
Published version (with publisher’s formatting)

This version is available at: http://eprints.mdx.ac.uk/14663/

Copyright:

Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this work are retained by the author and/or other copyright owners unless otherwise stated. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge.

Works, including theses and research projects, may not be reproduced in any format or medium, or extensive quotations taken from them, or their content changed in any way, without first obtaining permission in writing from the copyright holder(s). They may not be sold or exploited commercially in any format or medium without the prior written permission of the copyright holder(s).

Full bibliographic details must be given when referring to, or quoting from full items including the author’s name, the title of the work, publication details where relevant (place, publisher, date), pagination, and for theses or dissertations the awarding institution, the degree type awarded, and the date of the award.

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:

eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.

See also repository copyright: re-use policy: http://eprints.mdx.ac.uk/policies.html#copy
Language-Independent Model Transformation Verification

K. Lano, S. Kolahdouz-Rahimi, T. Clark

King’s College London; University of Middlesex

Abstract. One hinderance to model transformation verification is the large number of different MT languages which exist, resulting in a large number of different language-specific analysis tools. As an alternative, we define a single analysis process which can, in principle, analyse specifications in several different transformation languages, by making use of a common intermediate representation to express the semantics of transformations in any of these languages. Some analyses can be performed directly on the intermediate representation, and further semantic models in specific verification formalisms can be derived from it. We illustrate the approach by applying it to ATL.

1 Introduction

A large number of different transformation languages exist, ranging from declarative languages such as QVT-R [13] and Triple Graph Grammars, to hybrid languages such as ATL [6] and UML-RSDS [10], to imperative. There are nonetheless many commonalities between the processing carried out by transformations, regardless of the language they are written in.

In this paper we describe a general language-independent framework for transformation verification, and describe a range of language-independent verification techniques. The framework is based upon metamodels which provide language-independent representation of transformation specifications (Section 2). These representations can then be mapped via semantic mappings to suitable formalisms which support verification (such as theorem provers or constraint satisfaction checkers). This approach means that only one semantic mapping needs to be defined and verified for each target formalism, rather than semantic maps for each different transformation language and target formalism.

2 Metamodels for model transformations

Transformations operate on various models or texts which conform to some metamodel/language. There may be several input (source) models used by a transformation, and possibly several output (target) models. A transformation is termed update-in-place if a model is both an input and output, otherwise it is a separate-models transformation. Languages can be specified in many different ways, e.g., by UML class diagrams, by BNF syntax definitions, etc. Here we
will use UML class diagrams, together with OCL constraints. These form the concrete syntax of language descriptions.

Figure 1 shows a generic metamodel (termed \(\mathcal{LMM}\)) which can serve directly or indirectly as a metamodel (abstract syntax) for a wide range of modelling languages. The metamodel is also self-representative. \textit{EntityType} represents classes and interfaces, \textit{DataFeature} represents both attributes and associations. \textit{mult1lower} and \textit{mult1upper} refer to the multiplicity range of the source side of the attribute/association (i.e., the side with the entity type which owns the data feature), whilst \textit{mult2lower} and \textit{mult2upper} refer to the multiplicity range of the target side (the side with the type entity type). A value of \(-1\) for an upper bound indicates a *-multiplicity at that end. \textit{isOrdered} refers to the ordering of the target end.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{fig1.png}
\caption{Minimal metamodel (\(\mathcal{LMM}\)) for modelling languages}
\end{figure}

A metaclass \textit{Language} representing languages has a set \textit{entityTypes} of \textit{EntityType}, a set \textit{features} of \textit{DataFeature}, and a set \textit{constraints} of \textit{Constraint}. Many variations on constraint languages could be used, here we adopt the subset of OCL 2.3 used in UML-RSDS [11, 12]. This includes set and sequence collections from OCL, operation calls and other feature application and navigation expressions, but omits \textit{null} and \textit{invalid}. The set of all expressions formed over a given base language \(L\) (a class diagram) is denoted \(\text{Exp}(L)\). To support verification, we define a proof theory and (logical) model theory with respect to any language \(L\), by associating a formal first order language and logic to each instance of \(\mathcal{LMM}\). Table 1 gives examples showing how a formal first-order set theory (FOL) language \(L_L\) can be associated to instances \(L\) of \(\mathcal{LMM}\).

