20 Sep 1993

Constructing an Interval Temporal Logic for Real-Time Systems

Grace Tsai

Matt Insall
Missouri University of Science and Technology, insall@mst.edu

Bruce M. McMillin
Missouri University of Science and Technology, ff@mst.edu

CONSTRUCTING AN INTERVAL TEMPORAL LOGIC FOR REAL-TIME SYSTEMS†

Grace Tsai, Matt Insall and Bruce McMillin

CSC-93-025

September 20, 1993

† This work is supported by the research board of University of Missouri-Rolla, the National Science Foundation under Grant Numbers MSS-9216479 and CDA-9222827, and the Air Force Office of Scientific Research under contract number F49620-92-J-0546.

Grace Tsai and Bruce McMillin are with the Department of Computer Science at the University of Missouri-Rolla, Rolla, MO 65401.

Matt Insall is with the Department of Mathematics and Statistics at the University of Missouri-Rolla, Rolla, MO 65401.

INTRODUCTION

A real-time system is one that involves control of one or more physical devices with essential timing requirements. Examples of these systems are command and control systems, process control systems, flight control systems, and the space shuttle avionics systems. The characteristics of these systems are that severe consequences will occur if the logical and physical timing specifications of the systems are not met.

Formal specification and verification are among the techniques to achieve reliable software for real-time systems, in which testing may be impossible or too dangerous to perform. This paper presents a modal logic, *Interval Temporal Logic*, built upon a classical predicate logic L. In this logic system, we consider formulas that can be used to reason about timing properties of systems, in particular, *responsiveness assertions.* A responsiveness assertion describes constraints that a program must satisfy within an interval. Thus, it can be utilized to characterize behaviors of life-critical systems.

We assume that a program P can be identified with a *theory*, Σ_P, a collection of formulas characterizing sequences of states of P with arbitrary initial states. In the following, we describe syntax and semantics of the logic, present a proof rule for responsiveness assertions, and show soundness and relative completeness of responsiveness assertions that we consider. There are other approaches to build temporal logics for real-time systems, which are included in bibiography.

2. Interval Temporal Logic

Syntax

We describe a modal language ITL built upon a classical predicate logic L as follows. The symbols of ITL are those of classical predicate logic along with U, E, F, X, X^n, and $\hat{X}$. Let Φ be the smallest set of words over the symbols of ITL such that

- If $p \in L$ then $p \in \Phi$.
- If p, $q \in \Phi$, then $p \vee q$, $\neg p \in \Phi$.
- If p, $q \in \Phi$, then $p\mathrm{U}q$, $\mathrm{E}p$, $\mathrm{F}p$, $\mathrm{X}p$, $\mathrm{X}^n p$, $\hat{\mathrm{X}}p \in \Phi$.
- If p, q, $r \in \Phi$, then $[p]r$, $[p, q]r \in \Phi$.

We call a member of Φ a *formula*, and a formula of the language L a *state formula*. A *state* is a model of the given first order logic L.

Definition 2.1: Let $\sigma(i)$ denote the i^{th} state of a sequence of states, σ. We call i a *time index* of σ.

Definition 2.2: Let $|\sigma|$ denote the length (possibly infinite) of a sequence of states, σ. A sequence of states, $\xi = (\xi(0), \ldots, \xi(|\xi|))$ *refines* a given sequence of states, $\sigma = (\sigma(0), \ldots, \sigma(|\sigma|))$, iff

$$(\exists j \in [0, |\sigma|])((\sigma(j), \sigma(j+1), \cdots \sigma(j+|\xi|)) = \xi).$$

We let $R(\sigma) = \{\xi | \xi \leq \sigma\}$.

Semantics

In this logic system, formulas are quantified by fundamental operators E, F, P, U, X, $\hat{\mathrm{X}}$, and X^n, which are defined in the following semantics.

Definition 2.3: A *structure* of the language ITL is a sequence of states.

