }
43 }
```

```
1 package atm.quotes;
2
3 import org.overture.codegen.runtime.*;
4 import org.overture.codegen.vdm2jml.runtime.*;
5
6 @SuppressWarnings("all")
7 //@ nullable_by_default
8
9 final public class appendQuote implements java.io.Serializable {
10     private static int hc = 0;
11     private static appendQuote instance = null;
12
13     public appendQuote() {
14
15         if (Utils.equals(hc, 0)) {
16             hc = super.hashCode();
17         }
18     }
19
20     public static appendQuote getInstance() {
21
22         if (Utils.equals(instance, null)) {
23             instance = new appendQuote();
24         }
25
26         return instance;
27     }
28
29     public int hashCode() {
30
31         return hc;
32     }
33
34     public boolean equals(final Object obj) {
35
36         return obj instanceof appendQuote;
37     }
38
39     public String toString() {
```

## Appendix B. The code-generated ATM model

```
40
41     return "<append>";
42 }
43 }
```

```
1 package atm.quotes;
2
3 import org.overture.codegen.runtime.*;
4 import org.overture.codegen.vdm2jml.runtime.*;
5
6 @SuppressWarnings("all")
7 //@ nullable_by_default
8
9 final public class BusyQuote implements java.io.Serializable {
10     private static int hc = 0;
11     private static BusyQuote instance = null;
12
13     public BusyQuote() {
14
15         if (Utils.equals(hc, 0)) {
16             hc = super.hashCode();
17         }
18     }
19
20     public static BusyQuote getInstance() {
21
22         if (Utils.equals(instance, null)) {
23             instance = new BusyQuote();
24         }
25
26         return instance;
27     }
28
29     public int hashCode() {
30
31         return hc;
32     }
33
34     public boolean equals(final Object obj) {
35
36         return obj instanceof BusyQuote;
37     }
38
39     public String toString() {
40
41         return "<Busy>";
42     }
43 }
```





# Validation of the translation rules

Since the translation is not formally defined all the translation rules have been validated by running examples, or *regression tests*, through the tool (see section 2.8 for details). This appendix contains all the regression tests that are used to test the translation rules. For each test, the input model, the corresponding Java/JML and the OpenJML runtime assertion checker output is shown, respectively. Alternatively, all the examples, including the generated output, can be downloaded via [2].

## C.1 Map.vdmsl

---

```
1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : inmap nat to nat = {x |-> x | x in set {1,2,3} & x > 0} in skip;
14   let - : inmap nat to nat = {x |-> x | x in set {1,2,3}} in skip;
15   IO`println("After_legal_use");
16   IO`println("Before_violations");
17   let - : inmap nat to nat = {x |-> 2 | x in set {1,2,3} & x > 1} in skip;
18   let - : inmap nat to nat = {x |-> 2 | x in set {1,2,3}} in skip;
19   IO`println("After_violations");
20   return 0;
21 );
22
23 end Entry
```

```
1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
```

## Appendix C. Validation of the translation rules

```

5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         VDMMap mapCompResult_1 = MapUtil.map();
19         /* @ assert (V2J.isMap(mapCompResult_1) && (\forallall int i; 0 <= i && i <
20             V2J.size(mapCompResult_1); Utils.is_nat1(V2J.getDom(mapCompResult_1,
21                 i)) && Utils.is_nat1(V2J.getRng(mapCompResult_1,i)))));
22
23         VDMSet set_1 = SetUtil.set(1L, 2L, 3L);
24         /* @ assert (V2J.isSet(set_1) && (\forallall int i; 0 <= i && i < V2J.size(
25             set_1); Utils.is_nat1(V2J.get(set_1,i)))));
26
27         for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext(); ) {
28             Number x = ((Number) iterator_1.next());
29             /* @ assert Utils.is_nat1(x);
30
31             if (x.longValue() > 0L) {
32                 MapUtil.mapAdd(mapCompResult_1, new Maplet(x, x));
33             }
34         }
35
36         final VDMMap ignorePattern_1 = Utils.copy(mapCompResult_1);
37         /* @ assert (V2J.isInjMap(ignorePattern_1) && (\forallall int i; 0 <= i &&
38             i < V2J.size(ignorePattern_1); Utils.is_nat(V2J.getDom(
39                 ignorePattern_1,i)) && Utils.is_nat(V2J.getRng(ignorePattern_1,i))
40             ));
41
42         /* skip */
43     }
44
45     VDMMap mapCompResult_2 = MapUtil.map();
46     /* @ assert (V2J.isMap(mapCompResult_2) && (\forallall int i; 0 <= i && i <
47         V2J.size(mapCompResult_2); Utils.is_nat1(V2J.getDom(mapCompResult_2,
48             i)) && Utils.is_nat1(V2J.getRng(mapCompResult_2,i)))));
49
50     VDMSet set_2 = SetUtil.set(1L, 2L, 3L);
51     /* @ assert (V2J.isSet(set_2) && (\forallall int i; 0 <= i && i < V2J.size(
52         set_2); Utils.is_nat1(V2J.get(set_2,i)))));
53
54     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext(); ) {
55         Number x = ((Number) iterator_2.next());
56         /* @ assert Utils.is_nat1(x);
57
58         MapUtil.mapAdd(mapCompResult_2, new Maplet(x, x));
59     }
60 }
61 {
62     final VDMMap ignorePattern_2 = Utils.copy(mapCompResult_2);
63     /* @ assert (V2J.isInjMap(ignorePattern_2) && (\forallall int i; 0 <= i &&
64         i < V2J.size(ignorePattern_2); Utils.is_nat(V2J.getDom(
65             ignorePattern_2,i)) && Utils.is_nat(V2J.getRng(ignorePattern_2,i))

```

## Appendix C. Validation of the translation rules

```

54         ));
55     /* skip */
56 }
57
58 IO.println("After_legal_use");
59 IO.println("Before_violations");
60 VDMMap mapCompResult_3 = MapUtil.map();
61 //@ assert (V2J.isMap(mapCompResult_3) && (\forallall int i; 0 <= i && i <
    V2J.size(mapCompResult_3); Utils.is_nat1(V2J.getDom(mapCompResult_3,
    i)) && Utils.is_nat1(V2J.getRng(mapCompResult_3,i))));
62
63 VDMSet set_3 = SetUtil.set(1L, 2L, 3L);
64 //@ assert (V2J.isSet(set_3) && (\forallall int i; 0 <= i && i < V2J.size(
    set_3); Utils.is_nat1(V2J.get(set_3,i))));
65
66 for (Iterator iterator_3 = set_3.iterator(); iterator_3.hasNext(); ) {
67     Number x = ((Number) iterator_3.next());
68     //@ assert Utils.is_nat1(x);
69
70     if (x.longValue() > 1L) {
71         MapUtil.mapAdd(mapCompResult_3, new Maplet(x, 2L));
72     }
73 }
74 {
75     final VDMMap ignorePattern_3 = Utils.copy(mapCompResult_3);
76     //@ assert (V2J.isInjMap(ignorePattern_3) && (\forallall int i; 0 <= i &&
        i < V2J.size(ignorePattern_3); Utils.is_nat(V2J.getDom(
        ignorePattern_3,i)) && Utils.is_nat(V2J.getRng(ignorePattern_3,i))
        ));
77
78     /* skip */
79 }
80
81 VDMMap mapCompResult_4 = MapUtil.map();
82 //@ assert (V2J.isMap(mapCompResult_4) && (\forallall int i; 0 <= i && i <
    V2J.size(mapCompResult_4); Utils.is_nat1(V2J.getDom(mapCompResult_4,
    i)) && Utils.is_nat1(V2J.getRng(mapCompResult_4,i))));
83
84 VDMSet set_4 = SetUtil.set(1L, 2L, 3L);
85 //@ assert (V2J.isSet(set_4) && (\forallall int i; 0 <= i && i < V2J.size(
    set_4); Utils.is_nat1(V2J.get(set_4,i))));
86
87 for (Iterator iterator_4 = set_4.iterator(); iterator_4.hasNext(); ) {
88     Number x = ((Number) iterator_4.next());
89     //@ assert Utils.is_nat1(x);
90
91     MapUtil.mapAdd(mapCompResult_4, new Maplet(x, 2L));
92 }
93 {
94     final VDMMap ignorePattern_4 = Utils.copy(mapCompResult_4);
95     //@ assert (V2J.isInjMap(ignorePattern_4) && (\forallall int i; 0 <= i &&
        i < V2J.size(ignorePattern_4); Utils.is_nat(V2J.getDom(
        ignorePattern_4,i)) && Utils.is_nat(V2J.getRng(ignorePattern_4,i))
        ));
96
97     /* skip */
98 }
99
100 IO.println("After_violations");

```

```

101     return 0L;
102 }
103
104 public String toString() {
105
106     return "Entry{}";
107 }
108 }

```

```

"Before legal use"
"After legal use"
"Before violations"
Entry.java:76: JML assertion is false
    //@ assert (V2J.isInjMap(ignorePattern_3) && (\forall int i; 0 <= i && i
    < V2J.size(ignorePattern_3); Utils.is_nat (V2J.getDom(ignorePattern_3
    ,i)) && Utils.is_nat (V2J.getRng(ignorePattern_3,i)))));
    ^
Entry.java:95: JML assertion is false
    //@ assert (V2J.isInjMap(ignorePattern_4) && (\forall int i; 0 <= i && i
    < V2J.size(ignorePattern_4); Utils.is_nat (V2J.getDom(ignorePattern_4
    ,i)) && Utils.is_nat (V2J.getRng(ignorePattern_4,i)))));
    ^
"After violations"

```

## C.2 Seq.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : seq1 of nat = [x | x in set {1,2,3} & x > 0] in skip;
14   let - : seq1 of nat = [x | x in set {1,2,3}] in skip;
15   IO`println("After_legal_use");
16   IO`println("Before_violations");
17   let - : seq1 of nat = [x | x in set {1,2,3} & x > 4] in skip;
18   let - : seq1 of nat = [x | x in set xs()] in skip;
19   IO`println("After_violations");
20   return 0;
21 );
22
23 functions
24
25 xs : () -> set of nat
26 xs () == {};
27
28 end Entry

```

## Appendix C. Validation of the translation rules

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         VDMSeq seqCompResult_1 = SeqUtil.seq();
19         /* @ assert (V2J.isSeq(seqCompResult_1) && (\forallall int i; 0 <= i && i <
20             V2J.size(seqCompResult_1); Utils.is_nat1(V2J.get(seqCompResult_1,i)
21             ));
22
23         VDMSet set_1 = SetUtil.set(1L, 2L, 3L);
24         /* @ assert (V2J.isSet(set_1) && (\forallall int i; 0 <= i && i < V2J.size(
25             set_1); Utils.is_nat1(V2J.get(set_1,i)))));
26
27         for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext(); ) {
28             Number x = ((Number) iterator_1.next());
29             /* @ assert Utils.is_nat1(x);
30
31             if (x.longValue() > 0L) {
32                 seqCompResult_1.add(x);
33             }
34         }
35
36         final VDMSeq ignorePattern_1 = Utils.copy(seqCompResult_1);
37         /* @ assert (V2J.isSeq1(ignorePattern_1) && (\forallall int i; 0 <= i && i
38             < V2J.size(ignorePattern_1); Utils.is_nat(V2J.get(ignorePattern_1
39             ,i)))));
40
41         /* skip */
42     }
43
44     VDMSeq seqCompResult_2 = SeqUtil.seq();
45     /* @ assert (V2J.isSeq(seqCompResult_2) && (\forallall int i; 0 <= i && i <
46         V2J.size(seqCompResult_2); Utils.is_nat1(V2J.get(seqCompResult_2,i)
47         ));
48
49     VDMSet set_2 = SetUtil.set(1L, 2L, 3L);
50     /* @ assert (V2J.isSet(set_2) && (\forallall int i; 0 <= i && i < V2J.size(
51         set_2); Utils.is_nat1(V2J.get(set_2,i)))));
52
53     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext(); ) {
54         Number x = ((Number) iterator_2.next());
55         /* @ assert Utils.is_nat1(x);
56
57         seqCompResult_2.add(x);
58     }
59 }

```

## Appendix C. Validation of the translation rules

```

52     final VDMSeq ignorePattern_2 = Utils.copy(seqCompResult_2);
53     //@ assert (V2J.isSeq1(ignorePattern_2) && (\forall forall int i; 0 <= i && i
        < V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2
        ,i))));
54
55     /* skip */
56 }
57
58 IO.println("After_legal_use");
59 IO.println("Before_violations");
60 VDMSeq seqCompResult_3 = SeqUtil.seq();
61 //@ assert (V2J.isSeq(seqCompResult_3) && (\forall forall int i; 0 <= i && i <
        V2J.size(seqCompResult_3); Utils.is_nat1(V2J.get(seqCompResult_3,i)
        ));
62
63 VDMSet set_3 = SetUtil.set(1L, 2L, 3L);
64 //@ assert (V2J.isSet(set_3) && (\forall forall int i; 0 <= i && i < V2J.size(
        set_3); Utils.is_nat1(V2J.get(set_3,i))));
65
66 for (Iterator iterator_3 = set_3.iterator(); iterator_3.hasNext(); ) {
67     Number x = ((Number) iterator_3.next());
68     //@ assert Utils.is_nat1(x);
69
70     if (x.longValue() > 4L) {
71         seqCompResult_3.add(x);
72     }
73 }
74 {
75     final VDMSeq ignorePattern_3 = Utils.copy(seqCompResult_3);
76     //@ assert (V2J.isSeq1(ignorePattern_3) && (\forall forall int i; 0 <= i && i
        < V2J.size(ignorePattern_3); Utils.is_nat(V2J.get(ignorePattern_3
        ,i))));
77
78     /* skip */
79 }
80
81 VDMSeq seqCompResult_4 = SeqUtil.seq();
82 //@ assert (V2J.isSeq(seqCompResult_4) && (\forall forall int i; 0 <= i && i <
        V2J.size(seqCompResult_4); Utils.is_nat(V2J.get(seqCompResult_4,i))
        ));
83
84 VDMSet set_4 = xs();
85 //@ assert (V2J.isSet(set_4) && (\forall forall int i; 0 <= i && i < V2J.size(
        set_4); Utils.is_nat(V2J.get(set_4,i))));
86
87 for (Iterator iterator_4 = set_4.iterator(); iterator_4.hasNext(); ) {
88     Number x = ((Number) iterator_4.next());
89     //@ assert Utils.is_nat(x);
90
91     seqCompResult_4.add(x);
92 }
93 {
94     final VDMSeq ignorePattern_4 = Utils.copy(seqCompResult_4);
95     //@ assert (V2J.isSeq1(ignorePattern_4) && (\forall forall int i; 0 <= i && i
        < V2J.size(ignorePattern_4); Utils.is_nat(V2J.get(ignorePattern_4
        ,i))));
96
97     /* skip */
98 }
99

```

```

100     IO.println("After_violations");
101     return 0L;
102 }
103 /*@ pure @*/
104
105 public static VDMSet xs() {
106
107     VDMSet ret_1 = SetUtil.set();
108     //@ assert (V2J.isSet(ret_1) && (\forallall int i; 0 <= i && i < V2J.size(
109         ret_1); Utils.is_nat(V2J.get(ret_1,i))));
110
111     return Utils.copy(ret_1);
112 }
113
114 public String toString() {
115
116     return "Entry{}";
117 }

```

```

"Before legal use"
"After legal use"
"Before violations"
Entry.java:76: JML assertion is false
    //@ assert (V2J.isSeq1(ignorePattern_3) && (\forallall int i; 0 <= i && i <
        V2J.size(ignorePattern_3); Utils.is_nat(V2J.get(ignorePattern_3,i))
        );
    ^
Entry.java:95: JML assertion is false
    //@ assert (V2J.isSeq1(ignorePattern_4) && (\forallall int i; 0 <= i && i <
        V2J.size(ignorePattern_4); Utils.is_nat(V2J.get(ignorePattern_4,i))
        );
    ^
"After violations"

```

### C.3 Set.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12     IO`println("Before_legal_use");
13     let - : set of nat1 = {x| x in set {1,2,3} & x > 0} in skip;
14     let - : set of nat1 = {x| x in set {1,2,3}} in skip;
15     IO`println("After_legal_use");
16     IO`println("Before_violations");
17     let - : set of nat1 = {x| x in set {0,1,2} & x > -1} in skip;
18     let - : set of nat1 = {x| x in set {0,1,2}} in skip;
19     IO`println("After_violations");

```

## Appendix C. Validation of the translation rules

```

20     return 0;
21 );
22
23 end Entry

```

---

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         VDMSet setCompResult_1 = SetUtil.set();
19         //@ assert (V2J.isSet(setCompResult_1) && (\forallall int i; 0 <= i && i <
20             V2J.size(setCompResult_1); Utils.is_nat1(V2J.get(setCompResult_1,i))
21             ));
22
23         VDMSet set_1 = SetUtil.set(1L, 2L, 3L);
24         //@ assert (V2J.isSet(set_1) && (\forallall int i; 0 <= i && i < V2J.size(
25             set_1); Utils.is_nat1(V2J.get(set_1,i))));
26
27         for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext(); ) {
28             Number x = ((Number) iterator_1.next());
29             //@ assert Utils.is_nat1(x);
30
31             if (x.longValue() > 0L) {
32                 setCompResult_1.add(x);
33             }
34         }
35
36         final VDMSet ignorePattern_1 = Utils.copy(setCompResult_1);
37         //@ assert (V2J.isSet(ignorePattern_1) && (\forallall int i; 0 <= i && i
38             < V2J.size(ignorePattern_1); Utils.is_nat1(V2J.get(ignorePattern_1
39             ,i))));
40
41         /* skip */
42     }
43
44     VDMSet setCompResult_2 = SetUtil.set();
45     //@ assert (V2J.isSet(setCompResult_2) && (\forallall int i; 0 <= i && i <
46         V2J.size(setCompResult_2); Utils.is_nat1(V2J.get(setCompResult_2,i))
47         ));
48
49     VDMSet set_2 = SetUtil.set(1L, 2L, 3L);
50     //@ assert (V2J.isSet(set_2) && (\forallall int i; 0 <= i && i < V2J.size(
51         set_2); Utils.is_nat1(V2J.get(set_2,i))));
52
53     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext(); ) {
54         Number x = ((Number) iterator_2.next());
55         //@ assert Utils.is_nat1(x);
56     }
57 }

```



## Appendix C. Validation of the translation rules

```

48
49     setCompResult_2.add(x);
50 }
51 {
52     final VDMSet ignorePattern_2 = Utils.copy(setCompResult_2);
53     //@ assert (V2J.isSet(ignorePattern_2) && (\forall forall int i; 0 <= i && i
        < V2J.size(ignorePattern_2); Utils.is_nat1(V2J.get(ignorePattern_2
        ,i))));
54
55     /* skip */
56 }
57
58 IO.println("After_legal_use");
59 IO.println("Before_violations");
60 VDMSet setCompResult_3 = SetUtil.set();
61 //@ assert (V2J.isSet(setCompResult_3) && (\forall forall int i; 0 <= i && i <
        V2J.size(setCompResult_3); Utils.is_nat(V2J.get(setCompResult_3,i))
        ));
62
63 VDMSet set_3 = SetUtil.set(0L, 1L, 2L);
64 //@ assert (V2J.isSet(set_3) && (\forall forall int i; 0 <= i && i < V2J.size(
        set_3); Utils.is_nat(V2J.get(set_3,i))));
65
66 for (Iterator iterator_3 = set_3.iterator(); iterator_3.hasNext(); ) {
67     Number x = ((Number) iterator_3.next());
68     //@ assert Utils.is_nat(x);
69
70     if (x.longValue() > -1L) {
71         setCompResult_3.add(x);
72     }
73 }
74 {
75     final VDMSet ignorePattern_3 = Utils.copy(setCompResult_3);
76     //@ assert (V2J.isSet(ignorePattern_3) && (\forall forall int i; 0 <= i && i
        < V2J.size(ignorePattern_3); Utils.is_nat1(V2J.get(ignorePattern_3
        ,i))));
77
78     /* skip */
79 }
80
81 VDMSet setCompResult_4 = SetUtil.set();
82 //@ assert (V2J.isSet(setCompResult_4) && (\forall forall int i; 0 <= i && i <
        V2J.size(setCompResult_4); Utils.is_nat(V2J.get(setCompResult_4,i))
        ));
83
84 VDMSet set_4 = SetUtil.set(0L, 1L, 2L);
85 //@ assert (V2J.isSet(set_4) && (\forall forall int i; 0 <= i && i < V2J.size(
        set_4); Utils.is_nat(V2J.get(set_4,i))));
86
87 for (Iterator iterator_4 = set_4.iterator(); iterator_4.hasNext(); ) {
88     Number x = ((Number) iterator_4.next());
89     //@ assert Utils.is_nat(x);
90
91     setCompResult_4.add(x);
92 }
93 {
94     final VDMSet ignorePattern_4 = Utils.copy(setCompResult_4);
95     //@ assert (V2J.isSet(ignorePattern_4) && (\forall forall int i; 0 <= i && i
        < V2J.size(ignorePattern_4); Utils.is_nat1(V2J.get(ignorePattern_4
        ,i))));

```

## Appendix C. Validation of the translation rules

```
96
97     /* skip */
98 }
99
100 IO.println("After_violations");
101 return 0L;
102 }
103
104 public String toString() {
105
106     return "Entry{}";
107 }
108 }
```

```
"Before legal use"
"After legal use"
"Before violations"
Entry.java:76: JML assertion is false
    //@ assert (V2J.isSet(ignorePattern_3) && (\forall int i; 0 <= i && i <
        V2J.size(ignorePattern_3); Utils.is_nat1(V2J.get(ignorePattern_3,i)))
        );
        ^
Entry.java:95: JML assertion is false
    //@ assert (V2J.isSet(ignorePattern_4) && (\forall int i; 0 <= i && i <
        V2J.size(ignorePattern_4); Utils.is_nat1(V2J.get(ignorePattern_4,i)))
        );
        ^
"After violations"
```

### C.4 AtomicStateInvViolation.vdmsl

```
1 module Entry
2
3 imports from IO all
4 definitions
5
6 state St of
7   x : nat
8   init s == s = mk_St(1)
9   inv s == s.x = 1
10 end
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO`println("Before_first_atomic_(expecting_violation_after_atomic)");
18   atomic
19   (
20     x := 2;
21   );
22   IO`println("After_first_atomic_(expected_violation_before_this_print_statement)");
23   IO`println("Before_second_atomic");
24   atomic
25   (
```

## Appendix C. Validation of the translation rules

```

26     x := 1;
27 );
28 IO.println("After_second_atomic");
29 return 2;
30 );
31
32 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class St implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
13
14     public St(final Number _x) {
15
16         //@ assert Utils.is_nat(_x);
17
18         x = _x;
19         //@ assert Utils.is_nat(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.St)) {
27             return false;
28         }
29
30         project.Entrytypes.St other = ((project.Entrytypes.St) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.St copy() {
43
44         return new project.Entrytypes.St(x);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`St" + Utils.formatFields(x);
51     }
52     /*@ pure @*/

```

## Appendix C. Validation of the translation rules

```

53
54 public Number get_x() {
55
56     Number ret_1 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_1));
58
59     return ret_1;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_St(final Number _x) {
80
81     return Utils.equals(_x, 1L);
82 }
83 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ spec_public @*/
12
13     private static project.Entrytypes.St St = new project.Entrytypes.St(1L);
14     /*@ public ghost static boolean invChecksOn = true; @*/
15
16     private Entry() {}
17
18     public static Object Run() {
19
20         IO.println("Before_first_atomic_(expecting_violation_after_atomic)");
21         Number atomicTmp_1 = 2L;
22         //@ assert Utils.is_nat(atomicTmp_1);
23
24         {
25             /* Start of atomic statement */
26             //@ set invChecksOn = false;
27
28             //@ assert St != null;

```

```

29
30     St.set_x(atomicTmp_1);
31
32     //@ set invChecksOn = true;
33
34     //@ assert St.valid();
35
36 } /* End of atomic statement */
37
38 IO.println("After_first_atomic_(expected_violation_before_this_print_
39 statement)");
40 IO.println("Before_second_atomic");
41 Number atomicTmp_2 = 1L;
42 //@ assert Utils.is_nat(atomicTmp_2);
43 {
44     /* Start of atomic statement */
45     //@ set invChecksOn = false;
46
47     //@ assert St != null;
48
49     St.set_x(atomicTmp_2);
50
51     //@ set invChecksOn = true;
52
53     //@ assert St.valid();
54
55 } /* End of atomic statement */
56
57 IO.println("After_second_atomic");
58 return 2L;
59 }
60
61 public String toString() {
62
63     return "Entry{" + "St_:=_" + Utils.toString(St) + "}";
64 }
65 }

```

```

"Before first atomic (expecting violation after atomic)"
St.java:72: JML invariant is false on leaving method project.Entrytypes.St.
    valid()
    ^
St.java:12: Associated declaration
    //@ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
    ^
"After first atomic (expected violation before this print statement)"
"Before second atomic"
"After second atomic"

```

## C.5 AtomicStateInvNoViolation.vdmsl

```

1 module Entry
2
3 imports from IO all

```

## Appendix C. Validation of the translation rules

```

4 definitions
5
6 state St of
7   x : nat
8   init s == s = mk_St(1)
9   inv s == s.x = 1
10 end
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO`println("Before_atomic");
18   atomic
19   (
20     x := 2;
21     x := 1;
22   );
23   IO`println("After_atomic");
24
25   return x;
26 );
27
28 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class St implements Record {
11   public Number x;
12   // @ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
13
14   public St(final Number _x) {
15
16     // @ assert Utils.is_nat(_x);
17
18     x = _x;
19     // @ assert Utils.is_nat(x);
20
21   }
22   /* @ pure @ */
23
24   public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.St)) {
27       return false;
28     }
29
30     project.Entrytypes.St other = ((project.Entrytypes.St) obj);
31
32     return Utils.equals(x, other.x);
33   }
34   /* @ pure @ */

```

## Appendix C. Validation of the translation rules

```

35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.St copy() {
43
44     return new project.Entrytypes.St(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`St" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_1 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_1));
58
59     return ret_1;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_St(final Number _x) {
80
81     return Utils.equals(_x, 1L);
82 }
83 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 /*@ nullable_by_default
9
10 final public class Entry {

```

```

11  /*@ spec_public @*/
12
13  private static project.Entrytypes.St St = new project.Entrytypes.St(1L);
14  /*@ public ghost static boolean invChecksOn = true; @*/
15
16  private Entry() {}
17
18  public static Object Run() {
19
20      IO.println("Before_atomic");
21      Number atomicTmp_1 = 2L;
22      /*@ assert Utils.is_nat(atomicTmp_1);
23
24      Number atomicTmp_2 = 1L;
25      /*@ assert Utils.is_nat(atomicTmp_2);
26
27      {
28          /* Start of atomic statement */
29          /*@ set invChecksOn = false;
30
31          /*@ assert St != null;
32
33          St.set_x(atomicTmp_1);
34
35          /*@ assert St != null;
36
37          St.set_x(atomicTmp_2);
38
39          /*@ set invChecksOn = true;
40
41          /*@ assert St.valid();
42
43      } /* End of atomic statement */
44
45      IO.println("After_atomic");
46      return St.get_x();
47  }
48
49  public String toString() {
50
51      return "Entry{" + "St_:=_" + Utils.toString(St) + "}";
52  }
53  }

```

```

"Before atomic"
"After atomic"

```

## C.6 InvChecksOnFlagInOtherModule.vdmsl

```

1  module Mod
2
3  exports all
4  definitions
5  types
6
7  M :: x : int

```



```

8  inv m == m.x > 0;
9
10 operations
11
12 op : () ==> ()
13 op () ==
14 (
15     dcl m : M := mk_M(1);
16     atomic
17     (
18         m.x := -20;
19         m.x := 20;
20     );
21 );
22
23 end Mod
24
25 module Entry
26
27 exports all
28 imports from IO all
29 definitions
30 types
31
32 E :: x : int
33 inv e == e.x > 0;
34
35 operations
36
37 Run : () ==> ()
38 Run () ==
39 (
40     dcl e : E := mk_E(1);
41     atomic
42     (
43         e.x := -20;
44         e.x := 20;
45     );
46     IO.println("Done!_Expected_to_exit_without_any_errors");
47 );
48
49 end Entry

```

```

1  package project.Modtypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class M implements Record {
11     public Number x;
12     //@ public instance invariant project.Mod.invChecksOn ==> inv_M(x);
13
14     public M(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17

```

## Appendix C. Validation of the translation rules

```
18     x = _x;
19     //@ assert Utils.is_int(x);
20
21 }
22 /*@ pure @*/
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Modtypes.M)) {
27         return false;
28     }
29
30     project.Modtypes.M other = ((project.Modtypes.M) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Modtypes.M copy() {
43
44     return new project.Modtypes.M(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Mod`M" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_1 = x;
57     //@ assert project.Mod.invChecksOn ==> (Utils.is_int(ret_1));
58
59     return ret_1;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Mod.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Mod.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
```

## Appendix C. Validation of the translation rules

```

78
79  public static Boolean inv_M(final Number _x) {
80
81      return _x.longValue() > 0L;
82  }
83  }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Mod {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Mod() {}
14
15     public static void op() {
16
17         project.Modtypes.M m = new project.Modtypes.M(1L);
18         //@ assert Utils.is_(m,project.Modtypes.M.class);
19
20         Number atomicTmp_1 = -20L;
21         //@ assert Utils.is_int(atomicTmp_1);
22
23         Number atomicTmp_2 = 20L;
24         //@ assert Utils.is_int(atomicTmp_2);
25
26         {
27             /* Start of atomic statement */
28             //@ set invChecksOn = false;
29
30             //@ assert m != null;
31
32             m.set_x(atomicTmp_1);
33
34             //@ assert m != null;
35
36             m.set_x(atomicTmp_2);
37
38             //@ set invChecksOn = true;
39
40             //@ assert m.valid();
41
42         } /* End of atomic statement */
43     }
44
45     public String toString() {
46
47         return "Mod{}";
48     }
49 }

```

```

1  package project.Entrytypes;
2

```

## Appendix C. Validation of the translation rules

```
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class E implements Record {
11     public Number x;
12     //@ public instance invariant project.Mod.invChecksOn ==> inv_E(x);
13
14     public E(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17
18         x = _x;
19         //@ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.E)) {
27             return false;
28         }
29
30         project.Entrytypes.E other = ((project.Entrytypes.E) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.E copy() {
43
44         return new project.Entrytypes.E(x);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`E" + Utils.formatFields(x);
51     }
52     /*@ pure @*/
53
54     public Number get_x() {
55
56         Number ret_2 = x;
57         //@ assert project.Mod.invChecksOn ==> (Utils.is_int(ret_2));
58
59         return ret_2;
60     }
61
62     public void set_x(final Number _x) {
```

## Appendix C. Validation of the translation rules

```

63
64     //@ assert project.Mod.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Mod.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_E(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     private Entry() {}
12
13     public static void Run() {
14
15         project.Entrytypes.E e = new project.Entrytypes.E(1L);
16         //@ assert Utils.is_(e,project.Entrytypes.E.class);
17
18         Number atomicTmp_3 = -20L;
19         //@ assert Utils.is_int(atomicTmp_3);
20
21         Number atomicTmp_4 = 20L;
22         //@ assert Utils.is_int(atomicTmp_4);
23
24         {
25             /* Start of atomic statement */
26             //@ set project.Mod.invChecksOn = false;
27
28             //@ assert e != null;
29
30             e.set_x(atomicTmp_3);
31
32             //@ assert e != null;
33
34             e.set_x(atomicTmp_4);
35
36             //@ set project.Mod.invChecksOn = true;
37
38             //@ assert e.valid();

```

```

39
40     } /* End of atomic statement */
41
42     IO.println("Done!_Expected_to_exit_without_any_errors");
43 }
44
45 public String toString() {
46
47     return "Entry{}";
48 }
49 }

```

```
"Done! Expected to exit without any errors"
```

## C.7 AtomicRecUnion.vdmsl

```

1 module Entry
2
3 imports from IO all
4 exports all
5
6 definitions
7
8 types
9 R1 :: x : int
10 inv r1 == r1.x > 0;
11
12 R2 :: x : int
13 inv r2 == r2.x > 0;
14
15 operations
16
17 Run : () ==> ?
18 Run () ==
19 (dcl r : R1 | R2 := mk_R1(1);
20
21   IO`println("Before_valid_use");
22   atomic
23   (
24     r.x := -5;
25     r.x := 5;
26   );
27   IO`println("After_valid_use");
28
29   IO`println("Before_illegal_use");
30   atomic
31   (
32     r.x := -5;
33   );
34   IO`println("After_illegal_use");
35
36   return 0;
37 )
38
39 end Entry

```

## Appendix C. Validation of the translation rules

```
1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R1 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R1(x);
13
14     public R1(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17
18         x = _x;
19         //@ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R1)) {
27             return false;
28         }
29
30         project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.R1 copy() {
43
44         return new project.Entrytypes.R1(x);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry'R1" + Utils.formatFields(x);
51     }
52     /*@ pure @*/
53
54     public Number get_x() {
55
56         Number ret_1 = x;
57         //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_1));
58
59         return ret_1;
```

## Appendix C. Validation of the translation rules

```

60     }
61
62     public void set_x(final Number _x) {
63
64         //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66         x = _x;
67         //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69     }
70     /*@ pure @*/
71
72     public Boolean valid() {
73
74         return true;
75     }
76     /*@ pure @*/
77     /*@ helper @*/
78
79     public static Boolean inv_R1(final Number _x) {
80
81         return _x.longValue() > 0L;
82     }
83 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R2 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(x);
13
14     public R2(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17
18         x = _x;
19         //@ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R2)) {
27             return false;
28         }
29
30         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35

```



## Appendix C. Validation of the translation rules

```

36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R2 copy() {
43
44     return new project.Entrytypes.R2(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry'R2" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_2 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59     return ret_2;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R2(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 /*@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/

```

## Appendix C. Validation of the translation rules

```

12
13 private Entry() {}
14
15 public static Object Run() {
16
17     Object r = new project.Entrytypes.R1(1L);
18     //@ assert (Utils.is_(r,project.Entrytypes.R1.class) || Utils.is_(r,
19         project.Entrytypes.R2.class));
20
21     IO.println("Before_valid_use");
22     Number atomicTmp_1 = -5L;
23     //@ assert Utils.is_int(atomicTmp_1);
24
25     Number atomicTmp_2 = 5L;
26     //@ assert Utils.is_int(atomicTmp_2);
27
28     {
29         /* Start of atomic statement */
30         //@ set invChecksOn = false;
31
32         if (r instanceof project.Entrytypes.R1) {
33             //@ assert r != null;
34
35             ((project.Entrytypes.R1) r).set_x(atomicTmp_1);
36
37         } else if (r instanceof project.Entrytypes.R2) {
38             //@ assert r != null;
39
40             ((project.Entrytypes.R2) r).set_x(atomicTmp_1);
41
42         } else {
43             throw new RuntimeException("Missing_member:_x");
44         }
45
46         if (r instanceof project.Entrytypes.R1) {
47             //@ assert r != null;
48
49             ((project.Entrytypes.R1) r).set_x(atomicTmp_2);
50
51         } else if (r instanceof project.Entrytypes.R2) {
52             //@ assert r != null;
53
54             ((project.Entrytypes.R2) r).set_x(atomicTmp_2);
55
56         } else {
57             throw new RuntimeException("Missing_member:_x");
58         }
59
60         //@ set invChecksOn = true;
61
62         //@ assert r instanceof project.Entrytypes.R1 ==> ((project.Entrytypes
63             .R1) r).valid();
64
65         //@ assert r instanceof project.Entrytypes.R2 ==> ((project.Entrytypes
66             .R2) r).valid();
67
68     } /* End of atomic statement */
69
70     IO.println("After_valid_use");
71     IO.println("Before_illegal_use");

```

## Appendix C. Validation of the translation rules

```

69      Number atomicTmp_3 = -5L;
70      //@ assert Utils.is_int(atomicTmp_3);
71
72      {
73          /* Start of atomic statement */
74          //@ set invChecksOn = false;
75
76          if (r instanceof project.Entrytypes.R1) {
77              //@ assert r != null;
78
79              ((project.Entrytypes.R1) r).set_x(atomicTmp_3);
80
81          } else if (r instanceof project.Entrytypes.R2) {
82              //@ assert r != null;
83
84              ((project.Entrytypes.R2) r).set_x(atomicTmp_3);
85
86          } else {
87              throw new RuntimeException("Missing_member:_x");
88          }
89
90          //@ set invChecksOn = true;
91
92          //@ assert r instanceof project.Entrytypes.R1 ==> ((project.Entrytypes
93              .R1) r).valid();
94
95          //@ assert r instanceof project.Entrytypes.R2 ==> ((project.Entrytypes
96              .R2) r).valid();
97
98          } /* End of atomic statement */
99
100      IO.println("After_illegal_use");
101      return 0L;
102  }
103
104  public String toString() {
105      return "Entry{}";
106  }

```

```

"Before valid use"
"After valid use"
"Before illegal use"
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/AtomicRecUnion/
project/Entrytypes/R1.java:72: JML invariant is false on leaving method
project.Entrytypes.R1.valid()
public Boolean valid() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/AtomicRecUnion/
project/Entrytypes/R1.java:12: Associated declaration: /home/peter/git-
repos/ovt/core/codegen/vdm2jml/target/jml/code/AtomicRecUnion/project/
Entrytypes/R1.java:72:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R1(x);
    ^
"After illegal use"

```

### C.8 NamedTypeInvValues.vdmsl

```

1  module Entry
2
3  exports all
4  definitions
5
6  values
7
8  fOk : CN = 'a';
9  fBreak : CN = 'b';
10
11 types
12
13 CN = C|N
14 inv cn == is_char(cn) => cn = 'a';
15 N = nat;
16 C = char;
17
18 operations
19
20 Run : () ==> ?
21 Run () ==
22     return 0;
23
24 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     //@ public static invariant ((fOk == null) || ((Utils.is_char(fOk) &&
12         inv_Entry_C(fOk)) || (Utils.is_nat(fOk) && inv_Entry_N(fOk))) &&
13         inv_Entry_CN(fOk));
14
15     public static final Object fOk = 'a';
16     //@ public static invariant ((fBreak == null) || ((Utils.is_char(fBreak)
17         && inv_Entry_C(fBreak)) || (Utils.is_nat(fBreak) && inv_Entry_N(fBreak)
18         ))) && inv_Entry_CN(fBreak));
19
20     public static final Object fBreak = 'b';
21     /*@ public ghost static boolean invChecksOn = true; @*/
22
23     private Entry() {}
24
25     public static Object Run() {
26
27         return 0L;
28     }
29
30     public String toString() {
31
32         return "Entry{" + "fOk_=" + Utils.toString(fOk) + ",_fBreak_=" + Utils
33             .toString(fBreak) + "}";
34     }
35 }

```

## Appendix C. Validation of the translation rules

```

29     }
30
31     /*@ pure @*/
32     /*@ helper @*/
33
34     public static Boolean inv_Entry_CN(final Object check_cn) {
35
36         Object cn = ((Object) check_cn);
37
38         Boolean orResult_1 = false;
39
40         if (!(Utils.is_char(cn))) {
41             orResult_1 = true;
42         } else {
43             orResult_1 = Utils.equals(cn, 'a');
44         }
45
46         return orResult_1;
47     }
48
49     /*@ pure @*/
50     /*@ helper @*/
51
52     public static Boolean inv_Entry_N(final Object check_elem) {
53
54         return true;
55     }
56
57     /*@ pure @*/
58     /*@ helper @*/
59
60     public static Boolean inv_Entry_C(final Object check_elem) {
61
62         return true;
63     }
64 }

```

```

Entry.java:10: JML static initialization may not be correct
final public class Entry {
    ^
Entry.java:14: Associated declaration
/*@ public static invariant ((fBreak == null) || ((Utils.is_char(fBreak) &&
    inv_Entry_C(fBreak)) || (Utils.is_nat(fBreak) && inv_Entry_N(fBreak))) &&
    inv_Entry_CN(fBreak));
    ^
Main.java:7: JML invariant is false on entering method project.Entry.Run()
    from Main.main(java.lang.String[])
        project.Entry.Run();
        ^
Entry.java:14: Associated declaration
/*@ public static invariant ((fBreak == null) || ((Utils.is_char(fBreak) &&
    inv_Entry_C(fBreak)) || (Utils.is_nat(fBreak) && inv_Entry_N(fBreak))) &&
    inv_Entry_CN(fBreak));
    ^
Entry.java:21: JML invariant is false on leaving method project.Entry.Run()
    public static Object Run() {
        ^
Entry.java:14: Associated declaration
/*@ public static invariant ((fBreak == null) || ((Utils.is_char(fBreak) &&
    inv_Entry_C(fBreak)) || (Utils.is_nat(fBreak) && inv_Entry_N(fBreak))) &&

```

```
inv_Entry_CN(fBreak));
      ^
```

## C.9 NamedTypeInvMapUpdate.vdmsl

```
1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 M = map ? to ?
10 inv m == forall x in set dom m & (is_nat(x) and is_nat(m(x))) => x + 1 = m(x)
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   dcl m : M := {'a' |-> 1, 1 |-> 2};
18   m('a') := 2;
19   m(1) := 2;
20   IO`println("Breaking_named_type_invariant_for_sequence");
21   m(2) := 10;
22   return 0;
23 );
24
25 end Entry
```

```
1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     VDMMMap m = MapUtil.map(new Maplet('a', 1L), new Maplet(1L, 2L));
18     //@ assert ((V2J.isMap(m) && (\forall int i; 0 <= i && i < V2J.size(m);
19       true && true)) && inv_Entry_M(m));
20
21     //@ assert m != null;
22
23     Utils.mapSeqUpdate(m, 'a', 2L);
24     //@ assert ((V2J.isMap(m) && (\forall int i; 0 <= i && i < V2J.size(m);
25       true && true)) && inv_Entry_M(m));
```

## Appendix C. Validation of the translation rules

```

24
25     //@ assert m != null;
26
27     Utils.mapSeqUpdate(m, 1L, 2L);
28     //@ assert ((V2J.isMap(m) && (\forall int i; 0 <= i && i < V2J.size(m);
29         true && true)) && inv_Entry_M(m));
30
31     IO.println("Breaking_named_type_invariant_for_sequence");
32     //@ assert m != null;
33
34     Utils.mapSeqUpdate(m, 2L, 10L);
35     //@ assert ((V2J.isMap(m) && (\forall int i; 0 <= i && i < V2J.size(m);
36         true && true)) && inv_Entry_M(m));
37
38     return 0L;
39 }
40
41 public String toString() {
42     return "Entry{}";
43 }
44
45 /*@ pure @*/
46 /*@ helper @*/
47 public static Boolean inv_Entry_M(final Object check_m) {
48
49     VDMMap m = ((VDMMap) check_m);
50
51     Boolean forAllExpResult_1 = true;
52     VDMSet set_1 = MapUtil.dom(Utils.copy(m));
53     for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() &&
54         forAllExpResult_1; ) {
55         Object x = ((Object) iterator_1.next());
56         Boolean orResult_1 = false;
57
58         Boolean andResult_1 = false;
59
60         if (Utils.is_nat(x)) {
61             if (Utils.is_nat(Utils.get(m, x))) {
62                 andResult_1 = true;
63             }
64         }
65
66         if (!(andResult_1)) {
67             orResult_1 = true;
68         } else {
69             orResult_1 = Utils.equals(((Number) x).doubleValue() + 1L, Utils.get
70                 (m, x));
71         }
72
73         forAllExpResult_1 = orResult_1;
74     }
75     return forAllExpResult_1;
76 }

```

"Breaking named type invariant for sequence"  
Entry.java:34: JML assertion is false

```
//@ assert ((V2J.isMap(m) && (\forall int i; 0 <= i && i < V2J.size(m);
  true && true)) && inv_Entry_M(m));
^
```

## C.10 NamedTypeInvSeqUpdate.vdmsl

```
1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 S = seq of ?
10 inv s == forall x in set elems s & is_nat(x) => x > 5;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   dcl s : S := [10,11,12];
18   s(1) := 'a';
19   s(2) := nil;
20   IO.println("Breaking_named_type_invariant_for_sequence");
21   s(3) := 4;
22   return 0;
23 );
24
25 end Entry
```

```
1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     VDMSeq s = SeqUtil.seq(10L, 11L, 12L);
18     //@ assert ((V2J.isSeq(s) && (\forall int i; 0 <= i && i < V2J.size(s);
19       true)) && inv_Entry_S(s));
20
21     //@ assert s != null;
22
23     Utils.mapSeqUpdate(s, 1L, 'a');
24     //@ assert ((V2J.isSeq(s) && (\forall int i; 0 <= i && i < V2J.size(s);
25       true)) && inv_Entry_S(s));
```



