Declarative Specification of Bidirectional Transformations Using Design Patterns

KEVIN LANO1, SHEKOUFEH KOLAHDOUZ-RAHIMI2, AND SOBHAN YASSIPOUR-TEHRANI1

1Department of Informatics, King’s College London, London WC2B 4BG, U.K.
2Department of Software Engineering, University of Isfahan, Isfahan 81746-73441, Iran

Corresponding author: Kevin Lano (kevin.lano@kcl.ac.uk)

ABSTRACT Bidirectional transformations (bx) are a specific form of model transformation (MT) used in model-driven engineering to maintain consistency between two models, which may change independently. Currently bx are defined using a number of specialized transformation languages, which have had limited uptake due to complex semantics and poor efficiency. In contrast, unidirectional transformation languages such as ATL have been widely adopted, but require separate forward and reverse transformations to be written to address model synchronization requirements. In this paper, we provide declarative specification techniques for bx, systematically constructed using MT design patterns. We define two approaches to declarative bx definition: 1) by automatically bidirectionalizing unidirectional transformation specifications and 2) by developing specification guidelines for the QVT-R standard language to make it more effective for bx in practice. The approaches are evaluated using a large-scale code-generator bx from UML to ANSI C and other examples. Their semantic validity is demonstrated by rigorous arguments.

INDEX TERMS Bidirectional transformations, design patterns, model transformations, QVT-R, UML-RSDS.

I. INTRODUCTION

Model-driven engineering (MDE) and Model-based development (MBD) have reached a point of significant application in industry, particularly in the automotive industry and more recently in finance. These development approaches use models (such as UML class diagrams) as key artifacts within their processes. In some cases the models are used as the complete definition of an application, with executable code being generated automatically from the models.

Model transformations (MT) are a key element of MDE and MBD approaches for software, supporting code generation, migration, refinement, reverse-engineering and many other capabilities. Bidirectional model transformations (bx) are a specific type of MT which provide a means to maintain a consistency relation \( R \) between two models which may both change. This is in contrast to unidirectional transformations, which establish \( R \) by constructing a target model from a source model, and do not subsequently maintain the consistency of these models.

Bx are significant for a wide range of model based engineering scenarios involving model synchronization:
- Incremental execution of transformations, for example, it is desirable for a code generator to only make the minimal necessary changes to generated code if a source model is changed, rather than regenerating the entire code set again.
- Round-trip engineering [28], where either an application specification or design may change and the consistency of the two models at different levels of abstraction must be automatically maintained.
- Automatic consistency maintenance of multiple inter-related models at the same level of abstraction [18], such as UML class diagrams and sequence diagrams, to support agility in model-based development.
- Application and database co-evolution [5].

The motivating case for this paper was a code generator from UML to ANSI C [44]. For realistic applications involving large-scale models with thousands of elements, incremental code generation of C is a practical necessity. Additionally, the use of a bx in this case is motivated by considerations of semantic correctness of the generated code, and by the desirability of round-trip engineering capabilities.

A bx can be used to enforce a relation \( R \) between two different representations of similar semantic information. For example, a UML class and a corresponding ANSI C struct. Such a bx is responsible for ensuring that changes to one of these representations is propagated to the other to maintain their mutual consistency. There may however be additional...
information in one model which has no counterpart in the other. For example, in the well-known Families to Persons bx benchmark [1], the persons model includes birthday information, whilst the families model differentiates parents and children. These features are specific to just one of the linked models.

In the theoretical framework of [59], bx are characterized by a binary relation $R : SL \leftrightarrow TL$ between a source language (metamodel) $SL$ and a target language $TL$. $R(m, n)$ holds for a pair of models $m$ of $SL$ and $n$ of $TL$ when the models consist of data which correspond under $R$.

The key idea of a bx is that instead of defining two separate transformations from $SL$ to $TL$ and from $TL$ to $SL$, to establish $R$, it should be possible to automatically derive from the definition of $R$ both forward and reverse transformations

$$R^{-} : SL \times TL \rightarrow TL$$

$$R^{+} : SL \times TL \rightarrow SL$$

which establish/maintain $R$ between the two models, given both existing source and target models. This eliminates the risk that forward and reverse transformations could become inconsistent with each other, and reduces the workload involved in maintaining two separate transformation specifications instead of one.

The $R^{-}$, $R^{+}$ transformations should satisfy two key conditions [46], [59]:

1) **Correctness**: the forward and reverse transformations derived from a relation $R$ do establish $R$:

$$R(m, R^{-}(m, n))$$

$$R(R^{+}(m, n), n)$$

for each $m : SL$, $n : TL$.

2) **Hippocraticness**: if source and target models already satisfy $R$ then the forward and reverse transformations do not modify the models [48]:

$$R(m, n) \Rightarrow R^{-}(m, n) = n$$

$$R(m, n) \Rightarrow R^{+}(m, n) = m$$

for each $m : SL$, $n : TL$.

Hippocraticness is a global property, in practice a stronger local property is desirable: if any part of a target (source) model is already consistent with the corresponding part of the source (target) model, then neither part should be modified by forward or reverse transformations. We refer to this as local Hippocraticness. Further, it is preferable that updates to a model by $R^{-}$ or $R^{+}$ should be minimal necessary to restore $R$: this is termed the principle of least change [48].

In the following, we will consider only separate-models transformations, where source and target models are distinct, and not update-in-place transformations, which operate on a single model which is both the source and target.

We describe two alternative approaches to bx definition:

1) In the first approach, unidirectional separate-models transformations $\tau$ are defined declaratively using the Object Constraint Language (OCL) [52], and a bx relation $R$ and forward and reverse transformations $R^{-}$, $R^{+}$ are derived syntactically from the specification of $\tau$.

We consider specifically the unidirectional MT language UML-RSDS [42].

2) In the second approach, a bx $\tau$ is defined using a restricted subset of QVT-R [51], with the specification of $\tau$ organized so that both $R^{-}$ and $R^{+}$ exist and satisfy the bx properties wrt $R$ derived from the specification.

An original contribution of our work is an emphasis on the role of design patterns in the definition of $\tau$ in order to achieve bx properties.

Section II describes related work, Section III describes UML-RSDS, Section IV describes model transformation and bx design patterns, and Section V defines our approach to bx specification in UML-RSDS. Section VI considers inverse transformations and the bx properties of $R^{-}$. Section VII describes a large case study of a bx transformation between UML and C. Section VIII describes our QVT-R based approach to bx definition. Section IX gives an evaluation of the approaches, and Section X gives conclusions. The appendix provides an argument that the bx properties for $R^{-}$ are satisfied by transformations defined using our first approach.

II. RELATED WORK

Bx are the subject of extensive theoretical research [10], [12], [46], [58]–[60] and an annual conference, BX. The most well-known transformation language which supports definition of bx is QVT-R [51], which uses an OCL-based expression language. However, QVT-R has had limited uptake because of its complex semantics and specification style, compared to simpler unidirectional MT languages such as ATL [31] and ETL [33]. The semantic basis of the language remains unclear [8], [46], [60]. The combination of bx and update-in-place processing involves aspects such as implicit deletion (if an element is not required to exist by any rule, then it is deleted), which are difficult to use, and are implemented differently by different QVT-R tools [8], [40]. Although the language is intended to be declarative, the meaning of a specification can depend on procedural aspects (rule invocation relationships) in addition to logical predicates. As the examples of [46] show, this leads to specifications which are difficult to understand and liable to subtle errors.

Triple Graph Grammars (TGG) are a graph transformation-based formalism which supports bx definition [14], although with a restricted expression language compared to OCL. Other approaches, such as JTL [11], and extensions of TGG [2], use constraint-based programming techniques to interpret relations $P(s, t)$ between source and target elements as specifications in both forward and reverse directions. Model finding using Alloy is used to bidirectionalize ATL in [46], and to backward propagate view changes in [58]. These approaches have problems of efficiency for large-scale models. An alternative constraint-based approach
is to generate constraints restricting target models, instead of the models themselves [13]. This allows greater freedom of choice in the construction of the target model, but requires an additional step to actually derive specific models.

Another research direction has focused on the special case of asymmetric bx known as lenses, in which the source to target mapping is independent of the existing target model. The target model \( f : TL \) is computed as a view or abstraction \( \text{get}(s) \) containing partial information from the source model \( s : SL \) [6], [15]. A dual map \( \text{put} : SL \times TL \rightarrow SL \) propagates view changes to the source, such that \( \text{put}(s, \text{get}(s)) = s \) and \( \text{get}(\text{put}(s, t)) = t \). Various semantic and syntactic techniques have been developed for deriving the put function from get in different cases [34], [61].

In previous papers we have briefly introduced some bx design patterns [39] and techniques for bx verification [41]. In this paper we extend these previous works by comprehensively defining an approach to bx specification using UML-RSDS, and we identify additional bx patterns. We also introduce an approach using QVT-R with the bx patterns. We provide rigorous arguments to show the correctness of the UML-RSDS approach, provide an evaluation, and give new examples and extensive details of a large case study.

III. UML-RSDS

In our first approach to bx definition, we look at an unidirectional MT language, UML-RSDS. In this approach, unidirectional transformations \( \tau \) are specified using UML use cases with OCL postconditions \( Post_\tau \) and invariants \( Inv_\tau \). We then statically-computed bx relation \( R_\tau \) for \( \tau \) is defined as \( Post_\tau \land Inv_\tau \) for \( \tau \), together with a forward transformation \( \tau^+ \) extending \( \tau \), and an inverse \( \tau^- \) of \( \tau^+ \). These play the role of \( R^+ \) and \( R^- \) in bx theory. The bx relation and transformations are derived from \( \tau \) using a higher-order transformation. This is generally more efficient than the use of constraint programming and model finding.

UML-RSDS is a precise subset of UML 2 and OCL 2.4, with a formal semantics [35] and an established toolset [36], [42]. We use a variant notation for OCL, with \( E.allInstances() \) abbreviated to \( E \) for entity types on the lhs of a \( \rightarrow \) operator. \( x : s \) is used for \( s \rightarrow \text{includes}(x) \), \( s1 <: s2 \) for \( s2 \rightarrow \text{includesAll}(s1) \), & is used for conjunction, \( \implies \) for implication.1 Logical expressions \( P \) may be used operationally, to stand for behaviors \( \text{stat}_{LC}(P) \) which establish \( P \) (Section III-C). In particular, the predicate \( x \rightarrow \text{isDeleted}() \) is used to express that the element \( x \) is to be removed from all entity types and other collections in which it resides. \( s \rightarrow \text{isDeleted}() \) for collection \( s \) means \( s \rightarrow \text{forall}(\text{forAll}(x \rightarrow \text{isDeleted}())) \). The general iterate operator is excluded from our subset, as are tuples and invalid. null cannot be explicitly referred to, but only tested using \( x \rightarrow \text{oclIsUndefined}() \).

A. TRANSFORMATION SPECIFICATION

Model transformations \( \tau \) are specified in UML-RSDS as UML use cases, defined declaratively by two main predicates, expressed in our OCL variant:  

1) Postconditions \( Post_\tau \) which define the intended effect of the transformation at its termination. These are an ordered conjunction \( \text{C}_1 \land \ldots \land \text{C}_n \) of OCL constraints (also termed rules [52]) in the following and also serve to define a procedural implementation of the transformation.

2) Invariants \( Inv_\tau \) which define expected invariant properties which should hold during the transformation execution (their truth is preserved by individual transformation rule applications). The invariants can be derived from \( Post_\tau \), or can be specified explicitly by the developer.

From a declarative viewpoint, \( Post_\tau \) defines the conditions which should be established by the transformation. From an implementation perspective, the constraints of \( Post_\tau \) also define the intended computation steps of the transformation: each computation step is an application of a postcondition constraint (transformation rule) to a specific source model element or to a tuple of source model elements. The computation steps should preserve \( Inv_\tau \).

A typical postcondition constraint/rule has the form:

\[
S_i :: \quad \text{Cond} \implies \text{Pred}
\]

where \( S_i \) is the context entity type of the constraint, \( \text{Cond} \) is the application condition of the constraint, and \( \text{Pred} \) its predicate or succedent. The logical meaning of the constraint is that for each instance \( \text{self} \) of \( S_i \) which exists in the source model, if \( \text{self} \) satisfies \( \text{Cond} \), then \( \text{Pred} \) is true for \( \text{self} \). The operational meaning of the constraint is that for each instance \( \text{self} \) of \( S_i \) which exists in the source model, if \( \text{self} \) satisfies \( \text{Cond} \), then \( \text{Pred} \) is made true for \( \text{self} \), using the activity \( \text{stat}_{LC}(\text{Pred}) \).

Typically, \( \text{Pred} \) will specify the existence of instances \( t \) of target entity types \( T_j \) via formulae \( T_j \rightarrow \text{exists}(t|P) \) for concrete entity type \( T_j \), where \( t \)’s feature values are specified in \( P \).

For example, the simple Families to Persons [1] forward transformation \( \text{family2person} \) (Figure 1 shows the basic metamodels of this transformation) could have two rules:

**Family::**

- \( m : \text{mother} \rightarrow \text{union}(\text{daughters}) \) =>  
  - \( \text{Female} \rightarrow \text{exists}(p | \ 
p.\text{name} = \text{name} + \ "\, \, " \ + \text{m.name} ) \)

**Family::**

- \( m : \text{father} \rightarrow \text{union}(\text{sons}) \) =>  
  - \( \text{Male} \rightarrow \text{exists}(p | \ 
p.\text{name} = \text{name} + \ "\, \, " \ + \text{m.name} ) \)

These rules \( Post_{\text{family2person}} \) express that for each \( \text{Family} \) instance, and for each \( \text{FamilyMember} \) \( m \) which is either a father or son of the family, there should exist a corresponding \( \text{Male} \) instance with a name formed as the concatenation of
the family and family member names. Likewise, mothers and daughters are mapped to Female instances. The invariants \( \text{Inv}_{\text{family2person}} \) can be derived syntactically from these rules by inverting the quantifiers (Table 5, case 2):

Female::
- Family->exists( fx | FamilyMember->exists( m | m : fx.mother->union(fx.daughters) & name = fx.name + ", " + m.name ) )

Male::
- Family->exists( fx | FamilyMember->exists( m | m : fx.father->union(fx.sons) & name = fx.name + ", " + m.name ) )

These invariants are preserved by the \( \text{family2person} \) rules: if a new Female instance is created by the first rule, then it necessarily satisfies the first invariant because of the context entity type and application conditions of the rule. The new instance does not affect the truth of the second invariant, which only restricts Male instances. Likewise, the second rule preserves both invariants.

