Ensuring Correctness of Model Transformations while Remaining Decidable *

Jon Haël Brenas[1], Rachid Echahed[1], and Martin Strecker[2]

[1] CNRS and Université de Grenoble Alpes
[2] Université de Toulouse / IRIT

Abstract. This paper is concerned with the interplay of the expressiveness of model and graph transformation languages, of assertion formalisms making correctness statements about transformations, and the decidability of the resulting verification problems. We put a particular focus on transformations arising in graph-based knowledge bases and model-driven engineering. We then identify requirements that should be satisfied by logics dedicated to reasoning about model transformations, and investigate two promising instances which are decidable fragments of first-order logic.

Keywords: Graph Transformations, Programming Language Semantics, Description Logic, Modal Logic, Model Theory

1 Introduction

We tackle the problem of model transformations and their correctness, where transformations are specified with the aid of rules and correctness properties are stated as logical formulas. By model we intend a graph structure enriched with logical formulas which label either nodes and edges. In our approach, a rule is composed of a left-hand side which is a graph annotated with logical formulas, and a right-hand side which is a sequence of actions. The shape of the graph and the formulas yield an applicability condition of the rule at a matching subgraph of the model; the right-hand side transforms this subgraph with actions such as creation, deletion or cloning of nodes or insertion and deletion of arcs.

Rewrite systems come with a specification in the form of pre- and postconditions, and we aim at full deductive verification, ascertaining that any model satisfying the precondition is transformed into a model satisfying the postcondition.

The correctness of model transformations has attracted some attention in the last years. One prominent approach is model checking, such as implemented by the Groove tool [13]. The idea is to carry out a symbolic exploration of the state space, starting from a given model, in order to find out whether certain invariants are maintained or certain states (*i.e.* , model configurations) are reachable. The

* This research has been supported by the *Climt* project (ANR-11-BS02-016).

Viatra tool has similar model checking capabilities [26] and in addition allows the verification of elaborate well-formedness constraints imposed on models [24]. Well-formedness is within the realm of our approach (and amounts to checking the consistency of a formula), but is not the primary goal of this paper which is on the dynamics of models.

The Alloy analyser [18] uses bounded model checking for exploring relational designs and transformations (see for example [5] for an application in graph transformations). Counter-examples are presented in graphical form. All the aforementioned techniques use powerful SAT- or SMT-solvers, but do not carry out a complete deductive verification. In our paper, we aim at full-fledged verification of transformations.

General-purpose program verification with systems such as AutoProof [25] and Dafny [19] becomes increasingly automated and thus interesting as push-button technology for model transformations. In this context, fragments of first-order logic have been proposed that are decidable and are useful for dealing with pointer structures [17].

The question explored in this paper is: which requirements does a logic have to fulfill in order to allow for such a verification technique to succeed?

Several different logics have been proposed over the years to tackle the problem of graph transformation verification. Among the most prominent approaches figure nested conditions [15,21] that are explicitly created to describe graph properties. Another widely used logic in graph transformation verification is monadic second-order logic [10,22] that allows to go beyond first-order definable properties. [4] introduces a logic closer to modal logic that allows to express both graph properties and the transformations at the same time.

Nonetheless, these approaches are not flawless. They are all undecidable in general and thus either cannot be used to prove correctness of graph transformations in an automated way or only work on limited classes of graphs. Starting from the other side of the logical spectrum, one could consider using Description Logics to describe graph properties [1,6] that are decidable. Another choice could be the use of modal logics as they are suited to reason about programs. Obviously, this comes at a cost in term of expressiveness.

Separation logic [23] is another choice that is worth considering when dealing with transformations of graphs. It has been developed especially to be able to talk about pointers in conventional programming languages.

In this paper, we proceed in an orthogonal direction. Instead of introducing a logic and advising users to tailor their problem so that it is expressible in our logic and that its models comply with the restrictions so that the verification is actually possible, we aim at providing a means for the users to decide whether the logic they have used to represent their problem will actually allow them to prove their transformations correct or whether they have to use several different systems in parallel.

We are in particular interested in decidable logics, and so we instantiate our general framework with two decidable logics: Two-variable logic with counting (in Section 5.1) and logics with exists-forall-prefix (in Section 5.2). The fragment

of effectively propositional logic [20], that is implemented by the Z3 prover [11] and is closely related to the logical fragment we discuss in Section 5.2, has been known for a long time to be decidable [8]. The use of two-variable logics [14] for the verification of model transformation is relatively novel even though it contains all Description Logics without role inclusions. Once more the goal is not to advocate the use of any logic but to give the user the ability to decide if the logics that are planned to be used satisfy some minimal conditions so that the verification works.

The rest of the paper is structured as follows: we start with an example, in Section 2, motivating our model transformation approach, which we then make more formal in Section 3. We expose general principles that a logic has to fulfill to be usable for verifying model transformations in Section 4 and then instantiate it with the two aforementioned logics in Section 5. We conclude in Section 6. Some missing proofs can be found in the appendix.

2 Motivating Example

In order to better illustrate our purpose, an example modelling a sample of the information system of a hospital is introduced. Figure 1 is the UML model of this sample.

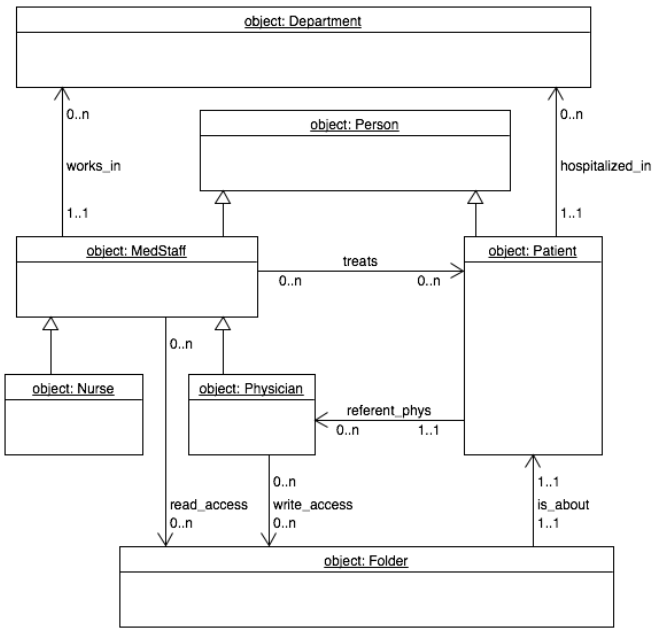

Fig. 1: A sample UML model for the hospital example

We consider persons (shortened to PE). Some of them work in the hospital and form the medical staff (MS) and others are patients (PA). The medical staff is partitioned into physicians (PH) and nurses (NU). In addition, the hospital is split into several departments (DE) or services. Documents pertaining to patients are stored in folders (FO).

Each member of the medical staff is assigned (denoted by *works_in*) to a department. The same way, each patient is hospitalized (*hospital_in*) in one of the departments. There may be several members of the medical staff that may collaborate to treat (*treats*) a patient at a given time but one of them is considered as the referent physician (*ref_phys*), that is to say she is in charge of the patient. Part of the medical staff can access the folder containing the documents about (*is_about*) a patient either to read (*read_access*) or to write (*write_access*) information.

The fact is the hospital is bound to evolve: new patients arrive to be cured and others leave, new medical staffers are hired and others move out. To illustrate our purpose, four possible transformations are defined below.

Transformation 1 *The first transformation is New_Ph(*PH_1, D_1*). It creates a new physician to which is associated an identifier* PH_1*. This physician will be working in the department identified with* D_1*.*

Transformation 2 *The second transformation is New_Pa(*PA_1, PH_1, FO_1*). It adds a new patient. The patient* PA_1 *is created alongside his folder* FO_1*. He is then assigned* PH_1 *as referent physician.*

Transformation 3 *The third transformation is Del_Pa(*PA_1*). It removes patient* PA_1*.*

Transformation 4 *The last transformation is Del_Ph(*PH_1, PH_2*). It deletes the physician* PH_1 *and forwards all his patients to the physician* PH_2*.* PH_1 *and* PH_2 *have to work in the same department.*

Despite the transformations, there are some properties of the hospital that should not be altered. We give a list of six such expected properties in the following.

Expected property 1 *Each member of the medical staff is either a nurse or a physician but not both.*

Expected property 2 *All patients and all medical staffers are persons.*

Expected property 3 *Each person that can write in a folder can also read it.*

Expected property 4 *Each person that can read a folder about a patient treats that patient.*

Expected property 5 *Only medical staffers can treat persons and only patients can be treated.*

Expected property 6 *Every patient has exactly one referent physician.*

3 A Model Transformation Framework

In this section, a framework used to describe models as well as their transformations is introduced. A model is considered hereafter as a graph, labeled by logical formulae. The logic in which these formulae are expressed is considered as a parameter, say $\mathcal{L}$ of the proposed framework. Required features of such a logic are discussed in the next section. Nevertheless, we assume in this section that the logic $\mathcal{L}$ is endowed with a relation $\models$ over its formulae. That is to say, $n \models B$ (resp. $e \models B$) should be understood as "formula B is satisfied at node n (resp. edge e)".

Definition 1 (Graph). *Let $\mathcal{L}$ be a logic. A* graph *G is a tuple (N, E, $\mathcal{C}$, $\mathcal{R}$, ϕ_N, ϕ_E, s, t) where N is a set of* nodes*, E is a set of* edges*, $\mathcal{C}$ is a set of* (node) formulae *(of $\mathcal{L}$) or* concepts*, $\mathcal{R}$ is the set of* edge formulae *(of $\mathcal{L}$) or* roles*, ϕ_N is the* node labeling *function, $\phi_N : N \to \mathcal{P}(\mathcal{C})$, ϕ_E is the* edge labeling *function, $\phi_E : E \to \mathcal{R}$, s is the* source function *$s : E \to N$ and t is the* target function *$t : E \to N$.*

Labeling a graph with logical formulae is quite usual in Kripke structures. In this paper, labeling formulae will play a role either in the transformation process or in the generation of proof obligations for the properties intended to be proved.

Transformations of models are performed by means of graph rewrite systems. These rewrite systems are extensions of those defined in [12] where graphs are labeled with formulae. Thus, the left-hand sides of the rules are labeled graphs as defined in Definition 1, whereas the right-hand sides are defined as sequences of elementary actions. Elementary actions constitute a set of basic transformations used in graph transformation processes. They are given in the following definition.