```

24
25     //@ assert s != null;
26
27     Utils.mapSeqUpdate(s, 2L, null);
28     //@ assert ((V2J.isSeq(s) && (\forallall int i; 0 <= i && i < V2J.size(s);
        true)) && inv_Entry_S(s));
29
30     IO.println("Breaking_named_type_invariant_for_sequence");
31     //@ assert s != null;
32
33     Utils.mapSeqUpdate(s, 3L, 4L);
34     //@ assert ((V2J.isSeq(s) && (\forallall int i; 0 <= i && i < V2J.size(s);
        true)) && inv_Entry_S(s));
35
36     return 0L;
37 }
38
39 public String toString() {
40
41     return "Entry{}";
42 }
43
44 /*@ pure @*/
45 /*@ helper @*/
46
47 public static Boolean inv_Entry_S(final Object check_s) {
48
49     VDMSeq s = ((VDMSeq) check_s);
50
51     Boolean forAllExpResult_1 = true;
52     VDMSet set_1 = SeqUtil.elems(Utils.copy(s));
53     for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() &&
        forAllExpResult_1; ) {
54         Object x = ((Object) iterator_1.next());
55         Boolean orResult_1 = false;
56
57         if (!(Utils.is_nat(x))) {
58             orResult_1 = true;
59         } else {
60             orResult_1 = ((Number) x).doubleValue() > 5L;
61         }
62
63         forAllExpResult_1 = orResult_1;
64     }
65     return forAllExpResult_1;
66 }
67 }

```

```

"Breaking named type invariant for sequence"
Entry.java:34: JML assertion is false
    //@ assert ((V2J.isSeq(s) && (\forallall int i; 0 <= i && i < V2J.size(s);
        true)) && inv_Entry_S(s));
        ^

```

## C.11 RecursionConservativeChecking.vdmsl

## Appendix C. Validation of the translation rules

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6 types
7
8 T = nat | seq of T;
9
10 T1 = nat | nat * T1;
11
12 operations
13
14 tNat : () ==> T
15 tNat () == return 1;
16
17 tSeq : () ==> T
18 tSeq () == return [[[1]]];
19
20 t1Nat : () ==> T1
21 t1Nat () == return 1;
22
23 t1Tup : () ==> T1
24 t1Tup () == return mk_(1,2);
25
26 Run : () ==> ?
27 Run () ==
28 (
29   IO`println("Before_legal_use");
30   let - = tNat() in skip;
31   let - = t1Nat() in skip;
32   IO`println("Before_legal_use");
33   IO`println("Before_illegal_use");
34   let - = tSeq() in skip;
35   let - = t1Tup() in skip;
36   IO`println("After_illegal_use");
37   return 0;
38 );
39
40 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object tNat() {
16
17     Object ret_1 = 1L;
18     //@ assert ((Utils.is_nat(ret_1) || (V2J.isSeq(ret_1) && (\forallall int i;
19       0 <= i && i < V2J.size(ret_1); false))) && inv_Entry_T(ret_1));

```

## Appendix C. Validation of the translation rules

```

19
20     return Utils.copy(ret_1);
21 }
22
23 public static Object tSeq() {
24
25     Object ret_2 = SeqUtil.seq(SeqUtil.seq(SeqUtil.seq(1L)));
26     //@ assert ((Utils.is_nat(ret_2) || (V2J.isSeq(ret_2) && (\forallall int i;
        0 <= i && i < V2J.size(ret_2); false))) && inv_Entry_T(ret_2));
27
28     return Utils.copy(ret_2);
29 }
30
31 public static Object t1Nat() {
32
33     Object ret_3 = 1L;
34     //@ assert (((V2J.isTup(ret_3,2) && Utils.is_nat(V2J.field(ret_3,0)) &&
        false) || Utils.is_nat(ret_3)) && inv_Entry_T1(ret_3));
35
36     return Utils.copy(ret_3);
37 }
38
39 public static Object t1Tup() {
40
41     Object ret_4 = Tuple.mk_(1L, 2L);
42     //@ assert (((V2J.isTup(ret_4,2) && Utils.is_nat(V2J.field(ret_4,0)) &&
        false) || Utils.is_nat(ret_4)) && inv_Entry_T1(ret_4));
43
44     return Utils.copy(ret_4);
45 }
46
47 public static Object Run() {
48
49     IO.println("Before_legal_use");
50     {
51         final Object ignorePattern_1 = tNat();
52         //@ assert ((Utils.is_nat(ignorePattern_1) || (V2J.isSeq(
            ignorePattern_1) && (\forallall int i; 0 <= i && i < V2J.size(
            ignorePattern_1); false))) && inv_Entry_T(ignorePattern_1));
53
54         /* skip */
55     }
56
57     {
58         final Object ignorePattern_2 = t1Nat();
59         //@ assert (((V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
            ignorePattern_2,0)) && false) || Utils.is_nat(ignorePattern_2)) &&
            inv_Entry_T1(ignorePattern_2));
60
61         /* skip */
62     }
63
64     IO.println("Before_legal_use");
65     IO.println("Before_illegal_use");
66     {
67         final Object ignorePattern_3 = tSeq();
68         //@ assert ((Utils.is_nat(ignorePattern_3) || (V2J.isSeq(
            ignorePattern_3) && (\forallall int i; 0 <= i && i < V2J.size(
            ignorePattern_3); false))) && inv_Entry_T(ignorePattern_3));
69

```

## Appendix C. Validation of the translation rules

```

70     /* skip */
71 }
72
73 {
74     final Object ignorePattern_4 = t1Tup();
75     //@ assert (((V2J.isTup(ignorePattern_4,2) && Utils.is_nat(V2J.field(
76         ignorePattern_4,0)) && false) || Utils.is_nat(ignorePattern_4)) &&
77         inv_Entry_T1(ignorePattern_4));
78
79     /* skip */
80 }
81
82 IO.println("After_illegal_use");
83 return 0L;
84 }
85
86 public String toString() {
87     return "Entry{}";
88 }
89
90 /*@ pure @*/
91 /*@ helper @*/
92
93 public static Boolean inv_Entry_T(final Object check_elem) {
94     return true;
95 }
96
97 /*@ pure @*/
98 /*@ helper @*/
99
100 public static Boolean inv_Entry_T1(final Object check_elem) {
101     return true;
102 }
103 }
104 }

```

```

"Before legal use"
"Before legal use"
"Before illegal use"
Entry.java:26: JML assertion is false
    //@ assert ((Utils.is_nat(ret_2) || (V2J.isSeq(ret_2) && (\forall int i; 0
    <= i && i < V2J.size(ret_2); false))) && inv_Entry_T(ret_2));
    ^
Entry.java:68: JML assertion is false
    //@ assert ((Utils.is_nat(ignorePattern_3) || (V2J.isSeq(ignorePattern_3
    ) && (\forall int i; 0 <= i && i < V2J.size(ignorePattern_3); false))
    ) && inv_Entry_T(ignorePattern_3));
    ^
Entry.java:42: JML assertion is false
    //@ assert (((V2J.isTup(ret_4,2) && Utils.is_nat(V2J.field(ret_4,0)) &&
    false) || Utils.is_nat(ret_4)) && inv_Entry_T1(ret_4));
    ^
Entry.java:75: JML assertion is false
    //@ assert (((V2J.isTup(ignorePattern_4,2) && Utils.is_nat(V2J.field(
    ignorePattern_4,0)) && false) || Utils.is_nat(ignorePattern_4)) &&
    inv_Entry_T1(ignorePattern_4));
    ^
"After illegal use"

```

## C.12 NamedTypeInvLocalDecls.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  types
8
9  No = Even | Large;
10
11 Even = nat
12 inv ev == ev mod 2 = 0;
13
14 Large = real
15 inv la == la > 1000;
16
17 operations
18
19 typeUseOk : () ==> ()
20 typeUseOk () ==
21 let   - = 1,
22       even : No = 2,
23       - = 3
24 in
25   skip;
26
27 typeUseNotOk : () ==> ()
28 typeUseNotOk () ==
29 (
30   IO`println("Before_breaking_named_type_invariant");
31   (
32     dcl notLarge : No := 999;
33     IO`println("After_breaking_named_type_invariant");
34     skip;
35   );
36 );
37
38 Run : () ==> ?
39 Run () ==
40 (
41   typeUseOk();
42   typeUseNotOk();
43   return 0;
44 );
45
46 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6

```

## Appendix C. Validation of the translation rules

```

7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static void typeUseOk() {
16
17         final Number ignorePattern_1 = 1L;
18         //@ assert Utils.is_nat1(ignorePattern_1);
19
20         final Object even = 2L;
21         //@ assert (((Utils.is_nat(even) && inv_Entry_Even(even)) || (Utils.
22             is_real(even) && inv_Entry_Large(even))) && inv_Entry_No(even));
23
24         final Number ignorePattern_2 = 3L;
25         //@ assert Utils.is_nat1(ignorePattern_2);
26
27         /* skip */
28     }
29
30     public static void typeUseNotOk() {
31
32         IO.println("Before_breaking_named_type_invariant");
33         {
34             Object notLarge = 999L;
35             //@ assert (((Utils.is_nat(notLarge) && inv_Entry_Even(notLarge)) || (
36                 Utils.is_real(notLarge) && inv_Entry_Large(notLarge))) &&
37                 inv_Entry_No(notLarge));
38
39             IO.println("After_breaking_named_type_invariant");
40             /* skip */
41         }
42
43     }
44
45     public static Object Run() {
46
47         typeUseOk();
48         typeUseNotOk();
49         return 0L;
50     }
51
52     public String toString() {
53
54         return "Entry{}";
55     }
56
57     /*@ pure @*/
58     /*@ helper @*/
59
60     public static Boolean inv_Entry_No(final Object check_elem) {
61
62         return true;
63     }
64
65     /*@ pure @*/
66     /*@ helper @*/

```

```

64
65  public static Boolean inv_Entry_Even(final Object check_ev) {
66
67      Number ev = ((Number) check_ev);
68
69      return Utils.equals(Utils.mod(ev.longValue(), 2L), 0L);
70  }
71
72  /*@ pure @*/
73  /*@ helper @*/
74
75  public static Boolean inv_Entry_Large(final Object check_la) {
76
77      Number la = ((Number) check_la);
78
79      return la.doubleValue() > 1000L;
80  }
81  }

```

```

"Before breaking named type invariant"
Entry.java:35: JML assertion is false
    //@ assert (((Utils.is_nat(notLarge) && inv_Entry_Even(notLarge)) || (
        Utils.is_real(notLarge) && inv_Entry_Large(notLarge))) &&
        inv_Entry_No(notLarge));
        ^
"After breaking named type invariant"

```

## C.13 NamedTypeInvReturn.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  types
8
9  A = [B | C]
10 inv c == is_char(c) => c = 'a';
11 B = real;
12 C = char
13 inv c == c = 'a' or c = 'b';
14
15 operations
16
17 Run : () ==> ?
18 Run () ==
19 let - = idC('b'),
20      - = idC('a'),
21      - = idA(nil),
22      - = idA(2.1),
23      - = constFunc()
24 in
25 (
26   IO`println("Breaking_named_type_invariant_for_return_value");
27   let - = idA('b') in skip;

```

## Appendix C. Validation of the translation rules

```

28     return 0;
29 );
30
31 functions
32
33 idC : C -> C
34 idC (c) ==
35     c;
36
37 idA : A -> A
38 idA (a) ==
39     a;
40
41 constFunc : () -> A
42 constFunc () ==
43     'a';
44
45 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         final Character ignorePattern_1 = idC('b');
18         /* @ assert (Utils.is_char(ignorePattern_1) && inv_Entry_C(
19             ignorePattern_1));
20
21         final Character ignorePattern_2 = idC('a');
22         /* @ assert (Utils.is_char(ignorePattern_2) && inv_Entry_C(
23             ignorePattern_2));
24
25         final Object ignorePattern_3 = idA(null);
26         /* @ assert ((ignorePattern_3 == null) || ((ignorePattern_3 == null) || (
27             Utils.is_real(ignorePattern_3) && inv_Entry_B(ignorePattern_3)) || (
28             Utils.is_char(ignorePattern_3) && inv_Entry_C(ignorePattern_3))) &&
29             inv_Entry_A(ignorePattern_3));
30
31         final Object ignorePattern_4 = idA(2.1);
32         /* @ assert ((ignorePattern_4 == null) || ((ignorePattern_4 == null) || (
33             Utils.is_real(ignorePattern_4) && inv_Entry_B(ignorePattern_4)) || (
34             Utils.is_char(ignorePattern_4) && inv_Entry_C(ignorePattern_4))) &&
35             inv_Entry_A(ignorePattern_4));
36
37         final Object ignorePattern_5 = constFunc();
38         /* @ assert ((ignorePattern_5 == null) || ((ignorePattern_5 == null) || (
39             Utils.is_real(ignorePattern_5) && inv_Entry_B(ignorePattern_5)) || (
40             Utils.is_char(ignorePattern_5) && inv_Entry_C(ignorePattern_5))) &&
41             inv_Entry_A(ignorePattern_5));

```



## Appendix C. Validation of the translation rules

```

31
32     {
33         IO.println("Breaking_named_type_invariant_for_return_value");
34         {
35             final Object ignorePattern_6 = idA('b');
36             //@ assert ((ignorePattern_6 == null) || ((ignorePattern_6 == null)
                || (Utils.is_real(ignorePattern_6) && inv_Entry_B(
                    ignorePattern_6)) || (Utils.is_char(ignorePattern_6) &&
                    inv_Entry_C(ignorePattern_6))) && inv_Entry_A(ignorePattern_6));
37
38             /* skip */
39         }
40
41         return 0L;
42     }
43 }
44 /*@ pure @*/
45
46 public static Character idC(final Character c) {
47
48     //@ assert (Utils.is_char(c) && inv_Entry_C(c));
49
50     Character ret_1 = c;
51     //@ assert (Utils.is_char(ret_1) && inv_Entry_C(ret_1));
52
53     return ret_1;
54 }
55 /*@ pure @*/
56
57 public static Object idA(final Object a) {
58
59     //@ assert ((a == null) || ((a == null) || (Utils.is_real(a) &&
                inv_Entry_B(a)) || (Utils.is_char(a) && inv_Entry_C(a))) &&
                inv_Entry_A(a));
60
61     Object ret_2 = a;
62     //@ assert ((ret_2 == null) || ((ret_2 == null) || (Utils.is_real(ret_2)
                && inv_Entry_B(ret_2)) || (Utils.is_char(ret_2) && inv_Entry_C(
                ret_2))) && inv_Entry_A(ret_2));
63
64     return ret_2;
65 }
66 /*@ pure @*/
67
68 public static Object constFunc() {
69
70     Object ret_3 = 'a';
71     //@ assert ((ret_3 == null) || ((ret_3 == null) || (Utils.is_real(ret_3)
                && inv_Entry_B(ret_3)) || (Utils.is_char(ret_3) && inv_Entry_C(
                ret_3))) && inv_Entry_A(ret_3));
72
73     return ret_3;
74 }
75
76 public String toString() {
77
78     return "Entry{}";
79 }
80
81 /*@ pure @*/

```

## Appendix C. Validation of the translation rules

```

82  /*@ helper @*/
83
84  public static Boolean inv_Entry_A(final Object check_c) {
85
86      Object c = ((Object) check_c);
87
88      Boolean orResult_1 = false;
89
90      if (!(Utils.is_char(c))) {
91          orResult_1 = true;
92      } else {
93          orResult_1 = Utils.equals(c, 'a');
94      }
95
96      return orResult_1;
97  }
98
99  /*@ pure @*/
100 /*@ helper @*/
101
102 public static Boolean inv_Entry_B(final Object check_elem) {
103
104     return true;
105 }
106
107 /*@ pure @*/
108 /*@ helper @*/
109
110 public static Boolean inv_Entry_C(final Object check_c) {
111
112     Character c = ((Character) check_c);
113
114     Boolean orResult_2 = false;
115
116     if (Utils.equals(c, 'a')) {
117         orResult_2 = true;
118     } else {
119         orResult_2 = Utils.equals(c, 'b');
120     }
121
122     return orResult_2;
123 }
124 }

```

```

"Breaking named type invariant for return value"
Entry.java:59: JML assertion is false
    //@ assert ((a == null) || ((a == null) || (Utils.is_real(a) &&
    inv_Entry_B(a)) || (Utils.is_char(a) && inv_Entry_C(a))) && inv_Entry_A
    (a));
    ^
Entry.java:62: JML assertion is false
    //@ assert ((ret_2 == null) || ((ret_2 == null) || (Utils.is_real(ret_2)
    && inv_Entry_B(ret_2)) || (Utils.is_char(ret_2) && inv_Entry_C(ret_2)))
    && inv_Entry_A(ret_2));
    ^
Entry.java:36: JML assertion is false
    //@ assert ((ignorePattern_6 == null) || ((ignorePattern_6 == null) ||
    (Utils.is_real(ignorePattern_6) && inv_Entry_B(ignorePattern_6))
    || (Utils.is_char(ignorePattern_6) && inv_Entry_C(ignorePattern_6))
    ) && inv_Entry_A(ignorePattern_6));

```

^

## C.14 NamedTypeInvMethodParam.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 Even = nat
10 inv n == n mod 2 = 0;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 let n1 = 2,
17     n2 = 3
18 in
19 (
20   let - = op(n1, 5, n1) in skip;
21   IO.println("Breaking_named_type_invariant_for_method_parameter");
22   let - = op(n1, 6, n2) in skip;
23   return 0;
24 );
25
26 op : Even * nat * Even ==> Even
27 op (a,b,c) ==
28   return b * (a + c);
29
30 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     final Number n1 = 2L;
18     //@ assert Utils.is_nat1(n1);
19
20     final Number n2 = 3L;
21     //@ assert Utils.is_nat1(n2);

```

## Appendix C. Validation of the translation rules

```

22
23 {
24 {
25     final Number ignorePattern_1 = op(n1, 5L, n1);
26     //@ assert (Utils.is_nat(ignorePattern_1) && inv_Entry_Even(
        ignorePattern_1));
27
28     /* skip */
29 }
30
31 IO.println("Breaking_named_type_invariant_for_method_parameter");
32 {
33     final Number ignorePattern_2 = op(n1, 6L, n2);
34     //@ assert (Utils.is_nat(ignorePattern_2) && inv_Entry_Even(
        ignorePattern_2));
35
36     /* skip */
37 }
38
39     return 0L;
40 }
41 }
42
43 public static Number op(final Number a, final Number b, final Number c) {
44
45     //@ assert (Utils.is_nat(a) && inv_Entry_Even(a));
46
47     //@ assert Utils.is_nat(b);
48
49     //@ assert (Utils.is_nat(c) && inv_Entry_Even(c));
50
51     Number ret_1 = b.longValue() * (a.longValue() + c.longValue());
52     //@ assert (Utils.is_nat(ret_1) && inv_Entry_Even(ret_1));
53
54     return ret_1;
55 }
56
57 public String toString() {
58
59     return "Entry{}";
60 }
61
62 /*@ pure @*/
63 /*@ helper @*/
64
65 public static Boolean inv_Entry_Even(final Object check_n) {
66
67     Number n = ((Number) check_n);
68
69     return Utils.equals(Utils.mod(n.longValue(), 2L), 0L);
70 }
71 }

```

```

"Breaking named type invariant for method parameter"
Entry.java:49: JML assertion is false
    //@ assert (Utils.is_nat(c) && inv_Entry_Even(c));
        ^

```

## C.15 NamedTypeInvNullAllowed.vdmsl

---

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 N = [X | Y];
10
11 X = nat;
12 Y = char;
13
14 operations
15
16 Run : () ==> ?
17 Run () ==
18 let e : N = nil
19 in
20   return e;
21
22 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     final Object e = null;
18     //@ assert ((e == null) || ((e == null) || (Utils.is_nat(e) &&
19         inv_Entry_X(e)) || (Utils.is_char(e) && inv_Entry_Y(e))) &&
20         inv_Entry_N(e));
21
22     return e;
23   }
24
25   public String toString() {
26
27     return "Entry{}";
28   }
29
30   /*@ pure @*/
31   /*@ helper @*/
32
33   public static Boolean inv_Entry_N(final Object check_elem) {

```

```

32
33     return true;
34 }
35
36 /*@ pure @*/
37 /*@ helper @*/
38
39 public static Boolean inv_Entry_X(final Object check_elem) {
40
41     return true;
42 }
43
44 /*@ pure @*/
45 /*@ helper @*/
46
47 public static Boolean inv_Entry_Y(final Object check_elem) {
48
49     return true;
50 }
51 }

```

## C.16 NamedTypeMadeOptional.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 Even = nat
10 inv e == e mod 2 = 0;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO`println("Before_valid_use");
18   (
19     dcl e : [Even] := 2;
20     e := nil;
21   );
22   IO`println("After_valid_use");
23
24   IO`println("Before_invalid_use");
25   (
26     dcl e : Even := 2;
27     e := Nil();
28   );
29   IO`println("After_invalid_use");
30   return 0;
31 );
32

```

## Appendix C. Validation of the translation rules

```
33 functions
34
35 Nil : () -> [Even]
36 Nil () == nil;
37
38 end Entry

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_valid_use");
18         {
19             Number e = 2L;
20             /* @ assert ((e == null) || Utils.is_nat(e) && inv_Entry_Even(e));
21
22             e = null;
23             /* @ assert ((e == null) || Utils.is_nat(e) && inv_Entry_Even(e));
24
25         }
26
27         IO.println("After_valid_use");
28         IO.println("Before_invalid_use");
29         {
30             Number e = 2L;
31             /* @ assert (Utils.is_nat(e) && inv_Entry_Even(e));
32
33             e = Nil();
34             /* @ assert (Utils.is_nat(e) && inv_Entry_Even(e));
35
36         }
37
38         IO.println("After_invalid_use");
39         return 0L;
40     }
41     /* @ pure @ */
42
43     public static Number Nil() {
44
45         Number ret_1 = null;
46         /* @ assert ((ret_1 == null) || Utils.is_nat(ret_1) && inv_Entry_Even(
47             ret_1));
48
49         return ret_1;
50     }
51
52     public String toString() {
```

```

53     return "Entry{}";
54 }
55
56 /*@ pure @*/
57 /*@ helper @*/
58
59 public static Boolean inv_Entry_Even(final Object check_e) {
60
61     Number e = ((Number) check_e);
62
63     return Utils.equals(Utils.mod(e.longValue(), 2L), 0L);
64 }
65 }

```

```

"Before valid use"
"After valid use"
"Before invalid use"
Entry.java:34: JML assertion is false
    /*@ assert (Utils.is_nat(e) && inv_Entry_Even(e));
    ^
"After invalid use"

```

## C.17 NamedTypeInvAsssignments.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 state St of
8     x : PT
9     init s == s = mk_St(1)
10 end
11
12 types
13
14 PT = PossiblyOne | True;
15 PossiblyOne = [nat]
16 inv p == p <> nil => p = 1;
17 True = bool
18 inv b == b;
19
20 operations
21
22 op1 : () ==> ()
23 op1 () ==
24 (
25     dcl p : PT := nil;
26     p := 1;
27     p := true;
28     St.x := nil;
29     St.x := 1;
30     St.x := true;
31     IO.println("Breaking_named_type_invariant_(assigning_record_field)");
32     St.x := false;

```



## Appendix C. Validation of the translation rules

```

33 | );
34 |
35 | op2 : () ==> ()
36 | op2 () ==
37 | (
38 |   dcl p1 : PT := nil;
39 |   St.x := true;
40 |   IO.println("Breaking_named_type_invariant_(assigning_local_variable)");
41 |   p1 := false;
42 | );
43 |
44 | Run : () ==> ?
45 | Run () ==
46 | (
47 |   op1();
48 |   op2();
49 |   return 0;
50 | );
51 |
52 | end Entry

```

```

1 | package project.Entrytypes;
2 |
3 | import java.util.*;
4 | import org.overture.codegen.runtime.*;
5 | import org.overture.codegen.vdm2jml.runtime.*;
6 |
7 | @SuppressWarnings("all")
8 | //@ nullable_by_default
9 |
10 | final public class St implements Record {
11 |   public Object x;
12 |
13 |   public St(final Object _x) {
14 |
15 |     //@ assert ((((_x == null) || Utils.is_nat(_x)) &&
16 |               inv_Entry_PossiblyOne(_x)) || (Utils.is_bool(_x) && inv_Entry_True(
17 |               _x))) && inv_Entry_PT(_x));
18 |
19 |     x = _x != null ? _x : null;
20 |     //@ assert (((((x == null) || Utils.is_nat(x)) && inv_Entry_PossiblyOne(
21 |               x)) || (Utils.is_bool(x) && inv_Entry_True(x))) && inv_Entry_PT(x));
22 |
23 |   }
24 |   /*@ pure @*/
25 |
26 |   public boolean equals(final Object obj) {
27 |
28 |     if (!(obj instanceof project.Entrytypes.St)) {
29 |       return false;
30 |     }
31 |
32 |     project.Entrytypes.St other = ((project.Entrytypes.St) obj);
33 |
34 |     return Utils.equals(x, other.x);
35 |   }
36 |   /*@ pure @*/
37 |
38 |   public int hashCode() {

```

## Appendix C. Validation of the translation rules

```

37     return Utils.hashCode(x);
38 }
39 /*@ pure @*/
40
41 public project.Entrytypes.St copy() {
42
43     return new project.Entrytypes.St(x);
44 }
45 /*@ pure @*/
46
47 public String toString() {
48
49     return "mk_Entry`St" + Utils.formatFields(x);
50 }
51 /*@ pure @*/
52
53 public Object get_x() {
54
55     Object ret_1 = x;
56     //@ assert project.Entry.invChecksOn ==> (((((ret_1 == null) || Utils.
        is_nat(ret_1)) && inv_Entry_PossiblyOne(ret_1)) || (Utils.is_bool(
        ret_1) && inv_Entry_True(ret_1))) && inv_Entry_PT(ret_1));
57
58     return ret_1;
59 }
60
61 public void set_x(final Object _x) {
62
63     //@ assert project.Entry.invChecksOn ==> (((((_x == null) || Utils.
        is_nat(_x)) && inv_Entry_PossiblyOne(_x)) || (Utils.is_bool(_x) &&
        inv_Entry_True(_x))) && inv_Entry_PT(_x));
64
65     x = _x;
66     //@ assert project.Entry.invChecksOn ==> (((((x == null) || Utils.
        is_nat(x)) && inv_Entry_PossiblyOne(x)) || (Utils.is_bool(x) &&
        inv_Entry_True(x))) && inv_Entry_PT(x));
67
68 }
69 /*@ pure @*/
70
71 public Boolean valid() {
72
73     return true;
74 }
75
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_Entry_PT(final Object check_elem) {
80
81     return true;
82 }
83
84 /*@ pure @*/
85 /*@ helper @*/
86
87 public static Boolean inv_Entry_PossiblyOne(final Object check_p) {
88
89     Number p = ((Number) check_p);
90

```

## Appendix C. Validation of the translation rules

```

91     Boolean orResult_1 = false;
92
93     if (!!(Utils.equals(p, null))) {
94         orResult_1 = true;
95     } else {
96         orResult_1 = Utils.equals(p, 1L);
97     }
98
99     return orResult_1;
100 }
101
102 /*@ pure @*/
103 /*@ helper @*/
104
105 public static Boolean inv_Entry_True(final Object check_b) {
106
107     Boolean b = ((Boolean) check_b);
108
109     return b;
110 }
111 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ spec_public @*/
12
13     private static project.Entrytypes.St St = new project.Entrytypes.St(1L);
14     /*@ public ghost static boolean invChecksOn = true; @*/
15
16     private Entry() {}
17
18     public static void op1() {
19
20         Object p = null;
21         //@ assert (((p == null) || Utils.is_nat(p)) && inv_Entry_PossiblyOne(
22             p)) || (Utils.is_bool(p) && inv_Entry_True(p)) && inv_Entry_PT(p));
23
24         p = 1L;
25         //@ assert (((p == null) || Utils.is_nat(p)) && inv_Entry_PossiblyOne(
26             p)) || (Utils.is_bool(p) && inv_Entry_True(p)) && inv_Entry_PT(p));
27
28         p = true;
29         //@ assert (((p == null) || Utils.is_nat(p)) && inv_Entry_PossiblyOne(
30             p)) || (Utils.is_bool(p) && inv_Entry_True(p)) && inv_Entry_PT(p));
31
32         //@ assert St != null;
33
34         St.set_x(null);
35
36         //@ assert St != null;
37
38         St.set_x(1L);

```

## Appendix C. Validation of the translation rules

```

36
37     //@ assert St != null;
38
39     St.set_x(true);
40
41     IO.println("Breaking_named_type_invariant_(assigning_record_field)");
42     //@ assert St != null;
43
44     St.set_x(false);
45 }
46
47 public static void op2() {
48
49     Object p1 = null;
50     //@ assert (((p1 == null) || Utils.is_nat(p1)) &&
51         inv_Entry_PossiblyOne(p1)) || (Utils.is_bool(p1) && inv_Entry_True(
52         p1)) && inv_Entry_PT(p1));
53
54     //@ assert St != null;
55
56     St.set_x(true);
57
58     IO.println("Breaking_named_type_invariant_(assigning_local_variable)");
59     p1 = false;
60     //@ assert (((p1 == null) || Utils.is_nat(p1)) &&
61         inv_Entry_PossiblyOne(p1)) || (Utils.is_bool(p1) && inv_Entry_True(
62         p1)) && inv_Entry_PT(p1));
63
64 }
65
66 public static Object Run() {
67
68     op1();
69     op2();
70     return 0L;
71 }
72
73 public String toString() {
74
75     return "Entry{" + "St:=" + Utils.toString(St) + "}";
76 }
77
78 /*@ pure @*/
79 /*@ helper @*/
80
81 public static Boolean inv_Entry_PT(final Object check_elem) {
82
83     return true;
84 }
85
86 /*@ pure @*/
87 /*@ helper @*/
88
89 public static Boolean inv_Entry_PossiblyOne(final Object check_p) {
90
91     Number p = ((Number) check_p);
92
93     Boolean orResult_1 = false;
94
95     if (!(Utils.equals(p, null))) {

```

```

92         orResult_1 = true;
93     } else {
94         orResult_1 = Utils.equals(p, 1L);
95     }
96
97     return orResult_1;
98 }
99
100 /*@ pure @*/
101 /*@ helper @*/
102
103 public static Boolean inv_Entry_True(final Object check_b) {
104
105     Boolean b = ((Boolean) check_b);
106
107     return b;
108 }
109 }

```

```

"Breaking named type invariant (assigning record field)"
St.java:63: JML assertion is false
    //@ assert project.Entry.invChecksOn ==> (((((_x == null) || Utils.is_nat
    (_x)) && inv_Entry_PossiblyOne(_x)) || (Utils.is_bool(_x) &&
    inv_Entry_True(_x))) && inv_Entry_PT(_x));
    ^
St.java:66: JML assertion is false
    //@ assert project.Entry.invChecksOn ==> (((((x == null) || Utils.is_nat(
    x)) && inv_Entry_PossiblyOne(x)) || (Utils.is_bool(x) && inv_Entry_True
    (x))) && inv_Entry_PT(x));
    ^
"Breaking named type invariant (assigning local variable)"
Entry.java:58: JML assertion is false
    //@ assert (((p1 == null) || Utils.is_nat(p1)) && inv_Entry_PossiblyOne(
    p1)) || (Utils.is_bool(p1) && inv_Entry_True(p1)) && inv_Entry_PT(p1))
    ;
    ^

```

## C.18 CaseExp.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12     let - = f(2) in skip;
13     IO`println("Done!_Expected_no_violations");
14     return 0;
15 );
16
17 functions

```

## Appendix C. Validation of the translation rules

```

18
19 f : nat -> nat
20 f (a) ==
21   cases a:
22     1 -> 4,
23     2 -> 8,
24     others -> 2
25 end;
26
27 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f(2L);
19       //@ assert Utils.is_nat(ignorePattern_1);
20
21       /* skip */
22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;
26   }
27   /*@ pure @*/
28
29   public static Number f(final Number a) {
30
31     //@ assert Utils.is_nat(a);
32
33     Number casesExpResult_1 = null;
34
35     Number intPattern_1 = a;
36     //@ assert Utils.is_nat(intPattern_1);
37
38     Boolean success_1 = Utils.equals(intPattern_1, 1L);
39     //@ assert Utils.is_bool(success_1);
40
41     if (!(success_1)) {
42       Number intPattern_2 = a;
43       //@ assert Utils.is_nat(intPattern_2);
44
45       success_1 = Utils.equals(intPattern_2, 2L);
46       //@ assert Utils.is_bool(success_1);
47
48       if (success_1) {
49         casesExpResult_1 = 8L;

```

```

50         // @ assert Utils.is_nat1(casesExpResult_1);
51
52     } else {
53         casesExpResult_1 = 2L;
54         // @ assert Utils.is_nat1(casesExpResult_1);
55
56     }
57
58 } else {
59     casesExpResult_1 = 4L;
60     // @ assert Utils.is_nat1(casesExpResult_1);
61
62 }
63
64 Number ret_1 = casesExpResult_1;
65 // @ assert Utils.is_nat(ret_1);
66
67 return ret_1;
68 }
69
70 public String toString() {
71
72     return "Entry{}";
73 }
74 }

```

```
"Done! Expected no violations"
```

## C.19 Ternarylf.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 Rec :: x : int
10 inv r == r.x > 0;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17     let - = f() in skip;
18     let - = g() in skip;
19     IO.println("Done!_Expected_no_violations");
20     return 0;
21 );
22
23 functions
24
25 g : () -> nat
26 g () ==

```

## Appendix C. Validation of the translation rules

```

27 let x = if 1 = 1 then 1 else 2
28 in
29   x;
30
31 f : () -> nat
32 f () ==
33   if 1 = 1 then 1 else 2;
34
35 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f();
19       // @ assert Utils.is_nat(ignorePattern_1);
20
21       /* skip */
22     }
23
24     {
25       final Number ignorePattern_2 = g();
26       // @ assert Utils.is_nat(ignorePattern_2);
27
28       /* skip */
29     }
30
31     IO.println("Done!_Expected_no_violations");
32     return 0L;
33   }
34   /* @ pure @ */
35
36   public static Number g() {
37
38     Number ternaryIfExp_1 = null;
39
40     if (Utils.equals(1L, 1L)) {
41       ternaryIfExp_1 = 1L;
42       // @ assert Utils.is_nat1(ternaryIfExp_1);
43     } else {
44       ternaryIfExp_1 = 2L;
45       // @ assert Utils.is_nat1(ternaryIfExp_1);
46     }
47
48   }
49
50   final Number x = ternaryIfExp_1;

```



## Appendix C. Validation of the translation rules

```

51     // @ assert Utils.is_nat1(x);
52
53     Number ret_1 = x;
54     // @ assert Utils.is_nat(ret_1);
55
56     return ret_1;
57 }
58 /* @ pure @ */
59
60 public static Number f() {
61
62     if (Utils.equals(1L, 1L)) {
63         Number ret_2 = 1L;
64         // @ assert Utils.is_nat(ret_2);
65
66         return ret_2;
67
68     } else {
69         Number ret_3 = 2L;
70         // @ assert Utils.is_nat(ret_3);
71
72         return ret_3;
73     }
74 }
75
76 public String toString() {
77
78     return "Entry{}";
79 }
80 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Rec implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_Rec(x);
13
14     public Rec(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.Rec)) {
27             return false;
28         }
29

```

## Appendix C. Validation of the translation rules

```
30     project.Entrytypes.Rec other = ((project.Entrytypes.Rec) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.Rec copy() {
43
44     return new project.Entrytypes.Rec(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry'Rec" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_4 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_4));
58
59     return ret_4;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_Rec(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }
```

"Done! Expected no violations"

### C.20 LetBeStStm.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   let - in set {1,2,3} in skip;
13   let x in set {1,2,3} be st x > 1 in skip;
14   IO`println("Done!_Expected_no_violations");
15   return 0;
16 );
17
18 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       Number ignorePattern_1 = null;
19
20       Boolean success_1 = false;
21       // @ assert Utils.is_bool(success_1);
22
23       VDMSet set_1 = SetUtil.set(1L, 2L, 3L);
24       // @ assert (V2J.isSet(set_1) && (\forall int i; 0 <= i && i < V2J.size
25         (set_1); Utils.is_nat1(V2J.get(set_1,i)))));
26
27       for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() &&
28         !(success_1); ) {
29         ignorePattern_1 = ((Number) iterator_1.next());
30         success_1 = true;
31         // @ assert Utils.is_bool(success_1);
32       }
33       if (!(success_1)) {
34         throw new RuntimeException("Let_Be_St_found_no_applicable_bindings")
35           ;
36       }
37
38       /* skip */
39

```

```

37     }
38
39     {
40         Number x = null;
41
42         Boolean success_2 = false;
43         //@ assert Utils.is_bool(success_2);
44
45         VDMSet set_2 = SetUtil.set(1L, 2L, 3L);
46         //@ assert (V2J.isSet(set_2) && (\forallall int i; 0 <= i && i < V2J.size
47             (set_2); Utils.is_nat1(V2J.get(set_2,i)))));
48
49         for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext() &&
50             !(success_2); ) {
51             x = (Number) iterator_2.next();
52             success_2 = x.longValue() > 1L;
53             //@ assert Utils.is_bool(success_2);
54         }
55         if (!(success_2)) {
56             throw new RuntimeException("Let_Be_St_found_no_applicable_bindings")
57                 ;
58         }
59
60         /* skip */
61     }
62
63     IO.println("Done!_Expected_no_violations");
64     return 0L;
65 }
66
67 public String toString() {
68     return "Entry{}";
69 }

```

```
"Done! Expected no violations"
```

## C.21 LetBeStExp.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12     let - = f() in skip;
13     let - = g() in skip;
14     IO.println("Done!_Expected_no_violations");
15     return 0;

```

## Appendix C. Validation of the translation rules

```

16 );
17
18 functions
19
20 f : () -> nat
21 f () ==
22   let - in set {1,2,3} in 0;
23
24 g : () -> nat
25 g () ==
26   let x in set {1,2,3} be st x > 1 in 0;
27
28 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f();
19       /* @ assert Utils.is_nat(ignorePattern_1);
20
21       /* skip */
22     }
23
24     {
25       final Number ignorePattern_2 = g();
26       /* @ assert Utils.is_nat(ignorePattern_2);
27
28       /* skip */
29     }
30
31     IO.println("Done!_Expected_no_violations");
32     return 0L;
33   }
34   /* @ pure @ */
35
36   public static Number f() {
37
38     Number letBeStExp_1 = null;
39     Number ignorePattern_3 = null;
40
41     Boolean success_1 = false;
42     /* @ assert Utils.is_bool(success_1);
43
44     VDMSset set_1 = SetUtil.set(1L, 2L, 3L);
45     /* @ assert (V2J.isSet(set_1) && (\forall int i; 0 <= i && i < V2J.size(
46       set_1); Utils.is_nat1(V2J.get(set_1,i)))));

```

## Appendix C. Validation of the translation rules

```

46
47     for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() && !(
48         success_1); ) {
49         ignorePattern_3 = ((Number) iterator_1.next());
50         success_1 = true;
51         //@ assert Utils.is_bool(success_1);
52     }
53     if (!(success_1)) {
54         throw new RuntimeException("Let_Be_St_found_no_applicable_bindings");
55     }
56
57     letBeStExp_1 = 0L;
58     //@ assert Utils.is_nat(letBeStExp_1);
59
60     Number ret_1 = letBeStExp_1;
61     //@ assert Utils.is_nat(ret_1);
62
63     return ret_1;
64 }
65 /*@ pure @*/
66
67 public static Number g() {
68
69     Number letBeStExp_2 = null;
70     Number x = null;
71
72     Boolean success_2 = false;
73     //@ assert Utils.is_bool(success_2);
74
75     VDMSet set_2 = SetUtil.set(1L, 2L, 3L);
76     //@ assert (V2J.isSet(set_2) && (\forallall int i; 0 <= i && i < V2J.size(
77         set_2); Utils.is_nat1(V2J.get(set_2,i)))));
78
79     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext() && !(
80         success_2); ) {
81         x = ((Number) iterator_2.next());
82         success_2 = x.longValue() > 1L;
83         //@ assert Utils.is_bool(success_2);
84     }
85     if (!(success_2)) {
86         throw new RuntimeException("Let_Be_St_found_no_applicable_bindings");
87     }
88
89     letBeStExp_2 = 0L;
90     //@ assert Utils.is_nat(letBeStExp_2);
91
92     Number ret_2 = letBeStExp_2;
93     //@ assert Utils.is_nat(ret_2);
94
95     return ret_2;
96 }
97
98 public String toString() {
99
100     return "Entry{}";
101 }

```

"Done! Expected no violations"

## C.22 RealParamNil.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (dcl r : [real] := 1.23;
12   IO`println("Before_valid_use.");
13   doSkip(r);
14   r := nil;
15   IO`println("After_valid_use.");
16   IO`println("Before_invalid_use.");
17   doSkip(r);
18   IO`println("After_invalid_use.");
19   return 0;
20 );
21
22 operations
23
24 doSkip : real ==> ()
25 doSkip (-) == skip;
26
27 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     Number r = 1.23;
18     //@ assert ((r == null) || Utils.is_real(r));
19
20     IO.println("Before_valid_use.");
21     doSkip(r);
22     r = null;
23     //@ assert ((r == null) || Utils.is_real(r));
24

```

```

25     IO.println("After_valid_use.");
26     IO.println("Before_invalid_use.");
27     doSkip(r);
28     IO.println("After_invalid_use.");
29     return 0L;
30 }
31
32 public static void doSkip(final Number ignorePattern_1) {
33
34     //@ assert Utils.is_real(ignorePattern_1);
35
36     /* skip */
37
38 }
39
40 public String toString() {
41
42     return "Entry{}";
43 }
44 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:34: JML assertion is false
    //@ assert Utils.is_real(ignorePattern_1);
           ^
"After invalid use."

```

## C.23 QuoteAssignNil.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12     IO`println("Before_valid_use.");
13     (dcl aOpt : [<A>] := nil; skip);
14     IO`println("After_valid_use.");
15     IO`println("Before_invalid_use.");
16     (dcl a : <A> := Nil(); skip);
17     IO`println("After_invalid_use.");
18     return 0;
19 );
20
21 functions
22
23 Nil : () -> [<A>]
24 Nil () == nil;
25

```



26 `end Entry`

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_valid_use.");
18         {
19             project.quotes.AQuote aOpt = null;
20             /* @ assert ((aOpt == null) || Utils.is_(aOpt, project.quotes.AQuote.
21                 class));
22
23             /* skip */
24         }
25
26         IO.println("After_valid_use.");
27         IO.println("Before_invalid_use.");
28         {
29             project.quotes.AQuote a = Nil();
30             /* @ assert Utils.is_(a, project.quotes.AQuote.class);
31
32             /* skip */
33         }
34
35         IO.println("After_invalid_use.");
36         return 0L;
37     }
38     /* @ pure @ */
39
40     public static project.quotes.AQuote Nil() {
41
42         project.quotes.AQuote ret_1 = null;
43         /* @ assert ((ret_1 == null) || Utils.is_(ret_1, project.quotes.AQuote.
44             class));
45
46         return ret_1;
47     }
48
49     public String toString() {
50
51         return "Entry{}";
52     }
53 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."

```

```

Entry.java:29: JML assertion is false
    //@ assert Utils.is_(a,project.quotes.AQuote.class);
           ^
"After invalid use."

```

## C.24 NatParamNil.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   dcl n : [nat] := 0;
13   IO`println("Before_valid_use.");
14   n := 1;
15   n := nil;
16   IO`println("After_valid_use.");
17   IO`println("Before_invalid_use.");
18   n := idNat(n);
19   IO`println("After_invalid_use.");
20   return 0;
21 );
22
23 functions
24
25 idNat : nat -> nat
26 idNat (x) == x;
27
28 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     Number n = 0L;
18     //@ assert ((n == null) || Utils.is_nat(n));
19
20     IO.println("Before_valid_use.");

```

```

21     n = 1L;
22     //@ assert ((n == null) || Utils.is_nat(n));
23
24     n = null;
25     //@ assert ((n == null) || Utils.is_nat(n));
26
27     IO.println("After_valid_use.");
28     IO.println("Before_invalid_use.");
29     n = idNat(n);
30     //@ assert ((n == null) || Utils.is_nat(n));
31
32     IO.println("After_invalid_use.");
33     return 0L;
34 }
35 /*@ pure @*/
36
37 public static Number idNat(final Number x) {
38
39     //@ assert Utils.is_nat(x);
40
41     Number ret_1 = x;
42     //@ assert Utils.is_nat(ret_1);
43
44     return ret_1;
45 }
46
47 public String toString() {
48
49     return "Entry{}";
50 }
51 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:39: JML assertion is false
    //@ assert Utils.is_nat(x);
    ^
Entry.java:42: JML assertion is false
    //@ assert Utils.is_nat(ret_1);
    ^
"After invalid use."

