Annals of Mathematics and Artificial Intelligence
https://doi.org/10.1007/s10472-019-09656-4

# Two AGM-style characterizations of model repair

**Paulo T. Guerra**[1] · **Renata Wassermann**[2]

Published online: 02 August 2019



## Abstract

This work explores formal aspects of *model repair*, i.e., how to rationally modify Kripke models representing the behavior of a system in order to satisfy a desired property. We investigate the problem in the light of Alchourrón, Gärdenfors, and Makinson's work on belief revision. We propose two AGM-style characterizations of model repair: one based on belief sets and the other based on structural changes. In the first characterization, we define a set of rationality postulates over formulas with a close correspondence to those in the classical belief revision theory. We show that the proposed set of postulates fully characterizes the expected rationality of modifications in the model repair problem. In the second characterization, we propose a new set of rationality postulates based on structural modifications on models. These postulates have a close correspondence to the classical approach of model repair, while preserving the same rationality of the first characterization. We provide two representation results and the connection between them.


**Keywords** Belief revision · Model repair · Model checking · Representation theorem

**Mathematics Subject Classification (2010)** 03B42 · 03B44

## 1 Introduction

Model checking [10] is an efficient and widely used technique for formal system verification. In this approach, a system is represented by formally defined structures as labeled transition systems or a Kripke structure, and desired properties are specified in some logic formalism such as Computational Tree Logic [9]. The model checking method consists in

The first author was funded by grant 2010/15392-3, São Paulo Research Foundation (FAPESP). This work was funded by the Brazilian Research Council (CNPq) grant number 447178/2014-8.

**Electronic supplementary material** The online version of this article (https://doi.org/10.1007/s10472-019-09656-4) contains supplementary material, which is available to authorized users.

✉ Paulo T. Guerra
paulodetarso@ufc.br

1 Federal University of Ceará, Campus Quixadá, Quixadá, Brazil

2 Institute of Mathematics and Statistics, University of São Paulo, São Paulo, Brazil

performing a systematic analysis of the system model in order to verify whether it satisfies a desired property.

Model checkers can perform complex verification, being able to handle huge search spaces with more than $10^{20}$ possible configurations [6]. However, most of the current model checkers lack mechanisms to assist in the task of fixing the detected errors.

*Model repair* is the problem of how to modify a system model minimally in order to satisfy a desired property. The aim is to find suitable modifications that generate admissible models, representing the intended design for the system. Several approaches have been used to address this problem in the literature, such as abductive reasoning [5], belief change theory [16, 30], game theory [19] and other techniques [2, 4, 7, 25, 27]. The problem is also addressed from other perspectives such as abstract models [8, 15] and probabilistic systems [3].

Belief revision is a theory about how idealized rational agents should adapt their beliefs in order to be consistent with some new belief. The mechanics of belief adaptation with consistency maintenance makes it a suitable theory to address the model repair problem. The general idea consists in assuming the system model as a representation for the initial beliefs and the desired property as the belief to be incorporated. If the model does not entail the property, principles of belief revision are used to guide the modifications needed in the model to ensure that the property is satisfied.

The principle of rational change was addressed by Alchourrón, Gärdenfors, and Makinson [1] in what became known as the AGM theory, by describing a set of expected behaviors that a revision function should obey, the so called *rationality postulates*. AGM postulates intend to capture the intuition of performing changes in beliefs in a rational way, ensuring, for example, the success and consistency of the operations. The authors also presented a construction method for revision functions and showed a direct correspondence between the postulates and their construction, in the sense that every function defined by their construction satisfies the rationality postulates and that every function that satisfies them can be constructed by their method.

In this work, we propose an AGM-style characterization of the model repair operation. We propose a set of rationality postulates with a close correspondence to the AGM postulates and the classical belief revision theory. We show that the proposed set fully characterizes the admissible modifications for model repair. We then propose a second characterization of the repair operation with *easy-to-use* postulates focused on structural modifications applied to models. We also show that this set of postulates characterizes the intended behavior of the model repair operation.

The paper is organized as follows. In Section 2 we introduce some preliminary concepts that are needed for this work. In Section 3 we present the key aspects of the model repair problem. In Section 4 we show the proposed characterizations of model repair. Finally, in Section 5 we present our conclusions and final remarks.

This paper is a revised and extended version of [17].

## 2 Preliminaries

In this section, we introduce the background for our proposal. We first sketch the classical AGM theory of belief revision. Then, we present the temporal logic that we will use in the paper, CTL (Computational Tree Logic).

**Notation** In this work, we assume a language containing at least a set of propositional variables and the Boolean connectives ($\neg$ and $\wedge$). As usual, the other connectives ($\vee$, $\rightarrow$, $\leftrightarrow$) can be used to abbreviate expressions. We use the letters $p$ and $q$ to denote propositional variables, Greek lowercase letters ($\alpha$, $\beta$, $\varphi$) to denote formulas and uppercase letters to denote sets of formulas. We denote by $\mathcal{L}$ the set of all formulas of the language. We use $s$ with or without subscripts to denote states in a transition system. Models are denoted by $\mathcal{M}$, possibly with decorations or subscripts. Given a set of formulas $X$, $Mod(X)$ denotes the set of models that satisfy all formulas in $X$. If $X$ is a singleton $\{\alpha\}$, we may write $Mod(\alpha)$ instead of $Mod(\{\alpha\})$. We say that $X$ entails $\alpha$, denoted by $X \models \alpha$, if $Mod(X) \subseteq Mod(\alpha)$. We use $\alpha \models \beta$ to abbreviate $\{\alpha\} \models \beta$.

### 2.1 Belief revision

Belief revision [1] deals with the problem of adapting a set of beliefs in order to incorporate new information, even if inconsistent with what was believed. Alchourrón, Gärdenfors, and Makinson [1] defined a set of rationality postulates in order to specify what is expected from a rational revision function.

In the AGM theory, belief states are represented by *belief sets*, sets of formulas closed under a consequence operator such that for a belief set $K$, $Cn(K) = K$.

Let $K$ be a belief set, $\alpha$ an input formula and $Cn$ a consequence operator. The AGM theory proposes the following postulates to characterize the rationality of a revision operation, where $K * \alpha$ is the result of revising $K$ by $\alpha$ and $K + \alpha$ denotes the expansion of $K$ with $\alpha$, i.e., adding $\alpha$ to $K$ and closing it with respect to $Cn$ ($K + \alpha = Cn(K \cup \{\alpha\})$):

(K*1) $K * \alpha$ is a belief set.
(K*2) $\alpha \in K * \alpha$.
(K*3) $K * \alpha \subseteq K + \alpha$.
(K*4) If $\neg\alpha \notin K$, then $K + \alpha \subseteq K * \alpha$.
(K*5) $K * \alpha$ is unsatisfiable if and only if $\neg\alpha \in Cn(\emptyset)$.
(K*6) If $\models \alpha \leftrightarrow \beta$, then $K * \alpha = K * \beta$.
(K*7) $K * (\alpha \wedge \beta) \subseteq (K * \alpha) + \beta$.
(K*8) If $\neg\beta \notin K * \alpha$, then $(K * \alpha) + \beta \subseteq K * (\alpha \wedge \beta)$.

Postulate (K*1) says that the revision of a belief set must be another belief set. (K*2) says that the revised belief set must contain the formula by which it is revised. Postulate (K*3) says that no other information besides the formula should be added. Postulate (K*4) says that if the new formula is consistent with the current beliefs no belief should be discarded. Postulate (K*5) says that the revised belief set must be consistent, unless the formula itself is inconsistent. Postulate (K*6) assures that equivalent formulas should result in the same revised belief set. Postulates (K*7) and (K*8) deal with the possibility of performing revision by conjunctions in two steps, through a revision followed by the simple addition (expansion).

The AGM postulates, however, do not define an operator of belief revision, but only restrict the set of possible rational operators. Alchourrón, Gärdenfors, and Makinson [1] also provide a construction for building rational revision operators, called *partial meet construction* which relies on remainder sets.

A *remainder set* $K \perp \alpha$ contains the maximal subsets of $K$ which do not entail a formula $\alpha$:

**Definition 1** Let $K$ be a belief set and $\alpha$ a formula. The *remainder set* $K\perp\alpha$ is a collection of sets $X$ such that

1. $X \subseteq K$
2. $X \nvDash \alpha$
3. For all $X'$ such that $X \subset X' \subseteq K$, $X' \vDash \alpha$

A revised belief set is obtained by selecting some of the elements of $K\perp\alpha$ and taking their intersection.

**Definition 2** A *selection function* $\gamma$ is a function that selects some of the elements of $K\perp\alpha$, such that

1. $\emptyset \subset \gamma(K\perp\alpha) \subseteq K\perp\alpha$ if $K\perp\alpha \neq \emptyset$;
2. $\gamma(K\perp\alpha) = \{K\}$ otherwise.

**Definition 3** Let $K$ be a belief set, $\alpha$ a formula and $\gamma$ a selection function for $K\perp\neg\alpha$. A *partial meet revision* function over $K$ is given by

$$K * \alpha = Cn\left(\bigcap \gamma(K\perp\neg\alpha) \cup \{\alpha\}\right),$$

where $\gamma$ is a selection function such that $\emptyset \subset \gamma(K\perp\neg\alpha) \subseteq K\perp\neg\alpha$ if $K\perp\neg\alpha \neq \emptyset$, or $\gamma(K\perp\neg\alpha) = \{K\}$, otherwise.

In their paper [1], Alchourrón, Gärdenfors, and Makinson show that the partial meet construction has a special relation with the AGM rationality postulates.

**Theorem 1** [1] *Let $*$ be a function which, given a formula $\alpha$, takes a belief set $K$ into a new belief set $K * \alpha$. For every belief set $K$, $*$ is a partial meet revision operation if and only if $*$ satisfies postulates (K*1)—(K*6).*

**Definition 4** A selection function $\gamma$ for $K$ is said to be *transitively relational over $K$* if and only if there is a transitive relation $\leq$ over $2^K$ such that the following identity holds: $\gamma(K \perp \alpha) = \{X \in K \perp \alpha | X' \leq X \text{ for all } X' \in K \perp \alpha\}$.

**Definition 5** A partial meet function $*$ is *transitively relational* if and only if it can be determined by some transitively relational selection function.

**Theorem 2** [1] *For every belief set $K$, $*$ is a transitively relational partial meet revision function if and only if $*$ satisfies (K*1)–(K*8).*

Theorems 1 and 2 are called *representation theorems* and give a full characterization of the revision operations according to their expected rationality.

The seminal work of Alchourrón, Gärdenfors, and Makinson [1] has influenced several authors to adopt this style of characterization of operators, by precisely defining change functions in terms of rationality postulates [11, 18, 23].

Although originally developed for propositional logic, the AGM theory has been successfully adapted to other formalisms [13, 14, 26, 29]. However, its use in non-classical logics demands a careful adaptation since many of them do not fulfill the assumptions made by Alchourrón, Gärdenfors, and Makinson in their original paper: to be Tarskian, compact, supraclassical and to satisfy the deduction theorem.

An operation related to revision has been studied by Katsuno and Mendelzon [20]. While belief revision is concerned with the acquisition of information about a static world, *belief update* deals with updating the knowledge base after some change in the world. Katsuno and Mendelzon have provided a construction as well as a set of rationality postulates characterizing the construction.

Given a finite belief base $\psi$ and a input belief $\varphi$, the update of $\psi$ by $\varphi$, denoted by $\psi \diamond \varphi$, was characterized by Katsuno and Mendelzon [20] by the following set of postulates:

(U1) $\psi \diamond \varphi \models \varphi$.
(U2) If $\psi \models \varphi$, then $\psi \diamond \varphi \equiv \psi$.
(U3) If both $\psi$ and $\varphi$ are satisfiable, then $\psi \diamond \varphi$ is also satisfiable.
(U4) If $\psi_1 \equiv \psi_2$ and $\varphi_1 \equiv \varphi_2$, then $\psi_1 \diamond \varphi_1 \equiv \psi_2 \diamond \varphi_2$.
(U5) $(\psi \diamond \varphi) \wedge \mu \models \psi \diamond (\varphi \wedge \mu)$
(U6) If $\psi \diamond \varphi_1 \models \varphi_2$ and $\psi \diamond \varphi_2 \models \varphi_1$, then $\psi \diamond \varphi_1 \equiv \psi \diamond \varphi_2$
(U7) If $\psi$ is complete (i.e has a unique model) then $(\psi \diamond \varphi_1) \wedge (\psi \diamond \varphi_2) \models \psi \diamond (\varphi_1 \vee \varphi_2)$
(U8) $(\psi_1 \vee \psi_2) \diamond \varphi \equiv (\psi_1 \diamond \varphi) \vee (\psi_2 \diamond \varphi)$

Herzig [31] has shown that, more than distinct, revision and update are mutually incompatible, since no operator is able to satisfies both revision and update postulates. Katsuno and Mendelzon's postulates [20] are an example that the definition of belief change operations might require a different set of rationality postulates to properly characterize the construction.