Definition 2 (Elementary action, action). *An* elementary action*, say a, has one of the following forms:*

- *a* concept assignment *$c := i$ where i is a node and c is an atomic formula (a unary predicate). It sets the valuation of c such that the only node labeled by c is i.*
- *a* concept addition *$c := c + i$ (resp.* concept deletion *$c := c - i$) where i is a node and c is an atomic formula (a unary predicate). It adds the node i to (resp. removes the node i from) the valuation of the formula c.*
- *a* role addition *$r := r + (i, j)$ (resp.* role deletion *$r := r - (i, j)$) where i and j are nodes and r is an atomic role (a binary predicate). It adds the pair (i, j) to (resp. removes the pair (i, j) from) the valuation of the role r.*
- *a* node addition *$new(i)$ (resp.* node deletion *$del_I(i)$) where i is a new node (resp. an existing node). It creates the node i. i has no incoming nor outgoing edge and there is no atomic formula such that i belongs to its valuation (resp. it deletes i and all its incoming and outgoing edges).*
- *a* global incoming edge redirection *$i \gg^{in} j$ where i and j are nodes. It redirects all incoming edges of i towards j.*

– *a* global outgoing edge redirection $i \gg^{out} j$ *where* i *and* j *are nodes. It redefines the source of all outgoing edges of* i *as* j*.*
– *a* node cloning $clone(i, i')$ *where* i *is a node,* i' *is a node that does not exist yet. It creates a new node* i' *that has the same labels as* i *and the same incoming and outgoing edges.*

The result of performing the elementary action α *on a graph* $G = (N^G, E^G, \mathcal{C}^G, \mathcal{R}^G, \phi_N^G, \phi_E^G, s^G, t^G)$*, written* $G[\alpha]$*, produces the graph* $G' = (N^{G'}, E^{G'}, \mathcal{C}^{G'}, \mathcal{R}^{G'}, \phi_N^{G'}, \phi_E^{G'} s^{G'}, t^{G'})$ *as defined in Figure 2. An* action*, say* α*, is a sequence of elementary actions of the form* $\alpha = a_1; a_2; \ldots; a_n$*. The result of performing* α *on a graph* G *is written* $G[\alpha]$*.* $G[a; \alpha] = (G[a])[\alpha]$ *and* $G[\epsilon] = G$*,* ϵ *being the empty sequence.*

Definition 3 (Rule, Graph Rewrite Systems). *A* rule $\rho[\boldsymbol{n}]$ *is a pair* (lhs,α) *where* $\boldsymbol{n}$ *is a vector of concept variables. These variables are instantiated by means of actual concepts when a rule is applied.* lhs*, called the left-hand side, is a graph and* α*, called the right-hand side, is an action. Rules are usually written* $\rho[\boldsymbol{n}] : lhs \rightarrow \alpha$*. Concept variables* n_i *in* $\boldsymbol{n}$ *may appear both in* lhs *and in* α*. A graph rewrite system is a set of rules.*

The rewrite systems defined above could be seen as a generalization of [7] where the labeling logic is a parameter, with an additional elementary action which is dedicated to node cloning. There are many ways to define node cloning. We have chosen here an operational semantics which has the same effect as the one defined by means of sesquipushout [9].

Notice that a rule $\rho[\boldsymbol{n}] : lhs \rightarrow \alpha$ may be considered as a generic rule which yields an actual rewrite rule for every instance of the variables $\boldsymbol{n}$. We write $\rho[\boldsymbol{c}]$ to denote the rule obtained from $\rho[\boldsymbol{n}] : lhs \rightarrow \alpha$ by replacing every variable concept n_i appearing either in lhs or in α by the actual concept c_i. Now let us define when a rule can be applied to a graph.

Definition 4 (Match). *Let* $\rho[\boldsymbol{n}] : lhs \rightarrow \alpha$ *be a rule and* G *be a graph. Let* $\rho[\boldsymbol{c}]$ *be the instance of rule* $\rho[\boldsymbol{n}]$ *and* $inst$ *be the instance function defined as* $inst(n_i) = c_i$ *for* $i \in \{0, \ldots, k\}$*. We say that the instance* $\rho[\boldsymbol{c}]$ *matches the graph* G *via the* match $h = (h_N, h_E)$*, where* $h_N : N_{lhs} \rightarrow N_G$ *and* $h_E : E_{lhs} \rightarrow E_G$ *if the following conditions hold:*

1. $\forall n \in N_{lhs}, \forall c \in \phi_{N_{lhs}}(n), h_N(n) \models inst(c)$
2. $\forall e \in E_{lhs}, \forall r \in \phi_{E_{lhs}}(e), h_E(e) \models inst(r)$[3]
3. $\forall e \in E_{lhs}, s_G(h_E(e)) = h_N(s_{lhs}(e))$
4. $\forall e \in E_{lhs}, t_G(h_E(e)) = h_N(t_{lhs}(e))$

[3] $inst(r)$ (resp. $inst(c)$) replaces in r (resp. in c) every occurrence of a concept variable n_i by its instance c_i. The formal definition of the function $inst$ depends on the structure of the considered concepts.

If $\alpha = c := i$ **then:**
$N^{G'} = N^G, E^{G'} = E^G, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G$
$\phi_N^{G'}(n) = \begin{cases} \phi_N^G(n) \cup \{c\} \text{ if } n = i \\ \phi_N^G(n) \backslash \{c\} \quad \text{if } n \neq i \end{cases}, \phi_E^{G'} = \phi_E^G,$
$s^{G'} = s^G$, $t^{G'} = t^G$

If $\alpha = c := c + i$ **then:**
$N^{G'} = N^G, E^{G'} = E^G, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G,$
$\phi_E^{G'} = \phi_E^G, \phi_N^{G'}(n) = \begin{cases} \phi_N^G(n) \cup \{c\} \text{ if } n = i \\ \phi_N^G(n) \quad \text{if } n \neq i \end{cases}$
$s^{G'} = s^G$, $t^{G'} = t^G$

If $\alpha = c := c - i$ **then:**
$N^{G'} = N^G, E^{G'} = E^G, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G,$
$\phi_E^{G'} = \phi_E^G$, $\phi_N^{G'}(n) = \begin{cases} \phi_N^G(n) \backslash \{c\} \text{ if } n = i \\ \phi_N^G(n) \quad \text{if } n \neq i \end{cases}$
$s^{G'} = s^G$, $t^{G'} = t^G$

If $\alpha = r := r + (i, j)$ **then** :
$N^{G'} = N^G, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G,$
$E^{G'} = E^G \cup \{e\}$ where e is a new element
$\phi_N^{G'} = \phi_N^G$, $\phi_E^{G'}(e') = \begin{cases} r \quad \text{if } e' = e \\ \phi_E^G(e') \text{ if } e' \neq e \end{cases}$,
$s^{G'}(e') = \begin{cases} i \quad \text{if } e' = e \\ s^G(e') \text{ if } e' \neq e \end{cases}$,
$t^{G'}(e') = \begin{cases} j \quad \text{if } e' = e \\ t^G(e') \text{ if } e' \neq e \end{cases}$

If $\alpha = r := r - (i, j)$ **then:**
$N^{G'} = N^G, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G$
$E^{G'} = E^G \backslash r_{i,j},$
$\phi_N^{G'} = \phi_N^G, \phi_E^{G'}$ is the restriction of ϕ_E^G to $E^{G'}$
$s^{G'}$ is the restriction of s^G to $E^{G'}$
$t^{G'}$ is the restriction of t^G to $E^{G'}$

If $\alpha = new(i)$ **then:**
$N^{G'} = N^G \cup \{i\}$ where i is a new node,
$E^{G'} = E^G, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G,$
$\phi_N^{G'}(n') = \begin{cases} \emptyset \quad \text{if } n' = n \\ \phi_N^G(n') \text{ if } n' \neq n \end{cases}$
$\phi_E^{G'} = \phi_E^G$, $s^{G'} = s^G$, $t^{G'} = t^G$

If $\alpha = del(i)$ **then:**
$N^{G'} = N^G \backslash \{i\}, \mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G,$
$E^{G'} = E^G \backslash \{e | s^G(e) = i \vee t^G(e) = i\}$
$\phi_N^{G'}$ is the restriction of ϕ_N^G to $N^{G'}$
$\phi_E^{G'}$ is the restriction of ϕ_E^G to $E^{G'}$
$s^{G'}$ is the restriction of s^G to $E^{G'}$
$t^{G'}$ is the restriction of t^G to $E^{G'}$

If $\alpha = i \gg^{in} j$ **then** :
$N^{G'} = N^G, E^{G'} = E^G, \mathcal{C}^{G'} = \mathcal{C}^G,$
$\mathcal{R}^{G'} = \mathcal{R}^G, \phi_N^{G'} = \phi_N^G, \phi_E^{G'} = \phi_E^G,$
$s^{G'} = s^G, t^{G'}(e) = \begin{cases} j \quad \text{if } t^G(e) = i \\ t^G(e) \text{ if } t^G(e) \neq i \end{cases}$

If $\alpha = i \gg^{out} j$ **then:**
$N^{G'} = N^G, E^{G'} = E^G, \mathcal{C}^{G'} = \mathcal{C}^G,$
$\mathcal{R}^{G'} = \mathcal{R}^G, \phi_N^{G'} = \phi_N^G, \phi_E^{G'} = \phi_E^G,$
$\phi_N^{G'} = \phi_N^G, t^{G'} = t^G,$
$s^{G'}(e) = \begin{cases} j \quad \text{if } s^G(e) = i \\ s^G(e) \text{ if } s^G(e) \neq i \end{cases}$

If $\alpha = clone(i, i')$ **then:**
$N^{G'} = N^G \cup \{i'\}$, $E^{G'} = E^G \cup E'$
$\mathcal{C}^{G'} = \mathcal{C}^G, \mathcal{R}^{G'} = \mathcal{R}^G$
$\phi_N^{G'}(n) = \begin{cases} \phi_N^G(n) \text{ if } n \neq i' \\ \phi_N^G(i) \text{ otherwise} \end{cases}$
$\phi_E^{G'}(e) = \begin{cases} \phi_E^G(e) \text{ if } e \notin E' \\ \phi_E^G(co(e)) \text{ otherwise} \end{cases}$
$t^{G'}(e) = \begin{cases} t^G(e) \text{ if } e \notin E' \\ t^G(co(e)) \text{ if } e \in E^{out} \\ i' \text{ if } e \in E^{in} \cup E^{loop} \end{cases}$
$s^{G'}(e) = \begin{cases} s^G(e) \text{ if } e \notin E' \\ s^G(co(e)) \text{ if } e \in E^{in} \\ i' \text{ if } e \in E^{out} \cup E^{loop} \end{cases}$

Fig. 2: Summary of the effects of atomic actions where $r_{i,j} = \{e | s^G(e) = i \wedge t^G(e) = j \wedge \phi_E^G(e) = r\}, E^{in} = \{e^{in} | \exists e \in E^G, t^G(e) = i\}$, $E^{out} = \{e^{out} | \exists e \in E^G, s^G(e) = i\}$, $E^{loop} = \{e^{loop} | \exists e \in E^G, s^G(e) = t^G(e) = i\}$, $E' = E^{in} \cup E^{out} \cup E^{loop}$ and, for $e' \in E'$, $co(e')$ is the edge e that e' is a copy of.