Definition 2.4: Let σ be a structure, let i be an integer with $0 \leq i < |\sigma|$, let f be a state formula, and let p, q, ϕ, ψ be any formulas. Then, we write

$(\sigma, i) \models f$	if $\sigma(i) \models f$,
$(\sigma, i) \models p \vee q$	if $(\sigma, i) \models p$ or $(\sigma, i) \models q$,
$(\sigma, i) \models \neg p$	if not $(\sigma, i) \models p$,
$(\sigma, i) \models pUq$	if there exists $i \leq j < |\sigma|$, such that both $(\sigma, j) \models q$ and for every k such that $i \leq k < j$, $(\sigma, k) \models p$,
$(\sigma, i) \models \mathrm{P}\phi$	if there exists $j \leq i$ such that $(\sigma, j) \models \phi$,
$(\sigma, i) \models \mathrm{X}\phi$	if $|\sigma| \geq$ i+1 and $(\sigma, i+1) \models \phi$,
$(\sigma, i) \models \mathrm{X}^n\phi$	if $(\sigma, i+n) \models \phi$,
$(\sigma, i) \models \hat{\mathrm{X}}\phi$	if $(\exists n \geq i)((\sigma, i) \models \mathrm{X}^n\phi)$,
$(\sigma, i) \models \mathrm{F}\phi$	if $\exists (k \geq i)\ (\forall j \geq k)\ (\sigma, j) \models \phi$,
$(\sigma, i) \models [p]\phi$	if $(\sigma, i) \models p$ implies $(\sigma, i) \models \phi$,
$(\sigma, i) \models [p, q]\phi$	if for every $\xi \in R(\sigma)$ such that $(\xi, 0) \models p$ and $(\xi, |\xi|) \models q$, if there exists $k_i \in \{0, 1, \ldots, |\xi|\})(\xi(k_i) = \sigma(i))$, then $(\xi, k_i) \models \phi$,
$\sigma \models \phi$	if for all $i \in \{0, \ldots, |\sigma|\}$, $(\sigma, i) \models \phi$.

In each case, the symbol $\models$ is read "satisfies". We abbreviate $(\neg\phi \wedge \hat{\mathrm{X}}\phi)$ by $\mathrm{E}\phi$. The following proposition shows that if a model σ satisfies $[p, q]\mathrm{EF}\phi$, then essentially ϕ is satisfied at the times when q is satisfied.

Proposition 1: Assume that $(\sigma, i) \models [p, q]\mathrm{EF}\phi$. Then, for all $\xi \in R(\sigma)$ such that $(\xi, 0) \models p$, $(\xi, |\xi|) \models q$, and there exists an index k_i, $\xi(k_i) = \sigma(i)$, we have $(\xi, |\xi|) \models \phi$.

Proof: Since $(\sigma, i) \models [p, q]\mathrm{EF}\phi$, it follows that for every $\xi \in R(\sigma)$ such that $(\xi, 0) \models p$, $(\xi, |\xi|) \models q$, and there exists $k_l \in \{0, 1, \ldots, |\xi|\})(\xi(k_l) = \sigma(i))$, we have $(\xi, k_l) \models \mathrm{EF}\phi$ This means that for every such subsequence ξ, there exists an $l > k_l$ such that $(\xi, l) \models \mathrm{F}\phi$. Equivalently, for every such subsequence ξ, there exists an $m \geq l$ such that $\forall (n \geq m)$, we have $(\xi, n) \models \phi$, in particular, $(\xi, |\xi|) \models \phi$.□

Definition 2.5: For a structure σ, an *interval* $[\phi, \psi]_\sigma$, bounded by formulas ϕ and ψ, is given by $[\phi, \psi]_\sigma = \{\xi \in R(\sigma) \mid (\xi, 0) \models \phi, (\xi, |\xi|) \models \psi\}$. The symbol $\models$ denotes the satisfaction relation of ITL.