The importance of transformation invariants in verification is that they can be used to prove transformation contracts: conditions \( P \) and \( Q \) such that, if transformation \( \tau \) is executed on models satisfying \( P \), it is ensured to terminate in a state with the models satisfying \( Q \) [7], [19]. If \( I \) is a condition such that \( P \) implies \( I \), with \( I \) preserved by each rule application of \( \tau \), and such that \( I \) together with the fact that no rule is enabled implies \( Q \), then the correctness part of the contract is established.

The key idea of our first bx approach is that change-propagation from the source model to the target can be achieved by extending a forward transformation \( \tau \) by additional constraints/rules derived automatically from \( \text{Inv}_\tau \). In addition, a reverse transformation \( \tau^- \) can also be derived automatically from \( \text{Inv}_\tau \). The reverse transformation is based on interpreting the invariants as rules in the inverse direction (notice that the form of the invariants in the \( \text{family2person} \) example is very similar to that of use case postconditions).

A rule predicate \( P \) such as \( t\text{.name} = s\text{.name} + "*" \) is converted to an explicit inverse form \( P^- \) such as \( s\text{.name} = t\text{.name}.front \) in order to provide a computationally explicit version of the invariants. This approach therefore achieves the aims of bx in enabling a single transformation specification to be used for both forward and reverse transformations.

B. TRANSFORMATION IMPLEMENTATION

Designs for model transformations and for general applications are defined in UML-RSDS using class diagrams, with UML activities expressing the explicit algorithms of operations and use cases.

The following concrete syntax is used for a subset of UML structured activities:

\[
\begin{align*}
\text{< statement> ::= } & \text{< loop> | < creation> |} \\
& \text{< conditional> |} \\
& \text{< sequence> | < choice> |} \\
& \text{< basic>}
\end{align*}
\]

\[
\begin{align*}
\text{< conditional> ::= } & \text{< if> | < expression> |} \\
& \text{< then> | < statement> |} \\
& \text{< else> | < basic>}
\end{align*}
\]

\[
\begin{align*}
\text{< sequence> ::= } & \text{< statement> |<;> < statement> |} \\
\text{< choice> ::= } & \text{< statement> |<][> < statement> |} \\
\text{< creation> ::= } & \text{< expression> |<identifier> |<;> < identifier> |} \\
\text{< basic> ::= } & \text{< expression> |<;> < expression> |} \\
& \text{< return> |} \\
& \text{< execute> |<;> < expression> |}
\end{align*}
\]

For use cases, their procedural implementation as an activity is derived as a composition of the activities \( \text{stat}_{LC}(Cn) \) for each postcondition constraint \( Cn. \text{stat}_{LC}(Cn) \) is constructed.

FIGURE 1. Family to Person metamodels.
so that it establishes \( Cn: \{ \text{stat}_{LC}(Cn) \} Cn \), where \( \{ \text{act} \} P \) is the weakest-precondition of predicate \( P \) with respect to statement/activity \( \text{act} \). As a predicate transformer, \( \text{stat}_{LC}(Cn) \) is chosen as a minimal (least-refined) transformer which establishes \( Cn \). In terms of the refinement calculus \([50]\):

\[
[C]P \iff (\text{stat}_{LC}(P) \subseteq C)
\]

for statements \( C \) which do not update more variables than \( \text{stat}_{LC}(P) \). Intuitively, this means that \( \text{stat}_{LC}(P) \) performs the minimal necessary data modifications needed to establish \( P \), operating on the write frame \( wr(P) \) of \( P \). A definition of \( \text{stat}_{LC} \) is given in Section III-C. There may not be a unique least-refined statement that establishes a given predicate, in such cases a suitable minimally-refined statement is selected instead.

Data-dependency relations between the \textit{Post} constraints are important in ensuring the correctness of both unidirectional and bidirectional UML-RSDS transformations. Let \( rd(Cn) \) denote the read-frame of a constraint \( Cn \), the set of entity type names and data features that it reads, and \( wr(Cn) \) denote its write frame. These are defined in \([36]\). The definition of \( wr(P) \) for a predicate \( P \) interpreted operationally as \( \text{stat}_{LC}(P) \), includes features and entity types affected by implicit updates which may arise due to metamodel constraints involving parts of the metamodel explicitly updated by \( \text{stat}_{LC}(P) \). There are five main cases of such implicit updates:

1. A bi-directional association \( A \) with multiplicities \( m1_{ar}, m2_{br} \) between entity types \( A \) and \( B \), for any multiplicities \( m1, m2 \); changes to \( ar \) will also produce updates to \( br \) and vice-versa.
2. An association \( A \) with multiplicities \( m1_{br} \) between entity types \( A \) and \( B \); deletion of \( B \) instances will remove these from \( br \).
3. An association \( A \) with multiplicities \( m2_{br} \) between entity types \( A \) with a 1-multiplicity end at entity type \( A \): deletion of \( A \) instances \( ax \) will result in deletion of all \( B \) instances linked to \( ax \) via \( br \). For example, in Figure 1, deletion of a \textit{Family} instance leads to deletion of its linked \textit{FamilyMembers}.
4. A composition or aggregation: deletion of the composite will result in deletion of its linked parts.
5. Creation or deletion of instances of a subclass \( B \) of a class \( A \) will also result in addition/removal of these instances from the extent of \( A \).

In Figure 1, deletion of \textit{Family} instances will also affect \textit{FamilyRegister} \( :: \) \textit{families}, even though this feature is not explicitly modified by the transformation. Likewise for \textit{Person} and \textit{PersonRegister} \( :: \) \textit{persons}. We say that there is deletion propagation from entity type \( E_i \) to entity type \( E_j \) if there is a non-empty chain of dependencies of kinds 3, 4 and 5 above between \( E_i \) and \( E_j \) such that deletion of an \( E_i \) instance may cause deletion of an \( E_j \) instance.

A dependency ordering \( Cn < Cm \) is defined between constraints by \( wr(Cn) \cap \overline{rd(Cm)} \neq \emptyset \) “\( Cm \) depends on \( Cn \)”. A use case with postconditions \( C_1, \ldots, C_n \) should satisfy the syntactic non-interference conditions:

1. If \( C_i < C_j \), with \( i \neq j \), then \( i < j \).
2. If \( i \neq j \) then \( wr(C_i) \cap wr(C_j) = \emptyset \).

Together, these conditions ensure that the activities \( \text{stat}_{LC}(C_i) \) of subsequent constraints \( C_j \) cannot invalidate earlier constraints \( C_i \), for \( i < j \).

A constraint is termed a type 1 constraint if its write and read frames are disjoint. Such constraints usually have an implementation as a bounded loop, as opposed to a fixed-point/unbounded iteration. Both of the rules for \textit{Family} to \textit{Person} above are of type 1.

Entity types may have \textit{identity} attributes of \textit{String} type. These uniquely identify instances of the entity: two different instances must have different values of the attribute. The first such attribute is used as a primary key for the entity type.

If entity type \( E \) has a primary key \( \textit{att} : \textit{String} \), then \( E[\textit{v}] \) denotes the instance \( x \) of \( E \) with key value \( x.\textit{att} \) equal to \( v \), or the collection of \( E \) instances with key value in \( v \), if \( v \) is a collection.

### C. Definition of Activities for Predicates

Table 1 gives the definition of \( \text{stat}_{LC} \) for simple predicates.

<table>
<thead>
<tr>
<th>Predicate ( P )</th>
<th>( \text{stat}_{LC}(P) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x = e )</td>
<td>( x := e )</td>
</tr>
<tr>
<td>( e : x ) (Assignable basic expression ( x ))</td>
<td>( x := x \rightarrow \text{including}(e) )</td>
</tr>
<tr>
<td>( e : x ) (Set-valued)</td>
<td>( \text{if } x \rightarrow \text{includes}(e) ) then skip else ( x := x \rightarrow \text{append}(e) )</td>
</tr>
<tr>
<td>( e / : x ) (Sequence-valued)</td>
<td>( x := x \rightarrow \text{excluding}(e) )</td>
</tr>
<tr>
<td>( e &lt;: f ) (For ( x : e ) do)</td>
<td>( \text{for } x : e \rightarrow \text{stat}_{LC}(x, f) )</td>
</tr>
<tr>
<td>( e / &lt;: f ) (Assignable basic expression ( f ))</td>
<td>( f := f - e )</td>
</tr>
</tbody>
</table>

An assignable basic expression \( x \) is either a variable, a non-frozen feature \( f \) or a basic expression \( obj.f \) or \( obj[f[i] \) whose modified feature \( f \) is non-frozen. \( \text{stat}_{LC}(x \rightarrow \text{includes}(e)) \) is the same as \( \text{stat}_{LC}(e : x) \), and likewise \( x \rightarrow \text{excludes}(e) \) is considered the same as \( e / : x \) and \( x \rightarrow \text{includesAll}(e) \) the same as \( e <: x \).

\( \text{stat}_{LC}(\text{true}) \) is \( \text{skip} \). For \( x \rightarrow \text{isDeleted}() \), where \( x \) is an instance of class \( E \), \( \text{stat}_{LC} \) removes \( x \) from the set of instances of \( E \), and performs all the deletion propagation actions from \( E \) listed in the preceding subsection.

\( \text{stat}_{LC}(P \ & \ Q) \) is \( \text{stat}_{LC}(P) \ & \ \text{stat}_{LC}(Q) \) under the assumption that \( P \iff [\text{stat}_{LC}(Q)]P \).
form: with primary key value

createByPKE

e

e

For existential quantifiers $E \rightarrow \exists (e|P_1 \& \ldots \& P_n)$, their $stat_{LC}$ effect only creates a new $e : E$ instance in cases where there is no existing $e : E$ that satisfies $P$ partially or completely. In the case of partial satisfaction the updates only for the unsatisfied conjuncts are carried out.

If $E$ has a primary key $pk$ and a conjunct $P_i$ is of the form $e.pk = value$, then $stat_{LC}(E \rightarrow \exists (e|P_1 \& \ldots \& P_n))$ is

$$\begin{align*}
\text{var } e & : E; \\
\text{e} & := \text{createByPKE(value)}; \\
\text{stat}_{LC} & (\text{Pred})
\end{align*}$$

Where $\text{Pred}$ is $P_1 \& \ldots \& P_n$ with $P_i$ omitted. $\text{createByPKE(val)}$ looks up $E[val]$, if this is non-null it returns the instance, otherwise it creates a new $E$ instance with primary key value $val$, and returns this instance.

Otherwise, $stat_{LC}(E \rightarrow \exists (e|P_1 \& \ldots \& P_n))$ has the form:

$$\begin{align*}
\text{var } e & : E; \\
\text{var eset : Set(E);} \\
\text{eset} & := E.\text{allInstances}(); \\
\text{if } \text{eset} \rightarrow \text{isEmpty}() & \text{then} \\
\text{e} & := \text{createE}(); \\
\text{stat}_{LC} & (P_1 \& \ldots \& P_n) \\
\text{else} & \\
\text{(e} & := \text{eset} \rightarrow \text{any}(); \\
\text{eset} & := \text{eset} \rightarrow \text{select}(P_1); \\
\text{if } \text{eset} \rightarrow \text{isEmpty}() & \text{then} \\
\text{e} & := \text{createE}(); \\
\text{stat}_{LC} & (P_1 \& \ldots \& P_n) \\
\text{else} & \\
\text{(e} & := \text{eset} \rightarrow \text{any}(); \\
\text{eset} & := \text{eset} \rightarrow \text{select}(P_2); \\
\text{if } \text{eset} \rightarrow \text{isEmpty}() & \text{then} \\
\text{stat}_{LC} & (P_2 \& \ldots \& P_n) \\
\text{else} & \\
\ldots & \text{case for 3 \ldots})
\end{align*}$$

The general case for $k \geq 2, k < n$ is

$$\begin{align*}
\text{e} & := \text{eset} \rightarrow \text{any}(); \\
\text{eset} & := \text{eset} \rightarrow \text{select}(P_k); \\
\text{if } \text{eset} \rightarrow \text{isEmpty}() & \text{then} \\
\text{stat}_{LC} & (P_k \& \ldots \& P_n) \\
\text{else} & \\
\ldots & \text{case for } k + 1 \ldots
\end{align*}$$

For $k = n$, if $P_k$ is an assignment $\text{result} = e$, then the code of the case is simply $e := \text{eset} \rightarrow \text{any}(); \text{result} := e$. Otherwise it is

$$\begin{align*}
\text{e} & := \text{eset} \rightarrow \text{any}(); \\
\text{eset} & := \text{eset} \rightarrow \text{select}(P_n); \\
\text{if } \text{eset} \rightarrow \text{isEmpty}() & \text{then} \\
\text{stat}_{LC} & (P_n) \\
\text{else} & \\
\text{e} & := \text{eset} \rightarrow \text{any}()
\end{align*}$$

By reusing $e : E$ instances where possible, the redundant creation of instances is avoided, however this also introduces the possibility of conflicts where one target instance is required to have conflicting attribute values to satisfy a constraint wrt 2 source instances.

### IV. PATTERNS FOR MODEL TRANSFORMATIONS

In [38] we identified 29 design patterns which have been used for model transformation specification and design. According to [43], some of the most widely-used MT patterns in practice are Entity Splitting, Structure Preservation, Map Objects before Links and Entity Merging. Our approach to bx specification using UML-RSDS applies to transformations $\tau$ constructed using these patterns and others, and enables the automatic derivation of inverse transformations $\tau^\rightarrow$ which also use the patterns, according to Table 2.

### TABLE 2. Correspondence of MT patterns.

<table>
<thead>
<tr>
<th>Pattern in $\tau$</th>
<th>Pattern in $\tau^\rightarrow$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Splitting</td>
<td>Entity Merging</td>
</tr>
<tr>
<td>Entity Merging</td>
<td>Entity Splitting</td>
</tr>
<tr>
<td>Map Objects before Links</td>
<td>Map Objects before Links</td>
</tr>
<tr>
<td>Structure Preservation</td>
<td>Structure Preservation</td>
</tr>
<tr>
<td>Phased Construction</td>
<td>Phased Construction</td>
</tr>
<tr>
<td>Flattening</td>
<td>Unflattening</td>
</tr>
<tr>
<td>Unflattening</td>
<td>Flattening</td>
</tr>
<tr>
<td>Inverse Recursive Descent</td>
<td>Inverse Recursive Descent</td>
</tr>
</tbody>
</table>

Here we give a more precise characterization of the patterns, and explain their specialization for use in bx. In each case in the following patterns, the predicates $TCond, P$ contain no quantifiers or calls to update operations, and
have an operational interpretation statLC. They can contain calls of purely functional operations that do not create instances or modify data.