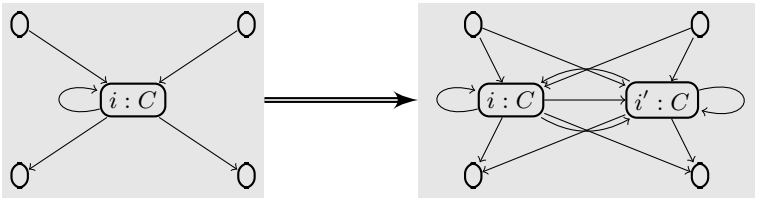

Fig. 3: Example of node cloning. The action $clone(i, i')$ is performed.

The third and the fourth conditions are classical and say that the source and target functions and the match have to agree. The first condition says that for every node n of the left-hand side, the node to which it is associated, $h_N(n)$, in G has to satisfy every concept that n satisfies. This condition clearly expresses additional negative and positive conditions which are added to the "structural" pattern matching. The second condition expresses the same conditions on the edges.

Definition 5 (Rule application). *We define the applicability condition as:* $App(\rho[\boldsymbol{c}], G)$ *iff there exists a match* h *from the instance* $\rho[\boldsymbol{c}]$ *to* G*. A graph* G *rewrites to graph* G' *using a rule* $\rho[\boldsymbol{c}] : lhs \to \alpha$ *iff* $App(\rho[\boldsymbol{c}], G)$ *and* G' *is obtained from* G *by performing actions in* $h(\alpha)$[4]*. Formally,* $G' = G[h(\alpha)]$*. We write* $G \to_{\rho[\boldsymbol{c}]} G'$ *or* $G \to_{\rho[\boldsymbol{c}],h} G'$*.*

Example 1. Let us consider again the example given in Section 2. We provide in Figure 4, for every transformation already presented informally, a corresponding rewrite rule.

Very often, transforming models by means of rewrite rules necessitates the use of the notion of strategies. Informally, a strategy acts as a recipe indicating in which order the rules are applied.

Definition 6 (Strategy). *Given a graph rewriting system* $\mathcal{R}$*, a* strategy *is a word of the following language defined by* s*:*

$s := \rho[c_0, \ldots, c_k]$ *(Rule application)* $\mid s^*$ *(Closure)*
$\quad s; s$ *(Composition)* $\mid s \oplus s$ *(Choice)*

where $\rho[c_0, \ldots, c_k]$ *is an instance of a rule in* $\mathcal{R}$*.*

We write $G \Rightarrow_{\mathcal{S}} G'$ *when* G *rewrites to* G' *following the rules given by the strategy* $\mathcal{S}$*.*

Informally, the strategy "$\rho_1; \rho_2$" means that rule ρ_1 should be applied first, followed by the application of rule ρ_2. Notice that the strategies as defined above allow one to define infinite derivations from a given graph G because we have included the Kleene star construct s^* as a constructor of strategies. Handling the Kleene star does not introduce much more difficulties but requires the use

[4] $h(\alpha)$ is obtained from α by replacing every node name, n, of lhs by $h(n)$.

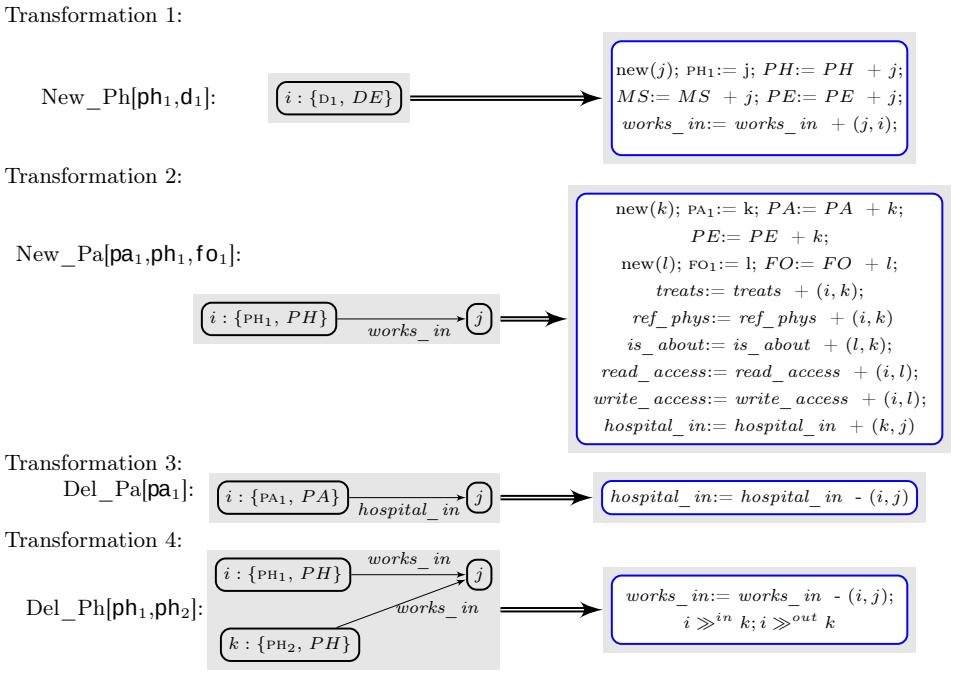

Fig. 4: Transformation rules for the sample hospital model

of the notion of invariants in the verification procedures, as it is the case for while loops in imperative languages. It also requires us to extend the notion of applicability from rules to strategies:

$\mathrm{App}(s^*, G) = \mathrm{true}$ $\quad$ $\mathrm{App}(s_0; s_1, G) = \mathrm{App}(s_0, G)$

$\mathrm{App}(s_0 \oplus s_1, G) = \mathrm{App}(s_0, G) \wedge \mathrm{App}(s_1, G)$

In Figure 5, we provide the rules that specify how strategies are used to rewrite a model (graph).

To end this section we define the notion of a specification which consists in providing *Pre* and *Post* conditions that one may want to ensure for a given strategy. More precisely, we propose the following definitions.

Definition 7 (Program, Specification). *A* program *is a tuple* $(\mathcal{R}, \mathcal{S})$ *where* $\mathcal{R}$ *is a graph rewrite system and* $\mathcal{S}$ *is a strategy.*
A specification *SP is a tuple* $(Pre,\ Post,\ \mathcal{P})$ *where Pre and Post are formulae and* $\mathcal{P}$ *is a program.*

Notice that *Pre* and *Post* are supposed to be formulae of a given logic. We do not specify such a logic in the above definition. We provide actual examples in Section 5. A specification $(Pre,\ Post,\ \mathcal{P})$ asserts that for all models G that satisfies the formula *Pre*, all models G' obtained after rewriting G according to strategy $\mathcal{S}$ of program $\mathcal{P} = (\mathcal{R}, \mathcal{S})$, (i.e. $G \Rightarrow_{\mathcal{S}} G'$), G' satisfies formula *Post*.

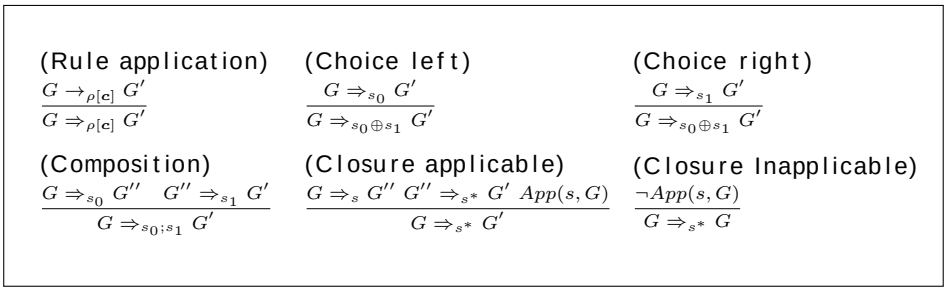

Fig. 5: Strategy application rules

4 General Logical Framework

Our aim in this section is to discuss general requirements for a logic, say $\mathcal{L}$, that one may consider either to specify pre and post conditions of specifications or to label models.

Let $SP = (Pre,\ Post,\ \mathcal{P})$ be a specification. If SP is correct, then if a model $G \models Pre$ and G rewrites to model G' via a strategy $\mathcal{S}$ of program $\mathcal{P} = (\mathcal{R}, \mathcal{S})$, then $G' \models Post$. We also provide in this section a Hoare calculus dedicated to helping prove the correctness of specifications.

The first, and most obvious, requirements for a logic, $\mathcal{L}$, is that it can express the labeling of models with formulae which specify nodes and edges.

Requirement 1 *Interpretations of node formulae (concepts) should be nodes.*

Requirement 2 *Interpretations of edge formulae (roles) should be edges.*

The conditions *Pre* and *Post* are properties of models. Thus, we have the following requirement.

Requirement 3 *Interpretations of Pre and Post assertions should be graphs (i.e., models).*

The main ingredient of the verification calculus consists in computing weakest preconditions of postconditions (see function *wp* defined in Fig 6). The basic cases of the computations of weakest precondition deal with elementary actions. For that, to every elementary action is associated a so called substitution [16]. Such substitutions are the elementary building blocks allowing the verification of a program.