```

## C.25 CharReturnNil.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (

```

## Appendix C. Validation of the translation rules

```
12 IO.println("Before_valid_use.");
13 let - : char = charA() in skip;
14 IO.println("After_valid_use.");
15 IO.println("Before_invalid_use.");
16 let - : char = charNil() in skip;
17 IO.println("After_invalid_use.");
18 return 0;
19 );
20
21 functions
22
23 charA : () -> [char]
24 charA () == 'a';
25
26 charNil : () -> [char]
27 charNil () == nil;
28
29 end Entry
```

```
1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_valid_use.");
18         {
19             final Character ignorePattern_1 = charA();
20             // @ assert Utils.is_char(ignorePattern_1);
21
22             /* skip */
23         }
24
25         IO.println("After_valid_use.");
26         IO.println("Before_invalid_use.");
27         {
28             final Character ignorePattern_2 = charNil();
29             // @ assert Utils.is_char(ignorePattern_2);
30
31             /* skip */
32         }
33
34         IO.println("After_invalid_use.");
35         return 0L;
36     }
37     /* @ pure @ */
38
39     public static Character charA() {
40
41         Character ret_1 = 'a';
```

```

42     // @ assert ((ret_1 == null) || Utils.is_char(ret_1));
43
44     return ret_1;
45 }
46 /* @ pure @ */
47
48 public static Character charNil() {
49
50     Character ret_2 = null;
51     // @ assert ((ret_2 == null) || Utils.is_char(ret_2));
52
53     return ret_2;
54 }
55
56 public String toString() {
57
58     return "Entry{}";
59 }
60 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:29: JML assertion is false
    // @ assert Utils.is_char(ignorePattern_2);
           ^
"After invalid use."

```

## C.26 Nat1InitWithZero.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12     dcl n : nat1 := 1;
13     IO`println("Before_valid_use.");
14     n := 1;
15     IO`println("After_valid_use.");
16     IO`println("Before_invalid_use.");
17     (dcl n1 : nat1 := -1 + 1; skip);
18     IO`println("After_invalid_use.");
19     return 0;
20 );
21
22 end Entry

```

```

1 package project;
2
3 import java.util.*;

```

```

4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Number n = 1L;
18         //@ assert Utils.is_nat1(n);
19
20         IO.println("Before_valid_use.");
21         n = 1L;
22         //@ assert Utils.is_nat1(n);
23
24         IO.println("After_valid_use.");
25         IO.println("Before_invalid_use.");
26         {
27             Number n1 = -1L + 1L;
28             //@ assert Utils.is_nat1(n1);
29
30             /* skip */
31         }
32
33         IO.println("After_invalid_use.");
34         return 0L;
35     }
36
37     public String toString() {
38
39         return "Entry{}";
40     }
41 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:28: JML assertion is false
    //@ assert Utils.is_nat1(n1);
           ^
"After invalid use."

```

## C.27 IntAssignNonInt.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations

```

## Appendix C. Validation of the translation rules

```
8
9 Run : () ==> ?
10 Run () ==
11 (
12   dcl i : int := -1;
13   IO`println("Before_valid_use.");
14   i := 1;
15   IO`println("After_valid_use.");
16   IO`println("Before_invalid_use.");
17   i := i + 0.5;
18   IO`println("After_invalid_use.");
19   return 0;
20 );
21
22 end Entry
```

```
1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     Number i = -1L;
18     /* @ assert Utils.is_int(i);
19
20     IO.println("Before_valid_use.");
21     i = 1L;
22     /* @ assert Utils.is_int(i);
23
24     IO.println("After_valid_use.");
25     IO.println("Before_invalid_use.");
26     i = i.longValue() + 0.5;
27     /* @ assert Utils.is_int(i);
28
29     IO.println("After_invalid_use.");
30     return 0L;
31   }
32
33   public String toString() {
34
35     return "Entry{}";
36   }
37 }
```

```
"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:27: JML assertion is false
/* @ assert Utils.is_int(i);
```

```

      ^
"After invalid use."

```

## C.28 BoolReturnNil.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12   dcl b : bool;
13   IO`println("Before_valid_use.");
14   b := true;
15   IO`println("After_valid_use.");
16   IO`println("Before_invalid_use.");
17   b := boolNil();
18   IO`println("After_invalid_use.");
19   return 0;
20 );
21
22 functions
23
24 boolTrue : () -> bool
25 boolTrue () == true;
26
27 boolNil : () -> [bool]
28 boolNil () == nil;
29
30 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     Boolean b = false;
18     //@ assert Utils.is_bool(b);
19
20     IO.println("Before_valid_use.");

```



```

21     b = true;
22     //@ assert Utils.is_bool(b);
23
24     IO.println("After_valid_use.");
25     IO.println("Before_invalid_use.");
26     b = boolNil();
27     //@ assert Utils.is_bool(b);
28
29     IO.println("After_invalid_use.");
30     return 0L;
31 }
32 /*@ pure @*/
33
34 public static Boolean boolTrue() {
35
36     Boolean ret_1 = true;
37     //@ assert Utils.is_bool(ret_1);
38
39     return ret_1;
40 }
41 /*@ pure @*/
42
43 public static Boolean boolNil() {
44
45     Boolean ret_2 = null;
46     //@ assert ((ret_2 == null) || Utils.is_bool(ret_2));
47
48     return ret_2;
49 }
50
51 public String toString() {
52
53     return "Entry{}";
54 }
55 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:27: JML assertion is false
    //@ assert Utils.is_bool(b);
        ^
"After invalid use."

```

## C.29 RatAssignBool.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==

```

## Appendix C. Validation of the translation rules

```

11 | (
12 |   dcl i : rat := 123.456;
13 |   IO`println("Before_valid_use.");
14 |   i := i * i;
15 |   IO`println("After_valid_use.");
16 |   IO`println("Before_invalid_use.");
17 |   i := ratOpt();
18 |   IO`println("After_invalid_use.");
19 |   return 0;
20 | );
21 |
22 | functions
23 |
24 | ratOpt : () -> [rat]
25 | ratOpt () == nil;
26 |
27 | end Entry

```

```

1 | package project;
2 |
3 | import java.util.*;
4 | import org.overture.codegen.runtime.*;
5 | import org.overture.codegen.vdm2jml.runtime.*;
6 |
7 | @SuppressWarnings("all")
8 | //@ nullable_by_default
9 |
10 | final public class Entry {
11 |   /*@ public ghost static boolean invChecksOn = true; @*/
12 |
13 |   private Entry() {}
14 |
15 |   public static Object Run() {
16 |
17 |     Number i = 123.456;
18 |     //@ assert Utils.is_rat(i);
19 |
20 |     IO.println("Before_valid_use.");
21 |     i = i.doubleValue() * i.doubleValue();
22 |     //@ assert Utils.is_rat(i);
23 |
24 |     IO.println("After_valid_use.");
25 |     IO.println("Before_invalid_use.");
26 |     i = ratOpt();
27 |     //@ assert Utils.is_rat(i);
28 |
29 |     IO.println("After_invalid_use.");
30 |     return 0L;
31 |   }
32 |   /*@ pure @*/
33 |
34 |   public static Number ratOpt() {
35 |
36 |     Number ret_1 = null;
37 |     //@ assert ((ret_1 == null) || Utils.is_rat(ret_1));
38 |
39 |     return ret_1;
40 |   }
41 |
42 |   public String toString() {

```

```

43
44     return "Entry{}";
45 }
46 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:27: JML assertion is false
    //@ assert Utils.is_rat(i);
           ^
"After invalid use."

```

## C.30 TokenAssignNil.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  values
8
9  n : [token] = nil;
10 t : [token] = mk_token("");
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO`println("Before_valid_use.");
18   let - : token = t in skip;
19   IO`println("After_valid_use.");
20   IO`println("Before_invalid_use.");
21   let - : token = n in skip;
22   IO`println("After_invalid_use.");
23   return 0;
24 );
25
26 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     //@ public static invariant ((n == null) || Utils.is_token(n));
12
13     public static final Token n = null;
14     //@ public static invariant ((t == null) || Utils.is_token(t));

```

```

15
16 public static final Token t = new Token("");
17 /*@ public ghost static boolean invChecksOn = true; @*/
18
19 private Entry() {}
20
21 public static Object Run() {
22
23     IO.println("Before_valid_use.");
24     {
25         final Token ignorePattern_1 = t;
26         /*@ assert Utils.is_token(ignorePattern_1);
27
28         /* skip */
29     }
30
31     IO.println("After_valid_use.");
32     IO.println("Before_invalid_use.");
33     {
34         final Token ignorePattern_2 = n;
35         /*@ assert Utils.is_token(ignorePattern_2);
36
37         /* skip */
38     }
39
40     IO.println("After_invalid_use.");
41     return 0L;
42 }
43
44 public String toString() {
45
46     return "Entry{" + "n_=" + Utils.toString(n) + ",_t_=" + Utils.toString
47         (t) + "}";
48 }

```

```

"Before valid use."
"After valid use."
"Before invalid use."
Entry.java:35: JML assertion is false
    /*@ assert Utils.is_token(ignorePattern_2);
        ^
"After invalid use."

```

## C.31 RecLet.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 R ::
10     x : nat

```

## Appendix C. Validation of the translation rules

```

11  y : nat;
12
13  operations
14
15  Run : () ==> ?
16  Run () ==
17  (
18    let - = f() in skip;
19    IO.println("Done!_Expected_no_violations");
20    return 0;
21  );
22
23  functions
24
25  f : () -> nat
26  f () ==
27  let mk_R(a,b) = mk_R(1,2)
28  in
29    a + b;
30
31  end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f();
19       //@ assert Utils.is_nat(ignorePattern_1);
20
21       /* skip */
22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;
26   }
27   /*@ pure @*/
28
29   public static Number f() {
30
31     final project.Entrytypes.R recordPattern_1 = new project.Entrytypes.R(1L
32       , 2L);
33     //@ assert Utils.is_(recordPattern_1,project.Entrytypes.R.class);
34
35     Boolean success_1 = true;
36     //@ assert Utils.is_bool(success_1);
37
38     Number a = null;

```

## Appendix C. Validation of the translation rules

```

38
39     Number b = null;
40
41     a = recordPattern_1.get_x();
42     //@ assert Utils.is_nat(a);
43
44     b = recordPattern_1.get_y();
45     //@ assert Utils.is_nat(b);
46
47     if (!(success_1)) {
48         throw new RuntimeException("Record_pattern_match_failed");
49     }
50
51     Number ret_1 = a.longValue() + b.longValue();
52     //@ assert Utils.is_nat(ret_1);
53
54     return ret_1;
55 }
56
57 public String toString() {
58
59     return "Entry{}";
60 }
61 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R implements Record {
11     public Number x;
12     public Number y;
13
14     public R(final Number _x, final Number _y) {
15
16         //@ assert Utils.is_nat(_x);
17
18         //@ assert Utils.is_nat(_y);
19
20         x = _x;
21         //@ assert Utils.is_nat(x);
22
23         y = _y;
24         //@ assert Utils.is_nat(y);
25
26     }
27     /*@ pure @*/
28
29     public boolean equals(final Object obj) {
30
31         if (!(obj instanceof project.Entrytypes.R)) {
32             return false;
33         }
34
35         project.Entrytypes.R other = ((project.Entrytypes.R) obj);

```

## Appendix C. Validation of the translation rules

```
36
37     return (Utils.equals(x, other.x)) && (Utils.equals(y, other.y));
38 }
39 /*@ pure @*/
40
41 public int hashCode() {
42
43     return Utils.hashCode(x, y);
44 }
45 /*@ pure @*/
46
47 public project.Entrytypes.R copy() {
48
49     return new project.Entrytypes.R(x, y);
50 }
51 /*@ pure @*/
52
53 public String toString() {
54
55     return "mk_Entry`R" + Utils.formatFields(x, y);
56 }
57 /*@ pure @*/
58
59 public Number get_x() {
60
61     Number ret_2 = x;
62     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_2));
63
64     return ret_2;
65 }
66
67 public void set_x(final Number _x) {
68
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
70
71     x = _x;
72     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
73
74 }
75 /*@ pure @*/
76
77 public Number get_y() {
78
79     Number ret_3 = y;
80     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_3));
81
82     return ret_3;
83 }
84
85 public void set_y(final Number _y) {
86
87     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(_y));
88
89     y = _y;
90     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(y));
91
92 }
93 /*@ pure @*/
94
95 public Boolean valid() {
```

```

96
97     return true;
98 }
99 }

```

```
"Done! Expected no violations"
```

## C.32 TupLet.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12   let - = f() in skip;
13   IO.println("Done!_Expected_no_violations");
14   return 0;
15 );
16
17 functions
18
19 f : () -> nat
20 f () ==
21 let mk_(a,b) = mk_(1,2)
22 in
23   a + b;
24
25 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         {
18             final Number ignorePattern_1 = f();
19             //@ assert Utils.is_nat(ignorePattern_1);
20
21             /* skip */

```



```

22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;
26 }
27 /*@ pure @*/
28
29 public static Number f() {
30
31     final Tuple tuplePattern_1 = Tuple.mk_(1L, 2L);
32     //@ assert (V2J.isTup(tuplePattern_1,2) && Utils.is_nat1(V2J.field(
33         tuplePattern_1,0)) && Utils.is_nat1(V2J.field(tuplePattern_1,1)));
34
35     Boolean success_1 = tuplePattern_1.compatible(Number.class, Number.class
36         );
37     //@ assert Utils.is_bool(success_1);
38
39     Number a = null;
40
41     Number b = null;
42
43     if (success_1) {
44         a = ((Number) tuplePattern_1.get(0));
45         //@ assert Utils.is_nat1(a);
46
47         b = ((Number) tuplePattern_1.get(1));
48         //@ assert Utils.is_nat1(b);
49
50     }
51
52     if (!(success_1)) {
53         throw new RuntimeException("Tuple_pattern_match_failed");
54     }
55
56     Number ret_1 = a.longValue() + b.longValue();
57     //@ assert Utils.is_nat(ret_1);
58
59     return ret_1;
60 }
61
62 public String toString() {
63     return "Entry{}";
64 }

```

```
"Done! Expected no violations"
```

### C.33 RecParam.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6

```

```

7 | types
8 |
9 | R ::
10 |   b : bool;
11 |
12 | operations
13 |
14 | Run : () ==> ?
15 | Run () ==
16 | (
17 |   let - = f() in skip;
18 |   IO.println("Done!_Expected_no_violations");
19 |   return 0;
20 | );
21 |
22 | functions
23 |
24 | f : () -> bool
25 | f () ==
26 | let mk_R(true) in set {mk_R(false), mk_R(true)}
27 | in
28 |   true;
29 |
30 | end Entry

```

```

1 | package project;
2 |
3 | import java.util.*;
4 | import org.overture.codegen.runtime.*;
5 | import org.overture.codegen.vdm2jml.runtime.*;
6 |
7 | @SuppressWarnings("all")
8 | //@ nullable_by_default
9 |
10 | final public class Entry {
11 |   /*@ public ghost static boolean invChecksOn = true; @*/
12 |
13 |   private Entry() {}
14 |
15 |   public static Object Run() {
16 |
17 |     {
18 |       final Boolean ignorePattern_1 = f();
19 |       //@ assert Utils.is_bool(ignorePattern_1);
20 |
21 |       /* skip */
22 |     }
23 |
24 |     IO.println("Done!_Expected_no_violations");
25 |     return 0L;
26 |   }
27 |   /*@ pure @*/
28 |
29 |   public static Boolean f() {
30 |
31 |     Boolean letBeStExp_1 = null;
32 |     project.Entrytypes.R recordPattern_1 = null;
33 |
34 |     Boolean success_1 = false;
35 |     //@ assert Utils.is_bool(success_1);

```

## Appendix C. Validation of the translation rules

```

36
37     VDMSet set_1 = SetUtil.set(new project.Entrytypes.R(false), new project.
38         Entrytypes.R(true));
39     //@ assert (V2J.isSet(set_1) && (\forall int i; 0 <= i && i < V2J.size(
40         set_1); Utils.is_(V2J.get(set_1,i),project.Entrytypes.R.class)));
41
42     for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() && !(
43         success_1); ) {
44         recordPattern_1 = ((project.Entrytypes.R) iterator_1.next());
45         //@ assert Utils.is_(recordPattern_1,project.Entrytypes.R.class);
46
47         success_1 = true;
48         //@ assert Utils.is_bool(success_1);
49
50         Boolean boolPattern_1 = recordPattern_1.get_b();
51         //@ assert Utils.is_bool(boolPattern_1);
52
53         success_1 = Utils.equals(boolPattern_1, true);
54         //@ assert Utils.is_bool(success_1);
55
56         if (!(success_1)) {
57             continue;
58         }
59
60         success_1 = true;
61         //@ assert Utils.is_bool(success_1);
62
63     }
64
65     if (!(success_1)) {
66         throw new RuntimeException("Let_Be_St_found_no_applicable_bindings");
67     }
68
69     letBeStExp_1 = true;
70     //@ assert Utils.is_bool(letBeStExp_1);
71
72     Boolean ret_1 = letBeStExp_1;
73     //@ assert Utils.is_bool(ret_1);
74
75     return ret_1;
76 }
77
78 public String toString() {
79
80     return "Entry{}";
81 }
82 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R implements Record {
11     public Boolean b;
12
13     public R(final Boolean _b) {

```

## Appendix C. Validation of the translation rules

```
14
15     // @ assert Utils.is_bool(_b);
16
17     b = _b;
18     // @ assert Utils.is_bool(b);
19
20 }
21 /* @ pure @ */
22
23 public boolean equals(final Object obj) {
24
25     if (!(obj instanceof project.Entrytypes.R)) {
26         return false;
27     }
28
29     project.Entrytypes.R other = ((project.Entrytypes.R) obj);
30
31     return Utils.equals(b, other.b);
32 }
33 /* @ pure @ */
34
35 public int hashCode() {
36
37     return Utils.hashCode(b);
38 }
39 /* @ pure @ */
40
41 public project.Entrytypes.R copy() {
42
43     return new project.Entrytypes.R(b);
44 }
45 /* @ pure @ */
46
47 public String toString() {
48
49     return "mk_Entry `R" + Utils.formatFields(b);
50 }
51 /* @ pure @ */
52
53 public Boolean get_b() {
54
55     Boolean ret_2 = b;
56     // @ assert project.Entry.invChecksOn ==> (Utils.is_bool(ret_2));
57
58     return ret_2;
59 }
60
61 public void set_b(final Boolean _b) {
62
63     // @ assert project.Entry.invChecksOn ==> (Utils.is_bool(_b));
64
65     b = _b;
66     // @ assert project.Entry.invChecksOn ==> (Utils.is_bool(b));
67
68 }
69 /* @ pure @ */
70
71 public Boolean valid() {
72
73     return true;
```

```

74 |   }
75 | }

```

```
"Done! Expected no violations"
```

## C.34 TupParam.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   let - = f(mk_(4,'a')) in skip;
13   IO`println("Done!_Expected_no_violations");
14   return 0;
15 );
16
17 functions
18
19 f : (nat * char) -> nat
20 f (mk_(a,-)) ==
21   a;
22
23 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f(Tuple.mk_(4L, 'a'));
19       //@ assert Utils.is_nat(ignorePattern_1);
20
21       /* skip */
22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;

```

```

26   }
27   /*@ pure @*/
28
29   public static Number f(final Tuple tuplePattern_1) {
30
31       /*@ assert (V2J.isTup(tuplePattern_1,2) && Utils.is_nat(V2J.field(
32           tuplePattern_1,0)) && Utils.is_char(V2J.field(tuplePattern_1,1)));
33
34       Boolean success_1 = tuplePattern_1.compatible(Number.class, Character.
35           class);
36       /*@ assert Utils.is_bool(success_1);
37
38       Number a = null;
39
40       if (success_1) {
41           a = (Number) tuplePattern_1.get(0);
42           /*@ assert Utils.is_nat(a);
43
44       }
45
46       if (!(success_1)) {
47           throw new RuntimeException("Tuple_pattern_match_failed");
48       }
49
50       Number ret_1 = a;
51       /*@ assert Utils.is_nat(ret_1);
52
53       return ret_1;
54   }
55
56   public String toString() {
57
58       return "Entry{}";
59   }
60 }

```

```
"Done! Expected no violations"
```

### C.35 SeqNat1BoolMaskedAsNamedTypeInv.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 SeqNat1Bool = seq of (nat1 | bool);
10
11 operations
12
13 Run : () ==> ?
14 Run () ==
15 (
16   IO`println("Before_legal_use");

```

## Appendix C. Validation of the translation rules

```

17 let - : SeqNat1Bool = [1,true,2,false,3] in skip;
18 IO`println("After_legal_use");
19 IO`println("Before_illegal_use");
20 let - : SeqNat1Bool = [1,true,2,false,minusOne()] in skip;
21 IO`println("After_illegal_use");
22 return 0;
23 );
24
25 functions
26
27 minusOne : () -> int
28 minusOne () == -1;
29
30 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         {
19             final VDMSeq ignorePattern_1 = SeqUtil.seq(1L, true, 2L, false, 3L);
20             /* @ assert ((V2J.isSeq(ignorePattern_1) && (\forallall int i; 0 <= i && i
21                < V2J.size(ignorePattern_1); (Utils.is_bool(V2J.get(
22                    ignorePattern_1,i)) || Utils.is_nat1(V2J.get(ignorePattern_1,i))))
23                ) && inv_Entry_SeqNat1Bool(ignorePattern_1));
24
25             /* skip */
26         }
27
28         IO.println("After_legal_use");
29         IO.println("Before_illegal_use");
30         {
31             final VDMSeq ignorePattern_2 = SeqUtil.seq(1L, true, 2L, false,
32                 minusOne());
33             /* @ assert ((V2J.isSeq(ignorePattern_2) && (\forallall int i; 0 <= i && i
34                < V2J.size(ignorePattern_2); (Utils.is_bool(V2J.get(
35                    ignorePattern_2,i)) || Utils.is_nat1(V2J.get(ignorePattern_2,i))))
36                ) && inv_Entry_SeqNat1Bool(ignorePattern_2));
37
38             /* skip */
39         }
40
41         IO.println("After_illegal_use");
42         return 0L;
43     }
44     /* @ pure @ */
45 }

```

```

39  public static Number minusOne() {
40
41      Number ret_1 = -1L;
42      //@ assert Utils.is_int(ret_1);
43
44      return ret_1;
45  }
46
47  public String toString() {
48
49      return "Entry{}";
50  }
51
52  /*@ pure @*/
53  /*@ helper @*/
54
55  public static Boolean inv_Entry_SeqNat1Bool(final Object check_elem) {
56
57      return true;
58  }
59  }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert ((V2J.isSeq(ignorePattern_2) && (\forallall int i; 0 <= i && i <
        V2J.size(ignorePattern_2); (Utils.is_bool(V2J.get(ignorePattern_2,i)
        ) || Utils.is_nat1(V2J.get(ignorePattern_2,i)))) &&
        inv_Entry_SeqNat1Bool(ignorePattern_2));
        ^
"After illegal use"

```

## C.36 SeqOfNatNilElem.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : seq of nat = [1,2,3] in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_uses");
16   let - : seq of nat = seqOfNatsAndNil() in skip;
17   IO`println("After_illegal_uses");
18   return 0;
19 );
20
21 functions

```



## Appendix C. Validation of the translation rules

```

22
23 seqOfNatsAndNil : () -> seq of [nat]
24 seqOfNatsAndNil () == [1,nil,3];
25
26 end Entry

```

---

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         {
19             final VDMSeq ignorePattern_1 = SeqUtil.seq(1L, 2L, 3L);
20             /* @ assert (V2J.isSeq(ignorePattern_1) && (\forallall int i; 0 <= i && i
21                 < V2J.size(ignorePattern_1); Utils.is_nat(V2J.get(ignorePattern_1,
22                     i)))));
23
24             /* skip */
25         }
26
27         IO.println("After_legal_use");
28         IO.println("Before_illegal_uses");
29         {
30             final VDMSeq ignorePattern_2 = seqOfNatsAndNil();
31             /* @ assert (V2J.isSeq(ignorePattern_2) && (\forallall int i; 0 <= i && i
32                 < V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2,
33                     i)))));
34
35             /* skip */
36         }
37
38         IO.println("After_illegal_uses");
39         return 0L;
40     }
41     /* @ pure @ */
42
43     public static VDMSeq seqOfNatsAndNil() {
44
45         VDMSeq ret_1 = SeqUtil.seq(1L, null, 3L);
46         /* @ assert (V2J.isSeq(ret_1) && (\forallall int i; 0 <= i && i < V2J.size(
47             ret_1); ((V2J.get(ret_1,i) == null) || Utils.is_nat(V2J.get(ret_1,i)
48                 ))));
49
50         return Utils.copy(ret_1);
51     }
52
53     public String toString() {

```

```

49     return "Entry{}";
50   }
51 }

```

```

"Before legal use"
"After legal use"
"Before illegal uses"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isSeq(ignorePattern_2) && (\forall int i; 0 <= i && i <
        V2J.size(ignorePattern_2); Utils.is_nat (V2J.get (ignorePattern_2,i)))
        ;
        ^
"After illegal uses"

```

### C.37 Seq1EvenNatsMaskedAsNamedTypeInv.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 Seq1Even = seq1 of nat
10 inv xs == forall x in set elems xs & x mod 2 = 0;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO`println("Before_legal_use");
18   let - : Seq1Even = [2,4,6] in skip;
19   IO`println("After_legal_use");
20   IO`println("Before_illegal_use");
21   let - : Seq1Even = [2,4,6,9] in skip;
22   let - : Seq1Even = emptySeqOfNat() in skip;
23   IO`println("After_illegal_use");
24   return 0;
25 );
26
27 functions
28
29 emptySeqOfNat : () -> seq of nat
30 emptySeqOfNat () == [];
31
32 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")

```

## Appendix C. Validation of the translation rules

```

8  // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         {
19             final VDMSeq ignorePattern_1 = SeqUtil.seq(2L, 4L, 6L);
20             /* @ assert ((V2J.isSeq1(ignorePattern_1) && (\forallall int i; 0 <= i &&
                i < V2J.size(ignorePattern_1); Utils.is_nat(V2J.get(
                ignorePattern_1,i)))) && inv_Entry_Seq1Even(ignorePattern_1));
21
22             /* skip */
23         }
24
25         IO.println("After_legal_use");
26         IO.println("Before_illegal_use");
27         {
28             final VDMSeq ignorePattern_2 = SeqUtil.seq(2L, 4L, 6L, 9L);
29             /* @ assert ((V2J.isSeq1(ignorePattern_2) && (\forallall int i; 0 <= i &&
                i < V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(
                ignorePattern_2,i)))) && inv_Entry_Seq1Even(ignorePattern_2));
30
31             /* skip */
32         }
33
34         {
35             final VDMSeq ignorePattern_3 = emptySeqOfNat();
36             /* @ assert ((V2J.isSeq1(ignorePattern_3) && (\forallall int i; 0 <= i &&
                i < V2J.size(ignorePattern_3); Utils.is_nat(V2J.get(
                ignorePattern_3,i)))) && inv_Entry_Seq1Even(ignorePattern_3));
37
38             /* skip */
39         }
40
41         IO.println("After_illegal_use");
42         return 0L;
43     }
44     /* @ pure @ */
45
46     public static VDMSeq emptySeqOfNat() {
47
48         VDMSeq ret_1 = SeqUtil.seq();
49         /* @ assert (V2J.isSeq(ret_1) && (\forallall int i; 0 <= i && i < V2J.size(
                ret_1); Utils.is_nat(V2J.get(ret_1,i)))));
50
51         return Utils.copy(ret_1);
52     }
53
54     public String toString() {
55
56         return "Entry{}";
57     }
58
59     /* @ pure @ */
60     /* @ helper @ */

```

```

61
62 public static Boolean inv_Entry_Seq1Even(final Object check_xs) {
63
64     VDMSeq xs = ((VDMSeq) check_xs);
65
66     Boolean forAllExpResult_1 = true;
67     VDMSet set_1 = SeqUtil.elems(Utils.copy(xs));
68     for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() &&
        forAllExpResult_1; ) {
69         Number x = ((Number) iterator_1.next());
70         forAllExpResult_1 = Utils.equals(Utils.mod(x.longValue(), 2L), 0L);
71     }
72     return forAllExpResult_1;
73 }
74 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert ((V2J.isSeq1(ignorePattern_2) && (\forall int i; 0 <= i && i
    < V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2,i))
    )) && inv_Entry_Seq1Even(ignorePattern_2));
    ^
Entry.java:36: JML assertion is false
    //@ assert ((V2J.isSeq1(ignorePattern_3) && (\forall int i; 0 <= i && i
    < V2J.size(ignorePattern_3); Utils.is_nat(V2J.get(ignorePattern_3,i))
    )) && inv_Entry_Seq1Even(ignorePattern_3));
    ^
"After illegal use"

```

## C.38 Seq1AssignEmptySet.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : seq1 of nat = [1] in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : seq1 of nat = emptySeqOfNat() in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 emptySeqOfNat : () -> seq of nat

```

## Appendix C. Validation of the translation rules

```

24 emptySeqOfNat () == [];
25
26 end Entry

```

---

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         {
19             final VDMSeq ignorePattern_1 = SeqUtil.seq(1L);
20             /* @ assert (V2J.isSeq1(ignorePattern_1) && (\forallall int i; 0 <= i && i
21                 < V2J.size(ignorePattern_1); Utils.is_nat(V2J.get(ignorePattern_1
22                     ,i)))));
23
24             /* skip */
25         }
26
27         IO.println("After_legal_use");
28         IO.println("Before_illegal_use");
29         {
30             final VDMSeq ignorePattern_2 = emptySeqOfNat();
31             /* @ assert (V2J.isSeq1(ignorePattern_2) && (\forallall int i; 0 <= i && i
32                 < V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2
33                     ,i)))));
34
35             /* skip */
36         }
37
38         IO.println("After_illegal_use");
39         return 0L;
40     }
41     /* @ pure @ */
42
43     public static VDMSeq emptySeqOfNat() {
44
45         VDMSeq ret_1 = SeqUtil.seq();
46         /* @ assert (V2J.isSeq(ret_1) && (\forallall int i; 0 <= i && i < V2J.size(
47             ret_1); Utils.is_nat(V2J.get(ret_1,i)))));
48
49         return Utils.copy(ret_1);
50     }
51
52     public String toString() {
53
54         return "Entry{}";
55     }
56 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isSeq1(ignorePattern_2) && (\forall int i; 0 <= i && i <
        V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2,i)))
        );
        ^
"After illegal use"

```

## C.39 SeqEven.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 SeqEven = seq of Even;
10
11 Even = nat
12 inv e == e mod 2 = 0;
13
14 operations
15
16 Run : () ==> ?
17 Run () ==
18 (
19   IO`println("Before_legal_use");
20   let - : SeqEven = [] in skip;
21   let - : SeqEven = [2,4,6,8] in skip;
22   IO`println("After_legal_use");
23   IO`println("Before_illegal_use");
24   let - : SeqEven = [2,4,6,8,9] in skip;
25   IO`println("After_illegal_use");
26   return 0;
27 );
28
29 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12

```

## Appendix C. Validation of the translation rules

```

13 private Entry() {}
14
15 public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19         final VDMSeq ignorePattern_1 = SeqUtil.seq();
20         //@ assert ((V2J.isSeq(ignorePattern_1) && (\forallall int i; 0 <= i && i
                < V2J.size(ignorePattern_1); (Utils.is_nat(V2J.get(
                ignorePattern_1,i)) && inv_Entry_Even(V2J.get(ignorePattern_1,i)))
                )) && inv_Entry_SeqEven(ignorePattern_1));
21
22         /* skip */
23     }
24
25     {
26         final VDMSeq ignorePattern_2 = SeqUtil.seq(2L, 4L, 6L, 8L);
27         //@ assert ((V2J.isSeq(ignorePattern_2) && (\forallall int i; 0 <= i && i
                < V2J.size(ignorePattern_2); (Utils.is_nat(V2J.get(
                ignorePattern_2,i)) && inv_Entry_Even(V2J.get(ignorePattern_2,i)))
                )) && inv_Entry_SeqEven(ignorePattern_2));
28
29         /* skip */
30     }
31
32     IO.println("After_legal_use");
33     IO.println("Before_illegal_use");
34     {
35         final VDMSeq ignorePattern_3 = SeqUtil.seq(2L, 4L, 6L, 8L, 9L);
36         //@ assert ((V2J.isSeq(ignorePattern_3) && (\forallall int i; 0 <= i && i
                < V2J.size(ignorePattern_3); (Utils.is_nat(V2J.get(
                ignorePattern_3,i)) && inv_Entry_Even(V2J.get(ignorePattern_3,i)))
                )) && inv_Entry_SeqEven(ignorePattern_3));
37
38         /* skip */
39     }
40
41     IO.println("After_illegal_use");
42     return 0L;
43 }
44
45 public String toString() {
46
47     return "Entry{}";
48 }
49
50 /*@ pure @*/
51 /*@ helper @*/
52
53 public static Boolean inv_Entry_SeqEven(final Object check_elem) {
54
55     return true;
56 }
57
58 /*@ pure @*/
59 /*@ helper @*/
60
61 public static Boolean inv_Entry_Even(final Object check_e) {
62
63     Number e = ((Number) check_e);

```

## Appendix C. Validation of the translation rules

```
64
65     return Utils.equals(Utils.mod(e.longValue(), 2L), 0L);
66 }
67 }
```

```
"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:36: JML assertion is false
    //@ assert ((V2J.isSeq(ignorePattern_3) && (\forall int i; 0 <= i && i <
        V2J.size(ignorePattern_3); (Utils.is_nat(V2J.get(ignorePattern_3,i))
        && inv_Entry_Even(V2J.get(ignorePattern_3,i)))) &&
        inv_Entry_SeqEven(ignorePattern_3));
        ^
"After illegal use"
```

### C.40 RecUnion.vdmsl

```
1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6  types
7
8  R1 :: r2 : R2
9  inv r1 == r1.r2.x <> -1;
10
11 R2 :: x : int
12 inv r2 == r2.x <> -2;
13
14 operations
15
16 Run: () ==> ?
17 Run () ==
18 (
19   dcl r1 : R1 | nat := mk_R1(mk_R2(5));
20   r1.r2.x := -1;
21   IO.println("\invariant_for_is_not_implemented_in_OpenJML_RAC_" ^
22     "so_the_\invariant_for_check_will_not_detect_the_invariant_violation");
23   return 0;
24 )
25
26 end Entry
```

```
1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R1 implements Record {
11   public project.Entrytypes.R2 r2;
```



## Appendix C. Validation of the translation rules

```

12  // @ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14  public R1(final project.Entrytypes.R2 _r2) {
15
16      // @ assert Utils.is_(_r2,project.Entrytypes.R2.class);
17
18      r2 = _r2 != null ? Utils.copy(_r2) : null;
19      // @ assert Utils.is_(r2,project.Entrytypes.R2.class);
20
21  }
22  /* @ pure @ */
23
24  public boolean equals(final Object obj) {
25
26      if (!(obj instanceof project.Entrytypes.R1)) {
27          return false;
28      }
29
30      project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32      return Utils.equals(r2, other.r2);
33  }
34  /* @ pure @ */
35
36  public int hashCode() {
37
38      return Utils.hashCode(r2);
39  }
40  /* @ pure @ */
41
42  public project.Entrytypes.R1 copy() {
43
44      return new project.Entrytypes.R1(r2);
45  }
46  /* @ pure @ */
47
48  public String toString() {
49
50      return "mk_Entry 'R1" + Utils.formatFields(r2);
51  }
52  /* @ pure @ */
53
54  public project.Entrytypes.R2 get_r2() {
55
56      project.Entrytypes.R2 ret_1 = r2;
57      // @ assert project.Entry.invChecksOn ==> (Utils.is_(ret_1,project.
          Entrytypes.R2.class));
58
59      return ret_1;
60  }
61
62  public void set_r2(final project.Entrytypes.R2 _r2) {
63
64      // @ assert project.Entry.invChecksOn ==> (Utils.is_(_r2,project.
          Entrytypes.R2.class));
65
66      r2 = _r2;
67      // @ assert project.Entry.invChecksOn ==> (Utils.is_(r2,project.
          Entrytypes.R2.class));
68

```

## Appendix C. Validation of the translation rules

```

69     }
70     /*@ pure @*/
71     /*@ helper @*/
72
73     public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
74
75         return !(Utils.equals(_r2.x, -1L));
76     }
77 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R2 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(x);
13
14     public R2(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17
18         x = _x;
19         //@ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R2)) {
27             return false;
28         }
29
30         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.R2 copy() {
43
44         return new project.Entrytypes.R2(x);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`R2" + Utils.formatFields(x);

```

## Appendix C. Validation of the translation rules

```

51     }
52     /*@ pure @*/
53
54     public Number get_x() {
55
56         Number ret_2 = x;
57         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59         return ret_2;
60     }
61
62     public void set_x(final Number _x) {
63
64         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66         x = _x;
67         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69     }
70     /*@ pure @*/
71     /*@ helper @*/
72
73     public static Boolean inv_R2(final Number _x) {
74
75         return !(Utils.equals(_x, -2L));
76     }
77 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  /*@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Object r1 = new project.Entrytypes.R1(new project.Entrytypes.R2(5L));
18         /*@ assert (Utils.is_(r1,project.Entrytypes.R1.class) || Utils.is_nat(r1
19             ));
20
21         project.Entrytypes.R2 apply_1 = null;
22         if (r1 instanceof project.Entrytypes.R1) {
23             apply_1 = ((project.Entrytypes.R1) r1).get_r2();
24             /*@ assert Utils.is_(apply_1,project.Entrytypes.R2.class);
25
26         } else {
27             throw new RuntimeException("Missing_member:_r2");
28         }
29
30         project.Entrytypes.R2 stateDes_1 = apply_1;
31         /*@ assert stateDes_1 != null;

```

```

32     stateDes_1.set_x(-1L);
33     //@ assert (Utils.is_(r1,project.Entrytypes.R1.class) || Utils.is_nat(r1
        ));
34
35     //@ assert r1 instanceof project.Entrytypes.R1 ==> \invariant_for(((
        project.Entrytypes.R1) r1));
36
37     IO.println(
38         "\\invariant_for_is_not_implemented_in_OpenJML_RAC_"
39         + "so_the_\\invariant_for_check_will_not_detect_the_invariant_
            violation");
40     return 0L;
41 }
42
43 public String toString() {
44
45     return "Entry{}";
46 }
47 }

```

"\invariant\_for is not implemented in OpenJML RAC so the \invariant\_for check will not detect the invariant violation"

## C.41 Simple.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6 types
7
8 R1 :: r2 : R2
9 inv r1 == r1.r2.x <> -1;
10
11 R2 :: x : int
12 inv r2 == r2.x <> -2;
13
14 operations
15
16 Run: () ==> ?
17 Run () ==
18 (
19     dcl r1 : R1 := mk_R1(mk_R2(5));
20     r1.r2.x := -1;
21     IO.println("\\invariant_for_is_not_implemented_in_OpenJML_RAC_" ^
22         "so_the_\\invariant_for_check_will_not_detect_the_invariant_violation");
23     return 0;
24 )
25 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;

```

## Appendix C. Validation of the translation rules

```

6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R1 implements Record {
11     public project.Entrytypes.R2 r2;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14     public R1(final project.Entrytypes.R2 _r2) {
15
16         // @ assert Utils.is_(_r2, project.Entrytypes.R2.class);
17
18         r2 = _r2 != null ? Utils.copy(_r2) : null;
19         // @ assert Utils.is_(r2, project.Entrytypes.R2.class);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R1)) {
27             return false;
28         }
29
30         project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32         return Utils.equals(r2, other.r2);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(r2);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.R1 copy() {
43
44         return new project.Entrytypes.R1(r2);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry `R1" + Utils.formatFields(r2);
51     }
52     /* @ pure @ */
53
54     public project.Entrytypes.R2 get_r2() {
55
56         project.Entrytypes.R2 ret_1 = r2;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_(ret_1, project.
58             Entrytypes.R2.class));
59
60         return ret_1;
61     }
62
63     public void set_r2(final project.Entrytypes.R2 _r2) {
64
65         // @ assert project.Entry.invChecksOn ==> (Utils.is_(_r2, project.