- **Structure Preservation**: a rule in which one source entity type $S_i$ is mapped to one target entity type $T_j$, with no dependency upon any other target entity types.

  Rules $C_i$ have the form

  $$ S_i ::
  SCond_i(self) \implies T_j \rightarrow \exists t(TCond_j(t) \land P_i(self, t)) $$

  where $SCond_i$ refers only to source model entity types and features. In the case of a bx, identity attributes $idS_i$ and $idT_j$ of the entity types can be used to correlate instances of $S_i$ and $T_j$.

- **Phased Construction**: as for Structure Preservation, but with previously-created instances of target entity types $TRef$, derived from $SRef$ instances being looked up in the succedent of a rule creating an instance of target entity $T_j$, in order to define the value of a $TRef$-typed role $rr$ of the $T_j$ instance, as in Figure 2. $P_j$ in this case contains some equation $t.rr = TRef[r.idSRef]$. For example:

  $$ S_i ::
  SCond_i(self) \implies T_j \rightarrow \exists t(t.rr = TRef[r.idSRef]) $$

  This can be used for single-valued $r$, $rr$ as well as for collection-valued association ends.

- **Entity Splitting**: this pattern involves one source entity type mapping to two or more different target entity types. There are two variants of this pattern: (i) horizontal: two or more separate rules map from $S_i$, with disjoint $SCond_i$ application conditions, to distinct target entity types $T_k$, $T_l$; (ii) vertical: a single rule maps one $S_i$ instance to multiple linked instances of different $T_k$, $T_l$.

  The second case is common in refinement transformations. Constraints, eg., $C_i$, will have the form

  $$ S_i ::
  SCond_i(self) \implies T_k \rightarrow \exists t_1 | T_l \rightarrow \exists t_2 | TCond_1(t_1) \land TCond_2(t_1, t_2) \land P(self, t_1, t_2)) $$

  Some explicit means of recording the semantic link between $t_1$ and $t_2$ is needed to support bx definition for such transformations, this link data can be based on identity attributes. This should be the only constraint in the transformation that creates $T_l$ instances. Other constraints can create $T_k$ instances if their $TCond$ conditions are disjoint from $TCond_1$.

- **Entity Merging**: As with Entity Splitting, there are two variants, which are inverses to the corresponding versions of Entity Splitting. In horizontal Entity Merging, two or more source entity types $S_i$, $S_j$ are mapped to the same target entity type $T_k$ by separate rules:

  $$ S_i ::
  SCond_i(self) \implies T_k \rightarrow \exists t(t | TCond_i(t) \land P_i(self, t)) $$

  and

  $$ S_j ::
  SCond_j(self) \implies T_k \rightarrow \exists t(t | TCond_j(t) \land P_j(self, t)) $$

  For bx, sufficient information must be inserted into the $T_k$ instances to enable the source entity of the instance ($S_i$ or $S_j$) to be identified. Usually $TCond_i$ and $TCond_j$ would be logically disjoint for this reason:

  $$ TCond_i \implies \neg(TCond_j) $$

  In vertical Entity Merging, two or more source instances are used to construct a single target instance, in a single rule:

  $$ S_i ::
  SCond_i(self) \land s_2 : S_2 \land SCond_2(self, s_2) \implies T \rightarrow \exists t(t | TCond(t) \land P(self, s_2, t)) $$

  This rule iterates over pairs $s_1 : S_1$, $s_2 : S_2$, potentially creating a $t : T$ instance for each pair that satisfies the antecedent conditions.

- **Map Objects before Links**: This pattern, also known as Entities before Relations [49], separates the construction of target instances from the linking of target instances based on source links (Figure 2).

![FIGURE 2. Map Objects before Links pattern.](image-url)
model elements \(T_i[idS_i]\) and \(TRef[v.idSRef]\) which have already been created by preceding entity mapping rule(s).

The Families to Persons transformation illustrates Entity Splitting (variant (i)). In the forward direction, FamilyMember instances are mapped to Male instances if they occur in the father or sons collections of some family, and to Female instances if they occur in the mother or daughters collections. This is an example of Entity Splitting variant (i): an instance of one source entity is mapped to one instance of possibly different alternative target entities under disjoint collections. This is an example of Entity Splitting variant (i):

We have also identified a number of specialized patterns for bx, based on inspection of published examples of bx [43]:

- **Auxiliary Correspondence Model**: using auxiliary entity types or features, maintain an explicit correspondence between source model and target model elements to facilitate change-propagation in source to target or target to source directions (Figure 3). This pattern is a built-in mechanism of the TGG language and has been used in numerous transformation cases [3], [16], [17], [21], [22], [24], [25], [27], [29], [32], [41], [55], [58], [67]. In QVT-R there are implicit trace entities for each relation [51].

- **Cleanup before Construct**: to enable change-propagation for \(R^-\), define additional rules that remove superfluous target model elements which are not in the bx relation \(R\) with any source elements, before constructing target elements related to source elements, and similarly for \(R^-\) (Figure 4). This pattern involves the introduction of additional rules, prior to the main rules of the transformation, to remove target elements which fail to correspond to source elements. Alternatively, cleanup actions can be performed after the main transformation, as with QVT-R delete actions [51].

- **Unique Instantiation for bx**: With this pattern, the \(E \rightarrow \exists s(e|P)\) quantifier in rule succeeds, for concrete entity type \(E\), is interpreted as “create a new instance \(e\) of \(E\) and establish \(P\) for \(e\), unless there already exists an \(e : E\) satisfying \(P^*\). This corresponds to the ‘check before enforce’ semantics for QVT-R [59].

As described in Section III-C, in the case that \(E\) has a primary key \(eld\), \(E \rightarrow \exists s(e|eld = v \& P)\) is interpreted as the sequence of steps: (i) lookup \(E[v]\), if this exists then assign it to \(e\), otherwise create a new \(E\) instance with \(eld = v\) and assign this to \(e\); (ii) try to establish \(P\) for \(e\), taking no action if \(P\) already holds.

This avoids the deletion and recreation of elements \(t\) in one model which correspond by key to an element \(s\) in the other model, but which have divergent data. Instead the data of \(t\) is modified to enforce the transformation relation.

If \(E\) does not have a primary key, then \(statLC\) \((E \rightarrow \exists s(e|P))\) selects an \(e : E\) for which a maximal initial part \(P_1\) of \(P\) holds and tries to establish the remainder of \(P\) for this \(e\), or it creates a new \(e\) and establishes \(P\) for it, if no element of \(E\) satisfies any initial part \(P_1\) of \(P\).

- **Lens**: the source to target mapping is independent of the target model data, with the target model \(t : TL\) computed as a view or abstraction \(get(s)\) containing partial information from the source model \(s : SL\) [15], [6]. A dual map \(put : SL \times TL \rightarrow SL\) propagates view changes to the source, such that \(put(s, get(s)) = s\) and \(get(put(s, t)) = t\).

Our approach to implement Auxiliary Correspondence Model is to introduce String-valued identity attributes (primary keys) for source and target entities. These attributes are used to record which source and target instances correspond: target instance \(t\) corresponds to source \(s\) if they have the same primary key values. For example, the person to family case would be extended by this pattern as shown in Figure 5.

In addition, we introduce here two new bx patterns, which we have used in a large-scale code generation transformation (Section VII):
Inverse Recursive Descent: if a forward transformation \( \tau \rightarrow \) is defined using structural recursion on the source language \( SL \), the reverse transformation \( \tau \leftarrow \) may be derived from \( \tau \rightarrow \) as a dual structural recursion on \( TL \) (Figure 6). If source entity \( E \) has subelements \( esub : \text{Collection}(ESub) \), and the corresponding target entity \( F \) has corresponding subelements \( fsub : \text{Collection}(FSub) \), then a forward rule

\[
E ::
true \rightarrow \text{self}.op1()
\]

based on operations \( op1 \) and \( op \) of \( E \) of the form

\[
E ::
op1() : \text{FSup}
pre : \text{true}
post :
result = op(esub.op1())
\]

\[
E ::
op(fs : \text{Collection}(FSub)) : F
pre : fs = FSub[esub.eld]
post :
ECond \rightarrow F \rightarrow \exists f \mid f.eld = fId & FCond(f) & f.fsub = fs & P(\text{self}, f) & \text{result} = f
\]

has the transformation invariant

\[
F ::
FCond \rightarrow E \rightarrow \exists e \mid e.eld = fId & ECond(e) & e.esub = ESub[fsub.fld] & P(e, \text{self})
\]

provided that \( F \) is only created/modified by \( op \).

The inverse operations for the reverse transformation are:

\[
F ::
op1^\sim() : \text{FSup}
pre : \text{true}
post :
\text{result} = op^\sim(\text{fsub}.op1^\sim())
\]

\[
F ::
op^\sim(es : \text{Collection}(ESub)) : E
pre : es = ESub[fsub.fld]
post :
FCond \rightarrow E \rightarrow \exists e \mid e.eld = fId & ECond(e) & e.esub = es & P^\sim(e, \text{self}) & \text{result} = e
\]
The operation \( op1^- \) is used in an inverse rule:

\[
F::
\text{true} \implies \text{self}.\text{op1}^(-)
\]

- **Flattening/Unflattening**: a special case of Entity Merging/Splitting where a nesting of components within a composite element is removed in the forward direction and restored in the reverse direction (Figure 7). A forward rule will have the form:

\[
E::
\begin{align*}
  f : & fs & F\text{Cond}(f) \implies \\
  G \implies & \exists(g) \text{gfld} = f.gld & \text{g.eld} = \text{eld} & \\
  & G\text{Cond}(g) & P(\text{self}, f, g))
\end{align*}
\]

The corresponding invariant is

\[
G::
\begin{align*}
  G\text{Cond}(self) \implies \\
  E \implies & \exists(e) \text{e.eld} = \text{eld} & \\
  F \implies & \exists(f) \text{fld} = \text{glid} & \text{f.fs} & \\
  & F\text{Cond}(f) & P(\text{e.fs}, \text{self}))
\end{align*}
\]

The Family to Persons transformation also illustrates Flattening/Unflattening, with the containment hierarchy of Family-Member within Family being flattened in the target model. The case uses an additional attribute `familyId` (playing the role of `eld` in Figure 7) to record in the target model element which source composite its corresponding source instance belongs to.

![Flattening/Unflattening pattern](image)

**FIGURE 7.** Flattening/Unflattening pattern.

The enhanced rules of `family2person` using the Auxiliary Correspondence Model and Flattening/Unflattening patterns are then:

Family::

\[
\begin{align*}
  \text{m} : & \text{mother} \rightarrow \text{union}(\text{daughters}) \Rightarrow \\
  \text{Female} \rightarrow & \exists(p) \text{p.personId} = \text{m.memberId} & \\
  & \text{p.familyId} = \text{id} & \\
  & \text{p.name} = \text{name} + ", " + \text{m.name}
\end{align*}
\]

There are corresponding derived invariants. Other forms of flattening discard certain model elements (eg., if only leaf classes in a class diagram are mapped to relational tables) and associations between elements (eg., state composition links in the state machine flattening example of [46]). The reverse transformation then needs to reconstruct the model elements or structure.

We can extend the patterns of Table 2 to include update operation calls within succedents, provided the operations are invertible in the manner of the inverse recursive descent pattern above. An operation defined as

\[
S_i::
\begin{align*}
  \text{op}() : & T_j \\
  \text{post} : \\
  \exists(s) \mathbf{S}\text{Cond}(s) \implies \\
  T_j \rightarrow & \exists(t) T\text{Cond}(t) & P_j(\text{self}, t) & \text{result} = t
\end{align*}
\]

can be inverted to:

\[
T_j::
\begin{align*}
  \text{op}^-() : & S_i \\
  \text{post} : \\
  \exists(s) \mathbf{T}\text{Cond}(s) \implies \\
  S_i \rightarrow & \exists(s) \mathbf{S}\text{Cond}(s) & P_j^- (s, \text{self}) & \text{result} = s
\end{align*}
\]

Applications \( y.rr = x.r.op() \) in a constraint succedent invert to \( x.r = y.rr.op^-() \).

If \( T_j \) elements are only created/modified by \( op \), then the transformation satisfies the invariant:

\[
T_j::
\begin{align*}
  \mathbf{T}\text{Cond}(s) \implies \\
  S_i \rightarrow & \exists(s) \mathbf{S}\text{Cond}(s) & P_j(\text{self}, s)
\end{align*}
\]

**V. APPLICATION OF PATTERNS TO CONSTRUCT BX**

A unidirectional transformation \( t_0 \) defined using the patterns of Table 2, and consisting of type 1 constraints satisfying syntactic non-interference, can be extended by the use of the Auxiliary Correspondence Model and Cleanup before Construct patterns to a transformation \( \tau \rightarrow \) which is the forward part of a bx. The bx relation and reverse transformation \( \tau^- \) can also be derived.

An alternative condition to syntactic non-interference is semantic non-interference: a use case with postconditions \( C_1 \) to \( C_n \) satisfies this property if for \( i < j \):

\[
C_i \implies [\text{stat}_L(C_j)]C_i
\]
TABLE 3. Inverses of predicates and expressions.

