

Strong Next-Time Operators for Multiple-Valued μ -Calculus

Benet Devereux
Department of Computer Science,
University of Toronto,
Toronto, ON M5S 3G4, Canada.
Email: benet@cs.toronto.edu

April 20, 2002

1 Introduction

Multiple-valued logics [2] provide an interesting alternative to classical boolean logic for modeling and reasoning about systems. By allowing additional truth values, they support the explicit modeling of uncertainty and disagreement.

In order to do temporal reasoning over multiple-valued systems, we must extend a classical temporal logic to the multiple-valued case. For instance, the branching-time temporal logic CTL is a fragment of the modal μ -calculus [5]: it has conjunction, disjunction, negation, two next-time operators, weak (EX) and strong (AX) [4], and several additional temporal operators described as least or greatest fixpoints. For example, the property $\text{EF}\varphi$, “eventually φ may become true”, is the least fixpoint:

$$\text{EF}\varphi \triangleq \mu Z. (\varphi \vee (\text{EX}Z))$$

and $\text{AG}\varphi$, “ φ holds everywhere”, is the greatest fixpoint:

$$\text{AG}\varphi \triangleq \nu Z. (\varphi \wedge (\text{AX}Z))$$

The necessary conditions for finite-time convergence of fixpoint computations are the finiteness of the state-space, the finiteness of the set of state valuations, and the monotone increasing property of EX and AX.

The intuitive idea of the weak next-time operator $\text{EX}\varphi$ is “there exists a successor state where φ holds”. If S is the (finite) state-space, and R the system’s transition relation, then for any state s :

$$(\text{EX}\varphi)(s) \triangleq \exists s' \in S \cdot (R(s, s') \wedge \varphi(s'))$$

The sense of $\text{AX}\varphi$, however, involves causation: “if there is a transition to state s' , then φ holds there”, and is defined using implication:

$$(\text{AX}\varphi)(s) \triangleq \forall s' \in S \cdot (R(s, s') \rightarrow \varphi(s'))$$

In this work, we focus on possible multiple-valued generalizations of AX. We begin with a review of multiple-valued model-checking, described in greater detail elsewhere [3]. We choose to use finite sets of truth values, in order to guarantee finite-time convergence of fixpoints. Following that, we state the conditions for implication operators which both correspond to intuition, and allow a monotone increasing AX to be defined, which is needed to prove the existence of fixpoints. As an example, we choose three implications for a particular multiple-valued logic, and discuss the relationships between them, and with EX. Finally we show a structural condition on both multiple-valued models and implications that allows us to guarantee that AX is stronger than EX, while still permitting flexibility in modelling partial systems.

2 Background

Let \mathcal{L} be a finite set of logic values, partially ordered by truth degree. We use sets of truth values that have the structure of a *De Morgan algebra* [6] $(\mathcal{L}, \sqsubseteq, \sqcap, \sqcup, \neg)$: a distributive lattice with an antimonotonic and involute negation operator \neg : if $x \sqsubseteq y$, then $\neg y \sqsubseteq \neg x$, and $x = \neg\neg x$. The least element of the lattice is denoted \perp , and the highest element \top . Figure 1(a) shows the truth

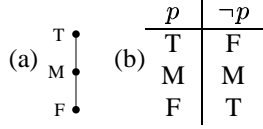


Figure 1: (a) Lattice for 3-valued logic, and (b) table for its De Morgan negation.

ordering for a 3-valued logic, and Figure 1(b) defines the De Morgan negation. Here $\top=T$ and $\perp=F$.

A λ Kripke structure [3] is a tuple (S, s_0, R, I, A, L) where:

1. S is a finite state space, s_0 an initial state;
2. $L = (\mathcal{L}, \sqsubseteq, \sqcap, \sqcup, \neg)$ is a De Morgan algebra;
3. $R : S \times S \rightarrow \mathcal{L}$ is a (valued) transition relation, assigning degrees of truth to transitions between states;
4. A is a finite set of state variables;
5. $I : S \times A \rightarrow \mathcal{L}$ is the interpretation function assigning values to variables in states.

Some examples of λ Kripke structures are shown in Figure 2. The form of R is constrained to ensure that states have successors. In classical Kripke structures, this totality condition is formalized as $\forall s \cdot \exists s' \cdot R(s, s')$. There are three possible ways to generalize this condition for λ Kripke structures:

$$\begin{aligned} \forall s \cdot \exists s' \cdot R(s, s') &= \top && \text{(strong totality)} \\ \forall s \cdot (\bigsqcup_{s' \in S} R(s, s')) &= \top && \text{(join totality)} \\ \forall s \cdot \exists s' \cdot R(s, s') &\neq \perp && \text{(weak totality)} \end{aligned}$$

All of these definitions collapse to ordinary totality in the classical case; and in the three-valued case, strong totality and join totality coincide. For example, the λ Kripke structures of Figure 2 satisfy weak totality, but not strong.