```

## Appendix C. Validation of the translation rules

```

        Entrytypes.R2.class));
65
66     r2 = _r2;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r2,project.
        Entrytypes.R2.class));
68
69 }
70 /*@ pure @*/
71 /*@ helper @*/
72
73 public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
74
75     return !(Utils.equals(_r2.x, -1L));
76 }
77 }

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R2 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(x);
13
14     public R2(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17
18         x = _x;
19         //@ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R2)) {
27             return false;
28         }
29
30         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.R2 copy() {
43
44         return new project.Entrytypes.R2(x);

```

## Appendix C. Validation of the translation rules

```

45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`R2" + Utils.formatFields(x);
51     }
52     /*@ pure @*/
53
54     public Number get_x() {
55
56         Number ret_2 = x;
57         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59         return ret_2;
60     }
61
62     public void set_x(final Number _x) {
63
64         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66         x = _x;
67         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69     }
70     /*@ pure @*/
71     /*@ helper @*/
72
73     public static Boolean inv_R2(final Number _x) {
74
75         return !(Utils.equals(_x, -2L));
76     }
77 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  /*@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         project.Entrytypes.R1 r1 = new project.Entrytypes.R1(new project.
18             Entrytypes.R2(5L));
19         /*@ assert Utils.is_(r1,project.Entrytypes.R1.class);
20
21         project.Entrytypes.R2 stateDes_1 = r1.get_r2();
22         /*@ assert stateDes_1 != null;
23
24         stateDes_1.set_x(-1L);
25         /*@ assert Utils.is_(r1,project.Entrytypes.R1.class);

```

```

26      //@ assert \invariant_for(r1);
27
28      IO.println(
29          "\\invariant_for_is_not_implemented_in_OpenJML_RAC_"
30          + "so_the_\\invariant_for_check_will_not_detect_the_invariant_
              violation");
31      return 0L;
32  }
33
34  public String toString() {
35
36      return "Entry{}";
37  }
38  }

```

```

"\\invariant_for is not implemented in OpenJML RAC so the \\invariant_for check
will not detect the invariant violation"

```

## C.42 AtomicRecUnion.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6  types
7
8  R1 :: r2 : R2
9  inv r1 == r1.r2.x <> -1;
10
11 R2 :: x : int
12 inv r2 == r2.x <> -2;
13
14 operations
15
16 Run: () ==> ?
17 Run () ==
18 (
19     dcl r1 : R1 | nat := mk_R1(mk_R2(5));
20
21     atomic
22     (
23         r1.r2.x := -1;
24         r1.r2.x := 1;
25     );
26
27     IO`println("\\invariant_for_is_not_implemented_in_OpenJML_RAC_" ^
28         "so_the_\\invariant_for_check_will_not_detect_the_invariant_violation");
29     return 0;
30 )
31 end Entry

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;

```



## Appendix C. Validation of the translation rules

```
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R1 implements Record {
11     public project.Entrytypes.R2 r2;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14     public R1(final project.Entrytypes.R2 _r2) {
15
16         // @ assert Utils.is_(_r2,project.Entrytypes.R2.class);
17
18         r2 = _r2 != null ? Utils.copy(_r2) : null;
19         // @ assert Utils.is_(r2,project.Entrytypes.R2.class);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R1)) {
27             return false;
28         }
29
30         project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32         return Utils.equals(r2, other.r2);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(r2);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.R1 copy() {
43
44         return new project.Entrytypes.R1(r2);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry`R1" + Utils.formatFields(r2);
51     }
52     /* @ pure @ */
53
54     public project.Entrytypes.R2 get_r2() {
55
56         project.Entrytypes.R2 ret_1 = r2;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_(ret_1,project.
58             Entrytypes.R2.class));
59
60         return ret_1;
61     }
62
63     public void set_r2(final project.Entrytypes.R2 _r2) {
```

## Appendix C. Validation of the translation rules

```

64      // @ assert project.Entry.invChecksOn ==> (Utils.is_(_r2, project.
        Entrytypes.R2.class));
65
66      r2 = _r2;
67      // @ assert project.Entry.invChecksOn ==> (Utils.is_(_r2, project.
        Entrytypes.R2.class));
68
69  }
70  /* @ pure */
71  /* @ helper */
72
73  public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
74
75      return !(Utils.equals(_r2.x, -1L));
76  }
77  }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  // @ nullable_by_default
9
10 final public class R2 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R2(x);
13
14     public R2(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R2)) {
27             return false;
28         }
29
30         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /* @ pure */
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /* @ pure */
41
42     public project.Entrytypes.R2 copy() {
43

```

## Appendix C. Validation of the translation rules

```

44     return new project.Entrytypes.R2(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R2" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_2 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59     return ret_2;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71 /*@ helper @*/
72
73 public static Boolean inv_R2(final Number _x) {
74
75     return !(Utils.equals(_x, -2L));
76 }
77 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Object r1 = new project.Entrytypes.R1(new project.Entrytypes.R2(5L));
18         //@ assert (Utils.is_(r1,project.Entrytypes.R1.class) || Utils.is_nat(r1
19             ));
20
21         Number atomicTmp_1 = -1L;
22         //@ assert Utils.is_int(atomicTmp_1);
23
24         Number atomicTmp_2 = 1L;
25         //@ assert Utils.is_int(atomicTmp_2);

```

## Appendix C. Validation of the translation rules

```

25 {
26     /* Start of atomic statement */
27     //@ set invChecksOn = false;
28
29     project.Entrytypes.R2 apply_1 = null;
30     if (r1 instanceof project.Entrytypes.R1) {
31         apply_1 = ((project.Entrytypes.R1) r1).get_r2();
32     } else {
33         throw new RuntimeException("Missing_member:_r2");
34     }
35
36     project.Entrytypes.R2 stateDes_1 = apply_1;
37     //@ assert stateDes_1 != null;
38
39     stateDes_1.set_x(atomicTmp_1);
40
41     project.Entrytypes.R2 apply_2 = null;
42     if (r1 instanceof project.Entrytypes.R1) {
43         apply_2 = ((project.Entrytypes.R1) r1).get_r2();
44     } else {
45         throw new RuntimeException("Missing_member:_r2");
46     }
47
48     project.Entrytypes.R2 stateDes_2 = apply_2;
49     //@ assert stateDes_2 != null;
50
51     stateDes_2.set_x(atomicTmp_2);
52
53     //@ set invChecksOn = true;
54
55     //@ assert \invariant_for(stateDes_1);
56
57     //@ assert (Utils.is_(r1,project.Entrytypes.R1.class) || Utils.is_nat(
58         r1));
59
60     //@ assert r1 instanceof project.Entrytypes.R1 ==> \invariant_for(((
61         project.Entrytypes.R1) r1));
62
63     //@ assert \invariant_for(stateDes_2);
64 } /* End of atomic statement */
65
66 IO.println(
67     "\\invariant_for_is_not_implemented_in_OpenJML_RAC_"
68     + "so_the_\\invariant_for_check_will_not_detect_the_invariant_
69     violation");
70 return 0L;
71 }
72
73 public String toString() {
74     return "Entry{}";
75 }
76 }

```

"\invariant\_for is not implemented in OpenJML RAC so the \invariant\_for check will not detect the invariant violation"

## C.43 SetEvenNamedTypeInv.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 SetEven = set of Even;
10 Even = nat
11 inv e == e mod 2 = 0;
12
13 operations
14
15 Run : () ==> ?
16 Run () ==
17 (
18   IO`println("Before_legal_use");
19   let - : SetEven = {2, 4, 6} in skip;
20   IO`println("After_legal_use");
21   IO`println("Before_illegal_use");
22   let xs : SetEven = {2},
23       ys : set of nat = {1},
24       - : SetEven = xs union ys
25   in
26     skip;
27   IO`println("After_illegal_use");
28   return 0;
29 );
30
31 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       final VDMSet ignorePattern_1 = SetUtil.set(2L, 4L, 6L);
20       //@ assert ((V2J.isSet(ignorePattern_1) && (\forallall int i; 0 <= i && i
21         < V2J.size(ignorePattern_1); (Utils.is_nat(V2J.get(
22           ignorePattern_1,i)) && inv_Entry_Even(V2J.get(ignorePattern_1,i)))
23         )) && inv_Entry_SetEven(ignorePattern_1));

```

## Appendix C. Validation of the translation rules

```

22     /* skip */
23 }
24
25 IO.println("After_legal_use");
26 IO.println("Before_illegal_use");
27 {
28     final VDMSet xs = SetUtil.set(2L);
29     //@ assert ((V2J.isSet(xs) && (\forallall int i; 0 <= i && i < V2J.size(
        xs); (Utils.is_nat(V2J.get(xs,i)) && inv_Entry_Even(V2J.get(xs,i))
        ))) && inv_Entry_SetEven(xs));
30
31     final VDMSet ys = SetUtil.set(1L);
32     //@ assert (V2J.isSet(ys) && (\forallall int i; 0 <= i && i < V2J.size(ys
        ); Utils.is_nat(V2J.get(ys,i)))));
33
34     final VDMSet ignorePattern_2 = SetUtil.union(Utils.copy(xs), Utils.
        copy(ys));
35     //@ assert ((V2J.isSet(ignorePattern_2) && (\forallall int i; 0 <= i && i
        < V2J.size(ignorePattern_2); (Utils.is_nat(V2J.get(
        ignorePattern_2,i)) && inv_Entry_Even(V2J.get(ignorePattern_2,i)))
        )) && inv_Entry_SetEven(ignorePattern_2));
36
37     /* skip */
38 }
39
40 IO.println("After_illegal_use");
41 return 0L;
42 }
43
44 public String toString() {
45
46     return "Entry{}";
47 }
48
49 /*@ pure @*/
50 /*@ helper @*/
51
52 public static Boolean inv_Entry_SetEven(final Object check_elem) {
53
54     return true;
55 }
56
57 /*@ pure @*/
58 /*@ helper @*/
59
60 public static Boolean inv_Entry_Even(final Object check_e) {
61
62     Number e = ((Number) check_e);
63
64     return Utils.equals(Utils.mod(e.longValue(), 2L), 0L);
65 }
66 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:35: JML assertion is false
    //@ assert ((V2J.isSet(ignorePattern_2) && (\forallall int i; 0 <= i && i <
        V2J.size(ignorePattern_2); (Utils.is_nat(V2J.get(ignorePattern_2,i))
        && inv_Entry_Even(V2J.get(ignorePattern_2,i)))))) &&

```

```

        inv_Entry_SetEven(ignorePattern_2));
        ^
    "After illegal use"

```

## C.44 SetOfNat.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : set of nat = {2,4,6} in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : set of nat = setOfNat() in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 setOfNat : () -> [set of nat]
24 setOfNat () == nil;
25
26 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       final VDMSet ignorePattern_1 = SetUtil.set(2L, 4L, 6L);
20       //@ assert (V2J.isSet(ignorePattern_1) && (\forall int i; 0 <= i && i
21         < V2J.size(ignorePattern_1); Utils.is_nat(V2J.get(ignorePattern_1,

```

```

22      /* skip */
23    }
24
25    IO.println("After_legal_use");
26    IO.println("Before_illegal_use");
27    {
28      final VDMSet ignorePattern_2 = setOfNat();
29      //@ assert (V2J.isSet(ignorePattern_2) && (\forallall int i; 0 <= i && i
        < V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2,
        i))));
30
31      /* skip */
32    }
33
34    IO.println("After_illegal_use");
35    return 0L;
36  }
37  /*@ pure @*/
38
39  public static VDMSet setOfNat() {
40
41    VDMSet ret_1 = null;
42    //@ assert ((ret_1 == null) || (V2J.isSet(ret_1) && (\forallall int i; 0 <=
        i && i < V2J.size(ret_1); Utils.is_nat(V2J.get(ret_1,i))));
43
44    return Utils.copy(ret_1);
45  }
46
47  public String toString() {
48
49    return "Entry{}";
50  }
51 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isSet(ignorePattern_2) && (\forallall int i; 0 <= i && i <
        V2J.size(ignorePattern_2); Utils.is_nat(V2J.get(ignorePattern_2,i)))
        ;
        ^
"After illegal use"

```

## C.45 SetPassNil.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==

```



## Appendix C. Validation of the translation rules

```

11 (
12   IO.println("Before_legal_use");
13   (dcl r : set of bool := idSet({true, false}); skip);
14   IO.println("After_legal_use");
15   IO.println("Before_illegal_use");
16   (
17     dcl xs : [set of bool] := nil;
18     dcl r : set of bool := idSet(xs);
19     skip;
20   );
21   IO.println("After_illegal_use");
22   return 0;
23 );
24
25 functions
26
27 idSet : set of bool -> set of bool
28 idSet (xs) ==
29   xs;
30
31 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       VDMSet r = idSet(SetUtil.set(true, false));
20       /* @ assert (V2J.isSet(r) && (\forallall int i; 0 <= i && i < V2J.size(r);
21         Utils.is_bool(V2J.get(r,i)))));
22
23       /* skip */
24     }
25
26     IO.println("After_legal_use");
27     IO.println("Before_illegal_use");
28     {
29       VDMSet xs = null;
30       /* @ assert ((xs == null) || (V2J.isSet(xs) && (\forallall int i; 0 <= i
31         && i < V2J.size(xs); Utils.is_bool(V2J.get(xs,i)))));
32
33       VDMSet r = idSet(Utils.copy(xs));
34       /* @ assert (V2J.isSet(r) && (\forallall int i; 0 <= i && i < V2J.size(r);
35         Utils.is_bool(V2J.get(r,i)))));
36
37       /* skip */
38     }
39

```

```

36
37     IO.println("After_illegal_use");
38     return 0L;
39 }
40 /*@ pure @*/
41
42 public static VDMSet idSet(final VDMSet xs) {
43
44     //@ assert (V2J.isSet(xs) && (\forallall int i; 0 <= i && i < V2J.size(xs);
45         Utils.is_bool(V2J.get(xs,i))));
46
47     VDMSet ret_1 = Utils.copy(xs);
48     //@ assert (V2J.isSet(ret_1) && (\forallall int i; 0 <= i && i < V2J.size(
49         ret_1); Utils.is_bool(V2J.get(ret_1,i))));
50
51     return Utils.copy(ret_1);
52 }
53
54 public String toString() {
55
56     return "Entry{}";
57 }
58 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:44: JML assertion is false
    //@ assert (V2J.isSet(xs) && (\forallall int i; 0 <= i && i < V2J.size(xs);
        Utils.is_bool(V2J.get(xs,i))));
        ^
Entry.java:47: JML assertion is false
    //@ assert (V2J.isSet(ret_1) && (\forallall int i; 0 <= i && i < V2J.size(
        ret_1); Utils.is_bool(V2J.get(ret_1,i))));
        ^
Entry.java:32: JML assertion is false
    //@ assert (V2J.isSet(r) && (\forallall int i; 0 <= i && i < V2J.size(r);
        Utils.is_bool(V2J.get(r,i))));
        ^
"After illegal use"

```

## C.46 RecTypesUnion.vdmsl

```

1 module Entry
2
3 imports from IO all
4 exports all
5
6 definitions
7
8 types
9 R1 :: x : int
10 inv r1 == r1.x > 0;
11
12 R2 :: x : int
13 inv r2 == r2.x > 0;

```

## Appendix C. Validation of the translation rules

```

14
15 operations
16
17 Run : () ==> ?
18 Run () ==
19 (dcl r : R1 | R2 := mk_R1(1);
20
21   IO`println("Before_valid_use");
22   r.x := 5;
23   IO`println("After_valid_use");
24
25   IO`println("Before_illegal_use");
26   r.x := -5;
27   IO`println("After_illegal_use");
28
29   return 0;
30 )
31
32 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R1 implements Record {
11   public Number x;
12   //@ public instance invariant project.Entry.invChecksOn ==> inv_R1(x);
13
14   public R1(final Number _x) {
15
16     //@ assert Utils.is_int(_x);
17
18     x = _x;
19     //@ assert Utils.is_int(x);
20
21   }
22   /*@ pure @*/
23
24   public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.R1)) {
27       return false;
28     }
29
30     project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32     return Utils.equals(x, other.x);
33   }
34   /*@ pure @*/
35
36   public int hashCode() {
37
38     return Utils.hashCode(x);
39   }
40   /*@ pure @*/

```

## Appendix C. Validation of the translation rules

```

41
42 public project.Entrytypes.R1 copy() {
43
44     return new project.Entrytypes.R1(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry'R1" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_1 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_1));
58
59     return ret_1;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R1(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 /*@ nullable_by_default
9
10 final public class R2 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(x);
13
14     public R2(final Number _x) {
15
16         //@ assert Utils.is_int(_x);

```

## Appendix C. Validation of the translation rules

```

17
18     x = _x;
19     //@ assert Utils.is_int(x);
20
21 }
22 /*@ pure @*/
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.R2)) {
27         return false;
28     }
29
30     project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R2 copy() {
43
44     return new project.Entrytypes.R2(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R2" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_2 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59     return ret_2;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/

```

## Appendix C. Validation of the translation rules

```

77  /*@ helper @*/
78
79  public static Boolean inv_R2(final Number _x) {
80
81      return _x.longValue() > 0L;
82  }
83  }

```

---

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Object r = new project.Entrytypes.R1(1L);
18         //@ assert (Utils.is_(r,project.Entrytypes.R1.class) || Utils.is_(r,
19             project.Entrytypes.R2.class));
20
21         IO.println("Before_valid_use");
22         if (r instanceof project.Entrytypes.R1) {
23             //@ assert r != null;
24
25             ((project.Entrytypes.R1) r).set_x(5L);
26
27         } else if (r instanceof project.Entrytypes.R2) {
28             //@ assert r != null;
29
30             ((project.Entrytypes.R2) r).set_x(5L);
31
32         } else {
33             throw new RuntimeException("Missing_member:_x");
34         }
35
36         IO.println("After_valid_use");
37         IO.println("Before_illegal_use");
38         if (r instanceof project.Entrytypes.R1) {
39             //@ assert r != null;
40
41             ((project.Entrytypes.R1) r).set_x(-5L);
42
43         } else if (r instanceof project.Entrytypes.R2) {
44             //@ assert r != null;
45
46             ((project.Entrytypes.R2) r).set_x(-5L);
47
48         } else {
49             throw new RuntimeException("Missing_member:_x");
50         }
51
52         IO.println("After_illegal_use");

```

```

52     return 0L;
53 }
54
55 public String toString() {
56
57     return "Entry{}";
58 }
59 }

```

```

"Before valid use"
"After valid use"
"Before illegal use"
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/RecTypesUnion/
project/Entrytypes/R1.java:62: JML invariant is false on leaving method
project.Entrytypes.R1.set_x(java.lang.Number)
public void set_x(final Number _x) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/RecTypesUnion/
project/Entrytypes/R1.java:12: Associated declaration: /home/peter/git-
repos/ovt/core/codegen/vdm2jml/target/jml/code/RecTypesUnion/project/
Entrytypes/R1.java:62:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R1(x);
    ^
"After illegal use"

```

## C.47 OptionalBasicUnion.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   (
14     dcl a : nat1 | char | bool := true;
15     a := 1;
16     a := 'a';
17     a := true;
18   );
19   (
20     dcl b : [nat1 | char] | bool := true;
21     b := nil;
22   );
23   IO`println("After_legal_use");
24   IO`println("Before_illegal_use");
25   (
26     dcl a : nat1 | char | bool := charNil();
27     skip;
28   );
29   IO`println("After_illegal_use");

```

## Appendix C. Validation of the translation rules

```
30 | return 0;
31 | );
32 |
33 | functions
34 |
35 | charNil : () -> [char]
36 | charNil () == nil;
37 |
38 | end Entry
```

---

```
1 | package project;
2 |
3 | import java.util.*;
4 | import org.overture.codegen.runtime.*;
5 | import org.overture.codegen.vdm2jml.runtime.*;
6 |
7 | @SuppressWarnings("all")
8 | //@ nullable_by_default
9 |
10 | final public class Entry {
11 |     /*@ public ghost static boolean invChecksOn = true; @*/
12 |
13 |     private Entry() {}
14 |
15 |     public static Object Run() {
16 |
17 |         IO.println("Before_legal_use");
18 |         {
19 |             Object a = true;
20 |             //@ assert (Utils.is_bool(a) || Utils.is_char(a) || Utils.is_nat1(a));
21 |
22 |             a = 1L;
23 |             //@ assert (Utils.is_bool(a) || Utils.is_char(a) || Utils.is_nat1(a));
24 |
25 |             a = 'a';
26 |             //@ assert (Utils.is_bool(a) || Utils.is_char(a) || Utils.is_nat1(a));
27 |
28 |             a = true;
29 |             //@ assert (Utils.is_bool(a) || Utils.is_char(a) || Utils.is_nat1(a));
30 |
31 |         }
32 |
33 |         {
34 |             Object b = true;
35 |             //@ assert ((b == null) || Utils.is_char(b) || Utils.is_nat1(b)) ||
36 |                 Utils.is_bool(b));
37 |
38 |             b = null;
39 |             //@ assert ((b == null) || Utils.is_char(b) || Utils.is_nat1(b)) ||
40 |                 Utils.is_bool(b));
41 |
42 |         }
43 |
44 |         IO.println("After_legal_use");
45 |         IO.println("Before_illegal_use");
46 |         {
47 |             Object a = charNil();
48 |             //@ assert (Utils.is_bool(a) || Utils.is_char(a) || Utils.is_nat1(a));
49 |
50 |             /* skip */
```



```

49     }
50
51     IO.println("After_illegal_use");
52     return 0L;
53 }
54 /*@ pure @*/
55
56 public static Character charNil() {
57
58     Character ret_1 = null;
59     //@ assert ((ret_1 == null) || Utils.is_char(ret_1));
60
61     return ret_1;
62 }
63
64 public String toString() {
65
66     return "Entry{}";
67 }
68 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:46: JML assertion is false
    //@ assert (Utils.is_bool(a) || Utils.is_char(a) || Utils.is_nat1(a));
           ^
"After illegal use"

```

## C.48 RecWithRecFieldUpdate.vdmsl

```

1  module Entry
2
3  imports from IO all
4  exports all
5
6  definitions
7
8  types
9  A1 :: f : A2
10 inv a1 == a1.f.x > 0;
11
12 A2 :: x : int
13 inv a2 == a2.x > 0;
14
15 B1 :: f : B2
16 inv b1 == b1.f.x > 0;
17
18 B2 :: x : int
19 inv b2 == b2.x > 0;
20
21
22 operations
23
24 Run : () ==> ?
25 Run () ==

```

## Appendix C. Validation of the translation rules

```

26 (dcl r : A1 | B1 := mk_A1(mk_A2(1));
27
28 IO`println("Before_valid_use");
29 r.f.x := 5;
30 IO`println("After_valid_use");
31
32 IO`println("Before_illegal_use");
33 r.f.x := -5;
34 IO`println("After_illegal_use");
35
36 return 0;
37 )
38
39 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class B2 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_B2(x);
13
14     public B2(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.B2)) {
27             return false;
28         }
29
30         project.Entrytypes.B2 other = ((project.Entrytypes.B2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.B2 copy() {
43
44         return new project.Entrytypes.B2(x);
45     }

```

## Appendix C. Validation of the translation rules

```

46  /*@ pure @*/
47
48  public String toString() {
49
50      return "mk_Entry`B2" + Utils.formatFields(x);
51  }
52  /*@ pure @*/
53
54  public Number get_x() {
55
56      Number ret_4 = x;
57      /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_4));
58
59      return ret_4;
60  }
61
62  public void set_x(final Number _x) {
63
64      /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66      x = _x;
67      /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69  }
70  /*@ pure @*/
71
72  public Boolean valid() {
73
74      return true;
75  }
76  /*@ pure @*/
77  /*@ helper @*/
78
79  public static Boolean inv_B2(final Number _x) {
80
81      return _x.longValue() > 0L;
82  }
83  }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  /*@ nullable_by_default
9
10 final public class A1 implements Record {
11     public project.Entrytypes.A2 f;
12     /*@ public instance invariant project.Entry.invChecksOn ==> inv_A1(f);
13
14     public A1(final project.Entrytypes.A2 _f) {
15
16         /*@ assert Utils.is(_f,project.Entrytypes.A2.class);
17
18         f = _f != null ? Utils.copy(_f) : null;
19         /*@ assert Utils.is(f,project.Entrytypes.A2.class);
20
21     }

```

## Appendix C. Validation of the translation rules

```

22  /*@ pure @*/
23
24  public boolean equals(final Object obj) {
25
26      if (!(obj instanceof project.Entrytypes.A1)) {
27          return false;
28      }
29
30      project.Entrytypes.A1 other = ((project.Entrytypes.A1) obj);
31
32      return Utils.equals(f, other.f);
33  }
34  /*@ pure @*/
35
36  public int hashCode() {
37
38      return Utils.hashCode(f);
39  }
40  /*@ pure @*/
41
42  public project.Entrytypes.A1 copy() {
43
44      return new project.Entrytypes.A1(f);
45  }
46  /*@ pure @*/
47
48  public String toString() {
49
50      return "mk_Entry `A1" + Utils.formatFields(f);
51  }
52  /*@ pure @*/
53
54  public project.Entrytypes.A2 get_f() {
55
56      project.Entrytypes.A2 ret_1 = f;
57      //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_1,project.
          Entrytypes.A2.class));
58
59      return ret_1;
60  }
61
62  public void set_f(final project.Entrytypes.A2 _f) {
63
64      //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.
          Entrytypes.A2.class));
65
66      f = _f;
67      //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.Entrytypes
          .A2.class));
68
69  }
70  /*@ pure @*/
71
72  public Boolean valid() {
73
74      return true;
75  }
76  /*@ pure @*/
77  /*@ helper @*/
78

```

## Appendix C. Validation of the translation rules

```
79 public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
80
81     return _f.x.longValue() > 0L;
82 }
83 }
```

```
1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Object r = new project.Entrytypes.A1(new project.Entrytypes.A2(1L));
18         //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
19             project.Entrytypes.B1.class));
20
21         IO.println("Before_valid_use");
22         Object apply_1 = null;
23         if (r instanceof project.Entrytypes.A1) {
24             apply_1 = ((project.Entrytypes.A1) r).get_f();
25             //@ assert (Utils.is_(apply_1,project.Entrytypes.A2.class) || Utils.
26                 is_(apply_1,project.Entrytypes.B2.class));
27
28         } else if (r instanceof project.Entrytypes.B1) {
29             apply_1 = ((project.Entrytypes.B1) r).get_f();
30             //@ assert (Utils.is_(apply_1,project.Entrytypes.A2.class) || Utils.
31                 is_(apply_1,project.Entrytypes.B2.class));
32
33         } else {
34             throw new RuntimeException("Missing_member:_f");
35         }
36
37         Object stateDes_1 = apply_1;
38         if (stateDes_1 instanceof project.Entrytypes.A2) {
39             //@ assert stateDes_1 != null;
40
41             ((project.Entrytypes.A2) stateDes_1).set_x(5L);
42             //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
43                 project.Entrytypes.B1.class));
44
45             //@ assert r instanceof project.Entrytypes.B1 ==> ((project.Entrytypes
46                 .B1) r).valid();
47
48             //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
49                 .A1) r).valid();
50
51         } else if (stateDes_1 instanceof project.Entrytypes.B2) {
52             //@ assert stateDes_1 != null;
53
54             ((project.Entrytypes.B2) stateDes_1).set_x(5L);
55         }
56     }
57 }
```

## Appendix C. Validation of the translation rules

```
49      //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
50      project.Entrytypes.B1.class));
51
52      //@ assert r instanceof project.Entrytypes.B1 ==> ((project.Entrytypes
53      .B1) r).valid();
54
55      //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
56      .A1) r).valid();
57
58      } else {
59      throw new RuntimeException("Missing_member:_x");
60      }
61
62      IO.println("After_valid_use");
63      IO.println("Before_illegal_use");
64      Object apply_2 = null;
65      if (r instanceof project.Entrytypes.A1) {
66      apply_2 = ((project.Entrytypes.A1) r).get_f();
67      //@ assert (Utils.is_(apply_2,project.Entrytypes.A2.class) || Utils.
68      is_(apply_2,project.Entrytypes.B2.class));
69
70      } else if (r instanceof project.Entrytypes.B1) {
71      apply_2 = ((project.Entrytypes.B1) r).get_f();
72      //@ assert (Utils.is_(apply_2,project.Entrytypes.A2.class) || Utils.
73      is_(apply_2,project.Entrytypes.B2.class));
74
75      } else {
76      throw new RuntimeException("Missing_member:_f");
77      }
78
79      Object stateDes_2 = apply_2;
80      if (stateDes_2 instanceof project.Entrytypes.A2) {
81      //@ assert stateDes_2 != null;
82
83      ((project.Entrytypes.A2) stateDes_2).set_x(-5L);
84      //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
85      project.Entrytypes.B1.class));
86
87      //@ assert r instanceof project.Entrytypes.B1 ==> ((project.Entrytypes
88      .B1) r).valid();
89
90      //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
91      .A1) r).valid();
92
93      //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
94      .A1) r).valid();
95
96      } else {
97      throw new RuntimeException("Missing_member:_x");
98      }
```

## Appendix C. Validation of the translation rules

```

98
99     IO.println("After_illegal_use");
100     return 0L;
101 }
102
103 public String toString() {
104
105     return "Entry{}";
106 }
107 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class B1 implements Record {
11     public project.Entrytypes.B2 f;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_B1(f);
13
14     public B1(final project.Entrytypes.B2 _f) {
15
16         //@ assert Utils.is_(_f,project.Entrytypes.B2.class);
17
18         f = _f != null ? Utils.copy(_f) : null;
19         //@ assert Utils.is_(f,project.Entrytypes.B2.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.B1)) {
27             return false;
28         }
29
30         project.Entrytypes.B1 other = ((project.Entrytypes.B1) obj);
31
32         return Utils.equals(f, other.f);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(f);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.B1 copy() {
43
44         return new project.Entrytypes.B1(f);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49

```

## Appendix C. Validation of the translation rules

```

50     return "mk_Entry`B1" + Utils.formatFields(f);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.B2 get_f() {
55
56     project.Entrytypes.B2 ret_3 = f;
57     /*@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
        Entrytypes.B2.class));
58
59     return ret_3;
60 }
61
62 public void set_f(final project.Entrytypes.B2 _f) {
63
64     /*@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.
        Entrytypes.B2.class));
65
66     f = _f;
67     /*@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.Entrytypes
        .B2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_B1(final project.Entrytypes.B2 _f) {
80
81     return _f.x.longValue() > 0L;
82 }
83 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  /*@ nullable_by_default
9
10 final public class A2 implements Record {
11     public Number x;
12     /*@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
13
14     public A2(final Number _x) {
15
16         /*@ assert Utils.is_int(_x);
17
18         x = _x;
19         /*@ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/

```



## Appendix C. Validation of the translation rules

```
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.A2)) {
27         return false;
28     }
29
30     project.Entrytypes.A2 other = ((project.Entrytypes.A2) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.A2 copy() {
43
44     return new project.Entrytypes.A2(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry'A2" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_2 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59     return ret_2;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_A2(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
```

```

"Before valid use"
"After valid use"
"Before illegal use"
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:62: JML invariant is false
    on leaving method project.Entrytypes.A2.set_x(java.lang.Number)
  public void set_x(final Number _x) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:12: Associated declaration
    : /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:62:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79: JML caller invariant
    is false on leaving calling method (Parameter: _f, Caller: project.
    Entrytypes.A1.inv_A1(project.Entrytypes.A2), Callee: java.lang.Number.
    longValue())
  public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:12: Associated declaration
    : /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79: JML invariant is false
    on leaving method project.Entrytypes.A1.inv_A1(project.Entrytypes.A2) (
    parameter _f)
  public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:12: Associated declaration
    : /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79: JML caller invariant
    is false on leaving calling method (Parameter: _f, Caller: project.
    Entrytypes.A1.inv_A1(project.Entrytypes.A2), Callee: java.lang.Number.
    longValue())
  public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:12: Associated declaration
    : /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79: JML invariant is false
    on leaving method project.Entrytypes.A1.inv_A1(project.Entrytypes.A2) (
    parameter _f)
  public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^

```

```

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:12: Associated declaration
  : /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
      ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:72: JML invariant is false
  on leaving method project.Entrytypes.A1.valid()
  public Boolean valid() {
      ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:12: Associated declaration
  : /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A1.java:72:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A1(f);
      ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldUpdate/project/Entrytypes/A2.java:12: JML invariant is false
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
      ^

"After illegal use"

```

## C.49 RecWithRecFieldAtomicViolation.vdmsl

```

1  module Entry
2
3  imports from IO all
4  exports all
5
6  definitions
7
8  types
9  A1 :: f : A2
10 inv a1 == a1.f.x > 0;
11
12 A2 :: x : int
13 inv a2 == a2.x > 0;
14
15 B1 :: f : B2
16 inv b1 == b1.f.x > 0;
17
18 B2 :: x : int
19 inv b2 == b2.x > 0;
20
21
22 operations
23
24 Run : () ==> ?
25 Run () ==
26 (dcl r : A1 | B1 := mk_A1(mk_A2(1));
27
28   IO`println("Before_valid_use");
29   atomic
30   (
31     r.f.x := -5;
32     r.f.x := 5;

```

## Appendix C. Validation of the translation rules

```

33  );
34  IO`println("After_valid_use");
35
36  IO`println("Before_illegal_use");
37  atomic
38  (
39    r.f.x := 5;
40    r.f.x := -5;
41  );
42  IO`println("After_illegal_use");
43
44  return 0;
45 )
46
47 end Entry

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class B2 implements Record {
11   public Number x;
12   //@ public instance invariant project.Entry.invChecksOn ==> inv_B2(x);
13
14   public B2(final Number _x) {
15
16     //@ assert Utils.is_int(_x);
17
18     x = _x;
19     //@ assert Utils.is_int(x);
20
21   }
22   /*@ pure @*/
23
24   public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.B2)) {
27       return false;
28     }
29
30     project.Entrytypes.B2 other = ((project.Entrytypes.B2) obj);
31
32     return Utils.equals(x, other.x);
33   }
34   /*@ pure @*/
35
36   public int hashCode() {
37
38     return Utils.hashCode(x);
39   }
40   /*@ pure @*/
41
42   public project.Entrytypes.B2 copy() {
43
44     return new project.Entrytypes.B2(x);

```

## Appendix C. Validation of the translation rules

```

45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`B2" + Utils.formatFields(x);
51     }
52     /*@ pure @*/
53
54     public Number get_x() {
55
56         Number ret_4 = x;
57         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_4));
58
59         return ret_4;
60     }
61
62     public void set_x(final Number _x) {
63
64         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66         x = _x;
67         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69     }
70     /*@ pure @*/
71
72     public Boolean valid() {
73
74         return true;
75     }
76     /*@ pure @*/
77     /*@ helper @*/
78
79     public static Boolean inv_B2(final Number _x) {
80
81         return _x.longValue() > 0L;
82     }
83 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  /*@ nullable_by_default
9
10 final public class A1 implements Record {
11     public project.Entrytypes.A2 f;
12     /*@ public instance invariant project.Entry.invChecksOn ==> inv_A1(f);
13
14     public A1(final project.Entrytypes.A2 _f) {
15
16         /*@ assert Utils.is_(_f,project.Entrytypes.A2.class);
17
18         f = _f != null ? Utils.copy(_f) : null;
19         /*@ assert Utils.is_(f,project.Entrytypes.A2.class);
20

```

## Appendix C. Validation of the translation rules

```

21 }
22 /*@ pure @*/
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.A1)) {
27         return false;
28     }
29
30     project.Entrytypes.A1 other = ((project.Entrytypes.A1) obj);
31
32     return Utils.equals(f, other.f);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(f);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.A1 copy() {
43
44     return new project.Entrytypes.A1(f);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`A1" + Utils.formatFields(f);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.A2 get_f() {
55
56     project.Entrytypes.A2 ret_1 = f;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_1,project.
        Entrytypes.A2.class));
58
59     return ret_1;
60 }
61
62 public void set_f(final project.Entrytypes.A2 _f) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_f,project.
        Entrytypes.A2.class));
65
66     f = _f;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.Entrytypes
        .A2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/

```

## Appendix C. Validation of the translation rules

```

78
79     public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
80
81         return _f.x.longValue() > 0L;
82     }
83 }

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Object r = new project.Entrytypes.A1(new project.Entrytypes.A2(1L));
18         /* @ assert (Utils.is_(r, project.Entrytypes.A1.class) || Utils.is_(r,
19             project.Entrytypes.B1.class));
20
21         IO.println("Before_valid_use");
22         Number atomicTmp_1 = -5L;
23         /* @ assert Utils.is_int(atomicTmp_1);
24
25         Number atomicTmp_2 = 5L;
26         /* @ assert Utils.is_int(atomicTmp_2);
27
28         {
29             /* Start of atomic statement */
30             /* @ set invChecksOn = false;
31
32             Object apply_1 = null;
33             if (r instanceof project.Entrytypes.A1) {
34                 apply_1 = ((project.Entrytypes.A1) r).get_f();
35             } else if (r instanceof project.Entrytypes.B1) {
36                 apply_1 = ((project.Entrytypes.B1) r).get_f();
37             } else {
38                 throw new RuntimeException("Missing_member:_f");
39             }
40
41             Object stateDes_1 = apply_1;
42             if (stateDes_1 instanceof project.Entrytypes.A2) {
43                 /* @ assert stateDes_1 != null;
44
45                 ((project.Entrytypes.A2) stateDes_1).set_x(atomicTmp_1);
46
47             } else if (stateDes_1 instanceof project.Entrytypes.B2) {
48                 /* @ assert stateDes_1 != null;
49
50                 ((project.Entrytypes.B2) stateDes_1).set_x(atomicTmp_1);
51
52             } else {
53                 throw new RuntimeException("Missing_member:_x");

```

## Appendix C. Validation of the translation rules

```

53     }
54
55     Object apply_2 = null;
56     if (r instanceof project.Entrytypes.A1) {
57         apply_2 = ((project.Entrytypes.A1) r).get_f();
58     } else if (r instanceof project.Entrytypes.B1) {
59         apply_2 = ((project.Entrytypes.B1) r).get_f();
60     } else {
61         throw new RuntimeException("Missing_member:_f");
62     }
63
64     Object stateDes_2 = apply_2;
65     if (stateDes_2 instanceof project.Entrytypes.A2) {
66         //@ assert stateDes_2 != null;
67
68         ((project.Entrytypes.A2) stateDes_2).set_x(atomicTmp_2);
69
70     } else if (stateDes_2 instanceof project.Entrytypes.B2) {
71         //@ assert stateDes_2 != null;
72
73         ((project.Entrytypes.B2) stateDes_2).set_x(atomicTmp_2);
74
75     } else {
76         throw new RuntimeException("Missing_member:_x");
77     }
78
79     //@ set invChecksOn = true;
80
81     //@ assert stateDes_1 instanceof project.Entrytypes.A2 ==> ((project.
        Entrytypes.A2) stateDes_1).valid();
82
83     //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
        project.Entrytypes.B1.class));
84
85     //@ assert r instanceof project.Entrytypes.B1 ==> ((project.Entrytypes
        .B1) r).valid();
86
87     //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
        .A1) r).valid();
88
89     //@ assert stateDes_1 instanceof project.Entrytypes.B2 ==> ((project.
        Entrytypes.B2) stateDes_1).valid();
90
91     //@ assert stateDes_2 instanceof project.Entrytypes.A2 ==> ((project.
        Entrytypes.A2) stateDes_2).valid();
92
93     //@ assert stateDes_2 instanceof project.Entrytypes.B2 ==> ((project.
        Entrytypes.B2) stateDes_2).valid();
94
95     } /* End of atomic statement */
96
97     IO.println("After_valid_use");
98     IO.println("Before_illegal_use");
99     Number atomicTmp_3 = 5L;
100    //@ assert Utils.is_int(atomicTmp_3);
101
102    Number atomicTmp_4 = -5L;
103    //@ assert Utils.is_int(atomicTmp_4);
104
105    {

```



## Appendix C. Validation of the translation rules

```

106      /* Start of atomic statement */
107      //@ set invChecksOn = false;
108
109      Object apply_3 = null;
110      if (r instanceof project.Entrytypes.A1) {
111          apply_3 = ((project.Entrytypes.A1) r).get_f();
112      } else if (r instanceof project.Entrytypes.B1) {
113          apply_3 = ((project.Entrytypes.B1) r).get_f();
114      } else {
115          throw new RuntimeException("Missing_member:_f");
116      }
117
118      Object stateDes_3 = apply_3;
119      if (stateDes_3 instanceof project.Entrytypes.A2) {
120          //@ assert stateDes_3 != null;
121
122          ((project.Entrytypes.A2) stateDes_3).set_x(atomicTmp_3);
123
124      } else if (stateDes_3 instanceof project.Entrytypes.B2) {
125          //@ assert stateDes_3 != null;
126
127          ((project.Entrytypes.B2) stateDes_3).set_x(atomicTmp_3);
128
129      } else {
130          throw new RuntimeException("Missing_member:_x");
131      }
132
133      Object apply_4 = null;
134      if (r instanceof project.Entrytypes.A1) {
135          apply_4 = ((project.Entrytypes.A1) r).get_f();
136      } else if (r instanceof project.Entrytypes.B1) {
137          apply_4 = ((project.Entrytypes.B1) r).get_f();
138      } else {
139          throw new RuntimeException("Missing_member:_f");
140      }
141
142      Object stateDes_4 = apply_4;
143      if (stateDes_4 instanceof project.Entrytypes.A2) {
144          //@ assert stateDes_4 != null;
145
146          ((project.Entrytypes.A2) stateDes_4).set_x(atomicTmp_4);
147
148      } else if (stateDes_4 instanceof project.Entrytypes.B2) {
149          //@ assert stateDes_4 != null;
150
151          ((project.Entrytypes.B2) stateDes_4).set_x(atomicTmp_4);
152
153      } else {
154          throw new RuntimeException("Missing_member:_x");
155      }
156
157      //@ set invChecksOn = true;
158
159      //@ assert stateDes_3 instanceof project.Entrytypes.A2 ==> ((project.
        Entrytypes.A2) stateDes_3).valid();
160
161      //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
        project.Entrytypes.B1.class));
162
163      //@ assert r instanceof project.Entrytypes.B1 ==> ((project.Entrytypes

```

## Appendix C. Validation of the translation rules

```

164         .B1) r).valid();
165     //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
166         .A1) r).valid();
167     //@ assert stateDes_3 instanceof project.Entrytypes.B2 ==> ((project.
168         Entrytypes.B2) stateDes_3).valid();
169     //@ assert stateDes_4 instanceof project.Entrytypes.A2 ==> ((project.
170         Entrytypes.A2) stateDes_4).valid();
171     //@ assert stateDes_4 instanceof project.Entrytypes.B2 ==> ((project.
172         Entrytypes.B2) stateDes_4).valid();
173     } /* End of atomic statement */
174
175     IO.println("After_illegal_use");
176     return 0L;
177 }
178
179 public String toString() {
180
181     return "Entry{}";
182 }
183 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class B1 implements Record {
11     public project.Entrytypes.B2 f;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_B1(f);
13
14     public B1(final project.Entrytypes.B2 _f) {
15
16         //@ assert Utils.is_(_f,project.Entrytypes.B2.class);
17
18         f = _f != null ? Utils.copy(_f) : null;
19         //@ assert Utils.is_(f,project.Entrytypes.B2.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.B1)) {
27             return false;
28         }
29
30         project.Entrytypes.B1 other = ((project.Entrytypes.B1) obj);
31
32         return Utils.equals(f, other.f);
33     }
34     /*@ pure @*/

```

## Appendix C. Validation of the translation rules

```

35
36 public int hashCode() {
37
38     return Utils.hashCode(f);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.B1 copy() {
43
44     return new project.Entrytypes.B1(f);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`B1" + Utils.formatFields(f);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.B2 get_f() {
55
56     project.Entrytypes.B2 ret_3 = f;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
        Entrytypes.B2.class));
58
59     return ret_3;
60 }
61
62 public void set_f(final project.Entrytypes.B2 _f) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_f,project.
        Entrytypes.B2.class));
65
66     f = _f;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.Entrytypes
        .B2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_B1(final project.Entrytypes.B2 _f) {
80
81     return _f.x.longValue() > 0L;
82 }
83 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")

```

## Appendix C. Validation of the translation rules

```

8  // @ nullable_by_default
9
10 final public class A2 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
13
14     public A2(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.A2)) {
27             return false;
28         }
29
30         project.Entrytypes.A2 other = ((project.Entrytypes.A2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /* @ pure */
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /* @ pure */
41
42     public project.Entrytypes.A2 copy() {
43
44         return new project.Entrytypes.A2(x);
45     }
46     /* @ pure */
47
48     public String toString() {
49
50         return "mk_Entry'A2" + Utils.formatFields(x);
51     }
52     /* @ pure */
53
54     public Number get_x() {
55
56         Number ret_2 = x;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59         return ret_2;
60     }
61
62     public void set_x(final Number _x) {
63
64         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66         x = _x;
67         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(x));

```

## Appendix C. Validation of the translation rules

```

68
69     }
70     /*@ pure @*/
71
72     public Boolean valid() {
73
74         return true;
75     }
76     /*@ pure @*/
77     /*@ helper @*/
78
79     public static Boolean inv_A2(final Number _x) {
80
81         return _x.longValue() > 0L;
82     }
83 }

```

```

"Before valid use"
"After valid use"
"Before illegal use"
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:72: JML invariant
    is false on leaving method project.Entrytypes.A2.valid()
  public Boolean valid() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:72:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79: JML caller
  invariant is false on leaving calling method (Parameter: _f, Caller:
  project.Entrytypes.A1.inv_A1(project.Entrytypes.A2), Callee: java.lang.
  Number.longValue())
  public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79: JML invariant
  is false on leaving method project.Entrytypes.A1.inv_A1(project.Entrytypes
  .A2) (parameter _f)
  public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79: JML caller
  invariant is false on leaving calling method (Parameter: _f, Caller:
  project.Entrytypes.A1.inv_A1(project.Entrytypes.A2), Callee: java.lang.