Definition 8. *Let a be an elementary action, as defined in Definition 2. The substitution $[a]$ associated to a is the formula constructor that to each formula ϕ of $\mathcal{L}$ associates the formula $\phi[a]$. Given a model $\mathcal{M}$, $\phi[a]$ is defined such that $\mathcal{M} \models \phi[a] \Leftrightarrow$ for all models $\mathcal{M}', \mathcal{M}' \Rightarrow_a \mathcal{M}$ implies $\mathcal{M}' \models \phi$.*

A logic $\mathcal{L}'$ is said to be closed under substitutions if for each action a, for each formula ϕ of $\mathcal{L}'$, $\phi[a]$ is also a formula of $\mathcal{L}'$.

$$wp(\rho[\boldsymbol{c}],\ Q) = App(tag(\rho[\boldsymbol{c}])) \Rightarrow wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Q)$$
$$wp(s_0; s_1,\ Q) = wp(s_0,\ wp(s_1,\ Q)) \qquad wp(s^*) = inv_s$$
$$wp(s_0 \oplus s_1,\ Q) = wp(s_0, Q) \wedge wp(s_1, Q)$$

Fig. 6: Weakest preconditions for strategies.

$$vc(\rho[\boldsymbol{c}],\ Q) = \text{true} \qquad vc(s_0; s_1,\ Q) = vc(s_0,\ wp(s_1,\ Q)) \wedge vc(s_1, Q)$$
$$vc(s_0 \oplus s_1,\ Q) = vc(s_0, Q) \wedge vc(s_1, Q)$$
$$vc(s^*,\ Q) = (inv_s \wedge App(s) \Rightarrow wp(s, inv_s)) \wedge (inv_s \wedge \neg App(s) \Rightarrow Q) \wedge vc(s, inv_s) \wedge vc(s_1, Q)$$

Fig. 7: Verification conditions for strategies.

Weakest preconditions for actions come in two flavors: for elementary actions a, we have $wp(a, Q) = Q[a]$, and for composite actions, $wp(a; \alpha,\ Q) = wp(a,\ wp(\alpha,\ Q))$. On this basis, we can define weakest preconditions for strategies (Figure 6), which follow usual Hoare Logic calculi [16] except for the one dedicated to rules, viz. $wp(\rho[\boldsymbol{c}],\ Q)$. This latter corresponds essentially to an "if-then" structure in imperative programs. Put it simply, it checks three properties that are required for the application of a rule to be correct. Up until now, *App* depended on G. We want the procedure to work with whichever graph it is given and thus we modify *App* to be dependent only on the rules and strategies. First, *App* is a function which applies to a rule $\rho[\boldsymbol{c}]$ and returns a formula of $\mathcal{L}$ stating that there exists a match from the left-hand side of $\rho[\boldsymbol{c}]$ to a potential graph. If the formula $App(\rho[\boldsymbol{c}])$ is satisfied, the rule can be performed. Second, whenever the formula $App(\rho[\boldsymbol{c}]) \Rightarrow wp(\alpha_{\rho[\boldsymbol{c}]}, Q)$ is valid, then if there exists a match, the conditions, viz. $wp(\alpha_{\rho[\boldsymbol{c}]}, Q)$, which ensure the postcondition to be satisfied, are satisfied too. This corresponds to the usual weakest-precondition in Hoare Logic.

There is one additional issue which deserves to be handled carefully. Actually, one same rule can be fired several times during the execution of a program. It is thus mandatory to keep track of where each occurence of the rule is applied. To be more precise, *App* introduces a condition that uses the names of the nodes in the left-hand side of the rule. As these names uniquely define a node, if the same rule was to be used again, if the same name were reused, one would have to be applied at the exact same nodes. This is solved by renaming the individuals (i.e., nodes) each time the rule is fired. This is done through the function *tag*. That is why $wp(\rho[\boldsymbol{c}], Q) = App(tag(\rho[\boldsymbol{c}])) \Rightarrow wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Q)$.

Finally, as is usual in Hoare logic calculi [16], the closure of a strategy, s^*, needs the definition of an invariant, inv_s, and the introduction of verification conditions, $vc(s^*, Q)$, shown in Figure 7. Basically, the idea is that a closure is considered as a subprogram whose correctness is proven on the side. The

verification condition checks that the specification of this subprogram whose pre- and postcondition are the invariant.

From the discussion above, we come to a new requirement about the logic $\mathcal{L}$, regarding the use of substitutions within weakest preconditions.

Requirement 4 *$\mathcal{L}$ must be closed under substitutions.*

If this last requirement is not satisfied, the computation of weakest preconditions will lead to formulas not expressible in $\mathcal{L}$. Thus the verification of the correctness of specifications would need new proof procedures different from those of $\mathcal{L}$.

In addition, $App(\rho[\boldsymbol{c}])$ must be definable in $\mathcal{L}$. Obviously, this depends mainly on the rules one wants to use. It is thus possible, for a given problem, to use one logic that may not be powerful enough for other problems. Nonetheless, one of the requirements this entails on $\mathcal{L}$ is that it must allow some kind of existential quantification so that the graph can be traversed to look for a match. Obviously, the $\exists$-quantifier of first-order logic is a prime candidate but some other mechanisms like individual assertions $a : C$ in Description Logics[3] or the @ operator of hybrid logic[2] can be used.

Requirement 5 *$\mathcal{L}$ must be able to express $App(\rho[\boldsymbol{c}])$ for all rules $\rho[\boldsymbol{c}]$ of the graph rewrite system under study.*

Theorem 1 (Soundness). *Let $\mathcal{L}$ be a logic satisfying requirements 1 to 5. Let $SP = (Pre, Post, (\mathcal{R}, \mathcal{S}))$ be a specification. If $(Pre \Rightarrow wp(\mathcal{S}, Post)) \wedge vc(\mathcal{S}, Post)$ is valid in $\mathcal{L}$, then for all graphs G, G' such that $G \Rightarrow_{\mathcal{S}} G'$, $G \models Pre$ implies $G' \models Post$.*

The proof of this theorem is quite straightforward. One just has to check for every atomic strategy s that if $Pre \Rightarrow wp(s, Post)$ and $G \models Pre$ then $G' \models Post$. We give the proof for the rule application which is the most complex.

Proof. Assume $\mathcal{S} = \rho[\boldsymbol{c}]$ where $\rho[\boldsymbol{c}]$ is a rule of $\mathcal{R}$. Let us assume $Pre \Rightarrow wp(\rho[\boldsymbol{c}], Post)$ is valid. Because

$$wp(\rho[\boldsymbol{c}], Post) = App(tag(\rho[\boldsymbol{c}])) \Rightarrow wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Post)$$

also $(Pre \wedge App(tag(\rho[\boldsymbol{c}]))) \Rightarrow wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Post)$ is valid. Let G be a graph. If $G \models App(\rho[\boldsymbol{c}])$, there is a match h. Let G' be such that $G \Rightarrow_{\rho[\boldsymbol{c}],h} G'$. By definition of the substitutions, $G \Rightarrow_{\rho[\boldsymbol{c}],h} G'$ and $G \models wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Post)$ implies $G' \models Post$. On the other hand, if $G \not\models App(\rho[\boldsymbol{c}])$, there does not exist any G' such that $G \Rightarrow_{\rho[\boldsymbol{c}]} G'$ and thus the program fails. Thus $G \models Pre$ implies that $G' \models Post$.

After performing the calculus, one gets a formula $vc(\mathcal{S}, Post) \wedge (Pre \Rightarrow wp(\mathcal{S}, Post))$. Obviously, in order to be able to decide whether or not a program is correct, one has to prove that the obtained formula is valid. Hence the following requirement.

Requirement 6 *The validity problem for $\mathcal{L}$ is decidable.*

Nevertheless, this last requirement could be optional if one wants to use interactive proof procedures.

5 Instances of the Example

Hereafter, we illustrate the general logical framework proposed in the previous section through the Hospital example by providing logics which fulfill the six proposed requirements. First, let us observe that all of the invariants that we defined can be expressed in first-order logic (Formulae on the right).

Property 1:
$MS = NU \oplus PH \quad \rightsquigarrow \forall x.\ MS(x) \Leftrightarrow (NU(x) \wedge \neg\ PH(x)) \vee (\neg NU(x) \wedge\ PH(x))$

Property 2:
$PA \cup MS \subseteq PE \quad \rightsquigarrow \forall x. PA(x) \vee \mathrm{MS}(x) \Rightarrow PE(x)$

Property 3:
$write\_access \subseteq read\_access \quad \rightsquigarrow \forall x, y. write\_access(x, y) \Rightarrow read\_access(x, y)$

Property 4:
$read\_access \circ is\_about \subseteq treats \quad \rightsquigarrow \forall x, y, z. read\_access(x, y) \wedge is\_about(y, z) \Rightarrow treats(x, z)$

Property 5:
$treats \subseteq MS \times PA \quad \rightsquigarrow \forall x, y. treats(x, y) \Rightarrow MS(x) \wedge PA(y)$

Property 6:
$PA \Rightarrow \exists^{=1}\ ref\_phys \quad \rightsquigarrow \forall x. PA(x) \Rightarrow (\exists y.\ ref\_phys(x, y) \wedge \forall z. ref\_phys(x, z) \Rightarrow z = y)$

First-order logic is not decidable though, and thus one may want to use a different logic in order to be able to decide the correctness of the considered properties. In the following, we use the 2-variable fragment of first-order logic with counting $(\mathcal{C}^2)$[14] and $\exists^*\forall^*$, the fragment of first-order logic whose formula in prenex form are of the form $\exists i_0, \ldots, i_k. \forall j_0, \ldots, j_l. A(i_0, \ldots, i_k, j_0, \ldots, j_l)$.

None of these three logics comes with a mechanism to create or remove elements. In order to circumvent this limitation, we add to the signature of the logic, that is to the set of node and edge labels, a unary predicate *Active*. Creating a new node becomes adding it to the *Active* nodes. This also requires to add that $\forall x, y. \neg Active(x) \Rightarrow (\bigwedge_{\psi \text{ an atomic unary predicate}} \neg\psi(x) \wedge \bigwedge_{r \text{ an atomic binary predicate}} \neg r(x, y) \wedge \neg r(y, x))$. I.e., non active nodes are not assumed to satisfy any property.

Let SPH be the specification $(Pre, Post, \mathcal{P})$ associated to the hospital example. Assume the strategy is $\mathcal{S} = New\_Ph[\text{NPH,NEONAT}]; Del\_Pa[\text{OPA}]$ while the considered rewrite system $\mathcal{R}$ is the one from Figure 4. This program $\mathcal{P}$ creates a new physician NPH and lets the patient OPA leave the hospital. Let inv denote the conjunction of the expected properties. Let the precondition Pre be $inv \wedge \exists x.(\text{NEONAT}(x) \wedge \text{DE}(x)) \wedge \exists x.(\text{OPA}(x) \wedge \text{PA}(x)) \wedge \forall x. \neg\text{NPH}(x)$. Let the postcondition $Post$ be $inv \wedge \exists x, y.(\text{NPH}(x)$

$\wedge \text{PH}(x) \wedge works\_in(x,y) \wedge \text{NEONAT}(y) \wedge DE(y))$. Proving the correctness of SPH amounts to proving that $Pre \Rightarrow wp(\mathcal{S}, Post)$ is valid. This is a formula in first-order logic. In the following two subsections, this specification is proven to be correct using two different decidable logics that are able to express part of Pre and $Post$.

