On Counterpart Semantics for a Predicate Modal μ-Calculus*

Fabio Gadducci[1], Alberto Lluch Lafuente[2], and Andrea Vandin[2]

[1] Department of Computer Science, University of Pisa, Italy
[2] IMT Institute for Advanced Studies Lucca, Italy

1 Introduction

Visual specification formalisms should rely on the existence of suitable languages for expressing properties, as well as on the availability of tools for their verification. As far as graph transformation systems are concerned, after the pioneering work of Courcelle [3], various variants of graph logics have been proposed. In particular, the need to reason about the possible the evolution of the topology of a graph lead to the idea of combining temporal and graph logics. The first approaches consisted on propositional temporal logics whose state observations were limited to pure graph formulae. The impossibility to interleave the graphical and temporal dimensions was thus forbidding the reasoning about the evolution of individual components within a graph. To overcome this limitation predicate temporal logics were proposed, where graph connectives such as quantifiers over nodes or edges are allowed to be interleaved with temporal connectives. This requires to consider semantical models that allow for keeping track of the identity of components, an issue known as the *trans-world indentity* problem (see [7] as well as [2] for a survey of the related philosophical issues). The most widely adopted solution follows the so-called "Kripke semantics" approach: roughly, a set of universal items is chosen, and its elements are used to form each state. However, Kripke-like solutions do not fit too well with the possibility of merging components or re-using component names, and in most cases it results in a limited and often less intuitive logic semantics. To overcome such drawbacks we investigate the use of "Lewis counterpart theory" for defining the semantics of temporal graph logics. Roughly, the main idea is to exploit *counterpart relations* and *formulas-in-context*. Counterpart relations are (partial) functions among states, explicitly relating components of different states and thus denoting the removal, addition, renaming and merging of components. Formulas-in-context are formulas decorated with information regarding the variables that are being used to keep track of the evolution of individual components. Such information is exploited in the semantics of temporal modalities to discard irrelevant states. As a result, the semantics of these logics become more natural and intuitive, in particular when fixpoint operators are considered.

* Supported by the MIUR Project `SisteR`.

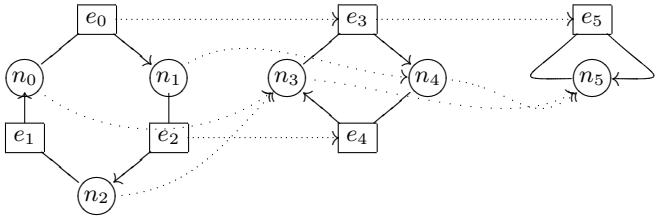

Fig. 1. A counterpart model with three worlds $\{w_0, w_1, w_2\}$

2 Counterpart Semantics for a Quantified μ-Calculus

We are developing a novel counterpart-like semantics for a quantified μ-calculus. The main motivation arised due to the difficulties encontered in previous works [1, 5], proposing the combination of temporal logics based on modal μ-calculus with monadic second-order logics for graphs. The starting point for our alternative proposal was the survey on quantified modal logic proposed by Belardinelli [2], further instantiated to graph transformations in the master's thesis of the third author [10] and currently being extended to deal with fix-point operators [6].

We represent systems with *counterpart models* roughly based on [7], where states are algebras and the evolution relation is given by a family of partial homomorphisms. Such models are very flexible and can be instantiated to well-known models such as graph transition systems. Fig. 1, for instance, represents a model with three states, each one of them being a graph (formally expressed with an algebra) where circles, boxes, lines and arrows respectively denote nodes, edges, edge source and edge target. Dotted lines denote the evolution of individual components from world to world.

Our logic basically follows the (monadic) second-order μ-calculus proposed in [1]. The main ingredients are first and second-order quantifiers, used to range over elements of the algebra (nodes and items for the graph case); a membership predicate used to require one element to belong to a set (which can be used to express equality); a next-time modal operator $\Diamond$ to express the existence of a world reachable in one step; and a fixpoint operator to express recursive properties. In addition, we have the ordinary boolean connectives.

As an example we use some liveness properties, starting with a propositional variant. The property expresses the fact that at some reachable state there will be a component (edge) x pointing to itself (edge e_5 ensures this in the example of Fig. 1). Technically, the property is described with the formula $\mu Z.[\exists x.s(x) = t(x) \vee \Diamond Z]$ where the key point is that the fixpoint and modal operators (ν and $\Diamond$) are combined in the well-known pattern of eventuality of an event p: $\mu Z.[p \vee \Diamond Z]$. Such event is the existence of a self-pointing component x, expressed with the *variable-closed* formula $\exists x.s(x) = t(x)$, where s and x denote the source and target of an edge. Clearly, both the above formulas hold in all the states of the simple example of Fig. 1 but do they hold if we consider variants where we talk about *all* the components?

The above examples do suggest that the definition of the semantics must take into account the merging of elements as well as the removal of elements being quantified. However, the situation is even more interesting when we consider the semantics of open formulas. For instance, consider the subformula $s(x) = t(x) \vee \Diamond Z$ of the above property: once the value of x is chosen in the current state, how is such value passed to the states denoted by the fixpoint variable Z?

We handle this situation by interpreting open formulas over sets of pairs (w, σ), for w a state and σ an assignment over w (that is, a substitution associating formula variables to components of the state w). The idea is to associate worlds and sets of assignments to open formulas, instead of just worlds: it allows for a straightforward interpretation of fix-points and for their smooth integration with the evaluation of quantifiers, at the same time properly extending the standard intepretation for closed formulas.