```

## Appendix C. Validation of the translation rules

```
Number.longValue()
public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: Associated
declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
/RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79: JML invariant
is false on leaving method project.Entrytypes.A1.inv_A1(project.Entrytypes
.A2) (parameter _f)
public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: Associated
declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
/RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:72: JML invariant
is false on leaving method project.Entrytypes.A1.valid()
public Boolean valid() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:12: Associated
declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
/RecWithRecFieldAtomicViolation/project/Entrytypes/A1.java:72:
//@ public instance invariant project.Entry.invChecksOn ==> inv_A1(f);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: JML invariant
is false
//@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:72: JML invariant
is false on leaving method project.Entrytypes.A2.valid()
public Boolean valid() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:12: Associated
declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
/RecWithRecFieldAtomicViolation/project/Entrytypes/A2.java:72:
//@ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
    ^
"After illegal use"
```

### C.50 CharUnionEven.vdmsl

```
1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
```

```

6
7 types
8
9 Even = nat
10 inv n == n mod 2 = 0;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO`println("Before_legal_use");
18   let - : char | Even = charA() in skip;
19   IO`println("After_legal_use");
20   IO`println("Before_illegal_use");
21   let - : char | Even = charNil() in skip;
22   IO`println("After_illegal_use");
23   return 0;
24 );
25
26 functions
27
28 charA : () -> char
29 charA () == 'a';
30
31 charNil : () -> [char]
32 charNil () == nil;
33
34 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       final Object ignorePattern_1 = charA();
20       //@ assert ((Utils.is_nat(ignorePattern_1) && inv_Entry_Even(
21         ignorePattern_1)) || Utils.is_char(ignorePattern_1));
22
23       /* skip */
24     }
25
26     IO.println("After_legal_use");
27     IO.println("Before_illegal_use");
28     {
29       final Object ignorePattern_2 = charNil();

```

## Appendix C. Validation of the translation rules

```
29      //@ assert ((Utils.is_nat(ignorePattern_2) && inv_Entry_Even(
30          ignorePattern_2)) || Utils.is_char(ignorePattern_2));
31      /* skip */
32  }
33
34  IO.println("After_illegal_use");
35  return 0L;
36  }
37  /*@ pure @*/
38
39  public static Character charA() {
40
41      Character ret_1 = 'a';
42      //@ assert Utils.is_char(ret_1);
43
44      return ret_1;
45  }
46  /*@ pure @*/
47
48  public static Character charNil() {
49
50      Character ret_2 = null;
51      //@ assert ((ret_2 == null) || Utils.is_char(ret_2));
52
53      return ret_2;
54  }
55
56  public String toString() {
57
58      return "Entry{}";
59  }
60
61  /*@ pure @*/
62  /*@ helper @*/
63
64  public static Boolean inv_Entry_Even(final Object check_n) {
65
66      Number n = ((Number) check_n);
67
68      return Utils.equals(Utils.mod(n.longValue(), 2L), 0L);
69  }
70  }
```

```
"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
      //@ assert ((Utils.is_nat(ignorePattern_2) && inv_Entry_Even(
          ignorePattern_2)) || Utils.is_char(ignorePattern_2));
          ^
"After illegal use"
```

### C.51 RecWithRecFieldAtomicNoViolation.vdmsl

```
1 || module Entry
```



```

2
3 imports from IO all
4 exports all
5
6 definitions
7
8 types
9 A1 :: f : A2
10 inv a1 == a1.f.x > 0;
11
12 A2 :: x : int
13 inv a2 == a2.x > 0;
14
15 B1 :: f : B2
16 inv b1 == b1.f.x > 0;
17
18 B2 :: x : int
19 inv b2 == b2.x > 0;
20
21
22 operations
23
24 Run : () ==> ?
25 Run () ==
26 (dcl r : A1 | B1 := mk_A1(mk_A2(1));
27   atomic
28   (
29     r.f.x := 5;
30   );
31   IO.println("Done!_Expected_no_violations");
32   return 0;
33 )
34
35 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class B2 implements Record {
11   public Number x;
12   // @ public instance invariant project.Entry.invChecksOn ==> inv_B2(x);
13
14   public B2(final Number _x) {
15
16     // @ assert Utils.is_int(_x);
17
18     x = _x;
19     // @ assert Utils.is_int(x);
20
21   }
22   /* @ pure @ */
23
24   public boolean equals(final Object obj) {
25

```

## Appendix C. Validation of the translation rules

```

26     if (!(obj instanceof project.Entrytypes.B2)) {
27         return false;
28     }
29
30     project.Entrytypes.B2 other = ((project.Entrytypes.B2) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.B2 copy() {
43
44     return new project.Entrytypes.B2(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`B2" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_4 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_4));
58
59     return ret_4;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_B2(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }

```

```

1 package project.Entrytypes;

```

## Appendix C. Validation of the translation rules

```

2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class A1 implements Record {
11     public project.Entrytypes.A2 f;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_A1(f);
13
14     public A1(final project.Entrytypes.A2 _f) {
15
16         // @ assert Utils.is_(_f,project.Entrytypes.A2.class);
17
18         f = _f != null ? Utils.copy(_f) : null;
19         // @ assert Utils.is_(f,project.Entrytypes.A2.class);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.A1)) {
27             return false;
28         }
29
30         project.Entrytypes.A1 other = ((project.Entrytypes.A1) obj);
31
32         return Utils.equals(f, other.f);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(f);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.A1 copy() {
43
44         return new project.Entrytypes.A1(f);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry`A1" + Utils.formatFields(f);
51     }
52     /* @ pure @ */
53
54     public project.Entrytypes.A2 get_f() {
55
56         project.Entrytypes.A2 ret_1 = f;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_(ret_1,project.
58             Entrytypes.A2.class));
59
60         return ret_1;
61     }

```

## Appendix C. Validation of the translation rules

```

61
62 public void set_f(final project.Entrytypes.A2 _f) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.
        Entrytypes.A2.class));
65
66     f = _f;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.Entrytypes
        .A2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_A1(final project.Entrytypes.A2 _f) {
80
81     return _f.x.longValue() > 0L;
82 }
83 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; /*@
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Object r = new project.Entrytypes.A1(new project.Entrytypes.A2(1L));
18         //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
            project.Entrytypes.B1.class));
19
20         Number atomicTmp_1 = 5L;
21         //@ assert Utils.is_int(atomicTmp_1);
22
23         {
24             /* Start of atomic statement */
25             //@ set invChecksOn = false;
26
27             Object apply_1 = null;
28             if (r instanceof project.Entrytypes.A1) {
29                 apply_1 = ((project.Entrytypes.A1) r).get_f();
30             } else if (r instanceof project.Entrytypes.B1) {
31                 apply_1 = ((project.Entrytypes.B1) r).get_f();
32             } else {
33                 throw new RuntimeException("Missing_member:_f");

```

## Appendix C. Validation of the translation rules

```

34     }
35
36     Object stateDes_1 = apply_1;
37     if (stateDes_1 instanceof project.Entrytypes.A2) {
38         //@ assert stateDes_1 != null;
39
40         ((project.Entrytypes.A2) stateDes_1).set_x(atomicTmp_1);
41
42     } else if (stateDes_1 instanceof project.Entrytypes.B2) {
43         //@ assert stateDes_1 != null;
44
45         ((project.Entrytypes.B2) stateDes_1).set_x(atomicTmp_1);
46
47     } else {
48         throw new RuntimeException("Missing_member:_x");
49     }
50
51     //@ set invChecksOn = true;
52
53     //@ assert stateDes_1 instanceof project.Entrytypes.A2 ==> ((project.
54         Entrytypes.A2) stateDes_1).valid();
55
56     //@ assert (Utils.is_(r,project.Entrytypes.A1.class) || Utils.is_(r,
57         project.Entrytypes.B1.class));
58
59     //@ assert r instanceof project.Entrytypes.B1 ==> ((project.Entrytypes
60         .B1) r).valid();
61
62     //@ assert r instanceof project.Entrytypes.A1 ==> ((project.Entrytypes
63         .A1) r).valid();
64
65     //@ assert stateDes_1 instanceof project.Entrytypes.B2 ==> ((project.
66         Entrytypes.B2) stateDes_1).valid();
67
68     } /* End of atomic statement */
69
70     IO.println("Done!_Expected_no_violations");
71     return 0L;
72 }
73
74 public String toString() {
75
76     return "Entry{}";
77 }
78 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class B1 implements Record {
11     public project.Entrytypes.B2 f;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_B1(f);
13
14     public B1(final project.Entrytypes.B2 _f) {

```

## Appendix C. Validation of the translation rules

```

15
16     //@ assert Utils.is_(_f,project.Entrytypes.B2.class);
17
18     f = _f != null ? Utils.copy(_f) : null;
19     //@ assert Utils.is_(f,project.Entrytypes.B2.class);
20
21 }
22 /*@ pure @*/
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.B1)) {
27         return false;
28     }
29
30     project.Entrytypes.B1 other = ((project.Entrytypes.B1) obj);
31
32     return Utils.equals(f, other.f);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(f);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.B1 copy() {
43
44     return new project.Entrytypes.B1(f);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`B1" + Utils.formatFields(f);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.B2 get_f() {
55
56     project.Entrytypes.B2 ret_3 = f;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
58         Entrytypes.B2.class));
59
60     return ret_3;
61 }
62
63 public void set_f(final project.Entrytypes.B2 _f) {
64
65     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_f,project.
66         Entrytypes.B2.class));
67
68     f = _f;
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_(f,project.Entrytypes
70         .B2.class));
71
72 }
73 /*@ pure @*/

```

## Appendix C. Validation of the translation rules

```
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_B1(final project.Entrytypes.B2 _f) {
80
81     return _f.x.longValue() > 0L;
82 }
83 }
```

```
1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class A2 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_A2(x);
13
14     public A2(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.A2)) {
27             return false;
28         }
29
30         project.Entrytypes.A2 other = ((project.Entrytypes.A2) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.A2 copy() {
43
44         return new project.Entrytypes.A2(x);
45     }
46     /*@ pure @*/
47 }
```

```

48 public String toString() {
49
50     return "mk_Entry'A2" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_2 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
58
59     return ret_2;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_A2(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }

```

```
"Done! Expected no violations"
```

## C.52 RecInRecInAtomic.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 types
10
11 R1 :: r2 : R2
12 inv r1 == r1.r2.r3.x <> 1;
13 R2 :: r3 : R3
14 inv r2 == r2.r3.x <> 2;
15 R3 :: x : int

```



```

16 inv r3 == r3.x <> 3;
17
18 operations
19
20 Run : () ==> ?
21 Run () ==
22 (
23   IO`println("Before_useOk");
24   let - = useOk() in skip;
25   IO`println("After_useOk");
26   IO`println("Before_useNotOk");
27   let - = useNotOk() in skip;
28   IO`println("After_useNotOk");
29   return 0;
30 );
31
32 useOk : () ==> nat
33 useOk () ==
34 (
35   dcl r1 : R1 := mk_R1(mk_R2(mk_R3(5)));
36
37   atomic
38   (
39     r1.r2.r3.x := 1;
40     r1.r2.r3.x := 5;
41   );
42
43   return 0;
44 );
45
46 useNotOk : () ==> nat
47 useNotOk () ==
48 (
49   dcl r1 : R1 := mk_R1(mk_R2(mk_R3(5)));
50
51   atomic
52   (
53     r1.r2.r3.x := 1;
54   );
55
56   return 0;
57 );
58
59 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R1 implements Record {
11   public project.Entrytypes.R2 r2;
12   // @ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14   public R1(final project.Entrytypes.R2 _r2) {
15

```

## Appendix C. Validation of the translation rules

```
16      //@ assert Utils.is_(_r2,project.Entrytypes.R2.class);
17
18      r2 = _r2 != null ? Utils.copy(_r2) : null;
19      //@ assert Utils.is_(r2,project.Entrytypes.R2.class);
20
21  }
22  /*@ pure @*/
23
24  public boolean equals(final Object obj) {
25
26      if (!(obj instanceof project.Entrytypes.R1)) {
27          return false;
28      }
29
30      project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32      return Utils.equals(r2, other.r2);
33  }
34  /*@ pure @*/
35
36  public int hashCode() {
37
38      return Utils.hashCode(r2);
39  }
40  /*@ pure @*/
41
42  public project.Entrytypes.R1 copy() {
43
44      return new project.Entrytypes.R1(r2);
45  }
46  /*@ pure @*/
47
48  public String toString() {
49
50      return "mk_Entry`R1" + Utils.formatFields(r2);
51  }
52  /*@ pure @*/
53
54  public project.Entrytypes.R2 get_r2() {
55
56      project.Entrytypes.R2 ret_3 = r2;
57      //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
58          Entrytypes.R2.class));
59
60      return ret_3;
61  }
62
63  public void set_r2(final project.Entrytypes.R2 _r2) {
64
65      //@ assert project.Entry.invChecksOn ==> (Utils.is_(_r2,project.
66          Entrytypes.R2.class));
67
68      r2 = _r2;
69      //@ assert project.Entry.invChecksOn ==> (Utils.is_(r2,project.
70          Entrytypes.R2.class));
71
72  }
73  /*@ pure @*/
74
75  public Boolean valid() {
```

## Appendix C. Validation of the translation rules

```

73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
80
81     return !(Utils.equals(_r2.r3.x, 1L));
82 }
83 }

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R2 implements Record {
11     public project.Entrytypes.R3 r3;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R2(r3);
13
14     public R2(final project.Entrytypes.R3 _r3) {
15
16         // @ assert Utils.is_(_r3,project.Entrytypes.R3.class);
17
18         r3 = _r3 != null ? Utils.copy(_r3) : null;
19         // @ assert Utils.is_(r3,project.Entrytypes.R3.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R2)) {
27             return false;
28         }
29
30         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
31
32         return Utils.equals(r3, other.r3);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(r3);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.R2 copy() {
43
44         return new project.Entrytypes.R2(r3);
45     }
46     /*@ pure @*/
47
48     public String toString() {

```

## Appendix C. Validation of the translation rules

```

49
50     return "mk_Entry`R2" + Utils.formatFields(r3);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.R3 get_r3() {
55
56     project.Entrytypes.R3 ret_4 = r3;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_4,project.
58         Entrytypes.R3.class));
59
60     return ret_4;
61 }
62
63 public void set_r3(final project.Entrytypes.R3 _r3) {
64
65     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r3,project.
66         Entrytypes.R3.class));
67
68     r3 = _r3;
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r3,project.
70         Entrytypes.R3.class));
71
72 }
73 /*@ pure @*/
74
75 public Boolean valid() {
76
77     return true;
78 }
79 /*@ pure @*/
80 /*@ helper @*/
81
82 public static Boolean inv_R2(final project.Entrytypes.R3 _r3) {
83
84     return !(Utils.equals(_r3.x, 2L));
85 }
86 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_useOk");
18         {
19             final Number ignorePattern_1 = useOk();
20             //@ assert Utils.is_nat(ignorePattern_1);
21

```

## Appendix C. Validation of the translation rules

```

22      /* skip */
23  }
24
25  IO.println("After_useOk");
26  IO.println("Before_useNotOk");
27  {
28      final Number ignorePattern_2 = useNotOk();
29      //@ assert Utils.is_nat(ignorePattern_2);
30
31      /* skip */
32  }
33
34  IO.println("After_useNotOk");
35  return 0L;
36  }
37
38  public static Number useOk() {
39
40      project.Entrytypes.R1 r1 =
41          new project.Entrytypes.R1(new project.Entrytypes.R2(new project.
42              Entrytypes.R3(5L)));
43      //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
44
45      Number atomicTmp_1 = 1L;
46      //@ assert Utils.is_int(atomicTmp_1);
47
48      Number atomicTmp_2 = 5L;
49      //@ assert Utils.is_int(atomicTmp_2);
50
51      {
52          /* Start of atomic statement */
53          //@ set invChecksOn = false;
54
55          project.Entrytypes.R2 stateDes_1 = r1.get_r2();
56
57          project.Entrytypes.R3 stateDes_2 = stateDes_1.get_r3();
58
59          //@ assert stateDes_2 != null;
60
61          stateDes_2.set_x(atomicTmp_1);
62
63          project.Entrytypes.R2 stateDes_3 = r1.get_r2();
64
65          project.Entrytypes.R3 stateDes_4 = stateDes_3.get_r3();
66
67          //@ assert stateDes_4 != null;
68
69          stateDes_4.set_x(atomicTmp_2);
70
71          //@ set invChecksOn = true;
72
73          //@ assert stateDes_2.valid();
74
75          //@ assert Utils.is_(stateDes_1,project.Entrytypes.R2.class);
76
77          //@ assert stateDes_1.valid();
78
79          //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
80
81          //@ assert r1.valid();

```

## Appendix C. Validation of the translation rules

```
81
82     //@ assert stateDes_4.valid();
83
84     //@ assert Utils.is_(stateDes_3,project.Entrytypes.R2.class);
85
86     //@ assert stateDes_3.valid();
87
88     } /* End of atomic statement */
89
90     Number ret_1 = 0L;
91     //@ assert Utils.is_nat(ret_1);
92
93     return ret_1;
94 }
95
96 public static Number useNotOk() {
97
98     project.Entrytypes.R1 r1 =
99         new project.Entrytypes.R1(new project.Entrytypes.R2(new project.
100             Entrytypes.R3(5L)));
101     //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
102
103     Number atomicTmp_3 = 1L;
104     //@ assert Utils.is_int(atomicTmp_3);
105
106     {
107         /* Start of atomic statement */
108         //@ set invChecksOn = false;
109
110         project.Entrytypes.R2 stateDes_5 = r1.get_r2();
111
112         project.Entrytypes.R3 stateDes_6 = stateDes_5.get_r3();
113
114         //@ assert stateDes_6 != null;
115
116         stateDes_6.set_x(atomicTmp_3);
117
118         //@ set invChecksOn = true;
119
120         //@ assert stateDes_6.valid();
121
122         //@ assert Utils.is_(stateDes_5,project.Entrytypes.R2.class);
123
124         //@ assert stateDes_5.valid();
125
126         //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
127
128         //@ assert r1.valid();
129     } /* End of atomic statement */
130
131     Number ret_2 = 0L;
132     //@ assert Utils.is_nat(ret_2);
133
134     return ret_2;
135 }
136
137 public String toString() {
138
139     return "Entry{}";
```

## Appendix C. Validation of the translation rules

```

140     }
141 }

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R3 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R3(x);
13
14     public R3(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R3)) {
27             return false;
28         }
29
30         project.Entrytypes.R3 other = ((project.Entrytypes.R3) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.R3 copy() {
43
44         return new project.Entrytypes.R3(x);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry`R3" + Utils.formatFields(x);
51     }
52     /* @ pure @ */
53
54     public Number get_x() {
55
56         Number ret_5 = x;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_5));

```

```

58
59     return ret_5;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R3(final Number _x) {
80
81     return !(Utils.equals(_x, 3L));
82 }
83 }

```

```

"Before useOk"
"After useOk"
"Before useNotOk"
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInAtomic/project/Entrytypes/R1.java:72: JML invariant is false on
  leaving method project.Entrytypes.R1.valid()
  public Boolean valid() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInAtomic/project/Entrytypes/R1.java:12: Associated declaration: /
  home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInAtomic/project/Entrytypes/R1.java:72:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
    ^
"After useNotOk"

```

## C.53 NamedTypeInvUnionTypeRec.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 types
10
11 R1 :: r2 : R2

```



## Appendix C. Validation of the translation rules

```

12 inv r1 == r1.r2.t3.r4.x <> 1;
13
14 R2 :: t3 : T3
15 inv r2 == r2.t3.r4.x <> 2;
16
17 T3 = R3 | X
18 inv t3 == (is_(t3,R3) ==> t3.r4.x <> 10) and (is_(t3, X) ==> t3.b);
19
20 R3 :: r4 : R4
21 inv r3 == r3.r4.x <> 3;
22
23 R4 :: x : int
24 inv r4 == r4.x <> 4;
25
26 X :: b : bool;
27
28 operations
29
30 Run : () ==> ?
31 Run () ==
32 (
33   IO`println("Before_useOk");
34   let - = useOk() in skip;
35   IO`println("After_useOk");
36   IO`println("Before_useNotOk");
37   let - = useNotOk() in skip;
38   IO`println("After_useNotOk");
39   return 0;
40 );
41
42 useOk : () ==> nat
43 useOk () ==
44 (
45   dcl r1 : R1 := mk_R1 (mk_R2 (mk_R3 (mk_R4 (5) ) ) );
46
47   atomic
48   (
49     r1.r2.t3.r4.x := 10;
50     r1.r2.t3.r4.x := 3;
51     r1.r2.t3.r4.x := 5;
52   );
53
54   return 0;
55 );
56
57 useNotOk : () ==> nat
58 useNotOk () ==
59 (
60   dcl r1 : R1 := mk_R1 (mk_R2 (mk_R3 (mk_R4 (5) ) ) );
61
62   atomic
63   (
64     r1.r2.t3.r4.x := 3;
65   );
66
67   return 0;
68 );
69
70 end Entry

```

## Appendix C. Validation of the translation rules

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R1 implements Record {
11     public project.Entrytypes.R2 r2;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14     public R1(final project.Entrytypes.R2 _r2) {
15
16         // @ assert Utils.is_(_r2, project.Entrytypes.R2.class);
17
18         r2 = _r2 != null ? Utils.copy(_r2) : null;
19         // @ assert Utils.is_(r2, project.Entrytypes.R2.class);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R1)) {
27             return false;
28         }
29
30         project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32         return Utils.equals(r2, other.r2);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(r2);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.R1 copy() {
43
44         return new project.Entrytypes.R1(r2);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry'R1" + Utils.formatFields(r2);
51     }
52     /* @ pure @ */
53
54     public project.Entrytypes.R2 get_r2() {
55
56         project.Entrytypes.R2 ret_3 = r2;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3, project.
58             Entrytypes.R2.class));

```

## Appendix C. Validation of the translation rules

```

59     return ret_3;
60 }
61
62 public void set_r2(final project.Entrytypes.R2 _r2) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_r2,project.
        Entrytypes.R2.class));
65
66     r2 = _r2;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r2,project.
        Entrytypes.R2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
80
81     Object obj_2 = Utils.copy(_r2.t3);
82     project.Entrytypes.R4 apply_6 = null;
83     if (obj_2 instanceof project.Entrytypes.R3) {
84         apply_6 = Utils.copy(((project.Entrytypes.R3) obj_2).r4);
85     } else {
86         throw new RuntimeException("Missing_member:_r4");
87     }
88
89     return !(Utils.equals(apply_6.x, 1L));
90 }
91
92 /*@ pure @*/
93 /*@ helper @*/
94
95 public static Boolean inv_Entry_T3(final Object check_t3) {
96
97     Object t3 = ((Object) check_t3);
98
99     Boolean andResult_1 = false;
100
101     Boolean orResult_1 = false;
102
103     if (!(Utils.is_(t3, project.Entrytypes.R3.class))) {
104         orResult_1 = true;
105     } else {
106         project.Entrytypes.R4 apply_9 = null;
107         if (t3 instanceof project.Entrytypes.R3) {
108             apply_9 = ((project.Entrytypes.R3) t3).get_r4();
109         } else {
110             throw new RuntimeException("Missing_member:_r4");
111         }
112
113         orResult_1 = !(Utils.equals(apply_9.get_x(), 10L));
114     }
115
116     if (orResult_1) {

```

## Appendix C. Validation of the translation rules

```

117     Boolean orResult_2 = false;
118
119     if (!(Utils.is_(t3, project.Entrytypes.X.class))) {
120         orResult_2 = true;
121     } else {
122         Boolean apply_10 = null;
123         if (t3 instanceof project.Entrytypes.X) {
124             apply_10 = ((project.Entrytypes.X) t3).get_b();
125         } else {
126             throw new RuntimeException("Missing_member:_b");
127         }
128
129         orResult_2 = apply_10;
130     }
131
132     if (orResult_2) {
133         andResult_1 = true;
134     }
135 }
136
137 return andResult_1;
138 }
139 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class X implements Record {
11     public Boolean b;
12
13     public X(final Boolean _b) {
14
15         //@ assert Utils.is_bool(_b);
16
17         b = _b;
18         //@ assert Utils.is_bool(b);
19     }
20     /*@ pure @*/
21
22     public boolean equals(final Object obj) {
23
24         if (!(obj instanceof project.Entrytypes.X)) {
25             return false;
26         }
27
28         project.Entrytypes.X other = ((project.Entrytypes.X) obj);
29
30         return Utils.equals(b, other.b);
31     }
32     /*@ pure @*/
33
34     public int hashCode() {
35
36

```

## Appendix C. Validation of the translation rules

```

37     return Utils.hashCode(b);
38 }
39 /*@ pure @*/
40
41 public project.Entrytypes.X copy() {
42
43     return new project.Entrytypes.X(b);
44 }
45 /*@ pure @*/
46
47 public String toString() {
48
49     return "mk_Entry`X" + Utils.formatFields(b);
50 }
51 /*@ pure @*/
52
53 public Boolean get_b() {
54
55     Boolean ret_7 = b;
56     //@ assert project.Entry.invChecksOn ==> (Utils.is_bool(ret_7));
57
58     return ret_7;
59 }
60
61 public void set_b(final Boolean _b) {
62
63     //@ assert project.Entry.invChecksOn ==> (Utils.is_bool(_b));
64
65     b = _b;
66     //@ assert project.Entry.invChecksOn ==> (Utils.is_bool(b));
67
68 }
69 /*@ pure @*/
70
71 public Boolean valid() {
72
73     return true;
74 }
75
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_Entry_T3(final Object check_t3) {
80
81     Object t3 = ((Object) check_t3);
82
83     Boolean andResult_1 = false;
84
85     Boolean orResult_1 = false;
86
87     if (!(Utils.is_(t3, project.Entrytypes.R3.class))) {
88         orResult_1 = true;
89     } else {
90         project.Entrytypes.R4 apply_9 = null;
91         if (t3 instanceof project.Entrytypes.R3) {
92             apply_9 = ((project.Entrytypes.R3) t3).get_r4();
93         } else {
94             throw new RuntimeException("Missing_member:_r4");
95         }
96

```

## Appendix C. Validation of the translation rules

```

97         orResult_1 = !(Utils.equals(apply_9.get_x(), 10L));
98     }
99
100     if (orResult_1) {
101         Boolean orResult_2 = false;
102
103         if (!(Utils.is_(t3, project.Entrytypes.X.class))) {
104             orResult_2 = true;
105         } else {
106             Boolean apply_10 = null;
107             if (t3 instanceof project.Entrytypes.X) {
108                 apply_10 = ((project.Entrytypes.X) t3).get_b();
109             } else {
110                 throw new RuntimeException("Missing_member:_b");
111             }
112
113             orResult_2 = apply_10;
114         }
115
116         if (orResult_2) {
117             andResult_1 = true;
118         }
119     }
120
121     return andResult_1;
122 }
123 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R2 implements Record {
11     public Object t3;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(t3);
13
14     public R2(final Object _t3) {
15
16         //@ assert ((Utils.is_(t3,project.Entrytypes.R3.class) || Utils.is_(t3
17             ,project.Entrytypes.X.class)) && inv_Entry_T3(t3));
18
19         t3 = _t3 != null ? Utils.copy(t3) : null;
20         //@ assert ((Utils.is_(t3,project.Entrytypes.R3.class) || Utils.is_(t3,
21             project.Entrytypes.X.class)) && inv_Entry_T3(t3));
22     }
23     /*@ pure @*/
24
25     public boolean equals(final Object obj) {
26
27         if (!(obj instanceof project.Entrytypes.R2)) {
28             return false;
29         }
30
31         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);

```

```

31
32     return Utils.equals(t3, other.t3);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(t3);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R2 copy() {
43
44     return new project.Entrytypes.R2(t3);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R2" + Utils.formatFields(t3);
51 }
52 /*@ pure @*/
53
54 public Object get_t3() {
55
56     Object ret_4 = t3;
57     //@ assert project.Entry.invChecksOn ==> (((Utils.is_(ret_4,project.
        Entrytypes.R3.class) || Utils.is_(ret_4,project.Entrytypes.X.class))
        && inv_Entry_T3(ret_4)));
58
59     return ret_4;
60 }
61
62 public void set_t3(final Object _t3) {
63
64     //@ assert project.Entry.invChecksOn ==> (((Utils.is_(_t3,project.
        Entrytypes.R3.class) || Utils.is_(_t3,project.Entrytypes.X.class))
        && inv_Entry_T3(_t3)));
65
66     t3 = _t3;
67     //@ assert project.Entry.invChecksOn ==> (((Utils.is_(t3,project.
        Entrytypes.R3.class) || Utils.is_(t3,project.Entrytypes.X.class)) &&
        inv_Entry_T3(t3)));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R2(final Object _t3) {
80
81     Object obj_4 = _t3;
82     project.Entrytypes.R4 apply_8 = null;
83     if (obj_4 instanceof project.Entrytypes.R3) {
84         apply_8 = Utils.copy(((project.Entrytypes.R3) obj_4).r4);

```

## Appendix C. Validation of the translation rules

```

85     } else {
86         throw new RuntimeException("Missing_member:_r4");
87     }
88
89     return !(Utils.equals(apply_8.x, 2L));
90 }
91
92 /*@ pure @*/
93 /*@ helper @*/
94
95 public static Boolean inv_Entry_T3(final Object check_t3) {
96
97     Object t3 = ((Object) check_t3);
98
99     Boolean andResult_1 = false;
100
101     Boolean orResult_1 = false;
102
103     if (!(Utils.is_(t3, project.Entrytypes.R3.class))) {
104         orResult_1 = true;
105     } else {
106         project.Entrytypes.R4 apply_9 = null;
107         if (t3 instanceof project.Entrytypes.R3) {
108             apply_9 = ((project.Entrytypes.R3) t3).get_r4();
109         } else {
110             throw new RuntimeException("Missing_member:_r4");
111         }
112
113         orResult_1 = !(Utils.equals(apply_9.get_x(), 10L));
114     }
115
116     if (orResult_1) {
117         Boolean orResult_2 = false;
118
119         if (!(Utils.is_(t3, project.Entrytypes.X.class))) {
120             orResult_2 = true;
121         } else {
122             Boolean apply_10 = null;
123             if (t3 instanceof project.Entrytypes.X) {
124                 apply_10 = ((project.Entrytypes.X) t3).get_b();
125             } else {
126                 throw new RuntimeException("Missing_member:_b");
127             }
128
129             orResult_2 = apply_10;
130         }
131
132         if (orResult_2) {
133             andResult_1 = true;
134         }
135     }
136
137     return andResult_1;
138 }
139 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;

```



## Appendix C. Validation of the translation rules

```
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class R4 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R4(x);
13
14     public R4(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R4)) {
27             return false;
28         }
29
30         project.Entrytypes.R4 other = ((project.Entrytypes.R4) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.R4 copy() {
43
44         return new project.Entrytypes.R4(x);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry`R4" + Utils.formatFields(x);
51     }
52     /* @ pure @ */
53
54     public Number get_x() {
55
56         Number ret_6 = x;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_6));
58
59         return ret_6;
60     }
61
62     public void set_x(final Number _x) {
63
64         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
```

## Appendix C. Validation of the translation rules

```

65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R4(final Number _x) {
80
81     return !(Utils.equals(_x, 4L));
82 }
83
84 /*@ pure @*/
85 /*@ helper @*/
86
87 public static Boolean inv_Entry_T3(final Object check_t3) {
88
89     Object t3 = ((Object) check_t3);
90
91     Boolean andResult_1 = false;
92
93     Boolean orResult_1 = false;
94
95     if (!(Utils.is_(t3, project.Entrytypes.R3.class))) {
96         orResult_1 = true;
97     } else {
98         project.Entrytypes.R4 apply_9 = null;
99         if (t3 instanceof project.Entrytypes.R3) {
100             apply_9 = ((project.Entrytypes.R3) t3).get_r4();
101         } else {
102             throw new RuntimeException("Missing_member:_r4");
103         }
104
105         orResult_1 = !(Utils.equals(apply_9.get_x(), 10L));
106     }
107
108     if (orResult_1) {
109         Boolean orResult_2 = false;
110
111         if (!(Utils.is_(t3, project.Entrytypes.X.class))) {
112             orResult_2 = true;
113         } else {
114             Boolean apply_10 = null;
115             if (t3 instanceof project.Entrytypes.X) {
116                 apply_10 = ((project.Entrytypes.X) t3).get_b();
117             } else {
118                 throw new RuntimeException("Missing_member:_b");
119             }
120
121             orResult_2 = apply_10;
122         }
123
124         if (orResult_2) {

```

## Appendix C. Validation of the translation rules

```

125         andResult_1 = true;
126     }
127 }
128
129     return andResult_1;
130 }
131 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_useOk");
18         {
19             final Number ignorePattern_1 = useOk();
20             // @ assert Utils.is_nat(ignorePattern_1);
21
22             /* skip */
23         }
24
25         IO.println("After_useOk");
26         IO.println("Before_useNotOk");
27         {
28             final Number ignorePattern_2 = useNotOk();
29             // @ assert Utils.is_nat(ignorePattern_2);
30
31             /* skip */
32         }
33
34         IO.println("After_useNotOk");
35         return 0L;
36     }
37
38     public static Number useOk() {
39
40         project.Entrytypes.R1 r1 =
41             new project.Entrytypes.R1(
42                 new project.Entrytypes.R2(new project.Entrytypes.R3(new project.
43                     Entrytypes.R4(5L))));
44             // @ assert Utils.is_(r1, project.Entrytypes.R1.class);
45
46         Number atomicTmp_1 = 10L;
47         // @ assert Utils.is_int(atomicTmp_1);
48
49         Number atomicTmp_2 = 3L;
50         // @ assert Utils.is_int(atomicTmp_2);
51
52         Number atomicTmp_3 = 5L;

```

## Appendix C. Validation of the translation rules

```

52  // @ assert Utils.is_int(atomicTmp_3);
53
54  {
55      /* Start of atomic statement */
56      // @ set invChecksOn = false;
57
58      project.Entrytypes.R2 stateDes_1 = r1.get_r2();
59
60      Object stateDes_2 = stateDes_1.get_t3();
61
62      project.Entrytypes.R4 apply_1 = null;
63      if (stateDes_2 instanceof project.Entrytypes.R3) {
64          apply_1 = ((project.Entrytypes.R3) stateDes_2).get_r4();
65      } else {
66          throw new RuntimeException("Missing_member:_r4");
67      }
68
69      project.Entrytypes.R4 stateDes_3 = apply_1;
70      // @ assert stateDes_3 != null;
71
72      stateDes_3.set_x(atomicTmp_1);
73
74      project.Entrytypes.R2 stateDes_4 = r1.get_r2();
75
76      Object stateDes_5 = stateDes_4.get_t3();
77
78      project.Entrytypes.R4 apply_2 = null;
79      if (stateDes_5 instanceof project.Entrytypes.R3) {
80          apply_2 = ((project.Entrytypes.R3) stateDes_5).get_r4();
81      } else {
82          throw new RuntimeException("Missing_member:_r4");
83      }
84
85      project.Entrytypes.R4 stateDes_6 = apply_2;
86      // @ assert stateDes_6 != null;
87
88      stateDes_6.set_x(atomicTmp_2);
89
90      project.Entrytypes.R2 stateDes_7 = r1.get_r2();
91
92      Object stateDes_8 = stateDes_7.get_t3();
93
94      project.Entrytypes.R4 apply_3 = null;
95      if (stateDes_8 instanceof project.Entrytypes.R3) {
96          apply_3 = ((project.Entrytypes.R3) stateDes_8).get_r4();
97      } else {
98          throw new RuntimeException("Missing_member:_r4");
99      }
100
101      project.Entrytypes.R4 stateDes_9 = apply_3;
102      // @ assert stateDes_9 != null;
103
104      stateDes_9.set_x(atomicTmp_3);
105
106      // @ set invChecksOn = true;
107
108      // @ assert stateDes_3.valid();
109
110      // @ assert ((Utils.is_(stateDes_2, project.Entrytypes.R3.class) ||
          Utils.is_(stateDes_2, project.Entrytypes.X.class)) && inv_Entry_T3(

```

## Appendix C. Validation of the translation rules

```

stateDes_2));
111
112 // @ assert stateDes_2 instanceof project.Entrytypes.X ==> ((project.
    Entrytypes.X) stateDes_2).valid();
113
114 // @ assert stateDes_2 instanceof project.Entrytypes.R3 ==> ((project.
    Entrytypes.R3) stateDes_2).valid();
115
116 // @ assert Utils.is_(stateDes_1,project.Entrytypes.R2.class);
117
118 // @ assert stateDes_1.valid();
119
120 // @ assert Utils.is_(r1,project.Entrytypes.R1.class);
121
122 // @ assert r1.valid();
123
124 // @ assert stateDes_6.valid();
125
126 // @ assert ((Utils.is_(stateDes_5,project.Entrytypes.R3.class) ||
    Utils.is_(stateDes_5,project.Entrytypes.X.class)) && inv_Entry_T3(
    stateDes_5));
127
128 // @ assert stateDes_5 instanceof project.Entrytypes.X ==> ((project.
    Entrytypes.X) stateDes_5).valid();
129
130 // @ assert stateDes_5 instanceof project.Entrytypes.R3 ==> ((project.
    Entrytypes.R3) stateDes_5).valid();
131
132 // @ assert Utils.is_(stateDes_4,project.Entrytypes.R2.class);
133
134 // @ assert stateDes_4.valid();
135
136 // @ assert stateDes_9.valid();
137
138 // @ assert ((Utils.is_(stateDes_8,project.Entrytypes.R3.class) ||
    Utils.is_(stateDes_8,project.Entrytypes.X.class)) && inv_Entry_T3(
    stateDes_8));
139
140 // @ assert stateDes_8 instanceof project.Entrytypes.X ==> ((project.
    Entrytypes.X) stateDes_8).valid();
141
142 // @ assert stateDes_8 instanceof project.Entrytypes.R3 ==> ((project.
    Entrytypes.R3) stateDes_8).valid();
143
144 // @ assert Utils.is_(stateDes_7,project.Entrytypes.R2.class);
145
146 // @ assert stateDes_7.valid();
147
148 } /* End of atomic statement */
149
150 Number ret_1 = 0L;
151 // @ assert Utils.is_nat(ret_1);
152
153 return ret_1;
154 }
155
156 public static Number useNotOk() {
157
158     project.Entrytypes.R1 r1 =
159         new project.Entrytypes.R1(

```

## Appendix C. Validation of the translation rules

```

160         new project.Entrytypes.R2(new project.Entrytypes.R3(new project.
161             Entrytypes.R4(5L)));
162     //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
163     Number atomicTmp_4 = 3L;
164     //@ assert Utils.is_int(atomicTmp_4);
165
166     {
167         /* Start of atomic statement */
168         //@ set invChecksOn = false;
169
170         project.Entrytypes.R2 stateDes_10 = r1.get_r2();
171
172         Object stateDes_11 = stateDes_10.get_t3();
173
174         project.Entrytypes.R4 apply_4 = null;
175         if (stateDes_11 instanceof project.Entrytypes.R3) {
176             apply_4 = ((project.Entrytypes.R3) stateDes_11).get_r4();
177         } else {
178             throw new RuntimeException("Missing_member:_r4");
179         }
180
181         project.Entrytypes.R4 stateDes_12 = apply_4;
182         //@ assert stateDes_12 != null;
183
184         stateDes_12.set_x(atomicTmp_4);
185
186         //@ set invChecksOn = true;
187
188         //@ assert stateDes_12.valid();
189
190         //@ assert ((Utils.is_(stateDes_11,project.Entrytypes.R3.class) ||
191             Utils.is_(stateDes_11,project.Entrytypes.X.class)) && inv_Entry_T3
192             (stateDes_11));
193
194         //@ assert stateDes_11 instanceof project.Entrytypes.X ==> ((project.
195             Entrytypes.X) stateDes_11).valid();
196
197         //@ assert stateDes_11 instanceof project.Entrytypes.R3 ==> ((project.
198             Entrytypes.R3) stateDes_11).valid();
199
200         //@ assert Utils.is_(stateDes_10,project.Entrytypes.R2.class);
201
202         //@ assert stateDes_10.valid();
203
204         //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
205
206         //@ assert r1.valid();
207
208     } /* End of atomic statement */
209
210     Number ret_2 = 0L;
211     //@ assert Utils.is_nat(ret_2);
212
213     return ret_2;
214 }
215
216 public String toString() {
217
218     return "Entry{}";
219 }

```

## Appendix C. Validation of the translation rules

```

215     }
216
217     /*@ pure @*/
218     /*@ helper @*/
219
220     public static Boolean inv_Entry_T3(final Object check_t3) {
221
222         Object t3 = ((Object) check_t3);
223
224         Boolean andResult_1 = false;
225
226         Boolean orResult_1 = false;
227
228         if (!(Utils.is_(t3, project.Entrytypes.R3.class))) {
229             orResult_1 = true;
230         } else {
231             project.Entrytypes.R4 apply_9 = null;
232             if (t3 instanceof project.Entrytypes.R3) {
233                 apply_9 = ((project.Entrytypes.R3) t3).get_r4();
234             } else {
235                 throw new RuntimeException("Missing_member:_r4");
236             }
237
238             orResult_1 = !(Utils.equals(apply_9.get_x(), 10L));
239         }
240
241         if (orResult_1) {
242             Boolean orResult_2 = false;
243
244             if (!(Utils.is_(t3, project.Entrytypes.X.class))) {
245                 orResult_2 = true;
246             } else {
247                 Boolean apply_10 = null;
248                 if (t3 instanceof project.Entrytypes.X) {
249                     apply_10 = ((project.Entrytypes.X) t3).get_b();
250                 } else {
251                     throw new RuntimeException("Missing_member:_b");
252                 }
253
254                 orResult_2 = apply_10;
255             }
256
257             if (orResult_2) {
258                 andResult_1 = true;
259             }
260         }
261
262         return andResult_1;
263     }
264 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9

```

## Appendix C. Validation of the translation rules

```

10 final public class R3 implements Record {
11     public project.Entrytypes.R4 r4;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
13
14     public R3(final project.Entrytypes.R4 _r4) {
15
16         //@ assert Utils.is_(r4,project.Entrytypes.R4.class);
17
18         r4 = _r4 != null ? Utils.copy(_r4) : null;
19         //@ assert Utils.is_(r4,project.Entrytypes.R4.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R3)) {
27             return false;
28         }
29
30         project.Entrytypes.R3 other = ((project.Entrytypes.R3) obj);
31
32         return Utils.equals(r4, other.r4);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(r4);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.R3 copy() {
43
44         return new project.Entrytypes.R3(r4);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`R3" + Utils.formatFields(r4);
51     }
52     /*@ pure @*/
53
54     public project.Entrytypes.R4 get_r4() {
55
56         project.Entrytypes.R4 ret_5 = r4;
57         //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_5,project.
58             Entrytypes.R4.class));
59
60         return ret_5;
61     }
62
63     public void set_r4(final project.Entrytypes.R4 _r4) {
64
65         //@ assert project.Entry.invChecksOn ==> (Utils.is_(r4,project.
66             Entrytypes.R4.class));
67
68         r4 = _r4;
69         //@ assert project.Entry.invChecksOn ==> (Utils.is_(r4,project.

```



## Appendix C. Validation of the translation rules

```

        Entrytypes.R4.class));
68
69     }
70     /*@ pure @*/
71
72     public Boolean valid() {
73
74         return true;
75     }
76     /*@ pure @*/
77     /*@ helper @*/
78
79     public static Boolean inv_R3(final project.Entrytypes.R4 _r4) {
80
81         return !(Utils.equals(_r4.x, 3L));
82     }
83
84     /*@ pure @*/
85     /*@ helper @*/
86
87     public static Boolean inv_Entry_T3(final Object check_t3) {
88
89         Object t3 = ((Object) check_t3);
90
91         Boolean andResult_1 = false;
92
93         Boolean orResult_1 = false;
94
95         if (!(Utils.is_(t3, project.Entrytypes.R3.class))) {
96             orResult_1 = true;
97         } else {
98             project.Entrytypes.R4 apply_9 = null;
99             if (t3 instanceof project.Entrytypes.R3) {
100                 apply_9 = ((project.Entrytypes.R3) t3).get_r4();
101             } else {
102                 throw new RuntimeException("Missing_member:_r4");
103             }
104
105             orResult_1 = !(Utils.equals(apply_9.get_x(), 10L));
106         }
107
108         if (orResult_1) {
109             Boolean orResult_2 = false;
110
111             if (!(Utils.is_(t3, project.Entrytypes.X.class))) {
112                 orResult_2 = true;
113             } else {
114                 Boolean apply_10 = null;
115                 if (t3 instanceof project.Entrytypes.X) {
116                     apply_10 = ((project.Entrytypes.X) t3).get_b();
117                 } else {
118                     throw new RuntimeException("Missing_member:_b");
119                 }
120
121                 orResult_2 = apply_10;
122             }
123
124             if (orResult_2) {
125                 andResult_1 = true;
126             }

```

## Appendix C. Validation of the translation rules

```

127     }
128
129     return andResult_1;
130 }
131 }

```

```

"Before useOk"
"After useOk"
"Before useNotOk"
Entry.java:233: JML invariant is false on entering method project.Entrytypes.
    R3.get_r4() from project.Entry.inv_Entry_T3(java.lang.Object)
        apply_9 = ((project.Entrytypes.R3) t3).get_r4();
                    ^
Entry.java:233:
    //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:54: JML invariant is
    false on leaving method project.Entrytypes.R3.get_r4()
    public project.Entrytypes.R4 get_r4() {
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
    declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
    /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:54:
    //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:72: JML invariant is
    false on leaving method project.Entrytypes.R3.valid()
    public Boolean valid() {
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
    declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
    /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:72:
    //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:44: JML caller
    invariant is false on leaving calling method (Caller: project.Entrytypes.R3
    .copy(), Callee: project.Entrytypes.R3.R3(project.Entrytypes.R4))
    return new project.Entrytypes.R3(r4);
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
    declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
    /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:44:
    //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:14: JML invariant is
    false on leaving method project.Entrytypes.R3.R3(project.Entrytypes.R4)
    public R3(final project.Entrytypes.R4 _r4) {
        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
    NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
    declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
    /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:14:
    //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);

```

## Appendix C. Validation of the translation rules

```

      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42: JML invariant is
    false on leaving method project.Entrytypes.R3.copy()
  public project.Entrytypes.R3 copy() {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42: JML invariant is
    false on leaving method project.Entrytypes.R3.copy() (for result type)
  public project.Entrytypes.R3 copy() {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:44: JML caller
  invariant is false on leaving calling method (Caller: project.Entrytypes.R3
  .copy(), Callee: project.Entrytypes.R3.R3(project.Entrytypes.R4))
  return new project.Entrytypes.R3(r4);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:44:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:14: JML invariant is
    false on leaving method project.Entrytypes.R3.R3(project.Entrytypes.R4)
  public R3(final project.Entrytypes.R4 _r4) {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:14:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42: JML invariant is
    false on leaving method project.Entrytypes.R3.copy()
  public project.Entrytypes.R3 copy() {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42: JML invariant is
    false on leaving method project.Entrytypes.R3.copy() (for result type)
```

```

public project.Entrytypes.R3 copy() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:12: Associated
  declaration: /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code
  /NamedTypeInvUnionTypeRec/project/Entrytypes/R3.java:42:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
"After useNotOk"

```

## C.54 RecWithMapOfRec.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 types
10
11 A :: m : map nat to B
12 inv a == forall i in set dom a.m & a.m(i).x = 2;
13 B :: x : nat;
14
15 operations
16
17 Run : () ==> ?
18 Run () ==
19 (
20   IO`println("Before_useOk");
21   let - = useOk() in skip;
22   IO`println("After_useOk");
23   IO`println("Before_useNotOk");
24   let - = useNotOk() in skip;
25   IO`println("After_useNotOk");
26   return 0;
27 );
28
29 useOk : () ==> nat
30 useOk () ==
31 (
32   dcl a : A := mk_A({|->});
33   a.m := a.m munion {1 |-> mk_B(2)};
34   return 0;
35 );
36
37 useNotOk : () ==> nat
38 useNotOk () ==
39 (
40   dcl a : A := mk_A({|->});
41   a.m := a.m munion {1 |-> mk_B(1)};
42   return 0;
43 );
44
45 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_useOk");
18         {
19             final Number ignorePattern_1 = useOk();
20             /* @ assert Utils.is_nat(ignorePattern_1);
21
22             /* skip */
23         }
24
25         IO.println("After_useOk");
26         IO.println("Before_useNotOk");
27         {
28             final Number ignorePattern_2 = useNotOk();
29             /* @ assert Utils.is_nat(ignorePattern_2);
30
31             /* skip */
32         }
33
34         IO.println("After_useNotOk");
35         return 0L;
36     }
37
38     public static Number useOk() {
39
40         project.Entrytypes.A a = new project.Entrytypes.A(MapUtil.map());
41         /* @ assert Utils.is_(a, project.Entrytypes.A.class);
42
43         /* @ assert a != null;
44
45         a.set_m(
46             MapUtil.munion(
47                 Utils.copy(a.get_m()), MapUtil.map(new Maplet(1L, new project.
48                     Entrytypes.B(2L)))));
49
50         Number ret_1 = 0L;
51         /* @ assert Utils.is_nat(ret_1);
52
53         return ret_1;
54     }
55
56     public static Number useNotOk() {
57
58         project.Entrytypes.A a = new project.Entrytypes.A(MapUtil.map());

```

## Appendix C. Validation of the translation rules

```

58      //@ assert Utils.is_(a,project.Entrytypes.A.class);
59
60      //@ assert a != null;
61
62      a.set_m(
63          MapUtil.munion(
64              Utils.copy(a.get_m()), MapUtil.map(new Maplet(1L, new project.
65                  Entrytypes.B(1L)))));
66
67      Number ret_2 = 0L;
68      //@ assert Utils.is_nat(ret_2);
69
70      return ret_2;
71  }
72
73  public String toString() {
74
75      return "Entry{}";
76  }
77  }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class A implements Record {
11     public VDMMap m;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_A(m);
13
14     public A(final VDMMap _m) {
15
16         //@ assert (V2J.isMap(_m) && (\forallall int i_1; 0 <= i_1 && i_1 < V2J.
17             size(_m); Utils.is_nat(V2J.getDom(_m,i_1)) && Utils.is_(V2J.getRng(
18                 _m,i_1),project.Entrytypes.B.class)));
19
20         m = _m != null ? Utils.copy(_m) : null;
21         //@ assert (V2J.isMap(m) && (\forallall int i_1; 0 <= i_1 && i_1 < V2J.size
22             (m); Utils.is_nat(V2J.getDom(m,i_1)) && Utils.is_(V2J.getRng(m,i_1),
23                 project.Entrytypes.B.class)));
24
25     }
26     /*@ pure @*/
27
28     public boolean equals(final Object obj) {
29
30         if (!(obj instanceof project.Entrytypes.A)) {
31             return false;
32         }
33
34         project.Entrytypes.A other = ((project.Entrytypes.A) obj);
35
36         return Utils.equals(m, other.m);
37     }
38     /*@ pure @*/
39 }