5.1 Two-Variable Logic with Counting : $\mathcal{C}^2$

$\mathcal{C}^2$ is the two-variable fragment of first-order logic with counting. Its formulas are those of first-order logic than can be expressed with only two variables and using the counting quantifier constructor $\exists^{<n} x.P$ expressing that there are less than n values x that satisfy P. In our case, this constructor will mostly be used to express that there exist less than n different r-successors, *i.e.* nodes $m_0, m_1 \ldots$ such that $r(m, m_i)$ holds.

Definition 9. *Let $\mathcal{U}$ be a set of unary predicates, $u \in \mathcal{U}$, $\mathcal{B}$ be a set of binary predicates, $b \in \mathcal{B}$, n an integer. A formula ϕ of $\mathcal{C}^2$ is defined as:*

$$\begin{aligned}
\phi &:= \top \mid \phi \wedge \phi \mid \neg\phi \mid \exists^{<n} x.\phi_x \mid \exists^{<n} y.\phi_y \\
\phi_x &:= \phi \mid u(x) \mid b(x,x) \mid \phi_x \wedge \phi_x \mid \neg\phi_x \mid \exists^{<n} x.\phi_x \mid \exists^{<n} y.\phi_{x,y} \\
\phi_y &:= \phi \mid u(y) \mid b(y,y) \mid \phi_y \wedge \phi_y \mid \neg\phi_y \mid \exists^{<n} y.\phi_y \mid \exists^{<n} x.\phi_{x,y} \\
\phi_{x,y} &:= \phi_x \mid \phi_y \mid b(x,y) \mid b(y,x) \mid \phi_{x,y} \wedge \phi_{x,y} \mid \neg\phi_{x,y} \mid \exists^{<n} x.\phi_{x,y} \mid \exists^{<n} y.\phi_{x,y}
\end{aligned}$$

As usual, $\bot$ means $\neg\top$, $\phi \vee \psi$ means $\neg(\neg\phi \wedge \neg\psi)$, $\phi \Rightarrow \psi$ means $\neg\phi \vee \psi$, $\exists^{\geq n} v.\phi$ means $\neg\exists^{<n} v.\phi$, $\exists v.\phi$ means $\exists^{\geq 1} v.\phi$, $\forall v.\phi$ means $\neg\exists v.\neg\phi$.

Definition 10. *Let $\mathcal{G} = (N, E, \mathcal{C}, \mathcal{R}, \phi_N, \phi_E, s, t)$ be a graph. We define the valuation of formulae:*

$$\top^I = \textit{true}$$

$$(\phi \wedge \psi)^I = \phi^I \textit{ and } \psi^I$$

$$(\neg\phi)^I = \textit{not } \phi^I$$

$$(\exists^{<n} x.\phi_x)^I = \begin{cases} \textit{true} \quad \textit{if there does not exist } n \textit{ nodes } m_1, \ldots, m_n, \\ \qquad m_i \neq m_j \textit{ for } 0 < i < j \leq n \textit{ such that } m_i \models \phi_x \\ \textit{false} \quad \textit{otherwise} \end{cases}$$

$(\exists^{<n} y.\phi_y)^I$ is defined the same as $(\exists^{<n} x.\phi_x)^I$ but replacing x's with y's

Let us now focus on $m \models \phi_x$:

$$\begin{aligned}
m \models \phi &\quad \textit{iff } \phi^I \\
m \models u(x) &\quad \textit{iff } u \in \phi_N(m) \\
m \models b(x,x) &\quad \textit{iff there exists } e \in E. s(e) = m,\ t(e) = m \textit{ and } b = \phi_E(e) \\
m \models (\phi_x \wedge \psi_x) &\quad \textit{iff } m \models \phi_x \textit{ and } m \models \psi_x \\
m \models \neg\phi_x &\quad \textit{iff } m \not\models \phi_x \\
m \models \exists^{<n} x.\phi_x &\quad \textit{iff there does not exist } n \textit{ nodes } m'_1, \ldots, m'_n, \\
&\qquad\qquad m_i \neq m_j \textit{ for } 0 < i < j \leq n \textit{ such that } m'_i \models \phi_x \\
m \models \exists^{<n} y.\phi_{x,y} &\quad \textit{iff there does not exist } n \textit{ nodes } w_1, \ldots, w_n, \\
&\qquad\qquad w_i \neq w_j \textit{ for } 0 < i < j \leq n \textit{ such that } (m, w_i) \models \phi_{x,y}
\end{aligned}$$

$m \models \phi_y$ is defined the same way but swapping the x's and the y's.

Let us now focus on $(m, m') \models \phi_{x,y}$*:*

$(m, m') \models \phi_x$ *iff* $m \models \phi_x$

$(m, m') \models \phi_y$ *iff* $m' \models \phi_y$

$(m, m') \models b(x, y)$ *iff there exists* $e \in E.s(e) = m$, $t(e) = m'$ *and* $b = \phi_E(e)$

$(m, m') \models b(y, x)$ *iff there exists* $e \in E.s(e) = m'$, $t(e) = m$ *and* $b = \phi_E(e)$

$(m, m') \models (\phi_{x,y} \wedge \psi_{x,y})$ *iff* $(m, m') \models \phi_{x,y}$ *and* $(x, y) \models \psi_{x,y}$

$(m, m') \models \neg\phi_{x,y}$ *iff* $(m, m') \not\models \phi_{x,y}$

$(m, m') \models \exists^{<n} x.\phi_{x,y}$ *iff there does not exist* n *nodes* $m_1, \ldots, m_n$, $m_i \neq m_j$ *for all* $0 < i < j \leq n$ *such that* $(m_i, m') \models \phi_{x,y}$

$(m, m') \models \exists^{<n} y.\phi_{x,y}$ *iff there does not exist* n *nodes* $m'_1, \ldots, m'_n$, $m'_i \neq m'_j$ *for all* $0 < i < j \leq n$ *such that* $(m, m'_i) \models \phi_{x,y}$

Theorem 2 ([14]). *The validity problem of* $\mathcal{C}^2$ *is decidable.*

Let us now check the six requirements of the previous section. $\mathcal{C}^2$ contains unary predicates that are interpreted on nodes and binary predicates that are interpreted on edges. *Pre* and *Post* are interpreted on graphs.

Theorem 3. $\mathcal{C}^2$ *is closed under substitutions.*

The proof relies on the fact that first-order logic is closed under substitution. The proof provides a system of rewrite rules that removes substitutions. As it does not introduce new variables, it also works for $\mathcal{C}^2$. We give three example rules to understand better how does it work:

- $(\phi \wedge \psi)[\sigma] \rightsquigarrow \phi[\sigma] \wedge \psi[\sigma]$ as if $\phi \wedge \psi$ is satisfied after performing σ, so must be ϕ and ψ and the other way round.
- $r(x, y)[r := r + (i, j)] \rightsquigarrow r(x, y) \vee (i(x) \wedge j(y))$ as $r^{I'}$ is $r^I \cup (i^I, j^I)$.
- $r(x, y)[clone(i, i')] \rightsquigarrow r(x, y) \vee (i'(x) \wedge \exists x.(i(x) \wedge r(x, y))) \vee (i'(y) \wedge \exists y.(i(y) \wedge r(x, y))) \vee (i'(x) \wedge i'(y) \wedge \exists x.(i(x) \wedge r(x, x)))$.

Example 2. $\mathcal{C}^2$ can express all the predicates $App(\rho)$ for the rules of the considered example (see Figure 4):

- $App(N\_Ph(\text{PH}_1,\text{D}_1)) = \exists x.(\text{D}_1(x) \wedge \text{DE}(x)) \wedge \exists x.(\neg Active(x) \wedge \text{PH}_1(x))$
- $App(N\_Pa(\text{PA}_1,\text{PH}_1,\text{FO}_1,\text{X})) = \exists x, y.(\text{PH}_1(x) \wedge \text{PH}(x) \wedge works\_in(x, y)) \wedge \exists x.(\neg Active(x) \wedge \text{PA}_1(x)) \wedge \exists x.(\neg Active(x) \wedge \text{FO}_1(x))$
- $App(D\_Pa(\text{PA}_1)) = \exists x, y.(\text{PA}_1(x) \wedge \text{PA}(x) \wedge hospital\_in(x, y))$
- $App(D\_Ph(\text{PH}_1,\text{PH}_2)) = \exists x, y.(\text{PH}_1(x) \wedge \text{PH}(x) \wedge works\_in(x, y) \wedge \exists x.(\text{PH}_2(x) \wedge \text{PH}(x) \wedge works\_in(x, y)))$

One should also be interested in the ability of the logic to express the properties to be verified.

Example 3. $\mathcal{C}^2$ is not able to express Property 4: $read\_access \circ is\_about \subseteq treats$ as one would need to keep track of three variables at a time. On the other hand, Property 6: $\forall x.\text{PA}(x) \Rightarrow \exists^{=1} ref\_phys.\top$ is a formula of $\mathcal{C}^2$.

5.2 Exist-Forall-Prefix

The logic $\exists^*\forall^*$ is the fragment of first-order logic such that its prefix in prenex normal form is composed of a sequence of existential quantifiers and then a sequence of universal quantifiers.

Definition 11. *Let $\mathcal{U}$ be a set of unary predicates, $u \in \mathcal{U}$ and $\mathcal{B}$ a set of binary predicates, $b \in \mathcal{B}$. Let $x_1, \ldots, x_k, a_1, \ldots, a_l$ be variables and v, w denote two of them. A formula ϕ of $\exists^*\forall^*$ is defined as:*
$\phi := \exists x_0, \ldots, x_k, \forall a_0, \ldots, a_l.\psi(x_1, \ldots, x_k, a_1, \ldots, a_l)$
$\psi := \top \mid \psi \wedge \psi \mid \neg\phi \mid u(v) \mid b(v, w)$

As usual, $\bot$ means $\neg\top$, $\phi \vee \psi$ means $\neg(\neg\phi \wedge \neg\psi)$, $\phi \Rightarrow \psi$ means $\neg\phi \vee \psi$.

