Towards Rigorously Faking Bidirectional Model Transformations

Christopher M. Poskitt\textsuperscript{1*}, Mike Dodds\textsuperscript{2}, Richard F. Paige\textsuperscript{2}, and Arend Rensink\textsuperscript{3}

\textsuperscript{1} Department of Computer Science, ETH Zürich, Switzerland
\textsuperscript{2} Department of Computer Science, The University of York, UK
\textsuperscript{3} Department of Computer Science, University of Twente, The Netherlands

Abstract. Bidirectional model transformations (\textit{bx}) are mechanisms for automatically restoring consistency between multiple concurrently modified models. They are, however, challenging to implement; many model transformation languages not supporting them at all. In this paper, we propose an approach for automatically obtaining the consistency guarantees of \textit{bx} without the complexities of a \textit{bx} language. First, we show how to “fake” true bidirectionality using pairs of unidirectional transformations and inter-model consistency constraints in Epsilon. Then, we propose to automatically verify that these transformations are consistency preserving—thus indistinguishable from true \textit{bx}—by defining translations to graph rewrite rules and nested conditions, and leveraging recent proof calculi for graph transformation verification.

1 Introduction and Motivation

Model transformations are operations for automatically translating models conforming to one language (i.e. a metamodel) into models conforming to another, in a way that maintains some sense of consistency between them. At their most basic, model transformations are unidirectional: given a source model (e.g. some high-level yet user-modifiable view of a system), they generate a target model (perhaps a lower-level view, such as code) whose data is “consistent” with the source, in a sense that is either left implicit, or captured by textual constraints or an inter-model consistency relation.

Many situations arise where the source and target models may both be modified by users in concurrent engineering activities, e.g. when integrating parts of systems that are modelled separately but must remain consistent. Bidirectional model transformations (\textit{bx}) \cite{5,17} are a mechanism for automatically restoring inter-model consistency in such a scenario; in particular, \textit{bx} simultaneously describe transformations in both directions—from source to target and target to source—with their compatibility guaranteed by construction \cite{5}.

While this advantage is certainly an attractive one, \textit{bx} are challenging to implement on account of the inherent complexity that they must encode. Model transformation languages supporting them often do so with conditions: some require that \textit{bx} are bijective (e.g. BOTL \cite{3}), essentially restricting their use to models presenting identical data in

\* Received funding from the European Research Council under the European Union’s Seventh Framework Programme (FP7/2007-2013) / ERC Grant agreement no. 291389.
different ways, whereas others require users to work with specific formalisms such as
triple graph grammars (e.g. MOFLON \cite{Behr:2001}). The QVT-R language—part of the OMG’s
Queries, Views, and Transformations standard—allows bx to be expressed, but suffers
an ambiguous semantics \cite{Wolter:2006} and limited tool support (the most successful ones often
departing from the original semantics \cite{Wadhwa:2008}). Moreover, many modern transformation
languages do not provide any support for bx (e.g. ATL \cite{Prasad:2006}), meaning that users must ex-
press them as two separate unidirectional transformations. While this seems a practical
workaround, it comes with the major risk that the compatibility of the transformations
might not be maintained over time.

A trade-off between the benefits (but complexity) of bx and the practicality (but
possible incoherence) of unidirectional transformations can be achieved in Epsilon, a
platform of interoperable model management languages. Epsilon has languages sup-
sporting the specification of unidirectional transformations in either a rule-based (ETL),
update-in-place (EWL), or operational (EOL) \cite{Rothermel:2013} style. Furthermore, it provides an
inter-model consistency language (EVL \cite{Rothermel:2013}) that can be used to express and evaluate
constraints between models conforming to different metamodels. With these languages
together, bx can be “faked” in a practical way, by: (1) defining pairs of unidirectional
transformations for separately updating the source and target models; and (2) defining
“consistency” via inter-model constraints in EVL, the violation of which will trigger
appropriate transformations to restore consistency.

Although this process gives us a means of checking consistency and automatically
triggering a transformation to restore it, we lack the important guarantee that bx give
us: the compatibility of the transformations. It might be the case that after the execution
of one transformation, the other does not actually restore consistency, leading to further
EVL violations. How do we check for, and maintain, compatibility?