```

## Appendix C. Validation of the translation rules

```

36 public int hashCode() {
37
38     return Utils.hashCode(m);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.A copy() {
43
44     return new project.Entrytypes.A(m);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry'A" + Utils.formatFields(m);
51 }
52 /*@ pure @*/
53
54 public VDMMap get_m() {
55
56     VDMMap ret_3 = m;
57     //@ assert project.Entry.invChecksOn ==> ((V2J.isMap(ret_3) && (\forallall
        int i_1; 0 <= i_1 && i_1 < V2J.size(ret_3); Utils.is_nat(V2J.getDom(
        ret_3,i_1)) && Utils.is_(V2J.getRng(ret_3,i_1),project.Entrytypes.B.
        class)))));
58
59     return ret_3;
60 }
61
62 public void set_m(final VDMMap _m) {
63
64     //@ assert project.Entry.invChecksOn ==> ((V2J.isMap(_m) && (\forallall int
        i_1; 0 <= i_1 && i_1 < V2J.size(_m); Utils.is_nat(V2J.getDom(_m,i_1)
        )) && Utils.is_(V2J.getRng(_m,i_1),project.Entrytypes.B.class)))));
65
66     m = _m;
67     //@ assert project.Entry.invChecksOn ==> ((V2J.isMap(m) && (\forallall int
        i_1; 0 <= i_1 && i_1 < V2J.size(m); Utils.is_nat(V2J.getDom(m,i_1))
        && Utils.is_(V2J.getRng(m,i_1),project.Entrytypes.B.class)))));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_A(final VDMMap _m) {
80
81     Boolean forAllExpResult_2 = true;
82     VDMSet set_2 = MapUtil.dom(_m);
83     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext() &&
        forAllExpResult_2; ) {
84         Number i = ((Number) iterator_2.next());
85         forAllExpResult_2 = Utils.equals(((project.Entrytypes.B) Utils.get(_m,
            i)).x, 2L);
86     }

```

## Appendix C. Validation of the translation rules

```

87     return forAllExpResult_2;
88 }
89 }

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class B implements Record {
11     public Number x;
12
13     public B(final Number _x) {
14
15         // @ assert Utils.is_nat(_x);
16
17         x = _x;
18         // @ assert Utils.is_nat(x);
19     }
20     /* @ pure @ */
21
22     public boolean equals(final Object obj) {
23
24         if (!(obj instanceof project.Entrytypes.B)) {
25             return false;
26         }
27
28         project.Entrytypes.B other = ((project.Entrytypes.B) obj);
29
30         return Utils.equals(x, other.x);
31     }
32     /* @ pure @ */
33
34     public int hashCode() {
35
36         return Utils.hashCode(x);
37     }
38     /* @ pure @ */
39
40     public project.Entrytypes.B copy() {
41
42         return new project.Entrytypes.B(x);
43     }
44     /* @ pure @ */
45
46     public String toString() {
47
48         return "mk_Entry`B" + Utils.formatFields(x);
49     }
50     /* @ pure @ */
51
52     public Number get_x() {
53
54         Number ret_4 = x;
55         // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_4));
56

```



```

57
58     return ret_4;
59 }
60
61 public void set_x(final Number _x) {
62
63     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
64
65     x = _x;
66     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
67
68 }
69 /*@ pure @*/
70
71 public Boolean valid() {
72
73     return true;
74 }
75 }

```

```

"Before useOk"
"After useOk"
"Before useNotOk"
A.java:62: JML invariant is false on leaving method project.Entrytypes.A.set_m
  (org.overture.codegen.runtime.VDMMMap)
  public void set_m(final VDMMMap _m) {
    ^
A.java:12: Associated declaration
  //@ public instance invariant project.Entry.invChecksOn ==> inv_A(m);
    ^
"After useNotOk"

```

## C.55 RecInRecInvViolation.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 T1 :: t2 : T2
10 inv t1 == t1.t2.t3.t4.x > 1;
11
12 T2 :: t3 : T3
13 inv t2 == t2.t3.t4.x > 2 and t2.t3.t4.x <> 60;
14
15 T3 :: t4 : T4
16 inv t3 == t3.t4.x > 3;
17
18 T4 :: x : nat
19 inv t4 == t4.x > 4;
20
21 operations
22

```

## Appendix C. Validation of the translation rules

```

23 useOk : () ==> nat
24 useOk () ==
25 (
26   dcl t1 : T1 := mk_T1 (mk_T2 (mk_T3 (mk_T4 (5)))));
27   t1.t2.t3.t4.x := 6;
28   t1.t2.t3.t4.x := 7;
29   return 0;
30 );
31
32 useNotOk : () ==> nat
33 useNotOk () ==
34 (
35   dcl t1 : T1 := mk_T1 (mk_T2 (mk_T3 (mk_T4 (5)))));
36   t1.t2.t3.t4.x := 60;
37   t1.t2.t3.t4.x := 5;
38   return 0;
39 );
40
41 Run : () ==> ?
42 Run () ==
43 (
44   IO`println("Before_useOk");
45   let - = useOk() in skip;
46   IO`println("After_useOk");
47   IO`println("Before_useNotOk");
48   let - = useNotOk() in skip;
49   IO`println("After_useNotOk");
50   return 0;
51 );
52
53 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Number useOk() {
16
17     project.Entrytypes.T1 t1 =
18       new project.Entrytypes.T1(
19         new project.Entrytypes.T2(new project.Entrytypes.T3(new project.
20           Entrytypes.T4(5L))));
21     //@ assert Utils.is_(t1,project.Entrytypes.T1.class);
22
23     project.Entrytypes.T2 stateDes_1 = t1.get_t2();
24
25     project.Entrytypes.T3 stateDes_2 = stateDes_1.get_t3();
26
27     project.Entrytypes.T4 stateDes_3 = stateDes_2.get_t4();
28

```

## Appendix C. Validation of the translation rules

```
28      //@ assert stateDes_3 != null;
29
30      stateDes_3.set_x(6L);
31      //@ assert Utils.is_(stateDes_2,project.Entrytypes.T3.class);
32
33      //@ assert stateDes_2.valid();
34
35      //@ assert Utils.is_(stateDes_1,project.Entrytypes.T2.class);
36
37      //@ assert stateDes_1.valid();
38
39      //@ assert Utils.is_(t1,project.Entrytypes.T1.class);
40
41      //@ assert t1.valid();
42
43      project.Entrytypes.T2 stateDes_4 = t1.get_t2();
44
45      project.Entrytypes.T3 stateDes_5 = stateDes_4.get_t3();
46
47      project.Entrytypes.T4 stateDes_6 = stateDes_5.get_t4();
48
49      //@ assert stateDes_6 != null;
50
51      stateDes_6.set_x(7L);
52      //@ assert Utils.is_(stateDes_5,project.Entrytypes.T3.class);
53
54      //@ assert stateDes_5.valid();
55
56      //@ assert Utils.is_(stateDes_4,project.Entrytypes.T2.class);
57
58      //@ assert stateDes_4.valid();
59
60      //@ assert Utils.is_(t1,project.Entrytypes.T1.class);
61
62      //@ assert t1.valid();
63
64      Number ret_1 = 0L;
65      //@ assert Utils.is_nat(ret_1);
66
67      return ret_1;
68  }
69
70  public static Number useNotOk() {
71
72      project.Entrytypes.T1 t1 =
73          new project.Entrytypes.T1(
74              new project.Entrytypes.T2(new project.Entrytypes.T3(new project.
75                  Entrytypes.T4(5L))));
76      //@ assert Utils.is_(t1,project.Entrytypes.T1.class);
77
78      project.Entrytypes.T2 stateDes_7 = t1.get_t2();
79
80      project.Entrytypes.T3 stateDes_8 = stateDes_7.get_t3();
81
82      project.Entrytypes.T4 stateDes_9 = stateDes_8.get_t4();
83
84      //@ assert stateDes_9 != null;
85
86      stateDes_9.set_x(60L);
87      //@ assert Utils.is_(stateDes_8,project.Entrytypes.T3.class);
```

## Appendix C. Validation of the translation rules

```
87
88     // @ assert stateDes_8.valid();
89
90     // @ assert Utils.is_(stateDes_7, project.Entrytypes.T2.class);
91
92     // @ assert stateDes_7.valid();
93
94     // @ assert Utils.is_(t1, project.Entrytypes.T1.class);
95
96     // @ assert t1.valid();
97
98     project.Entrytypes.T2 stateDes_10 = t1.get_t2();
99
100    project.Entrytypes.T3 stateDes_11 = stateDes_10.get_t3();
101
102    project.Entrytypes.T4 stateDes_12 = stateDes_11.get_t4();
103
104    // @ assert stateDes_12 != null;
105
106    stateDes_12.set_x(5L);
107    // @ assert Utils.is_(stateDes_11, project.Entrytypes.T3.class);
108
109    // @ assert stateDes_11.valid();
110
111    // @ assert Utils.is_(stateDes_10, project.Entrytypes.T2.class);
112
113    // @ assert stateDes_10.valid();
114
115    // @ assert Utils.is_(t1, project.Entrytypes.T1.class);
116
117    // @ assert t1.valid();
118
119    Number ret_2 = 0L;
120    // @ assert Utils.is_nat(ret_2);
121
122    return ret_2;
123 }
124
125 public static Object Run() {
126
127     IO.println("Before_useOk");
128     {
129         final Number ignorePattern_1 = useOk();
130         // @ assert Utils.is_nat(ignorePattern_1);
131
132         /* skip */
133     }
134
135     IO.println("After_useOk");
136     IO.println("Before_useNotOk");
137     {
138         final Number ignorePattern_2 = useNotOk();
139         // @ assert Utils.is_nat(ignorePattern_2);
140
141         /* skip */
142     }
143
144     IO.println("After_useNotOk");
145     return 0L;
146 }
```

## Appendix C. Validation of the translation rules

```

147
148     public String toString() {
149
150         return "Entry{}";
151     }
152 }

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class T3 implements Record {
11     public project.Entrytypes.T4 t4;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_T3(t4);
13
14     public T3(final project.Entrytypes.T4 _t4) {
15
16         // @ assert Utils.is_(_t4, project.Entrytypes.T4.class);
17
18         t4 = _t4 != null ? Utils.copy(_t4) : null;
19         // @ assert Utils.is_(t4, project.Entrytypes.T4.class);
20
21     }
22     /* @ pure @ */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.T3)) {
27             return false;
28         }
29
30         project.Entrytypes.T3 other = ((project.Entrytypes.T3) obj);
31
32         return Utils.equals(t4, other.t4);
33     }
34     /* @ pure @ */
35
36     public int hashCode() {
37
38         return Utils.hashCode(t4);
39     }
40     /* @ pure @ */
41
42     public project.Entrytypes.T3 copy() {
43
44         return new project.Entrytypes.T3(t4);
45     }
46     /* @ pure @ */
47
48     public String toString() {
49
50         return "mk_Entry`T3" + Utils.formatFields(t4);
51     }
52     /* @ pure @ */
53

```

## Appendix C. Validation of the translation rules

```

54 public project.Entrytypes.T4 get_t4() {
55
56     project.Entrytypes.T4 ret_5 = t4;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_5,project.
        Entrytypes.T4.class));
58
59     return ret_5;
60 }
61
62 public void set_t4(final project.Entrytypes.T4 _t4) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_t4,project.
        Entrytypes.T4.class));
65
66     t4 = _t4;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(t4,project.
        Entrytypes.T4.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_T3(final project.Entrytypes.T4 _t4) {
80
81     return _t4.x.longValue() > 3L;
82 }
83 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class T4 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_T4(x);
13
14     public T4(final Number _x) {
15
16         //@ assert Utils.is_nat(_x);
17
18         x = _x;
19         //@ assert Utils.is_nat(x);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.T4)) {

```

## Appendix C. Validation of the translation rules

```

27     return false;
28 }
29
30 project.Entrytypes.T4 other = ((project.Entrytypes.T4) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.T4 copy() {
43
44     return new project.Entrytypes.T4(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`T4" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_6 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_6));
58
59     return ret_6;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_T4(final Number _x) {
80
81     return _x.longValue() > 4L;
82 }
83 }

```

```

1 package project.Entrytypes;
2

```

## Appendix C. Validation of the translation rules

```

3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class T1 implements Record {
11     public project.Entrytypes.T2 t2;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_T1(t2);
13
14     public T1(final project.Entrytypes.T2 _t2) {
15
16         //@ assert Utils.is_(_t2,project.Entrytypes.T2.class);
17
18         t2 = _t2 != null ? Utils.copy(_t2) : null;
19         //@ assert Utils.is_(t2,project.Entrytypes.T2.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.T1)) {
27             return false;
28         }
29
30         project.Entrytypes.T1 other = ((project.Entrytypes.T1) obj);
31
32         return Utils.equals(t2, other.t2);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {
37
38         return Utils.hashCode(t2);
39     }
40     /*@ pure @*/
41
42     public project.Entrytypes.T1 copy() {
43
44         return new project.Entrytypes.T1(t2);
45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`T1" + Utils.formatFields(t2);
51     }
52     /*@ pure @*/
53
54     public project.Entrytypes.T2 get_t2() {
55
56         project.Entrytypes.T2 ret_3 = t2;
57         //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
58             Entrytypes.T2.class));
59
60         return ret_3;
61     }

```



## Appendix C. Validation of the translation rules

```

62 public void set_t2(final project.Entrytypes.T2 _t2) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_t2,project.
        Entrytypes.T2.class));
65
66     t2 = _t2;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(t2,project.
        Entrytypes.T2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
80
81     return _t2.t3.t4.x.longValue() > 1L;
82 }
83 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class T2 implements Record {
11     public project.Entrytypes.T3 t3;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
13
14     public T2(final project.Entrytypes.T3 _t3) {
15
16         //@ assert Utils.is_(_t3,project.Entrytypes.T3.class);
17
18         t3 = _t3 != null ? Utils.copy(_t3) : null;
19         //@ assert Utils.is_(t3,project.Entrytypes.T3.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.T2)) {
27             return false;
28         }
29
30         project.Entrytypes.T2 other = ((project.Entrytypes.T2) obj);
31
32         return Utils.equals(t3, other.t3);
33     }
34     /*@ pure @*/
35

```

## Appendix C. Validation of the translation rules

```
36 public int hashCode() {
37
38     return Utils.hashCode(t3);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.T2 copy() {
43
44     return new project.Entrytypes.T2(t3);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`T2" + Utils.formatFields(t3);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.T3 get_t3() {
55
56     project.Entrytypes.T3 ret_4 = t3;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_4,project.
        Entrytypes.T3.class));
58
59     return ret_4;
60 }
61
62 public void set_t3(final project.Entrytypes.T3 _t3) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(t3,project.
        Entrytypes.T3.class));
65
66     t3 = _t3;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(t3,project.
        Entrytypes.T3.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_T2(final project.Entrytypes.T3 _t3) {
80
81     Boolean andResult_2 = false;
82
83     if (_t3.t4.x.longValue() > 2L) {
84         if (!(Utils.equals(_t3.t4.x, 60L))) {
85             andResult_2 = true;
86         }
87     }
88
89     return andResult_2;
90 }
91 }
```

## Appendix C. Validation of the translation rules

```
"Before useOk"
"After useOk"
"Before useNotOk"
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T2.java:72: JML invariant is false
  on leaving method project.Entrytypes.T2.valid()
  public Boolean valid() {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
  /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T2.java:72:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79: JML caller invariant is
  false on leaving calling method (Parameter: _t2, Caller: project.
  Entrytypes.T1.inv_T1(project.Entrytypes.T2), Callee: java.lang.Number.
  longValue())
  public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
  /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79: JML invariant is false
  on leaving method project.Entrytypes.T1.inv_T1(project.Entrytypes.T2) (
  parameter _t2)
  public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
  /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79: JML caller invariant is
  false on leaving calling method (Parameter: _t2, Caller: project.
  Entrytypes.T1.inv_T1(project.Entrytypes.T2), Callee: java.lang.Number.
  longValue())
  public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
  /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  RecInRecInvViolation/project/Entrytypes/T1.java:79: JML invariant is false
  on leaving method project.Entrytypes.T1.inv_T1(project.Entrytypes.T2) (
  parameter _t2)
  public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
```

## Appendix C. Validation of the translation rules

```
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: JML invariant is false
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t2, Caller: project.
Entrytypes.T1.inv_T1(project.Entrytypes.T2), Callee: java.lang.Number.
longValue())
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML invariant is false
on leaving method project.Entrytypes.T1.inv_T1(project.Entrytypes.T2) (
parameter _t2)
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t2, Caller: project.
Entrytypes.T1.inv_T1(project.Entrytypes.T2), Callee: java.lang.Number.
longValue())
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML invariant is false
on leaving method project.Entrytypes.T1.inv_T1(project.Entrytypes.T2) (
parameter _t2)
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
```

## Appendix C. Validation of the translation rules

```
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML caller invariant is
  false on leaving calling method (Parameter: _t2, Caller: project.
Entrytypes.T1.inv_T1(project.Entrytypes.T2), Callee: java.lang.Number.
  longValue())
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML invariant is false
on leaving method project.Entrytypes.T1.inv_T1(project.Entrytypes.T2) (
parameter _t2)
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:54: JML invariant is false
on leaving method project.Entrytypes.T1.get_t2() (for result type)
public project.Entrytypes.T2 get_t2() {
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:54:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: JML invariant is false
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML caller invariant is
  false on leaving calling method (Parameter: _t2, Caller: project.
Entrytypes.T1.inv_T1(project.Entrytypes.T2), Callee: java.lang.Number.
  longValue())
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79: JML invariant is false
on leaving method project.Entrytypes.T1.inv_T1(project.Entrytypes.T2) (
parameter _t2)
public static Boolean inv_T1(final project.Entrytypes.T2 _t2) {
  ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
```

```

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T1.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
Entry.java:100: JML invariant is false on entering method project.Entrytypes.
T2.get_t3() from project.Entry.useNotOk()
project.Entrytypes.T3 stateDes_11 = stateDes_10.get_t3();
      ^
Entry.java:100:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:54: JML invariant is false
on leaving method project.Entrytypes.T2.get_t3()
public project.Entrytypes.T3 get_t3() {
      ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
RecInRecInvViolation/project/Entrytypes/T2.java:54:
//@ public instance invariant project.Entry.invChecksOn ==> inv_T2(t3);
      ^
"After useNotOk"
```

## C.56 MaskedRecNamedTypeInv.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  types
10
11 R1 :: r2 : R2
12 inv r1 == r1.r2.t3.r4.x <> 1;
13
14 R2 :: t3 : T3
15 inv r2 == r2.t3.r4.x <> 2;
16
17 T3 = R3
18 inv t3 == t3.r4.x <> 10;
19
20 R3 :: r4 : R4
21 inv r3 == r3.r4.x <> 3;
22
23 R4 :: x : int
24 inv r4 == r4.x <> 4;
25
26 operations
27
28 Run : () ==> ?
29 Run () ==
30 (
31   IO`println("Before_useOk");
```

## Appendix C. Validation of the translation rules

```

32  let - = useOk() in skip;
33  IO`println("After_useOk");
34  IO`println("Before_useNotOk");
35  let - = useNotOk() in skip;
36  IO`println("After_useNotOk");
37  return 0;
38 );
39
40 useOk : () ==> nat
41 useOk () ==
42 (
43   dcl r1 : R1 := mk_R1 (mk_R2 (mk_R3 (mk_R4 (5) ) ) );
44
45   atomic
46   (
47     r1.r2.t3.r4.x := 10;
48     r1.r2.t3.r4.x := 5;
49   );
50
51   return 0;
52 );
53
54 useNotOk : () ==> nat
55 useNotOk () ==
56 (
57   dcl r1 : R1 := mk_R1 (mk_R2 (mk_R3 (mk_R4 (5) ) ) );
58
59   atomic
60   (
61     r1.r2.t3.r4.x := 10;
62   );
63
64   return 0;
65 );
66
67 end Entry

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R1 implements Record {
11   public project.Entrytypes.R2 r2;
12   //@ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14   public R1(final project.Entrytypes.R2 _r2) {
15
16     //@ assert Utils.is_(_r2,project.Entrytypes.R2.class);
17
18     r2 = _r2 != null ? Utils.copy(_r2) : null;
19     //@ assert Utils.is_(r2,project.Entrytypes.R2.class);
20
21   }
22   /*@ pure @*/
23

```

## Appendix C. Validation of the translation rules

```
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.R1)) {
27         return false;
28     }
29
30     project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32     return Utils.equals(r2, other.r2);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(r2);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R1 copy() {
43
44     return new project.Entrytypes.R1(r2);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R1" + Utils.formatFields(r2);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.R2 get_r2() {
55
56     project.Entrytypes.R2 ret_3 = r2;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
        Entrytypes.R2.class));
58
59     return ret_3;
60 }
61
62 public void set_r2(final project.Entrytypes.R2 _r2) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_r2,project.
        Entrytypes.R2.class));
65
66     r2 = _r2;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r2,project.
        Entrytypes.R2.class));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
80
```



## Appendix C. Validation of the translation rules

```

81     return !(Utils.equals(_r2.t3.r4.x, 1L));
82 }
83
84 /*@ pure @*/
85 /*@ helper @*/
86
87 public static Boolean inv_Entry_T3(final Object check_t3) {
88
89     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
90
91     return !(Utils.equals(t3.get_r4().get_x(), 10L));
92 }
93 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R2 implements Record {
11     public project.Entrytypes.R3 t3;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(t3);
13
14     public R2(final project.Entrytypes.R3 _t3) {
15
16         //@ assert (Utils.is_(_t3,project.Entrytypes.R3.class) && inv_Entry_T3(
17             _t3));
18
19         t3 = _t3 != null ? Utils.copy(_t3) : null;
20         //@ assert (Utils.is_(t3,project.Entrytypes.R3.class) && inv_Entry_T3(t3
21             ));
22     }
23     /*@ pure @*/
24
25     public boolean equals(final Object obj) {
26
27         if (!(obj instanceof project.Entrytypes.R2)) {
28             return false;
29         }
30
31         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
32
33         return Utils.equals(t3, other.t3);
34     }
35     /*@ pure @*/
36
37     public int hashCode() {
38
39         return Utils.hashCode(t3);
40     }
41     /*@ pure @*/
42
43     public project.Entrytypes.R2 copy() {
44
45         return new project.Entrytypes.R2(t3);

```

## Appendix C. Validation of the translation rules

```

45     }
46     /*@ pure @*/
47
48     public String toString() {
49
50         return "mk_Entry`R2" + Utils.formatFields(t3);
51     }
52     /*@ pure @*/
53
54     public project.Entrytypes.R3 get_t3() {
55
56         project.Entrytypes.R3 ret_4 = t3;
57         //@ assert project.Entry.invChecksOn ==> ((Utils.is_(ret_4,project.
           Entrytypes.R3.class) && inv_Entry_T3(ret_4)));
58
59         return ret_4;
60     }
61
62     public void set_t3(final project.Entrytypes.R3 _t3) {
63
64         //@ assert project.Entry.invChecksOn ==> ((Utils.is_(t3,project.
           Entrytypes.R3.class) && inv_Entry_T3(t3)));
65
66         t3 = _t3;
67         //@ assert project.Entry.invChecksOn ==> ((Utils.is_(t3,project.
           Entrytypes.R3.class) && inv_Entry_T3(t3)));
68
69     }
70     /*@ pure @*/
71
72     public Boolean valid() {
73
74         return true;
75     }
76     /*@ pure @*/
77     /*@ helper @*/
78
79     public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
80
81         return !(Utils.equals(_t3.r4.x, 2L));
82     }
83
84     /*@ pure @*/
85     /*@ helper @*/
86
87     public static Boolean inv_Entry_T3(final Object check_t3) {
88
89         project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
90
91         return !(Utils.equals(t3.get_r4().get_x(), 10L));
92     }
93 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")

```

## Appendix C. Validation of the translation rules

```

8  // @ nullable_by_default
9
10 final public class R4 implements Record {
11     public Number x;
12     // @ public instance invariant project.Entry.invChecksOn ==> inv_R4(x);
13
14     public R4(final Number _x) {
15
16         // @ assert Utils.is_int(_x);
17
18         x = _x;
19         // @ assert Utils.is_int(x);
20
21     }
22     /* @ pure */
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R4)) {
27             return false;
28         }
29
30         project.Entrytypes.R4 other = ((project.Entrytypes.R4) obj);
31
32         return Utils.equals(x, other.x);
33     }
34     /* @ pure */
35
36     public int hashCode() {
37
38         return Utils.hashCode(x);
39     }
40     /* @ pure */
41
42     public project.Entrytypes.R4 copy() {
43
44         return new project.Entrytypes.R4(x);
45     }
46     /* @ pure */
47
48     public String toString() {
49
50         return "mk_Entry'R4" + Utils.formatFields(x);
51     }
52     /* @ pure */
53
54     public Number get_x() {
55
56         Number ret_6 = x;
57         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_6));
58
59         return ret_6;
60     }
61
62     public void set_x(final Number _x) {
63
64         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66         x = _x;
67         // @ assert project.Entry.invChecksOn ==> (Utils.is_int(x));

```

## Appendix C. Validation of the translation rules

```

68
69     }
70     /*@ pure @*/
71
72     public Boolean valid() {
73
74         return true;
75     }
76     /*@ pure @*/
77     /*@ helper @*/
78
79     public static Boolean inv_R4(final Number _x) {
80
81         return !(Utils.equals(_x, 4L));
82     }
83
84     /*@ pure @*/
85     /*@ helper @*/
86
87     public static Boolean inv_Entry_T3(final Object check_t3) {
88
89         project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
90
91         return !(Utils.equals(t3.get_r4().get_x(), 10L));
92     }
93 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_useOk");
18         {
19             final Number ignorePattern_1 = useOk();
20             //@ assert Utils.is_nat(ignorePattern_1);
21
22             /* skip */
23         }
24
25         IO.println("After_useOk");
26         IO.println("Before_useNotOk");
27         {
28             final Number ignorePattern_2 = useNotOk();
29             //@ assert Utils.is_nat(ignorePattern_2);
30
31             /* skip */
32         }
33

```

## Appendix C. Validation of the translation rules

```
34     IO.println("After_useNotOk");
35     return 0L;
36 }
37
38 public static Number useOk() {
39
40     project.Entrytypes.R1 r1 =
41         new project.Entrytypes.R1(
42             new project.Entrytypes.R2(new project.Entrytypes.R3(new project.
43                 Entrytypes.R4(5L))));
44     //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
45
46     Number atomicTmp_1 = 10L;
47     //@ assert Utils.is_int(atomicTmp_1);
48
49     Number atomicTmp_2 = 5L;
50     //@ assert Utils.is_int(atomicTmp_2);
51
52     {
53         /* Start of atomic statement */
54         //@ set invChecksOn = false;
55
56         project.Entrytypes.R2 stateDes_1 = r1.get_r2();
57
58         project.Entrytypes.R3 stateDes_2 = stateDes_1.get_t3();
59
60         project.Entrytypes.R4 stateDes_3 = stateDes_2.get_r4();
61
62         //@ assert stateDes_3 != null;
63
64         stateDes_3.set_x(atomicTmp_1);
65
66         project.Entrytypes.R2 stateDes_4 = r1.get_r2();
67
68         project.Entrytypes.R3 stateDes_5 = stateDes_4.get_t3();
69
70         project.Entrytypes.R4 stateDes_6 = stateDes_5.get_r4();
71
72         //@ assert stateDes_6 != null;
73
74         stateDes_6.set_x(atomicTmp_2);
75
76         //@ set invChecksOn = true;
77
78         //@ assert stateDes_3.valid();
79
80         //@ assert (Utils.is_(stateDes_2,project.Entrytypes.R3.class) &&
81             inv_Entry_T3(stateDes_2));
82
83         //@ assert stateDes_2.valid();
84
85         //@ assert Utils.is_(stateDes_1,project.Entrytypes.R2.class);
86
87         //@ assert stateDes_1.valid();
88
89         //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
90
91         //@ assert r1.valid();
92
93         //@ assert stateDes_6.valid();
94     }
```

## Appendix C. Validation of the translation rules

```

92
93     //@ assert (Utils.is_(stateDes_5,project.Entrytypes.R3.class) &&
94         inv_Entry_T3(stateDes_5));
95
96     //@ assert stateDes_5.valid();
97
98     //@ assert Utils.is_(stateDes_4,project.Entrytypes.R2.class);
99
100    //@ assert stateDes_4.valid();
101
102    } /* End of atomic statement */
103
104    Number ret_1 = 0L;
105    //@ assert Utils.is_nat(ret_1);
106
107    return ret_1;
108  }
109
110  public static Number useNotOk() {
111
112    project.Entrytypes.R1 r1 =
113      new project.Entrytypes.R1(
114        new project.Entrytypes.R2(new project.Entrytypes.R3(new project.
115          Entrytypes.R4(5L))));
116    //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
117
118    Number atomicTmp_3 = 10L;
119    //@ assert Utils.is_int(atomicTmp_3);
120
121    {
122      /* Start of atomic statement */
123      //@ set invChecksOn = false;
124
125      project.Entrytypes.R2 stateDes_7 = r1.get_r2();
126
127      project.Entrytypes.R3 stateDes_8 = stateDes_7.get_t3();
128
129      project.Entrytypes.R4 stateDes_9 = stateDes_8.get_r4();
130
131      //@ assert stateDes_9 != null;
132
133      stateDes_9.set_x(atomicTmp_3);
134
135      //@ set invChecksOn = true;
136
137      //@ assert stateDes_9.valid();
138
139      //@ assert (Utils.is_(stateDes_8,project.Entrytypes.R3.class) &&
140          inv_Entry_T3(stateDes_8));
141
142      //@ assert stateDes_8.valid();
143
144      //@ assert Utils.is_(stateDes_7,project.Entrytypes.R2.class);
145
146      //@ assert stateDes_7.valid();
147
148      //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
149
150      //@ assert r1.valid();

```

## Appendix C. Validation of the translation rules

```

149     } /* End of atomic statement */
150
151     Number ret_2 = 0L;
152     //@ assert Utils.is_nat(ret_2);
153
154     return ret_2;
155 }
156
157 public String toString() {
158
159     return "Entry{}";
160 }
161
162 /*@ pure @*/
163 /*@ helper @*/
164
165 public static Boolean inv_Entry_T3(final Object check_t3) {
166
167     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
168
169     return !(Utils.equals(t3.get_r4().get_x(), 10L));
170 }
171 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R3 implements Record {
11     public project.Entrytypes.R4 r4;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
13
14     public R3(final project.Entrytypes.R4 _r4) {
15
16         //@ assert Utils.is_(_r4,project.Entrytypes.R4.class);
17
18         r4 = _r4 != null ? Utils.copy(_r4) : null;
19         //@ assert Utils.is_(r4,project.Entrytypes.R4.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.R3)) {
27             return false;
28         }
29
30         project.Entrytypes.R3 other = ((project.Entrytypes.R3) obj);
31
32         return Utils.equals(r4, other.r4);
33     }
34     /*@ pure @*/
35
36     public int hashCode() {

```

## Appendix C. Validation of the translation rules

```

37
38     return Utils.hashCode(r4);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R3 copy() {
43
44     return new project.Entrytypes.R3(r4);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R3" + Utils.formatFields(r4);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.R4 get_r4() {
55
56     project.Entrytypes.R4 ret_5 = r4;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_5,project.
58         Entrytypes.R4.class));
59
60     return ret_5;
61 }
62
63 public void set_r4(final project.Entrytypes.R4 _r4) {
64
65     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r4,project.
66         Entrytypes.R4.class));
67
68     r4 = _r4;
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r4,project.
70         Entrytypes.R4.class));
71
72 }
73 /*@ pure @*/
74
75 public Boolean valid() {
76
77     return true;
78 }
79 /*@ pure @*/
80 /*@ helper @*/
81
82 public static Boolean inv_R3(final project.Entrytypes.R4 _r4) {
83
84     return !(Utils.equals(_r4.x, 3L));
85 }
86
87 /*@ pure @*/
88 /*@ helper @*/
89
90 public static Boolean inv_Entry_T3(final Object check_t3) {
91
92     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
93
94     return !(Utils.equals(t3.get_r4().get_x(), 10L));
95 }
96
97 }

```



```

"Before useOk"
"After useOk"
"Before useNotOk"
Entry.java:137: JML assertion is false
    //@ assert (Utils.is_(stateDes_8,project.Entrytypes.R3.class) &&
        inv_Entry_T3(stateDes_8));
        ^
"After useNotOk"

```

## C.57 MaskedRecInvViolated.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  types
10
11 R1 :: r2 : R2
12 inv r1 == r1.r2.t3.r4.x <> 1;
13
14 R2 :: t3 : T3
15 inv r2 == r2.t3.r4.x <> 2;
16
17 T3 = R3
18 inv t3 == t3.r4.x <> 10;
19
20 R3 :: r4 : R4
21 inv r3 == r3.r4.x <> 3;
22
23 R4 :: x : int
24 inv r4 == r4.x <> 4;
25
26 operations
27
28 Run : () ==> ?
29 Run () ==
30 (
31   IO`println("Before_useOk");
32   let - = useOk() in skip;
33   IO`println("After_useOk");
34   IO`println("Before_useNotOk");
35   let - = useNotOk() in skip;
36   IO`println("After_useNotOk");
37   return 0;
38 );
39
40 useOk : () ==> nat
41 useOk () ==
42 (
43   dcl r1 : R1 := mk_R1(mk_R2(mk_R3(mk_R4(5))));
44
45   atomic

```

## Appendix C. Validation of the translation rules

```

46  (
47    r1.r2.t3.r4.x := 10;
48    r1.r2.t3.r4.x := 3;
49    r1.r2.t3.r4.x := 5;
50  );
51
52  return 0;
53 );
54
55 useNotOk : () ==> nat
56 useNotOk () ==
57 (
58   dcl r1 : R1 := mk_R1 (mk_R2 (mk_R3 (mk_R4 (5))));
59
60   atomic
61   (
62     r1.r2.t3.r4.x := 3;
63   );
64
65   return 0;
66 );
67
68 end Entry

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class R1 implements Record {
11   public project.Entrytypes.R2 r2;
12   //@ public instance invariant project.Entry.invChecksOn ==> inv_R1(r2);
13
14   public R1(final project.Entrytypes.R2 _r2) {
15
16     //@ assert Utils.is_(_r2,project.Entrytypes.R2.class);
17
18     r2 = _r2 != null ? Utils.copy(_r2) : null;
19     //@ assert Utils.is_(r2,project.Entrytypes.R2.class);
20
21   }
22   /*@ pure @*/
23
24   public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.R1)) {
27       return false;
28     }
29
30     project.Entrytypes.R1 other = ((project.Entrytypes.R1) obj);
31
32     return Utils.equals(r2, other.r2);
33   }
34   /*@ pure @*/
35
36   public int hashCode() {

```

## Appendix C. Validation of the translation rules

```

37
38     return Utils.hashCode(r2);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R1 copy() {
43
44     return new project.Entrytypes.R1(r2);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry `R1" + Utils.formatFields(r2);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.R2 get_r2() {
55
56     project.Entrytypes.R2 ret_3 = r2;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_3,project.
58         Entrytypes.R2.class));
59
60     return ret_3;
61 }
62
63 public void set_r2(final project.Entrytypes.R2 _r2) {
64
65     //@ assert project.Entry.invChecksOn ==> (Utils.is_(_r2,project.
66         Entrytypes.R2.class));
67
68     r2 = _r2;
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r2,project.
70         Entrytypes.R2.class));
71
72 }
73 /*@ pure @*/
74
75 public Boolean valid() {
76
77     return true;
78 }
79 /*@ pure @*/
80 /*@ helper @*/
81
82 public static Boolean inv_R1(final project.Entrytypes.R2 _r2) {
83
84     return !(Utils.equals(_r2.t3.r4.x, 1L));
85 }
86
87 /*@ pure @*/
88 /*@ helper @*/
89
90 public static Boolean inv_Entry_T3(final Object check_t3) {
91
92     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
93
94     return !(Utils.equals(t3.get_r4().get_x(), 10L));
95 }
96
97 }

```

## Appendix C. Validation of the translation rules

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R2 implements Record {
11     public project.Entrytypes.R3 t3;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R2(t3);
13
14     public R2(final project.Entrytypes.R3 _t3) {
15
16         //@ assert (Utils.is_(_t3,project.Entrytypes.R3.class) && inv_Entry_T3(
17             _t3));
18
19         t3 = _t3 != null ? Utils.copy(_t3) : null;
20         //@ assert (Utils.is_(t3,project.Entrytypes.R3.class) && inv_Entry_T3(t3
21             ));
22     }
23     /*@ pure @*/
24
25     public boolean equals(final Object obj) {
26
27         if (!(obj instanceof project.Entrytypes.R2)) {
28             return false;
29         }
30
31         project.Entrytypes.R2 other = ((project.Entrytypes.R2) obj);
32
33         return Utils.equals(t3, other.t3);
34     }
35     /*@ pure @*/
36
37     public int hashCode() {
38
39         return Utils.hashCode(t3);
40     }
41     /*@ pure @*/
42
43     public project.Entrytypes.R2 copy() {
44
45         return new project.Entrytypes.R2(t3);
46     }
47     /*@ pure @*/
48
49     public String toString() {
50
51         return "mk_Entry`R2" + Utils.formatFields(t3);
52     }
53     /*@ pure @*/
54
55     public project.Entrytypes.R3 get_t3() {
56
57         project.Entrytypes.R3 ret_4 = t3;
58         //@ assert project.Entry.invChecksOn ==> ((Utils.is_(ret_4,project.

```

## Appendix C. Validation of the translation rules

```

58         Entrytypes.R3.class) && inv_Entry_T3(ret_4)));
59     return ret_4;
60 }
61
62 public void set_t3(final project.Entrytypes.R3 _t3) {
63
64     //@ assert project.Entry.invChecksOn ==> ((Utils.is_(_t3,project.
        Entrytypes.R3.class) && inv_Entry_T3(_t3)));
65
66     t3 = _t3;
67     //@ assert project.Entry.invChecksOn ==> ((Utils.is_(t3,project.
        Entrytypes.R3.class) && inv_Entry_T3(t3)));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
80
81     return !(Utils.equals(_t3.r4.x, 2L));
82 }
83
84 /*@ pure @*/
85 /*@ helper @*/
86
87 public static Boolean inv_Entry_T3(final Object check_t3) {
88
89     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
90
91     return !(Utils.equals(t3.get_r4().get_x(), 10L));
92 }
93 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R4 implements Record {
11     public Number x;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R4(x);
13
14     public R4(final Number _x) {
15
16         //@ assert Utils.is_int(_x);
17
18         x = _x;
19         //@ assert Utils.is_int(x);
20

```

## Appendix C. Validation of the translation rules

```
21 }
22 /*@ pure @*/
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.R4)) {
27         return false;
28     }
29
30     project.Entrytypes.R4 other = ((project.Entrytypes.R4) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R4 copy() {
43
44     return new project.Entrytypes.R4(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R4" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_6 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_6));
58
59     return ret_6;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_R4(final Number _x) {
80
```

## Appendix C. Validation of the translation rules

```

81     return !(Utils.equals(_x, 4L));
82 }
83
84 /*@ pure @*/
85 /*@ helper @*/
86
87 public static Boolean inv_Entry_T3(final Object check_t3) {
88
89     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
90
91     return !(Utils.equals(t3.get_r4().get_x(), 10L));
92 }
93 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_useOk");
18         {
19             final Number ignorePattern_1 = useOk();
20             //@ assert Utils.is_nat(ignorePattern_1);
21
22             /* skip */
23         }
24
25         IO.println("After_useOk");
26         IO.println("Before_useNotOk");
27         {
28             final Number ignorePattern_2 = useNotOk();
29             //@ assert Utils.is_nat(ignorePattern_2);
30
31             /* skip */
32         }
33
34         IO.println("After_useNotOk");
35         return 0L;
36     }
37
38     public static Number useOk() {
39
40         project.Entrytypes.R1 r1 =
41             new project.Entrytypes.R1(
42                 new project.Entrytypes.R2(new project.Entrytypes.R3(new project.
43                     Entrytypes.R4(5L))));
44         //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
45
46         Number atomicTmp_1 = 10L;

```

## Appendix C. Validation of the translation rules

```
46 // @ assert Utils.is_int(atomicTmp_1);
47
48 Number atomicTmp_2 = 3L;
49 // @ assert Utils.is_int(atomicTmp_2);
50
51 Number atomicTmp_3 = 5L;
52 // @ assert Utils.is_int(atomicTmp_3);
53
54 {
55     /* Start of atomic statement */
56     // @ set invChecksOn = false;
57
58     project.Entrytypes.R2 stateDes_1 = r1.get_r2();
59
60     project.Entrytypes.R3 stateDes_2 = stateDes_1.get_t3();
61
62     project.Entrytypes.R4 stateDes_3 = stateDes_2.get_r4();
63
64     // @ assert stateDes_3 != null;
65
66     stateDes_3.set_x(atomicTmp_1);
67
68     project.Entrytypes.R2 stateDes_4 = r1.get_r2();
69
70     project.Entrytypes.R3 stateDes_5 = stateDes_4.get_t3();
71
72     project.Entrytypes.R4 stateDes_6 = stateDes_5.get_r4();
73
74     // @ assert stateDes_6 != null;
75
76     stateDes_6.set_x(atomicTmp_2);
77
78     project.Entrytypes.R2 stateDes_7 = r1.get_r2();
79
80     project.Entrytypes.R3 stateDes_8 = stateDes_7.get_t3();
81
82     project.Entrytypes.R4 stateDes_9 = stateDes_8.get_r4();
83
84     // @ assert stateDes_9 != null;
85
86     stateDes_9.set_x(atomicTmp_3);
87
88     // @ set invChecksOn = true;
89
90     // @ assert stateDes_3.valid();
91
92     // @ assert (Utils.is_(stateDes_2, project.Entrytypes.R3.class) &&
93         inv_Entry_T3(stateDes_2));
94
95     // @ assert stateDes_2.valid();
96
97     // @ assert Utils.is_(stateDes_1, project.Entrytypes.R2.class);
98
99     // @ assert stateDes_1.valid();
100
101     // @ assert Utils.is_(r1, project.Entrytypes.R1.class);
102
103     // @ assert r1.valid();
104
105     // @ assert stateDes_6.valid();
```



## Appendix C. Validation of the translation rules

```
105
106      //@ assert (Utils.is_(stateDes_5,project.Entrytypes.R3.class) &&
      inv_Entry_T3(stateDes_5));
107
108      //@ assert stateDes_5.valid();
109
110      //@ assert Utils.is_(stateDes_4,project.Entrytypes.R2.class);
111
112      //@ assert stateDes_4.valid();
113
114      //@ assert stateDes_9.valid();
115
116      //@ assert (Utils.is_(stateDes_8,project.Entrytypes.R3.class) &&
      inv_Entry_T3(stateDes_8));
117
118      //@ assert stateDes_8.valid();
119
120      //@ assert Utils.is_(stateDes_7,project.Entrytypes.R2.class);
121
122      //@ assert stateDes_7.valid();
123
124      } /* End of atomic statement */
125
126      Number ret_1 = 0L;
127      //@ assert Utils.is_nat(ret_1);
128
129      return ret_1;
130  }
131
132  public static Number useNotOk() {
133
134      project.Entrytypes.R1 r1 =
135          new project.Entrytypes.R1(
136              new project.Entrytypes.R2(new project.Entrytypes.R3(new project.
                  Entrytypes.R4(5L))));
137      //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
138
139      Number atomicTmp_4 = 3L;
140      //@ assert Utils.is_int(atomicTmp_4);
141
142      {
143          /* Start of atomic statement */
144          //@ set invChecksOn = false;
145
146          project.Entrytypes.R2 stateDes_10 = r1.get_r2();
147
148          project.Entrytypes.R3 stateDes_11 = stateDes_10.get_t3();
149
150          project.Entrytypes.R4 stateDes_12 = stateDes_11.get_r4();
151
152          //@ assert stateDes_12 != null;
153
154          stateDes_12.set_x(atomicTmp_4);
155
156          //@ set invChecksOn = true;
157
158          //@ assert stateDes_12.valid();
159
160          //@ assert (Utils.is_(stateDes_11,project.Entrytypes.R3.class) &&
              inv_Entry_T3(stateDes_11));
```

## Appendix C. Validation of the translation rules

```

161
162     //@ assert stateDes_11.valid();
163
164     //@ assert Utils.is_(stateDes_10,project.Entrytypes.R2.class);
165
166     //@ assert stateDes_10.valid();
167
168     //@ assert Utils.is_(r1,project.Entrytypes.R1.class);
169
170     //@ assert r1.valid();
171
172     } /* End of atomic statement */
173
174     Number ret_2 = 0L;
175     //@ assert Utils.is_nat(ret_2);
176
177     return ret_2;
178 }
179
180 public String toString() {
181
182     return "Entry{}";
183 }
184
185 /*@ pure @*/
186 /*@ helper @*/
187
188 public static Boolean inv_Entry_T3(final Object check_t3) {
189
190     project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
191
192     return !(Utils.equals(t3.get_r4().get_x(), 10L));
193 }
194 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class R3 implements Record {
11     public project.Entrytypes.R4 r4;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
13
14     public R3(final project.Entrytypes.R4 _r4) {
15
16         //@ assert Utils.is_(_r4,project.Entrytypes.R4.class);
17
18         r4 = _r4 != null ? Utils.copy(_r4) : null;
19         //@ assert Utils.is_(r4,project.Entrytypes.R4.class);
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25