<table>
<thead>
<tr>
<th>P(s,t)</th>
<th>P~(s,t)</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>t.g = s.f</td>
<td>s.f = t.g</td>
<td>Assignable features f, g</td>
</tr>
<tr>
<td>t.g = s.f fun</td>
<td>s.f = t.g fun~</td>
<td>Invertible function/composition fun, Eg., (cos(x).log~) is exp.acosh</td>
</tr>
<tr>
<td>t.y = if C(x,y) then f(x,y) else g(x,y) endif</td>
<td>s.x = if C'(x,y) then f~(x,y) else g~(x,y) endif</td>
<td>f on C, g on not(C) are invertible with disjoint ranges, C'(x) expresses that z is in the range of f on C.</td>
</tr>
<tr>
<td>t.g = 1/s.f fun</td>
<td>s.f = (1/t.g).f~()</td>
<td>Invertible double-valued fun</td>
</tr>
<tr>
<td>t.g = s.f→pow(x)</td>
<td>s.f = t.g→pow(1.0/x)</td>
<td>x non-zero, independent of s.f</td>
</tr>
<tr>
<td>t.g = a→pow(s.f)</td>
<td>s.f = t.g→log()/a→log()</td>
<td>a &gt; 0, constant</td>
</tr>
<tr>
<td>t.g = s.f.exp()</td>
<td>s.f = t.g.log()</td>
<td>t.g &gt; 0</td>
</tr>
<tr>
<td>t.g = s.f.sin()</td>
<td>s.f = t.g.asin()</td>
<td>-1 ≤ t.g ≤ 1</td>
</tr>
<tr>
<td>t.g = s.f.cos()</td>
<td>s.f = t.g.acos()</td>
<td>-1 ≤ t.g ≤ 1</td>
</tr>
<tr>
<td>t.g = s.f.tan()</td>
<td>s.f = t.g.atan()</td>
<td></td>
</tr>
<tr>
<td>t.b2 = not(s.b1)</td>
<td>s.b1 = not(t.b2)</td>
<td>Boolean attributes b1, b2</td>
</tr>
<tr>
<td>t.g = K*s.f + L</td>
<td>s.f = (t.g - L)/K</td>
<td>f, g numeric attributes</td>
</tr>
<tr>
<td>t.g = s.f + SK</td>
<td>s.f = t.g.subrange(1, t.g.size - SK.size)</td>
<td>String constant SK</td>
</tr>
<tr>
<td>t.g = SK + s.f</td>
<td>s.f = t.g.subrange(SK.size + 1, t.g.size)</td>
<td>String constant SK</td>
</tr>
<tr>
<td>t.g = s.f1 + s.f2</td>
<td>s.f1 = StringLib.before(t.g, SK) &amp; s.f2 = StringLib.after(t.g, SK)</td>
<td>not occurring in s.f1, s.f2</td>
</tr>
<tr>
<td>t.g = s.f→reverse()</td>
<td>s.f = t.g→reverse()</td>
<td>String valued f</td>
</tr>
<tr>
<td>t.g = StringLib.rotate(s.f, n)</td>
<td>s.f = StringLib.rotate(t.g, -n)</td>
<td>String-valued f</td>
</tr>
<tr>
<td>R(s,t) &amp; Q(s,t)</td>
<td>R~(s,t) &amp; Q~(s,t)</td>
<td></td>
</tr>
<tr>
<td>s.f~forall(s)</td>
<td>t.g~forall(s)</td>
<td></td>
</tr>
<tr>
<td>F→exists(y</td>
<td>P(x,y) &amp; y : t.g)</td>
<td>E→exists(x</td>
</tr>
</tbody>
</table>

Syntactic non-interference implies semantic non-interference, but not conversely.

The bx derivation process consists of the following steps to enhance \( \tau_0 \):

1) Introduce identity attributes in source and target entity types where necessary to support the Auxiliary Correspondence Model and Flattening/Unflattening patterns, and extend the postconditions to use these attributes, forming extended postconditions \( \text{Post}_\tau \) of an enhanced transformation \( \tau \) of \( \tau_0 \) (cf., the step from Figure 1 to Figure 5).

2) Compute the invariant \( \text{Inv}_\tau \) of this extended transformation.

3) The conjunction \( \text{Post}_\tau \& \text{Inv}_\tau \) is the bx relation \( R_\tau \) of the extended transformation (and the logical relation of the ‘transformation model’ of \( \tau \) in the sense of [9]).

4) Further extend \( \tau \) to a forward transformation \( \tau \rightarrow \) by applying Cleanup before Construct to add rules (applied before the main rules of \( \tau \)) which remove target instances that fail to satisfy \( \text{Inv}_\tau \) with respect to corresponding source instances.

5) Compute an explicit form \( \text{Post}_\tau^\sim \) of \( \text{Inv}_\tau \), to form the basis \( \tau^\sim \) of the reverse transformation \( \tau^\sim \). This step requires that the computations \( t.g = \text{get}_E(s.f) \) of target data \( t.g \) in terms of source data \( s.f \) used within the postcondition predicates of \( \tau \) are invertible using view update functions \( \text{put}_E \) in the sense of a lens.

For transformation postconditions conforming to the patterns of Table 2 and consisting only of type 1 constraints, using invertible computations of target data based on source data which are known as valid get/put pairs, \( \text{Inv}_\tau \) and \( \text{Post}_\tau^\sim \) can be derived mechanically from \( \text{Post}_\tau \) using the definition of invariant predicates and inverse predicates \( \text{P}^\sim \) given in Tables 3, 4, 5, 6 and in other catalogued cases. Steps 2) to 5) can therefore be automated for transformations satisfying these restrictions. Note that in the final case of Table 3 we permit a quantification of the form \( \text{forall exists} \) within the \( \text{P} \) predicate of a constraint, thus extending slightly the range of constraints to which the bidirectionalization procedure can be applied.

Given a type 1 structure preservation rule \( C_i \) of the form

\[
S_i :: \quad \text{SCond}(\text{self}) \implies T_j \rightarrow \exists (t | TCond_j(t) \& P_j(\text{self}, t))
\]

the corresponding invariant constraint \( \text{Inv}_i \) is:

\[
T_j :: \quad \text{TCond}_j(\text{self}) \implies S_i \rightarrow \exists (t | \text{SCond}(s) \& P_j(s, \text{self}))
\]

The invariant derived from the rule expresses that each target model instance of \( T_j \) corresponds to some source model instance of \( S_i \) via that rule.

Tables 3 and 4 show some examples of inverses \( \text{P}^\sim \) of expressions and predicates \( P \). The computation of these inverses are implemented in the UML-RSDS tools as a higher-order transformation (the reverse option for use cases). Intersection on sequences is treated as \( \text{select} \):
TABLE 4. Inverse of predicates on associations.

<table>
<thead>
<tr>
<th>(P(s,t))</th>
<th>(P^{-1}(s,t))</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>(t.rr = s.r \rightarrow \text{reverse}(\cdot))</td>
<td>(s.r = t.rr \rightarrow \text{reverse}(\cdot))</td>
<td>(r, rr) ordered association ends</td>
</tr>
<tr>
<td>(t.rr = s.r \rightarrow \text{first}(\cdot))</td>
<td>(s.r = t.rr \rightarrow \text{first}(\cdot))</td>
<td>(r) ordered association end</td>
</tr>
<tr>
<td>(t.rr = s.r \rightarrow \text{last}(\cdot))</td>
<td>(s.r = t.rr \rightarrow \text{last}(\cdot))</td>
<td>(r) ordered association end</td>
</tr>
<tr>
<td>(t.rr = s.r \rightarrow \text{including}(s.p))</td>
<td>(s.p = t.rr \rightarrow \text{front}(\cdot)) &amp; (s.p = t.rr \rightarrow \text{last}(\cdot))</td>
<td>(rr, r) ordered association end (p 1)-multiplicity end</td>
</tr>
<tr>
<td>(t.rr = \text{Sequence}{s.p1, s.p2})</td>
<td>(s.p1 = t.rr \rightarrow \text{at}(1)) &amp; (s.p2 = t.rr \rightarrow \text{at}(2))</td>
<td>(rr) ordered association end (p 1, p 2)-multiplicity ends</td>
</tr>
</tbody>
</table>

\(t.rr = s.r \rightarrow \text{select}(P)\) | \(s.r = s.r \@ \text{pre} \rightarrow \text{reject}(P) \cup t.rr \rightarrow \text{select}(P)\) | \(r, rr\) set-valued |
| \(t.rr = s.r \rightarrow \text{sort}(\cdot)\) | \(s.r = t.rr \rightarrow \text{hasSet}(\cdot)\) | \(r\) set-valued, \(rr\) sequence-valued |
| \(t.rr = s.r \rightarrow \text{asSequence}(\cdot)\) | \(s.r = (s.r \@ \text{pre} \land t.rr) \land (t.rr - s.r \@ \text{pre})\) | \(r, rr\) sequence-valued |

TABLE 5. Inverse of constraints.

<table>
<thead>
<tr>
<th>(Cn)</th>
<th>(Cn^{-})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S_i:: )</td>
<td>(T_i:: )</td>
</tr>
<tr>
<td>(S) Cond(self) (\Rightarrow T_i\rightarrow \text{exists}(t</td>
<td>) TCond(t) &amp; P(self, t)) )</td>
</tr>
<tr>
<td>(S) Cond(self) (&amp; ) (v : F &amp; S) Cond(self, v) (\Rightarrow T_i\rightarrow \text{exists}(t</td>
<td>) TCond(t) &amp; P(self, v, t)) )</td>
</tr>
<tr>
<td>(S) Cond(self) (&amp; ) (v = e &amp; S) Cond(self, v) (\Rightarrow T_i\rightarrow \text{exists}(t</td>
<td>) TCond(t) &amp; P(self, v, t)) )</td>
</tr>
<tr>
<td>(S) Cond(self) (&amp; ) (v = TRef[.r.idTRef] &amp; S) Cond(self) (\Rightarrow T_i\rightarrow \text{exists}(t</td>
<td>) TCond(t) &amp; t.rr = v &amp; P(self, t)) )</td>
</tr>
</tbody>
</table>

sq1 \(\rightarrow\) intersection(sq2) abbreviates sq1 \(\rightarrow\) select(x \(|\) x : sq2) and hence retains the order of sq1. In some cases the inverse predicate is based on a functional inverse to the source-to-target mapping. For example, \(t.g = \text{not}(s.f)\) can be trivially inverted to \(s.f = \text{put}(t.g)\), so that the view-update \(s.f = \text{put}(\text{not}(s.f \@ \text{pre}, t.g))\) for \(\text{get}\) not defined as not does not need to take account of the previous value \(s.f \@ \text{pre}\) of \(s.f\). The case of \(t.rr = s.r \rightarrow \text{select}(P)\) is an example of a non-trivial view update \(s.r = \text{put}(\text{select}(s.r \@ \text{pre}, t.rr))\): given a value of \(t.rr\), we determine an updated \(s.r\) by taking the union of \(s.r \@ \text{pre} \rightarrow \text{reject}(P)\) and \(t.rr \rightarrow \text{select}(P)\). The first set are those elements of \(s.r\) which are unaffected by changes to \(t.rr\), whilst the second set consists of possibly new elements introduced by changes to \(t.rr\). View updates are discussed in more detail in Section VI.

Table 5 summarises the inverse forms of different constraint kinds involving let variable definitions \(v = E\), \(v = T\) Ref \([i\)d\]} or additional quantified variables \(v : F\).

In terms of the framework of [59], the source-target relation \(R_t\) associated with a UML-RSDS transformation \(\tau\) is \(\text{Post}_\tau\) \& \(\text{Inv}_\tau\). \(R_t\) is not necessarily bijective (eg., in the Family to Person transformation only part of the target model is significant for the bx relation, so multiple non-isomorphic target models can be related to the same source model). For unidirectional transformations \(\tau\), the design and implementation of the forward direction of \(\tau\) is normally computed as \(\text{stat}_\text{LC}(\text{Post}_\tau)\): the UML activity derived from \(\text{Post}_\tau\) when interpreted procedurally [35]. However, in order to achieve the correctness and hippocraticness bx properties, \(\text{Inv}_\tau\) must also be considered: before \(\text{stat}_\text{LC}(\text{Post}_\tau)\) is applied to the source model \(m\) and target model \(n\), \(n\) must be cleared of elements which fail to satisfy \(\text{Inv}_\tau\). This is a case of the Cleanup before Construct pattern (Section IV).

The general cleanup constraint \(\text{Cleanup}_i\) derived from \(\text{Inv}_i\) is:

\(T_i::\)

\(\text{TCond}(\text{self}) \& \) \(\text{not}(S_i \rightarrow \text{exists}(s | S\) Cond(s) \& P_j(s, self))) \(\implies \) \(self \rightarrow \text{isDeleted}()\)

This expresses that if a target instance \(t\) does not satisfy \(\text{Inv}_i(s, t)\) for any \(s : S_i\), then \(t\) is deleted.

However, this rule may delete more \(T_i\) instances than are necessary: not only instances which correspond (i) to deleted \(S_i\) instances, or (ii) to \(S_i\) instances that no longer satisfy \(S\) Cond\(_i\), but also (iii) to \(S_i\) instances satisfying \(S\) Cond\(_i\), but not \(P_j(s, self)\). In this last case, \(self\) should not be deleted, instead \(\text{stat}_\text{LC}(P_j)\) should be performed to re-establish \(P_j\) between the modified \(s\) and \(self\). Therefore, some form of source-target tracing is required, to distinguish these cases.

\(^2\)Let \(v : T = e\) in \(E\) is written as \(v = e \implies E\) in our notation.
We apply the Auxiliary Correspondence Model pattern to introduce String-valued identity attributes (primary keys) for source and target entities, to record and identify which source and target instances correspond: source instance \( s \) corresponds to target instance \( t \) when \( s . sId = t . tId \). This also means that \( S_i[t . tId] = s \) and \( T_j[s . sId] = t \). By using the Entity Splitting and Entity Merging patterns, described in Section IV, one-many and many-one relations between source and target instances can also be recorded using this technique.

Tables 3 and 4 can be extended to include assignments to features based on object indexing lookups (Table 6).

If identity attributes have been introduced using Auxiliary Correspondence Model, the postconditions (rules) \( C_i \) of \( \tau \) have the typical form

\[
S_i ::
SCond_i(self) \implies
T_j \rightarrow exists(t | t . tId = s . sId &
TCond_j(t) & P_j(self , t))
\]

and the corresponding invariant constraints \( Inv_i \) are:

\[
T_j ::
TCond_j(self) \implies
S_i \rightarrow exists(s | s . sId = t . tId &
SCond_i(s) & P_j(s , self))
\]

The cleanup constraints can then be simplified to:

\[
T_j ::
TCond_j(self) &
not(t . tId : S_i \rightarrow collect(s . sId)) \implies self \rightarrow isDeleted()
\]

and

\[
T_j ::
TCond_j(self) &
t . tId : S_i \rightarrow collect(s . sId) &
not(SCond_i(S_j[t . tId])) \implies self \rightarrow isDeleted()
\]

A single consolidated Cleanup constraint is:

\[
T_j ::
TCond_j(self) \implies
if S_i[t . tId] \rightarrow oclIsUndefined()
then self \rightarrow isDeleted()
else if not(SCond_i(S_i[t . tId]))
then self \rightarrow isDeleted()
else true
endif endif
\]

A similar analysis and formation of invariants and cleanup constraints can be carried out for the other bx pattern cases of Table 2. Details are given in the appendix.
\( \tau \rightarrow \) operates on both the source and target model, and propagates changes in the source model \( m \) to the target \( n \): if elements of \( m \) are deleted, so are the corresponding elements of \( n \). If elements of \( m \) are modified so that no rule applies to map an \( m \) element to a particular target element, then that target is deleted (this is the implicit deletion semantics of QVT-R [8], here made explicit by the \( \tau \rightarrow \) rules). Otherwise, if a modified source element still corresponds by identity to a valid target element, that target is updated according to the forward rules. Finally, if a rule applies to map a source element (new or modified) to a target which does not already exist, an appropriate target is created. Changes to identity attribute values are not permitted.