We aim to address this shortcoming and obtain the guarantees of bx without the need
for bx languages. Instead, we will use rigorous proof techniques to verify that faked bx
are consistency preserving, and thus indistinguishable to users from true bx. To this end,
we propose to apply techniques from graph transformation verification. Given a faked
bx in Epsilon, we will model the unidirectional transformations as graph transformation
rules, and EVL constraints as nested graph conditions \cite{Gogolla:2004}. Then, by leveraging graph
transformation proof calculi \cite{Gorlach:2011,Gorlach:2012} in a weakest precondition style, we aim to auto-
matically prove compatibility of the unidirectional transformations with respect to the
EVL constraints. Furthermore, we aim to exploit the model checker GROOVE \cite{Gorlach:2012}
to automatically search for counterexamples when consistency preservation does not hold.

The overarching goal of our work is to achieve the ideal that Stevens \cite{Stevens:2006} con-
templated in her survey of bx: that “if a framework existed in which it were possible
to write the directions of a transformation separately and then check, easily, that they
were coherent, we might be able to have the best of both worlds.”

2 Example bx in Epsilon: Class Diagrams to Databases

To illustrate the ideas of our proposal, we recall a common model transformation prob-
lem that concerns the consistency of class diagram and relational database models
(CD2RDBM). Class diagram models conform to a simple language describing famil-
iar object-oriented concepts (e.g. classes, attributes, relationships), whereas relational database models conform to a language describing how databases are constructed (e.g. tables, columns, primary keys). Here, consistency is defined in terms of a correspondence between the data in the models, e.g. every table \( n \) corresponds to a class \( n \), and every column \( m \) corresponds to an attribute \( m \). Figure 1 contains two simple models that are consistent in this sense (we omit the metamodels for lack of space).

Users of the models should be able to create new classes (or tables) whilst maintaining inter-model consistency. A \( bx \) would be well suited for this: upon the creation of a new class (resp. table), a table (resp. class) should be created with the same name to restore consistency. We can fake this simple \( bx \) in Epsilon with a pair of unidirectional transformations (one for updating the class diagram model, one for updating the relational database) and a set of EVL constraints. For the former, we can use the Epsilon Wizard Language (EWL) to define a pair of update-in-place transformations, \( \text{AddClass} \) and \( \text{AddTable} \) (for simplicity, here we assume the new class/table name \( \text{newName} \) to be pre-determined and unique, but Epsilon does support the capturing and sharing of such data between wizards).

Using the Epsilon Validation Language (EVL), we express the relevant notion of inter-model consistency: that for every class \( n \), there exists a table named \( n \) (and vice versa). If one of the constraints is violated, Epsilon can automatically trigger the relevant transformation to attempt to restore consistency. For example, after executing the transformation \( \text{AddClass} \), the constraint \( \text{TableExists} \) will be violated, indicating that the transformation \( \text{AddTable} \) should be executed to restore consistency.

This example of a \( bx \), “faked” in Epsilon, is a deliberately simple one chosen to illustrate the concepts. Note even that the CD2RDBM problem can lead to more interesting (i.e. less symmetric) \( bx \), e.g. manipulating inheritance in the class model.

### 3 Checking Compatibility of the Transformations

The critical difference between the “faked” \( bx \) in the previous section and a true \( bx \) is the absence of guarantees about the compatibility of the transformations: upon the violation of \( \text{TableExists} \), for example, does the execution of \( \text{AddTable} \) actually restore...
consistency? For this simple example, a manual inspection will quickly confirm that the transformations are indeed compatible in this sense. But what about more intricate $bx$? And what about $bx$ that evolve and change over time? For the Epsilon-based approach to be a convincing alternative to a $bx$ language, it is imperative that the compatibility (or not) of the transformations can be checked, and—crucially—that this can be done in a simple and automatic way. To this end, we propose to leverage and adapt some recent developments in the verification of graph transformations.

Graph transformation is a computation abstraction: the state of a computation is represented as a graph, and the computational steps as applications of rules (i.e., akin to string rewriting in Chomsky grammars, but lifted to graphs). Modelling a problem using graph transformation brings an immediate benefit in visualisation, but also an important one in terms of semantics: the abstraction has a well-developed algebraic theory that can be used for formal reasoning. This has been exploited to facilitate the verification of graph transformation systems, i.e., calculi for systematically proving specifications about graph properties before and after any execution of some given rules. Furthermore, such calculi have been generalised to graph programs, which augment the abstraction with expressions over labels and familiar control constructs (e.g., sequential composition, branching) for restricting the application of rules.