Definition 12. *Let $\mathcal{G} = (N, E, \mathcal{C}, \mathcal{R}, \phi_N, \phi_E, s, t)$ be a graph. We defined the valuation of formulae: $(\exists x_1, \ldots, x_k, \forall a_1, \ldots, a_l.\psi(x_0, \ldots, x_k, a_0, \ldots, a_l))^I = N$ iff there exist k nodes $(x_1, \ldots, x_k)$ such that for all choices of l nodes $(a_1, \ldots, a_l)$, $(x_1, \ldots, x_k, a_1, \ldots, a_l) \models \psi$.*
Let us define $(x_1, \ldots, x_k, a_1, \ldots, a_l) \models \psi$:
$(x_1, \ldots, a_l) \models \top$ *iff true*
$(x_1, \ldots, a_l) \models (\phi \wedge \psi)$ *iff* $(x_1, \ldots, a_l) \models \phi$ *and* $(x_1, \ldots, a_l) \models \psi$
$(x_1, \ldots, a_l) \models (\neg\phi)$ *iff* $(x_1, \ldots, a_l) \not\models \phi$
$(x_1, \ldots, a_l) \models u(v)$ *iff* $u \in \phi_N(v)$
$(x_1, \ldots, a_l) \models b(v, w)$ *iff there exists* $e \in E$. $s(e) = v$, $t(e) = w$ *and* $b = \phi_E(e)$

Theorem 4. *The validity problem of $\exists^*\forall^*$ is decidable.*

This is a well-known result ([8], chapter 6).

The six requirements of the previous section clearly hold for this logic. $\exists^*\forall^*$ contains unary predicate that are interpreted on nodes and binary predicates that are interpreted on edges.

Theorem 5. *$\exists^*\forall^*$ is closed under substitutions.*

The proof is exactly the same as the one for $\mathcal{C}^2$ and $\mathcal{FO}$. One needs to be careful though as additional quantifiers are introduced. One can see though that they are always of the form $\exists x.(i(x) \wedge c(x))$ or $\exists x.(i(x) \wedge r(x, y))$ that can be rewritten as $\forall x.(\neg i(x) \vee c(x))$ or $\forall x.(\neg i(x) \vee r(x, y))$. Thus one can consider that only universal quantifiers are introduced.

Example 4. $\exists^*\forall^*$ can express all the predicates $App(\rho)$ for the rules of the considered example (see Figure 4):

- $App(N\_Ph(\mathrm{PH}_1,\mathrm{D}_1)) = \exists x.(\mathrm{D}_1(x) \wedge \mathrm{DE}(x)) \wedge \exists x.(\neg Active(x) \wedge \mathrm{PH}_1(x))$
- $App(N\_Pa(\mathrm{PA}_1,\mathrm{PH}_1,\mathrm{FO}_1)) = \exists x, y.(\mathrm{PH}_1(x) \wedge \mathrm{PH}(x) \wedge works\_in(x, y)) \wedge \exists x.(\neg Active(x) \wedge \mathrm{PA}_1(x)) \wedge \exists x.(\neg Active(x) \wedge \mathrm{FO}_1(x))$
- $App(D\_Pa(\mathrm{PA}_1)) = \exists x, y.(\mathrm{PA}_1(x) \wedge \mathrm{PA}(x) \wedge hospital\_in(x, y))$
- $App(D\_Ph(\mathrm{PH}_1,\mathrm{PH}_2)) = \exists x, y, z.(\mathrm{PH}_1(x) \wedge \mathrm{PH}(x) \wedge works\_in(x, y) \wedge \mathrm{PH}_2(z) \wedge \mathrm{PH}(z) \wedge works\_in(z, y))$

It is worth noting that the definition of $App(\rho)$ introduces new existential quantifiers as it checks for the existence of a match. This could seem to lead to a problem as the formula no longer is in $\exists^*\forall^*$. Actually, as the existentially quantified variables do not depend on the previously defined universally quantified variables, it is possible to move them at the beginning thus yielding a formula in $\exists^*\forall^*$.

Once more one has to check whether all properties can be expressed in the chosen logic.

Example 5. $\exists^*\forall^*$ is not able to express Property 6:$PA\Rightarrow \exists^{=1}$ *ref_phys* as it needs an existential quantifier after the universal ones to express the existence of an edge labeled with *ref_phys*. On the other hand, Property 4:
$\forall x, y, z.read\_access(x, y) \wedge is\_about(y, z) \Rightarrow treats(x, z)$ is part of $\exists^*\forall^*$.

6 Conclusions

We considered the verification problem of model/graph transformations. We introduced a notion of specification consisting of pre- and postcondition which specify the correctness of the run of rewrite rules performed according to a given rewrite strategy.

Deciding the correctness of a given specification is not an easy and decidable task in general. We proposed some criteria which may be helpful to choose the most appropriate logics one can use to express proof obligations related to the correctness problem. We illustrated our proposal by considering a running example for which two decidable logics have been used to prove its correctness.

Even in the relatively simple considered example, none of the investigated logics is expressive enough to be able to deal with all the discussed properties. This is a deliberate choice. Our point is that one has to select for each problem one or several logics that are relevant and we proposed some criteria that help to select such logics.

References

1. S. Ahmetaj, D. Calvanese, M. Ortiz, and M. Simkus. Managing change in graph-structured data using description logics. In *Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence, July 27 -31, 2014, Québec City, Québec, Canada.*, pages 966–973, 2014.
2. C. Areces, P. Blackburn, and M. Marx. Hybrid logics: Characterization, interpolation and complexity. *J. Symb. Log.*, 66(3):977–1010, 2001.
3. F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. Patel-Schneider, editors. *The Description Logic Handbook: Theory, Implementation, and Applications.* Cambridge University Press, 2003.
4. P. Balbiani, R. Echahed, and A. Herzig. A dynamic logic for termgraph rewriting. In *Procs. of ICGT 2010*, pages 59–74, 2010.
5. L. Baresi and P. Spoletini. *Procs. of ICGT 2006*, chapter On the Use of Alloy to Analyze Graph Transformation Systems, pages 306–320. Springer, 2006.

6. J. H. Brenas, R. Echahed, and M. Strecker. On the closure of description logics under substitutions. In *Proceedings of the 29th International Workshop on Description Logics, Cape Town, South Africa, April 22-25, 2016.*, 2016.
7. J. H. Brenas, R. Echahed, and M. Strecker. Proving correctness of graph rewriting systems using c2pdl. lig-membres.imag.fr/echahed/progverifGRT.pdf, 2016.
8. E. Börger, E. Grädel, and Y. Gurevich. *The classical decision problem*. Springer, 2000.
9. A. Corradini, T. Heindel, F. Hermann, and B. König. Sesqui-pushout rewriting. In *Graph Transformations, ICGT 2006*, pages 30–45, 2006.
10. B. Courcelle. The monadic second-order logic of graphs. i. recognizable sets of finite graphs. *Inf. Comput.*, 85(1):12–75, 1990.
11. L. M. de Moura and N. Bjørner. Z3: an efficient SMT solver. In *Procs. of TACAS 2008*, pages 337–340, 2008.
12. R. Echahed. Inductively sequential term-graph rewrite systems. In *4th International Conference on Graph Transformations, ICGT*, volume 5214 of *Lecture Notes in Computer Science*, pages 84–98. Springer, 2008.
13. A. H. Ghamarian, M. de Mol, A. Rensink, E. Zambon, and M. Zimakova. Modelling and analysis using GROOVE. *STTT*, 14(1):15–40, 2012.
14. E. Grädel, M. Otto, and E. Rosen. Two-Variable Logic with Counting is Decidable. In *Proceedings of 12th IEEE Symposium on Logic in Computer Science LICS '97, Warschau*, 1997.
15. A. Habel and K. Pennemann. Correctness of high-level transformation systems relative to nested conditions. *Mathematical Structures in Computer Science*, 19(2):245–296, 2009.
16. C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, 1969.
17. S. Itzhaky, A. Banerjee, N. Immerman, A. Nanevski, and M. Sagiv. Effectively-propositional reasoning about reachability in linked data structures. In *Procs of CAV 2013*, pages 756–772, 2013.
18. D. Jackson. *Software Abstractions*. MIT Press, 2011.
19. K. R. M. Leino. Dafny: An automatic program verifier for functional correctness. In *Procs. of LPAR 2010*, pages 348–370. Springer, 2010.
20. R. Piskac, L. M. de Moura, and N. Bjørner. Deciding effectively propositional logic using DPLL and substitution sets. *J. Autom. Reasoning*, 44(4):401–424, 2010.
21. C. M. Poskitt and D. Plump. A hoare calculus for graph programs. In *Procs. of ICGT 2010*, pages 139–154, 2010.
22. C. M. Poskitt and D. Plump. Verifying monadic second-order properties of graph programs. In *Procs. of ICGT 2014*, pages 33–48, 2014.
23. J. C. Reynolds. An overview of separation logic. In *Verified Software: Theories, Tools, Experiments, First IFIP TC 2/WG 2.3 Conference, VSTTE 2005, Zurich, Switzerland, October 10-13, 2005, Revised Selected Papers and Discussions*, pages 460–469, 2005.
24. O. Semeráth, Á. Barta, Z. Szatmári, Á. Horváth, and D. Varró. Formal validation of domain-specific languages with derived features and well-formedness constraints. *International Journal on Software and Systems Modeling*, 07/2015 2015.
25. J. Tschannen, C. A. Furia, M. Nordio, and N. Polikarpova. *Procs. of TACAS 2015*, chapter AutoProof: Auto-Active Functional Verification of Object-Oriented Programs, pages 566–580. Springer, 2015.
26. D. Varró. Automated formal verification of visual modeling languages by model checking. *Software and System Modeling*, 3(2):85–113, 2004.

Appendix

6.1 Soundness

Theorem 1.
Let $\mathcal{L}$ be a logic satisfying requirements 1 to 5. Let $SP = (Pre, Post, (\mathcal{R}, \mathcal{S}))$ be a specification. If $Pre \Rightarrow wp(\mathcal{S}, Post)$ is valid in $\mathcal{L}$, then for all graphs G, G' such that $G \Rightarrow_{\mathcal{S}} G'$, $G \models Pre$ implies $G' \models Post$.

Proof. The proof of the soundness is done by induction on the structure of the strategy.