VI. INVERSE TRANSFORMATIONS AND VIEW UPDATES

For the reverse transformation \( \tau \leftarrow \), the roles of \( \text{Post}_t \) and \( \text{Inv}_t \) are interchanged: elements of the source model which fail to satisfy \( \text{Post}_t \) with respect to some element of the target model should be deleted or modified. The postcondition of the reverse transformation \( \tau \leftarrow \) is \( \text{Post}_t \), the explicit form of \( \text{Inv}_t \). The key difference between \( \tau \rightarrow \) and \( \tau \leftarrow \) is that \( \text{Post}_t \) may involve view updates [4] of the source model, using implicit changes to source elements based on target data, because \( \tau \) is specified using explicit updates of the target based on the source.

If a predicate such as \( t, g = s.f \rightarrow \text{last}() \) or \( t, g = s.f \rightarrow \text{select}(P1) \) is inverted, the result is a predicate \( s.f \rightarrow \text{last}() = t \) or \( s.f \rightarrow \text{select}(P1) = t \). These are termed view updates, because they specify an update to \( s.f \) based on the required value of some view, function or selection of its data. There may not be a unique way to perform such an update.

We extend the definition of \( \text{stat}_{LC}(P) \) so that the procedural interpretation \( \text{stat}_{LC}(P) \) of a view update predicate \( P \) is a statement which makes \( P \) true by making minimal necessary changes to \( s.f \), using suitable \( \text{put}_E \) functions which take as input the previous value \( s.f @ \text{pre} \) of \( s.f \) and the updated value \( t.g \) of the target feature: \( s.f := \text{put}_E(s.f @ \text{pre}, t.g) \). This approach can be used to implement target-to-source change propagation for a bx where the target model is constructed from views of the source model.

Tables 7, 8, 9 show the extended definitions of \( \text{stat}_{LC} \) for some common view update predicates.

In the cases for \( \text{tail} \) and \( \text{front} \) in Table 7, \( d \) is the default element of the element type of \( f \). In the case for \( \text{collect} \), \( e^{-} \) is an inverse to \( e \), defined, for example, according to Table 3. Notice that in this case, elements are deleted from \( f \) if their \( e \) value is not in \( g \), then any extra elements \( y \) where \( y.e \) is in \( g \) but \( y \) is not in \( f @ \text{pre} \), are added to \( f \). \( s \rightarrow \text{intersection}(t) \) is treated as for \( s \rightarrow \text{select}(x | x : t) \).

An assignment \( t.g = D[s.f \rightarrow \text{select}(P) \rightarrow \text{collect}(blid)] \) can be inverted to \( s.f \rightarrow \text{select}(P) = B[t.g.blid] \) if \( D \) is the corresponding target entity type for source entity \( B \), and similarly for other cases of binary and unary collection operators in place of \( \text{select} \). The view update definitions can therefore also be used for bx that involve source-target correspondences using identity attributes.

| TABLE 7. View update interpretations for \( \tau \rightarrow \) |
|---|---|
| \( P \) | \( \text{stat}_{LC}(P) \) |
| \( f \rightarrow \text{last}() = x \) | if \( f . size = 0 \) then \( f := \text{Sequence}(x) \) else \( f . size = x \) |
| \( f \rightarrow \text{front}() = g \) | if \( f . size > 0 \) then \( f := g \cup \text{Sequence}(\{ \text{last} \}) \) else \( f := g \cup \text{Sequence}(d) \) |
| \( f \rightarrow \text{first}() = x \) | if \( f . size = 0 \) then \( f := \text{Sequence}(x) \) else \( f[1] = x \) |
| \( f \rightarrow \text{tail}() = g \) | if \( f . size > 0 \) then \( f := \text{Sequence}(\{ \text{first} \}) \cup g \) else \( f := \text{Sequence}(d) \cup g \) |
| \( f \rightarrow \text{select}(P) = g \) | \( f := f \rightarrow \text{select}(x | x : g \cup \text{P} \cup \text{not}(P)) \cap \text{sequence-valued}(f (g - f \cap \text{pre}) \] |
| \( f \rightarrow \text{reject}(P) = g \) | \( \text{Same as } f \rightarrow \text{select}(\text{not}(P)) = g \) |
| \( f \rightarrow \text{collect}(e) = g \) | \( f := f @ \text{pre} \rightarrow \text{reject}(x | x.e \notin g) \cap \{ g \rightarrow \text{collect}(e^{-}) - f @ \text{pre} \} \] |

| TABLE 8. View update interpretations for \( \tau \leftarrow \) |
|---|---|
| \( P \) | \( \text{derived predicate} \) |
| \( x : a \rightarrow \text{intersection}(b) \) | \( x : a \cap x : b \) |
| \( x : a \rightarrow \text{union}(b) \) | \( x : a \cup x : b \) |
| \( x : a \rightarrow \text{select}(P) \) | \( x : a \cap x : P \) |
| \( x : a \rightarrow \text{reject}(P) \) | \( x : a \cap x : \text{not}(P) \) |
| \( x : a \rightarrow \text{hasSet}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{hasSequence}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{sort}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{sortedBy}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{reverse}(f) \) | \( x : a \rightarrow \text{preprend}(x) \) |
| \( x : a \rightarrow \text{union}(b) \) | \( \text{if } a \rightarrow \text{union}(b) \rightarrow \text{includes}(x) \text{ then skip else } a := a \rightarrow \text{including}(x) \) |
| \( \times \rightarrow \text{multiplicity a} \) | \( x : a \rightarrow \text{union}(b) \) |
| \( \times \rightarrow \text{multiplicity 0.1} \) | \( \text{if } a \rightarrow \text{union}(b) \rightarrow \text{includes}(x) \text{ then skip else if } a.size = 0 \text{ then } a := a \rightarrow \text{including}(x) \text{ else } b := b \rightarrow \text{including}(x) \) |

| TABLE 9. View update interpretations for \( \tau \leftarrow \) |
|---|---|
| \( P \) | \( \text{derived predicate} \) |
| \( x : a \rightarrow \text{intersection}(b) \) | \( x : a \cap x : b \) |
| \( x : a \rightarrow \text{union}(b) \) | \( x : a \cup x : b \) |
| \( x : a \rightarrow \text{select}(P) \) | \( x : a \cap x : P \) |
| \( x : a \rightarrow \text{reject}(P) \) | \( x : a \cap x : \text{not}(P) \) |
| \( x : a \rightarrow \text{hasSet}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{hasSequence}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{sort}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{sortedBy}(f) \) | \( x : a \) |
| \( x : a \rightarrow \text{union}(b) \) | \( x : a \cap x : b \) |

An example of a case from Table 8 is the inverse mapping \( \text{person2family} \) of \( \text{family2person} \). The \( \tau \rightarrow \) rules in this case have the form:

\text{Family::} \exists (fx | fx.id = familyId \& FamilyMember->exists(m | m.memberId = personId \& m : fx.mother->union(fx.daughters))}
fx.name = StringLib.before(name, "," ) &
m.name = StringLib.after(name, "," ) }

The update \( m : \text{fx.mother} \rightarrow \text{union(fx.daughters)} \) adds \( m \) preferentially to \( \text{fx.mother} \), only adding to \( \text{fx.daughters} \) if \( \text{fx.mother} \) is already set.

The cleanup constraints for \( \tau^\leftarrow \) are as follows in the general case:

\[
S_i::
S\text{Cond}_i(\text{self}) \& \lnot(s\text{Id} : T_j \rightarrow \text{collect}(s\text{Id})) \implies \text{self} \rightarrow \text{isDeleted()}
\]

for each \( C_i \), and

\[
S_i::
S\text{Cond}_i(\text{self}) \& s\text{Id} : T_j \rightarrow \text{collect}(s\text{Id}) \& \lnot(T\text{Cond}(T_j(s\text{Id}))) \implies \text{self} \rightarrow \text{isDeleted()}
\]

The latter is omitted if \( T\text{Cond}_i \) is not present (ie., it is true).

As with the forward transformation, \( \tau^\leftarrow = \tau^\rightarrow \cdot x; \tau^\rightarrow \cdot s\text{Id} \). \( \text{stat}_{LC}(\text{Post}^\leftarrow) \) establishes \( \text{Inv} \), whilst the cleanup constraints together with \( \text{Post}^\leftarrow \) establish \( \text{Post} \). Thus \( \tau^\leftarrow \) satisfies correctness. Hippocraticness follows since neither the cleanup or \( \text{Post}^\leftarrow \) constraints modify the source model if \( R \) already holds.

View updates can be defined for certain cases of user-defined functions by using syntactically-derived view update functions as in [34], [47], and [61]. In particular, any constraint predicate \( P(s, t) \) which computes a sequence-valued feature \( t.g = \text{get}(s.f) \) from sequence-valued \( s.f \) by using a recursively-defined function \( \text{get} \) on the elements of \( s.f \) can be inverted to \( s.f = \text{put}(s.f @ \text{pre}, t.g) \) for a recursively-defined view update function \( \text{put} \).

If \( \text{get} \) is schematically of the form:

\[
\text{get}(x) = \begin{cases} 
\text{Sequence}[] & \text{if } x.\text{size} = 0 \\
\text{Sequence}[\text{get}1(x.\text{first})] \rightarrow \text{get}(x.\text{tail}) & \text{else if } P_1(x.\text{first}, x.\text{tail}) \\
\text{else if } \ldots & \\
\text{else get}(x.\text{tail}) & \text{endif}
\end{cases}
\]

Then a corresponding \( \text{put} \) is defined by:

\[
\text{put}(x, y) = \begin{cases} 
\text{Sequence}[] & \text{if } x.\text{size} = 0 \\
\text{Sequence}[\text{put}1(x.\text{first}, y.\text{first})] \rightarrow \text{put}(x.\text{tail}, y.\text{tail}) & \text{else if } P_1(x.\text{first}, x.\text{tail}) \\
\text{else if } \ldots & \\
\text{else put}(x.\text{tail}, y.\text{tail}) & \text{endif}
\end{cases}
\]

where each \( \text{put}_i \) is an update function inverse to \( \text{get}_i \). Similarly for recursively-defined \( \text{get} \) functions from trees to sequences [62].

![FIGURE 8. UML2C transformation architecture.](image)

VII. CASE STUDY: MAPPING UML TO C

UML-RSDS already contains code generators for three versions of Java, and for C# and C++. If a code generator for a new language or language version is required, this can be written as a UML-RSDS transformation from the design metamodel (Figure 9 together with an OCL metamodel and activities metamodel) of UML-RSDS to the abstract and concrete syntax of the new target language, and then incorporated as a plugin into the UML-RSDS tools [44]. Here we consider the generation of ANSI C code from UML, and the extraction of a UML model from a C model. The code generator is factored into a model-to-model bx and a model-to-text transformation using the architecture of Figure 8.

The model-to-model bx design2C has source language the combined UML-RSDS metamodels for class diagrams, expressions and activities. Figure 9 shows the class diagram metamodel. The target language is a simplified version of the abstract syntax of C programs (Figure 10 shows the type and program structure parts of this metamodel).

We define design2C using the patterns of Table 2, to enable it to be used as the basis of a bx between UML and C. design2C consists of five subtransformations, mapping separately (i) types, (ii) class diagrams, (iii) expressions, (iv) activities, (v) use cases to C. Here we consider specifically the type mapping (i), and give extracts from (ii) and (iii).

<table>
<thead>
<tr>
<th>TABLE 10. Informal mapping between UML and C.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UML element</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Class ( E )</td>
</tr>
<tr>
<td>Property ( p : T )</td>
</tr>
<tr>
<td>String</td>
</tr>
<tr>
<td>int, long, double types</td>
</tr>
<tr>
<td>boolean type</td>
</tr>
<tr>
<td>Entity type ( E )</td>
</tr>
<tr>
<td>Set(( E )) type</td>
</tr>
<tr>
<td>Sequence(( E )) type</td>
</tr>
<tr>
<td>Operation ( op(p : P) : T ) of ( E )</td>
</tr>
</tbody>
</table>

Table 10 shows the informal mapping between UML and C for classes, types and attributes.

Primitive types, entity types and collection types are successively mapped. typeld : String and typeld : String are new identity attributes introduced for Auxiliary Correspond-
dence Model. These provide a correspondence between the occurrences of types in the source UML-RSDS design and in the target C implementation. typeId is a string consisting of digits.

The postconditions mapping UML types to C are:

PrimitiveType::
  name = "int" =>
  CPrimitiveType->exists(p | p.typeId = typeId & p.name = "int")

PrimitiveType::
  name = "long" =>
  CPrimitiveType->exists(p | p.typeId = typeId & p.name = "long")

PrimitiveType::
  name = "double" =>
  CPrimitiveType->exists(p |
p.ctypeId = typeId &
p.name = "double"

PrimitiveType::
name = "boolean" =>
CPrimitiveType->exists( p |
p.ctypeId = typeId &
p.name = "unsigned char"
)

PrimitiveType::
name = "String" =>
CPointerType->exists( t |
t.ctypeId = typeId &
CPrimitiveType->exists( p |
p.name = "char" &
t.pointsTo = p )
)

CollectionType::
nname = "Sequence" =>
CArrayType->exists( a |
a.ctypeId = typeId &
a.duplicates = true &
a.componentType = CType[elementType.typeId]
)

CollectionType::
nname = "Set" =>
CArrayType->exists( c |
c.ctypeId = typeId &
c.duplicates = false &
c.componentType = CType[elementType.typeId]
)

For this mapping we require that collection types cannot have
collection element types. Classes correspond to structs by
name, this is a distinct correspondence to that of UML and
C types. The char type has ctypeId equal to the empty string.

In subtransformation (ii), the attributes (and association
ends) owned by a class are mapped to members of its cor-
responding struct:

Entity::
CPointerType->exists( p |
p.ctypeId = typeId &
CStruct->exists( c |
c.name = name &
c.ctypeId = name & p.pointsTo = c )
)

CStruct::
("struct " + name)->display() &
"{"->display() &
members->forAll( m |
(" " + m.type + " " +
m.name + ");")->display() &
"}"
->display()

The CStruct[name] instance is looked-up by the name
primary key, and is not re-created, according to the Unique
Instantiation for bx pattern. The CType instance correspond-
ing to p.type for each property p is looked up by its ctypeId.