Definition 2.6: If Σ is a set of formulas of ITL, and σ is a structure of ITL such that for all $\phi \in \Sigma$, $\sigma \models \phi$, then we say that σ is a *model* of Σ.

Definition 2.7: A set of formulas of ITL is said to be *consistent* if it has a model. We call a set of consistent formulas a *theory*.

Definition 2.8: A *responsiveness assertion* is a formula of the form $([p]\phi \rightarrow [p, q]\mathrm{EF}\psi)$, where p, q, ϕ, and ψ are formulas of ITL.

A responsiveness assertion $([p]\phi \rightarrow [p, q]\mathrm{EF}\psi)$ is satisfied by a structure σ, iff the following holds: if ϕ holds where p holds, then for every q following p, ψ holds where q holds. The following Progress Rule can be applied to reason about responsiveness properties.

Progress Rule: Let $p, q, r, \phi_0, \phi_1, \phi_2$ be formulas. Then, we may derive $([p]\phi_0 \rightarrow [p, r]\mathrm{EF}\phi_2)$ from $([p]\phi_0 \rightarrow [p, q]\mathrm{EF}\phi_1)$, $([q]\phi_1 \rightarrow [q, r]\mathrm{EF}\phi_2)$, and $[p, r]\mathrm{E}q$.

Notice that the premise $[p, r]\mathrm{E}q$ is necessary as follows. Consider a structure σ with an index i, such that $\sigma(i) \models (p \wedge \phi_0)$, $\sigma(i+1) \models (r \wedge \neg\phi_2)$, $\sigma(i+2) \models (q \wedge \phi_1)$, $\sigma(i+3) \models (r \wedge \phi_2)$, and for all $j \notin \{i, i+1, i+2, i+3\}$, $\sigma(j) \not\models (p \wedge \phi_0)$, $\sigma(j) \not\models (r \wedge \neg\phi_2)$, $\sigma(j) \not\models (q \wedge \phi_1)$, $\sigma(j) \not\models (r \wedge \phi_2)$. Clearly, $\sigma \models [p]\phi_0 \rightarrow [p, q]\mathrm{EF}\phi_1$ $\sigma \models [q]\phi_1 \rightarrow [q, r]\mathrm{EF}\phi_2$. However, $\sigma \not\models [p]\phi_0 \rightarrow [p, r]\mathrm{EF}\phi_2$.

We take as an axiom system of ITL the axioms of L.

Definition 2.9: A *proof* of a formula ϕ is a finite sequence, say $\phi_1, \ldots, \phi_n$, of formulas such that $\phi = \phi_n$ and for each $i \leq n$, either ϕ_i is an axiom, or for some $j < i$, ϕ_i is an immediate consequence of ϕ_j and ϕ_k according to modus ponens or the Progress Rule. A formula ϕ is said to be provable if there is a proof of it. We denote this by $\vdash \phi$.

The following definition is needed for the proofs of soundness and relative completeness of the Progress Rule.

Definition 2.10: If Σ is a collection of formulas, then $\Sigma \models \phi$ (read "ϕ is a *consequence of* Σ") means every model of Σ satisfies ϕ.

Theorem 1 (Soundness): The Progress Rule is sound.

Proof: Assume that all the premises hold, i.e.,

(1) $\Sigma \models [p]\phi_0 \rightarrow [p,q]\mathrm{EF}\phi_1$,

(2) $\Sigma \models [q]\phi_1 \rightarrow [q,r]\mathrm{EF}\phi_2$, and

(3) $\Sigma \models [p,r]\mathrm{E}q$.

Let σ be an arbitrary model of Σ,i.e., $\sigma \models \Sigma$. Then,

(4) for all i, $(\sigma,i) \models [p]\phi_0 \rightarrow [p,q]\mathrm{EF}\phi_1$,

(5) for all i, $(\sigma,i) \models [q]\phi_1 \rightarrow [q,r]\mathrm{EF}\phi_2$, and

(6) for all i, $(\sigma,i) \models [p,r]\mathrm{E}q$.