- Assume $\mathcal{S} = \epsilon$ then $wp(\mathcal{S}, Post) = Post$. Thus $(Pre \Rightarrow wp(\mathcal{S}, Post))$ is equivalent to $Pre \Rightarrow Post$. Hence, for any graph G, if $G \models Pre$ then $G \models Post$. As, G is the only G' such that $G \Rightarrow_{\mathcal{S}} G'$, $G \models Pre$ implies $G' \models Post$.
- Assume $\mathcal{S} = \rho[\boldsymbol{c}]$ where $\rho[\boldsymbol{c}]$ is a rule of $\mathcal{R}$. Let us assume $Pre \Rightarrow wp(\rho[\boldsymbol{c}], Post)$ is valid. As $wp(\rho[\boldsymbol{c}], Post) = App(tag(\rho[\boldsymbol{c}])) \Rightarrow wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Post)$, then $(Pre \wedge$
  $App(tag(\rho[\boldsymbol{c}]))) \Rightarrow wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Post)$ is valid. Let G be a graph. If $G \models App(\rho[\boldsymbol{c}])$, there is a match h. Let G' be such that $G \Rightarrow_{\rho[\boldsymbol{c}],h} G'$. By definition of the substitutions, $G \Rightarrow_{\rho[\boldsymbol{c}],h} G'$ and $G \models wp(tag(\alpha_{\rho[\boldsymbol{c}]}), Post)$ implies $G' \models Post$. On the other hand, if $G \not\models App(\rho[\boldsymbol{c}])$, there does not exist any G' such that $G \Rightarrow_{\rho[\boldsymbol{c}]} G'$ and thus the program fails. Thus $G \models Pre$ implies that $G' \models Post$.
- Assume $\mathcal{S} = s_0; s_1$ then $wp(s_0; s_1, Post) = wp(s_0, wp(s_1, Post))$. Then, if $Pre \Rightarrow$
  $wp(s_0; s_1, Post)$ is valid, so is $Pre \Rightarrow wp(s_0, wp(s_1, Post)$ then, for any G and G'' such that $G \Rightarrow_{s_0} G''$,
  $G \models Pre$ implies $G'' \models wp(s_1, Post)$ by induction. But, as $vc(s_1, Post)$ is valid and $wp(s_1, Post) \Rightarrow wp(s_1, Post)$, for any G' such that $G'' \Rightarrow_{s_1} G'$, $G' \models Post$.
- Assume $\mathcal{S} = s_0 \oplus s_1$ then $wp(s_0 \oplus s_1, Post) = wp(s_0, Post) \wedge wp(s_1, Post)$. Let G and G' be such that $G \Rightarrow_{s_0 \oplus s_1} G'$ and $Pre \Rightarrow wp(s_0 \oplus s_1, Post)$ be valid. Then, either $G \Rightarrow_{s_0} G'$ in which case, $Pre \Rightarrow wp(s_0, Post)$ being valid, $G \models Pre$ implies $G' \models Post$ by induction, or $G \Rightarrow_{s_1} G'$ in which case, $Pre \Rightarrow wp(s_1, Post) \wedge vc(s_1, Post)$ being valid, $G \models Pre$ implies $G' \models Post$.

6.2 $\mathcal{C}^2$

Theorem 3.
$\mathcal{C}^2$ is closed under substitutions.

Proof. Let c, c' be unary predicates, r be binary predicates, i, j be nominals, a be an attribute, Xbe an attribute value, ϕ, ψ be a formulae, σ an atomic action. We consider whether or not a formula is satisfiable at a node n,

- $(\exists x.\phi)[\sigma]) \rightsquigarrow \exists x.(\phi[\sigma])$ as the substitutions do not modify the existence or not of a node.

- $(\phi \wedge \psi)[\sigma] \rightsquigarrow \phi[\sigma] \wedge \psi[\sigma]$ as if $\phi \wedge \psi$ is satisfied after performing σ, so must be ϕ and ψ and the other way round.
- $(\neg\phi)[\sigma] \rightsquigarrow \neg(\phi[\sigma])$ as if ϕ is not satisfied after performing σ, it is not possible that ϕ be satisfied after performing σ.
- $\top[\sigma] \rightsquigarrow \top$ as no matter what action is performed, $\top$ is satisfied.
- $c'(x)[c := i] \rightsquigarrow c'(x)$ as the valuation of c' is left untouched.
- $c(x)[c := i] \rightsquigarrow i(x)$ as the $c^{I'}$ after performing $c := i$ is i^I.
- $c'(x)[c := c + i] \rightsquigarrow c'(x)$ as the valuation of c' is left untouched.
- $c(x)[c := c + i] \rightsquigarrow c(x) \vee i(x)$ as the $c^{I'}$ after performing $c := c + i$ is $c^I \cup i^I$.
- $c'(x)[c := c - i] \rightsquigarrow c'(x)$ as the valuation of c' is left untouched.
- $c(x)[c := c - i] \rightsquigarrow c(x) \wedge \neg i(x)$ as the $c^{I'}$ after performing $c := c - i$ is $c^I \backslash i^I$.
- $c(x)[r := r + (i, j)] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[r := r - (i, j)] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[new(i)] \rightsquigarrow c(x)$ for $c \neq \mathit{Active}$ as the valuation of c is left untouched.
- $\mathit{Active}(x)[new(i)] \rightsquigarrow \mathit{Active}(x) \vee i(x)$ as the valuation of Active becomes $c^{\mathcal{I}} \cup i^{\mathcal{I}}$.
- $c(x)[del(i)] \rightsquigarrow c(x) \wedge \neg i(x)$ as $c^{I'} = c^I \backslash i^I$.
- $c(x)[i \gg^{in} j] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[i \gg^{out} j)] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[clone(i, i')] \rightsquigarrow c(x) \vee (i'(x) \wedge \exists x.(i(x) \wedge c(x)))$ as all node that satisfied $c(x)$ before the action still do and the only new node is i' that satisfies c if and only if i does. Note that it also works for Active.
- $r(x, y)[c := i] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r(x, y)[c := c + i] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r(x, y)[c := c - i] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r'(x, y)[r := r + (i, j)] \rightsquigarrow r'(x, y)$ as the valuation of r' is left untouched.
- $r(x, y)[r := r + (i, j)] \rightsquigarrow r(x, y) \vee (i(x) \wedge j(y))$ as $r^{I'}$ is $r^I \cup (i^I, j^I)$.
- $r'(x, y)[r := r - (i, j)] \rightsquigarrow r'(x, y)$ as the valuation of r' is left untouched.
- $r(x, y)[r := r - (i, j)] \rightsquigarrow r(x, y) \wedge (\neg i(x) \vee \neg j(y))$ as $r^{I'}$ is $r^I \backslash (i^I, j^I)$.
- $r(x, y)[new(i)] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r(x, y)[del(i)] \rightsquigarrow r(x, y) \wedge \neg i(x) \wedge \neg i(y)$ as $r^{I'} = r^I \backslash \{(a, b) | a \in i^I \text{ or } b \in i^I\}$.
- $r(x, y)[i \gg^{in} j] \rightsquigarrow (r(x, y) \wedge \neg i(y)) \vee (r(x, i) \wedge j(y))$ as $r^{I'} = r^I \cup \{(a, j) | (a, i) \in r^I\} \backslash \{(a, i) \in r^I\}$.
- $r(x, y)[i \gg^{out} j] \rightsquigarrow (r(x, y) \wedge \neg i(x)) \vee (r(i, y) \wedge j(x))$ as $r^{I'} = r^I \cup \{(j, b) | (i, b) \in r^I\} \backslash \{(i, b) \in r^I\}$.
- $r(x, y)[clone(i, i')] \rightsquigarrow r(x, y) \vee (i'(y) \wedge \exists y.(i(y) \wedge r(x, y))) \vee (i'(x) \wedge \exists x.(i(x) \wedge r(x, y))) \vee (i'(x) \wedge i'(y) \wedge \exists x.(i(x) \wedge r(x, x)))$.

These conditions are enough to be able to express the existence of the matches. Nonetheless, $\mathcal{C}^2$ is limited to two variables and one may have to deal with more nodes than that in rules. In order to tackle this problem, it has been decided to rename rules using special unary concepts o_i. These concepts are such that it is possible to uniquely identify elements inside the application of a rule so the condition that $\exists^{=1} x.o_i(x)$ is added for each o_i that is used this way. One could see that this condition states that the nodes where the actions will be performed are, so to speak, pre-selected that is the original model already contains

nodes labeled with these concepts. This may seem wrong as one wants to prove that the post-condition will stand no matter where the match is found. The calculus actually solves the problem as it requires that the weakest precondition be valid. As these new concepts never occur outside of the scope of the match, given two graphs that differ only on which nodes satisfy these concepts, that is two graphs such that the nodes where the match are found are different, one can prove that the post-condition will stand.

As said previously, $\mathcal{C}^2$ is not able to keep track of all variables so one needs to use concepts to keep track of the modified nodes. The actual concepts used are those obtained from *tag*. The expressions of *App* become:

- $App(N\_Ph(\text{PH}_1,\text{D}_1)) = \exists x.(\text{D}_1(x) \wedge \text{DE}(x) \wedge i(x)) \wedge \exists x.(\neg Active(x) \wedge \text{PH}_1(x) \wedge j(x))$
- $App(N\_Pa(\text{PA}_1,\text{PH}_1,\text{FO}_1)) = \exists x,y.(\text{PH}_1(x) \wedge \text{PH}(x) \wedge i(x) \wedge works\_in(x,y) \wedge j(y)) \wedge \exists x.(\neg Active(x) \wedge \text{PA}_1(x) \wedge k(x)) \wedge \exists x.(\neg Active(x) \wedge \text{FO}_1(x) \wedge l(x))$
- $App(D\_Pa(\text{PA}_1)) = \exists x,y.(\text{PA}_1(x) \wedge \text{PA}(x) \wedge i(x) \wedge hospital\_in(x,y) \wedge j(y))$
- $App(D\_Ph(\text{PH}_1,\text{PH}_2)) = \exists x,y.(\text{PH}_1(x) \wedge \text{PH}(x) \wedge i(x) \wedge works\_in(x,y) \wedge j(y) \wedge \exists x.(\text{PH}_2(x) \wedge \text{PH}(x) \wedge k(x) \wedge works\_in(x,y)))$

Back to the problem The specification considered henceforth is $SP_2 = (Pre_2, Post_2, \mathcal{S})$. Pre_2 is obtained from Pre (resp. $Post_2$ from $Post$) by replacing inv with $inv_2 = \forall x.(\ MS(x) \Leftrightarrow ((NU(x) \wedge \neg\ PH(x)) \vee (\neg NU(x) \wedge\ PH(x)))) \wedge \forall x.(PA \vee\ MS(x) \Rightarrow PE(x)) \wedge \forall x,y.(write\_access(x,y) \Rightarrow read\_access(x,y)) \wedge \forall x,y.(treats(x,y) \Rightarrow MS(x) \wedge\ PA(y)) \wedge \forall x.(\text{PA}(x) \Rightarrow \exists^{=1} ref\_phys.\top)$. Additionally, both Pre_2 and $Post_2$ must contain the condition on the uniqueness of the matched nodes. As two rules are applied and each uses two elements i and j, $\exists^{=1}x.i_0(x) \wedge \exists^{=1}x.j_0(x) \wedge \exists^{=1}x.i_1(x) \wedge \exists^{=1}x.j_1(x)$ is added to both Pre and $Post$ to mark the elements that are used.