The type mapping constraints conform to the patterns of
Table 2. In particular they include an example of the Entity
Merging (horizontal) pattern: CPointerType instances can
 correspond either to String type instances or to entity type
instances. These cases are distinguished in the C language
model, enabling a valid inverse map to be defined. The
mapping of entity types is an example of (vertical) Entity
Splitting: a UML class (entity type) is mapped to a C pointer
type and to a C struct. In this case these target instances both
belong to the same class hierarchy, so they are given distinct
ctypeId key values, both of which are derived 1-1 from the
source instance.

Following the model-to-model transformation design2C,
a model-to-text transformation genCtext produces C text
from the C metamodel. For example:

CPrimitiveType::<
"(" + name + ");"->display() &
"{"->display() &
members->forAll( m |
(" " + m.type + " " +
m.name + ");")->display() &
"}"
->display()

A toString() operation is defined on each CType subclass
to give the text representation of the C type.

Using the results of the appendix, we can show that
design2C can be used as the basis for a bx. Apart from the
practical benefits of change propagation in either direction,
the bx property has important theoretical consequences. For
high-integrity refinement transformations, the property of
conservativeness or model-coverage is important [56]: that
all data and information in the refined model is derived from
the original model. The invariant of a refinement expresses
that this property holds. Similarly, the bx relation can
encode model-level semantic preservation/semantic equiva-
lence of the source and target models: that they have equiv-
alent semantics. Finally, the existence of change-propagation
in both directions helps to support round-trip engineering
between UML and C.

Transformation invariants and cleanup constraints can
be derived for design2C→, following the definitions in
Section V and the appendix. The invariants express that
the C representation is derived entirely from the source
UML-RSDS design, and hence conservativeness of the trans-
formation.

The Post∼ constraints provide an explicit inverse (reverse-
engineering or abstraction) transformation design2C←, and
can be derived automatically:

CPrimitiveType::<
"(" + name + ");"->display() &
"{"->display() &
members->forAll( m |
(" " + m.type + " " +
m.name + ");")->display() &
"}"
->display()
t.typeId = ctypeId &
t.name = "boolean"
)

CPointerType::
p : CPrimitiveType & p.name = "char" &
pointsTo = p =>
PrimitiveType->exists( t |
t.typeId = ctypeId &
t.name = "String"
)

CPointerType::
c : CStruct & pointsTo = c =>
Entity->exists( e |
e.typeId = ctypeId &
e.name = c.name )

CArrayType::
duplicates = true =>
CollectionType->exists( t |
t.typeId = ctypeId &
t.name = "Sequence" &
t.elementType =
Type[componentType.ctypeId] )

CArrayType::
duplicates = false =>
CollectionType->exists( t |
t.typeId = ctypeId &
t.name = "Set" &
t.elementType =
Type[componentType.ctypeId] )

The inverse mapping from C members to UML properties
is (from Tables 3, 6):

CStruct::
Enterity->exists( e |
e.name = name &
members->forAll( m |
    p.name = m.name &
p.isUnique = m.isKey &
p.type = Type[m.type.ctypeId] &
p : e.ownedAttribute ) )

CArrayType::
name = "Sequence" =>
CArrayType->exists( a |
a.typeId = typeId &
a.duplicates = true &
a.componentType =
CType[elementType.typeId] )

applies to set duplicates = true for the corresponding C type.

Other parts of the UML to C translation can also be
defined as a bx in the same manner: mappings from
(ii) class diagrams, (iii) expressions and (iv) activities to
corresponding C elements have been defined as part of a
code generator for C in the UML-RSDS tools version 1.8
(https://nms.kcl.ac.uk/kevin.lano/uml2web/). The mappings
(iii) and (iv) use a Recursive Descent style of transformation,
due to the self-recursive structure of expressions and
activities. To invert such transformations, the Inverse Recur-
sive Descent pattern can be used (Figure 6), based upon the
Auxiliary Correspondence Model and Unique Instantiation
patterns for bx, with invariants and inverse rules defined in
a similar manner as for non-recursive rules. As an example,
for the mapping of expressions from OCL to C, we have the
following operation in the role of op in the pattern:

BinaryExpression::
mapBinaryExpression(lexp : CExpression,
    rexp : CExpression) : CExpression
pre:
    lexp = CExpression[left.expId] &
    rexp = CExpression[right.expId]
post:
    CBinaryExpression->exists( c |
        c.operator =
            Expression.cop(operator) &
        c.left = lexp & c.right = rexp &
        c.type = CType[type.typeId] &
        result = c )

This has the inverse op~ from C to OCL:

CBinaryExpression::
mapCBinaryExpression(lexp : Expression,
    rexp : Expression) : Expression
pre:
    lexp = Expression[left.cexpId] &
    rexp = Expression[right.cexpId]
post:
    BinaryExpression->exists( e |
        e.operator =
            CExpression.uop(operator) &
        e.left = lexp & e.right = rexp &
        e.type = Type[type.ctypeId] &
        result = e )

where cop and uop are dual functions defining the cor-
responding operators in the two languages. For example,
the OCL operator and (&) corresponds to the C operator &&.

The complete transformation consists of over 250 rules and
operations, and is one of the largest UML-RSDS transforma-
tions that have been developed.

VIII. BX SPECIFICATION IN QVT-R

QVT-R [51] was designed as a declarative MT language
supporting (in principle) specification of bidirectional and
multi-directional transformations. However to achieve bidi-
rectionality, various restrictions need to be placed on QVT-R
specifications.

In particular, the use of recursive where invocations
between QVT-R relations can prevent the use of a transfor-
mation as a bx [46], as can the use of ‘black box’ imple-
mentations of relations [51]. In addition, the semantics in
the standard is incomplete and lacks formality. There is
a lack of guidance for the correct organization of specifi-
cations, in particular how data-dependencies and conflicts
between relations should be managed, and there is a lack of
guidance on the construction of specifications that support
bidirectional/multi-directional execution.

To address these problems, we have implemented a formal
and extended version of the logical semantics of [51] as a
mapping from QVT-R to UML-RSDS. The mapping makes explicit the semantic meaning of a QVT-R specification in a form that can be manually inspected or formally analyzed, including the use of formal proof.

A. QVT-RELATIONS (QVT-R)

QVT-R transformations are defined using relations, which are rules that relate elements of a source model to corresponding elements of a target model. For example, the UML2C mapping from classes to C structs (and vice-versa) can be defined by:

```java
top relation Class2CPointerType
{ enforce domain design e : Entity
  { name = n);
  enforce domain C p : CPointerType
  { name = n, ctypeName = n };
}
```

Relations include at least one domain, each domain is associated to some model involved in the transformation. Domain root variables represent elements of the domain model, in this case an Entity instance e of the design model, and a c : CStruct instance of the C model. The keyword enforce indicates that the domain elements may be modified by the relation when executed in the direction of the model of the domain.

The relation maps an Entity instance to a CStruct instance when execution is performed in the C model direction. If instead the relation was executed in the design direction, a mapping from CStruct to Entity would result. The variable n : String is an auxiliary (local) variable of the relation, used to transfer feature values from one domain to the other.

Top relations correspond to use case postcondition constraints in UML-RSDS: they are applied to all source elements which satisfy their application conditions, in an arbitrary order. QVT-R also has non-top relations, which only execute if explicitly invoked from the when clause of a relation, and in this case the source elements are supplied as inputs to the called relation via the call parameters. Non-top relations correspond to update operations in UML-RSDS.

The UML2C mapping from classes to pointer types in QVT-R is:

```java
top relation Class2CPointerType
{ enforce domain design e : Entity
  { typeId = t);
  enforce domain C p : CPointerType
  { typeId = t };
}
```

As with UML-RSDS rules, QVT-R relations R_i may depend upon results of previously-executed relations R_j. In QVT-R these dependencies can be explicitly stated by a when \{R_i(pars)\} clause in R_j. For example, the following relation creates links between existing CPointerType and CStruct instances:

```java
top relation LinkCPointerTypeCStruct
{ enforce domain design e : Entity { };
  enforce domain C p : CPointerType
  { pointsTo = c : CStruct { } };
  when
  { Class2CStruct(e, c) and
    Class2CPointerType(e, p) }
}
```

This is an example of the Map objects before links pattern: the pointsTo link is only set once the objects c and p are available to link.

We refer to the domain root variables (e and p here) and the object template variables of their patterns (eg., c) as the object variables of the relation.

B. USING BX PATTERNS IN QVT-R

Most of the bx patterns described in Section IV can also be used in QVT-R, to define bx in the language:

- Structure Preservation: simple top relations such as Class2CStruct above, with no when clause and a single enforce domain for each model.
- Phased Construction: top relations R which construct a target element t and reference another top relation R’ in their when clause to look up a target element t’ which R links to t.
- Entity Splitting (horizontal): two or more top relations which each map the same source domain s : S_i to target elements of different concrete entity types; the relations have disjoint when conditions; (vertical): top relations with a single source domain s : S_i and multiple (> 1) target domains/variables.
- Entity Merging (horizontal): two or more top relations which map source domains of different entity types to a common target domain t : T, the top relations have disjoint when conditions; (vertical): top relations with multiple source domains/object variables and single target domains/variables.
- Map Objects before Links: a top relation does not create target elements, instead it links elements created by other relations, which are listed in its when clause. E.g., LinkCPointerTypeCStruct above.
- Lens: relation R computes a target feature t.g as a get function of source feature(s) s.f. The assignment t.g = get(s.f) and its inverse s.f = put(s.f @pre, t.g) must both be included in the when clause of R.\textsuperscript{3}
- Flattening/unflattening: hierarchical structure in the source model is discarded in the mapping to the target, possibly together with source elements. The reverse direction must reassemble the structure/elements.

The Auxiliary Correspondence Model pattern is implicitly provided by the trace mechanism of QVT-R. It can also be explicitly introduced by means of key declarations, specifying that designated attributes are identities. Cleanup before Construct is internally implemented by deletion actions (scheduled after creation/update actions [51]). Unique Instantiation is internally implemented by QVT-R’s check-before-enforce semantics.

\textsuperscript{3}This use of @pre is supported by the QVT-R to UML-RSDS translation.
The same concepts of read and write frames \( rd() \), \( wr() \) from UML-RSDS can be adopted for QVT-R. A significant difference to UML-RSDS is that relations have a designated application direction, with some domains considered as sources and others considered as targets. Only features and entities of target domains can be written by the relation. In addition, elements bound in the \( when \) clause are assumed to already exist and are not created by the relation. Eg., for LinkCPointerTypeCStruct above, \( wr() \) in the \( C \) direction is just (\( \text{PointerType}::\text{pointsTo} \)), and in the \( design \) direction is empty (the relation has no effect).

Relations may use auxiliary variables to transfer data between domains, eg., the string-valued variable \( t \) in Class2CPointerType. These are considered internal to the relation, and – as with local variables in UML-RSDS – they are not included in its write and read frame.

### C. MAPPING QVT-R TO UML-RSDS

For a QVT-R transformation \( \tau \) on distinct models \( s : SL \) and \( t : TL \), we can define corresponding unidirectional UML-RSDS transformations \( \tau^{-} \) and \( \tau^{-} \) for the two possible execution directions \( s \to t \) and \( t \to s \) of \( \tau \). Top relations are mapped to UML-RSDS rules, and non-top relations to UML-RSDS operations.

The enforce semantics of QVT-R ([51, Sec. B.2]) is based upon two predicates \( \text{create}(R, m) \) and \( \text{delete}(R, m) \) for each relation \( R \) and model \( m \) of the transformation. Enforcement of \( R \) in the \( m \) direction consists of applying \( \text{create}(R, m) \) to carry out necessary creation/update actions on \( m \) required by \( R \), and then \( \text{delete}(R, m) \) to delete elements of \( m \) which are not required to exist by \( R \).

In our mappings from QVT-R to UML-RSDS we give separate formal interpretations \( \text{Pres}(m) \), \( \text{Con}(m) \) and \( \text{Cleanup}(m) \) for the update, creation and deletion phases of a relational transformation \( \tau \) executed in the direction of model \( m \). As in the QVT-R to QVT-Core mapping of [51], trace entities \( R\text{Strace} \) are used to record when relations \( R \) on source domains \( s \) and target domains \( t \) have been successfully applied: \( R\text{Strace} \) has properties \( x : E \) for all the object variables \( x : E \) of \( R \). A tuple \((a, b)\) for source elements \( a \) and target elements \( b \) should be in the trace \( R\text{Strace} \) iff \( R \) has been successfully applied to \( a \) to update or create \( b \), and all these elements exist. These traces are tested when \( R(a, b) \) occurs as a rule call in a \( when \) clause.

For relation \( R \), \( \text{Pres}(m) \) is an UML-RSDS constraint that defines \( R \)'s change-propagation actions for elements that have already been matched (ie., by a previous execution of \( \tau \)), it is defined as

\[
R\text{Strace} : \quad \text{whenp} \land \bigwedge_{d \in \text{edom}} \text{cpred}(d) \implies \bigwedge_{d \in \text{edom}} \text{epred}(d) \land \text{wherep}
\]

\( \text{whenp} \) is the logical interpretation of the \( when \) clause, \( \text{wherep} \) of the \( where \) clause, \( \text{cpred}(d) \) of a non-target domain \( d \), \( \text{epred}(d) \) of a target domain \( d \) of \( m \), and the conjunction is taken over all non-target domains \( sdom \) in the antecedent (ie., domains with models \( m' \), \( m' \neq m \)), and over target domains \( tdom \) in the succedent (ie., domains with model \( m \)).

The scope of any \( \exists \) quantifiers in the \( \text{epred} \) formulae are extended over the remainder of the succedent. Details of \( \text{whenp} \), \( \text{wherep} \), \( \text{cpred} \) and \( \text{epred} \) are given in [36]. We collect all \( \text{Pres}(m) \) constraints for both top and non-top \( R \) into a UML-RSDS use case \( \text{Pres}_i(m) \) representing a first transformation phase \( \text{Pres}_i(m) \) of \( \tau \) executed in the \( m \) direction. This phase propagates element feature changes from source models to \( m \).

For example, \( \text{Pres}_\text{Class2CStruct}(C) \) is

\[
\text{Class2CStructStrace} : \quad n = e.\text{name} \implies c.\text{name} = n \land c.\text{ctypeld} = n
\]

This constraint propagates name changes from \( \text{Entity} \) instances to \( \text{CStructs} \).