Fix $i \geq 0$ and $l \geq i$ such that $(\sigma,i) \models [p]\phi_0$ and $(\sigma,l) \models r$. By (4), since $(\sigma,i) \models [p]\phi_0$, we get $(\sigma,i) \models [p,q]\mathrm{EF}\phi_1$. From (6) there exists a k, $i < k \leq l$, such that q holds, i.e., $(\sigma,k) \models q$. From Proposition 1, $(\sigma,k) \models \phi_1$.

By (5), since $(\sigma,k) \models [q]\phi_1$, it follows that $(\sigma,k) \models [q,r]\mathrm{EF}\phi_2$. Again, using Proposition 1, we have $(\sigma,l) \models \phi_2$. Hence $(\sigma,l) \models [r]\phi_2$, and so $(\sigma,i) \models [p,r]\mathrm{EF}\phi_2$. Thus, $(\sigma,i) \models [p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2$.

Hence, for all i, $(\sigma,i) \models [p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2$. Thus $\sigma \models [p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2$. So $\Sigma \models [p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2$, as desired.□

Definition 2.11: An *ITL algebra* is a tuple $\mathbf{B} = (B, \wedge, \vee, \neg, U, X, ([\_,\_]\_), P, \hat{X}, F, ([\_]\_), 0, 1)$ where $(B, \wedge, \vee, \neg, 0, 1)$ is a boolean algebra and we have that

(1) U and $[\_]\_$ are binary operations on B,

(2)$[\_,\_]\_$ is a ternary operation on B, and

(3) X, P, $\hat{X}$ and F are unary operations on B, such that

(a) for all $b \in B$, $(Xb) \wedge (\hat{X}b) = Xb$.

(b) for all $b, c, x \in B$, $(\neg b) \wedge [b,c]x = \neg b$.

(c) for all $b, x \in B$, $(\neg b) \wedge [b]x = \neg b$.

(d) for all $b, x \in B$, $(XUb) \wedge (\hat{X}b \wedge x) = XUb$.

(e) for all $x \in B$, $(\neg[\hat{X}(\neg x)]) \wedge (x \wedge Xx) = x \wedge Xx$.

(f) for all $b, c, x \in B$, $(b \wedge [b,c]x) \vee (\neg c \vee x) = \neg c \vee x$.

(g) for all $b, c, x \in B$, $((b \wedge \hat{X}c) \wedge [b,c]x) \vee (\hat{X}x) = \hat{X}x$.

An ITL algebra can be used to study the relationship between syntax and semantics for the language ITL in the way that the Lindenbaum algebra is used to relate syntax and semantics for classical predicate logic. The structure we define for an ITL algebra is that of boolean algebra with operators. Boolean algebras with operators have been studied by Goldblatt,... We here describe what is necessary to prove relative completeness of our logic system.

Definition 2.12: Let $\mathbf{B} = (B, \wedge, \vee, \neg, U, X, ([\_,\_]\_), P, \hat{X}, F, [\_]\_, 0, 1)$ be an ITL algebra. A *congruence* on **B** is an equivalence relation ~ on **B** such that

(a) $(a_1 \wedge b_1) \sim (a_2 \wedge b_2)$ if $a_1 \sim a_2$ and $b_1 \sim b_2$.

(b) $(a_1 \vee b_1) \sim (a_2 \vee b_2)$ if $a_1 \sim a_2$ and $b_1 \sim b_2$.

(c) $(\neg a_1) \sim (\neg a_2)$ if $a_1 \sim a_2$.

(d) $(a_1 \mathrm{U} b_1) \sim (a_2 \mathrm{U} b_2)$ if $a_1 \sim a_2$ and $b_1 \sim b_2$.