A temporal logic formula is interpreted in a given λ Kripke structure as a map $S \rightarrow \mathcal{L}$. For $p \in A$, and formulas φ and ψ , some of the connectives are defined as follows:

$$\begin{aligned} p(s) &\triangleq I(s, p) \\ (\varphi \wedge \psi)(s) &\triangleq \varphi(s) \sqcap \psi(s) \\ (\text{EX}\varphi)(s) &\triangleq \bigsqcup_{s' \in S} (R(s, s') \wedge \varphi(s)) \end{aligned}$$

For example, $\text{EX}\varphi$ in state s of Figure 2(b) is computed as $(R(s, t) \sqcap \varphi(t)) \sqcup (R(s, u) \sqcap \varphi(u)) = (M \sqcap M) \sqcup (M \sqcap F) = M \sqcup F = M$. The other connectives are defined similarly, and fixpoints have the standard definition.

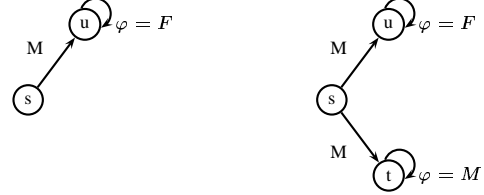


Figure 2: Example multiple-valued Kripke structures.

3 Multi-Valued Implications

A common approach to defining implication for multiple-valued logics is through residuation of a monoid operation on the logic values [1]. We take a simpler approach: defining the criteria for an implication, and then exploring the space of candidates for applicability.

We propose the following criteria for a useful implication operator \rightarrow , for all $x, y, z \in \mathcal{L}$:

$$\begin{aligned} (\perp \rightarrow x) &= \top && \text{(vacuity)} \\ \text{if } x \sqsubseteq y \text{ then } (z \rightarrow x) &\sqsubseteq (z \rightarrow y) && \text{(monotonicity)} \\ (\top \rightarrow x) &\sqsubseteq x && \text{(sub-identity)} \\ (\top \rightarrow \top) &= \top, (\perp \rightarrow \top) = \top && \text{(reduction to classical)} \\ (\perp \rightarrow \perp) &= \top, (\top \rightarrow \perp) = \perp \end{aligned}$$

The reason for the vacuity condition is as follows: suppose, for some state $s \in S$, $\text{AX}\varphi$ has a computed value. Now we adjoin some new state t to S , with no transition from s to t ($R(s, t) = \perp$). The value of $\text{AX}\varphi$ in s should not change!

Monotonicity guarantees that AX , as defined using \rightarrow , is also monotonic, which is required for the existence of a fixpoint. The sub-identity rule formalizes the intuition that the statement $\top \rightarrow x$ indicates that “under any conditions, x holds”, and it does not make sense for this expression to be any *more* true than the truth value of x . Finally, we want the implication to behave classically when only classical truth-values are used, since if we define a system using only \top and \perp as values, then analysis should yield the same results as classical model-checking.

Under these conditions, a 3-valued logic yields 33 possible implication operators, so we restrict our attention to three: *material implication*, defined as $x \rightarrow_M y = \neg x \sqcup y$; *Gödel implication*, where $x \rightarrow_G y = \top$ if $x \sqsubseteq y$, and y

\rightarrow_M	T	M	F	\rightarrow_G	T	M	F
T	T	M	F	T	T	M	F
M	T	M	M	M	T	T	F
F	T	T	T	F	T	T	T

\rightarrow_L	T	M	F
T	T	M	F
M	T	T	M
F	T	T	T

Figure 3: Material (\rightarrow_M), Gödel (\rightarrow_G), and Łukasiewicz (\rightarrow_L) implication tables for the 3-valued logic of Figure 1.

otherwise; and *Łukasiewicz implication*, which is defined on an n -valued, totally ordered logic by mapping truth values into the fractions k/n . The tables for these implications are shown in Figure 3.

4 Strong Next-time Operators

In this section, we define three different AX operators using multi-valued implications, and give some of their properties. We also discuss the ordering between these operators: for one operator to be stronger than another corresponds to the intuitive notion that it is a more conservative definition of “in all next states”.

For an implication operator \rightarrow , we define a strong next-time operator as follows:

$$(AX\varphi)(s) \triangleq \prod_{s' \in S} (R(s, s') \rightarrow \varphi(s'))$$

Using the three implication operators, we define three next-time operators, AX_M , AX_G , and AX_L . Since the monotonicity rule holds for all three implications, the AX operators are monotonic as well:

Proposition 1 *If $\varphi \sqsubseteq \psi$, then $AX_A\varphi \sqsubseteq AX_A\psi$, for $A \in \{M, G, L\}$.*

Any ordering between implication operations is inherited by the AX operators defined using them:

Proposition 2 *For any $\rightarrow_A, \rightarrow_B, AX_A, AX_B$, with $A, B \in \{M, G, L\}$, and any formula φ :*

if $\forall x, y \cdot (x \rightarrow_A y) \sqsubseteq (x \rightarrow_B y)$ then $AX_A\varphi \sqsubseteq AX_B\varphi$

By inspection, it is easy to see that the following relationship holds:

$$AX_M\varphi \sqcup AX_G\varphi = AX_L\varphi \quad (1)$$

In general, for n -valued logics, Equation 1 does *not* hold; a simple counterexample in the 5-valued totally-ordered logic can be found.