\( \text{Con}(m) \) deals with the case of creation of new \( m \) elements and \( R \) traces, for top relations \( R \). It only applies if the source elements \( s_1, \ldots \) are not already in \( R\text{Strace} \):

\[
\text{whenp} \land \bigwedge_{d \in \text{edom}} \text{cpred}(d) \land \text{not}(R\text{Strace} \rightarrow \exists (tr | \bigwedge_{i} tr.s_i = s_i)) \implies \bigwedge_{d \in \text{edom}} \text{epred}(d) \land \text{wherep}
\]

\( \text{wherep} \) includes the creation \( R\text{Strace} \rightarrow \exists (tr | \bigwedge_{i} tr.s_i = s_i \land \bigwedge_{j} tr.t_j = t_j) \) of a new trace. Again, \( \exists \) quantifiers in the succedent apply over all of the succedent following their introduction. A predicate \( \theta_{\text{Con}}(m) \) is formed as for \( \text{Con}(m) \) but without the predicates on \( R\text{Strace} \). The \( \text{Con}(m) \) constraints are placed in a use case representing a second \( \tau \) phase, \( \text{Con}_i(m) \). These constraints propagate element creation from source models to \( m \).

For example, \( \text{Con}_\text{Class2CStruct}(C) \) is:

\[
\text{e : Entity & n = e.\text{name} & not(Class2CStructStrace \rightarrow \exists (tr | tr.e = e)) \implies CStruct \rightarrow \exists (c | c.\text{name} = n \land c.\text{ctypeld} = n \land CStructStrace \rightarrow \exists (tr | tr.e = e \land tr.e = c))}
\]

Unique instantiation/least change semantics is used for the operational interpretation of the \( \exists \) quantifier: if \( x : X \) already exists such that \( P \) holds for \( x \), then \( X \rightarrow \exists x(P) \) in a succedent does not recreate \( x \). Target elements identified by a key value are looked-up by that value and re-used if they already exist. We use the \( \text{statLc}(P) \) semantics of Section III-C for the least-change procedural interpretation of predicates \( P \).
The \textit{Cleanup}_\tau(m)\ phase of \tau removes any spurious target elements which have not been produced by any relation. For target entity \(E\) of \(m\), \textit{Cleanup}_E is defined as:
\[
E ::
\begin{align*}
\text{not}(r1\text{\$trace}\rightarrow\text{exists}(r1|\tau_1.e1 = \text{self})) & \text{ } & \ldots & \text{ } & \text{not}(rm\text{\$trace}\rightarrow\text{exists}(rm|rm.em = \text{self})) \implies \\
\text{self}\rightarrow\text{isDeleted()}
\end{align*}
\]
where the \(rk, k = 1\) to \(m\), are all the relations (top or non-top) in which the entity \(E\) occurs as the type of some target domain or target object template \(ek : E\). All \textit{Cleanup} constraints are placed in a final \(\tau\) phase, \textit{Cleanup}_\tau(m). Unlike in UML-RSDS, where the cleanup constraints precede the main transformation, in QVT-R the cleanup actions must follow the \textit{Con}_\tau(m) phase because traces are explicitly constructed by that phase, instead of being implicit based on identity attribute values.

For example, \textit{Cleanup}_CStruct is:
\[
CStruct ::
\begin{align*}
\text{not}(\text{Class\$2\text{\$CStruct}\$\text{\$trace}\rightarrow\text{exists}(tr|}
\text{\text{tr.c = self})) & \text{ } & \ldots & \text{not}(\text{Link\text{\$CPointerType\$CStruct}\$\text{\$trace}\rightarrow\text{exists}(tr|}
\text{\text{tr.c = self})) \implies \\
\text{self}\rightarrow\text{isDeleted()}
\end{align*}
\]
The \textit{Cleanup} constraints propagate element deletion from source models to \(m\), because if any element of a trace object is deleted, so is the trace.

Additionally, non-top rules \(R\) are interpreted as operations with postconditions defined as for \textit{Con}_\tau(m). Details are in [36]. Regarding the \textit{overrides} clause, we follow [64] in removing this by expanding out the definition of an overridden relation to include an additional \textit{when} predicate which expresses that no overriding relation is applicable. A \textit{when} test on an overridden abstract relation \(R(pars)\) is expanded to be a disjunction \(R_1(pars)\) or \(\ldots\) or \(R_n(pars)\) on all the concrete relations \(R_i\) overriding \(R\).

For each execution direction, the three phases are executed in the order \textit{Pres}_\tau(m); \textit{Con}_\tau(m); \textit{Cleanup}_\tau(m), and together should establish the following as post-conditions of \(\tau\): (i) that any existing target object \(tx : E\) of \(m\) must appear as a target property of some trace: \(E \rightarrow \text{forall}(tx|\text{\$trace}\rightarrow\text{exists}(tx|\tau_1.t1 = tx) \text{ } \ldots \text{ } \text{or } \text{\$trace}\rightarrow\text{exists}(tm|tm.tm = tx))\) where the \(ri\) are as for \textit{Cleanup}_\tau; (ii) that all trace objects in \$\text{\$trace}\ satisfy the logical relation \(\theta_\tau(m)\) defined by \(R\) (ie., \textit{Pres}_\tau(m) holds); (iii) for top relations \(R\), that any tuple of source elements that satisfy the antecedent \(\varphi_R\) of \(\theta_\tau(m)\) appears in some \$\text{\$trace}\.

The following restrictions are needed on the QVT-R specification \(\tau\) in order that (i), (ii), (iii) are established by its logical interpretation: (a) No target features/entity names occur in the \textit{when} clause or source domain patterns of any relation; (b) If two relations both write to the same target features or entities, these updates are non-conflicting (ie., they create/update disjoint sets of elements of the same target entity, or update disjoint sets of features of instances of the entity); (c) there are no self-conflicts of a relation \(R\), ie., one application of \(R\) cannot invalidate a different application; (d) for any mandatory target model association \(A\rightarrow^{-1}B\), the \textit{a.r} element for \(a : A\) must be created/linked to \(a\) by \(\tau\) if \(a\) is created by \(\tau\).

Assuming (a), (b) and (c), the \textit{Pres}_\tau(m)\ phase establishes invariant (ii), since by (a) no target features/entities occur on the LHS of a \textit{Pres} constraint, and by (b) and (c) the effect of one \textit{Pres} constraint application is not invalidated by any other. Likewise, the \textit{Con}_\tau(m)\ phase establishes (iii) at its termination and preserves (ii), if there is no conflict between relation applications (of the same or different relations). For separate-models transformations, the \textit{Cleanup} constraints establish (i) and do not invalidate (ii) or (iii) because they only update the target model, not the source or traces. Condition (d) ensures that deletion propagation from a whole to a part object does not delete elements that are in traces (if the part is in a trace, so must the whole be). Thus by (a) and (d) \textit{Cleanup}_\tau(m)\ does not affect the truth of any \textit{Con} or \textit{Pres} constraint for target model \(m\).

If conditions (i), (ii) and (iii) hold, then neither \textit{Pres}_\tau(m), \textit{Con}_\tau(m) or \textit{Cleanup}_\tau(m) have any effect. Therefore \(\tau\) directed at \(m\) satisfies the \(\text{bx}\) conditions of correctness and hippocraticness with respect to (i), (ii) and (iii) as a definition of the transformation consistency relation \(R\) between source and target models (Section I).

It is possible for \(\tau\) to satisfy the correctness conditions (a) to (d) in one execution direction but not in others. For a \text{bx}, we require that the conditions hold in all execution directions.

The following design guidelines for QVT-R should also be observed: (e) Use \textit{when} dependencies between top-level relations where possible, in preference to \textit{where} invocations of relations; (f) The \textit{when} dependencies should be acyclic and reflect data-dependency relations between relations. Map Objects Before Links can be used to remove circular dependencies; (g) Relations should be listed in order of their dependencies so that later relations depend only on earlier ones; (h) There should be no \textit{where} clauses invoking top relations, and no negated relation calls in \textit{when} clauses.

If these conditions and the previous restrictions (a) to (d) are satisfied for a separate-models transformation \(\tau\), then the constraints of \textit{Con}_\tau(m) and \textit{Pres}_\tau(m) can be implemented as bounded loops over their source elements, simplifying verification and potentially improving efficiency.

While the above semantics follows closely that given in [51], it is not optimally efficient. Further improvements in efficiency can be made by using traces to lookup target elements based on source elements, as in UML-RSDS and ATL, instead of performing iterations through all traces.

We have automated this optimised mapping from QVT-R to UML-RSDS as a facility to import QVT-R transformations in UML-RSDS version 1.8.
IX. EVALUATION

In this section we evaluate the efficiency of the bx produced by our two approaches, using the list reversal example of [63], identify differences in the expressiveness of the approaches, and summarise the advantages and disadvantages of the approaches.

The list reversal case is used by [63] to compare different implementation approaches for QVT-R. Figure 11 shows the metamodels of the case.

![List reversal metamodels](image)

FIGURE 11. List reversal metamodels.

In the UML-RSDS version of this case study the name attributes of the list and element classes are assumed to be identity attributes. The forward rules are:

\[
\text{DoublyLinkedList} ::
\]
\[
\text{DoublyLinkedList}^1 \rightarrow \exists(l | l\text{.name} = \text{name})
\]

\[
\text{Element} ::
\]
\[
\text{Element}^1 \rightarrow \exists(e | e\text{.name} = \text{name} & e\text{.list} = \text{DoublyLinkedList}^1\{\text{list}\text{.name}\})
\]

\[
\text{Element} ::
\]
\[
e = \text{Element}^1\{\text{name}\} \implies e\text{.target} = \text{Element}^1\{\text{source}\text{.name}\}
\]

This uses Structure preservation, Phased construction and Map objects before links, and is automatically invertible according to Tables 5, 6.

In our QVT-R version, Map objects before links is used to remove dependence of element2element on itself:

```java
{ list = rList : DoublyLinkedList1{},
  name = n };
when { list2list(fList,rList) }
}
top relation link2link
{ enforce domain forward
  fElement : Element
  { target = fTarget : Element {} };
  enforce domain reverse
  rElement : Element1
  { source = rSource : Element1 {} };
when
  { element2element(fElement,rElement) } and
  element2element(fTarget, rSource) }
```

The QVT-R version does not need to assume that name attributes are identities for tracing purposes, but instead this restriction is needed in order to ensure absence of self-conflicts in the relations (if two different elements in the source list had the same names they would be mapped to a single target element by element2element, and link2link would then attempt to set conflicting links for this element).

![Efficiency of QVT-R versus UML-RSDS](image)

FIGURE 12. Efficiency of QVT-R versus UML-RSDS.

Figure 12 shows the execution time in ms of the UML-RSDS version and the QVT-R (translated via UML-RSDS) version, using generated Java 4 code on a 32-bit JVM and single core of a 2.53GHz Intel i3 Windows 7 laptop. The UML-RSDS version has a low time complexity, and is comparable to the performance of optimised versions of the case presented in [63]. The QVT-R via UML-RSDS version is less efficient, because of its more complex trace management. We also show the execution time using Medini QVT (projects.ikv.de/qvt) to execute the QVT-R version. This uses a 32-bit JVM on a 2.6GHz Intel i7 machine. The execution time is substantially higher than the QVT-R via UML-RSDS implementation approach.

The expressiveness of UML-RSDS and QVT-R is similar, when restricted to follow bx pattern structures and the
A structure-preservation constraint $C_i$ using Auxiliary Correspondence Model

$$S_i := SCond_i(self) \implies T_j \rightarrow \exists \text{t.t1Id = sId & } TCond_j(t) \&( P_j(self,t))$$

in UML-RSDS corresponds to a QVT-R relation:

```plaintext
top relation mapSiToTj
( { enforce domain src s : Si
   { sId = id })( SCond1(s) };
   enforce domain trg t : Tj
   { tId = id }{ TCond1(t) };
   where { Pj(s,t) } )
)
```

executed in the $trg$ direction. This is a structure preservation relation in QVT-R.

A difference in expressiveness in this case is that the $where$ clause in our extended QVT-R can also contain the dual predicate $P_i^\rightarrow(s,t)$. This is not possible in UML-RSDS because there is no restriction of constraint write-frames based on execution direction.

A phased construction constraint has the same structure but $P_j(s,t)$ has the form $PCond_j(s,t) \& t.rr = TRef[s,r.idSRef]$ to assign a value to an association role end by a single assignment as in UML-RSDS.

A flattened constraint

$$f : fs \& FCond(f) \implies G \rightarrow \exists \text{g}
\{ gId = fid, eId = id \}{ GCond(g) } \& P(self,f,g)$$

corresponds to a flattening relation in QVT-R:

```plaintext
top relation mapEToG
( { enforce domain src e : E
   { eId = id, fs = f }{ FCond(f) };
   enforce domain trg g : G
   { gId = fid, eId = id }{ GCond(g) };
   where { P(e,f,g) } )
)
```

A map objects before links linking constraint

$$S_i := T_j[idS_j], rr = TRef[r.idSRef]$$

This is a phased construction relation in QVT-R. Note that the mapping from $r$ to $rr$ is done element-by-element instead of by a single assignment as in UML-RSDS.

An entity-splitting (vertical) constraint

$$S_i := SCond_i(self) \implies T_k \rightarrow \exists t1.t1Id = sId & TCond_k(t1) \& P_j(self,t1,t2))$$

corresponds to an entity-splitting (vertical) relation:

```plaintext
top relation mapSiToTkTl
( { enforce domain src s : Si
   { sId = id })( SCond1(s) };
   enforce domain trg t1 : Tk
   { t1Id = id }{ TCond1(t1) };
   enforce domain trg t2 : Tl
   { t2Id = id }{ TCond2(t1,t2) };
   where { P(s,t1,t2) } )
)
```

Likewise for horizontal splitting and for entity merging constraints.

A flattening constraint

$$E ::
\{ f : fs \& FCond(f) \implies G \rightarrow \exists \text{g}
\{ gId = fid, eId = id \}{ GCond(g) } \& P(self,f,g)$$

A map objects before links linking constraint

$$S_i := T_j[idS_j], rr = TRef[r.idSRef]$$

This is a phased construction relation in QVT-R. Note that the mapping from $r$ to $rr$ is done element-by-element instead of by a single assignment as in UML-RSDS.

An entity-splitting (vertical) constraint

$$S_i ::
\begin{align*}
\text{SCond}_i(self) \implies T_k \rightarrow \exists t1.t1Id = sId & TCond_k(t1) \\
T_j \rightarrow \exists t2 \quad t2.t2Id = sId & TCond_j(t1) \& P_j(self,t1,t2))
\end{align*}$$

corresponds to an entity-splitting (vertical) relation:
inheritance. We can conclude that the expressiveness of the approaches is similar when restricted to the bx patterns and guidelines, and that usages of patterns in UML-RSDS translate into usages of the same patterns in QVT-R.