## 2.2 Computation tree logic

Computation Tree Logic (CTL) is a temporal logic proposed by Clarke and Emerson [9] as a tool for formal design and verification of concurrent systems. CTL is built on an interpretation of multiple futures, where several time-flows can succeed the same instant of time. CTL is specially useful to specify properties of systems in which execution flows may have many possible branches.

**Definition 6** The formulas of CTL are defined by the following grammar in Backus Naur form:

$$\begin{aligned}\phi ::= \; & \top \mid \bot \mid p \mid (\neg\phi) \mid (\phi \vee \phi) \mid (\phi \wedge \phi) \mid (\phi \rightarrow \phi) \mid \mathrm{EX}\phi \mid \\ & \mathrm{AX}\phi \mid \mathrm{EF}\phi \mid \mathrm{AF}\phi \mid \mathrm{EG}\phi \mid \mathrm{AG}\phi \mid \mathrm{E}[\phi \ \mathrm{U} \ \phi] \mid \mathrm{A}[\phi \ \mathrm{U} \ \phi]\end{aligned}$$

where $p$ ranges over a set $AP$ of propositional variables, $\neg, \vee, \wedge, \rightarrow$ are the classical logic connectives and the others are temporal operators composed by path quantifiers (E, "exists a path", or A, "for all paths") and state operators (X, "neXt state", F, "Future", G, "Globally", or U, "Until"). The set of all formulas of the language is denoted by $\mathcal{L}$.

The intuitive meaning of CTL temporal operators is depicted in Fig. 1.

CTL formulas are evaluated over Kripke models, variations of labeled transition systems where there is a map between propositions and states in the model representing whether a given proposition holds in a state.

**Definition 7** A Kripke model $\mathcal{M}$ is a transition system $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ such that:

1. $AP$ is an enumerable set of propositional atoms;
2. $S$ is a finite set of states;

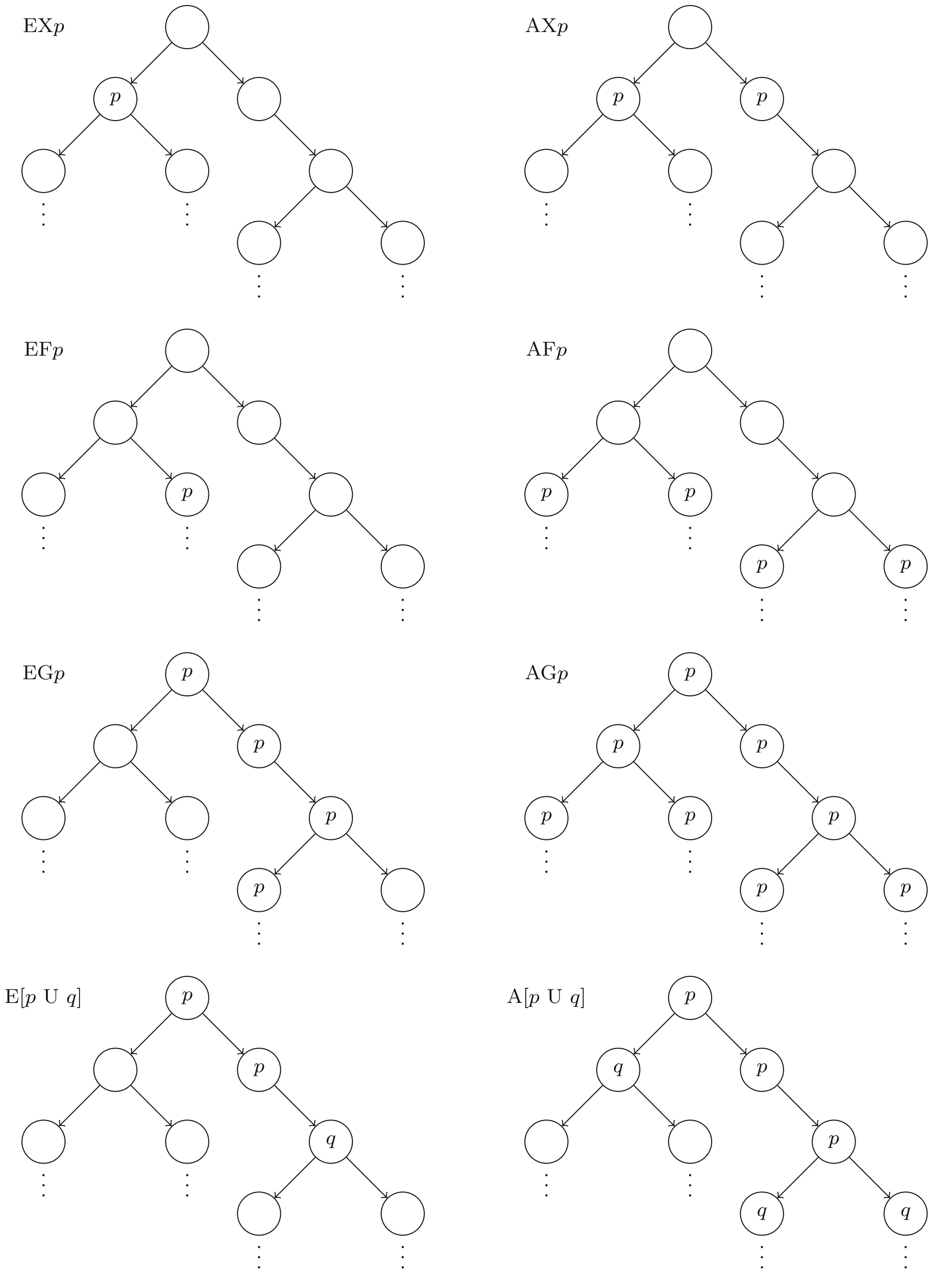



**Fig. 1** CTL temporal operators

3. $s_0 \in S$ is the initial state;
4. $R \subseteq S \times S$ is a serial transition relation[1] over states;

[1]A relation $R$ is serial if, for every $s$ there is a $s'$ such that $(s, s') \in R$.

5. $L : AP \rightarrow \mathcal{P}(S)$ is a labelling function that indicates in which states a given proposition holds in the model.

Figure 2 shows a graphic representation of a Kripke model $\mathcal{M} = \langle \{p, q\}, \{s_0, s_1, s_2\}, s_0, \{(s_0, s_1), (s_1, s_2), (s_2, s_2)\}, L\rangle$ where $L(p) = \{s_0, s_2\}$ and $L(q) = \{s_1, s_2\}$.

**Definition 8** A *path* in a Kripke model $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ is a sequence of states $\pi = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$ such that each $s_i \in \pi$ is in $S$ and for each $s_i, s_{i+1} \in \pi$, we have $(s_i, s_{i+1}) \in R$.

CTL has the following formal semantics, defined by the satisfaction relation $\models$ between a Kripke model and a state and formulas of CTL.

**Definition 9** Let $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ be a Kripke model, $s \in S$ a state of $\mathcal{M}$ and $\varphi$ a CTL formula. We define $\mathcal{M}, s \models \varphi$ inductively as follows:

1. $\mathcal{M}, s \models \top$.
2. $\mathcal{M}, s \not\models \bot$.
3. $\mathcal{M}, s \models p$ iff $s \in L(p)$.
4. $\mathcal{M}, s \models \neg\varphi$ iff $\mathcal{M}, s \not\models \varphi$.
5. $\mathcal{M}, s \models \varphi_1 \vee \varphi_2$ iff $\mathcal{M}, s \models \varphi_1$ or $\mathcal{M}, s \models \varphi_2$.
6. $\mathcal{M}, s \models \varphi_1 \wedge \varphi_2$ iff $\mathcal{M}, s \models \varphi_1$ and $\mathcal{M}, s \models \varphi_2$.
7. $\mathcal{M}, s \models \text{EX}\varphi$ iff there is $s' \in S$ such that $(s, s') \in R$ and $\mathcal{M}, s' \models \varphi$.
8. $\mathcal{M}, s \models \text{AX}\varphi$ iff $\forall s' \in S$ such that $(s, s') \in R$, $\mathcal{M}, s' \models \varphi$.
9. $\mathcal{M}, s \models \text{EF}\varphi$ iff there is a path $\pi = [s_0, s_1, \ldots]$ in $M$ such that $s_0 = s$ and $\mathcal{M}, s_i \models \varphi$ for some $i \geq 0$.
10. $\mathcal{M}, s \models \text{AF}\varphi$ iff for all paths $\pi = [s_0, s_1, \ldots]$ in $M$ such that $s_0 = s$, $\mathcal{M}, s_i \models \varphi$ for some $i \geq 0$.
11. $\mathcal{M}, s \models \text{EG}\varphi$ iff there is a path $\pi = s_0 \rightarrow s_1 \rightarrow \ldots$ in $\mathcal{M}$ such that $s_0 = s$ and $\mathcal{M}, s_i \models \varphi$ for all $i \geq 0$.
12. $\mathcal{M}, s \models \text{AG}\varphi$ iff for all paths $\pi = [s_0, s_1, \ldots]$ in $M$ such that $s_0 = s$, $\mathcal{M}, s_i \models \varphi$ for all $i \geq 0$.

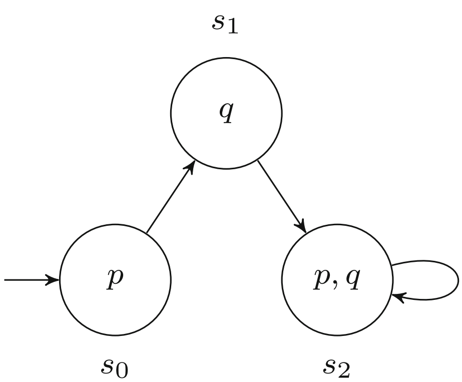



**Fig. 2** Example of Kripke model

13. $\mathcal{M}, s \models \mathrm{E}[\varphi_1 \mathrm{U} \varphi_2]$ iff there is a path $\pi = s_0 \rightarrow s_1 \rightarrow \ldots$ in $\mathcal{M}$ such that $s_0 = s$, $\mathcal{M}, s_i \models \varphi_2$ for some $i \geq 0$ and for all $j < i$, $\mathcal{M}, s_j \models \varphi_1$.
14. $\mathcal{M}, s \models \mathrm{A}[\varphi_1 \mathrm{U} \varphi_2]$ iff for all paths $\pi = [s_0, s_1, \ldots]$ in $M$ such that $s_0 = s$, $\exists i \geq 0$, $\mathcal{M}, s_i \models \varphi_2$ and $\forall j < i$, $\mathcal{M}, s_j \models \varphi_1$.

We use $\mathcal{M} \models \varphi$ to denote $\mathcal{M}, s_0 \models \varphi$.

Two different Kripke models may satisfy the same set of formulas. We can define equivalence between structures based on the notion of a *bissimulation relation*.

**Definition 10** [32] Let $\mathcal{M}_1 = \langle AP, S_1, s_{0_1}, R_1, L_1 \rangle$ and $\mathcal{M}_2 = \langle AP, S_2, s_{0_2}, R_2, L_2 \rangle$ be Kripke models. Then a relation $B \subseteq S_1 \times S_2$ is a bissimulation relation between $M_1$ and $M_2$ if and only if for all $s_1$ and $s_2$, if $(s_1, s_2) \in B$ then

1. $s_1 \in L_1(p)$ if and only if $s_2 \in L_2(p)$.
2. For every state $s_1' \in S_1$ such that $(s_1, s_1') \in R_1$ there is $(s_2, s_2') \in R_2$ and $(s_1', s_2') \in B$.
3. For every state $s_2' \in S_2$ such that $(s_2, s_2') \in R_2$ there is $(s_1, s_1') \in R_1$ and $(s_1', s_2') \in B$.

The structures $\mathcal{M}_1$ and $\mathcal{M}_2$ are bissimiliar (or bissimulation equivalent) if there is a bissimulation relation $B$ such that $(s_{0_1}, s_{0_2}) \in B$. We have then the following theorem:

**Theorem 3** [32] *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be bissimilar Kripke models. Then, for every CTL formula $\varphi$, $\mathcal{M}_1 \models \varphi$ if and only if $\mathcal{M}_2 \models \varphi$.*[2]

This theorem shows the invariance of CTL entailment with respect to bissimulation equivalence. This property plays an important role on the development of model checking algorithms by allowing the efficient computing of structures that are guaranteed to satisfy the same set of formulas.

### 2.2.1 Model checking

The *model checking problem* consists in determining whether an abstract representation of a system, defined by a Kripke model, satisfies a given CTL formula representing a formal specification of a desired property. When the formula is not satisfied, most model checkers return a trace (an execution path) that indicates how the property is violated. The time complexity of the model checking problem is linear both in the size of the model and in the size of the formula [10].