```

## Appendix C. Validation of the translation rules

```
26     if (!(obj instanceof project.Entrytypes.R3)) {
27         return false;
28     }
29
30     project.Entrytypes.R3 other = ((project.Entrytypes.R3) obj);
31
32     return Utils.equals(r4, other.r4);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(r4);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.R3 copy() {
43
44     return new project.Entrytypes.R3(r4);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`R3" + Utils.formatFields(r4);
51 }
52 /*@ pure @*/
53
54 public project.Entrytypes.R4 get_r4() {
55
56     project.Entrytypes.R4 ret_5 = r4;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_(ret_5,project.
58         Entrytypes.R4.class));
59
60     return ret_5;
61 }
62
63 public void set_r4(final project.Entrytypes.R4 _r4) {
64
65     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r4,project.
66         Entrytypes.R4.class));
67
68     r4 = _r4;
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_(r4,project.
70         Entrytypes.R4.class));
71
72 }
73 /*@ pure @*/
74
75 public Boolean valid() {
76
77     return true;
78 }
79 /*@ pure @*/
80 /*@ helper @*/
81
82 public static Boolean inv_R3(final project.Entrytypes.R4 _r4) {
83
84     return !(Utils.equals(_r4.x, 3L));
85 }
```

## Appendix C. Validation of the translation rules

```

83
84  /*@ pure @*/
85  /*@ helper @*/
86
87  public static Boolean inv_Entry_T3(final Object check_t3) {
88
89      project.Entrytypes.R3 t3 = ((project.Entrytypes.R3) check_t3);
90
91      return !(Utils.equals(t3.get_r4().get_x(), 10L));
92  }
93  }

```

```

"Before useOk"
"After useOk"
"Before useNotOk"
Entry.java:192: JML invariant is false on entering method project.Entrytypes.
R3.get_r4() from project.Entry.inv_Entry_T3(java.lang.Object)
return !(Utils.equals(t3.get_r4().get_x(), 10L));
                        ^
Entry.java:192:
  /*@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:54: JML invariant is false
on leaving method project.Entrytypes.R3.get_r4()
public project.Entrytypes.R4 get_r4() {
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:54:
  /*@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:72: JML invariant is false
on leaving method project.Entrytypes.R3.valid()
public Boolean valid() {
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:72:
  /*@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
  /*@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
                        ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (

```

## Appendix C. Validation of the translation rules

```
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: JML invariant is false
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
```

## Appendix C. Validation of the translation rules

```
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utills.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utills.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utills.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
^
```

## Appendix C. Validation of the translation rules

```
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
    /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
  on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
  parameter _t3)
  public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
    /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
  false on leaving calling method (Parameter: _t3, Caller: project.
  Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
  runtime.Utills.equals(java.lang.Object, java.lang.Object))
  public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
    /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
  on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
  parameter _t3)
  public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
    /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
  false on leaving calling method (Parameter: _t3, Caller: project.
  Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
  runtime.Utills.equals(java.lang.Object, java.lang.Object))
  public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
    /home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79:
  //@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^

/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
  MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
  on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
  parameter _t3)
```

## Appendix C. Validation of the translation rules

```
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
```



## Appendix C. Validation of the translation rules

```
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML caller invariant is
false on leaving calling method (Parameter: _t3, Caller: project.
Entrytypes.R2.inv_R2(project.Entrytypes.R3), Callee: org.overture.codegen.
runtime.Utils.equals(java.lang.Object, java.lang.Object))
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79: JML invariant is false
on leaving method project.Entrytypes.R2.inv_R2(project.Entrytypes.R3) (
parameter _t3)
public static Boolean inv_R2(final project.Entrytypes.R3 _t3) {
    ^
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R3.java:12: Associated declaration:
/home/peter/git-repos/ovt/core/codegen/vdm2jml/target/jml/code/
MaskedRecInvViolated/project/Entrytypes/R2.java:79:
//@ public instance invariant project.Entry.invChecksOn ==> inv_R3(r4);
    ^
"After useNotOk"
```

### C.58 ModifyRecInMap.vdmsl

```
1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
```

```

6
7 operations
8
9 types
10
11 A :: m : map nat to B
12 inv a == forall i in set dom a.m & a.m(i).x = 2;
13 B :: x : nat;
14
15 operations
16
17 Run : () ==> ?
18 Run () ==
19 (
20   IO.println("Before_useOk");
21   let - = useOk() in skip;
22   IO.println("After_useOk");
23   IO.println("Before_useNotOk");
24   let - = useNotOk() in skip;
25   IO.println("After_useNotOk");
26   return 0;
27 );
28
29 useOk : () ==> nat
30 useOk () ==
31 (
32   dcl a : A := mk_A({1 |-> mk_B(2)});
33   a.m(1).x := 2;
34   return 0;
35 );
36
37 useNotOk : () ==> nat
38 useNotOk () ==
39 (
40   dcl a : A := mk_A({1 |-> mk_B(2)});
41   a.m(1).x := 1;
42   return 0;
43 );
44
45 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_useOk");
18     {
19       final Number ignorePattern_1 = useOk();

```

## Appendix C. Validation of the translation rules

```
20      //@ assert Utils.is_nat(ignorePattern_1);
21
22      /* skip */
23  }
24
25  IO.println("After_useOk");
26  IO.println("Before_useNotOk");
27  {
28      final Number ignorePattern_2 = useNotOk();
29      //@ assert Utils.is_nat(ignorePattern_2);
30
31      /* skip */
32  }
33
34  IO.println("After_useNotOk");
35  return 0L;
36  }
37
38  public static Number useOk() {
39
40      project.Entrytypes.A a =
41          new project.Entrytypes.A(MapUtil.map(new Maplet(1L, new project.
42              Entrytypes.B(2L))));
43      //@ assert Utils.is_(a,project.Entrytypes.A.class);
44
45      VDMMap stateDes_1 = a.get_m();
46
47      project.Entrytypes.B stateDes_2 = ((project.Entrytypes.B) Utils.get(
48          stateDes_1, 1L));
49
50      //@ assert stateDes_2 != null;
51
52      stateDes_2.set_x(2L);
53      //@ assert (V2J.isMap(stateDes_1) && (\forall int i_1; 0 <= i_1 && i_1 <
54          V2J.size(stateDes_1); Utils.is_nat(V2J.getDom(stateDes_1,i_1)) &&
55          Utils.is_(V2J.getRng(stateDes_1,i_1),project.Entrytypes.B.class)));
56
57      //@ assert Utils.is_(a,project.Entrytypes.A.class);
58
59      //@ assert a.valid();
60
61      Number ret_1 = 0L;
62      //@ assert Utils.is_nat(ret_1);
63
64      return ret_1;
65  }
66
67  public static Number useNotOk() {
68
69      project.Entrytypes.A a =
70          new project.Entrytypes.A(MapUtil.map(new Maplet(1L, new project.
71              Entrytypes.B(2L))));
72      //@ assert Utils.is_(a,project.Entrytypes.A.class);
73
74      VDMMap stateDes_3 = a.get_m();
75
76      project.Entrytypes.B stateDes_4 = ((project.Entrytypes.B) Utils.get(
77          stateDes_3, 1L));
78
79      //@ assert stateDes_4 != null;
```

## Appendix C. Validation of the translation rules

```

74
75     stateDes_4.set_x(1L);
76     //@ assert (V2J.isMap(stateDes_3) && (\forallall int i_1; 0 <= i_1 && i_1 <
        V2J.size(stateDes_3); Utils.is_nat(V2J.getDom(stateDes_3,i_1)) &&
        Utils.is_(V2J.getRng(stateDes_3,i_1),project.Entrytypes.B.class));
77
78     //@ assert Utils.is_(a,project.Entrytypes.A.class);
79
80     //@ assert a.valid();
81
82     Number ret_2 = 0L;
83     //@ assert Utils.is_nat(ret_2);
84
85     return ret_2;
86 }
87
88 public String toString() {
89
90     return "Entry{}";
91 }
92 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class A implements Record {
11     public VDMMap m;
12     //@ public instance invariant project.Entry.invChecksOn ==> inv_A(m);
13
14     public A(final VDMMap _m) {
15
16         //@ assert (V2J.isMap(_m) && (\forallall int i_1; 0 <= i_1 && i_1 < V2J.
            size(_m); Utils.is_nat(V2J.getDom(_m,i_1)) && Utils.is_(V2J.getRng(
            _m,i_1),project.Entrytypes.B.class));
17
18         m = _m != null ? Utils.copy(_m) : null;
19         //@ assert (V2J.isMap(m) && (\forallall int i_1; 0 <= i_1 && i_1 < V2J.size
            (m); Utils.is_nat(V2J.getDom(m,i_1)) && Utils.is_(V2J.getRng(m,i_1),
            project.Entrytypes.B.class));
20
21     }
22     /*@ pure @*/
23
24     public boolean equals(final Object obj) {
25
26         if (!(obj instanceof project.Entrytypes.A)) {
27             return false;
28         }
29
30         project.Entrytypes.A other = ((project.Entrytypes.A) obj);
31
32         return Utils.equals(m, other.m);
33     }
34     /*@ pure @*/

```

```

35
36 public int hashCode() {
37
38     return Utils.hashCode(m);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.A copy() {
43
44     return new project.Entrytypes.A(m);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry'A" + Utils.formatFields(m);
51 }
52 /*@ pure @*/
53
54 public VDMMap get_m() {
55
56     VDMMap ret_3 = m;
57     //@ assert project.Entry.invChecksOn ==> ((V2J.isMap(ret_3) && (\forallall
        int i_1; 0 <= i_1 && i_1 < V2J.size(ret_3); Utils.is_nat(V2J.getDom(
        ret_3,i_1)) && Utils.is_(V2J.getRng(ret_3,i_1),project.Entrytypes.B.
        class)))));
58
59     return ret_3;
60 }
61
62 public void set_m(final VDMMap _m) {
63
64     //@ assert project.Entry.invChecksOn ==> ((V2J.isMap(_m) && (\forallall int
        i_1; 0 <= i_1 && i_1 < V2J.size(_m); Utils.is_nat(V2J.getDom(_m,i_1)
        )) && Utils.is_(V2J.getRng(_m,i_1),project.Entrytypes.B.class)))));
65
66     m = _m;
67     //@ assert project.Entry.invChecksOn ==> ((V2J.isMap(m) && (\forallall int
        i_1; 0 <= i_1 && i_1 < V2J.size(m); Utils.is_nat(V2J.getDom(m,i_1))
        && Utils.is_(V2J.getRng(m,i_1),project.Entrytypes.B.class)))));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_A(final VDMMap _m) {
80
81     Boolean forAllExpResult_2 = true;
82     VDMSet set_2 = MapUtil.dom(_m);
83     for (Iterator iterator_2 = set_2.iterator(); iterator_2.hasNext() &&
        forAllExpResult_2; ) {
84         Number i = ((Number) iterator_2.next());
85         forAllExpResult_2 = Utils.equals(((project.Entrytypes.B) Utils.get(_m,
            i)).x, 2L);

```

## Appendix C. Validation of the translation rules

```

86     }
87     return forAllExpResult_2;
88 }
89 }

```

```

1  package project.Entrytypes;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class B implements Record {
11     public Number x;
12
13     public B(final Number _x) {
14
15         //@ assert Utils.is_nat(_x);
16
17         x = _x;
18         //@ assert Utils.is_nat(x);
19     }
20     /*@ pure @*/
21
22     public boolean equals(final Object obj) {
23
24         if (!(obj instanceof project.Entrytypes.B)) {
25             return false;
26         }
27
28         project.Entrytypes.B other = ((project.Entrytypes.B) obj);
29
30         return Utils.equals(x, other.x);
31     }
32     /*@ pure @*/
33
34     public int hashCode() {
35
36         return Utils.hashCode(x);
37     }
38     /*@ pure @*/
39
40     public project.Entrytypes.B copy() {
41
42         return new project.Entrytypes.B(x);
43     }
44     /*@ pure @*/
45
46     public String toString() {
47
48         return "mk_Entry`B" + Utils.formatFields(x);
49     }
50     /*@ pure @*/
51
52     public Number get_x() {
53
54         Number ret_4 = x;
55

```

## Appendix C. Validation of the translation rules

```
56      // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_4));
57
58      return ret_4;
59    }
60
61    public void set_x(final Number _x) {
62
63      // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
64
65      x = _x;
66      // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
67
68    }
69    /* @ pure @ */
70
71    public Boolean valid() {
72
73      return true;
74    }
75  }
```

```
"Before useOk"
"After useOk"
"Before useNotOk"
A.java:72: JML invariant is false on leaving method project.Entrytypes.A.valid
()
  public Boolean valid() {
                ^
A.java:12: Associated declaration
  // @ public instance invariant project.Entry.invChecksOn ==> inv_A(m);
                ^
"After useNotOk"
```

### C.59 Bool.vdmsl

```
1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12   let - = f() in skip;
13   IO`println("Done!_Expected_no_violations");
14   return 0;
15 );
16
17 functions
18
19 f : () -> bool
20 f () ==
21 let true = true
```

## Appendix C. Validation of the translation rules

```

22 in
23   true;
24
25 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Boolean ignorePattern_1 = f();
19       // @ assert Utils.is_bool(ignorePattern_1);
20
21       /* skip */
22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;
26   }
27   /* @ pure @ */
28
29   public static Boolean f() {
30
31     final Boolean boolPattern_1 = true;
32     // @ assert Utils.is_bool(boolPattern_1);
33
34     Boolean success_1 = Utils.equals(boolPattern_1, true);
35     // @ assert Utils.is_bool(success_1);
36
37     if (!(success_1)) {
38       throw new RuntimeException("Bool_pattern_match_failed");
39     }
40
41     Boolean ret_1 = true;
42     // @ assert Utils.is_bool(ret_1);
43
44     return ret_1;
45   }
46
47   public String toString() {
48
49     return "Entry{}";
50   }
51 }

```

```
"Done! Expected no violations"
```



## C.60 Real.vdmsl

---

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   let - = f() in skip;
13   IO.println("Done!_Expected_no_violations");
14   return 0;
15 );
16
17 functions
18
19 f : () -> real
20 f () ==
21 let 1.5 = 1.5
22 in
23   1.5;
24
25 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f();
19       //@ assert Utils.is_real(ignorePattern_1);
20
21       /* skip */
22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;
26   }
27   /*@ pure @*/
28
29   public static Number f() {
30
31     final Number realPattern_1 = 1.5;

```

```

32      // @ assert Utils.is_rat(realPattern_1);
33
34      Boolean success_1 = Utils.equals(realPattern_1, 1.5);
35      // @ assert Utils.is_bool(success_1);
36
37      if (!(success_1)) {
38          throw new RuntimeException("Real_pattern_match_failed");
39      }
40
41      Number ret_1 = 1.5;
42      // @ assert Utils.is_real(ret_1);
43
44      return ret_1;
45  }
46
47  public String toString() {
48
49      return "Entry{}";
50  }
51  }

```

```
"Done! Expected no violations"
```

## C.61 String.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12     let - = f() in skip;
13     IO.println("Done!_Expected_no_violations");
14     return 0;
15 );
16
17 functions
18
19 f : () -> seq of char
20 f () ==
21 let "a" = "a"
22 in
23     "a";
24
25 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;

```

```

6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         {
18             final String ignorePattern_1 = f();
19             /* @ assert Utils.is_(ignorePattern_1,String.class);
20
21             /* skip */
22         }
23
24         IO.println("Done!_Expected_no_violations");
25         return 0L;
26     }
27     /* @ pure @ */
28
29     public static String f() {
30
31         final String stringPattern_1 = "a";
32         /* @ assert Utils.is_(stringPattern_1,String.class);
33
34         Boolean success_1 = Utils.equals(stringPattern_1, "a");
35         /* @ assert Utils.is_bool(success_1);
36
37         if (!(success_1)) {
38             throw new RuntimeException("String_pattern_match_failed");
39         }
40
41         String ret_1 = "a";
42         /* @ assert Utils.is_(ret_1,String.class);
43
44         return ret_1;
45     }
46
47     public String toString() {
48
49         return "Entry{}";
50     }
51 }

```

```
"Done! Expected no violations"
```

## C.62 Quote.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions

```

## Appendix C. Validation of the translation rules

```

6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   let - = f() in skip;
13   IO.println("Done!_Expected_no_violations");
14   return 0;
15 );
16
17 functions
18
19 f : () -> <A>
20 f () ==
21 let <A> = <A>
22 in
23   <A>;
24
25 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final project.quotes.AQuote ignorePattern_1 = f();
19       // @ assert Utils.is_(ignorePattern_1,project.quotes.AQuote.class);
20
21       /* skip */
22     }
23
24     IO.println("Done!_Expected_no_violations");
25     return 0L;
26   }
27   /* @ pure @ */
28
29   public static project.quotes.AQuote f() {
30
31     final project.quotes.AQuote quotePattern_1 = project.quotes.AQuote.
32       getInstance();
33     // @ assert Utils.is_(quotePattern_1,project.quotes.AQuote.class);
34
35     Boolean success_1 = Utils.equals(quotePattern_1, project.quotes.AQuote.
36       getInstance());
37     // @ assert Utils.is_bool(success_1);
38
39     if (!(success_1)) {

```

```

38         throw new RuntimeException("Quote_pattern_match_failed");
39     }
40
41     project.quotes.AQuote ret_1 = project.quotes.AQuote.getInstance();
42     //@ assert Utils.is_(ret_1,project.quotes.AQuote.class);
43
44     return ret_1;
45 }
46
47 public String toString() {
48
49     return "Entry{}";
50 }
51 }

```

```
"Done! Expected no violations"
```

## C.63 Int.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12     let - = f(1) in skip;
13     IO`println("Done!_Expected_no_violations");
14     return 0;
15 );
16
17 functions
18
19 f : nat -> nat
20 f (1) ==
21     2;
22
23 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}

```

```

14
15  public static Object Run() {
16
17      {
18          final Number ignorePattern_1 = f(1L);
19          //@ assert Utils.is_nat(ignorePattern_1);
20
21          /* skip */
22      }
23
24      IO.println("Done!_Expected_no_violations");
25      return 0L;
26  }
27  /*@ pure @*/
28
29  public static Number f(final Number intPattern_1) {
30
31      //@ assert Utils.is_nat(intPattern_1);
32
33      Boolean success_1 = Utils.equals(intPattern_1, 1L);
34      //@ assert Utils.is_bool(success_1);
35
36      if (!(success_1)) {
37          throw new RuntimeException("Integer_pattern_match_failed");
38      }
39
40      Number ret_1 = 2L;
41      //@ assert Utils.is_nat(ret_1);
42
43      return ret_1;
44  }
45
46  public String toString() {
47
48      return "Entry{}";
49  }
50  }

```

```
"Done! Expected no violations"
```

## C.64 Nil.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12     let - = f() in skip;
13     IO.println("Done!_Expected_no_violations");
14     return 0;

```

## Appendix C. Validation of the translation rules

```

15 );
16
17 functions
18
19 f : () -> [nat]
20 f () ==
21 let nil in set {nil}
22 in
23   nil;
24
25 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     {
18       final Number ignorePattern_1 = f();
19       /* @ assert ((ignorePattern_1 == null) || Utils.is_nat(ignorePattern_1)
20         );
21
22       /* skip */
23     }
24
25     IO.println("Done!_Expected_no_violations");
26     return 0L;
27   }
28   /* @ pure @ */
29
30   public static Number f() {
31
32     Object letBeStExp_1 = null;
33     Object nullPattern_1 = null;
34
35     Boolean success_1 = false;
36     /* @ assert Utils.is_bool(success_1);
37
38     VDMSet set_1 = SetUtil.set(null);
39     /* @ assert (V2J.isSet(set_1) && (\forallall int i; 0 <= i && i < V2J.size(
40       set_1); true));
41
42     for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() && !(
43       success_1); ) {
44       nullPattern_1 = ((Object) iterator_1.next());
45       success_1 = Utils.equals(nullPattern_1, null);
46       /* @ assert Utils.is_bool(success_1);
47
48       if (!(success_1)) {

```

```

46         continue;
47     }
48
49     success_1 = true;
50     //@ assert Utils.is_bool(success_1);
51
52 }
53 if (!(success_1)) {
54     throw new RuntimeException("Let_Be_St_found_no_applicable_bindings");
55 }
56
57 letBeStExp_1 = null;
58 Number ret_1 = ((Number) letBeStExp_1);
59 //@ assert ((ret_1 == null) || Utils.is_nat(ret_1));
60
61 return ret_1;
62 }
63
64 public String toString() {
65
66     return "Entry{}";
67 }
68 }

```

```
"Done! Expected no violations"
```

## C.65 Char.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12     let - = f() in skip;
13     IO.println("Done!_Expected_no_violations");
14     return 0;
15 );
16
17 functions
18
19 f : () -> char
20 f () ==
21 let 'a' in set {'a'}
22 in
23     'a';
24
25 end Entry

```

```

1 package project;
2

```



## Appendix C. Validation of the translation rules

```

3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         {
18             final Character ignorePattern_1 = f();
19             /* @ assert Utils.is_char(ignorePattern_1);
20
21             /* skip */
22         }
23
24         IO.println("Done!_Expected_no_violations");
25         return 0L;
26     }
27     /* @ pure @ */
28
29     public static Character f() {
30
31         Character letBeStExp_1 = null;
32         Character charPattern_1 = null;
33
34         Boolean success_1 = false;
35         /* @ assert Utils.is_bool(success_1);
36
37         VDMSet set_1 = SetUtil.set('a');
38         /* @ assert (V2J.isSet(set_1) && (\forall int i; 0 <= i && i < V2J.size(
39             set_1); Utils.is_char(V2J.get(set_1,i)))));
40
41         for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() && !(
42             success_1); ) {
43             charPattern_1 = ((Character) iterator_1.next());
44             /* @ assert Utils.is_char(charPattern_1);
45
46             success_1 = Utils.equals(charPattern_1, 'a');
47             /* @ assert Utils.is_bool(success_1);
48
49             if (!(success_1)) {
50                 continue;
51             }
52
53             success_1 = true;
54             /* @ assert Utils.is_bool(success_1);
55
56         }
57         if (!(success_1)) {
58             throw new RuntimeException("Let_Be_St_found_no_applicable_bindings");
59         }
60
61         letBeStExp_1 = 'a';
62         /* @ assert Utils.is_char(letBeStExp_1);

```

```

61
62     Character ret_1 = letBeStExp_1;
63     //@ assert Utils.is_char(ret_1);
64
65     return ret_1;
66 }
67
68 public String toString() {
69
70     return "Entry{}";
71 }
72 }

```

```
"Done! Expected no violations"
```

## C.66 StateInitViolatesInv.vdmsl

```

1 module Entry
2
3 exports all
4 definitions
5
6 state St of
7   x : int
8 init s == s = mk_St(-5)
9 inv s == s.x > 0
10 end
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16   return 1;
17
18 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class St implements Record {
11   public Number x;
12   //@ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
13
14   public St(final Number _x) {
15
16     //@ assert Utils.is_int(_x);
17
18     x = _x;
19     //@ assert Utils.is_int(x);
20

```

## Appendix C. Validation of the translation rules

```
21 }
22 /*@ pure @*/
23
24 public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.St)) {
27         return false;
28     }
29
30     project.Entrytypes.St other = ((project.Entrytypes.St) obj);
31
32     return Utils.equals(x, other.x);
33 }
34 /*@ pure @*/
35
36 public int hashCode() {
37
38     return Utils.hashCode(x);
39 }
40 /*@ pure @*/
41
42 public project.Entrytypes.St copy() {
43
44     return new project.Entrytypes.St(x);
45 }
46 /*@ pure @*/
47
48 public String toString() {
49
50     return "mk_Entry`St" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_1 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_1));
58
59     return ret_1;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_St(final Number _x) {
80
```

```

81     return _x.longValue() > 0L;
82 }
83 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ spec_public @*/
12
13     private static project.Entrytypes.St St = new project.Entrytypes.St(-5L);
14     /*@ public ghost static boolean invChecksOn = true; @*/
15
16     private Entry() {}
17
18     public static Object Run() {
19
20         return 1L;
21     }
22
23     public String toString() {
24
25         return "Entry{" + "St_:=_" + Utils.toString(St) + "}";
26     }
27 }

```

```

St.java:12: JML invariant is false
    //@ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
                                   ^

```

## C.67 RecTypeDefInv.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  types
8
9  Rec ::
10     x : int
11     y : int
12  inv mk_Rec(x,y) == x > 0 and y > 0;
13
14  operations
15
16  Run : () ==> ?
17  Run () ==
18  (

```

## Appendix C. Validation of the translation rules

```

19   recInvOk();
20   IO.println("Before_breaking_record_invariant");
21   recInvBreak();
22   IO.println("After_breaking_record_invariant");
23   return 0;
24 );
25
26 recInvOk : () ==> ()
27 recInvOk () ==
28 let - = mk_Rec(1,2)
29 in
30   skip;
31
32 recInvBreak : () ==> ()
33 recInvBreak () ==
34 let - = mk_Rec(1,-2)
35 in
36   skip;
37
38 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     recInvOk();
18     IO.println("Before_breaking_record_invariant");
19     recInvBreak();
20     IO.println("After_breaking_record_invariant");
21     return 0L;
22   }
23
24   public static void recInvOk() {
25
26     final project.Entrytypes.Rec ignorePattern_1 = new project.Entrytypes.
27       Rec(1L, 2L);
28     // @ assert Utils.is_(ignorePattern_1, project.Entrytypes.Rec.class);
29
30     /* skip */
31   }
32
33   public static void recInvBreak() {
34
35     final project.Entrytypes.Rec ignorePattern_2 = new project.Entrytypes.
36       Rec(1L, -2L);
37     // @ assert Utils.is_(ignorePattern_2, project.Entrytypes.Rec.class);
38
39   }
40 }

```

## Appendix C. Validation of the translation rules

```

38     /* skip */
39
40 }
41
42 public String toString() {
43
44     return "Entry{}";
45 }
46 }

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Rec implements Record {
11     public Number x;
12     public Number y;
13     // @ public instance invariant project.Entry.invChecksOn ==> inv_Rec(x,y);
14
15     public Rec(final Number _x, final Number _y) {
16
17         // @ assert Utils.is_int(_x);
18
19         // @ assert Utils.is_int(_y);
20
21         x = _x;
22         // @ assert Utils.is_int(x);
23
24         y = _y;
25         // @ assert Utils.is_int(y);
26
27     }
28     /* @ pure @ */
29
30     public boolean equals(final Object obj) {
31
32         if (!(obj instanceof project.Entrytypes.Rec)) {
33             return false;
34         }
35
36         project.Entrytypes.Rec other = ((project.Entrytypes.Rec) obj);
37
38         return (Utils.equals(x, other.x)) && (Utils.equals(y, other.y));
39     }
40     /* @ pure @ */
41
42     public int hashCode() {
43
44         return Utils.hashCode(x, y);
45     }
46     /* @ pure @ */
47
48     public project.Entrytypes.Rec copy() {
49
50         return new project.Entrytypes.Rec(x, y);

```

```

51     }
52     /*@ pure @*/
53
54     public String toString() {
55
56         return "mk_Entry`Rec" + Utils.formatFields(x, y);
57     }
58     /*@ pure @*/
59
60     public Number get_x() {
61
62         Number ret_1 = x;
63         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_1));
64
65         return ret_1;
66     }
67
68     public void set_x(final Number _x) {
69
70         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
71
72         x = _x;
73         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
74
75     }
76     /*@ pure @*/
77
78     public Number get_y() {
79
80         Number ret_2 = y;
81         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_2));
82
83         return ret_2;
84     }
85
86     public void set_y(final Number _y) {
87
88         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(_y));
89
90         y = _y;
91         /*@ assert project.Entry.invChecksOn ==> (Utils.is_int(y));
92
93     }
94     /*@ pure @*/
95
96     public Boolean valid() {
97
98         return true;
99     }
100     /*@ pure @*/
101     /*@ helper @*/
102
103     public static Boolean inv_Rec(final Number _x, final Number _y) {
104
105         Boolean success_2 = true;
106         Number x = null;
107         Number y = null;
108         x = _x;
109         y = _y;
110

```

```

111     if (!(success_2)) {
112         throw new RuntimeException("Record_pattern_match_failed");
113     }
114
115     Boolean andResult_2 = false;
116
117     if (x.longValue() > 0L) {
118         if (y.longValue() > 0L) {
119             andResult_2 = true;
120         }
121     }
122
123     return andResult_2;
124 }
125 }

```

```

"Before breaking record invariant"
Rec.java:15: JML invariant is false on leaving method project.Entrytypes.Rec.
    Rec(java.lang.Number,java.lang.Number)
    public Rec(final Number _x, final Number _y) {
        ^
Rec.java:13: Associated declaration
    //@ public instance invariant project.Entry.invChecksOn ==> inv_Rec(x,y);
        ^
"After breaking record invariant"

```

## C.68 StateInv.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  state St of
8      x : int
9  init s == s = mk_St(5)
10 inv s == s.x > 0
11 end
12
13 operations
14
15 Run : () ==> ?
16 Run () ==
17 (
18     opAtomic();
19     IO`println("Before_breaking_state_invariant");
20     op();
21     IO`println("After_breaking_state_invariant");
22     return x;
23 );
24
25 opAtomic : () ==> ()
26 opAtomic () ==
27 atomic
28 (

```



## Appendix C. Validation of the translation rules

```

29   x := -1;
30   x := 1;
31 );
32
33 op : () ==> ()
34 op () ==
35 (
36   x := -10;
37   x := 10;
38 );
39
40 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class St implements Record {
11   public Number x;
12   // @ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
13
14   public St(final Number _x) {
15
16     // @ assert Utils.is_int(_x);
17
18     x = _x;
19     // @ assert Utils.is_int(x);
20
21   }
22   /* @ pure @ */
23
24   public boolean equals(final Object obj) {
25
26     if (!(obj instanceof project.Entrytypes.St)) {
27       return false;
28     }
29
30     project.Entrytypes.St other = ((project.Entrytypes.St) obj);
31
32     return Utils.equals(x, other.x);
33   }
34   /* @ pure @ */
35
36   public int hashCode() {
37
38     return Utils.hashCode(x);
39   }
40   /* @ pure @ */
41
42   public project.Entrytypes.St copy() {
43
44     return new project.Entrytypes.St(x);
45   }
46   /* @ pure @ */
47

```

## Appendix C. Validation of the translation rules

```

48 public String toString() {
49
50     return "mk_Entry`St" + Utils.formatFields(x);
51 }
52 /*@ pure @*/
53
54 public Number get_x() {
55
56     Number ret_1 = x;
57     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_1));
58
59     return ret_1;
60 }
61
62 public void set_x(final Number _x) {
63
64     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
65
66     x = _x;
67     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
68
69 }
70 /*@ pure @*/
71
72 public Boolean valid() {
73
74     return true;
75 }
76 /*@ pure @*/
77 /*@ helper @*/
78
79 public static Boolean inv_St(final Number _x) {
80
81     return _x.longValue() > 0L;
82 }
83 }

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ spec_public @*/
12
13     private static project.Entrytypes.St St = new project.Entrytypes.St(5L);
14     /*@ public ghost static boolean invChecksOn = true; @*/
15
16     private Entry() {}
17
18     public static Object Run() {
19
20         opAtomic();
21         IO.println("Before_breaking_state_invariant");
22         op();
23         IO.println("After_breaking_state_invariant");

```

## Appendix C. Validation of the translation rules

```

24     return St.get_x();
25 }
26
27 public static void opAtomic() {
28
29     Number atomicTmp_1 = -1L;
30     //@ assert Utils.is_int(atomicTmp_1);
31
32     Number atomicTmp_2 = 1L;
33     //@ assert Utils.is_int(atomicTmp_2);
34
35     {
36         /* Start of atomic statement */
37         //@ set invChecksOn = false;
38
39         //@ assert St != null;
40
41         St.set_x(atomicTmp_1);
42
43         //@ assert St != null;
44
45         St.set_x(atomicTmp_2);
46
47         //@ set invChecksOn = true;
48
49         //@ assert St.valid();
50
51     } /* End of atomic statement */
52 }
53
54 public static void op() {
55
56     //@ assert St != null;
57
58     St.set_x(-10L);
59
60     //@ assert St != null;
61
62     St.set_x(10L);
63 }
64
65 public String toString() {
66
67     return "Entry{" + "St_:=_" + Utils.toString(St) + "}";
68 }
69 }

```

"Before breaking state invariant"

St.java:62: JML invariant is false on leaving method project.Entrytypes.St.  
set\_x(java.lang.Number)

```
public void set_x(final Number _x) {
```

^

St.java:12: Associated declaration

```
//@ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
```

^

Entry.java:62: JML invariant is false on entering method project.Entrytypes.St.  
.set\_x(java.lang.Number) from project.Entry.op()

```
St.set_x(10L);
```

^

St.java:12: Associated declaration

```
//@ public instance invariant project.Entry.invChecksOn ==> inv_St(x);
      ^
"After breaking state invariant"
```

## C.69 PostCond.vdmsl

```
1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 state St of
8   x : nat
9   init s == s = mk_St(0)
10 end
11
12 functions
13
14 f : nat -> nat
15 f (a) ==
16   if a mod 2 = 0 then a + 2 else a + 1
17 post RESULT mod 2 = 0;
18
19 operations
20
21 Run : () ==> ?
22 Run () ==
23   let - = opRet(1),
24       - = f(3)
25 in
26   (
27     opVoid();
28     IO`println("Before_breaking_post_condition");
29     let - = opRet(4) in skip;
30     IO`println("After_breaking_post_condition");
31     return 0;
32   );
33
34 opVoid : () ==> ()
35 opVoid () ==
36   x := x + 1
37 post x = x~+1;
38
39 opRet : nat ==> nat
40 opRet (a) ==
41   (
42     x := x + 1;
43     return x;
44   )
45 post x = x~+1 and RESULT = a;
46
47 end Entry
```

```
1 package project.Entrytypes;
2
```

## Appendix C. Validation of the translation rules

```

3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class St implements Record {
11     public Number x;
12
13     public St(final Number _x) {
14
15         // @ assert Utils.is_nat(_x);
16
17         x = _x;
18         // @ assert Utils.is_nat(x);
19     }
20     /* @ pure @ */
21
22     public boolean equals(final Object obj) {
23
24         if (!(obj instanceof project.Entrytypes.St)) {
25             return false;
26         }
27
28         project.Entrytypes.St other = ((project.Entrytypes.St) obj);
29
30         return Utils.equals(x, other.x);
31     }
32     /* @ pure @ */
33
34     public int hashCode() {
35
36         return Utils.hashCode(x);
37     }
38     /* @ pure @ */
39
40     public project.Entrytypes.St copy() {
41
42         return new project.Entrytypes.St(x);
43     }
44     /* @ pure @ */
45
46     public String toString() {
47
48         return "mk_Entry`St" + Utils.formatFields(x);
49     }
50     /* @ pure @ */
51
52     public Number get_x() {
53
54         Number ret_7 = x;
55         // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_7));
56
57         return ret_7;
58     }
59
60     public void set_x(final Number _x) {
61
62

```

## Appendix C. Validation of the translation rules

```

63     // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
64
65     x = _x;
66     // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
67
68 }
69 /* @ pure @ */
70
71 public Boolean valid() {
72
73     return true;
74 }
75 }

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  // @ nullable_by_default
9
10 final public class Entry {
11     /* @ spec_public @ */
12
13     private static project.Entrytypes.St St = new project.Entrytypes.St(0L);
14     /* @ public ghost static boolean invChecksOn = true; @ */
15
16     private Entry() {}
17
18     public static Object Run() {
19
20         final Number ignorePattern_1 = opRet(1L);
21         // @ assert Utils.is_nat(ignorePattern_1);
22
23         final Number ignorePattern_2 = f(3L);
24         // @ assert Utils.is_nat(ignorePattern_2);
25
26         {
27             opVoid();
28             IO.println("Before_breaking_post_condition");
29             {
30                 final Number ignorePattern_3 = opRet(4L);
31                 // @ assert Utils.is_nat(ignorePattern_3);
32
33                 /* skip */
34             }
35
36             IO.println("After_breaking_post_condition");
37             return 0L;
38         }
39     }
40     // @ ensures post_opVoid(\old(St.copy()), St);
41
42     public static void opVoid() {
43
44         // @ assert St != null;
45
46         St.set_x(St.get_x().longValue() + 1L);

```

## Appendix C. Validation of the translation rules

```

47     }
48     //@ ensures post_opRet(a, \result, \old(St.copy()), St);
49
50     public static Number opRet(final Number a) {
51
52         //@ assert Utils.is_nat(a);
53
54         //@ assert St != null;
55
56         St.set_x(St.get_x().longValue() + 1L);
57
58         Number ret_1 = St.get_x();
59         //@ assert Utils.is_nat(ret_1);
60
61         return ret_1;
62     }
63     //@ ensures post_f(a, \result);
64     /*@ pure @*/
65
66     public static Number f(final Number a) {
67
68         //@ assert Utils.is_nat(a);
69
70         if (Utils.equals(Utils.mod(a.longValue(), 2L), 0L)) {
71             Number ret_2 = a.longValue() + 2L;
72             //@ assert Utils.is_nat(ret_2);
73
74             return ret_2;
75
76         } else {
77             Number ret_3 = a.longValue() + 1L;
78             //@ assert Utils.is_nat(ret_3);
79
80             return ret_3;
81         }
82     }
83     /*@ pure @*/
84
85     public static Boolean post_opVoid(
86         final project.Entrytypes.St _St, final project.Entrytypes.St St) {
87
88         //@ assert Utils.is_(_St, project.Entrytypes.St.class);
89
90         //@ assert Utils.is_(St, project.Entrytypes.St.class);
91
92         Boolean ret_4 = Utils.equals(St.get_x(), _St.get_x().longValue() + 1L);
93         //@ assert Utils.is_bool(ret_4);
94
95         return ret_4;
96     }
97     /*@ pure @*/
98
99     public static Boolean post_opRet(
100         final Number a,
101         final Number RESULT,
102         final project.Entrytypes.St _St,
103         final project.Entrytypes.St St) {
104
105         //@ assert Utils.is_nat(a);
106

```

## Appendix C. Validation of the translation rules

```

107  // @ assert Utils.is_nat (RESULT);
108
109  // @ assert Utils.is_(St, project.Entrytypes.St.class);
110
111  // @ assert Utils.is_(St, project.Entrytypes.St.class);
112
113  Boolean andResult_1 = false;
114  // @ assert Utils.is_bool (andResult_1);
115
116  if (Utils.equals(St.get_x(), _St.get_x().longValue() + 1L)) {
117    if (Utils.equals(RESULT, a)) {
118      andResult_1 = true;
119      // @ assert Utils.is_bool (andResult_1);
120
121    }
122  }
123
124  Boolean ret_5 = andResult_1;
125  // @ assert Utils.is_bool (ret_5);
126
127  return ret_5;
128 }
129 /* @ pure @ */
130
131 public static Boolean post_f(final Number a, final Number RESULT) {
132
133   // @ assert Utils.is_nat (a);
134
135   // @ assert Utils.is_nat (RESULT);
136
137   Boolean ret_6 = Utils.equals(Utils.mod(RESULT.longValue(), 2L), 0L);
138   // @ assert Utils.is_bool (ret_6);
139
140   return ret_6;
141 }
142
143 public String toString() {
144
145   return "Entry{" + "St_:=_" + Utils.toString(St) + "}";
146 }
147 }

```

```

"Before breaking post condition"
Entry.java:50: JML postcondition is false
  public static Number opRet(final Number a) {
    ^
Entry.java:48: Associated declaration
  // @ ensures post_opRet(a, \result, \old(St.copy()), St);
    ^
"After breaking post condition"

```

### C.70 PreCond.vdmsl

```

1 module Entry
2
3 exports all

```



```

4 imports from IO all
5 definitions
6
7 state St of
8 x : nat
9 init s == s = mk_St(5)
10 end
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 let - = opRet(1)
17 in
18 (
19   opVoid(2);
20   IO`println("Before_breaking_pre_condition");
21   let - = id(-1) in skip;
22   IO`println("After_breaking_pre_condition");
23   return 0;
24 );
25
26 opRet : nat ==> nat
27 opRet (a) ==
28 (
29   x := a + 1;
30   return x;
31 )
32 pre x > 0;
33
34 opVoid : nat ==> ()
35 opVoid (a) ==
36   x := a + 1
37 pre St.x > 0;
38
39 functions
40
41 id : int -> int
42 id (a) == a
43 pre a > 0;
44
45 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class St implements Record {
11   public Number x;
12
13   public St(final Number _x) {
14
15     //@ assert Utils.is_nat(_x);
16
17     x = _x;

```

## Appendix C. Validation of the translation rules

```

18     // @ assert Utils.is_nat(x);
19
20 }
21 /* @ pure @ */
22
23 public boolean equals(final Object obj) {
24
25     if (!(obj instanceof project.Entrytypes.St)) {
26         return false;
27     }
28
29     project.Entrytypes.St other = ((project.Entrytypes.St) obj);
30
31     return Utils.equals(x, other.x);
32 }
33 /* @ pure @ */
34
35 public int hashCode() {
36
37     return Utils.hashCode(x);
38 }
39 /* @ pure @ */
40
41 public project.Entrytypes.St copy() {
42
43     return new project.Entrytypes.St(x);
44 }
45 /* @ pure @ */
46
47 public String toString() {
48
49     return "mk_Entry`St" + Utils.formatFields(x);
50 }
51 /* @ pure @ */
52
53 public Number get_x() {
54
55     Number ret_6 = x;
56     // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(ret_6));
57
58     return ret_6;
59 }
60
61 public void set_x(final Number _x) {
62
63     // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(_x));
64
65     x = _x;
66     // @ assert project.Entry.invChecksOn ==> (Utils.is_nat(x));
67
68 }
69 /* @ pure @ */
70
71 public Boolean valid() {
72
73     return true;
74 }
75 }

```

```

1 package project;

```

```

2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ spec_public @ */
12
13     private static project.Entrytypes.St St = new project.Entrytypes.St(5L);
14     /* @ public ghost static boolean invChecksOn = true; @ */
15
16     private Entry() {}
17
18     public static Object Run() {
19
20         final Number ignorePattern_1 = opRet(1L);
21         /* @ assert Utils.is_nat(ignorePattern_1);
22
23         {
24             opVoid(2L);
25             IO.println("Before_breaking_pre_condition");
26             {
27                 final Number ignorePattern_2 = id(-1L);
28                 /* @ assert Utils.is_int(ignorePattern_2);
29
30                 /* skip */
31             }
32
33             IO.println("After_breaking_pre_condition");
34             return 0L;
35         }
36     }
37     /* @ requires pre_opRet(a, St);
38
39     public static Number opRet(final Number a) {
40
41         /* @ assert Utils.is_nat(a);
42
43         /* @ assert St != null;
44
45         St.set_x(a.longValue() + 1L);
46
47         Number ret_1 = St.get_x();
48         /* @ assert Utils.is_nat(ret_1);
49
50         return ret_1;
51     }
52     /* @ requires pre_opVoid(a, St);
53
54     public static void opVoid(final Number a) {
55
56         /* @ assert Utils.is_nat(a);
57
58         /* @ assert St != null;
59
60         St.set_x(a.longValue() + 1L);
61     }

```

## Appendix C. Validation of the translation rules

```

62  //@ requires pre_id(a);
63  /*@ pure @*/
64
65  public static Number id(final Number a) {
66
67      //@ assert Utils.is_int(a);
68
69      Number ret_2 = a;
70      //@ assert Utils.is_int(ret_2);
71
72      return ret_2;
73  }
74  /*@ pure @*/
75
76  public static Boolean pre_opRet(final Number a, final project.Entrytypes.
    St St) {
77
78      //@ assert Utils.is_nat(a);
79
80      //@ assert Utils.is_(St,project.Entrytypes.St.class);
81
82      Boolean ret_3 = St.get_x().longValue() > 0L;
83      //@ assert Utils.is_bool(ret_3);
84
85      return ret_3;
86  }
87  /*@ pure @*/
88
89  public static Boolean pre_opVoid(final Number a, final project.Entrytypes.
    St St) {
90
91      //@ assert Utils.is_nat(a);
92
93      //@ assert Utils.is_(St,project.Entrytypes.St.class);
94
95      Boolean ret_4 = St.get_x().longValue() > 0L;
96      //@ assert Utils.is_bool(ret_4);
97
98      return ret_4;
99  }
100 /*@ pure @*/
101
102 public static Boolean pre_id(final Number a) {
103
104     //@ assert Utils.is_int(a);
105
106     Boolean ret_5 = a.longValue() > 0L;
107     //@ assert Utils.is_bool(ret_5);
108
109     return ret_5;
110 }
111
112 public String toString() {
113
114     return "Entry{" + "St_:=_" + Utils.toString(St) + "}";
115 }
116 }

```

"Before breaking pre condition"  
Entry.java:27: JML precondition is false

```

        final Number ignorePattern_2 = id(-1L);
                                   ^
Entry.java:62: Associated declaration
    //@ requires pre_id(a);
        ^
"After breaking pre condition"

```

## C.71 TupleSizeMismatch.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : nat * nat * char * bool = Tup4() in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : nat * nat * char * bool = Tup3() in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 Tup3 : () -> (nat * char * bool) | (nat * nat * char * bool)
24 Tup3 () == mk_(1, 'a', true);
25
26 Tup4 : () -> (nat * char * bool) | (nat * nat * char * bool)
27 Tup4 () == mk_(1, 2, 'b', false);
28
29 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");

```

## Appendix C. Validation of the translation rules

```

18  {
19      final Tuple ignorePattern_1 = ((Tuple) Tup4());
20      //@ assert (V2J.isTup(ignorePattern_1,4) && Utils.is_nat(V2J.field(
        ignorePattern_1,0)) && Utils.is_nat(V2J.field(ignorePattern_1,1))
        && Utils.is_char(V2J.field(ignorePattern_1,2)) && Utils.is_bool(
        V2J.field(ignorePattern_1,3)));