5 Relationships Between Next-time Operators

We are interested in how AX relates to EX, and also to its dual $\neg EX \neg$. Under strong totality, $AX\varphi \sqsubseteq EX\varphi$; under weak totality, this ordering does not necessarily hold. In the 3-valued case, join totality is equivalent to strong totality, but whether join totality guarantees the correct ordering remains an open question in the general case.

We state the result for strong totality more formally:

Proposition 3 *For all states s , if strong totality holds, then $AX\varphi \sqsubseteq EX\varphi$.*

Proof:

By strong totality, for any state s , there is $s' \in S$ such that $R(s, s') = T$. Then:

$$(AX\varphi)(s) \sqsubseteq (R(s, s') \rightarrow \varphi(s')) \sqsubseteq \varphi(s')$$

by sub-identity. In turn:

$$\varphi(s') = R(s, s') \sqcap \varphi(s') \sqsubseteq EX\varphi$$

and thus the desired property holds: □

Looking at the proof of Proposition 3, we can see that a weaker condition is possible. In order to define this in a simple manner, we need to state that if our next-time operators are correctly ordered in all propositional variables p and their negations $\neg p$, then they are also correctly ordered for any temporal logic formula:

Lemma 1 *Let EX and AX be monotonic operators. If, for all $p \in A$, $AXp \sqsubseteq EXp$, and $AX\neg p \sqsubseteq EX\neg p$, then:*

$$AX\varphi \sqsubseteq EX\varphi$$

for all temporal logic formulas φ .

We can also define a weaker condition ensuring $AX\varphi \sqsubseteq EX\varphi$. We call this condition *sufficient* totality, and it is defined relative to the AX operator being used.

Theorem 1 *If for all $p \in A$, and $s \in S$:*

$$\exists t, u \in S \cdot R(s, t) \rightarrow p(t) \sqsubseteq R(s, u) \sqcap p(u)$$

with $t \neq u$, and

$$\exists t, u \in S \cdot R(s, t) \rightarrow \neg p(t) \sqsubseteq R(s, u) \sqcap \neg p(u)$$

then $AX\varphi \sqsubseteq EX\varphi$ in all states.

Proof:

Direct, and by Lemma 1. □

In Figure 2(a), we have a λ Kripke structure which is only weakly total. It is sufficiently total for AX_G , but not for either of the other strong next-times: here $EX\varphi = F$ and $AX_M\varphi = AX_L\varphi = M$. In this case, our analysis seems to say that, on the one hand, there is no transition to a state where φ holds; but, on the other hand, maybe φ holds in any next state! By contrast, the structure in Figure 2(b) is sufficiently total for all three AX operators. In this case, $AX_M\varphi = AX_L\varphi = EX\varphi = M$, and $AX_G\varphi = F$.

We conclude with observations about the connection between $\neg EX\neg$ and AX operators. By definition, $AX_M\varphi = \neg EX\neg\varphi$, and thus:

Proposition 4 *$\neg EX\neg$ is stronger than AX_L :*

$$\neg EX\neg\varphi \sqsubseteq AX_L\varphi$$

and incomparable with AX_G .

We might say that AX_L is the most “optimistic” strong next-time operator.

6 Summary and Future Work

This work reports on our first investigations of the space of strong next-time operators for multiple-valued temporal logic. We have stated axioms for implications that can be used to define an AX operator, and discussed the relationships among candidate operations and their relationship to EX. Finally, we have given a weaker totality condition for λ Kripke structures which is parameterized in the choice of AX.

In the future, we plan to generalize this work to any (finite) multiple-valued logic, and discover more general relationships between classes of multiple-valued implications, and thus between the AX operators they define. As well, we hope to find applications in verification for the different AX operators, and incorporate them into our verification framework [3].

7 Acknowledgements

We would like to thank Marsha Chechik for helping improve the presentation of results in this paper, and also Wendy MacCaull and Arie Gurfinkel for advice and discussions.

References

- [1] T.S. Blyth and M.F. Janowitz. *Residuation Theory*. Pergamon Press, Oxford, 1972.
- [2] L. Bolc and P. Borowik. *Many-Valued Logics*. Springer-Verlag, 1992.
- [3] M. Chechik, B. Devereux, S. Easterbrook, and A. Gurfinkel. “Multi-Valued Symbolic Model-Checking”. CSRG Technical Report 448, Department of Computer Science, University of Toronto, 1997.
- [4] E. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 1999.
- [5] D. Kozen. “Results on the Propositional Mu-Calculus”. *Theoretical Computer Science*, pages 333–354, Dec. 1983.
- [6] H. Rasiowa. *An Algebraic Approach to Non-Classical Logics*. Studies in Logic and the Foundations of Mathematics. North-Holland, 1978.