*Example 1* Let $\mathcal{M}$ be the Kripke model illustrated in Fig. 2, we have that $\mathcal{M}, s_0 \models p$, $\mathcal{M}, s_0 \models \mathrm{EF}q$, $\mathcal{M}, s_1 \models \mathrm{AG}q$, $\mathcal{M}, s_2 \models \mathrm{AG}(p \wedge q)$, and that $\mathcal{M}, s_0 \not\models q$, $\mathcal{M}, s_1 \not\models \mathrm{EF}\neg q$, $\mathcal{M}, s_2 \not\models \mathrm{AX}\neg p$.

## 3 Model repair

A model must be repaired if it does not satisfy a desired property. When repairing, we look for rational modifications and, in particular, we expect that these modifications preserve as

[2]This theorem is originally stated in [32] for CTL$^*$ that contains CTL as sublanguage.

much as possible of the original structure. Our goal is to find a set of modifications such that each of them is in some aspect relevant to achieve the satisfiability of the goal property.

*Example 2* Suppose we want to modify the model of Fig. 2 in order to satisfy the formula $\mathrm{EX}(p \wedge q)$. Intuitively we accept as rational to modify the state $s_1$ so that it also satisfies $p$ (Fig. 3a) or to add a transition from $s_0$ to $s_2$ (Fig. 3b), however, the realization of both modifications is seen as unnecessary since only one of them is sufficient to reach the objective.

Zhang and Ding [30] have defined a set of primitive operations over models and rationality criteria for modifications of models based on these operations, in order to delimit the universe of admissible solutions to the model repair problem. The five primitive operations are:

PU1: Adding one relation element (arrow)
PU2: Removing one relation element (arrow)
PU3: Changing the labeling function on one state
PU4: Adding one state
PU5: Removing one isolated state

The operations PU1, PU2, PU4 and PU5 represent the most basic operations on a labeled transition system. Using these operations we can perform most of the needed changes to a Kripke model. These operations, however, may complicate the measure of a repair. For example, suppose we have a model $\mathcal{M}'$ with exactly the same structure as a model $\mathcal{M}$ except for one particular state that has one different proposition on its label. If we see $\mathcal{M}'$ as a result of a repair of model $\mathcal{M}$, we tend to think that $\mathcal{M}'$ is obtained from $\mathcal{M}$ with a single change in the state label, instead of a sequence of operations PU2, PU5, PU4 and PU1 to fully replace that state. This context motivated Zhang and Ding [30] to include PU3 as a primitive operation assuming it as fundamentally different from the combination of the other operations, since it does not require changes in the state name or in transitions in the original model. We follow [30] on the choice of the set of primitive operations.

Zhang and Ding [30] proposed to measure the similarity between modifications based on the effects that their primitive operations produce in the resulting models.

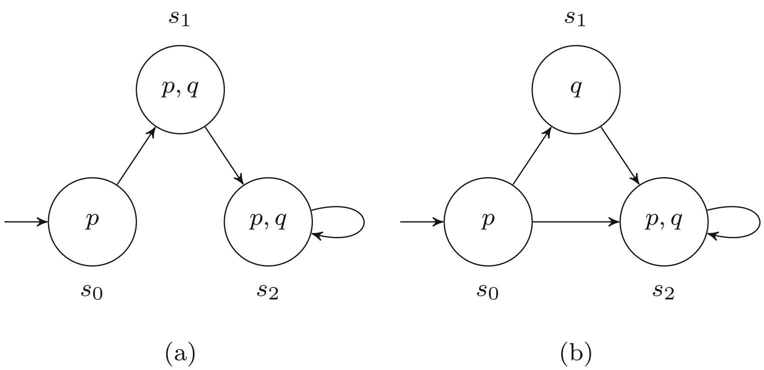



**Fig. 3** Examples of model repair

**Definition 11** [30] Let $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ and $\mathcal{M}' = \langle AP', S', s_0', R', L'\rangle$ be Kripke structures, the structural difference between $\mathcal{M}$ and $\mathcal{M}'$, denoted by $\mathit{Diff}(\mathcal{M}, \mathcal{M}')$, is given by $\mathit{Diff}(\mathcal{M}, \mathcal{M}') = (\mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}'), \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}'), \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}'), \mathit{Diff}_{PU4}(\mathcal{M}, \mathcal{M}'), \mathit{Diff}_{PU5}(\mathcal{M}, \mathcal{M}'))$, where:

1. $\mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}') = R' \setminus R$;
2. $\mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}') = R \setminus R'$;
3. $\mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}') = \bigcup_{p \in AP} \mathit{diff}(L(p), L'(p))$,
4. $\mathit{Diff}_{PU4}(\mathcal{M}, \mathcal{M}') = S' \setminus S$;
5. $\mathit{Diff}_{PU5}(\mathcal{M}, \mathcal{M}') = S \setminus S'$.

where $\mathit{diff}(A, B) = (A \setminus B) \cup (B \setminus A)$.

Zhang and Ding [30] defined a closeness ordering among models, indicating which of two models is more structurally similar to a given referential model.

**Definition 12** [30]. Let $\mathcal{M}$, $\mathcal{M}_1$ and $\mathcal{M}_2$ be three Kripke structures. We say that $\mathcal{M}_1$ is at least as close to $\mathcal{M}$ as $\mathcal{M}_2$, denoted by $\mathcal{M}_1 \leqslant_{\mathcal{M}} \mathcal{M}_2$, if and only if for each set of PU1-PU5 operations that transform $\mathcal{M}$ to $\mathcal{M}_2$, there exists a set of PU1-PU5 operations that transform $\mathcal{M}$ to $\mathcal{M}_1$ such that:

1. $\mathit{Diff}_{PUi}(\mathcal{M}, \mathcal{M}_1) \subseteq \mathit{Diff}_{PUi}(\mathcal{M}, \mathcal{M}_2)$, for $1 \leq i \leq 5$;
2. If $\mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_1) = \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_2)$, then for each $s \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_1)$ and for each $p \in AP$, if $s \in \mathit{diff}(L(p), L_1(p))$, then $s \in \mathit{diff}(L(p), L_2(p))$.

We say $\mathcal{M}_1 <_{\mathcal{M}} \mathcal{M}_2$ if $\mathcal{M}_1 \leqslant_{\mathcal{M}} \mathcal{M}_2$ and $\mathcal{M}_2 \not\leqslant_M \mathcal{M}_1$.

Zhang and Ding's ordering provides a measure of the difference between a pair of models with respect to a base model. Intuitively, a model $\mathcal{M}_1$ is closer to a model $\mathcal{M}$ with respect to a model $\mathcal{M}_2$ if (1) $\mathcal{M}_1$ can be obtained by applying primitive operations that result in fewer changes than those needed to obtain $\mathcal{M}_2$ and (2) in the case where states had changes in their labels, fewer propositional atoms where affected in $\mathcal{M}_1$ than in $\mathcal{M}_2$.

Having the closeness ordering between models, Zhang and Ding proceeded to define the possible updates of a model by a formula as those models of the formula which are closest to the initial model:

**Definition 13** (Adapted from Zhang and Ding [30]). Let $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ be a Kripke structure and $\varphi$ a temporal formula. The set of admissible updates of $\mathcal{M}$ by $\varphi$, denoted by $\mathit{Update}(\mathcal{M}, \varphi)$, is defined as the set of all models $\mathcal{M}'$ such that $\mathcal{M}' \models \varphi$ and there is no other model $\mathcal{M}''$ such that $\mathcal{M}'' \models \varphi$ and $\mathcal{M}'' <_M \mathcal{M}'$.

Zhang and Ding have shown the following result:

**Theorem 4** [30]. *Let $\psi$ and $\alpha$ be two temporal formulas, where $\psi$ represents a belief base, the operator $\diamond_c$ that produces $\psi \diamond_c \alpha$ as result of the update of $\psi$ by $\alpha$, such that*

$$Mod(\psi \diamond_c \phi) = \bigcup_{\mathcal{M} \in Mod(\psi)} Update(\mathcal{M}, \phi),$$

*satisfies the Katsuno and Mendelzon rationality postulates for belief update.*

However, despite showing consistency with the postulates, Zhang and Ding did not show that this set of postulates completely characterizes the repair operation.

Following the work by Zhang and Ding for model update, we have in previous work proposed a similar operation for revising a model:

**Definition 14** [16] Given two CTL formulas $\psi$ and $\phi$, the revision of $\psi$ by $\phi$, denoted by $\psi \circ_c \phi$ results in a CTL formula whose models are defined as

$$Mod(\psi \circ_c \phi) = Min_{Mod(\psi)}(Mod(\phi))$$

where $Min_{\mathcal{B}}(\mathcal{A})$ denotes the set of all minimal elements from $\mathcal{A}$ with respect to all orderings $\leqslant_{\mathcal{M}}$ such that $\mathcal{M}$ is an element of $\mathcal{B}$.

The operator $\circ_c$ performs a comparison among models and sets of models in order to determine the repair solution, in contrast to the pointwise operation $\diamond_c$ proposed by Zhang and Ding [30], which compares models with each model of the knowledge base. This difference makes $\circ_c$ more suitable than $\diamond_c$ for static contexts, in analogy to the difference between belief revision and belief update [16]. It is important to note that in [16] we dealt with partial beliefs, corresponding to sets of models and in this case, update and revision have different outcomes. In the present paper, we are dealing with complete beliefs, corresponding to a single model, as in [30] where update and revision coincide.

Again, the operation is shown to satisfy the revision postulates, but no representation theorem is given.

Our choice of focusing on complete belief sets is directly related to nature of the model repair problem, where we start with a single model and we want to obtain a single revised model. In future works we aim to provide an AGM-style characterization of repair operations for non-complete beliefs, since in the general case the lack of compactness of most temporal logics may rise some computability problems such as whether a non-complete belief set has a model. In [33], we address some computability issues related to revision of temporal beliefs.

Finally, it is important to notice that, in the context of model repair, contraction and revision have similar behavior: revise a model by $\alpha$ or contract by $\neg\alpha$ have the same effect since the resulting model will define a complete belief set. The expansion operation also has a limited behavior, either leaving the belief set unchanged or expanding it into an inconsistent set, because of the lack of undeterminacy in complete beliefs. The distinction among the classical operations happen on repair operations for non-complete beliefs, such as in [16], but it will not be addressed in the present work.

## 4 Characterizations of model repair

Model repair is an operation that, given a model inconsistent with some specification, returns a model satisfying the specification. The concept of admissible change provides a rational set of possible candidates, but the actual repair is actually the selection of one of these candidates to replace the inconsistent model.

Let $\mathbb{M}(K, \alpha)$ denote the set of all possible repair candidates for models of $K$ according to $\alpha$ such that

$$\mathbb{M}(K, \alpha) = \bigcup_{\mathcal{M} \in Mod(K)} Update(\mathcal{M}, \alpha)$$

We define the repair operation with a function among models of the set of admissible modifications $\mathbb{M}(K, \alpha)$.

**Definition 15** Let $K_{\mathcal{M}} = \{\varphi \in \mathcal{L} \mid \mathcal{M} \models \varphi\}$ and $\alpha \in \mathcal{L}$. Then $\gamma$ is a *repair function* for $K$ if the following conditions hold:

1. if $\models \neg\alpha$ or $\mathcal{M} \models \alpha$, $\gamma(K_{\mathcal{M}}, \alpha) = \mathcal{M}$.
2. if $\not\models \neg\alpha$, $\gamma(K_{\mathcal{M}}, \alpha) \in \mathbb{M}(K_{\mathcal{M}}, \alpha)$.
3. if $\alpha \equiv \beta$, $\gamma(K_{\mathcal{M}}, \alpha) = \gamma(K_{\mathcal{M}}, \beta)$. (*syntactical independence*)
4. if $\gamma(K_{\mathcal{M}}, \alpha) \in \mathbb{M}(K_{\mathcal{M}}, \beta)$, $\gamma(K_{\mathcal{M}}, \alpha) = \gamma(K_{\mathcal{M}}, \alpha \wedge \beta)$. (*choice preservation*)

Here we make some important assumptions: (a) $\gamma$ chooses[3] the model $\mathcal{M}$ that defines $K_{\mathcal{M}}$; (b) the repair is independent of the syntax of the input and should produce the same result for logically equivalent formulas; and (c) the repair preserves a coherence on its choices, in the sense that if a repair $\gamma(K, \alpha)$ selects a model $\mathcal{M}'$ and this model is also an admissible candidate for a repair by $\beta$ ($\mathcal{M}' \in \mathbb{M}(K, \beta)$), the repair by $\alpha \wedge \beta$ should preserve the preference by $\mathcal{M}'$ ($\gamma(K, \alpha \wedge \beta) = \mathcal{M}'$).