An optional association end (with \textit{mult2lower} = 0 and \textit{mult2upper} = 1) is formally represented as a set (or sequence) of size 0 or 1. A denumerable type
Object OBJ is included in each $\mathcal{L}_L$ to represent the set of all possible object references. A finite set $\text{objects} \subseteq \text{Object OBJ}$ represents the set of all existing objects at any point in time. Each entity type $E$ has $E \subseteq \text{objects}$. Constraints in the expression language $\text{Exp}(L)$ are mathematically represented as first-order set theory axioms in $\mathcal{L}_L$, for each base language $L$.

At the specification level, the effect of a transformation can be characterised by a collection of mapping specifications, which relate model elements of one or more models involved in the transformation to each other [5]. These mapping specifications define the intended relationships which the transformation should establish between the input (source) and output (target) models of the transformation, at its termination. That is, they define the postconditions Post of the transformation. In the case of in-place transformations, the initial values of entity types and features can be notated as $E@\text{pre}, f@\text{pre}$ in postconditions to distinguish them from their post-state values. We adapt the mapping metamodel of [5] to represent transformation specifications (Figure 2). This metamodel is referred to as $\mathcal{TMM}$ in the following.

In this figure, Mapping, TransformationSpecification, ModelEnd, and MappingEnd are subclasses of NamedElement. Each mapping has a corresponding computation step which defines the application of the mapping to specific source elements that satisfy its condition. Transformation specifications in declarative transformation languages can be expressed in this metamodel, using abstraction techniques such as those defined for TGG (triple graph grammars) and QVT-R in [4] and for declarative ATL in [3]: these techniques express the intended effect of transformations by OCL constraints describing the poststate of the transformation. In this paper we show how hybrid languages such as ATL can also be expressed in $\mathcal{TMM}$. In turn, formal representations of transformation specifications can be generated from representations in $\mathcal{TMM}$, into a range of formalisms such as B [9], Z3 [15] or Alloy [1], to support semantic analysis. The metamodel

<table>
<thead>
<tr>
<th>Modelling concept</th>
<th>$\mathcal{LMM}$ representation</th>
<th>Formal semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity type $E$</td>
<td>Element of EntityType</td>
<td>Type symbol $E'$, denoting the set of instances of $E$</td>
</tr>
<tr>
<td>Single-valued attribute $att : \text{Typ}$ of $E$</td>
<td>$\text{DataFeature element with mult}_2\text{upper} = 1, \text{mult}_2\text{lower} = 1$ and $\text{type} \in \text{PrimitiveDataType}$</td>
<td>Function symbol $att' : E' \rightarrow T'y'$ where $T'y'$ represents Typ</td>
</tr>
<tr>
<td>Single-valued role $r$ of $E$ with target entity type $E_1$</td>
<td>$\text{DataFeature element with mult}_2\text{upper} = 1, \text{mult}_2\text{lower} = 1$ and $\text{type} \in \text{EntityType}$</td>
<td>Function symbol $r' : E' \rightarrow E_1'$</td>
</tr>
<tr>
<td>Unordered many-valued role $r$ of $E$ with target entity type $E_1$</td>
<td>$\text{DataFeature element with mult}_2\text{upper} \neq 1$ or $\text{mult}_2\text{lower} \neq 1$ and $\text{isOrdered} = \text{false}$ and $\text{type} \in \text{EntityType}$</td>
<td>Function symbol $r' : E' \rightarrow F(E_1')$</td>
</tr>
<tr>
<td>Supertype $E_1$ of $E$</td>
<td>$E_1 \in E._{\text{general}}$</td>
<td>Type $E_1'$ with $E' \subseteq E_1'$</td>
</tr>
</tbody>
</table>

Table 1. Correspondence of $\mathcal{LMM}$ and first-order logics
could be extended to include generalisation relations between mappings, as in ATL and ETL [8].