Habel et al. developed weakest precondition calculi for proving specifications of the form $\{pre\} P \{post\}$, which express that if a graph satisfies the precondition $pre$, then any graph resulting from the execution of graph program $P$ will satisfy the postcondition $post$; these pre- and postconditions expressed using nested conditions, a graphical formalism for first-order (FO) structural properties over graphs. They defined constructions that, given a nested condition $post$ and program $P$, would return a weakest liberal precondition $Wlp(P, post)$, representing the weakest property that must hold for successful executions of $P$ to establish $post$. The specification would then be (dis)proven by checking the validity of $pre \Rightarrow Wlp(P, post)$ in an automatic FO theorem prover. Poskitt and Plump developed proof calculi in a similar spirit, separately addressing two extensions: programs and properties involving attribute manipulation, and reasoning about non-local structural properties.

We aim to exploit this work to check the compatibility of transformations in the Epsilon approach to $bx$. In particular, we are developing automatic translations of EWL transformations to graph programs (denoted $PS, PT$ for the source and target updates respectively), and translations from EVL constraints to nested conditions (denoted $evl$). Then, the task of checking compatibility of the transformations, as shown in Figure 2, reduces to proving the specifications $\{evl\} PS; PT \{evl\} PT; PS \{evl\}$ (here we assume the input graphs to be disjoint unions of the two models). Intuitively: if the models are consistent to start with, and executing the transformations in either order maintains consistency, then the transformations are compatible.

The technical challenges of the process fall into two main parts: computing the abstractions, and checking validity. Defining translations for the former requires care: we need to determine how much of the EWL language can be handled, we need to ensure that the graph-based semantics we abstract them to is “correct”, and we need to adapt the proof technology to our specific needs. The work in [14][15][16], for example, does not presently support type graphs (causing more effort to encode conformance to
Fig. 2. Overview of the process for checking compatibility of the transformations

metamodels). Similar concerns must be addressed for the translations of EVL to nested conditions (we can take inspiration from recent work on such translations for core OCL [2]). For the challenge of checking validity, we aim to leverage existing EVL to FO theorem provers (e.g. Vampire) as much as possible, adapting existing translations of nested conditions to FO logic [7,14]. Given the undecidability of FO validity, we also aim to explore the use of the GROOVE model checker [6] in finding counterexamples when the theorem provers respond with “no”, or do not appear to terminate.

Our example bx for the CD2RDBM problem is easily translated into graph programs and nested conditions, as given in Figure 3. The programs $P_S$, $P_T$ are the individual rules creating respectively a class or table node labelled $newName$ (here, $\emptyset$ denotes the empty graph, indicating that the rules can be applied without first matching any structure, i.e. unconditionally). The nested condition $evl$, given on the right, expresses that for every class (resp. table) node, there is a table (resp. class) node with the same name (we do not define here a formal interpretation, but note that $x$, $y$ are variables, and that the numbers indicate when nodes are the same down the nesting of the formula). Were the weakest liberal preconditions to be constructed, we would find:

$$Wlp(P_S; P_T, evl) \equiv Wlp(P_T; P_S, evl) \equiv evl.$$ 

Since $evl \Rightarrow evl$ is clearly valid, both $\{evl\} P_S; P_T \{evl\}$ and $\{evl\} P_T; P_S \{evl\}$ must hold, and—assuming correctness of the abstractions—the original EWL transformations are therefore compatible with respect to the EVL constraints.

Fig. 3. Our CD2RDBM bx expressed as graph transformation rules and a nested condition

4 Next Steps

After further exploring the CD2RDBM example, we will identify a selection of bx case studies—from the community repository [4] and beyond—that exhibit a broader range of characteristics and challenges to address. We will implement these bx using EWL transformations and EVL constraints, then manually translate them into graph transformations and nested conditions. These will serve as a proof of concept, but also as
guidance, helping us to determine how far we should adapt the proof calculi to support our goals (e.g. introducing type graphs for capturing the metamodels). After implementing the weakest precondition calculations and translations to FO logic, we will design and implement automatic translations from Epsilon $\mathcal{K}$ to their corresponding graph-based abstractions, initially focusing on a core (but expressive) subset of the languages. Finally, we will explore the use of GROOVE in finding counterexamples when verification fails, by exploring executions of the graph transformation rules.

References