*Example 3* Let $\mathcal{M}$ and $\mathcal{M}'$ be the models depicted in Figs. 2 and 3a, respectively, and $K = \{\phi \in \mathcal{L} \mid \mathcal{M} \models \phi\}$. A repair function $\gamma$ such that $\gamma(K, \mathrm{EX}(p \wedge q)) = \mathcal{M}'$ expresses that, in order to satisfy $\mathrm{EX}(p \wedge q)$, it is preferred to perform a repair by changing the labelling function of $\mathcal{M}$ than, for example, by changing its transition relation.

In AGM, a selection function that selects a single element of the remainder set gives rise to *maxichoice revision*, which has been criticized for generating complete belief sets, corresponding to a single model. Here, however, we are dealing with model repair, i.e., we start with a single model and we want to obtain a single revised model. It is also worth noting that as we are dealing with a single initial model, there is no difference between revision and update operations.

In order to establish the relation between model repair and classical belief revision theory, we need to formalize the representation of epistemic states. As most works following the AGM tradition deal with propositional logic, where there is a one to one relation between sets of models and sets of formulas, it is easy to move between representations based on formulas and representations based on models. However, this is not the case with CTL, where a single complete theory may correspond to more than one model. Two structurally different models can be logically equivalent, i.e., satisfy exactly the same set of formulas. In order to connect models and theories in CTL, we introduce a modification in our models. In our approach, beliefs are represented by sets of formulas that may be defined by an *internalized model*, i.e., a model in which the state names are also propositional variables and are valid exactly in the corresponding states:

**Definition 16** An *internalized model* is a Kripke structure $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ such that $S \subseteq AP$ and $L(s) = \{s\}$, for all $s \in S$.

Internalized models allow us to capture structural aspects of models on the set of formulas that hold on it. For example, a transition from an initial state $s_0$ to a state $s_1$ in a model

[3]Later in this work this assumption will not be needed since some restrictions will result in an *one-to-one* correspondence between sets and models.

$\mathcal{M}$ is reflected in the fact that $\mathcal{M} \models s_0 \wedge \mathrm{EX}s_1$ holds. Internalized models play an important role in this work by providing an explicit correlation between syntactical and semantic aspects of model repair.

Note that Zhang and Ding's ordering relation (Definition 12) does not distinguish equivalent modifications, in the sense that an addition of a state $s_1$ or a state $s_2$ will be seen as different modifications, even if they are isomorphic. For this reason, internalized models seem indeed necessary to address this particular aspect of Zhang and Ding's definitions.

Every Kripke structure could be turned into an internalized model by including its state symbols into its propositional signature. Figure 4 shows an internalized version of the model of Fig. 2.

It should be noted that from an internalized model, its non-internalized version can be trivially obtained by deleting the propositional variables which are in $S$. The model can also be seen as a compact representation of a (infinite) set of temporal beliefs.

**Definition 17** A set $K$ is said to be *definable by an internalized model* if and only if there is an internalized model $\mathcal{M}$ such that $K = \{\phi \in \mathcal{L} \mid \mathcal{M} \models \phi\}$.

Note that any set $K$ definable by an internalized model is a complete theory in CTL, since following Definition 9, each CTL formula will either hold or not on a given model.

It is also important to remark that not every belief set $K$ is definable by an internalized model. As an example, if we consider $AP = \{s_0, s_1\}$ a belief set containing $\{s_0, \neg s_1, \mathrm{EX}(s_0 \wedge s_1)\}$ cannot be defined by an internalized model.

We have the following relation between belief sets defined by internalized and non-internalized models:

**Proposition 1** *Let $\mathcal{L}_{AP}$ be the set of all formulas defined over propositional variables $AP$, $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$ be a Kripke model and $\mathcal{M}'$ the internalized version of $\mathcal{M}$. For two sets $K$ and $K'$ defined, respectively, by $\mathcal{M}$ and $\mathcal{M}'$ we have that $K \cap \mathcal{L}_{AP} = K' \cap \mathcal{L}_{AP}$.*

*Proof* We have that $K \cap \mathcal{L}_{AP} \subseteq K' \cap \mathcal{L}_{AP}$ by construction of $\mathcal{M}'$. It remains to show that $K' \cap \mathcal{L}_{AP} \subseteq K \cap \mathcal{L}_{AP}$. Suppose, for the purpose of contradiction, that $\varphi \in K' \cap \mathcal{L}_{AP}$ but $\varphi \notin K \cap \mathcal{L}_{AP}$. Since $\varphi \in K' \cap \mathcal{L}_{AP}$ we have that $\varphi \in K'$ and $\varphi \in \mathcal{L}_{AP}$. Since $\varphi \notin K \cap \mathcal{L}_{AP}$ it must be the case that $\varphi \notin K$. However $K$ is a complete belief set, then $\neg\varphi \in K$. Since $\neg\varphi \in \mathcal{L}_{AP}$ and $\neg\varphi \in K \cap \mathcal{L}_{AP}$, we have that $\neg\varphi \in K' \cap \mathcal{L}_{AP}$. Thus, it must be the case that $\{\varphi, \neg\varphi\} \subseteq K'$, a contradiction. Therefore, $K' \cap \mathcal{L}_{AP} \subseteq K \cap \mathcal{L}_{AP}$ and thus $K \cap \mathcal{L}_{AP} = K' \cap \mathcal{L}_{AP}$. □

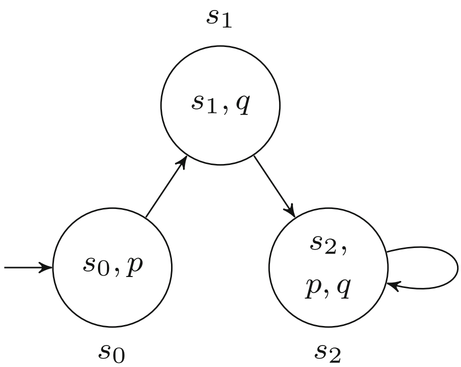



**Fig. 4** Internalized version of the model of Fig. 2

The use of internalized models also gives us some interesting properties with respect to the relation between models and formulas.

**Proposition 2** *If $K$ is definable by an internalized model, then there is only one internalized model without unreachable states that defines $K$. And given an internalized model without unreachable states, there is a single belief set corresponding to the formulas valid in the model.*

*Proof* Let $\mathcal{M}_1 = \langle AP, S_1, s_{0_1}, R_1, L_1\rangle$ and $\mathcal{M}_2 = \langle AP, S_2, s_{0_2}, R_2, L_2\rangle$ be two internalized models with only reachable states. We show that if $K = \{\phi \in \mathcal{L} \mid \mathcal{M}_1 \models \phi\} = \{\phi \in \mathcal{L} \mid \mathcal{M}_2 \models \phi\}$, then $\mathcal{M}_1 = \mathcal{M}_2$.

Suppose, for the purpose of contradiction, that $\mathcal{M}_1$ and $\mathcal{M}_2$ are not equal. Thus, since all states of $\mathcal{M}_1$ and $\mathcal{M}_2$ are reachable, we have that

1. if $s \in S_1$ and $s \notin S_2$, then $\mathcal{M}_1 \models \mathrm{EF}s$ and $\mathcal{M}_2 \not\models \mathrm{EF}s$ and thus $\{\phi \in \mathcal{L} \mid \mathcal{M}_1 \models \phi\} \neq \{\phi \in \mathcal{L} \mid \mathcal{M}_2 \models \phi\}$;
2. if $(s, r) \in R_1$ and $(s, r) \notin R_2$, then $\mathcal{M}_1 \models \mathrm{EF}(s \rightarrow \mathrm{EX}r)$ and $\mathcal{M}_2 \not\models \mathrm{EF}(s \rightarrow \mathrm{EX}r)$ and thus $\{\phi \in \mathcal{L} \mid \mathcal{M}_1 \models \phi\} \neq \{\phi \in \mathcal{L} \mid \mathcal{M}_2 \models \phi\}$;
3. if $s \in L_1(p)$ and $s \notin L_2(p)$, then $\mathcal{M}_1 \models \mathrm{EF}(s \wedge p)$ and $\mathcal{M}_2 \not\models \mathrm{EF}(s \wedge p)$ and thus $\{\phi \in \mathcal{L} \mid \mathcal{M}_1 \models \phi\} \neq \{\phi \in \mathcal{L} \mid \mathcal{M}_2 \models \phi\}$;

In all cases, the differences between $\mathcal{M}_1$ and $\mathcal{M}_2$ lead to a contradiction with the premise that $K = \{\phi \in \mathcal{L} \mid M_1 \models \phi\} = \{\phi \in \mathcal{L} \mid \mathcal{M}_2 \models \phi\}$, hence it should be the case that $\mathcal{M}_1 = \mathcal{M}_2$. □

We denote by $\mathbb{K}$ the set of all sets definable by an internalized model (without unreachable states). From now on, belief states will be assumed to be represented by belief sets in the set $\mathbb{K}$. The only exception in our representation will be the belief state that represents the inconsistent beliefs, which we represent by the set of all formulas of the language $\mathcal{L}$ that has no model.[4]

From this epistemic representation, we can then establish the following relation between the model repair and the classical AGM postulates:

**Proposition 3** *The repair function $*_\gamma$ for $K \in \mathbb{K}$ defined as*

$$K *_\gamma \alpha = \begin{cases} \{\phi \in \mathcal{L} \mid \gamma(K, \alpha) \models \phi\}, \textit{ if } \neg\alpha \notin Cn(\emptyset), \\ \mathcal{L}, \textit{ otherwise.} \end{cases}$$

*satisfies the postulates (K*1)–(K*8).*

*Proof* If $\alpha$ is inconsistent, all postulates are trivially satisfied. If $\alpha$ is satisfiable, (K*1) is trivially satisfied, given that our definition of belief sets is restricted to sets of formulas that can be defined by internalized models. By definition, $\mathit{Update}(K, \alpha) \subseteq \mathit{Mod}(\alpha)$, thus satisfying the Postulate (K*2). For the postulate (K*3), we have two cases: if $\alpha \notin K$, then $\neg\alpha \in K$ and $K + \alpha = \mathcal{L}$; otherwise, $\alpha \in K$ and $K *_\gamma \alpha = K$. In both cases $K *_\gamma \alpha \subseteq K + \alpha$ and the postulate (K*3) is satisfied. The postulate (K*4) is also satisfied, since if $\neg\alpha \notin K$, then $\alpha \in K$ and thus $K + \alpha = K \subseteq K = K *_\gamma \alpha$. For (K*5), if $\not\models \neg\alpha$, then $\mathit{Update}(K, \alpha) \neq \emptyset$, then $K *_\gamma \neq \mathcal{L}$. The other case is trivially satisfied by the definition

[4]This exception is relevant with respect to AGM postulates. Without it, postulates (K*1) and (K*5) would be incompatible.

of $*_\gamma$. For the postulate (K*6), if $\models \alpha \leftrightarrow \beta$ then $Mod(\alpha) = Mod(\beta)$, thus $\mathbb{M}(K, \alpha) = \mathbb{M}(K, \beta)$ and $\gamma(K, \alpha) = \gamma(K, \beta)$, hence $K *_\gamma \alpha = K *_\gamma \beta$, satisfying the postulate (K*6). For the postulate (K*7), if $\mathcal{M}' = \gamma(K, \alpha)$ and $\mathcal{M}' \not\models \beta$, then $(K *_\gamma \alpha) + \beta = \mathcal{L}$ and the postulate is trivially satisfied. If $\mathcal{M}' = \gamma(K, \alpha)$ and $\mathcal{M}' \models \beta$, then $\mathcal{M}' = \gamma(K, \alpha \wedge \beta)$ and thus $K *_\gamma (\alpha \wedge \beta) \subseteq (K *_\gamma \alpha) + \beta$, also satisfying the postulate (K*7). For the postulate (K*8), if $\neg\beta \notin K *_\gamma \alpha$, then $\beta \in K *_\gamma \alpha$. Thus, $\gamma(K, \alpha) = \gamma(K, \alpha \wedge \beta)$ and $(K *_\gamma \alpha) + \beta \subseteq K *_\gamma (\alpha \wedge \beta)$, satisfying the postulate (K*8). □

There are, however, revision operators that satisfy the postulates (K*1)–(K*8) but do not produce the expected rationality for model repair.

*Example 4* Let $*_p$ be a revision operator such that

$$K *_p \alpha = \begin{cases} K *_\gamma (\alpha \wedge \neg p), & \text{if } Update(\mathcal{M}, \alpha \wedge \neg p) \neq \emptyset, \\ K *_\gamma \alpha, & \text{othewise.} \end{cases}$$

where $\mathcal{M}$ is the model that defines $K$ and $*_\gamma$ is a repair function defined as in Proposition 3. We have that $*_p$ satisfies the postulates (K*1)–(K*8). However, for $\mathcal{M}$ depicted in Fig. 2 and $K$ defined by $\mathcal{M}$, we have that $\neg p \in K *_p \mathrm{EX}(p \wedge q)$, but no admissible update would remove $p$ from $s_0$ in order to satisfy $\mathrm{EX}(p \wedge q)$.