Another key point in our approach is in our interpretation of the temporal modality, which discards those worlds that are actually reachable but are not in counterpart relation with respect to the current context, i.e. when any quantified element is not preserved by the partial homomorphims between worlds. This is eased by the aforementioned notion of formulas-in-context. The rationale behind this is to ensure that the logic is normal (i.e. it satisfies the K-scheme of modal logics) and meaningful (see [2] for the philosophical stance supporting it).

As a consequence, our counterpart model faithfully represents the presence of cyclic behaviours, avoiding the limitations of existing approaches, and dispensing also from the reformulation of the transition relation. The resulting semantics is a streamlined and intuitively appealing one, yet it is general enough to cover most of the alternatives we are aware of.[3]

3 Conclusion and Future Works

We foresee a few obvious directions for further research. As a start, we would like to investigate if the correspondence results between quantified μ-calculi and Petri nets logics proposed in [1] could be lifted to our framework, and its richer family of counterpart relations. We would also like to better understand the relationship with spatial logics, along the lines of [5], possibly adopting a family of labelled counterpart relations, and the richer modal operators $\Diamond_{\langle p,Y \rangle}$, basically stating that the transition between worlds is caused by a specific rule, that may create a chosen set Y of new elements. Another interesting point is in understanding the tradeoff between expressivity and complexity regarding the choice of information being discarded in the semantics of the modal operator. We ignore those reachable worlds that are not in counterpart relation with respect to the current assignment, while other choices are possible like accepting the worlds, but making assignments undefined when the assigned element is deleted [4] or not discarding anything [1].

[3] For an overview of the existing literature (such as e.g. [1, 5, 9, 11]) and comparison with our work we refer the interested reader to [6].

Also the development of adequate proof systems should be pursued. Indeed, this is one the reasons for giving meaning to formulas-in-context, instead of just to naked formulas. So, a formula has associated a set of variables, its "context". Intuitively, the context of a formula contains at least the free variables of the formula, and does not contain the bounded variables of the formula. The use of formulas-in-context guarantees the so-called K-scheme, stating that $\Box(\psi_1 \to \psi_2)[\Gamma;\Delta]$ implies $\Box(\psi_1) \to \Box(\psi_2)[\Gamma;\Delta]$. The use of contexts is pivotal here, since otherwise the axiom might not always be satisfied. Instead, its validity tells us that the resulting logic is normal, which is a property of all classical modal logics [8], and a preliminar step in establishing any proof system.

References

1. Baldan, P., Corradini, A., König, B., Lluch Lafuente, A.: A temporal graph logic for verification of graph transformation systems. In: Fiadeiro, J.L., Schobbens, P.Y. (eds.) 18th International Workshop on Recent Trends in Algebraic Development Techniques (WADT'06). LNCS, vol. 4409, pp. 1–20. Springer (2007)
2. Belardinelli, F.: Quantified Modal Logic and the Ontology of Physical Objects. Ph.D. thesis, Scuola Normale Superiore of Pisa (2006)
3. Courcelle, B.: The expression of graph properties and graph transformations in monadic second-order logic. In: Rozenberg, G. (ed.) Handbook of Graph Grammars and Computing by Graph Transformation, pp. 313–400. World Scientific (1997)
4. Distefano, D., Rensink, A., Katoen, J.P.: Model checking birth and death. In: Baeza-Yates, R.A., Montanari, U., Santoro, N. (eds.) 2nd IFIP International Conference on Theoretical Computer Science (TCS'02). IFIP Conference Proceedings, vol. 223, pp. 435–447. Kluwer (2002)
5. Gadducci, F., Lluch Lafuente, A.: Graphical encoding of a spatial logic for the π-calculus. In: Mossakowski, T., Montanari, U., Haveraaen, M. (eds.) 2nd International Conference on Algebra and Coalgebra in Computer Science (CALCO'07). LNCS, vol. 4624, pp. 209–225. Springer (2007)
6. Gadducci, F., Lluch Lafuente, A., Vandin, A.: Counterpart semantics for a second-order μ-calculus. In: Ehrig, H., Rensink, A., Rozenberg, G., Schürr, A. (eds.) Proceedings of the 5th International Conference on Graph Transformation (ICGT'10). LNCS, Springer (to appear)
7. Hazen, A.: Counterpart-theoretic semantics for modal logic. The Journal of Philosophy 76(6), 319–338 (2004)
8. Huth, M., Ryan, M.: Logic in Computer Science: Modelling and Reasoning about Systems (Second Edition). Cambridge University Press (2004)
9. Rensink, A.: Model checking quantified computation tree logic. In: Baier, C., Hermanns, H. (eds.) 17th International Conference on Concurrency Theory (CONCUR'06). LNCS, vol. 4137, pp. 110–125. Springer (2006)
10. Vandin, A.: Algebraic models for a second-order modal logic. Master's thesis, University of Pisa (2009), http://www.di.unipi.it/∼vandin/thesis.pdf
11. Yahav, E., Reps, T.W., Sagiv, S., Wilhelm, R.: Verifying temporal heap properties specified via evolution logic. Logic Journal of the IGPL 14(5), 755–783 (2006)