(e) $(\mathrm{X} a_1) \sim (\mathrm{X} a_2)$ if $a_1 \sim a_2$.

(f) $([a_1, b_1]c_1) \sim ([a_2, b_2]c_2)$ if $a_1 \sim a_2$, $b_1 \sim b_2$ and $c_1 \sim c_2$.

(g) $(\mathrm{P} a_1) \sim (\mathrm{P} a_2)$ if $a_1 \sim a_2$.

(h) $(\hat{X} a_1) \sim (\hat{X} a_2)$ if $a_1 \sim a_2$.

(i) $(F a_1) \sim (F a_2)$ if $a_1 \sim a_2$.

(j) $([a_1]b_1) \sim ([a_2]b_2)$ if $a_1 \sim a_2$ and $b_1 \sim b_2$.

The definition of congruence agrees with that found in texts on universal algebra, and since for any ITL algebra $\mathbf{B} = (B, \wedge, \vee, \neg, U, X, ([\_,\_]\_), P, \hat{X}, F, [\_]\_, 0, 1)$, a congruence on **B** is also (clearly) a congruence on the underlying boolean algebra $(B, \wedge, \vee, \neg, 0, 1)$, it corresponds to a filter $F_{\sim}$ on this boolean algebra.

Assume that L is countable, and let $[\Pi]$ denote the collection of infima in $(B, \wedge, \vee, \neg, 0, 1)$ described by $((\forall v_k)\phi)_{\equiv} = inf\{(\phi(v_k/v_p))_{\equiv}: p \in \omega\}$. We say that an ultrafilter u on $(B, \wedge, \vee, \neg, 0, 1)$ preserves the meets $[\Pi]$ if $(((\forall v_k)\phi)_{\equiv}) \in u \Leftrightarrow \{(\phi(v_k/v_p))_{\equiv}: p \in \omega\} \subseteq u$.

Definition 2.13: Let ~ be a congruence on an ITL algebra $\mathbf{B} = (B, \wedge, \vee, \neg, U, X, ([\_,\_]\_), P, \hat{X}, F, [\_]\_, 0, 1)$, and let $F_{\sim}$ be the filter on $(B, \wedge, \vee, \neg, 0, 1)$, which is associated with ~. We will say that the congruence ~ is a *strong congruence* on **B** provided that $F_{\sim}$ is an ultrafilter which preserves the meets $[\Pi]$.

Definition 2.14: We write $\phi \equiv \psi$ iff $\vdash \phi \rightarrow \psi$ and $\vdash \psi \rightarrow \phi$, and for each formula ϕ, we let $\phi_{\equiv} = \{\psi \in ITL \mid \phi \equiv \psi\}$.

- $(\phi_{\equiv}) \wedge (\psi_{\equiv}) = (\phi \wedge \psi)_{\equiv}$.
- $(\phi_{\equiv}) \vee (\psi_{\equiv}) = (\phi \vee \psi)_{\equiv}$.
- $\neg(\phi_{\equiv}) = (\neg\phi)_{\equiv}$
- $(\phi_{\equiv}) \mathrm{U} (\psi_{\equiv}) = (\phi \mathrm{U} \psi)_{\equiv}$.

- $[(p_\equiv),(q_\equiv)](\phi_\equiv) = ([p,q]\phi)_\equiv$
- $\mathrm{P}(\phi_\equiv) = (\mathrm{P}\phi)_\equiv$
- $\hat{\mathrm{X}}(\phi_\equiv) = (\hat{\mathrm{X}}\phi)_\equiv$
- $\mathrm{F}(\phi_\equiv) = (\mathrm{F}\phi)_\equiv$
- $[(p_\equiv)](\phi_\equiv) = ([p]\phi)_\equiv$.

Observation: $\Phi/\equiv$ is an ITL algebra.

