Information and Computation 239 (2014) 303–339

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

# Refinement modal logic

Laura Bozzelli [a], Hans van Ditmarsch [b,*], Tim French [c], James Hales [c], Sophie Pinchinat [d]

[a] *Informática, Universidad Politécnica de Madrid, Spain*
[b] *LORIA, CNRS — Université de Lorraine, France*
[c] *Computer Science and Software Engineering, University of Western Australia, Australia*
[d] *IRISA, University of Rennes, France*

ARTICLE INFO

*Article history:*
Received 16 February 2012
Received in revised form 27 May 2014
Available online 1 August 2014

ABSTRACT

In this paper we present *refinement modal logic*. A refinement is like a bisimulation, except that from the three relational requirements only 'atoms' and 'back' need to be satisfied. Our logic contains a new operator ∀ in addition to the standard box modalities for each agent. The operator ∀ acts as a quantifier over the set of all refinements of a given model. As a variation on a bisimulation quantifier, this refinement operator or *refinement quantifier* ∀ can be seen as quantifying over a variable not occurring in the formula bound by it. The logic combines the simplicity of multi-agent modal logic with some powers of monadic second-order quantification. We present a sound and complete axiomatization of multi-agent refinement modal logic. We also present an extension of the logic to the modal $\mu$-calculus, and an axiomatization for the single-agent version of this logic. Examples and applications are also discussed: to software verification and design (the set of agents can also be seen as a set of actions), and to dynamic epistemic logic. We further give detailed results on the complexity of satisfiability, and on succinctness.



## 1. Introduction

Modal logic is frequently used for modelling knowledge in multi-agent systems. The semantics of modal logic uses the notion of "possible worlds", between which an agent is unable to distinguish. In dynamic systems agents acquire new knowledge (say by an announcement, or the execution of some action) that allows agents to distinguish between worlds that they previously could not separate. From the agent's point of view, what were "possible worlds" become inconceivable. Thus, a future informative event may be modelled by a reduction in the agent's accessibility relation. In [55] the *future event logic* is introduced. It augments the multi-agent logic of knowledge with an operation $\forall\varphi$ that stands for "$\varphi$ holds after all informative events" — the diamond version $\exists\varphi$ stands for "there is an informative event after which $\varphi$." The proposal was a generalization of a so-called arbitrary public announcement logic with an operator for "$\varphi$ holds after all announcements" [8]. The semantics of informative events encompasses action model execution à la Baltag et al. [9]: on finite models, it can be easily shown that a model resulting from action model execution is a refinement of the initial model, and for a given refinement of a model we can construct an action model such that the result of its execution is bisimilar to that refinement.

* Corresponding author.
*E-mail addresses:* laura.bozzelli@fi.upm.es (L. Bozzelli), hans.van-ditmarsch@loria.fr (H. van Ditmarsch), tim@csse.uwa.edu.au (T. French), james@csse.uwa.edu.au (J. Hales), Sophie.Pinchinat@irisa.fr (S. Pinchinat).

http://dx.doi.org/10.1016/j.ic.2014.07.013
0890-5401/

In [56] an axiomatization of the single-agent version of this logic is presented, and also expressivity and complexity results. These questions were visited in both the context of modal logic, and of the modal $\mu$-calculus.

In the original motivation, the main operator $\exists$ had a rather temporal sense — therefore the 'future event' name. However, we have come to realize that the structural transformation that interprets this operator is of much more general use, on many very different kinds of modal logic, namely anywhere where more than a mere model restriction or pruning is required. We have therefore come to call this the refinement operator, and the logic refinement modal logic.

Thus we may consider *refinement modal logic* to be a more abstract perspective of future event logic [55] applicable to other modal logics. To *any* other modal logic! This is significant in that it motivates the application of the new operator in many different settings. In logics for games [42,2] or in control theory [47,51], it may correspond to a player discarding some moves; for program logics [29] it may correspond to operational refinement [40]; and for logics for spatial reasoning it may correspond to sub-space projections [41].

*Let us give an example. Consider the following structure. The $\circ$ state is the designated point. The arrows can be associated with a modality.*



*E.g., $\Diamond\Diamond\Diamond\Box\bot$ is true in the point. From the point of view of the modal language, this structure is essentially the same structure (it is bisimilar) as*



*This one also satisfies $\Diamond\Diamond\Diamond\Box\bot$ and any other modal formula for that matter. A more radical structural transformation would be to consider submodels, such as*



*A distinguishing formula between the two is $\Diamond\Diamond\Box\bot$, which is true here and false above. Can we consider other 'submodel-like' transformations that are* neither *bisimilar structures* nor *strict submodels? Yes, we can. Consider*



*It is neither a submodel of the initial structure, nor is it bisimilar. It satisfies the formula $\Diamond\Diamond\Box\bot \wedge \Diamond\Diamond\Diamond\Box\bot$ that certainly is false in any submodel. We call this structure a refinement (or 'a refinement of the initial structure'), and the original structure a simulation of the latter. Now note that if we consider the three requirements 'atoms', 'forth', and 'back' of a bisimulation, that 'atoms' and 'back' are satisfied but not 'forth', e.g., from the length-three path in the original structure the last arrow has no image. There seems to be still some 'submodel-like' relation with the original structure. Look at its bisimilar duplicate (the one with seven states). The last structure is a submodel of that copy. Such a relation always holds: a refinement of a given structure can always be seen as the model restriction of a bisimilar copy of the given structure. This work deals with the semantic operation of refinement, as in this example, in full generality, and also applied to the multi-agent case.*

Previous works [19,37] employed a notion of refinement. In [37] it was shown that model restrictions were not sufficient to simulate informative events, and they introduced *refinement trees* for this purpose — a precursor of the dynamic epistemic logics developed later (for an overview, see [57]). This usage of refinement as a more general operation than model restriction is similar to ours.

In formal methods literature, see e.g. [62], *refinement of datatypes* is considered such that (datatype) $C$ refines $A$ if $A$ simulates $C$. This usage of refinement as the converse of simulation [1,11] comes close to ours — in fact, it inspired us to propose a similar notion, although the correspondence is otherwise not very close. A similar usage of refinement as in [62] is found in [3,4]. In the theory of modal specifications a refinement preorder is used, known as *modal refinement* [45,49]. Modal specifications are deterministic automata equipped with *may*-transitions and *must*-transitions. A must-transition is available in every component that implements the modal specification, while a may-transition need not be. This is close to our definition of refinement, as it also is some kind of submodel quantifier, but the two notions are incomparable, because 'must' is a subtype of 'may'.

We incorporate implicit quantification over informative events directly into the language using, again, a notion of *refinement*; also in our case a refinement is the converse of simulation. Our work is closely related to some recent work on bisimulation quantified modal logics [17,22]. The refinement operator, seen as refinement quantifier, is weaker than a bisimulation quantifier [55], as it is *only* based on simulations rather than bisimulations, and as it *only* allows us to vary the interpretation of a propositional variable that does not occur in the formula bound by it. Bisimulation quantified modal logic has previously been axiomatized by providing a provably correct translation to the modal $\mu$-calculus [16]. This is reputedly a very complicated one. The axiomatization for the refinement operator, in stark contrast, is quite simple and elegant.