In this sense, postulates (K*1)–(K*8) do not correspond to a suitable set of postulates for the characterization of the model repair operation.

### 4.1 AGM-style characterization

We need a set of postulates that capture the principle of minimal change expected for a model repair. We want to preserve as much of the original structure as possible, so we expect that the repair operator will not give up any belief about the structure that can be preserved. Indeed, the AGM postulates alone are not capable of capturing this principle, as noted by Parikh [22] among others.

In every set $K$ defined by an internalized model, there is a subset $K_c \subseteq K$ that contains a "description" of the model, which we call the *core* of $K$.

**Definition 18** Let $K$ be a set of formulas defined by an internalized model $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$. Then the core $K_c$ of $K$ is the smallest set of formulas such that

1. $\mathrm{AG}(s_i \rightarrow \mathrm{EX}s_j) \in K_c$, for all $(s_i, s_j) \in R$;
2. $\mathrm{AG}(s_i \rightarrow \neg\mathrm{EX}s_j) \in K_c$, for all $(s_i, s_j) \notin R$;
3. $\mathrm{AG}(s_i \rightarrow p) \in K_c$, for all $s_i \in S$ and $s_i \in L(p)$;
4. $\mathrm{AG}(s_i \rightarrow \neg p) \in K_c$, for all $s_i \in S$ and $s_i \notin L(p)$.

*Example 5* Let $\mathcal{M}$ be the model depicted in Fig. 4 and $K$ the set defined by $\mathcal{M}$, the core $K_c$ of $K$ is given by:

$$\begin{aligned} K_c = \{&\mathrm{AG}(s_0 \rightarrow \mathrm{EX}s_1), \mathrm{AG}(s_1 \rightarrow \mathrm{EX}s_2), \mathrm{AG}(s_2 \rightarrow \mathrm{EX}s_2), \\ &\mathrm{AG}(s_0 \rightarrow \neg\mathrm{EX}s_0), \mathrm{AG}(s_0 \rightarrow \neg\mathrm{EX}s_2), \mathrm{AG}(s_1 \rightarrow \neg\mathrm{EX}s_0), \\ &\mathrm{AG}(s_1 \rightarrow \neg\mathrm{EX}s_1), \mathrm{AG}(s_2 \rightarrow \neg\mathrm{EX}s_0), \mathrm{AG}(s_2 \rightarrow \neg\mathrm{EX}s_1), \\ &\mathrm{AG}(s_0 \rightarrow p), \mathrm{AG}(s_1 \rightarrow q), \mathrm{AG}(s_2 \rightarrow p), \mathrm{AG}(s_2 \rightarrow q), \\ &\mathrm{AG}(s_0 \rightarrow \neg q), \mathrm{AG}(s_1 \rightarrow \neg p)\}. \end{aligned}$$

The set $K_c$ contains formulas of $K$ that are closely related to transitions and labels of the model that defines $K$. An important feature in this set is that structural differences, such as those made by model repair, have a direct effect on the core set.

We propose then a new postulate of rationality related to the relevance of a repair based on the concept of core sets. The aim of this postulate is to link the rationality of the model repair operation to the preservation of the core of a belief set:

$$\text{If } \beta \in K_c \setminus K * \alpha \text{ and } \alpha \wedge \beta \text{ is satisfiable, then } K * \alpha \cap K_c \not\subseteq K * (\alpha \wedge \beta) \cap K_c. \quad \text{(K*R)}$$

Intuitively, the postulate (K*R) states that we can give up a core belief only if, in the case of preserving it, we do not generate a strictly better result with respect to the preservation of the core set.

It is important to notice that, although we use the name relevance, postulate (K*R) is essentially different from Hansson's relevance postulate [34]. In some sense, Hansson's postulate targets the relevance of contraction of formulas for the success of a revision. Postulate (K*R) however deals only with a core set of formulas and how a contraction of its formulas must be linked to preferences between possible structural changes. Postulate (K*R) ensures that an operator avoids changes in the core set unless strictly necessary.

*Example 6* Let $K$, $K'$, and $K''$ be sets defined by the models depicted in Figs. 4, 5 and 6, respectively. Let $*_p$ be the repair operation defined in Example 4 such that, for the CTL formulas $\alpha = \text{EX}(p \wedge q)$ and $\beta = \text{AG}(s_0 \rightarrow p)$, we have $K *_p \alpha = K'$ and $K *_p (\alpha \wedge \beta) = K''$. Although $*_p$ might satisfy (K*1)–(K*8), it does not satisfy (K*R) since we have $\beta \in K_c \setminus K *_p \alpha$, where $K_c$ is the core of $K$, $\alpha \wedge \beta$ is satisfiable, but $K *_p \alpha \cap K_c \subseteq K *_p (\alpha \wedge \beta) \cap K_c$.

There is a close relation between core sets and the closeness ordering among models given by Definition 12. This relation is shown in the following proposition:

**Proposition 4** *Let $\mathcal{M}$, $\mathcal{M}_1$, $\mathcal{M}_2$ be three Kripke models and $K_c$ the core of the set defined by $\mathcal{M}$.*

(a) *If $\mathcal{M}_1 \leqslant_{\mathcal{M}} \mathcal{M}_2$, then for each $\beta \in K_c$, $\mathcal{M}_2 \models \beta$ implies $\mathcal{M}_1 \models \beta$.*
(b) *If for each $\beta \in K_c$, $\mathcal{M}_2 \models \beta$ implies $\mathcal{M}_1 \models \beta$, then there is a model $\mathcal{M}'_1$ bisimilar to $\mathcal{M}_1$ such that $\mathcal{M}'_1 \leqslant_{\mathcal{M}} \mathcal{M}_2$.*
(c) *If $\mathcal{M}_1 <_{\mathcal{M}} \mathcal{M}_2$, then there is a $\beta \in K_c$ such that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.*

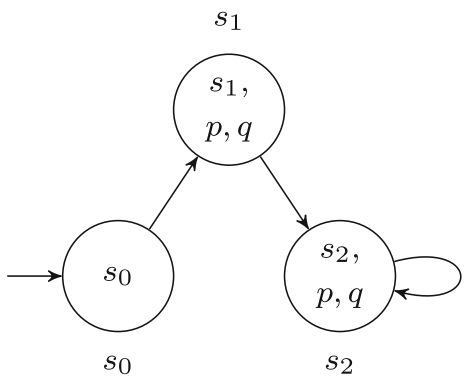



**Fig. 5** Model for $K *_p \alpha$ in Example 6

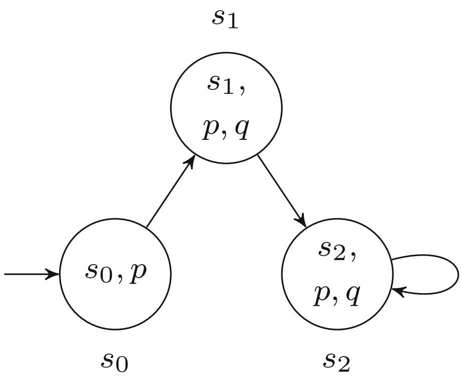



**Fig. 6** Model for $K *_p (\alpha \wedge \beta)$ in Example 6

*Proof* Let $\mathcal{M} = \langle AP, S, s_0, R, L\rangle$, $\mathcal{M}_1 = \langle AP, S_1, s_1, R_1, L_1\rangle$ and $\mathcal{M}_2 = \langle AP, S_2, s_2, R_2, L_2\rangle$ be Kripke models and $K_c$ be the core set of the belief set defined by $\mathcal{M}$.

**(a)** Suppose, for the purpose of contradiction, that $\mathcal{M}_1 \leqslant_{\mathcal{M}} \mathcal{M}_2$ and that for some $\beta \in K_c$ we have $\mathcal{M}_2 \models \beta$ and $\mathcal{M}_1 \not\models \beta$. We have the following cases:

1. if $\beta = \mathrm{AG}(s_i \rightarrow \neg\mathrm{EX}s_j)$ and $\mathcal{M}_1 \not\models \beta$, then there is $(s_i, s_j) \in \mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}_1)$, thus $(s_i, s_j) \in \mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}_2)$, and it can not be the case that $\mathcal{M}_2 \models \mathrm{AG}(s_i \rightarrow \neg\mathrm{EX}s_j)$;
2. if $\beta = \mathrm{AG}(s_i \rightarrow \mathrm{EX}s_j)$ and $\mathcal{M}_1 \not\models \beta$, then there is $(s_i, s_j) \in \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}_1)$, thus $(s_i, s_j) \in \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}_2)$, and it can not be the case that $\mathcal{M}_2 \models \mathrm{AG}(s_i \rightarrow \mathrm{EX}s_j)$;
3. if $\beta = \mathrm{AG}(s_i \rightarrow p)$ and $\mathcal{M}_1 \not\models \beta$, then there is $s_i \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_1)$ and $s_i \notin L_1(p)$, the same occurs in $\mathcal{M}_2$, and thus it can not be the case that $\mathcal{M}_2 \models \mathrm{AG}(s_i \rightarrow p)$;
4. if $\beta = \mathrm{AG}(s_i \rightarrow \neg p)$ and $\mathcal{M}_1 \not\models \beta$, then there is $s_i \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_1)$ and $s_i \in L_1(p)$, the same occurs in $\mathcal{M}_2$, and thus it can not be the case that $\mathcal{M}_2 \models \mathrm{AG}(s_i \rightarrow \neg s_j)$;

All cases lead to a contradiction, so if $\mathcal{M}_1 \leqslant_{\mathcal{M}} \mathcal{M}_2$, then for all $\beta \in K_c$, $\mathcal{M}_2 \models \beta$ implies $\mathcal{M}_1 \models \beta$.

**(b)** Suppose, for the purpose of contradiction, that for all $\beta \in K_c$, $\mathcal{M}_2 \models \beta$ implies $\mathcal{M}_1 \models \beta$, but $\mathcal{M}_1 \not\leqslant_{\mathcal{M}} \mathcal{M}_2$.

Suppose, for the purpose of contradiction, that for all $\beta \in K_c$, $\mathcal{M}_2 \models \beta$ implies $\mathcal{M}_1 \models \beta$, but for all models $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ we have $\mathcal{M}_1' \not\leqslant_{\mathcal{M}} \mathcal{M}_2$. We will show that $\mathcal{M}_1$ itself or another bisimilar model violates this assumption.

We have the following cases:

1. If $(s, r) \in \mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}_1)$ and $(s, r) \notin \mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}_2)$, then for $\mathrm{AG}(s \rightarrow \neg\mathrm{EX}r) \in K_c$, we have $\mathcal{M}_2 \models \mathrm{AG}(s \rightarrow \neg\mathrm{EX}r)$ and thus $\mathcal{M}_1 \models \mathrm{AG}(s \rightarrow \neg\mathrm{EX}r)$. If $s$ is a reachable state in $\mathcal{M}_1$, we have a contradiction. Otherwise, there is a model $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ such that $(s, r)$ does not belong to the model.
2. If $(s, r) \in \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}_1)$ and $(s, r) \notin \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}_2)$, then for $\mathrm{AG}(s \rightarrow \mathrm{EX}r) \in K_c$, we have $\mathcal{M}_2 \models \mathrm{AG}(s \rightarrow \mathrm{EX}r)$ and thus $\mathcal{M}_1 \models \mathrm{AG}(s \rightarrow \mathrm{EX}r)$. If $s$ is a reachable state in $\mathcal{M}_1$, we have a contradiction. Otherwise, there is a model $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ such that $(s, r)$ belongs to the model.

3. If $s \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_1)$ and $s \notin \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_2)$, or if for some $p \in AP$, $s \in L(p)$, $s \in L_2(p)$ and $s \notin L_1(p)$, then we have $\mathrm{AG}(s \to p) \in K_c$, thus we have that $\mathcal{M}_2 \models \mathrm{AG}(s \to p)$ and $\mathcal{M}_1 \models \mathrm{AG}(s \to p)$. If $s$ is a reachable state in $\mathcal{M}_1$, we have a contradiction. Otherwise, there is a model $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ such that $s \in L_1'(p)$. An analogous reasoning can be applied to the case where $s \notin L(p)$, $s \notin L_2(p)$ and $s \in L_1(p)$.
4. If $s \in \mathit{Diff}_{PU4}(\mathcal{M}, \mathcal{M}_1)$ and $s \notin \mathit{Diff}_{PU4}(\mathcal{M}, \mathcal{M}_2)$, then we have $\mathcal{M}_2 \models \mathrm{AG}(s \to p)$ and $\mathcal{M}_2 \models \mathrm{AG}(s \to \neg p)$, for all $\mathrm{AG}(s \to \neg p), \mathrm{AG}(s \to \neg p) \in K_c$. If $s$ is an reachable state in $\mathcal{M}_1$, we have a contradiction. Otherwise, there is a model $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ such that $s$ does not belong to the model.
5. If $s \in \mathit{Diff}_{PU5}(\mathcal{M}, \mathcal{M}_1)$ and $s \notin \mathit{Diff}_{PU5}(\mathcal{M}, \mathcal{M}_2)$, there is a model $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ such that $s$ belongs to the model $\mathcal{M}_1'$, being however unreachable.