Table 11 compares the advantages and disadvantages of the two approaches we have presented in this paper. Whilst the UML-RSDS approach has advantages of efficiency and conciseness, the reverse transformation is derived as a secondary construct from the forward transformation. In QVT-R a single specification text describes both directions. In the Lens case this enables the specifier to write both put and get functions together, and to create new function pairs as necessary, whilst in UML-RSDS the put is looked-up in a fixed catalogue of put/get pairs.

**X. CONCLUSION**

We have defined a declarative approach for defining bidirectional transformations in UML, based on use cases with dual postcondition and invariant relations between source and target models. These use cases permit many-to-one and one-to-many bx, in addition to bijections. The definition of bx and their analysis is supported by the UML-RSDS tools [42].

By using standard UML notations and concepts, our approach should enable bx specifications to be retained and maintained independently of particular transformation technologies. The use of OCL for transformation specification facilitates the automated derivation of transformation invariants and reverse rules. Translations from ATL and ETL to UML-RSDS have been developed [37], [40], and these potentially enable our bx approach to be also applied to unidirectional transformations in these languages. Our approach scales up to transformations of practical size, and we have given extracts from a UML to C code generator with over 250 mapping rules and operations.

We have also described an approach using QVT-R, utilising a translation from QVT-R to UML-RSDS to extend the expressiveness of QVT-R, and to provide efficient execution of different directions of the QVT-R specifications. We have described how bx patterns can be used in QVT-R to support the definition of bx in the language.

**APPENDIX**

**CORRECTNESS AND HIPPOCRATICNESS PROPERTIES FOR τ⁻¹**

In this section we give a formal justification that bx defined using the UML specification approach described in Section V do satisfy the bx properties of correctness and Hippocraticness, and that they satisfy local Hippocraticness and least change principles subject to some restrictions.

We consider the case of UML-RSDS transformations τ that satisfy the patterns of Table 2, with source language entities Si and target language entities Tj, and whose constraints are of type 1, satisfying syntactic non-interference. Identity attributes are used to implement Auxiliary Correspondence Model. This means that τ is a separate-models transformation with source language SL and target language TL, and postcondition Postτ is an ordered conjunction of constraints Cj each of the form:

\[
S_i ::= \quad SCond_i(self) \implies T_j \rightarrow \exists t | t.tId = sId & TCond_j(t) & P_j(self, t)
\]

Invτ is therefore a conjunction of constraints Invτ of the form

\[
T_j ::
TCond_j(self) \implies S_i \rightarrow \exists s | s.tId = sId & SCond_j(s) & P_j(s, self)
\]

A consequence is that \( S_i \rightarrow select(SCond_i) \) and \( T_j \rightarrow select(TCond_j) \) are isomorphic, with the isomorphism given by mapping \( s : S_i \) to \( T_j[s.sId] \).

The simplified cleanup constraints for \( \tau^{-1} \) are therefore:

\[
T_j ::
TCond_j(self) & S_i[tId] \rightarrow oclIsUndefined() \implies self \rightarrow isDeleted()
\]

and

\[
T_j ::
TCond_j(self) & tId : S_i \rightarrow collect(sId) & not(SCond_j(S_i[tId])) \implies self \rightarrow isDeleted()
\]

The second constraint is omitted if \( SCond_j \) is absent (ie., true).

We denote the collection of the cleanup constraints by Cleanup. These are the postconditions of \( \tau^{-1} \).

Bx correctness holds, since the cleanup constraints together with \( Post_\tau \) establish Invτ: the Cleanup constraints remove any target model elements that fail to correspond by identity to source model elements in the domain of \( \tau \), and \( Post_\tau \) modifies target model elements that do correspond to valid source elements, in order to re-establish Invτ. By construction, \( statSC(Post_\tau) \) preserves Invτ and establishes Postτ. Therefore, the sequential composition of
stat\_\text{LC}(\text{Cleanup})\) and \(\text{stat}\_\text{LC}(\text{Post}_t)\) establishes the bx relation \(R\) as \(\text{Post}_t\) & \text{Inv}_v\).

Hippocraticness holds, since \(\text{stat}\_\text{LC}(\text{Cleanup})\) has no effect if the models already satisfy \(R\), and neither does \(\text{stat}\_\text{LC}(\text{Post}_t)\), due to the Unique Instantiation interpretation of the \(\text{exists}\) operator. Local hippocraticness holds in the sense that if corresponding elements \(s: S_i\) and \(t = T_i[s.sld]\) already satisfy \(C_i\) and \text{Inv}_v\), then their attribute values are not modified by \(\tau\rightarrow t\).\(m\) may however be deleted as a consequence of target element deletions from cleanup actions of other rules, and to avoid this we need the condition on \(TL\) that \(T_i\) is not subject to deletion propagation from any entity type in \(wr(\tau)\). These restrictions are also assumed in the following cases.

The principle of least change is satisfied, since changes to the source model either lead to deletion of the target elements (and their incident links) which cannot be modified to correspond to source elements (cases (i) and (ii) in Section V), and deletion of any other elements required by deletion propagation, or to creation/modification of target elements, using \(\text{stat}\_\text{LC}(C_i)\). But \(\text{stat}\_\text{LC}(C_i)\) is designed as a minimally-intrusive update to the target model which will establish \(C_i\). Interpreting a quantifier \(T_j\rightarrow \text{exists}(t|P)\) using Unique Instantiation means that un-necessary creation of target elements is avoided.

A more complex case is Entity Merging (Section IV). In the horizontal version of this pattern two or more source entity types \(S_i\), \(S_j\) may map to the same target entity type \(T_k\):

\[
S_i ::
\text{SCond}_i(\text{self}) \implies T_k \rightarrow \text{exists}(t|s.tld = s1ld & T\text{Cond}_i(t) & P_i(s, t))
\]

and

\[
S_j ::
\text{SCond}_j(\text{self}) \implies T_k \rightarrow \text{exists}(t|s.tld = s2ld & T\text{Cond}_j(t) & P_j(s, t))
\]

Provided that the respective \(T\text{Cond}_i\), \(T\text{Cond}_j\) conditions are pairwise disjoint, and the sets of identities of \(S_i\rightarrow \text{select}(\text{SCond}_i)\) and \(S_j\rightarrow \text{select}(\text{SCond}_j)\) are disjoint, the same construction and argument for the bx correctness apply as in the Structure Preservation case. The invariants are

\[
T_k ::
\text{TCond}_i(\text{self}) \implies S_i \rightarrow \text{exists}(s|s.s1Id = tld & S\text{Cond}_i(s) & P_i(s, s))
\]

and

\[
T_k ::
\text{TCond}_j(\text{self}) \implies S_j \rightarrow \text{exists}(s|s.s2Id = tld & S\text{Cond}_j(s) & P_j(s, s))
\]

and hence \(S_i\rightarrow \text{select}(\text{SCond}_i)\) is isomorphic to \(T_k\rightarrow \text{select}(\text{TCond}_i)\) and \(S_j\rightarrow \text{select}(\text{SCond}_j)\) is isomorphic to \(T_k\rightarrow \text{select}(\text{TCond}_j)\). Semantic non-interference of \(\text{Post}_t\) holds, because the set of \(T_k\) instances produced from \(S_i\) is disjoint from the set produced from \(S_j\), although syntactic non-interference fails. Cleanup constraints can be derived from the invariants as for the previous cases. The vertical variant is treated similarly.

Entity Splitting (Section IV) involves one source entity type mapping to two or more different target entity types. As for entity merging, there are two versions of this pattern: (i) two or more separate postconditions on \(S_i\), with disjoint \(\text{SCond}_i\) conditions, mapping to distinct target entity types \(T_k\), \(T_j\); (ii) a single constraint which maps one \(S_i\) instance to multiple linked instances of different \(T_j\). The first case is the reverse of Entity Merging (horizontal), and can be treated in a similar way to the Structure Preservation case, provided that syntactic or semantic non-interference of \(\text{Post}_t\) holds. The second case is common in refinement transformations, and in some migrations. Constraints, eg., \(C_1\), will have the form

\[
S_1 ::
\text{SCond}_1(\text{self}) \implies T_1 \rightarrow \text{exists}(t|1.t1ld = sld & T_2 \rightarrow \text{exists}(t|2.t2ld = sld & T\text{Cond}_1(t1) & T\text{Cond}_2(t1, t2) & P_1(s, t1, t2)))
\]

Both \(t1\) and \(t2\) are given \(id\) values \(self.sld\) (in the case that \(T_1\) and \(T_2\) are not disjoint, distinct identifier values derived 1-1 from source instances should be used instead). This should be the only constraint in the transformation that creates \(T_2\) instances. Other constraints can create \(T_1\) instances if their \(T\text{Cond}\) conditions are disjoint from \(T\text{Cond}_1\).

\(\text{Inv}_v\) is of the form

\[
T_1 ::
\text{TCond}_1(\text{self}) & \text{t2} : T_2 & t2.t2ld = tld & T\text{Cond}_2(\text{self}, t2) \implies S_1 \rightarrow \text{exists}(s|1ld = s.sld & \text{SCond}_1(s) & P_1(s, self, t2))
\]

The \(t2\) : \(T_2\) expression acts like an additional \(T_2\rightarrow for\text{All}(t2)\ldots\) quantifier over the remainder of the constraint. The conjunction \(t2 : T_2 \& t2.t2Id = tld\) can be optimised to \(t2 = T_2[t1ld]\). For this type of rule, \(S_1\rightarrow \text{select}(\text{SCond}_1)\) is isomorphic to \(T_1\rightarrow \text{select}(\text{TCond}_1)\), however parts of the data of elements \(s: S_i\) may be represented in the \(t2 : T_2\) instances linked to the \(t1 : T_1\) instance corresponding to \(s\), rather than directly in \(t1\).

The cleanup constraints for such constraints are:

\[
T_1 ::
\text{TCond}_1(\text{self}) & t2 = T_2[t1ld] & \text{TCond}_2(\text{self}, t2) & \text{not}(S_1 \rightarrow \text{exists}(s|t1ld = s.sld & \text{SCond}_1(s))) \implies \text{self} \rightarrow \text{isDeleted}() & t2 \rightarrow \text{isDeleted}()
\]
The effect of such a bx is that a ‘cluster’ of target instances (such as t1, t2) are related to each source instance, with all elements of the cluster having identities based on the source instance identity value. An example in UML2C is the mapping of a UML class to a CStruct and a CPointerType.

Again, \( \text{stat}_{LC}(\text{Post}_t) \) establishes \( \text{Post}_t \) and preserves \( \text{Inv}_t \), whilst \( \text{stat}_{LC}(\text{Cleanup}) \) together with \( \text{stat}_{LC}(\text{Post}_t) \) establishes \( \text{Inv}_t \). Thus correctness follows. Hippocraticness holds because target model pairs (or clusters) \( t1, t2, \ldots \) are only deleted if they do not correspond to a source instance. Unique Instantiation can apply to multiple exists quantifiers in the same manner as to single quantifiers. Local hippocraticness applies to a source entity type instance and its corresponding target cluster. The principle of least change follows from the minimality of target cluster. The principle of least change follows from the minimality of target cluster.

From this the cleanup constraints can be derived as for Phased Construction above. The cleanup constraints propagate deletion of \( E \) instances to \( F \) instances. The operation calls propagate feature changes and object creation from the source to the target model – for elements that the operation is applied to. The specifier should ensure that the operation is always invoked on all instances of \( E \) satisfying \( \text{ECond} \).

For the Map Objects before Links pattern (Figure 2), the construction of target instances is separated from the linking of these instances. In the case that \( S_i \) corresponds to \( T_j \) and \( SRef \) to \( TRef \) via one of the other patterns considered above, the linking constraints have the form:

\[
\begin{align*}
S_i &::= T_j[\text{id}\_S_i].rr = TRef[.\text{id}\_SRef] \\
T_j &::= S_i[\text{id}\_T_j].r = SRef[.\text{id}\_TRef]
\end{align*}
\]

These define target model association ends \( rr \) from source model association ends \( r \), looking-up target model elements \( T_j[\text{id}\_S_i] \) and \( TRef[.\text{id}\_SRef] \) which have already been created by preceding constraint(s). The linking constraints can be inverted to a dual form which defines source data from target data as:

\[
\begin{align*}
T_j &::= S_i[\text{id}\_T_j].r = SRef[.\text{id}\_TRef] \\
S_i &::= T_j[\text{id}\_S_i].rr \subseteq TRef[.\text{id}\_SRef]
\end{align*}
\]

That is, every element of \( t.rr \) should correspond to an element of \( s.r \), if \( s \) and \( t \) correspond.

Cleanup constraints are not needed for linking constraints, because deletion of \( SRef \) instances is propagated to deletion of \( TRef \) instances by the cleanup constraint for \( TRef \) construction (destruction of an instance includes removing it from every association end in which it resides, in UML-RSDS semantics). Other modifications to \( r \) are propagated to \( rr \) by the linking constraint itself.

By a similar argument to the previous cases, bx correctness, hippocraticness and least change can be shown. The re-establishment of \( \text{Post}_t \) and \( \text{Inv}_t \) for corresponding source and target elements is now performed by combination of the construction and linking \( \text{Post}_t \) constraints.

REFERENCES


K. Lano et al.: Declarative Specification of bx Using Design Patterns


KEVIN LANO has worked for over 25 years in the fields of system specification and verification. He was one of the originators of model-driven engineering, and has been a leading advocate of improving the precision of software modeling, and in applying software engineering principles to transformation construction. In recent years, he has worked on the integration of model-based development and agile development.

SHEKOUFEH KOLAHDOUZ-RAHIMI received the Ph.D. degree in computer science from Kings College London, in 2013. She is an Assistant Professor with the Computer Engineering Department, University of Isfahan, where she is an Active Member of the Model Driven Software Engineering Research Group. Her research interests include design patterns for model transformation, specification and verification of model transformations, bidirectional model transformation, domain-specific modeling languages, and search-based software engineering.

SOBHAN YASSIPOUR-TEHRANI has been working on requirements engineering (RE) in model transformations (MT). He has developed a RE technique suitability framework for MT projects by which the developer(s) are able to select the most appropriate RE technique for a particular requirement or a set of requirements. His research interests include RE, MT, goal modeling, and agile software development.

* * *

KEVIN LANO

SHEKOUFEH KOLAHDOUZ-RAHIMI

SOBHAN YASSIPOUR-TEHRANI