Theorem 2 (Relative Completeness): Let Σ be a theory of ITL and let $([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2)$ be a responsiveness assertion. Suppose $\Sigma \models ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2)$, i.e., suppose every model σ of Σ satisfies $[p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2$. Then $\Sigma \vdash ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2)$.

Proof: We show this only in the case that Σ consists of state formulas and the formulas p, ϕ_0, r and ϕ_2 are state formulas. Without loss of generality, we may assume that Σ is finite, say $\Sigma = \{\gamma_0, \ldots, \gamma_n\}$. We will show that $\vdash(\wedge\Sigma \rightarrow [p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2))$ where $\wedge\Sigma = \gamma_0 \wedge \cdots \wedge \gamma_{n-1}$. We proceed as in [BeSl71].

Suppose, on the contrary, that the formula $\phi = (\wedge\Sigma \rightarrow ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2))$ is unprovable. We know that not $\vdash\phi$ i.e., $(\phi_\equiv) \neq 1$. So, the assumption that ϕ is unprovable implies that $\neg(\wedge\Sigma)_\equiv \vee \neg([p]\phi_0)_\equiv \vee ([p,r]\mathrm{EF}\phi_2)_\equiv \neq 1$. So, (1) $(\neg(\wedge\Sigma)_\equiv \vee \neg([p]\phi_0)_\equiv) \neq 1$, and (2) $(\neg(\wedge\Sigma)_\equiv \vee ([p,r]\mathrm{EF}\phi_2)_\equiv \neq 1$.

We let $\sim_0, \sim_1$ be strong congruences on B_{ITL}, such that $\wedge\Sigma \sim_0 \neg p \sim_0 \neg\phi_0 \sim_0 1$ and $\wedge\Sigma \sim_1 r \sim_1 \neg\phi_2 \sim_1 1$.

Define a relation $\approx$ on the set V of variables of L by $v_i \approx v_j$ iff $(v_i = v_j)_\equiv \sim_0 1$. For $v \in V$, let $v_\approx = \{v' \in V | v' \approx V\}$, and then let $V/_\approx = \{v_\approx | v \in V\}$. For each n-ary predicate symbol P of L, define a relation R_P on $V/_\approx$ by $R_P^{(0)} = \{((v_1)_\approx, \ldots, (v_n)_\approx) \in (V/_\approx)^n | (P(v_1, \ldots, v_n)) \sim_0 1\}$. Let $\sigma_0 = (V/_\approx, (R_P^{(0)})_{P \in P_L})$, where P_L is the set of all predicates of L.

Define a relation $\approx$ on the set V of variables of L by $v_i \approx v_j$ iff $(v_i = v_j)_\equiv \sim_1 1$. For $v \in V$, let $v_\approx = \{v' \in V | v' \approx V\}$, and let $V/_\approx = \{v_\approx | v \in V\}$. For each n-ary predicate symbol P of L, define a relation R_P on $V/_\approx$ by $R_P^{(0)} = \{((v_1)_\approx, \ldots, (v_n)_\approx) \in (V/_\approx)^n | (P(v_1, \ldots, v_n)) \sim_1 1\}$. Let $\sigma_1 = (V/_\approx, (R_P^{(1)})_{P \in P_L})$, where P_L is the set of all predicates of L.

Let $\sigma = (\sigma_0, \sigma_1)$. Then $(\sigma, 0) \models (\wedge\Sigma) \wedge \neg p \wedge \neg\phi_0$, $(\sigma, 1) \models (\wedge\Sigma) \wedge r \wedge \neg\phi_2$, and $\sigma \not\models (\wedge\Sigma) \rightarrow ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2$. Thus, σ is a model of Σ which fails to satisfy ϕ, contrary to our assumption.□

As an example, we present the construction of a structure σ which fails to satisfy a more complex formula which is assumed unprovable. Let Σ and ϕ be as follows.

$\Sigma = \{[a,b]c\}$, where a, b, c are state formulas.