In all cases, we can define a model $\mathcal{M}_1'$ bisimilar to $\mathcal{M}_1$ which does not show the structural differences with respect to $\mathcal{M}_2$, thus $\mathcal{M}_1' \leqslant_{\mathcal{M}} \mathcal{M}_2$.

**(c)** Suppose that $\mathcal{M}_1 <_{\mathcal{M}} \mathcal{M}_2$, we have $\mathcal{M}_2 \not\leqslant_{\mathcal{M}} \mathcal{M}_1$. We have one of the following cases:

1. If $(s, r) \in \mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}_2)$ and $(s, r) \notin \mathit{Diff}_{PU1}(\mathcal{M}, \mathcal{M}_1)$, given that $s$ is reachable in $\mathcal{M}_2$, then for $\beta = AG(s \to \neg \mathrm{EX}r) \in K_c$, we have that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.
2. If $(s, r) \in \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}_2)$ and $(s, r) \notin \mathit{Diff}_{PU2}(\mathcal{M}, \mathcal{M}_1)$, given that $s$ is reachable in $\mathcal{M}_2$, then for $\beta = AG(s \to \mathrm{EX}r) \in K_c$, we have that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.
3. If $s \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_2)$ and $s \notin \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_2)$, given that $s$ is reachable in $\mathcal{M}_2$, then for some $\beta = \mathrm{AG}(s \to p)$ or $\beta = \mathrm{AG}(s \to \neg p)$, we have that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.
4. If $s \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_2)$ and $s \in \mathit{Diff}_{PU3}(\mathcal{M}, \mathcal{M}_2)$, there is some $p \in AP$ such that $s \in L_2(p)$ and $s \notin L_1(s)$ or $s \notin L_2(p)$ and $s \in L_1(s)$. Given that $s$ is reachable in $\mathcal{M}_2$, then for some $\beta = \mathrm{AG}(s \to p)$ or $\beta = \mathrm{AG}(s \to \neg p)$, we have that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.
5. If $s \in \mathit{Diff}_{PU4}(\mathcal{M}, \mathcal{M}_2)$ and $s \notin \mathit{Diff}_{PU4}(\mathcal{M}, \mathcal{M}_1)$, given that $s$ is reachable in $\mathcal{M}_2$, then there is $\beta = AG(r \to \neg \mathrm{EX}s) \in K_c$ such that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.
6. If $s \in \mathit{Diff}_{PU5}(\mathcal{M}, \mathcal{M}_2)$ and $s \notin \mathit{Diff}_{PU5}(\mathcal{M}, \mathcal{M}_1)$, given that $s$ is reachable in $\mathcal{M}$ and $\mathcal{M}_1$, then there is $\beta = AG(r \to \mathrm{EX}s) \in K_c$ such that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$.

In all cases, there is $\beta \in K_c$ such that $\mathcal{M}_1 \models \beta$ and $\mathcal{M}_2 \not\models \beta$, then the property holds. □

We can now show that the set of postulates (K*1)–(K*8) and (K*R) completely characterizes the class of operations that produce admissible solutions for the model repair:

**Theorem 5** *Let $K \in \mathbb{K}$ be a belief set and $*$ a revision operator for $K$. Then $*$ satisfies (K*1)–(K*8) and (K*R) if and only if there is a repair function $\gamma$ for $K$ such that*

$$K * \alpha = \begin{cases} \{\phi \in \mathcal{L} \mid \gamma(K, \alpha) \models \phi\}, & \textit{if } \alpha \textit{ is satisfiable,} \\ \mathcal{L}, & \textit{otherwise.} \end{cases}$$

*Proof* (construction ⇒ postulates) Let $\gamma$ be a model repair function and $*$ be an operator such that $K * \alpha = \{\phi \in \mathcal{L} \mid \mathcal{M}' = \gamma(K, \alpha) \text{ and } \mathcal{M}' \models \phi\}$, if $\alpha$ is satisfiable, and $K * \alpha = \mathcal{L}$, otherwise. The satisfaction of the postulates (K*1)–(K*8) follows as in the proof of Theorem 3, it remains to be shown that $*$ satisfies (K*R).

Suppose that $\beta \in K_c \setminus K * \alpha$ and $\alpha \wedge \beta$ is satisfiable (for other cases the postulate is trivially satisfied). Let $\mathcal{M}$ be a model that defines $K$, $\mathcal{M}_1 = \gamma(K, \alpha)$ and $\mathcal{M}_2 = \gamma(K, \alpha \wedge \beta)$, we need to show that there is $\beta' \in K_c$ such that $\mathcal{M} \models \beta'$, $\mathcal{M}_1 \models \beta'$ and $\mathcal{M}_2 \not\models \beta'$. Suppose there is no such $\beta'$. As for each $\beta \in K_c$, $\mathcal{M}_1 \models \beta$ implies that $\mathcal{M}_2 \models \beta$, by Proposition 4(4), there exists a model $\mathcal{M}_2'$ bisimilar to $\mathcal{M}_2$ such that $\mathcal{M}_2' \leqslant_{\mathcal{M}} \mathcal{M}_1$. However, it is not the case that $\mathcal{M}_1 \not\leqslant_{\mathcal{M}} \mathcal{M}_2'$, since $\mathcal{M}_1 \not\models \beta$, thus $\mathcal{M}_1$ could not belong to $\mathbb{M}(K, \alpha)$, which contradicts the selection $\mathcal{M}_1 = \gamma(K, \alpha)$. Therefore, it should be the case where $\beta' \in K_c$ such that $\mathcal{M} \models \beta'$, $\mathcal{M}_1 \models \beta'$ and $\mathcal{M}_2 \not\models \beta'$, and thus $K * \alpha \cap K_c \not\subseteq K * (\alpha \wedge \beta) \cap K_c$.

(postulates ⇒ construction) Let $*$ be an operator satisfying the postulates (K*1)–(K*8) and (K*R). We will show that for $K \in \mathbb{K}$, if $\alpha$ satisfiable, there exists a $\mathcal{M}'$ such that for $\gamma(K, \alpha) = \mathcal{M}'$ we have $K * \alpha = \{\phi \in \mathcal{L} \mid \mathcal{M}' \models \phi\}$.[5]

Let $*$ be an operator satisfying the postulates (K*1)–(K*8) and (K*R). We will show that for $K \in \mathbb{K}$, if $\alpha$ is satisfiable, there exists a $\mathcal{M}'$ such that for $\gamma(K, \alpha) = \mathcal{M}'$ we have $K * \alpha = \{\phi \in \mathcal{L} \mid \mathcal{M}' \models \phi\}$.

Let $\mathcal{M}$ be the internalized model that defines $K$. If $\alpha \in K$, by the postulates (K*3) and (K*4) we have $K * \alpha = K$, and hence $\mathcal{M} = \mathcal{M}'$. Assume that $\alpha \notin K$. We must show there is always $\mathcal{M}' \in \mathbb{M}(K, \alpha)$ such that $K * \alpha = \{\phi \in \mathcal{L} \mid \mathcal{M}' \models \phi\}$.

Suppose, by contradiction, that for every $\mathcal{M}' \in \mathbb{M}(\mathcal{M}, \alpha)$, we have $K * \alpha \neq \{\phi \in \mathcal{L} \mid \mathcal{M}' \models \phi\}$. From (K*5), we have $Mod(K * \alpha) \neq \emptyset$. Therefore, for all $\mathcal{M} \in Mod(K)$ and $\mathcal{M}' \in Mod(K * \alpha)$, there is a model $\mathcal{M}'' \in \mathbb{M}(\mathcal{M}, \alpha)$ such that $\mathcal{M}'' <_{\mathcal{M}} \mathcal{M}'$.

Let $\mathcal{M}'$ be a model that defines $K * \alpha$, $\mathcal{M}'' \in \mathbb{M}(K, \alpha)$ a model such that $\mathcal{M}'' <_{\mathcal{M}} \mathcal{M}'$, for some $\mathcal{M} \in Mod(K)$, and $S^* = \{s_0, s_1, ..., s_n\}$ the union of the states of $\mathcal{M}$, $\mathcal{M}'$ and $\mathcal{M}''$. We have that $\phi_1 = \mathrm{AG}(s_0 \vee s_1 \vee ... \vee s_n) \in K * \alpha$, then, by the postulates (K*7) and (K*8), $K * \alpha = K * (\alpha \wedge \phi_1)$. We also have that for $\phi_2 = \bigwedge\{\beta \in K_c \mid \mathcal{M}' \models \beta$ and every state atom in $\beta$ belongs to $S^*\}$, $\phi_2 \in K * \alpha$ and thus $K * \alpha = K * (\alpha \wedge \phi_1 \wedge \phi_2)$.

Given that $\mathcal{M}'' <_{\mathcal{M}} \mathcal{M}'$, there is $\beta \in K_c$ such that $\mathcal{M}'' \models \beta$ and $\mathcal{M}' \not\models \beta$ (Proposition 4 (3)). As $\mathcal{M}'' \models \phi_1$ and, by Proposition 4 (1), $\mathcal{M}'' \models \phi_2$, we have that $(\alpha \wedge \phi_1 \wedge \phi_2) \wedge \beta$ is satisfiable, however this contradicts the postulate (K*R), since $K * (\alpha \wedge \phi_1 \wedge \phi_2) \cap K_c \subseteq K * ((\alpha \wedge \phi_1 \wedge \phi_2) \wedge \beta) \cap K_c$.

Therefore, for every $K * \alpha$ there is a $\mathcal{M}' \in \mathbb{M}(K, \alpha)$ such that $K * \alpha = \{\phi \in \mathcal{L} \mid \mathcal{M}' \models \phi\}$ and then we can define a selection function $\gamma$ such that $K * \alpha = \{\phi \in \mathcal{L} \mid \mathcal{M}' = \gamma(K, \alpha) \text{ and } \mathcal{M}' \models \phi\}$. □

From this theorem, we have an AGM-style characterization of the model repair operation in terms of the revision rationality postulates. To the best of our knowledge, this is the first complete characterization of model repair in terms of classical belief change theory. These postulates however seem hard to use in practical model repair applications. In the next section, we propose a new set of related postulates focused on the rationality of structural changes.

[5]In the case where $\alpha$ is not satisfiable, the equivalence follows directly from the statement, independent of the choice of the function

### 4.2 Rationality postulates for structural changes

One of the disadvantages of relating model repair to the classical belief revision theory is that the AGM paradigm is focused on the dynamics of sets of formulas. Then, we need to establish the relationship between models and formulas in order to define the correct characterizations between the two approaches.

Given the nature of the repair of models, it would be appropriate to characterize the rationality of a repair operation through specific postulates for this type of formalism. We thus propose the definition of postulates based on models and the changes that can transform them. Our intention is to capture in these postulates the principle of minimal structural changes.

**Definition 19** An *atomic modification* is a pair $\langle \mathcal{O}, \mathcal{D} \rangle$ that corresponds to a primitive update where $\mathcal{O} \in \{\text{PU1}, ..., \text{PU5}\}$ and

1. if $\mathcal{O} = \text{PU1}$ or $\mathcal{O} = \text{PU2}$, then $\mathcal{D} \in S \times S$, indicating the transition to be added or removed;
2. if $\mathcal{O} = \text{PU3}$, then $\mathcal{D} \in S \times AP$, indicating a change of a label of a state; or
3. if $\mathcal{O} = \text{PU4}$ or $\mathcal{O} = \text{PU5}$, then $\mathcal{D} \in S$, indicating the state to be added or removed.

In this sense, $\langle \text{PU1}, (s_0, s_2) \rangle$ is an atomic modification that represents an addition of a relation between two states, $s_0$ and $s_2$, and $\langle \text{PU3}, (s_1, q) \rangle$ an atomic modification represents a change of the label of a state $s_1$ in other for an atomic proposition $q$ to hold.