The rules\_relation constraints express the postconditions Post of the transformation. Typically each mapping relation constraint $Cn \in Post$ has the form of an implication $SCond \implies Succ$ forall-quantified over elements (the source mapping ends $s : S_i$) of the source models. The assumptions express the preconditions Asm of the transformation. The invariants define properties Inv which should be true initially, and which should be preserved by each computation step of the transformation.

3 Verification techniques

The following verification techniques can be applied to the $\mathcal{TMM}$ representation of transformations, as follows:

- Syntactic analysis to identify the definedness conditions $\text{def}(Cn)$ and determinacy conditions $\text{det}(Cn)$ of each mapping constraint $Cn$. These are the conditions necessary for $Cn$ to have a defined and determinate value, respectively [10].

- Data dependency analysis, to compute the read-frame $rd(Cn)$ and write-frame $wr(Cn)$ for each mapping constraint $Cn$\footnote{$wr(Cn)$ is the set of feature names and entity type names which $Cn$’s implementation may modify. $rd(Cn)$ is the set which may be read.} and to identify cases of invalid data-dependency and data-use.
- Syntactic analysis to establish confluence and termination in the case of transformations not involving fixed-point iteration.
- Translation to B AMN, to verify transformation invariants, syntactic correctness (that the transformation produces target models which conform to the target metamodel) and model-level semantic preservation (that the source and target models have equivalent semantics).
- Translation to Z3, to identify counter-examples to syntactic correctness.

Figure 3 shows an example of data dependency analysis being performed on the $TMM$ representation of an ATL specification: two rules are identified as writing to the same entity type and feature, so are potentially in conflict.

4 Mapping from ATL to transformation metamodel

Table 2 shows the mapping of ATL (standard mode) [6] elements to elements of $TMM$. We assume that all rule inheritance has been statically expanded out so that only leaf rules exist.

We denote the $TMM$ expression equivalent of an ATL expression $e$ by $e'$.

Given an ATL module

```
module M;
create OUT : T from IN : S;
rule r1
{ from s1 : S1, ..., sm : Sm (SCond)
  using { v1 : Typ1 = val1; ... }
  to t1 : T1 (TCond1), ..., tk : Tk (TCondk)
  do (Stat)
}
...
rule rn { ... }
```
the $TMM$ representation of $M$ is a transformation specification $M'$, and each matched rule $r_i$ is represented by two mappings $r_i\text{Matching}$ and $r_i\text{Initialisation}$ of $M'$, which both have readOnly mapping ends the $s_j : S_j$. The $tk : Tk$ are created mapping ends of $r_i\text{Matching}$, and updated ends of $r_i\text{Initialisation}$. The input conditions $S\text{Cond}$ are translated to a condition conjunct $S\text{Cond}'$ of $r_i\text{Matching}$ and $r_i\text{Initialisation}$. Any using variables are expressed by a conjunct $vt = valt'$ of the condition. The output variables become exists-quantified variables of the relations of the $r_i$ mappings. If an action block $Stat$ is specified, then a new update operation $opi(s_2 : S_2, ..., sm : Sm, t_1 : T_1, ..., tk : Tk)$ is introduced, this operation has activity given by the interpretation $Stat'$ of $Stat$ as a UML activity. The resulting relation of $r_i\text{Matching}$ has context $S_1$ and predicate

$$T_1 \rightarrow \exists (t_1 | t_1.id = \$id) \text{ and ... and } T_k \rightarrow \exists (tk | tk.id = \$id)$$

This creates target model elements corresponding to the source model elements that satisfy $S\text{Cond}'$, and establishes tracing relations from $s_1$ to $t_1$, ..., $tk$ by assignment of an identifier attribute $\$id$, which is added to each root class of the source or target metamodels. The relation of $r_i\text{Initialisation}$ has context $S_1$ and predicate

$$T_1 \rightarrow \exists (t_1 | t_1.id = \$id \text{ and } ... \text{ and } T_k \rightarrow \exists (tk | tk.id = \$id \text{ and } T\text{Cond}_1' \text{ and } ... \text{ and } T\text{Cond}_k' \text{ and } s_1.opi(s_2, ..., tk)))$$