One now has to compute $Pre_2 \Rightarrow wp(\mathcal{S}, Post_2)$ and prove its validity. In order to make things a little clearer, Pre_2 and $Post_2$ will be decomposed in smaller parts. Let P_i be the formula used to represent Property i. Let's prove that $Pre_2 \Rightarrow wp(\mathcal{S}, P_i)$.

Let us start with $P_1 = \forall x.(\ MS(x) \Leftrightarrow ((NU(x) \wedge \neg\ PH(x)) \vee (\neg NU(x) \wedge PH(x))))$. From the definition of weakest preconditions, $wp(\mathcal{S}, P_1) = wp(New\_Ph[\text{NPH,NEONAT}], wp(Del\_Pa[\text{OPA}], P_1))$. i_0 and j_0 are now used to compute $wp(Del\_Pa[\text{OPA}], P_1)$. Then $wp(Del\_Pa[\text{OPA}], P_1) = App(tag(Del\_Pa[\text{OPA}])) \Rightarrow Post_2[hospital\_in := hospital\_in - (i_0, j_0)]$ where $App(tag(Del\_Pa[\text{OPA}])) = \exists x,y.(\text{OPA}(x) \wedge \text{PA}(x) \wedge i_0(x) \wedge hospital\_in(x,y) \wedge j_0(y))$ and $P_1[hospital\_in := hospital\_in - (i_0, j_0)] = P_1$ as $hospital\_in$ does not occur in P_1. Instead of proving, $Pre_2 \Rightarrow wp(New\_Ph[\text{NPH,NEONAT}], App(tag(Del\_Pa[\text{OPA}])) \Rightarrow P_1)$, one can instead focus on $Pre_2 \Rightarrow wp(New\_Ph[\text{NPH,NEONAT}], P_1)$ which is stronger. Let us now compute $wp(New\_Ph[\text{NPH,NEONAT}], P_1)$. By definition, and using i_1 and j_1, $wp(N\_Ph(\text{NPH,NEONAT}), P_1) = App(tag(New\_Ph[\text{NPH,NEONAT}])) \Rightarrow P_1[\alpha_{New\_Ph[\text{NPH,NEONAT}]}])$. Let us compute $P_1[\alpha_{New\_Ph[\text{NPH,NEONAT}]}]$. As MS and PH are the only two concepts occurring in P_1 that are modified, $P_1[\alpha_{New\_Ph[\text{NPH,NEONAT}]}] =$

$\forall x.(\ (MS(x) \vee j_1(x)) \Leftrightarrow ((NU(x) \wedge \neg(PH(x)) \vee j_1(x)) \vee (\neg NU(x) \wedge (\ PH(x) \vee j_1(x))))$. As $App(tag(New\_Ph[\text{NPH,NEONAT}])) = \exists x.(\text{D}_1(x) \wedge \text{DE}(x) \wedge i_1(x)) \wedge \exists x.(\neg Active(x) \wedge \text{PH}_1(x) \wedge j_1(x))$, $Pre_2 \wedge App(tag(New\_Ph[\text{NPH,NEONAT}])) \Rightarrow Pre_2 \wedge \exists x.(\neg Active(x) \wedge \text{PH}_1(x) \wedge j_1(x))$. From that, one can prove that $P_1 \wedge \exists^{=1} x.j_1(x) \wedge \forall x.\neg(Active(x) \Rightarrow \neg\text{NU}(x)) \wedge \exists x.(\neg Active(x) \wedge \text{PH}_1(x) \wedge j_1(x)) \Rightarrow P_1 \wedge \exists^{=1} x.(j_1(x) \wedge \neg\text{NU}(x))$. Then, it is easy to see that $P_1 \wedge \exists^{=1} x.(j_1(x) \wedge \neg\text{NU}(x)) \Rightarrow \forall x.(\ (MS(x) \vee j_1(x)) \Leftrightarrow ((NU(x) \wedge \neg(PH(x)) \vee j_1(x)) \vee (\neg NU(x) \wedge (\ PH(x) \vee j_1(x))))$. Thus $Pre_2 \Rightarrow wp(\mathcal{S}, P_1)$.

The same can be done with the other P_i.

6.3 $\exists^*\forall^*$

Theorem 5.
$\exists^*\forall^*$ is closed under substitutions.

Proof. Let c, c' be unary predicates, r be binary predicates, i, j be nominals, a be an attribute, Xbe an attribute value, ϕ, ψ be a formulae, σ an atomic action. We consider whether or not a formula is satisfiable at a node n,

- $(\exists x.\phi)[\sigma]) \rightsquigarrow \exists x.(\phi[\sigma])$ as the substitutions do not modify the existence or not of a node.
- $(\phi \wedge \psi)[\sigma] \rightsquigarrow \phi[\sigma] \wedge \psi[\sigma]$ as if $\phi \wedge \psi$ is satisfied after performing σ, so must be ϕ and ψ and the other way round.
- $(\neg\phi)[\sigma] \rightsquigarrow \neg(\phi[\sigma])$ as if ϕ is not satisfied after performing σ, it is not possible that ϕ be satisfied after performing σ.
- $\top[\sigma] \rightsquigarrow \top$ as no matter what action is performed, $\top$ is satisfied.
- $c'(x)[c := i] \rightsquigarrow c'(x)$ as the valuation of c' is left untouched.
- $c(x)[c := i] \rightsquigarrow i(x)$ as the $c^{I'}$ after performing $c := c + i$ is i^I.
- $c'(x)[c := c + i] \rightsquigarrow c'(x)$ as the valuation of c' is left untouched.
- $c(x)[c := c + i] \rightsquigarrow c(x) \vee i(x)$ as the $c^{I'}$ after performing $c := c + i$ is $c^I \cup i^I$.
- $c'(x)[c := c - i] \rightsquigarrow c'(x)$ as the valuation of c' is left untouched.
- $c(x)[c := c - i] \rightsquigarrow c(x) \wedge \neg i(x)$ as the $c^{I'}$ after performing $c := c - i$ is $c^I \backslash i^I$.
- $c(x)[r := r + (i, j)] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[r := r - (i, j)] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[new(i)] \rightsquigarrow c(x)$ for $c \neq Active$ as the valuation of c is left untouched.
- $Active(x)[new(i)] \rightsquigarrow Active(x) \vee i(x)$ as the valuation of $Active$ becomes $c^{\mathcal{I}} \cup i^{\mathcal{I}}$.
- $c(x)[del(i)] \rightsquigarrow c(x) \wedge \neg i(x)$ as $c^{I'} = c^I \backslash i^I$.
- $c(x)[i \gg^{in} j] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $c(x)[i \gg^{out} j)] \rightsquigarrow c(x)$ as the valuation of c is left untouched.
- $r(x, y)[c := i] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r(x, y)[c := c + i] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r(x, y)[c := c - i] \rightsquigarrow r(x, y)$ as the valuation of r is left untouched.
- $r'(x, y)[r := r + (i, j)] \rightsquigarrow r'(x, y)$ as the valuation of r' is left untouched.
- $r(x, y)[r := r + (i, j)] \rightsquigarrow r(x, y) \vee (i(x) \wedge j(y))$ as $r^{I'}$ is $r^I \cup (i^I, j^I)$.
- $r'(x, y)[r := r - (i, j)] \rightsquigarrow r'(x, y)$ as the valuation of r' is left untouched.

- $r(x,y)[r := r-(i,j)] \rightsquigarrow r(x,y) \wedge (\neg i(x) \vee \neg j(y))$ as $r^{I'}$ is $r^I \backslash (i^I, j^I)$.
- $r(x,y)[new(i)] \rightsquigarrow r(x,y)$ as the valuation of r is left untouched.
- $r(x,y)[del(i)] \rightsquigarrow r(x,y) \wedge \neg i(x) \wedge \neg i(y)$ as $r^{I'} = r^I \backslash \{(a,b) | a \in i^I \text{ or } b \in i^I\}$.
- $r(x,y)[i \gg^{in} j] \rightsquigarrow (r(x,y) \wedge \neg i(y)) \vee (r(x,i) \wedge j(y))$ as $r^{I'} = r^I \cup \{(a,j) | (a,i) \in r^I\} \backslash \{(a,i) \in r^I\}$.
- $r(x,y)[i \gg^{out} j)] \rightsquigarrow (r(x,y) \wedge \neg i(x)) \vee (r(i,y) \wedge j(x))$ as $r^{I'} = r^I \cup \{(j,b) | (i,b) \in r^I\} \backslash \{(i,b) \in r^I\}$.

It is worth noting that the actions $i \gg^{in} j$ and $i \gg^{out} j$ require nominals to be both atomic unary predicates and constants. One thus has to, each time a new nominal o is introduced, add to the precondition that $\exists^{=1} x.o(x)$ and $o(o)$.

Back to the problem Thus the specification considered henceforth is $SP_{\exists\forall} = (Pre_{\exists\forall}, Post_{\exists\forall}, \mathcal{S})$ where $Pre_{\exists\forall}$ is obtained from Pre (resp. $Post_{\exists\forall}$ from $Post$) by replacing inv with $inv_{\exists\forall} = \forall x.(\ MS(x) \Leftrightarrow ((NU(x) \wedge \neg\ PH(x)) \vee (\neg NU(x) \wedge PH(x)))) \wedge \forall x.(PA(x) \Rightarrow PE(x)) \wedge \forall x.(MS(x) \Rightarrow PE(x)) \wedge \forall x, y.(write\_\ access(x,y) \Rightarrow read\_\ access(x,y)) \wedge$
$\forall x, y.(treats(x,y) \Rightarrow MS(x) \wedge\ PA(y)) \wedge \forall x, y, z.(read\_\ access(x,y) \wedge$
$is\_\ about(y,z) \Rightarrow treats(x,z))$.

As the substitutions do not concern either PA, *ref_ phys*, *read_ access*, *is_ about* or *treats*, $Pre_{\exists\forall} \Rightarrow wp(\mathcal{S}, Post_{\exists\forall})$ only differs from $Pre_2 \Rightarrow wp(\mathcal{S}, Post_2)$ in the parts of the formulae that are expressible only in one of the two logics.