21
22      /* skip */
23  }
24
25  IO.println("After_legal_use");
26  IO.println("Before_illegal_use");
27  {
28      final Tuple ignorePattern_2 = ((Tuple) Tup3());
29      //@ assert (V2J.isTup(ignorePattern_2,4) && Utils.is_nat(V2J.field(
        ignorePattern_2,0)) && Utils.is_nat(V2J.field(ignorePattern_2,1))
        && Utils.is_char(V2J.field(ignorePattern_2,2)) && Utils.is_bool(
        V2J.field(ignorePattern_2,3)));

30
31      /* skip */
32  }
33
34  IO.println("After_illegal_use");
35  return 0L;
36  }
37  /*@ pure @*/
38
39  public static Object Tup3() {
40
41      Object ret_1 = Tuple.mk_(1L, 'a', true);
42      //@ assert ((V2J.isTup(ret_1,3) && Utils.is_nat(V2J.field(ret_1,0)) &&
        Utils.is_char(V2J.field(ret_1,1)) && Utils.is_bool(V2J.field(ret_1
        ,2))) || (V2J.isTup(ret_1,4) && Utils.is_nat(V2J.field(ret_1,0)) &&
        Utils.is_nat(V2J.field(ret_1,1)) && Utils.is_char(V2J.field(ret_1,2)
        ) && Utils.is_bool(V2J.field(ret_1,3)));

43
44      return Utils.copy(ret_1);
45  }
46  /*@ pure @*/
47
48  public static Object Tup4() {
49
50      Object ret_2 = Tuple.mk_(1L, 2L, 'b', false);
51      //@ assert ((V2J.isTup(ret_2,3) && Utils.is_nat(V2J.field(ret_2,0)) &&
        Utils.is_char(V2J.field(ret_2,1)) && Utils.is_bool(V2J.field(ret_2
        ,2))) || (V2J.isTup(ret_2,4) && Utils.is_nat(V2J.field(ret_2,0)) &&
        Utils.is_nat(V2J.field(ret_2,1)) && Utils.is_char(V2J.field(ret_2,2)
        ) && Utils.is_bool(V2J.field(ret_2,3)));

52
53      return Utils.copy(ret_2);
54  }
55
56  public String toString() {
57
58      return "Entry{}";
59  }
60  }

```

```

"Before legal use"
"After legal use"

```

```

"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isTup(ignorePattern_2,4) && Utils.is_nat(V2J.field(
        ignorePattern_2,0)) && Utils.is_nat(V2J.field(ignorePattern_2,1)) &&
        Utils.is_char(V2J.field(ignorePattern_2,2)) && Utils.is_bool(V2J.
            field(ignorePattern_2,3)));
        ^
"After illegal use"

```

## C.72 NatBoolTupNil.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : nat * bool = mk_(1,true) in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : nat * bool = TupNil() in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 TupNil : () -> [nat1 * bool]
24 TupNil () == nil;
25
26 TupVal : () -> [nat1 * bool]
27 TupVal () == mk_(1,false);
28
29 end Entry

```

```

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {

```

## Appendix C. Validation of the translation rules

```

16
17     IO.println("Before_legal_use");
18     {
19         final Tuple ignorePattern_1 = Tuple.mk_(1L, true);
20         //@ assert (V2J.isTup(ignorePattern_1,2) && Utils.is_nat(V2J.field(
            ignorePattern_1,0)) && Utils.is_bool(V2J.field(ignorePattern_1,1))
            );
21
22         /* skip */
23     }
24
25     IO.println("After_legal_use");
26     IO.println("Before_illegal_use");
27     {
28         final Tuple ignorePattern_2 = TupNil();
29         //@ assert (V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
            ignorePattern_2,0)) && Utils.is_bool(V2J.field(ignorePattern_2,1))
            );
30
31         /* skip */
32     }
33
34     IO.println("After_illegal_use");
35     return 0L;
36 }
37 /*@ pure @*/
38
39 public static Tuple TupNil() {
40
41     Tuple ret_1 = null;
42     //@ assert ((ret_1 == null) || (V2J.isTup(ret_1,2) && Utils.is_nat1(V2J.
        field(ret_1,0)) && Utils.is_bool(V2J.field(ret_1,1)))));
43
44     return Utils.copy(ret_1);
45 }
46 /*@ pure @*/
47
48 public static Tuple TupVal() {
49
50     Tuple ret_2 = Tuple.mk_(1L, false);
51     //@ assert ((ret_2 == null) || (V2J.isTup(ret_2,2) && Utils.is_nat1(V2J.
        field(ret_2,0)) && Utils.is_bool(V2J.field(ret_2,1)))));
52
53     return Utils.copy(ret_2);
54 }
55
56 public String toString() {
57
58     return "Entry{}";
59 }
60 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
        ignorePattern_2,0)) && Utils.is_bool(V2J.field(ignorePattern_2,1)));
        ^
"After illegal use"

```



## C.73 NatBooolBasedNamedTypeInv.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 TrueEven = nat * bool
10 inv te == te.#1 > 1000 and te.#2;
11
12 operations
13
14 Run : () ==> ?
15 Run () ==
16 (
17   IO.println("Before_legal_use");
18   let - : TrueEven = mk_(1001,true) in skip;
19   IO.println("After_legal_use");
20   IO.println("Before_illegal_uses");
21   let - : TrueEven = mk_(1000,true) in skip;
22   let - : TrueEven = mk_(1001,false) in skip;
23   IO.println("After_illegal_uses");
24   return 0;
25 );
26
27 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       final Tuple ignorePattern_1 = Tuple.mk_(1001L, true);
20       /* @ assert ((V2J.isTup(ignorePattern_1,2) && Utils.is_nat(V2J.field(
21         ignorePattern_1,0)) && Utils.is_bool(V2J.field(ignorePattern_1,1))
22         ) && inv_Entry_TrueEven(ignorePattern_1));
23
24       /* skip */
25     }
26   }
27 }

```

## Appendix C. Validation of the translation rules

```

24
25     IO.println("After_legal_use");
26     IO.println("Before_illegal_uses");
27     {
28         final Tuple ignorePattern_2 = Tuple.mk_(1000L, true);
29         //@ assert ((V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
            ignorePattern_2,0)) && Utils.is_bool(V2J.field(ignorePattern_2,1))
            ) && inv_Entry_TrueEven(ignorePattern_2));
30
31         /* skip */
32     }
33
34     {
35         final Tuple ignorePattern_3 = Tuple.mk_(1001L, false);
36         //@ assert ((V2J.isTup(ignorePattern_3,2) && Utils.is_nat(V2J.field(
            ignorePattern_3,0)) && Utils.is_bool(V2J.field(ignorePattern_3,1))
            ) && inv_Entry_TrueEven(ignorePattern_3));
37
38         /* skip */
39     }
40
41     IO.println("After_illegal_uses");
42     return 0L;
43 }
44
45 public String toString() {
46
47     return "Entry{}";
48 }
49
50 /*@ pure @*/
51 /*@ helper @*/
52
53 public static Boolean inv_Entry_TrueEven(final Object check_te) {
54
55     Tuple te = ((Tuple) check_te);
56
57     Boolean andResult_1 = false;
58
59     if (((Number) te.get(0)).longValue() > 1000L) {
60         if (((Boolean) te.get(1))) {
61             andResult_1 = true;
62         }
63     }
64
65     return andResult_1;
66 }
67 }

```

```

"Before legal use"
"After legal use"
"Before illegal uses"
Entry.java:29: JML assertion is false
    //@ assert ((V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
        ignorePattern_2,0)) && Utils.is_bool(V2J.field(ignorePattern_2,1))
        && inv_Entry_TrueEven(ignorePattern_2));
    ^
Entry.java:36: JML assertion is false
    //@ assert ((V2J.isTup(ignorePattern_3,2) && Utils.is_nat(V2J.field(
        ignorePattern_3,0)) && Utils.is_bool(V2J.field(ignorePattern_3,1))

```

```

    && inv_Entry_TrueEven(ignorePattern_3));
    ^
    "After illegal uses"

```

## C.74 NatBoolNegField.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : nat * bool = mk_(1,true) in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : nat * bool = mk_(negInt(),true) in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 negInt : () -> int
24 negInt () == -1;
25
26 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       final Tuple ignorePattern_1 = Tuple.mk_(1L, true);
20       //@ assert (V2J.isTup(ignorePattern_1,2) && Utils.is_nat(V2J.field(
21         ignorePattern_1,0)) && Utils.is_bool(V2J.field(ignorePattern_1,1))

```

```

22     /* skip */
23 }
24
25 IO.println("After_legal_use");
26 IO.println("Before_illegal_use");
27 {
28     final Tuple ignorePattern_2 = Tuple.mk_(negInt(), true);
29     //@ assert (V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
        ignorePattern_2,0)) && Utils.is_bool(V2J.field(ignorePattern_2,1))
        );
30
31     /* skip */
32 }
33
34 IO.println("After_illegal_use");
35 return 0L;
36 }
37 /*@ pure @*/
38
39 public static Number negInt() {
40
41     Number ret_1 = -1L;
42     //@ assert Utils.is_int(ret_1);
43
44     return ret_1;
45 }
46
47 public String toString() {
48
49     return "Entry{}";
50 }
51 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isTup(ignorePattern_2,2) && Utils.is_nat(V2J.field(
        ignorePattern_2,0)) && Utils.is_bool(V2J.field(ignorePattern_2,1)));
        ^
"After illegal use"

```

## C.75 ReturnNonInjMapWhereInjMapRequired.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 types
8
9 V2 ::
10 x : int
11 y : int;
12

```

## Appendix C. Validation of the translation rules

```

13 operations
14
15 Run : () ==> ?
16 Run () ==
17 (
18   IO`println("Before_legal_use");
19   let - : inmap nat to V2 = consInjMap() in skip;
20   IO`println("After_legal_use");
21   IO`println("Before_illegal_use");
22   let - : inmap nat to V2 = consInjMapErr() in skip;
23   IO`println("After_illegal_use");
24   return 0;
25 );
26
27 functions
28
29 consInjMap : () -> inmap nat to V2
30 consInjMap () ==
31   {1 |-> mk_V2(1,2), 2 |-> mk_V2(2,1)};
32
33 consInjMapErr : () -> inmap nat to V2
34 consInjMapErr () ==
35   {1 |-> mk_V2(1,2), 2 |-> mk_V2(2,1), 3 |-> mk_V2(1,2)};
36
37 end Entry

```

```

1 package project.Entrytypes;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class V2 implements Record {
11   public Number x;
12   public Number y;
13
14   public V2(final Number _x, final Number _y) {
15
16     // @ assert Utils.is_int(_x);
17
18     // @ assert Utils.is_int(_y);
19
20     x = _x;
21     // @ assert Utils.is_int(x);
22
23     y = _y;
24     // @ assert Utils.is_int(y);
25
26   }
27   /* @ pure @ */
28
29   public boolean equals(final Object obj) {
30
31     if (!(obj instanceof project.Entrytypes.V2)) {
32       return false;
33     }
34

```

## Appendix C. Validation of the translation rules

```
35     project.Entrytypes.V2 other = ((project.Entrytypes.V2) obj);
36
37     return (Utils.equals(x, other.x)) && (Utils.equals(y, other.y));
38 }
39 /*@ pure @*/
40
41 public int hashCode() {
42
43     return Utils.hashCode(x, y);
44 }
45 /*@ pure @*/
46
47 public project.Entrytypes.V2 copy() {
48
49     return new project.Entrytypes.V2(x, y);
50 }
51 /*@ pure @*/
52
53 public String toString() {
54
55     return "mk_Entry`V2" + Utils.formatFields(x, y);
56 }
57 /*@ pure @*/
58
59 public Number get_x() {
60
61     Number ret_3 = x;
62     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_3));
63
64     return ret_3;
65 }
66
67 public void set_x(final Number _x) {
68
69     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_x));
70
71     x = _x;
72     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(x));
73
74 }
75 /*@ pure @*/
76
77 public Number get_y() {
78
79     Number ret_4 = y;
80     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(ret_4));
81
82     return ret_4;
83 }
84
85 public void set_y(final Number _y) {
86
87     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(_y));
88
89     y = _y;
90     //@ assert project.Entry.invChecksOn ==> (Utils.is_int(y));
91
92 }
93 /*@ pure @*/
94
```

## Appendix C. Validation of the translation rules

```

95     public Boolean valid() {
96
97         return true;
98     }
99 }

1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         {
19             final VDMMMap ignorePattern_1 = consInjMap();
20             //@ assert (V2J.isInjMap(ignorePattern_1) && (\forallall int i; 0 <= i &&
21                 i < V2J.size(ignorePattern_1); Utils.is_nat(V2J.getDom(
22                     ignorePattern_1,i)) && Utils.is_(V2J.getRng(ignorePattern_1,i),
23                     project.Entrytypes.V2.class)));
24
25             /* skip */
26         }
27
28         IO.println("After_legal_use");
29         IO.println("Before_illegal_use");
30         {
31             final VDMMMap ignorePattern_2 = consInjMapErr();
32             //@ assert (V2J.isInjMap(ignorePattern_2) && (\forallall int i; 0 <= i &&
33                 i < V2J.size(ignorePattern_2); Utils.is_nat(V2J.getDom(
34                     ignorePattern_2,i)) && Utils.is_(V2J.getRng(ignorePattern_2,i),
35                     project.Entrytypes.V2.class)));
36
37             /* skip */
38         }
39
40         IO.println("After_illegal_use");
41         return 0L;
42     }
43     /*@ pure @*/
44
45     public static VDMMMap consInjMap() {
46
47         VDMMMap ret_1 =
48             MapUtil.map(
49                 new Maplet(1L, new project.Entrytypes.V2(1L, 2L)),
50                 new Maplet(2L, new project.Entrytypes.V2(2L, 1L)));
51         //@ assert (V2J.isInjMap(ret_1) && (\forallall int i; 0 <= i && i < V2J.
52             size(ret_1); Utils.is_nat(V2J.getDom(ret_1,i)) && Utils.is_(V2J.
53                 getRng(ret_1,i),project.Entrytypes.V2.class)));
54     }
55 }

```

```

47     return Utils.copy(ret_1);
48 }
49 /*@ pure @*/
50
51 public static VDMMap consInjMapErr() {
52
53     VDMMap ret_2 =
54         MapUtil.map(
55             new Maplet(1L, new project.Entrytypes.V2(1L, 2L)),
56             new Maplet(2L, new project.Entrytypes.V2(2L, 1L)),
57             new Maplet(3L, new project.Entrytypes.V2(1L, 2L));
58     //@ assert (V2J.isInjMap(ret_2) && (\forall int i; 0 <= i && i < V2J.
        size(ret_2); Utils.is_nat(V2J.getDom(ret_2,i)) && Utils.is_(V2J.
        getRng(ret_2,i),project.Entrytypes.V2.class));
59
60     return Utils.copy(ret_2);
61 }
62
63 public String toString() {
64
65     return "Entry{}";
66 }
67 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:58: JML assertion is false
    //@ assert (V2J.isInjMap(ret_2) && (\forall int i; 0 <= i && i < V2J.size(
        ret_2); Utils.is_nat(V2J.getDom(ret_2,i)) && Utils.is_(V2J.getRng(ret_2
        ,i),project.Entrytypes.V2.class));
        ^
Entry.java:29: JML assertion is false
    //@ assert (V2J.isInjMap(ignorePattern_2) && (\forall int i; 0 <= i && i
        < V2J.size(ignorePattern_2); Utils.is_nat(V2J.getDom(ignorePattern_2
        ,i)) && Utils.is_(V2J.getRng(ignorePattern_2,i),project.Entrytypes.V2
        .class));
        ^
"After illegal use"

```

## C.76 AssignNonInjMapToInjMap.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12     IO`println("Before_legal_use");
13     let - : map nat to nat = {1 |-> 2, 3 |-> 4} in skip;
14     IO`println("After_legal_use");

```



## Appendix C. Validation of the translation rules

```

15 IO.println("Before_illegal_use");
16 let - : inmap nat to nat = {1 |-> 2, 3 |-> 2} in skip;
17 IO.println("After_illegal_use");
18 return 0;
19 );
20
21 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         IO.println("Before_legal_use");
18         {
19             final VDMMap ignorePattern_1 = MapUtil.map(new Maplet(1L, 2L), new
20                 Maplet(3L, 4L));
21             /* @ assert (V2J.isMap(ignorePattern_1) && (\forallall int i; 0 <= i && i
22                 < V2J.size(ignorePattern_1); Utils.is_nat (V2J.getDom(
23                 ignorePattern_1,i)) && Utils.is_nat (V2J.getRng(ignorePattern_1,i))
24                 ));
25
26             /* skip */
27         }
28
29         IO.println("After_legal_use");
30         IO.println("Before_illegal_use");
31         {
32             final VDMMap ignorePattern_2 = MapUtil.map(new Maplet(1L, 2L), new
33                 Maplet(3L, 2L));
34             /* @ assert (V2J.isInjMap(ignorePattern_2) && (\forallall int i; 0 <= i &&
35                 i < V2J.size(ignorePattern_2); Utils.is_nat (V2J.getDom(
36                 ignorePattern_2,i)) && Utils.is_nat (V2J.getRng(ignorePattern_2,i))
37                 ));
38
39             /* skip */
40         }
41
42         IO.println("After_illegal_use");
43         return 0L;
44     }
45
46     public String toString() {
47
48         return "Entry{}";
49     }
50 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isInjMap(ignorePattern_2) && (\forall int i; 0 <= i && i
        < V2J.size(ignorePattern_2); Utils.is_nat(V2J.getDom(ignorePattern_2
        ,i)) && Utils.is_nat(V2J.getRng(ignorePattern_2,i)))));
        ^
"After illegal use"

```

## C.77 MapBoolToNatAssignNil.vdmsl

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : map bool to nat = {false |-> 0, true |-> 1} in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : map bool to nat = mapNil() in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 mapNil : () -> [map bool to nat]
24 mapNil () == nil;
25
26 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");

```

```

18 {
19   final VDMMMap ignorePattern_1 = MapUtil.map(new Maplet(false, 0L), new
20     Maplet(true, 1L));
21   //@ assert (V2J.isMap(ignorePattern_1) && (\forall forall int i; 0 <= i && i
22     < V2J.size(ignorePattern_1); Utils.is_bool(V2J.getDom(
23       ignorePattern_1,i)) && Utils.is_nat(V2J.getRng(ignorePattern_1,i))
24     ));
25   /* skip */
26 }
27
28 IO.println("After_legal_use");
29 IO.println("Before_illegal_use");
30 {
31   final VDMMMap ignorePattern_2 = mapNil();
32   //@ assert (V2J.isMap(ignorePattern_2) && (\forall forall int i; 0 <= i && i
33     < V2J.size(ignorePattern_2); Utils.is_bool(V2J.getDom(
34       ignorePattern_2,i)) && Utils.is_nat(V2J.getRng(ignorePattern_2,i))
35     ));
36   /* skip */
37 }
38
39 IO.println("After_illegal_use");
40 return 0L;
41 }
42 /*@ pure @*/
43
44 public static VDMMMap mapNil() {
45   VDMMMap ret_1 = null;
46   //@ assert ((ret_1 == null) || (V2J.isMap(ret_1) && (\forall forall int i; 0 <=
47     i && i < V2J.size(ret_1); Utils.is_bool(V2J.getDom(ret_1,i)) &&
48     Utils.is_nat(V2J.getRng(ret_1,i))));
49
50   return Utils.copy(ret_1);
51 }
52
53 public String toString() {
54
55   return "Entry{}";
56 }
57 }

```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isMap(ignorePattern_2) && (\forall forall int i; 0 <= i && i <
        V2J.size(ignorePattern_2); Utils.is_bool(V2J.getDom(ignorePattern_2,i
        )) && Utils.is_nat(V2J.getRng(ignorePattern_2,i)));
        ^
"After illegal use"

```

## C.78 MapBoolToNatDetectNegInt.vdmsl

## Appendix C. Validation of the translation rules

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_legal_use");
13   let - : map bool to nat = {false |-> 0, true |-> 1} in skip;
14   IO`println("After_legal_use");
15   IO`println("Before_illegal_use");
16   let - : map bool to nat = mapBoolToInt() in skip;
17   IO`println("After_illegal_use");
18   return 0;
19 );
20
21 functions
22
23 mapBoolToInt : () -> map bool to int
24 mapBoolToInt () == {false |-> 0, true |-> -1}
25
26 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_legal_use");
18     {
19       final VDMMap ignorePattern_1 = MapUtil.map(new Maplet(false, 0L), new
20         Maplet(true, 1L));
21       //@ assert (V2J.isMap(ignorePattern_1) && (\forallall int i; 0 <= i && i
22         < V2J.size(ignorePattern_1); Utils.is_bool(V2J.getDom(
23         ignorePattern_1,i)) && Utils.is_nat(V2J.getRng(ignorePattern_1,i))
24         ));
25
26       /* skip */
27     }
28
29     IO.println("After_legal_use");
30     IO.println("Before_illegal_use");
31     {
32       final VDMMap ignorePattern_2 = mapBoolToInt();
33       //@ assert (V2J.isMap(ignorePattern_2) && (\forallall int i; 0 <= i && i

```

## Appendix C. Validation of the translation rules

```

    < V2J.size(ignorePattern_2); Utils.is_bool(V2J.getDom(
    ignorePattern_2,i)) && Utils.is_nat(V2J.getRng(ignorePattern_2,i))
    ));
30
31    /* skip */
32  }
33
34  IO.println("After_illegal_use");
35  return 0L;
36  }
37  /*@ pure @*/
38
39  public static VDMMap mapBoolToInt() {
40
41    VDMMap ret_1 = MapUtil.map(new Maplet(false, 0L), new Maplet(true, -1L))
42    ;
43    //@ assert (V2J.isMap(ret_1) && (\forall int i; 0 <= i && i < V2J.size(
44    ret_1); Utils.is_bool(V2J.getDom(ret_1,i)) && Utils.is_int(V2J.
45    getRng(ret_1,i)))));
46
47    return Utils.copy(ret_1);
48  }
49
50  public String toString() {
51    return "Entry{}";
52  }
53 }
```

```

"Before legal use"
"After legal use"
"Before illegal use"
Entry.java:29: JML assertion is false
    //@ assert (V2J.isMap(ignorePattern_2) && (\forall int i; 0 <= i && i <
    V2J.size(ignorePattern_2); Utils.is_bool(V2J.getDom(ignorePattern_2,i
    )) && Utils.is_nat(V2J.getRng(ignorePattern_2,i)))));
    ^
"After illegal use"
```

### C.79 AssignBoolTypeViolation.vdmsl

```

1 module Entry
2
3 imports from IO all
4 exports all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   decl b : bool := true;
13   decl bOpt : [bool] := nil;
14
15   IO`println("Before_doing_valid_assignments");
```

## Appendix C. Validation of the translation rules

```
16  bOpt := true;
17  b := bOpt;
18  bOpt := nil;
19  IO.println("After_doing_valid_assignments");
20
21  IO.println("Before_doing_illegal_assignments");
22  b := bOpt;
23  IO.println("After_doing_illegal_assignments");
24
25  return true;
26 );
27
28
29 end Entry
```

```
1  package project;
2
3  import java.util.*;
4  import org.overture.codegen.runtime.*;
5  import org.overture.codegen.vdm2jml.runtime.*;
6
7  @SuppressWarnings("all")
8  //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         Boolean b = true;
18         //@ assert Utils.is_bool(b);
19
20         Boolean bOpt = null;
21         //@ assert ((bOpt == null) || Utils.is_bool(bOpt));
22
23         IO.println("Before_doing_valid_assignments");
24         bOpt = true;
25         //@ assert ((bOpt == null) || Utils.is_bool(bOpt));
26
27         b = bOpt;
28         //@ assert Utils.is_bool(b);
29
30         bOpt = null;
31         //@ assert ((bOpt == null) || Utils.is_bool(bOpt));
32
33         IO.println("After_doing_valid_assignments");
34         IO.println("Before_doing_illegal_assignments");
35         b = bOpt;
36         //@ assert Utils.is_bool(b);
37
38         IO.println("After_doing_illegal_assignments");
39         return true;
40     }
41
42     public String toString() {
43
44         return "Entry{}";
45     }
46 }
```

46 | }

```

"Before doing valid assignments"
"After doing valid assignments"
"Before doing illegal assignments"
Entry.java:36: JML assertion is false
    //@ assert Utils.is_bool(b);
        ^
"After doing illegal assignments"

```

## C.80 VarDeclTypeViolation.vdmsl

```

1 module Entry
2
3 imports from IO all
4 exports all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_VALID_initialisation");
13   (dcl bOkay : nat := natOne(); skip);
14   IO`println("After_VALID_initialisation");
15
16   IO`println("Before_INVALID_initialisation");
17   (dcl bError : nat := natNil(); skip);
18   IO`println("After_INVALID_initialisation");
19
20   return true;
21 );
22
23 functions
24
25 natNil : () -> [nat]
26 natNil () == nil;
27
28 natOne : () -> [nat]
29 natOne () == 1;
30
31 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12

```

```

13  private Entry() {}
14
15  public static Object Run() {
16
17      IO.println("Before_VALID_initialisation");
18      {
19          Number bOkay = natOne();
20          //@ assert Utils.is_nat(bOkay);
21
22          /* skip */
23      }
24
25      IO.println("After_VALID_initialisation");
26      IO.println("Before_INVALID_initialisation");
27      {
28          Number bError = natNil();
29          //@ assert Utils.is_nat(bError);
30
31          /* skip */
32      }
33
34      IO.println("After_INVALID_initialisation");
35      return true;
36  }
37  /*@ pure @*/
38
39  public static Number natNil() {
40
41      Number ret_1 = null;
42      //@ assert ((ret_1 == null) || Utils.is_nat(ret_1));
43
44      return ret_1;
45  }
46  /*@ pure @*/
47
48  public static Number natOne() {
49
50      Number ret_2 = 1L;
51      //@ assert ((ret_2 == null) || Utils.is_nat(ret_2));
52
53      return ret_2;
54  }
55
56  public String toString() {
57
58      return "Entry{}";
59  }
60  }

```

```

"Before VALID initialisation"
"After VALID initialisation"
"Before INVALID initialisation"
Entry.java:29: JML assertion is false
    //@ assert Utils.is_nat(bError);
           ^
"After INVALID initialisation"

```

## C.81 FuncReturnTokenViolation.vdmsl



```

1 module Entry
2
3 imports from IO all
4 exports all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 (
12   IO`println("Before_evaluating_ok()");
13   let - = ok() in skip;
14   IO`println("After_evaluating_ok()");
15
16   IO`println("Before_evaluating_error()");
17   let - = err() in skip;
18   IO`println("After_evaluating_error()");
19
20   return true;
21 );
22
23 functions
24
25 ok : () -> token
26 ok () ==
27 let aOpt : [token] = mk_token("")
28 in
29   aOpt;
30
31
32 err : () -> token
33 err () ==
34 let aOpt : [token] = nil
35 in
36   aOpt;
37
38 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     IO.println("Before_evaluating_ok()");
18     {
19       final Token ignorePattern_1 = ok();

```

## Appendix C. Validation of the translation rules

```

20      //@ assert Utils.is_token(ignorePattern_1);
21
22      /* skip */
23  }
24
25  IO.println("After_evaluating_ok()");
26  IO.println("Before_evaluating_error()");
27  {
28      final Token ignorePattern_2 = err();
29      //@ assert Utils.is_token(ignorePattern_2);
30
31      /* skip */
32  }
33
34  IO.println("After_evaluating_error()");
35  return true;
36  }
37  /*@ pure @*/
38
39  public static Token ok() {
40
41      final Token aOpt = new Token("");
42      //@ assert ((aOpt == null) || Utils.is_token(aOpt));
43
44      Token ret_1 = aOpt;
45      //@ assert Utils.is_token(ret_1);
46
47      return ret_1;
48  }
49  /*@ pure @*/
50
51  public static Token err() {
52
53      final Token aOpt = null;
54      //@ assert ((aOpt == null) || Utils.is_token(aOpt));
55
56      Token ret_2 = aOpt;
57      //@ assert Utils.is_token(ret_2);
58
59      return ret_2;
60  }
61
62  public String toString() {
63
64      return "Entry{}";
65  }
66  }

```

```

"Before evaluating ok() "
"After evaluating ok() "
"Before evaluating error() "
Entry.java:57: JML assertion is false
    //@ assert Utils.is_token(ret_2);
    ^
Entry.java:29: JML assertion is false
    //@ assert Utils.is_token(ignorePattern_2);
    ^
"After evaluating error() "

```

## C.82 OpParamQuoteTypeViolation.vdmsl

```

1 module Entry
2
3 imports from IO all
4 exports all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 let aOpt : [<A>] = nil,
12     a : <A> = <A>
13 in
14 (
15   IO`println("Before_passing_LEGAL_value");
16   op(a);
17   IO`println("After_passing_LEGAL_value");
18
19   IO`println("Before_passing_ILLEGAL_value");
20   op(aOpt);
21   IO`println("After_passing_ILLEGAL_value");
22
23   return true;
24 );
25
26 op : <A> ==> ()
27 op (-) == skip;
28
29 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11   /* @ public ghost static boolean invChecksOn = true; @ */
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     final project.quotes.AQuote aOpt = null;
18     /* @ assert ((aOpt == null) || Utils.is_(aOpt, project.quotes.AQuote.class)) */
19
20     final project.quotes.AQuote a = project.quotes.AQuote.getInstance();
21     /* @ assert Utils.is_(a, project.quotes.AQuote.class); */
22
23     {
24       IO.println("Before_passing_LEGAL_value");
25       op(a);

```

```

26     IO.println("After_passing_LEGAL_value");
27     IO.println("Before_passing_ILLEGAL_value");
28     op(aOpt);
29     IO.println("After_passing_ILLEGAL_value");
30     return true;
31 }
32 }
33
34 public static void op(final project.quotes.AQuote ignorePattern_1) {
35
36     //@ assert Utils.is_(ignorePattern_1,project.quotes.AQuote.class);
37
38     /* skip */
39
40 }
41
42 public String toString() {
43
44     return "Entry{}";
45 }
46 }

```

```

"Before passing LEGAL value"
"After passing LEGAL value"
"Before passing ILLEGAL value"
Entry.java:36: JML assertion is false
    //@ assert Utils.is_(ignorePattern_1,project.quotes.AQuote.class);
               ^
"After passing ILLEGAL value"

```

## C.83 Exists.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 let - = f()
12 in
13 (
14   IO`println("Done!_Expected_no_errors");
15   return 0;
16 );
17
18 functions
19
20 f : () -> bool
21 f () ==
22   exists x in set {1,2,3} & x > 0;
23
24 end Entry

```

## Appendix C. Validation of the translation rules

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 // @ nullable_by_default
9
10 final public class Entry {
11     /* @ public ghost static boolean invChecksOn = true; @ */
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         final Boolean ignorePattern_1 = f();
18         /* @ assert Utils.is_bool(ignorePattern_1);
19
20         {
21             IO.println("Done!_Expected_no_errors");
22             return 0L;
23         }
24     }
25     /* @ pure @ */
26
27     public static Boolean f() {
28
29         Boolean existsExpResult_1 = false;
30         /* @ assert Utils.is_bool(existsExpResult_1);
31
32         VDMSet set_1 = SetUtil.set(1L, 2L, 3L);
33         /* @ assert (V2J.isSet(set_1) && (\forallall int i; 0 <= i && i < V2J.size(
34             set_1); Utils.is_nat1(V2J.get(set_1,i)))));
35
36         for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() && !(
37             existsExpResult_1); ) {
38             Number x = ((Number) iterator_1.next());
39             /* @ assert Utils.is_nat1(x);
40
41             existsExpResult_1 = x.longValue() > 0L;
42             /* @ assert Utils.is_bool(existsExpResult_1);
43
44             }
45             Boolean ret_1 = existsExpResult_1;
46             /* @ assert Utils.is_bool(ret_1);
47
48             return ret_1;
49         }
50
51         public String toString() {
52
53             return "Entry{}";
54         }
55     }

```

"Done! Expected no errors"

## C.84 ForAll.vdmsl

---

```

1 module Entry
2
3 exports all
4 imports from IO all
5 definitions
6
7 operations
8
9 Run : () ==> ?
10 Run () ==
11 let - = f()
12 in
13 (
14   IO.println("Done!_Expected_no_errors");
15   return 0;
16 );
17
18 functions
19
20 f : () -> bool
21 f () ==
22   forall x in set {1,2,3} & x > 0;
23
24 end Entry

```

```

1 package project;
2
3 import java.util.*;
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11   /*@ public ghost static boolean invChecksOn = true; @*/
12
13   private Entry() {}
14
15   public static Object Run() {
16
17     final Boolean ignorePattern_1 = f();
18     //@ assert Utils.is_bool(ignorePattern_1);
19
20     {
21       IO.println("Done!_Expected_no_errors");
22       return 0L;
23     }
24   }
25   /*@ pure @*/
26
27   public static Boolean f() {
28
29     Boolean forAllExpResult_1 = true;
30     //@ assert Utils.is_bool(forAllExpResult_1);
31
32     VDMSet set_1 = SetUtil.set(1L, 2L, 3L);

```

```

33      //@ assert (V2J.isSet(set_1) && (\forall int i; 0 <= i && i < V2J.size(
        set_1); Utils.is_nat1(V2J.get(set_1,i)))));
34
35      for (Iterator iterator_1 = set_1.iterator(); iterator_1.hasNext() &&
        forAllExpResult_1; ) {
36          Number x = ((Number) iterator_1.next());
37          //@ assert Utils.is_nat1(x);
38
39          forAllExpResult_1 = x.longValue() > 0L;
40          //@ assert Utils.is_bool(forAllExpResult_1);
41
42      }
43      Boolean ret_1 = forAllExpResult_1;
44      //@ assert Utils.is_bool(ret_1);
45
46      return ret_1;
47  }
48
49  public String toString() {
50
51      return "Entry{}";
52  }
53  }

```

```
"Done! Expected no errors"
```

## C.85 Exists1.vdmsl

```

1  module Entry
2
3  exports all
4  imports from IO all
5  definitions
6
7  operations
8
9  Run : () ==> ?
10 Run () ==
11 let - = f()
12 in
13 (
14   IO`println("Done!_Expected_no_errors");
15   return 0;
16 );
17
18 functions
19
20 f : () -> bool
21 f () ==
22   exists1 x in set {1,2,3} & x > 0;
23
24 end Entry

```

```

1  package project;
2
3  import java.util.*;

```

## Appendix C. Validation of the translation rules

```
4 import org.overture.codegen.runtime.*;
5 import org.overture.codegen.vdm2jml.runtime.*;
6
7 @SuppressWarnings("all")
8 //@ nullable_by_default
9
10 final public class Entry {
11     /*@ public ghost static boolean invChecksOn = true; @*/
12
13     private Entry() {}
14
15     public static Object Run() {
16
17         final Boolean ignorePattern_1 = f();
18         //@ assert Utils.is_bool(ignorePattern_1);
19
20         {
21             IO.println("Done!_Expected_no_errors");
22             return 0L;
23         }
24     }
25     /*@ pure @*/
26
27     public static Boolean f() {
28
29         Long exists1Counter_1 = 0L;
30
31         VDMSet set_1 = SetUtil.set(1L, 2L, 3L);
32         //@ assert (V2J.isSet(set_1) && (\forall int i; 0 <= i && i < V2J.size(
33             set_1); Utils.is_nat1(V2J.get(set_1,i)))));
34
35         for (Iterator iterator_1 = set_1.iterator();
36             iterator_1.hasNext() && (exists1Counter_1.longValue() < 2L);
37             ) {
38             Number x = ((Number) iterator_1.next());
39             //@ assert Utils.is_nat1(x);
40
41             if (x.longValue() > 0L) {
42                 exists1Counter_1++;
43             }
44             Boolean ret_1 = Utils.equals(exists1Counter_1, 1L);
45             //@ assert Utils.is_bool(ret_1);
46
47             return ret_1;
48         }
49
50     public String toString() {
51
52         return "Entry{}";
53     }
54 }
```



# Bibliography

- [1] Abrial, J.R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press (2010)
- [2] The test examples used to validate the JML translator using the OpenJML runtime assertion checker. [https://github.com/overturetool/overture/tree/development/core/codegen/vdm2jml/src/test/resources/dynamic\\_analysis/](https://github.com/overturetool/overture/tree/development/core/codegen/vdm2jml/src/test/resources/dynamic_analysis/) (2016)
- [3] Andrews, D., Bruun, H., Damm, F., Dawes, J., Hansen, B., Larsen, P., Parkin, G., Plat, N., Totenel, H.: A Formal Definition of VDM-SL. Tech. Rep. 1998/9, Leicester University (June 1998)
- [4] The Apache Maven Project website. <https://maven.apache.org> (2016)
- [5] Bjørner, D., Jones, C. (eds.): The Vienna Development Method: The Meta-Language, Lecture Notes in Computer Science, vol. 61. Springer-Verlag (1978)
- [6] Burdy, L., Cheon, Y., Cok, D., Ernst, M.D., Kiniry, J.R., Leavens, G.T., Leino, K.R.M., Poll, E.: An overview of JML Tools and Applications. Intl. Journal of Software Tools for Technology Transfer 7, 212–232 (2005)
- [7] Cok, D.R.: Reasoning with specifications containing method calls and model fields. Journal of Object Technology 4(8), 77–103 (2005)
- [8] Cok, D.: OpenJML: JML for Java 7 by Extending OpenJDK. In: Bobaru, M., Havelund, K., Holzmann, G., Joshi, R. (eds.) NASA Formal Methods, Lecture Notes in Computer Science, vol. 6617, pp. 472–479. Springer Berlin Heidelberg (2011), [http://dx.doi.org/10.1007/978-3-642-20398-5\\_35](http://dx.doi.org/10.1007/978-3-642-20398-5_35)
- [9] Filliâtre, J.C.: Why: a multi-language multi-prover verification tool. Research Report 1366, LRI, Université Paris Sud (March 2003), <http://www.lri.fr/~filliatr/ftp/publis/why-tool.ps.gz>
- [10] Fitzgerald, J.S., Larsen, P.G., Verhoef, M.: Vienna Development Method. Wiley Encyclopedia of Computer Science and Engineering (2008), edited by Benjamin Wah, John Wiley & Sons, Inc.
- [11] Fitzgerald, J., Larsen, P.G.: Modelling Systems – Practical Tools and Techniques in Software Development. Cambridge University Press, The Edinburgh Building, Cambridge CB2 2RU, UK, Second edn. (2009), ISBN 0-521-62348-0
- [12] Fitzgerald, J., Larsen, P.G., Mukherjee, P., Plat, N., Verhoef, M.: Validated Designs for Object-oriented Systems. Springer, New York (2005), <http://overturetool.org/publications/books/vdoos/>

## Bibliography

- [13] Hubbers, E., Oostdijk, M.: Generating JML specifications from UML state diagrams. In: Forum on Specification and Design Languages FDL'03. pp. 263–273 (2003)
- [14] Jin, D., Yang, Z.: Strategies of Modeling from VDM-SL to JML. Advanced Language Processing and Web Information Technology, International Conference on 0, 320–323 (2008)
- [15] Jones, C.B.: Software Development A Rigorous Approach. Prentice-Hall International, Englewood Cliffs, New Jersey (1980)
- [16] Jørgensen, P.W.V., Couto, L.D., Larsen, M.: A Code Generation Platform for VDM. In: Proceedings of the 12th Overture workshop (June 2014)
- [17] Klebanov, A.: Automata-Based Programming Technology Extension for Generation of JML Annotated Java Card Code. pp. 41–44. Proc. of the Spring/Summer Young Researchers' Colloquium on Software Engineering (2008)
- [18] Larsen, P.G.: Ten Years of Historical Development: “Bootstrapping” VDMTools. Journal of Universal Computer Science 7(8), 692–709 (2001)
- [19] Larsen, P.G., Battle, N., Ferreira, M., Fitzgerald, J., Lausdahl, K., Verhoef, M.: The Overture Initiative – Integrating Tools for VDM. SIGSOFT Softw. Eng. Notes 35(1), 1–6 (January 2010), <http://doi.acm.org/10.1145/1668862.1668864>
- [20] Larsen, P.G., Lausdahl, K., Battle, N.: Combinatorial Testing for VDM. In: Proceedings of the 2010 8th IEEE International Conference on Software Engineering and Formal Methods. pp. 278–285. SEFM '10, IEEE Computer Society, Washington, DC, USA (September 2010), <http://dx.doi.org/10.1109/SEFM.2010.32>, ISBN 978-0-7695-4153-2
- [21] Larsen, P.G., Lausdahl, K., Battle, N., Fitzgerald, J., Wolff, S., Sahara, S., Verhoef, M., Tran-Jørgensen, P.W.V., Oda, T., Chisholm, P.: The VDM-10 Language Manual. Tech. Rep. TR-2010-06, The Overture Open Source Initiative (April 2010)
- [22] Larsen, P.G., Lausdahl, K., Tran-Jørgensen, P.W.V., Ribeiro, A., Wolff, S., Battle, N.: Overture VDM-10 Tool Support: User Guide. Tech. Rep. TR-2010-02, The Overture Initiative, [www.overturetool.org](http://www.overturetool.org) (May 2010)
- [23] Lausdahl, K., Larsen, P.G., Battle, N.: A Deterministic Interpreter Simulating A Distributed real time system using VDM. In: Qin, S., Qiu, Z. (eds.) Proceedings of the 13th international conference on Formal methods and software engineering. Lecture Notes in Computer Science, vol. 6991, pp. 179–194. Springer-Verlag, Berlin, Heidelberg (October 2011), ISBN 978-3-642-24558-9
- [24] Leavens, G.T., Poll, E., Clifton, C., Cheon, Y., Ruby, C., Cok, D., Kiniry, J.: JML Reference Manual, revision 2344 edn. (May 2013)
- [25] Lensink, L., Smetsers, S., van Eekelen, M.: Generating Verifiable Java Code from Verified PVS Specifications. In: Goodloe, A., Person, S. (eds.) NASA Formal Methods, Lecture Notes in Computer Science, vol. 7226, pp. 310–325. Springer Berlin Heidelberg (2012), [http://dx.doi.org/10.1007/978-3-642-28891-3\\_30](http://dx.doi.org/10.1007/978-3-642-28891-3_30)
- [26] McCarthy, J.: A Basis for a Mathematical Theory of Computation. In: Western Joint Computer Conference (1961)
- [27] Meyer, B.: Object-oriented Software Construction. Prentice-Hall International (1988)

## Bibliography

- [28] Müller, P., Poetzsch-Heffter, A., Leavens, G.T.: Modular Invariants for Layered Object Structures. *Sci. Comput. Program.* 62(3), 253–286 (Oct 2006), <http://dx.doi.org/10.1016/j.scico.2006.03.001>
- [29] The OpenJML website. <http://www.openjml.org> (2016)
- [30] The Overture tool website. <http://overturetool.org/> (2015)
- [31] The Overture tool Github repository. <https://github.com/overturetool/overture> (2016)
- [32] Owre, S., Rushby, J.M., Shankar, N.: PVS: A Prototype Verification System. In: Kapur, D. (ed.) 11th International Conference on Automated Deduction (CADE). *Lecture Notes in Artificial Intelligence*, vol. 607, pp. 748–752. Springer-Verlag, Saratoga, NY (June 1992)
- [33] Rivera, V., Cataño, N., Wahls, T., Rueda, C.: Code generation for Event-B. *International Journal on Software Tools for Technology Transfer* pp. 1–22 (2015)
- [34] Rumbaugh, J., Jacobson, I., Booch, G.: *Unified Modeling Language Reference Manual*, The (2nd Edition). Pearson Higher Education (2004)
- [35] Tran-Jørgensen, P.W.V., Larsen, P.G., Battle, N.: Using JML-based Code Generation to Enhance Test Automation for VDM Models. In: *Proceedings of the 14th Overture Workshop* (November 2016)
- [36] Tran-Jørgensen, P.W.V., Larsen, P.G., Leavens, G.T.: Automated translation of vdm to jml-annotated java. *International Journal on Software Tools for Technology Transfer* pp. 1–25 (2017), <http://dx.doi.org/10.1007/s10009-017-0448-3>
- [37] Vilhena, C.: *Connecting between VDM++ and JML*. Master’s thesis, Minho University with exchange to Engineering College of Aarhus (July 2008)
- [38] Wing, J.M.: Writing Larch interface language specifications. *ACM Trans. Progr. Lang. Syst.* 9(1), 1–24 (Jan 1987), <http://doi.acm.org/10.1145/9758.10500>
- [39] Woodcock, J., Davies, J.: *Using Z – Specification, Refinement, and Proof*. Prentice Hall International Series in Computer Science (1996)
- [40] Yi, J., Robby, Deng, X., Roychoudhury, A.: Past Expression: Encapsulating Pre-states at Post-conditions by Means of AOP. In: *Proceedings of the 12th Annual International Conference on Aspect-oriented Software Development*. pp. 133–144. AOSD ’13, ACM (2013), <http://doi.acm.org/10.1145/2451436.2451453>
- [41] Zhen, Z.: *Java Card Technology for Smart Cards*. Prentice-Hall, Boston (2000)
- [42] Zhou, J., Jin, D.: Research on modeling from VDM-SL to JML for systematic software development. In: *Control and Decision Conference (CCDC), 2010 Chinese*. pp. 2312–2317. IEEE, Xuzhou (July 2010)