In this rule the previously created $t_j$ corresponding to $s_1$ are look-uped and their features initialised. Lazy rules $r$ with first input entity type $S_1$ are translated to operations $opi$ of $S_1$. Calls $this\text{Module}.r(v_1, ..., vm)$ to the rule are interpreted as calls $v_1.rop(v_2, ..., vm)$ of this operation. The operation $rop$ is stereotyped as $\ll \text{cached} \gg$ in the case of unique lazy rules$^2$. All $r_i\text{Matching}$ rules are listed

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
ATL element & Transformation metamodel representation \\
\hline
Module & TransformationSpecification \\
\hline
Matched rule & Mapping(s) \\
\hline
Lazy rule & Operation invoked from mapping constraint \\
\hline
Unique lazy rule & Operation using caching to avoid re-application \\
\hline
Implicit rule invocation & Object lookup using object indexing or traces \\
\hline
Using variable & Variable defined in mapping condition \\
\hline
Functional helper & Query operation \\
\hline
Attribute helper & Operation defining navigation expression \\
\hline
Action blocks & Operation with activity, invoked from mapping constraint \\
\hline
\end{tabular}
\caption{Mapping of ATL to $TMM$}
\end{table}

$^2$ Iterative target patterns are not treated by this translation. These are a deprecated feature of ATL since ATL 2.0.
before all the $r_{Initialisation}$ rules in $M’$. The translation from ATL to $\mathcal{TMM}$ can be extended to update-in-place transformations, i.e., to the refining mode of ATL (ATL 2010 version). The translation from ATL to $\mathcal{TMM}$ has been implemented in the UML-RSDS tools [11].

The translated transformation in $\mathcal{TMM}$ represents the usual execution semantics of the ATL transformation, in which target objects are created in a first phase, followed by links between objects [6]. Thus every computation of the translated specification corresponds to a computation of the original specification. The computation steps (rule applications) of the translation correspond to the steps of the original specification, so any invariant of the translation will also be an invariant of the original.

Using B, syntactic correctness can often be proved by using invariants of the transformation to relate the target model to the source model. Thus a proof of syntactic correctness of this kind also demonstrates syntactic correctness for the original transformation. Similarly, model-level semantic preservation can often be shown by invariant-based reasoning, which can be transferred from the translated specification to the original.

A counter-example produced by Z3 or another satisfaction-checking tool gives a pair $(m, n)$ of a source and target model which can result from completed execution of the translated transformation, and where $n$ violates some constraint of $T$. Such a pair is also a counter-example to syntactic correctness of the original ATL transformation. For refining mode transformations, termination and confluence of the translated specification establishes these properties of the original specification.

5 Evaluation

In this section we evaluate the approach by considering two example case studies: the simple UML to relational database example from the ATL Zoo, and the refactoring transformation of [7]. We use an imperative version of the UML to relational database ATL transformation. This has three lazy rules and one matched rule with an action block:

```java
rule makeTable {
    from c : Entity ( c.generalisation->size() = 0 )
    to t : Table ( rdbname <- c.name )
    do {
        for ( att in c.ownedAttribute )
            { if ( att.isPrimary )
                { t.tcols->includes(thisModule.makePrimaryKeyColumn(att)); } }
        for ( att in c.ownedAttribute )
            { if ( att.type.oclIsKindOf(Entity) )
                { t.tcols->includes(thisModule.makeForeignColumn(att)); } }
        for ( att in c.ownedAttribute )
            { if ( att.type.oclIsKindOf(PrimitiveType) or att.isPrimary = false )
```


lazy rule makePrimaryKeyColumn {
    from p : Property ( p.isPrimary )
    to c : Column ( rdbname <- p.name, type <- p.type.name )
}

lazy rule makeForeignKeyColumn {
    from p : Property ( p.type.oclIsKindOf(Entity) )
    to c : Column ( rdbname <- p.name, type <- "String" ),
    f : FKey ( references <- p.type, fcols <- Set{ c } )
}

lazy rule makeColumn {
    from p : Property ( true )
    to c : Column ( rdbname <- p.name, type <- p.type.name )
}

The matched rule is translated to two constraints $C_0$ and $C_1$ with context $Entity$:

generalisation.size = 0 implies Table->exists( t | t.$id = $id and t.rdbname = name )

generalisation.size = 0 implies Table->exists( t | t.$id = $id and self.makeTable1op(t) )