**Definition 20** Let $\mathcal{M} = \langle AP, S, s_0, R, L \rangle$ be a Kripke structure and $a$ an atomic modification. The application of $a$ to $\mathcal{M}$ results in a model $\mathcal{M}[a]$ such that:

1. For $a = \langle \text{PU1}, (s_i, s_j) \rangle$, if $s_i, s_j \in S$, then $\mathcal{M}[a] = \langle AP, S, s_0, R \cup \{(s_i, s_j)\}, L \rangle$;
2. For $a = \langle \text{PU2}, (s_i, s_j) \rangle$, if $(s_i, s_j) \in R$, then $\mathcal{M}[a] = \langle AP, S, s_0, R - \{(s_i, s_j)\}, L \rangle$;
3. For $a = \langle \text{PU3}, (s, p) \rangle$, if $s \notin L(p)$, then $\mathcal{M}[a] = \langle AP, S, s_0, R, L' \rangle$, where $L' = L$ except for $L'(p) = L(p) \cup \{s\}$;
4. For $a = \langle \text{PU3}, (s, p) \rangle$, if $s \in L(p)$, then $\mathcal{M}[a] = \langle AP, S, s_0, R, L' \rangle$, where $L' = L$ except for $L'(p) = L(p) - \{s\}$;
5. For $a = \langle \text{PU4}, (s) \rangle$, $\mathcal{M}[a] = \langle AP, S \cup \{s\}, s_0, R, L \rangle$;
6. For $a = \langle \text{PU5}, (s) \rangle$, if for all $(s_i, s_j) \in R$, $s \neq s_i$ and $s \neq s_j$, then $\mathcal{M}[a] = \langle AP, S - \{s\}, s_0, R, L \rangle$.
7. In all other cases, $\mathcal{M}[a] = \mathcal{M}$.

*Example 7* Let $\mathcal{M}$ be the model depicted in Fig. 2 and $a_1 = \langle \text{PU3}, (s_1, q) \rangle$, $a_2 = \langle \text{PU1}, (s_0, s_2) \rangle$ and $a_3 = \langle \text{PU5}, (s_0) \rangle$ atomic modifications. The application of $a_1$ in $\mathcal{M}$ produces the model $\mathcal{M}[a_1]$ depicted in Fig. 3a. The application of $a_2$ in $\mathcal{M}$ produces the model $\mathcal{M}[a_2]$ depicted in Fig. 3b. Finally, as $a_3 = \langle \text{PU5}, (s_0) \rangle$ does not fulfill the condition expressed in Definition 20, item 6, the application of $a_3$ in $\mathcal{M}$ has no effect and $\mathcal{M}[a_3] = \mathcal{M}$.

**Definition 21** Let $\mathcal{M}$ be a model, a *modification* $\Delta$ in $\mathcal{M}$ is a finite sequence of atomic modifications $\Delta = \langle a_1, a_2, ..., a_n \rangle$. We represent by $\mathcal{M}[\Delta]$ the model resulting from the application of $\Delta$ to $\mathcal{M}$, i.e., $\mathcal{M}[\Delta] = \mathcal{M}[a_1][a_2]...[a_n]$. In the case where $\Delta = \emptyset$ or that the application of $\Delta$ do no preserve Kripke models properties, as the serial transition relation over states, we have $\mathcal{M}[\Delta] = \mathcal{M}$.

A modification $\Delta$ represents a composition of atomic modifications which are applied to a model following a fixed order. Example 8 illustrates an application of a given modification in the model depicted in Fig. 2.

*Example 8* Let $\mathcal{M}$ be the model depicted in Fig. 2. The set of atomic modifications $\Delta = \{\langle \text{PU4}, s_3\rangle, \langle \text{PU3}, (s_3, p)\rangle, \langle \text{PU3}, (s_3, q)\rangle, \langle \text{PU2}, (s_0, s_2)\rangle, \langle \text{PU1}, (s_0, s_3)\rangle, \langle \text{PU1}, (s_3, s_0)\rangle, \langle \text{PU1}, (s_3, s_0)\rangle\}$ is a modification for $\mathcal{M}$ which generates the model in Fig. 7. Note that the atomic modification $\langle \text{PU2}, (s_0, s_2)\rangle$ has no structural effect on $\mathcal{M}$ and does not influence the result.

Let $\mathcal{M}$ be a model, $\alpha$ a temporal formula, and $\mathcal{R}\langle\mathcal{M}, \alpha\rangle$ a set of modifications given as a solution to the repair of $\mathcal{M}$ given $\alpha$. We propose the following postulates to define the expected rationality of $\mathcal{R}\langle\mathcal{M}, \alpha\rangle$.

$$\mathcal{R}\langle\mathcal{M}, \alpha\rangle = \emptyset \text{ if and only if } \models \neg\alpha \tag{R*1}$$

Postulate (R*1) states that the lack of repair may occur only in the case where $\alpha$ is unsatisfiable.

$$\text{For all } \Delta \in \mathcal{R}\langle\mathcal{M}, \alpha\rangle, \mathcal{M}[\Delta] \models \alpha \tag{R*2}$$

Postulate (R*2) is related to the *success* of a repair and states that every modification in $\mathcal{R}\langle\mathcal{M}, \alpha\rangle$ must lead to a model that satisfies $\alpha$

$$\text{If } \mathcal{M} \models \alpha, \text{ then } \mathcal{R}\langle\mathcal{M}, \alpha\rangle = \{\emptyset\} \tag{R*3}$$

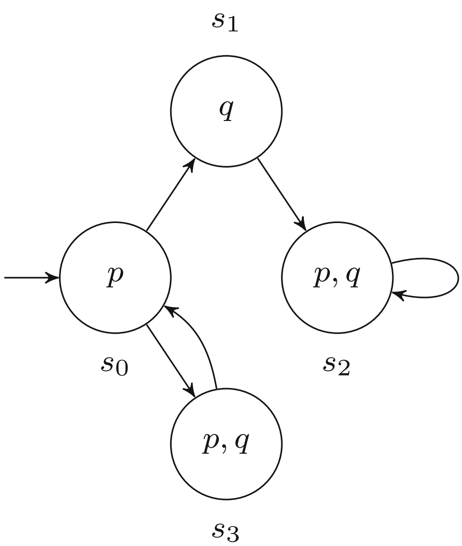
Postulate (R*3) deals with the *preservation* of models and states that in the case where $\mathcal{M}$ satisfies $\alpha$, no modification should be performed in $\mathcal{M}$.

$$\text{For all } \Delta \in \mathcal{R}\langle\mathcal{M}, \alpha\rangle, \text{ if } \Delta' \subset \Delta, \text{ then } \mathcal{M}[\Delta'] \not\models \alpha \tag{R*4}$$

Postulate (R*4) is related to the *relevance* of modifications and ensures that every individual solution contains only relevant atomic modifications in order to satisfy $\alpha$.

$$\begin{array}{l}\text{For all } \Delta \in \mathcal{R}\langle\mathcal{M}, \alpha\rangle, \text{ there is} \\ \Delta' \text{ such that } \mathcal{M}[\Delta][\Delta'] = \mathcal{M}\end{array} \tag{R*5}$$

**Fig. 7** Model after the application of a modification



Finally, Postulate (R*5) establishes that every modification in $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ must be reversible, so it would always be possible to recover the original model. Postulate (R*5) is a parallel to the AGM recovery postulate. In fact, it is trivially satisfied by operations PU1-PU5. However (R*1)–(R*5) were intended to be applied for any set of primitive operations and (R*5) postulates the reversibility of operations.

Theorem 6 states that the five proposed postulates indeed capture the rationality expected for a model repair operator. These postulates, however, have a focus on modifications in models, which makes them closer to the problem of repair than the postulates used in the previous section.

**Theorem 6** *Let $\mathcal{M}$ be a model and α a temporal formula. Then $\mathcal{M}' \in Update(\mathcal{M},\alpha)$ if and only if there is a set of modifications $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ that satisfies (R*1)–(R*5) and $\mathcal{M}' = \mathcal{M}[\Delta]$, for some $\Delta \in \mathcal{R}\langle\mathcal{M},\alpha\rangle$.*

*Proof* (⇒) If $Update(\mathcal{M},\alpha) = \emptyset$, the property is trivially satisfied. Suppose then that there are $\mathcal{M}' \in Update(\mathcal{M},\alpha)$ and $Diff(\mathcal{M},\mathcal{M}') = (\{t_1,t_2,...,t_j\}, \{\bar{t}_1,\bar{t}_2,...,\bar{t}_k\}, \{x_1,x_2,...,x_l\}, \{s_1,s_2,...,s_m\}, \{\bar{s}_1,\bar{s}_2,...,\bar{s}_n\})$. Let $d$ be a modification such that

$$\begin{aligned} d = \{&\langle \text{PU4}, s_1\rangle, ..., \langle \text{PU4}, s_m\rangle, \langle \text{PU1}, t_1\rangle, ..., \langle \text{PU1}, t_j\rangle,\\ &\langle \text{PU2}, \bar{t}_1\rangle, ..., \langle \text{PU2}, \bar{t}_k\rangle, \langle \text{PU3}, x_1\rangle, ..., \langle \text{PU3}, x_l\rangle,\\ &\langle \text{PU5}, \bar{s}_1\rangle, ..., \langle \text{PU5}, \bar{s}_j\rangle\}. \end{aligned}$$

We show that $\mathcal{R}\langle\mathcal{M},\alpha\rangle = \{d\}$ satisfies the property. By construction, $\mathcal{M}[d] = \mathcal{M}'$, so it remains to show that $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ satisfies the postulates (R*1)–(R*5).

The satisfaction of the postulate (R*1) follows trivially from the definition $\mathcal{R}\langle\mathcal{M},\alpha\rangle$. The satisfaction of the postulate (R*2) follows from the construction of $d$, since $\mathcal{M}[d] = \mathcal{M}'$ and, by definition, $\mathcal{M}' \models \alpha$. The postulate (R*3) is also satisfied by $\mathcal{R}\langle\mathcal{M},\alpha\rangle$, since $\mathcal{M} \models \alpha$, then $Update(\mathcal{M},\alpha) = \{\mathcal{M}\}$ and then $Diff(\mathcal{M},\mathcal{M}) = \{\emptyset,\emptyset,\emptyset,\emptyset,\emptyset\}$. Thus $d_{\mathcal{M},\alpha} = \emptyset$ and $\mathcal{R}\langle\mathcal{M},\alpha\rangle = \{\emptyset\}$. The operator $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ satisfies the postulate (R*4), since there is $d' \subset d$ e $\mathcal{M}[d'] \models \alpha$, then $\mathcal{M}[d'] <_{\mathcal{M}} \mathcal{M}'$, which contradicts the fact that $\mathcal{M}'$ belongs to the set $Update(\mathcal{M},\alpha)$. Finally, the operator $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ also satisfies the postulate (R*5), since we can define a modification

$$\begin{aligned} d^- = \{&\langle \text{PU4}, \bar{s}_1\rangle, ..., \langle \text{PU4}, \bar{s}_j\rangle.\langle \text{PU3}, x_1\rangle, ..., \langle \text{PU3}, x_l\rangle,\\ &\langle \text{PU1}, \bar{t}_1\rangle, ..., \langle \text{PU1}, \bar{t}_k\rangle, \langle \text{PU2}, t_1\rangle, ..., \langle \text{PU2}, t_j\rangle,\\ &\langle \text{PU5}, s_1\rangle, ..., \langle \text{PU5}, s_m\rangle\}. \end{aligned}$$

which undoes the modifications made by $d$, and thus $\mathcal{M}[d][d^-] = \mathcal{M}$.

Therefore, if $\mathcal{M}' \in Update(\mathcal{M},\alpha)$, then there is a repair operator $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ such that $\mathcal{M}' = \mathcal{M}[d]$ for some $d \in \mathcal{R}\langle\mathcal{M},\alpha\rangle$ and $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ satisfies (R*1)–(R*5).

(⇐) Suppose, for the purpose of contradiction, that $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ is a repair operator satisfying (R*1)–(R*5), that $d \in \mathcal{R}\langle\mathcal{M},\alpha\rangle$, but $\mathcal{M}[d] \notin Update(\mathcal{M},\alpha)$. From the postulate (R*2), $\mathcal{M}[d] \in Mod(\alpha)$, so there must be $\mathcal{M}' \in Mod(\alpha)$ such that $\mathcal{M}' \in Mod(\alpha)$ and $\mathcal{M}' <_{\mathcal{M}} \mathcal{M}[d]$. In this case $\mathcal{M}' \leq_{\mathcal{M}} \mathcal{M}[d]$ and $\mathcal{M}[d] \not\leq_{\mathcal{M}} \mathcal{M}'$, then there exists a $d'$ such that $\mathcal{M}[d'] = \mathcal{M}'$, $d' \subseteq d$, but $d \not\subseteq d'$. Since $\mathcal{M}[d'] \models \alpha$, we have a violation of the postulate (R*4). Therefore, it must be the case that $\mathcal{R}\langle\mathcal{M},\alpha\rangle$ is an operator that satisfies (R*1)–(R*5) and $d \in \mathcal{R}\langle\mathcal{M},\alpha\rangle$, thus $\mathcal{M}[d] \in Update(\mathcal{M},\alpha)$. □

Example 9 shows a repair operator for the model depicted in Fig. 2 and that satisfies postulates (R*1)–(R*5).