$\phi = [a,b]c \rightarrow ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2)$.

$p = \mathrm{X}q$, where q is a state formula.

$\phi_0 = \mathrm{F}q$, where d is a state formula.

$r = [e,f]g$, where e, f, g are state formulas.

$\phi_2 = h\mathrm{U}k$, where h, k are state formulas.

Now, we construct a model σ of Σ which fails to satisfy ϕ as follows. Suppose that the formula $\phi = (\wedge\Sigma \rightarrow ([a,b]c \rightarrow ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2))$ is unprovable. So, the assumption that ϕ is unprovable implies that $\neg(\wedge\Sigma)_\equiv \vee \neg([a,b]c)_\equiv \vee \neg([p]\phi_0)_\equiv \vee ([p,r]\mathrm{EF}\phi_2)_\equiv \neq 1$. So, (1) $(\neg(\wedge\Sigma)_\equiv \vee \neg([a,b]c)_\equiv) \neq 1$, (2) $(\neg(\wedge\Sigma)_\equiv \vee \neg([p]\phi_0)_\equiv) \neq 1$, and (3) $(\neg(\wedge\Sigma)_\equiv \vee ([p,r]\mathrm{EF}\phi_2)_\equiv \neq 1$.

We let $\sim_0, \sim_1, \sim_2$ be strong congruences on B_{ITL}, such that $\wedge\Sigma \sim_0 p \sim_0 \neg e \sim_0 1$, $\wedge\Sigma \sim_1 q \sim_1 \neg e \sim_1 1$, and $\wedge\Sigma \sim_2 r \sim_2 \neg\phi_2 \sim_2 \neg k \sim_2 \neg e \sim_2 1$. As in the above argument, we can construct $\sigma_0, \sigma_1, \sigma_2$ as follows: let $\sigma = (\sigma_0, \sigma_1, \sigma_2)$, $\sigma_0 \models p \wedge \neg e$, $\sigma_1 \models q \wedge \neg e$, $\sigma_2 \models r \wedge \neg\phi_2 \wedge \neg k \wedge \neg e$. So, $\sigma \not\models \wedge\Sigma \rightarrow ([a,b]c \rightarrow ([p]\phi_0 \rightarrow [p,r]\mathrm{EF}\phi_2))$.

CONCLUDING REMARK

In this paper, we construct a logic, Interval Temporal Logic (ITL), to represent behaviors of real-time systems. In the logic ITL, we construct a proof rule for responsiveness assertions, which can be used to reason about real-time properties. Given a program P identified with a theory Σ, we say that P *satisfies the specification* ϕ iff $\Sigma \models \phi$, where ϕ is a formula of ITL. This is an application of the model theory of the logic ITL to a program P.

Currently we only investigate soundness and relative completeness of the Progress Rule for the reasoning of responsiveness assertions. Future research will examine other important formulas and proof rules that may be derived and added into the logic ITL.

REFERENCES

[BeSl71] Bell, J. L. and Slomson, A. B., *Models and Ultraproducts: An Introduction,* North-Holand Publishing Company, Amsterdam, 1971.

[HaLi90] Harel, Eyal, Lichtenstein, Orna and Pnueli, Amir "Explicit clock temporal logic," *5th IEEE Symposium on Logic in Computer Science*, pp.402-413, 1990.

[MaPn89] Manna, Z. and Pnueli A. "Completing the temporal picture," *Lecture Notes in Computer Science #372, Automata. language and programming*, pp.534-558, 1989.

[PnHa88] Pnueli, A. and Harel, E. "Applications of temporal logic to the specification of real time systems," *Lecture Notes in Computer Science 331*, pp. 84-98, 1988.

[PePn90] Peled, D. and Pnueli, A. "Proving Partial Order Liveness Properties," *17th Colloquium on Automata, Language and Programming*, edited by M.S. Peterson, pp.553-571, 1990.