$C_1$ has the condition and relation of $makeTableMatching$, and creates table objects and sets their attribute values. $C_2$ has the condition and relation of $makeTableInitialisation$, and looks up table objects using the introduced primary key $\$id$ and creates and links columns to the tables. $makeTable1op(t)$ carries out the procedural code of $makeTable$’s action block, invoking operations $makePrimaryKeyColumnop$, $makeForeignKeyColumnop$ and $makeColumnop$ of $Property$ corresponding to the lazy rules. For example:

$makeColumnop()$: Column
post:
    Column->exists( c | c.$id = $id and c.rdbname = name and
c.type = type.name and result = c )

Figure 3 shows an example of data-dependency analysis on the translated specification. Verification properties of interest for this case study include: (i) termination; (ii) confluence (meaning that semantically equivalent source models are always mapped to equivalent target models); (iii) that the columns of the foreign keys are always contained in the set of columns of the tables, formalised as the transformation invariant $fcols \subseteq Table.tcols$ on $FKey$.

For this specification (i) can be shown by data-dependency analysis, establishing that a bounded iteration implementation is sufficient for $C_0$ and $C_1$. (ii)
fails because the association end Table :: tcols is ordered, so that different representations of the same input model may result in semantically distinct result models. Proof of (iii) can be carried out by establishing it as a transformation invariant in B. Table 3 shows the results of verification for the transformation. Atelier B version 4.0 was used.

<table>
<thead>
<tr>
<th>Property</th>
<th>ATL via TMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Termination</td>
<td>By data-dependency analysis</td>
</tr>
<tr>
<td>Foreign key columns contained in table columns</td>
<td>20 proof obligations,</td>
</tr>
<tr>
<td></td>
<td>15 automatically proved</td>
</tr>
</tbody>
</table>

Table 3. Proof effort for refinement transformation

The refactoring transformation of [7] is an update-in-place transformation operating on simplified UML class diagrams. It removes apparent attribute clones from the diagram by applying ‘pull up feature’ refactorings. We use the extended version of ATL refining mode supported by our translator, to define an ATL solution with a single rule. For this transformation, there are several required correctness properties that should be verified: (i) termination; (ii) preservation of the property of single inheritance, formalised as the invariant $generalisation \rightarrow size() \leq 1$ on $Entity$; (iii) preservation of the property of no attribute name conflicts within classes, formalised as the invariant $ownedAttribute \rightarrow isUnique(name)$ of $Entity$.

Since the transformation involves fixed-point iteration, termination is shown by proving that $Property.allInstances() \rightarrow size()$ is a variant, i.e., that the number of $Property$ instances in the model is always strictly decreased by applying the transformation rule. Table 4 shows the results of verification for the transformation.

<table>
<thead>
<tr>
<th>Property</th>
<th>ATL via TMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Termination</td>
<td>6 proof obligations, 5 automatically proved</td>
</tr>
<tr>
<td>Single inheritance</td>
<td>13 proof obligations, all automatically proved</td>
</tr>
<tr>
<td>No name conflicts</td>
<td>15 proof obligations, 13 automatically proved</td>
</tr>
</tbody>
</table>

Table 4. Proof effort for refactoring transformation

6 Related work

In [2], techniques for the forward engineering of ATL and other MT language specifications from a platform-independent transformation representation are defined. The focus is on development of new transformations rather than upon the reverse-engineering and verification of existing transformations. We explicitly
represent the semantics of the MT languages within our language-independent representation, including execution phases and the mechanism of target element lookup/implicit rule invocation. Such semantic representation is not detailed in [2]. In contrast to the ATL to OCL translations of [3, 4], we define a behavioural representation of ATL transformations, capturing the semantics of transformation computation steps (individual rule applications), instead of a static post-state relation. This permits analysis of invariants and other behavioural properties.

7 Conclusion

We have outlined a language-independent approach for model transformation verification, and illustrated this approach by applying it to ATL. We also intend to apply this approach to other hybrid MT languages, such as ETL, Flock, GrGen.NET and QVT-O.

References

12. K. Lano, Null considered harmfull (for transformation verification), VOLT 2014.