*Example 9* Let $\mathcal{M}$ be the model depicted in Fig. 2 and $\alpha = \text{EX}(p \wedge q)$ the property that triggers the repair. The repair $\mathcal{R}\langle\mathcal{M}, \alpha\rangle = \{\Delta_1, \Delta_2\}$, where $\Delta_1 = \{\langle \text{PU3}, (s_1, p)\rangle\}$ and $\Delta_2 = \{\langle \text{PU1}, (s_0, s_2)\rangle\}$, satisfies the postulates (R*1)–(R*5) and generates the models in Fig. 3a and b, both belonging to the set $\mathit{Update}(\mathcal{M}, \alpha)$.

Notice that for $\Delta$ in Example 8, $\mathcal{R}\langle\mathcal{M}, \alpha\rangle = \{\Delta\}$ does not satisfy the rationality postulates, since it violates (R*4). There is however a modification $\Delta'$ equal to $\Delta$ except for $\langle \text{PU2}, (s_0, s_2)\rangle$, such that $\mathcal{R}\langle\mathcal{M}, \alpha\rangle = \{\Delta'\}$ satisfies all postulates.

As a consequence of Theorems 5 and 6, we have the following corollary that relates operators of structural changes with operators on sets of formulas:

**Corollary 1** *For all sets $K$ defined by an internalized model $\mathcal{M}$ and a temporal formula $\alpha$, the revision operator $*$ for $K$ satisfies (K*1)–(K*8) and (K*R) if and only if there is a set of modifications $\mathcal{R}\langle\mathcal{M}, \alpha\rangle$ that satisfies (R*1)–(R*5) such that $K * \alpha = \{\varphi \in \mathcal{L} \mid \mathcal{M}[\Delta] \models \varphi\}$, for some $\Delta \in \mathcal{R}\langle\mathcal{M}, \alpha\rangle$.*

Corollary 1 presents a relation between the two proposed sets of postulates. By having a close correspondence to the structural change approach of model repair, postulates (R*1)–(R*5) could be seen as a set of *easy-to-use* rationality postulates for model repair operations that fully characterize the classical revision approach.

Postulates (R*1)–(R*5) then provide a rational definition of the model repair, in a way which is close to the intuitive operations over models, while maintaining the expected rationality of our first characterization.

## 5 Conclusions

We present in this work two AGM-style characterizations of model repair: one based on the classical AGM postulates, and the other based on structural modifications of models.

In the first characterization, we propose a new postulate, (K*R), to capture the relevance of structural modification in models based on the principle of *core sets*. We show that (K*R), combined with the classical AGM postulates (K*1)–(K*8), provides a full characterization of model repair functions.

In the second characterization, we propose a new set of postulates, with focus on structural changes in models. These postulates describe the expected rationality of performing modifications on models in order to make them satisfy a given formula. We argue that this set of postulates is more intuitive to be applied to model repair problems, remaining however fully compatible with the AGM theory.

In assuming models as representations of beliefs, our epistemic attitudes are complete, i.e., we will always believe in $\alpha$ or $\neg\alpha$, for any temporal formula $\alpha$. In this context of complete belief sets, belief revision and belief update produce equivalent results. Our characterizations are then also suitable for the problem of CTL model update addressed in [30].

Our approaches follow the AGM-style of characterization by providing a set of postulates to describe the expected rationality of a model repair. Works as [16, 30] follow the same approach, but both lack the complete characterization by a representation theorem. As of this work, we are not aware of any other complete characterization result for the model repair operation.

Although our approach focusses on CTL, it can be extended to other logic formalisms with Kripke-like semantics. We only use basic aspects of CTL to define the characterization, such as the next state modality, reachability and global validity. Other well-known formalism share these same aspects, such as Linear-time Temporal Logic [24], Propositional Dynamic Logic [12], and $\mu$-calculus [21], and similar results can be obtained.

In future work, we plan to investigate model change with non-complete beliefs. This can be dealt with either by using sets of models to represent beliefs, or by using partial structures, such as KMTSs [15]. In this context, revision and update functions could produce different results depending on what motivates the change. We aim to provide an AGM-style characterization of Zhang and Ding's [30] and Guerra and Wassermann's [16] operations for non-complete beliefs.

We also plan to provide implementations of model repair operations as in [28, 30] and to analyze the overall computational complexity of the problem. We intend to apply model repair to practical issues such as (semi-)automated repair of critical systems or in the development of intelligent agents with self-adaptive behaviors.

## References

1. Alchourron, C.E., Gärdenfors, P., Makinson, D.: On the logic of theory change: Partial meet contraction and revision functions. J. Symb. Log. **50**(2), 510–530 (1985)
2. Alrajeh, D., Kramer, J., Russo, A., Uchitel, S.: Automated support for diagnosis and repair. Commun. ACM **58**(2), 65–72 (2015). https://doi.org/10.1145/2658986
3. Bartocci, E., Grosu, R., Katsaros, P., Ramakrishnan, C.R., Smolka, S.A.: Model repair for probabilistic systems. In: Abdulla, P.A., Leino, K.R.M. (eds.) Tools and Algorithms for the Construction and Analysis of Systems: 17th International Conference, TACAS 2011, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2011, Saarbrücken, Germany, March 26?-April 3, 2011. Proceedings, pp. 326-340. Springer, Berlin (2011)
4. Bonakdarpour, B., Hajisheykhi, R., Kulkarni, S.S.: Knowledge-based automated repair of authentication protocols. In: Jones, C., Pihlajasaari, P., Sun, J. (eds.) FM 2014: Formal Methods: 19th International Symposium, Singapore, May 12–16, 2014. Proceedings, pp. 132–147. Springer International Publishing, Cham (2014)
5. Buccafurri, F., Eiter, T., Gottlob, G., Leone, N.: Enhancing model checking in verification by AI techniques. Artif. Intell. **112**(1-2), 57–104 (1999). https://doi.org/10.1016/S0004-3702(99)00039-9. http://linkinghub.elsevier.com/retrieve/pii/S0004370299000399
6. Burch, J., Clarke, E., McMillan, K., Dill, D., Hwang, L.: Symbolic model checking: 10^{20} states and beyond. Inf. Comput. **98**(2), 142–170 (1992). https://doi.org/10.1016/0890-5401(92)90017-A. http://www.sciencedirect.com/science/article/pii/089054019290017A
7. Carrillo, M., Rosenblueth, D.A.: CTL update of Kripke models through protections. Artif. Intell. **211**, 51–74 (2014). https://doi.org/10.1016/j.artint.2014.02.005. http://www.sciencedirect.com/science/article/pii/S0004370214000228
8. Chatzieleftheriou, G., Bonakdarpour, B., Smolka, S.A., Katsaros, P.: Abstract model repair. In: Goodloe, A., Person, S. (eds.) NASA Formal Methods, Lecture Notes in Computer Science, vol. 7226, pp. 341–355. Springer, Berlin (2012). https://doi.org/10.1007/978-3-642-28891-3_32
9. Clarke, E.M., Emerson, E.A.: Design and synthesis of synchronization skeletons using branching time temporal logic. In: Kozen, D. (ed.) Logics of Programs, Lecture Notes in Computer Science, vol. 131, pp. 52–71. Springer, Berlin (1982). https://doi.org/10.1007/BFb0025774
10. Clarke, E.M., Emerson, E.A., Sistla, A.P.: Automatic verification of finite-state concurrent systems using temporal logic specifications. ACM Trans. Program. Lang. Syst. (TOPLAS) **8**(2), 244–263 (1986). https://doi.org/10.1145/5397.5399
11. Fermé, E.L., Hansson, S.O.: AGM 25 years - twenty-five years of research in belief change. J. Philosophical Logic **40**(2), 295–331 (2011). https://doi.org/10.1007/s10992-011-9171-9
12. Fischer, M.J., Ladner, R.E.: Propositional dynamic logic of regular programs. J. Comput. Syst. Sci. **18**(2), 194–211 (1979). https://doi.org/10.1016/0022-0000(79)90046-1. http://www.sciencedirect.com/science/article/pii/0022000079900461

13. Flouris, G.: On belief change and ontology evolution. Ph.D. thesis, University of Crete (2006)
14. Gabbay, D., Rodrigues, O., Russo, A.: Belief revision in non-classical logics. The Review of Symbolic Logic **1**(03), 267–304 (2008)
15. Guerra, P.T., Andrade, A., Wassermann, R.: Toward the revision of CTL models through Kripke modal transition systems. In: Iyoda, J., de Moura, L.M. (eds.) Formal Methods: Foundations and Applications. 16th Brazilian Symposium on Formal Methods (SBMF 2013), Lecture Notes in Computer Science, vol. 8195, pp. 115–130. Springer, Berlin (2013)
16. Guerra, P.T., Wassermann, R.: Revision of CTL models. In: Kuri-Morales, A., Simari, G. (eds.) Advances in Artificial Intelligence – IBERAMIA 2010, LNCS, vol. 6433, pp. 153–162. Springer, Berlin (2010)
17. Guerra, P.T., Wassermann, R.: Two AGM-style characterizations of model repair. In: Proceedings of the 16th International Conference on Principles of Knowledge Representation and Reasoning (KR 2018), pp. 645–646 (2018)
18. Hansson, S.O.: A Textbook of Belief Dynamics. Theory Change and Database Updating. Kluwer, Boston (1999)
19. Jobstmann, B., Griesmayer, A., Bloem, R.: Program repair as a game. In: Proceedings of the 17th International Conference on Computer Aided Verification, CAV'05, pp. 226–238. Springer, Berlin (2005)
20. Katsuno, H., Mendelzon, A.O.: On the difference between updating a knowledge base and revising it. In: Gärdenfors, P. (ed.) Belief Revision, Cambridge Tracts in Theoretical Computer Science, vol. 29, pp. 183–203. Cambridge University Press (1992)
21. Kozen, D.: Results on the propositional $\mu$-calculus. Theor. Comput. Sci. **27**(3), 333–354 (1983). https://doi.org/10.1016/0304-3975(82)90125-6. http://www.sciencedirect.com/science/article/pii/0304397582901256
22. Parikh, R.: Beliefs, belief revision and splitting languages. In: Proceedings of Itallc-96 (1996)
23. Peppas, P.: Belief revision. In: Van Harmelen, F., Lifschitz, V., Porter, B.W. (eds.) Handbook of Knowledge Representation, pp. 317–359. Elsevier (2008). https://doi.org/10.1016/S1574-6526(07)03008-8
24. Pnueli, A.: The temporal logic of programs. In: Proceedings of the 18th Annual Symposium on Foundations of Computer Science, SFCS '77, pp. 46–57. IEEE Computer Society, Washington (1977). https://doi.org/10.1109/SFCS.1977.32
25. Reder, A., Egyed, A.: Computing repair trees for resolving inconsistencies in design models. In: 2012 Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering, pp. 220–229 (2012). https://doi.org/10.1145/2351676.2351707
26. Ribeiro, M.M.: Belief Revision in Non-classical Logics. Springer Briefs in Computer Science. Springer, Berlin (2013)
27. Seshia, S.A.: Sciduction: combining induction, deduction, and structure for verification and synthesis. In: Proceedings of the 49th Annual Design Automation Conference, DAC '12, pp. 356–365. ACM, New York (2012). https://doi.org/10.1145/2228360.2228425
28. Sousa, T.C., Wassermann, R.: Handling inconsistencies in CTL model-checking using belief revision Proceedings of the Brazilian Symposium on Formal Methods (2007)
29. Wassermann, R.: On AGM for non-classical logics. J. Philos. Log. **40**(2), 271–294 (2011). https://doi.org/10.1007/s10992-011-9178-2
30. Zhang, Y., Ding, Y.: CTL model update for system modifications. J. Artif. Intell. Res. **31**(1), 113–155 (2008)
31. Herzig, A.: Logics for belief base updating. In: Dubois, D., Prade, H. (eds.) Handbook of Defeasible Reasoning and Uncertainty Management, vol. Belief Cha, pp. 189–231. Kluwer Academic, Dordrecht (1998)
32. Clarke, E.M., Grumberg, O., Peled, D.A.: Model Checking. Springer, Berlin (1999)
33. Guerra, P.T., Wassermann, R.: On the uncomputability of partial meet contraction for linear-time temporal logic. South American Journal of Logic (to appear)
34. Hansson, S.O.: Belief contraction without recovery. Stud. Logica. **50**(2), 251–260 (1991). https://doi.org/10.1007/BF00370186